Linux - Installation d'un serveur proxy Squid

Objectif : mise en œuvre d'un serveur proxy

Présentation

Pour accéder à l'internet, différentes solutions sont envisageables :

- *Un* **routeur/NAT**
- *Un serveur* **proxy** *: Squid est un proxy-cache (serveur* **mandataire***) sous Unix. Il permet d'accélérer les requêtes sur l'internet en plaçant en cache les pages web les plus demandées ce qui permet d'économiser de la bande passante. Il permet aussi d'effectuer du filtrage (entrant ou sortant). Attention, il fonctionne uniquement avec les protocoles HTTP, HTTPS et FTP (protocoles sans connexion) . Squid n'est pas un proxy POP, IMAP, SMTP, NNTP : pour utiliser ces protocoles, il faudra utiliser la translation d'adresse (***NAT***) au niveau du noyau (iptables). Cette fonctionnalité est fournie par la plupart des couches de pare-feu.*

Comparatif routeur/NAT et serveur proxy

	Routeur NAT	**Proxy**
Niveau OSI	3/4 (Réseau/Transport)	7 (Application)
Capacité de filtrage	Limitée	Oui : très élaborée (adresse, domaines, entrant/sortant, mots clés, authentification, ...)
Économie de bande passante	Non	Oui (entre 10 et 30%)
Configuration clients	Passerelle par défaut (DHCP)	Navigateur (adresse + port)
Configuration machine	Simple	+ complexe
Protocoles utilisables	Tous	HTTP/HTTPS, FTP
Possibilités de logging	Aucune	Etendues

Squid

*C'est actuellement le standard en matière de serveur proxy***.**
La version courante est la 3 mais la 2 est encore utilisée.

Où trouver Squid

Squid est disponible dans toutes les distributions Linux. On peut aussi le télécharger sur le site de Squid (*http://www.squid-cache.org*). *On le trouve sous forme de fichiers tar.gz (sources) ou binaires (deb ou rpm).*

Avant l'installation

Squid n'est pas très exigeant en termes de ressources CPU (un Pentium à partir de 300 MHz peut suffire). Pour ce qui est de la mémoire, 128 Mo semble être le minimum. A propos des disques, les disques SCSI sont beaucoup plus performants que les disques IDE.
D'autre part, il est fortement recommandé de créer une partition **/var** *de taille suffisante (entre 1 et 4 Go) car squid met par défaut son cache dans le répertoire* **/var/spool**. *Les logs, de taille assez importante sont également stockés ans ce répertoire.*
Il peut être judicieux d'utiliser pour cette partition un système de fichiers journalisé (ext3/4, XFS) permettant de redémarrer assez rapidement après un arrêt non prévu.
Bien sûr, il faudra la plupart du temps une deuxième carte réseau même si le proxy peut fonctionner avec une seule carte réseau.
La configuration de la pile IP devra être correcte, en particulier l'adresse de la passerelle par défaut ainsi que le fichier **/etc/resolv.conf** *(adr. du serveur DNS et nom de domaine pour que la* **résolution de noms** *soit opérationnelle).*

Installation de Squid

Avec les rpm, taper pour une Mandriva : **urpmi squid***, avec une Debian, taper* **apt-get install squid3**
Il place alors les fichiers de log dans **/var/log/squid***, le fichier de configuration dans /***etc/squid/squid.conf***. Ce fichier est le seul fichier de configuration de squid. Il faut donc éditer ce fichier pour effectuer les paramétrages correspondant à*

la situation locale.

Lancement arrêt de Squid

- *service squid start : lance squid*
- *service squid stop*
- *service squid status*
- *service squid restart*
- *service squid reload : reprend en compte le nouveau fichier de configuration*

avec une Debian : **/etc/init.d/squid start | stop | restart | reload**

Configuration de Squid

Toute la configuration de Squid se trouve dans le fichier **squid.conf** *situé dans* **/etc/squid/** *ou /usr/local/squid/etc.*

Le fichier squid.conf est très violumineux avec de nombreux commentaires et doit être adapté à la situation locale.
La plupart des options par défaut du fichier squid.conf ne sont pas à changer (vous pouvez alors laisser le # pour conserver les options par défaut).

http_port*: le port à utiliser. Le plus fréquent est 8080. Par défaut Squid utilise 3128.*

icp_port *: Conserver le port 3130. Ceci permet de communiquer avec des proxy-cache parents ou voisins.*

cache_mem *: correspond au cache mémoire, la valeur dépend de la machine. Par défaut squid utilise 8 Mo. Cette taille doit être la plus grande possible afin d'améliorer les performances (Considérez 1/3 de la mémoire que vous réservez à Squid). Il faut avec cache_mem régler cache_mem_low et cache_mem_high qui sont les valeurs limites de remplissage du cache mémoire. Par défaut les valeurs sont 75 % et 90 %. Lorsque la valeur de 90 % est atteinte le cache mémoire se vide jusqu'à 75 %. Les valeurs par défaut sont bien adaptées dans la plupart des cas.*

cache_peer : *permet de décrire les proxy parents pour la mise en cascade*

cache_swap *: correspond à la taille du cache disque. Si la taille du disque le permet, et en fonction de la taille de l'entreprise (nombre de clients), mais aussi de la durée de rafraîchissement et du débit de la ligne, vous devez mettre la valeur qui vous semble correspondre à votre situation.*

acl QUERY urlpath_regex cgi-bin \? \.cgi \.pl \.php3 \.asp *: Type de page à ne pas garder dans le cache afin de pas avoir les données d'un formulaire par exemple.*

maximum_object_size *: taille maximale de l'objet qui sera sauvegardé sur le disque. On peut garder la valeur par défaut.*

cache_dir *: indiquer ici le volume du cache. On peut utiliser plusieurs fois cette ligne.*
cache_dir ufs /cache1 100 16 256 (cache de 100 Mb)

cache_dir ufs /cache2 200 16 256 (cache de 200 Mb)
Placer de préférence le cache sur une partition spécifique.

cache_access_log *; cache_log ; cache_store_log : Indique l'endroit ou se trouve les logs. Si vous ne souhaitez pas avoir de log (par exemple des objets cache_store_log) indiquer cache_store_log none.*

dns_children *: Par défaut le nombre de requêtes dns est de 5. Il peut être nécessaire d'augmenter ce nombre afin que Squid ne se trouve pas bloqué. Attention de ne pas trop l'augmenter, cela pouvant poser des problèmes à la machine (indiquer 10 ou 15).*

request_size *: Taille maximale des requêtes. Conserver la valeur par défaut, concerne les requêtes de type GET, POST..*

refresh_pattern *: Permet de configurer la durée de mise à jour du cache. Utiliser -i pour ne pas tenir compte des minuscules/majuscules. (voir le fichier squid.conf). Les valeurs Min et Max sont indiquées en minutes.*

visible_hostname *: indiquer ici le nom de votre serveur monproxy.mondomaine.fr*

dns_testnames *: Conserver les valeurs par défaut ou indiquer ns1.nic.fr*

logfile_rotate *: Pour faire tourner les logs et garder un nombre de copies. Par défaut 10, attention si le cache est très utilisé il peut générer un grand volume de logs, penser donc à réduire ce nombre.*

error_directory *: Pour avoir les messages d'erreur en français (indiquer le répertoire où ils se trouvent).*

Le contrôle d'accès : les ACL (Access Control List)

Pour contrôler tout ce qui passe par le cache, on doit utiliser les **ACL** *(Access Control List). Elles ont donc deux grandes fonctionnalités : contrôler qui a le droit d'utiliser le cache et les requêtes autorisées.*

On peut interdire/autoriser en fonction :

- *du domaine (source et/ou destination),*
- *du protocole,*
- *de l'adresse IP (source et/ou destination) ,*
- *du numéro de port,*
- *d'un mot,*
- *d'une période*
- *….*

Syntaxe d'une ACL :

acl aclname acltype string[string2]
http_access allow|deny [!]aclname
icp_access allow|deny [!]aclname

acltype *peut prendre les valeurs suivantes :*

- **src** *(pour la source) : adresse IP du client sous la forme adresse/masque. On peut aussi donner une plage d'adresse sous la forme adresse_IP_début-adresse_IP_fin*
- **dst** *(pour la destination) : idem que pour src, mais on vise l'adresse IP de l'ordinateur cible.*
- **srcdomain** *: Le domaine du client*
- **dstdomain** *: Le domaine de destination.*
- **url_regex** *: Une chaîne contenue dans l'URL (on peut utiliser les jokers $).*
- **urlpath_regex** *: Une chaîne comparée avec le chemin de l'URL (on peut utiliser les jokers).*
- **proto** *: Pour le protocole.*
- *...*

Remarque *: l'utilisation des ACL se fait en* **deux phases** *:*

- *la* **déclaration d'ACL** *(phase de définition de l'ACL). Exemple :* **acl pasbien dstdomain skyblog.com**
- *l'***utilisation de l'ACL** *. Exemple :* **http access deny pasbien**

Principe d'utilisation des ACL

Les ACL sont évaluées successivement dans l'ordre *jusqu'à ce qu'une expression soit vérifiée, auquel cas on arrête l'évaluation.*
Il faudra donc veiller à ce que la dernière expression soit du type http_access deny all

Exemple

http_access deny sitesinterdits
http_access allow reseauadmin
http_access deny ! heuresouvrables
http_access allow monreseau
http_access deny all

Il est possible d'utiliser le **et** *logique en mettant plusieurs ACL sur la même ligne : allow compta heuresouvrables*

Exemples :

- *Interdire l'accès à un domaine*

Supposons que nous souhaitions interdire l'accès à un domaine (par exemple le domaine tresglauque.com). On a donc

acl niet dstdomain tresglauque.com
http_access deny niet
http_access allow all

La dernière ligne ne doit exister qu'une fois dans le fichier squid.conf.

- *Interdire l'accès aux pages contenant les mots sexe* **ou** *porn.*

acl sexe url_regex –i sexe porn
http_access deny sexe

http_access allow all (Une seule fois à la fin des ACL).

Attention **url_regex** *est sensible aux majuscules/minuscules à moins d'ajouter l'option* **-i**. *On peut placer un nom de fichier à la place d'une série de mots ou d'adresses, pour cela donner le nom de fichier entre guillemets. Chaque ligne de ce fichier doit contenir une entrée.*

 # URL interdites
acl url_interdites url_regex "/usr/local/squid/etc/denied_url"
http_access deny url_interdites

- *Interdiction des mp3*

acl no_mp3 url_regex –i mp3$ # interdit les requêtes qui se terminent par **mp3**

Des produits associés à Squid permettent un contrôle plus simple (Squid n'a pas vocation à contrôler de nombreux sites). **SquidGuard** *permet d'interdire des milliers de sites. La base de données comportant plusieurs dizaines de milliers de sites interdits est entretenue par le rectorat de l'académie de Toulouse.*

Utilisation de Squidguard : http://doc.ubuntu-fr.org/tutoriel/comment_mettre_en_place_un_controle_parental

Pour contrôler qui a le droit d'utiliser le cache, créer une ACL du type :

acl mon_lycee src 192.168.0.0/24
http_access allow localhost
http_access allow mon_lycee
http_access deny all

Il est possible d'ajouter autant d'ACL qu'on le souhaite. Par exemple, si la configuration comporte plusieurs réseaux, 192.168.1.0/24 peut être modifié en fonction du plan d'adressage (jouer sur le masque).

*Il est maintenant possible d'utiliser une application (***dansguardian***) qui permet d'utiliser un filtrage plus élaboré sur le contenu (META ou texte de la page, mots clés). Attention toutefois aux problèmes de performances pour les proxy servant de nombreux clients : le proxy doit alors analyser chacune des pages en transit ...*

L'authentification

Il est souvent nécessaire d'autoriser l'accès à l'internet de manière différente selon les machines et les personnes.

La première consiste à contrôler les accès par machine (par adresse IP ou en fonction des noms de machine si l'on dispose d'un serveur DNS).

La deuxième solution est de contrôler en fonction des individus. Squid permet de le faire de plusieurs façons : avec le programme **ncsa_auth,** *par un serveur SMB/NT ou encore par un annuaire LDAP . L'authentification* **ncsa** *consiste à utiliser les couples utilisateurs/mots de passe situés dans un fichier comme avec Apache (utiliser htpasswd) . Il faudra utiliser la clause REQUIRED dans les ACL. Voir la documentation.*

Les modes d'authentification utilisables

- **LDAP***: Utilise un annuaire LDAP*
- **NCSA***: Utilise l'authentification NCSA*
- **MS/NT***: Uses a Windows NT authentication domain.*
- **PAM***: Utile les modules Linux Pluggable Authentication Modules .*
- **SMB***: Utilise un serveur SMB (Windows NT ou Samba)*
- **getpwam***: mots de passe unix ancienne version.*
- **sasl***: utilise les librairies SASL.*
- **winbind***: authentification Samba dans un domaine Windows NT (intéressant quand les comptes sont déjà créés)*

Authentification

acl mdp proxy_auth REQUIRED # authentification requise
acl all src 0/0
http_access allow mdp
http_access deny all

auth_param basic program /usr/lib/squid3/bin/ncsa_auth /etc/squid3/passwd

On utilise le programme **ncsa_auth** *et le fichier de mots de passe* **/etc/squid3/passwd**

Exemple d'utilisation au Lycée Mathias

Accès direct aux postes prof
acl STATIONDIRECT srcdomain /etc/squid/stationdirect

Pour les postes élèves : *Authentification ncsca*
acl ELEV proxy_auth REQUIRED

auth_param basic program /usr/bin/ncsa_auth /etc/squid/passwd

Les mots de passe sont stockés dans un fichier passwd spécifique (comme Apache, utiliser htpasswd). Le fichier passwd est construit en fonction des groupes et des heures
Il est possible d'authentifier par un PDC NT ou un serveur LDAP.

Interface web de Squid

Squid dispose en standard d'un script cgi qui donne des informations sur l'utilisation du cache. Pour cela il faut avoir Apache et placer **cachemgr.cgi** *dans cgi-bin puis le rendre exécutable.*
Ensuite, avec un navigateur, taper l'URL suivant : http://machine/cgi-bin/cachemgr.cgi

Interface web pour configurer Squid

Le plus simple est d'utiliser Webmin qui dispose d'un module de configuration de squid

Les logs de Squid

On peut surveiller les logs à l'aide de la commande tail -f access.log (les logs de Squid se trouvant dans le répertoire **/var/log/squid** *ou /usr/local/squid/log.*
access.log *donne les informations sur les requêtes qui ont transité par Squid.*
cache.log *informe sur l'état du serveur depuis son démarrage.*
store.log *informe sur les objets stockés dans le cache (peu utile)*
Voici les valeurs contenues dans le fichier access.log. Les codes commençant par TCP_ sont les requêtes sur le port 8080:

TCP_HIT	*Une copie valide se trouve dans le cache*
TCP_MISS	*Pas dans le cache*
TCP_REFRESH_HIT	*Objet dans le cache, mais périmé. Squid demande au serveur d'origine si une nouvelle version est disponible, la réponse étant pas de nouvelle version*
TCP_REF_FAIL_HIT	*Objet dans le cache, mais périmé. Squid demande une mise à jour, mais n'obtient pas de réponse du serveur. Il renvoie alors l'ancienne version.*
TCP_REFRESH_MISS	*Objet dans le cache, mais périmé. Squid demande une mise à jour qu'il reçoit*
TCP_CLIENT_REFRESH	*Le client envoie une requête avec une demande de ne pas utiliser le cache. Squid forwarde la requête. (transmet)*
TCP_IMS_HIT	*Le client demande une mise à jour, et l'objet est dans le cache et est récent. Squid ne forwarde pas la requête.*
TCP_IMS_MISS	*Le client demande une mise à jour. Squid forwarde la requête.*
TCP_SWAPFAIL	*Problème de swap. L'objet semble être dans le cache mais n'est pas accessible. La requête est forwardée.*
TCP_DENIED	*Accès est dénié. Pas les bons droits au début*

UDP_ sont des codes sur le port ICP:

UDP_HIT	*Une copie récente de la copie est dans le cache*
UDP_HIT_OBJET	*Idem que UDP_HIT, mais l'objet est envoyé dans un paquet UDP*
UDP_MISS	*Objet pas dans le cache ou périmé*
UDP_DENIED	*Accès interdit pour cette requête*
UDP_INVALID	*Requête invalide*
UDP_MISS_NOFETCH	*La requête n'a pas était faite à temps (arrêt ou démarrage du serveur)*

ERR_ sont des codes d'erreurs. Ils sont trop nombreux pour être traités ici.
Codes Hiérarchiques

DIRECT	*Squid forwarde directement la requête au serveur d'origine*
FIREWALL_IP_DIRECT	*Squid forwarde la requête directement au serveur d'origine, parce que le serveur d'origine est derrière un Firewall*
FIRST_UP_PARENT	*Squid forwarde la requête au premier parent disponible de la liste*
LOCAL_IP_DIRECT	*Squid forwarde directement la requête au serveur d'origine car l'adresse correspond à une adresse locale*
SIBLING_HIT	*Squid forwarde la requête à un cache sibling qui a envoyé un UDP_HIT*
NO_DIRECT_FAIL	*Squid ne peut pas forwarder la requête parce qu'un firewall l'interdit ou il n'y a pas de cache parent.*
PARENT_HIT	*Squid forward la requête à un cache parent qui a envoyé un UDP_HIT*
SINGLE_PARENT	*La requête est forwardée à un cache parent approprié pour cette requête. Il faut que le single_parent_bypass soit actif.*
SOURCE_FASTEST	*Squid forwarde la requête au serveur d'origine car la requête à ce serveur source_ping arrive plus vite.*
PARENT_UDP_HIT_OBJ	*Squid reçoit la réponse dans un UDP_HIT_OBJ du cache parent.*
SIBLING_UDP_HIT_OBJ	*Squid reçoit la réponse dans un UDP_HIT_OBJ du cache sibling.*
DEFAULT_PARENT	*Squid forwarde la requête à un cache parent par défaut sans envoyer une requête ICP avant.*
ROUNDROBIN_PARENT	*Squid forwarde la requête à un cache parent round-robin, sans envoyer de requête ICP avant*
CLOSEST_PARENT_MISS	*Squid forwarde la requête à un cache parent* *N'existe que si query_icmp est déclaré dans le fichier de configuration.*
NONE	*Squid ne forwarde aucune requête*

Produire des statistiques à partir des logs

Les produits les plus connus sont **Prostat** *et* **Calamaris** *mais il en existe d'autres. Ils sont tous les deux disponibles sur l'internet.*

Remarque : l'exploitation

Squid peut produire selon le nombre de clients connectés un volume de logs très importants (souvent 40 Mo/jour au Lycée Le Castel). Il conviendra donc de prévoir une partition spécifique pour le stockage des logs (/var ou /var/log) et de s'assurer de la configuration du démon **logrotate** *chargé de la rotation des logs (habituellement 1 rotation /semaine avec 4 semaines d'historique).*

Caches hiérarchiques **peu utilisé maintenant**

Squid est capable de "discuter" avec d'autres proxy cache, à l'aide de ICP (Internet Cache Protocole) sur un port particulier (3130 UDP par défaut). On peut ainsi cascader un certain nombre de caches.
Il faut pour cela dans le fichier de configuration de Squid, valider la ligne :
cache_peer type http_port icp_port options

Pour le type, on a comme possibilité :
parent *: Le cache ainsi défini contacte le cache parent et attend la réponse via ICP, si le cache parent ne possède pas la réponse il se la procure et la fait suivre au cache demandeur.*
sibling *: Le cache contact le cache parent, si celui ci n'a pas la réponse, le cache enfant se procure directement la page. Celle ci n'est pas chargée sur le cache parent.*

Pour http_port et icp_port utiliser 8080 et 3130, mais cela n'est pas obligatoire.

Pour les options on dispose des options suivantes :
proxy-only *: On indique à l'aide de cette option que les données envoyées par le proxy interrogé ne sont pas dans le cache local.*
weight *: pour avoir une pondération entre plusieurs caches*
no-query *: Afin de ne pas envoyer de requêtes ICP au proxy indiqué.*
round-robin *: Utiliser pour répartir la charge entre plusieurs proxy.*

Configuration des clients

La configuration de clients est plus lourde que pour le routage/NAT (passerelle et DNS suffisent) : il faut également indiquer au navigateur **l'adresse** *et le* **port** *du serveur proxy.*
Pour configurer les clients, on peut utiliser la configuration manuelle (cf. plus haut) ou la configuration automatique avec WPAD pour IE5.0 (cf sur l'internet)

Exemple de configuration automatique (mode WPAD) pour des navigateurs IE 5.0 + :

- *un serveur DNS doit être installé*
- *un* **ALIAS DNS** *appelé* **WPAD** *doit être créé et doit pointer sur une machine hébergeant un serveur web*
- *le client disposant du navigateur IE 5 et utilisant le serveur DNS*
- *sur la racine du serveur web , créer le fichier suivant et le sauvegarder sous le nom* **wpad.dat**

```
function FindProxyForURL(url, host)
{
if (isPlainHostName(host)                              # nom de machine sans nom de domaine
       || dnsDomainIs ( host,".mondomaine.fr")         # fait partie de mondomaine.fr (domaine local)
       || isInNet (host,"192.168.1.0/255.255.255.0"))#  adresse IP locale
       return "DIRECT";                                # ne pas utiliser le proxy
else return "proxy.mondomaine.fr:8080");               # sinon on utilise le proxy ( port 8080)
}
```

- *tester le client (vérifier que l'on utilise bien la configuration automatique et examiner les logs d'Apache pour s'assurer que le client récupère bien le wpad.dat)*

Le proxy transparent (compléter l'énoncé : présence d'un routeur …)

Il est possible d'utiliser le **proxy transparent** *pour que les clients n'aient pas à configurer spécifiquement leur navigateur. Le principe est le suivant : on redirige les requêtes arrivant sur le port 80 du proxy pour les transférer sur le port d'écoute du proxy (par exemple 3128 ou 8080) et forcer le passage à travers le proxy. La redirection des ports se fait avec i***ptables/netfilter.**

Le proxy transparent présente également l'intérêt de **forcer le client à utiliser le proxy** *: on peut donc mettre en place des règles de filtrage et d'autre part les clients laissent obligatoirement des traces dans les logs.*

Remarque : *le proxy transparent fait* **mauvais ménage** *avec les* **systèmes d'authentification** *: on devra choisir l'un ou l'autre.*

 # Modification du fichier squid.conf

http_port 3128 transparent

Les règles iptables

```
# Règles iptables
# On nettoie la table nat sur la chaîne PREROUTING en entrée
# On utilise le port 3128,  utilisé par défaut par Squid.
iptables -t nat -F PREROUTING

# ou toutes les chaînes de la table nat
iptables -t nat -F

# On laisse passer (en masquant en sortie) les requêtes autres que sur le port 80
 iptables -t nat -A POSTROUTING -j MASQUERADE

# On redirige les requêtes arrivant sur le port 80 vers le port 3128
iptables -t nat -A PREROUTING -j DNAT -i eth1 -p TCP --dport 80 --to-destination 192.168.0.1:3128
```

Supprimer toute configuration de proxy sur le client. Tester.

En conclusion

Squid est le serveur proxy de référence, il est très fiable, très utilisé et très modulable. Une version 3.0 est disponible. Des schémas d'authentification très complexes sont utilisables. La documentation, y compris en français est très vaste et les logiciels annexes sont très nombreux et puissants.

Selon les cas de figure, il est fréquent qu'il soit associé à une solution de routage/NAT pour prendre en compte les protocoles autres que HTTP/HTTPS/FTP.

Quelques liens

- *le site de Squid : squid-cache.org*
- *l'aide Ubuntu : help.ubuntu.com*
- *ubuntu-fr.org*

Exemple de configuration de base

- *couche réseau opérationnelle (passerelle, DNS : fichiers /etc/hosts, /etc/resolv.conf et /etc/network/interfaces (Debian)*
- *fichier /etc/squid/squid.conf :*

```
http_port 8080                  # on écoute sur le port 8080
acl  localnet src 192.168.0.0/24  # à ajouter à la fin de la partie de déclaration des ACL
http_access allow localnet      # à insérer avant la règle finale http_access deny all
```

Exercices

- *Installer squid (**squid3**)*
- *Mettre en place une configuration de base (écoute sur le port 8080, accès limité au réseau local)*

Squid - cache parent

- pour cascader un serveur proxy Squid sur le proxy Squid du BTS SIO, il est nécessaire d'utiliser **cache_peer** avec les options suivantes dans le fichier `squid.conf` (10.121.38.1 représentant le proxy parent) :

```
...
cache_peer 10.121.38.1 parent 8080 0 no-query default
...
never_direct allow all
...
```

- *Tester avec un client web et examiner les logs (/var/log/squid/access.log)*
- *Mettre en place le filtrage pour interdire des mots clés (tf1, ,,,)*
- *Autoriser les mots-clés pour une adresse IP (poste) donnée*
- *Mettre en place une authentification (ncsa, msnt, ntml)*
- *Mettre en place le transparent proxy*
- *Mettre en place la configuration automatique des navigateurs*