Mise en place d'un proxy Squid avec authentification Active Directory

Dans ce tutoriel nous allons voire la mise en place d'un proxy Squid avec une authentification transparente pour les utilisateurs d'active directory, l'intérêt de la manœuvre c'est que les utilisateurs n'auront pas besoin d'entrer de login et de mot de passe pour accéder à internet, il suffit juste de se loguer sous une session windows.

Notre test pour la mise en place de cette solution est effectué sur Ubuntu serveur 9.10 32 bits

Nota :

- Pensez à respecter la casse très important sous linux (Majuscule minuscule)
- Pensez à faire des sauvegardes de vos fichiers de conf : *cp* `nomdufichier nomdufichier.old`

Avant de commencer

- Avoir un réseau Windows
- Un contrôleur de domaine sous Windows serveur 2003
- Un domaine active directory
- Un poste pour Squid avec Ubuntu server dans notre cas

1. **Intégration de la machine au domaine**

    - Le nom de domaine : **domain.local**
    - Le nom du contrôleur de domaine : **dc**
    - Le compte administrateur : **Admin**
    - Le nom de la machine Squid : **SquidProxy**

(Ces valeurs sont à titre d'exemple elles devront être remplacé par vos valeurs)

Pour rejoindre le domaine nous allons devoir installer les paquets suivants :

- **samba** qui permet de faire le lien entre Windows et Linux
- **krb5-user** et **libpam-krb5** des librairies lié a Kerberos, le protocole d'authentification utilisé par active directory
- **ntpdate** pour synchroniser l'heure
- **winbind** le composant de samba communiquant avec active directory

Pour installer les différents paquets nous utiliserons la commande : `aptitude install`

Lors de l'installation de krb5 il vous sera demandé d'entrer le nom du serveur de domaine et du serveur administratif saisissez donc **dc**

Capture 1

Pour des raisons de sécurité Kerberos nécessite que l'heure locale soit synchronisée avec votre DC :

```
ntpdate ip_de_votre_dc
```

Vous pouvez vérifier que la date est l'heure de votre proxy soit synchronisé avec votre contrôleur de domaine :

AdminLor

```
date
```

Configurer Kerberos

Nous allons éditer le fichier /etc/krb5.conf pensez à sauvegarder le fichier de base. Entrer que le contenue suivant :

```
[libdefaults]
        default_realm = DOMAINE.LOCAL
        clock_skew = 300
        ticket_lifetime = 24000
        default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
        default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
        dns_lookup_realm = false
        dns_lookup_kdc = true
[realms]
        DOMAINE.LOCAL = {
                kdc = dc.DOMAINE.LOCAL
                admin_server = dc.DOMAINE.LOCAL
                default_domain = DOMAINE.LOCAL
                }
[domain_realm]
        .domaine.local = DOMAINE.LOCAL
         domaine.local = DOMAINE.LOCAL
```

Testons nos paramètres Kerberos avec la commande :
`kinit Admin` ensuite entrer le mot de passe de votre administrateur du DC

Avec la commande `klist` nous pouvons voire les tickets Kerberos en cache.

Pour procéder aux étapes suivante nous allons devoir couper les daemons Samba et Winbind avec les commandes suivantes :

```
/etc/init.d/winbind stop
/etc/init.d/samba stop
```

Maintenant à la configuration de Samba direction /etc/samba/smb.conf avant d'apporter les modifications on n'oubli pas de sauvegarde le fichier d'origine. Ne mettre que le contenue suivant :

```
[global]
   workgroup = DOMAINE
   realm = DOMAINE.LOCAL
   security = ads
   encrypt passwords = yes

   password server =dc. domaine.local

   idmap uid = 10000-20000
   idmap gid = 10000-20000
   winbind enum groups = yes
   winbind enum users = yes
   winbind use default domain = yes
```

Il nous faut maintenant redémarrer nos deux services

```
/etc/init.d/samba start
/etc/init.d/winbind start
```

AdminLor

Ensuite nous allons rejoindre le domaine avec la commande :
```
net ads join –U Admin
```

Maintenant effectuons une petite batterie de test afin de vérifier que tous va bien

`net ads testjoin` qui devrait nous retourner *`Join is OK.`*

Afficher la liste des groupes d'active directory
```
wbinfo –g
```

Afficher la liste des utilisateurs de l'AD
```
wbinfo –u
```

Si les commandes ne retourne pas les résultats attendu c'est que vous devez avoir une erreur dans le fichier **smb.conf**, n'oubliez pas de redémarrer Winbind à chaque modification du fichier.

Voilà notre machine à rejoint le domaine active directory

2. Installation et configuration du proxy Squid

Dans un premier temps on installe le paquet **Squid**
```
aptitude install squid
```

Testons la connexion au DC :
```
/usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic
```
Entrer un utilisateur et mot de passe d'un utilisateur de votre AD
```
Utilisateur mot_de_passe
```
Vous devriez avoir **Ok** comme réponse ctrl + c pour quitter

Maintenant éditons le fichier **/etc/squid/squid.conf** qui est le fichier de configuration de Squid, après avoir fait la sauvegarde du fichier d'origine.

Dans la partie TAG: auth_param entrez uniquement les lignes suivante :

```
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-
ntlmssp
auth_param ntlm children 5
auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-
basic
auth_param basic children 5
auth_param basic realm Squid AD
auth_param basic credentialsttl 2 hours
```

```
Pour autoriser l'accès à internet juste  à un groupe spécifique de votre
active directory il faut ajouter le paramètre require-membership-of au
ligne ci-dessus.
```

```
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-
ntlmssp --require-membership-of=DOMAINE.LOCAL\\groupead
```

```
auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-
basic --require-membership-of=DOMAINE.LOCAL\\groupead
```

Dans la partie TAG: acl ajoutez les lignes suivantes :

```
acl ntlm proxy_auth REQUIRED
```

Dans la partie TAG : http _access mettez uniquement la ligne suivante :

```
http_access allow ntlm
```

Dans la partie TAG : append_domain :

```
append_domain .domaine.local
```

Nous pouvons maintenant redémarrer Squid :

```
/etc/init.d/squid restart
```

L'utilisateur proxy de Squid nécessite d'appartenir au groupe root pour bénéficier des droits nécessaire sur les fichiers de log de squid, nous allons remédier à cela de manière à rendre l'authentification fonctionnelle :

```
chown –R proxy :root /var/log/squid
```

Voilà nous avons un proxy fonctionnel vous pouvez le vérifier en entrant manuellement dans votre navigateur web les paramètres proxy l'adresse IP se de votre proxy avec le port 3128.

3. Installation d'une solution de filtrage SquidGuard

Un proxy c'est bien beau, mais seul il perd un peu d'utilité, nous allons voire maintenant comment installer une solution filtrage afin de nous permettre de filtrer l'accès à certain sites ou catégories de site à partir d'une blacklist française.

On repart au charbon, en commençant par installer SquidGuard :

```
aptitude install squidguard
```

Ensuite nous allons mettre en place notre blacklist, nous utiliserons la blacklist mis à disposition gracieusement par L'Université Toulouse 1 Capitole qui diffuse depuis quelques années une liste noire d'URLs, gérée par Fabrice Prigent.

```
cd /tmp
wget ftp://ftp.univ-
tlse1.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz
tar zxvf blacklists.tar.gz -C /var/lib/squidguard/db/
cd /var/lib/squidguard/db
mv blacklists/* .
rm -rf blacklists
```

On passe à la configuration, dans un premier temps il faut configurer le fichier **/etc/squid/squid.conf**

```
url_rewrite_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf
url_rewrite_children 15
```

Nous allons éditer le fichier squidGuard.conf avec une configuration basique, juste de façon à comprendre comment le mettre en place, après vous l'affinerez selon vos besoins.
Supposons que nous avons un réseau adresser de la manière suivante 192.168.1.0/24 que nous voulons restreindre toutes les adresse de se réseau sauf l'administrateur qui à une adresse fixe 192.168.1.10 admettons.

Le fichier de configuration est **/etc/squid/squidGuard.conf** avant de faire les modifications on n'oubli pas de sauvegarder le fichier d'origine.

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard/db
logdir /var/log/squid

# Définition des sources :

src admin {
ip 192.168.1.10
}

src reseau {
ip 192.168.1.1-192.168.1.254
}


# Définition de la base de filtrage utilisée, ses catégories sont à titre
d'exemple vous pouvez en ajouter selon vos besoins ou en supprimer

dest adult {
        domainlist adult/domains
        urllist adult/urls
}

dest warez {
        domainlist warez/domains
        urllist warez/urls
}

dest porn {
        domainlist porn/domains
        urllist porn/urls
}

dest violence {
        domainlist violence/domains
        urllist violence/urls
}


# Définition des ACL

acl {

#on déclare déjà le groupe default qui correspond à tous se qui ne rentre
pas dans les destinations définit plus haut, dans se cas nous bloquons tous
default {
        pass none
        redirect http://mon_serveur_proxy/page_bloque.html
}

#On définit les accès pour l'administrateur accès à tous sauf porn et adult
admin {
        pass !porn !adult !warez all
        redirect http://mon_serveur_proxy/page_bloque.html
}
```

```
#On définit les accès pour le réseau
reseau {
        pass !porn !adult all
        redirect http://mon_serveur_proxy/page_bloque.html
}

}
```

Cette configuration est juste à titre d'exemple, à noter que l'ont peut aussi bloquer ou autoriser l'accès à certaines catégories de site en fonction de tranche horaires regarder l'exemple ci-dessous :

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard/db
logdir /var/log/squid

# Définition des sources :

# s = sun = dimanche, m = mon = lundi, t =tue = mercredi, w = wed = mercredi, h =
thu =jeudi, f = fri = vendredi, a = sat = samedi
# je définis les plages horaires travaillé
time workhours {
     weekly mtwhf 06:00-12:00 14:00-22:00
}

src reseau {
ip 192.168.1.1-192.168.1.254
}


# Définition de la base de filtrage utilisée, ses catégories sont à titre
d'exemple vous pouvez en ajouter selon vos besoins ou en supprimer

dest adult {
        domainlist adult/domains
        urllist adult/urls
}

dest warez {
        domainlist warez/domains
        urllist warez/urls
}

dest porn {
        domainlist porn/domains
        urllist porn/urls
}

dest violence {
        domainlist violence/domains
        urllist violence/urls
}

}

dest games {
        domainlist games/domains
```

```
        urllist games/urls
}


# Définition des ACL

acl {

#on déclare déjà le groupe default qui correspond à tous se qui ne rentre
pas dans les destinations définit plus haut, dans se cas nous bloquons tous
default {
        pass none
        redirect http://mon_serveur_proxy/page_bloque.html
}


#On définit les accès pour le réseau
Reseau within workhours {
        #Dans les horaires définit
        pass !porn !adult !warez !violence !games all
        redirect http://mon_serveur_proxy/page_bloque.html
}
else {
        #Horaires non définit
        pass !porn !adult !warez !violence all
        redirect http://mon_serveur_proxy/page_bloque.html
}

}

}
```

Pour terminer il nous faut faire une petite modification sur le répertoire db :

```
chown –R proxy :root /var/lib/squidGuard/db
```

Et enfin généré la base de données :

```
squidGuard.conf –C all
```

Cette commande prend beaucoup de temps à s'effectuer donc pas de panique si vous trouvez sa long c'est normal, vous pouvez vérifier si il y a des erreurs sur ce fichier **/var/log/squid/squidGuard.log** en général se sont des erreurs de frappe comme par exemple :

init domainlist /var/lib/squidguard/db/adlut/domains
Error db_open: No such file or directory

Ici nous pouvons voire une erreur de frappe sur adult au lieu de adult pour la corriger il suffit de faire la modification dans le fichier **/etc/squid/squidGuard.conf**

La redirection est très importante pour interdire l'accès `redirect http://mon_serveur_proxy/page_bloque.html` sans elle nous pouvons quand même accéder à des sites interdit, le proxy ne savant pas ou vous rediriger vous envoi vers la page demandé même si elle est censé être filtré c'est pourquoi nous allons voire comment mettre en place notre propre redirection.

AdminLor

Dans un premier temps il vous faut un serveur http fonctionnel, je vais partir dans le cas ou nous n'avons pas de serveur http. Nous allons donc mettre en place un serveur http apache sur notre proxy, avec la commande suivante :

```
aptitude install apache2
```

SquidGuard nous fournit des scripts cgi pour les redirections alors pourquoi s'en priver, nous allons récupérer l'un de ses scripts et le placer dans le répertoire de stockage apache des scripts :

```
cp /usr/share/doc/squidguard/examples/squidGuard.cgi.gz /usr/lib/cgi-bin/
```

Ensuite il faut le décompresser :

```
gunzip -d /usr/lib/cgi-bin/squidGuard.cgi.gz
```

Enfin changer l'appartenance et les droits sur notre script :

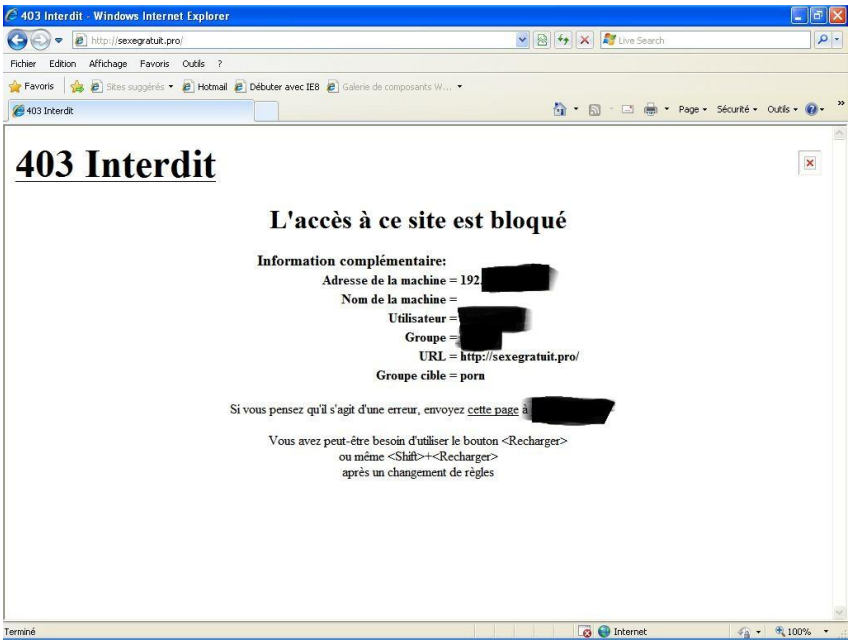
```
chown www-data /usr/lib/cgi-bin/squidGuard.cgi
chmod 700 /usr/lib/cgi-bin/squidGuard.cgi
```

Voilà maintenant tous est en place, il faut éditer le fichier /etc/squid/squidGuard.conf pour paramétrer notre redirection en modifiant les lignes redirect

```
redirect http://127.0.0.1/cgi-
bin/squidGuard.cgi?clientaddr=%a&clientuser=%i&targetgroup=%t&url=%u&client
group=%s
```

Redémarrez Squid

```
/etc/init.d/squid restart
```



Voilà nous avons un proxy opérationnel.

AdminLor

4. Administration du filtrage

Il peut arriver que certains sites dont vos utilisateurs ont besoin soit bloqués, ou encore d'autres qui devraient l'être mais qui ne le sont pas, nous allons voire comment ajouter des sites à bloquer et comment en enlever d'autres.

Exemple :
Le site SFR est bloqué, pour lever le blocage nous allons créer un fichier domains.diff à placer dans le répertoire /var/lib/squidguard/db/mobile-phone dans notre cas et ajouter la ligne :

```
-sfr.fr
```

Le site playboy n'est pas bloqué, nous voulons bloquer ce dernier dans se cas il nous faut créer un fichier domains.dif dans le répertoire /var/lib/squidguard/db/porn pour le cas suivant et ajouter la ligne :

```
+playboy.com
```

Pour enlever sfr.fr du domains.db de mobile-phone et ajouter playboy.com du domains.db de porn il faut exécuter la commande suivant qui va s'appuyer sur les fichiers domains.diff que nous avons créé pour effectuer les modifications :

```
squidGuard –u
squid –k reconfigure
```

Les modifications apportées resteront pérenne même après la mise à jour de la black-list.