07/03/2018

Sécurisation des accès internet par un proxy

Epreuve E6

Raphaël Andrieu
ARCONIC

Raphaël Andrieu

Table des matières

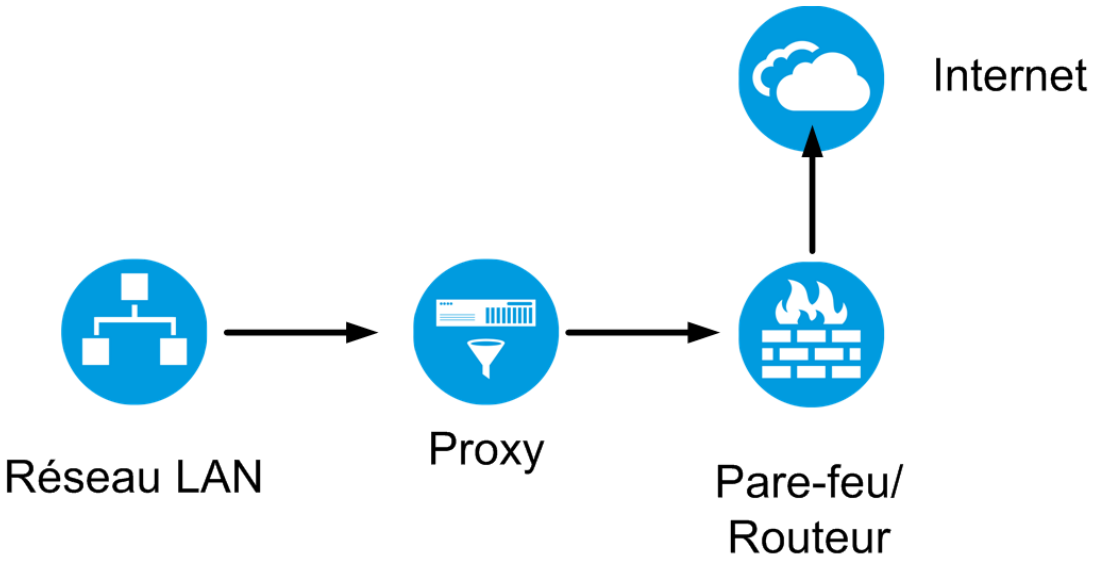
Problématiques

L'entreprise Xinthya à détecter que certains de ses employés naviguaient sur certains sites interdit pendant leur temps de travail, l'administration cherche donc à limiter l'accès, en mettant en place un système d'identification pour ces sites bloqués.

Cahier des charges

- Interdire l'accès au site adulte et de jeux.
- Mise en place d'un système d'authentification
- Mise en place d'une GPO pour paramétrer le proxy automatiquement sur les postes du domaine

Maquette



Raphaël Andrieu

Prérequis

- Un serveur Debian a jour avec comme adresse IP « 192.168.1.252 »
- Un poste informatique avec Firefox
- Un serveur Windows 2012 avec comme adresse IP « 192.168.1.145 » et un domaine « Xinthya »

Installation et configuration de Squid3

On installe Squid :

```
# Apt-get install squid3
```

Puis nous allons éditer la configuration en supprimant les commentaires inutiles

```
# Cd /etc/squid3

# Cp squid.conf squid.back

# grep -E -v '^(#|$)' squid.back > squid.conf

# nano squid.conf
```

```
 GNU nano 2.2.6                          Fichier : squid.conf

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
http_access deny all
http_port 3128
coredump_dir /var/spool/squid3
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320
```

Nous allons ajouter dans cette configuration l'ACL pour notre réseau, pour cela écrivez juste au-dessus de la ligne « acl CONNECT method CONNECT » , la ligne suivante

```
acl reseau_xinthya src 192.168.1.0/24
```

```
acl Safe_ports port 777         # multiling http
acl reseau_xinthya src 192.168.1.0/24
acl CONNECT method CONNECT
```

Puis nous allons autoriser cette ACL en écrivant au-dessus de la ligne « http_access deny all »

```
http_access allow reseau_xinthya
```

```
http_access allow localhost
http_access allow reseau_xinthya
http access deny all
```

Puis nous allons intégrer dans la configuration le module SquidGuard, que nous allons installer par la suite pour filtrer les sites que nous voulons grâce à des catégories, cette ligne permet de désigner SquidGuard comme outil pour le filtrage des URL.

```
redirect_program /usr/bin/squidGuard

redirect_children 20
```

La ligne « redirect_children 20 » permet de définir le nombre de processus enfants qui permettront de répodnre aux requêtes transmises par squid. Ce chiffre doit être assez grand pour pouvoir optimiser les temps de réponse tout en restant raisonnable sur les ressources du système (charge mémoire) (Ce chiffre ne peut pas dépasser 32)

```
redirect_program /usr/bin/squidGuard

redirect_children 20
```

Installation et configuration de SquidGuard

Nous allons maintenant installer SquidGuard qui va nous permettre de filtrer les URL

```
Apt-get install squidguard
```

Puis nous allons installer la Blacklist de l'université capitole 1 a Toulouse géré par Fabrice Prigent qui regroupe un très grand nombre de site par catégorie, ce qui nous permettra de bloquer l'accès au site de jeux, de shopping et porno sur notre réseau sans devoir lister tous les URL manuellement.

```
wget http://dsi.ut-capitole.fr/blacklists/download/blacklists.tar.gz
```

Puis nous allons extraire le dossier

```
tar -xzf blacklists.tar.gz
```

Puis nous allons copier le dossier vers le répertoire de squidGuard

```
cp -R blacklists/* /var/lib/squidguard/db/
```

Vous pouvez avoir la liste de toutes les catégories de cette base, en faisant « ls -l » dans le dossier « /var/lib/squidguard/db/ »

```
root@srv-ar-deb:/etc/squidguard# cd /var/lib/squidguard/db
root@srv-ar-deb:/var/lib/squidguard/db# ls -l
total 424
lrwxrwxrwx 1 root root     9 mars   7 19:19 ads -> publicite
drwxr-xr-x 2 root root  4096 mars   7 19:19 adult
lrwxrwxrwx 1 root root     8 mars   7 19:19 aggressive -> agressif
drwxr-xr-x 2 root root  4096 mars   7 19:19 agressif
drwxr-xr-x 2 root root  4096 mars   7 19:19 arjel
drwxr-xr-x 2 root root  4096 mars   7 19:19 associations_religieuses
drwxr-xr-x 2 root root  4096 mars   7 19:19 astrology
drwxr-xr-x 2 root root  4096 mars   7 19:19 audio-video
drwxr-xr-x 2 root root  4096 mars   7 19:19 bank
drwxr-xr-x 2 root root  4096 mars   7 19:19 bitcoin
drwxr-xr-x 2 root root  4096 mars   7 19:19 blog
-rw-r--r-- 1 root root 78194 mars   7 19:19 cc-by-sa-4-0.pdf
drwxr-xr-x 2 root root  4096 mars   7 19:19 celebrity
drwxr-xr-x 2 root root  4096 mars   7 19:19 chat
drwxr-xr-x 2 root root  4096 mars   7 19:19 child
drwxr-xr-x 2 root root  4096 mars   7 19:19 cleaning
drwxr-xr-x 2 root root  4096 mars   7 19:19 cooking
drwxr-xr-x 2 root root  4096 mars   7 19:19 cryptojacking
drwxr-xr-x 2 root root  4096 mars   7 19:19 dangerous_material
drwxr-xr-x 2 root root  4096 mars   7 19:19 dating
drwxr-xr-x 2 root root  4096 mars   7 19:19 ddos
drwxr-xr-x 2 root root  4096 mars   7 19:19 dialer
drwxr-xr-x 2 root root  4096 mars   7 19:19 download
drwxr-xr-x 2 root root  4096 mars   7 19:19 drogue
lrwxrwxrwx 1 root root     6 mars   7 19:19 drugs -> drogue
drwxr-xr-x 2 root root  4096 mars   7 19:19 educational_games
drwxr-xr-x 2 root root  4096 mars   7 19:19 filehosting
```

Maitenant nous pouvons passer à la configuration de squidguard, nous allons créer un backup du fichier de configuration de squidGuard en cas d'erreur

```
# cd /etc/squidguard/

# cp squidGuard.conf squidGuard.back
```

On va maintenant modifier le fichier de configuration de SquidGuard. Cette configuration comporte déjà pas mal de chose, mais nous allons supprimer certaines partie et ajouter les listes « jeux » , « porno » et « shopping » pour notre réseau.

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


src administration {
        ip              192.168.1.200
        user            root foo bar
}

dest adult{
        domainlist      adult/domains
        urllist adult/urls
        expressionlist  adult/expressions
        redirect https://www.google.fr
}

dest games{
        domainlist      games/domains
        urllist games/urls
        redirect https://www.google.fr
}

acl {
        administration {
                pass     any
        }
        default {
                pass     !adult !games all
                redirect https://www.google.fr #Redirection de l'utilisateur vers google
        }
}
```

Nous créons un groupe « administration » qui regroupe les adresses IP qui n'auront aucune restriction, puis nous créons 3 catégorie « adult », « games » « shopping » qui regroupe la liste des urls, des expressions et des domaines interdit, nous redirigeons tous ces sites vers le site de google.

Puis nous créons un lien symbolique du fichier squidGuard.conf dans le dossier de squid

```
# ln -s /etc/squidguard/squidGuard.conf /etc/squid3/
```

Puis on attribue les droits sur l'utilisateur proxy

```
# chown -R proxy:proxy /var/log/squid3 /var/lib/squidguard
```

On génère la base de données qui permettra un filtrage plus rapide des URL interdites par squidGuard.

```
# squidGuard -C all
```

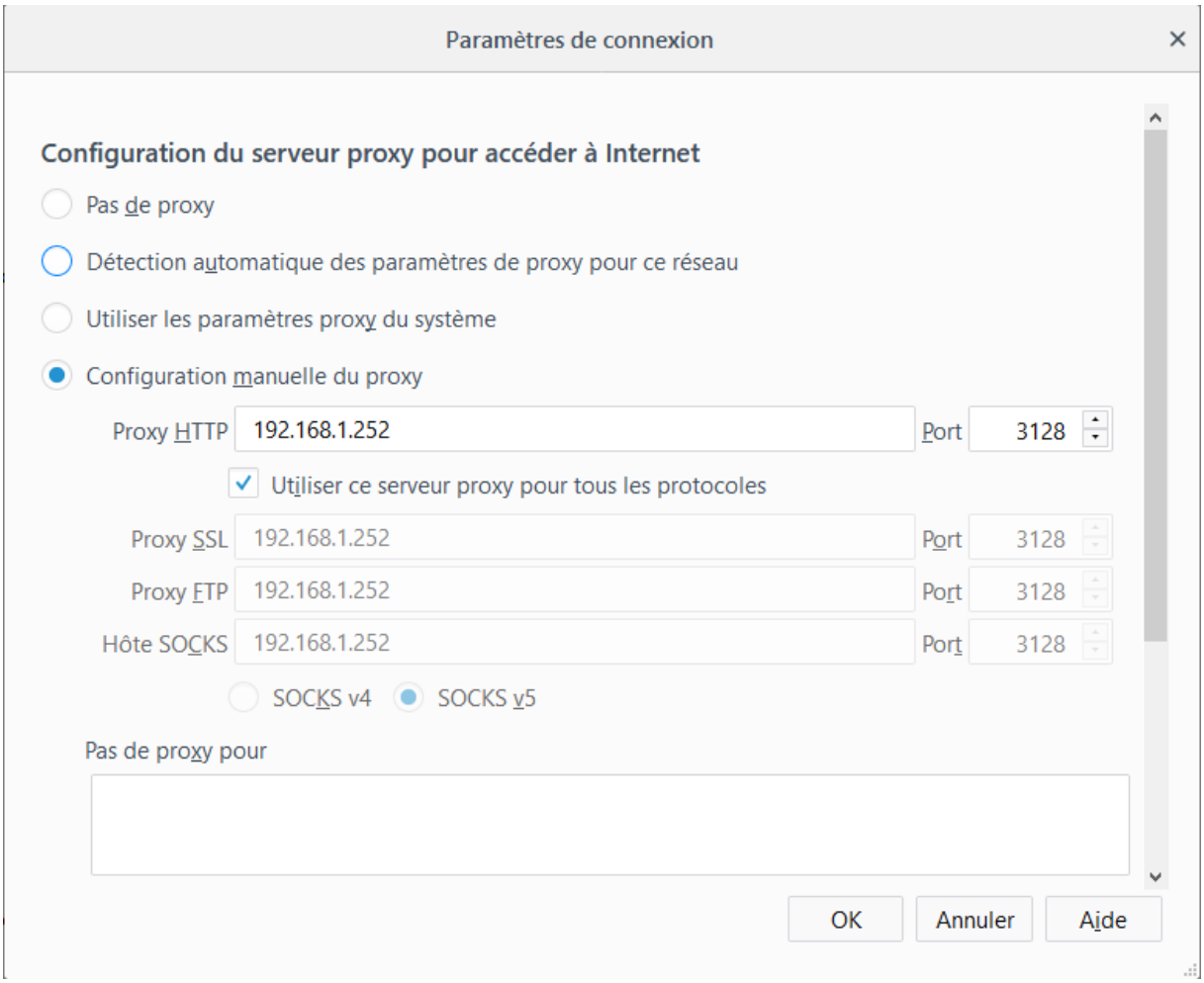
On redémarre les services de squid3

```
# service squid3 restart
```

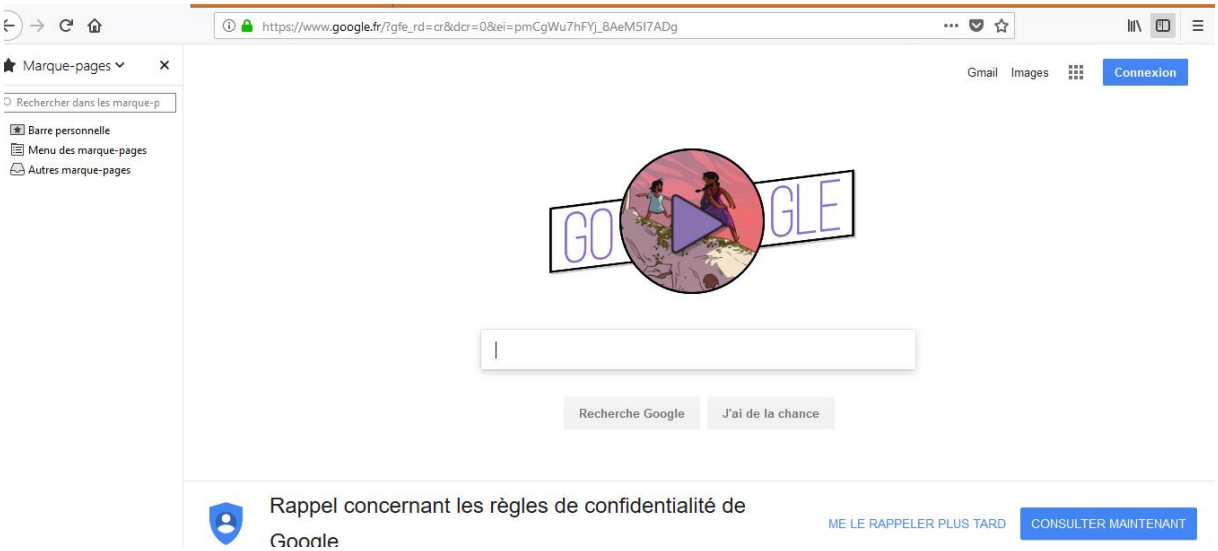
Test du proxy

Nous allons maintenant tester le proxy, pour cela nous allons utiliser le navigateur firefox avec comme serveur de proxy notre serveur debian

Raphaël Andrieu

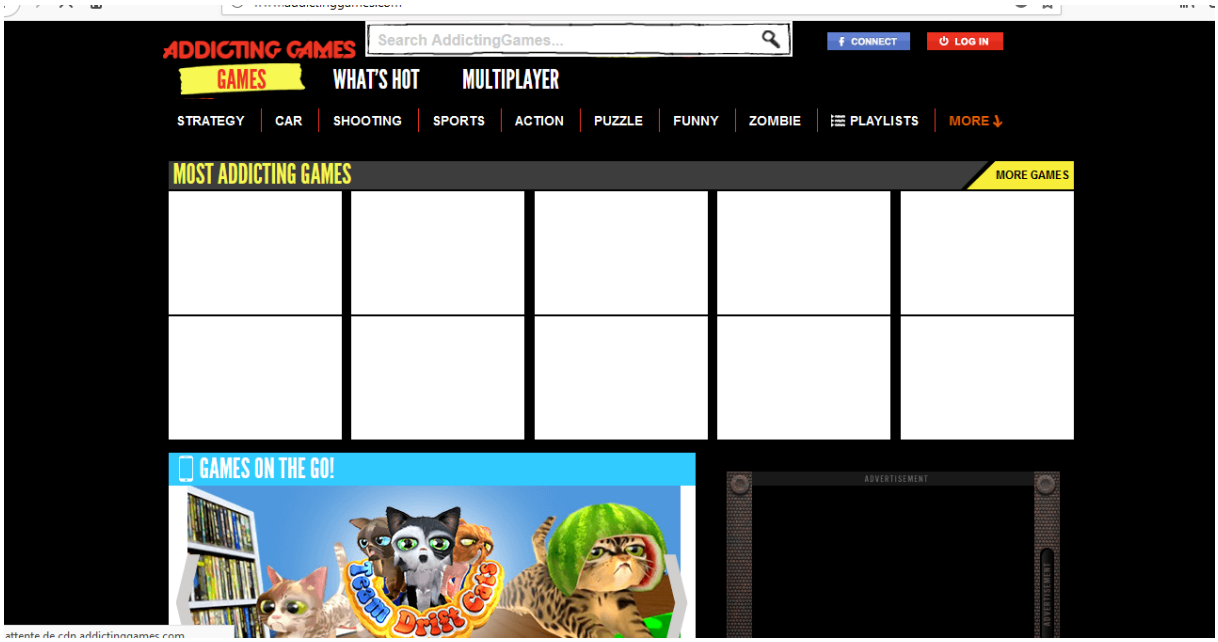


Nous allons essayer d’accéder a un site de jeux



Vous pouvez remarquer qu'une redirection a été faite vers l'url de google comme nous l'avons paramétré dans le squidGuard.conf.

Nous testons maintenant d'accéder au même URL avec l'adresse IP Administrateur « 192.168.1.200 »



Raphaël Andrieu

Système d'authentification

Nous allons ajouter un système d'authentification pour permettre d'accéder aux URLS non autorisées

```
# apt-get install apache2-utils

# htpasswd -c /etc/squid3/users squiddebian

New password: squiddebian

Re-type new password: squiddebian
```

Nous installons "apache2-utils" qui nous permettra d'utiliser la commande « htpasswd » pour créer le dossier des comptes utilisateurs, puis nous créons un utilisateur « squiddebian ». Puis nous allons modifier la configuration de squid3 pour mettre tout en haut de la celle-ci les lignes de configuration d'authentification.

```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid3/users #chemin vers le fichier des utilisateurs

auth_param basic children 5 #Nombre de connexion simultanée possible

auth_param basic realm Merci de vous identifier sur notre proxy #Contenue du POPUP de connexion

auth_param basic credentialsttl 2 hours  #On garde l'authentification durant 2heures

acl users proxy_auth REQUIRED # A ajouter au niveau des ACL

http_access allow reseau_xinthya users
```

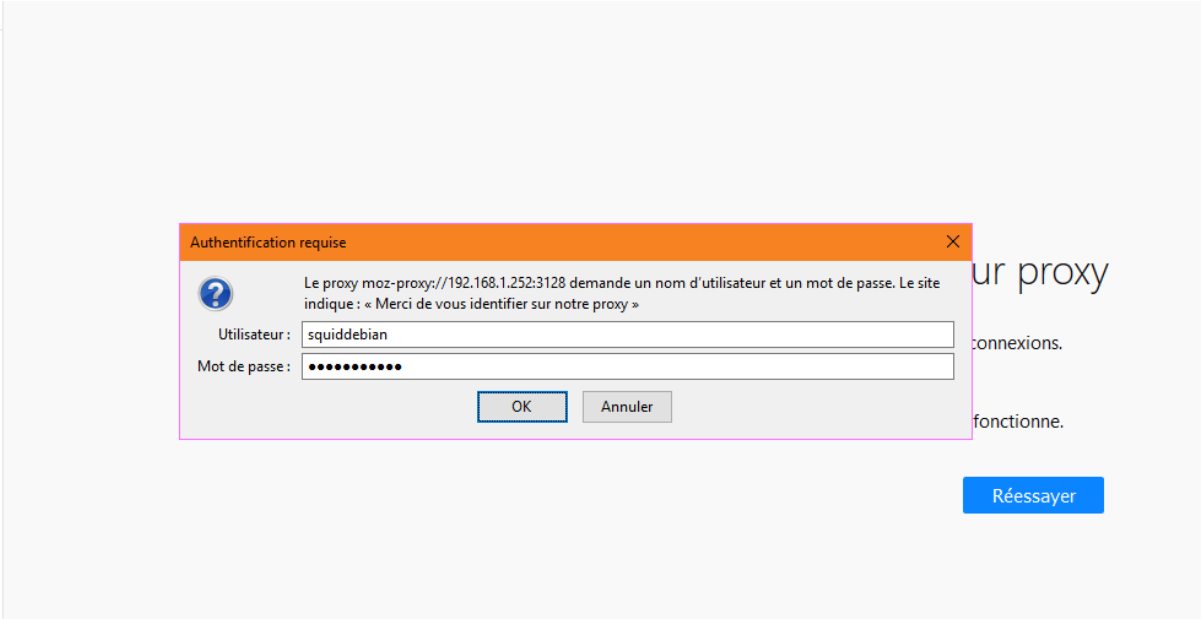
```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid3/users
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours

acl users proxy_auth REQUIRED
http_access allow LocalUsers users
```

```
acl users proxy_auth REQUIRED # L'Acl pour les utilisateurs authentifié

acl CONNECT method CONNECT
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost

http_access allow reseau_xinthya
http_access allow users # Http_access pour les utilisateurs authentifié
```

Puis on redémarre le service squid3

```
#service squid3 restart
```

Nous testons maintenant d'accéder à un URL depuis Firefox



Mise en place d'une GPO

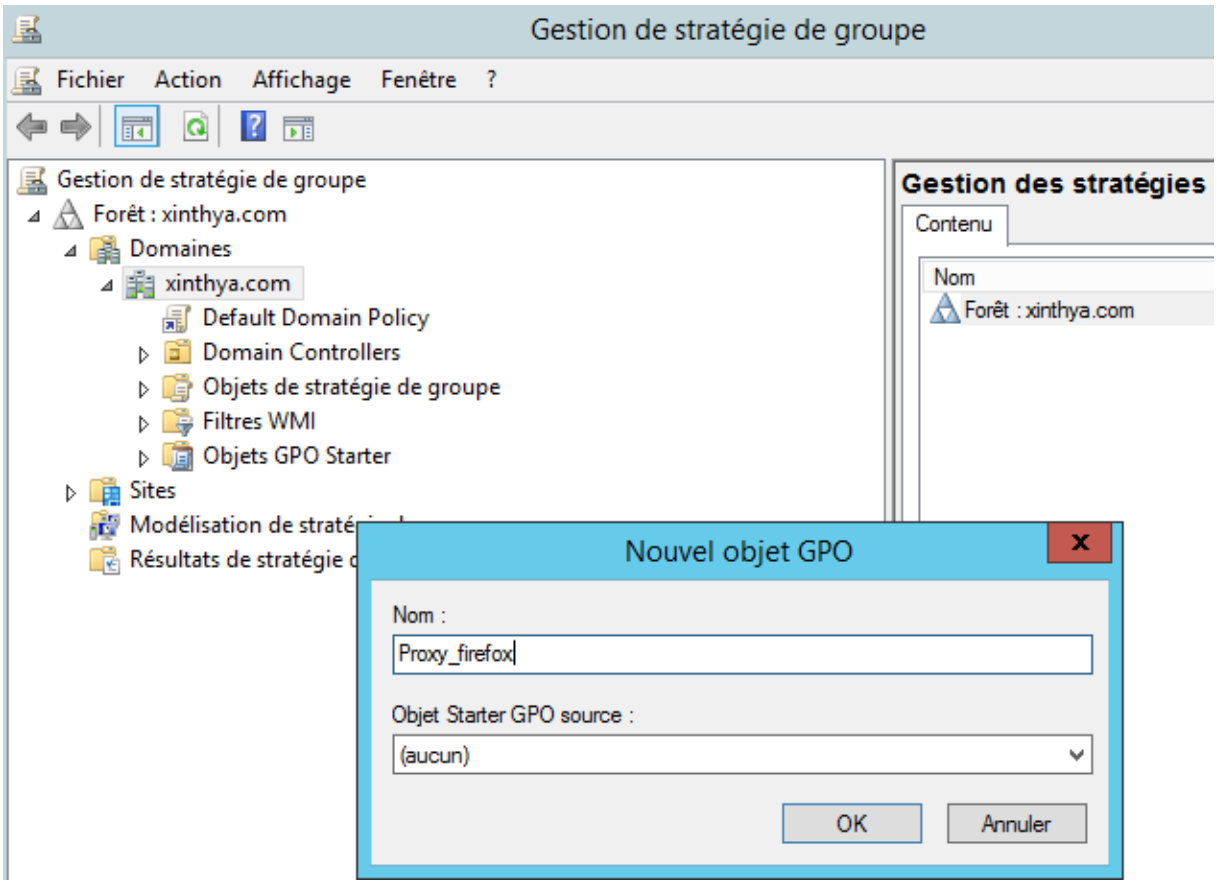
Maintenant que notre proxy est configuré, nous allons mettre en place une GPO permettant d'automatiser la mise en place du proxy sur nos postes disposant de Firefox.

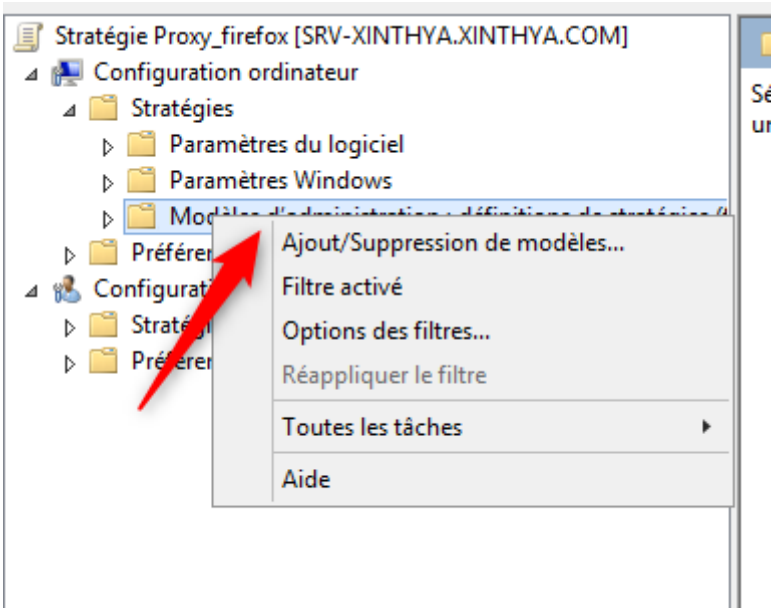
Pour cela téléchargez le fichier ADM suivant :

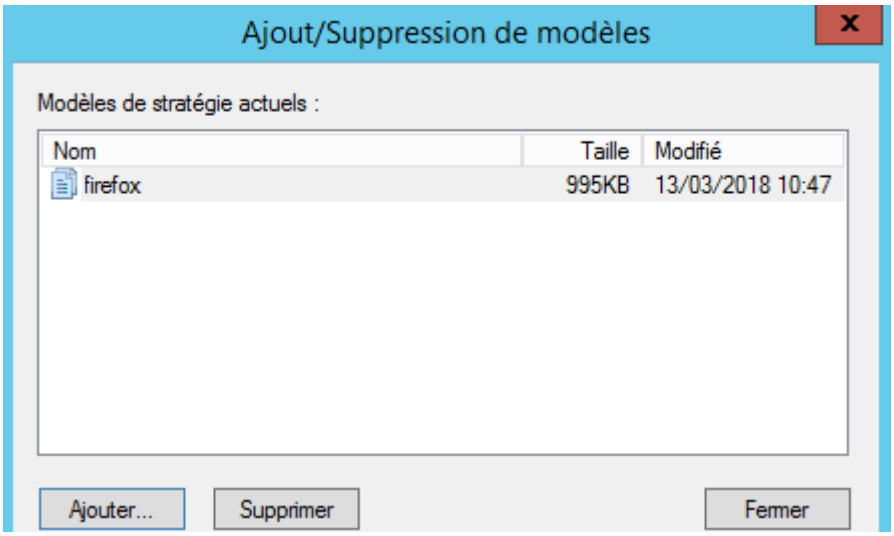
- http://sourceforge.net/projects/gpofirefox/files/firefox.adm/download

Sur le contrôleur de domaine, aller au niveau de la GPO, puis faire un clic-droit sur Modèles d'administration, puis cliquer sur Ajout/Suppression de modèles pour ajouter le fichier firefox.adm téléchargé précédemment.

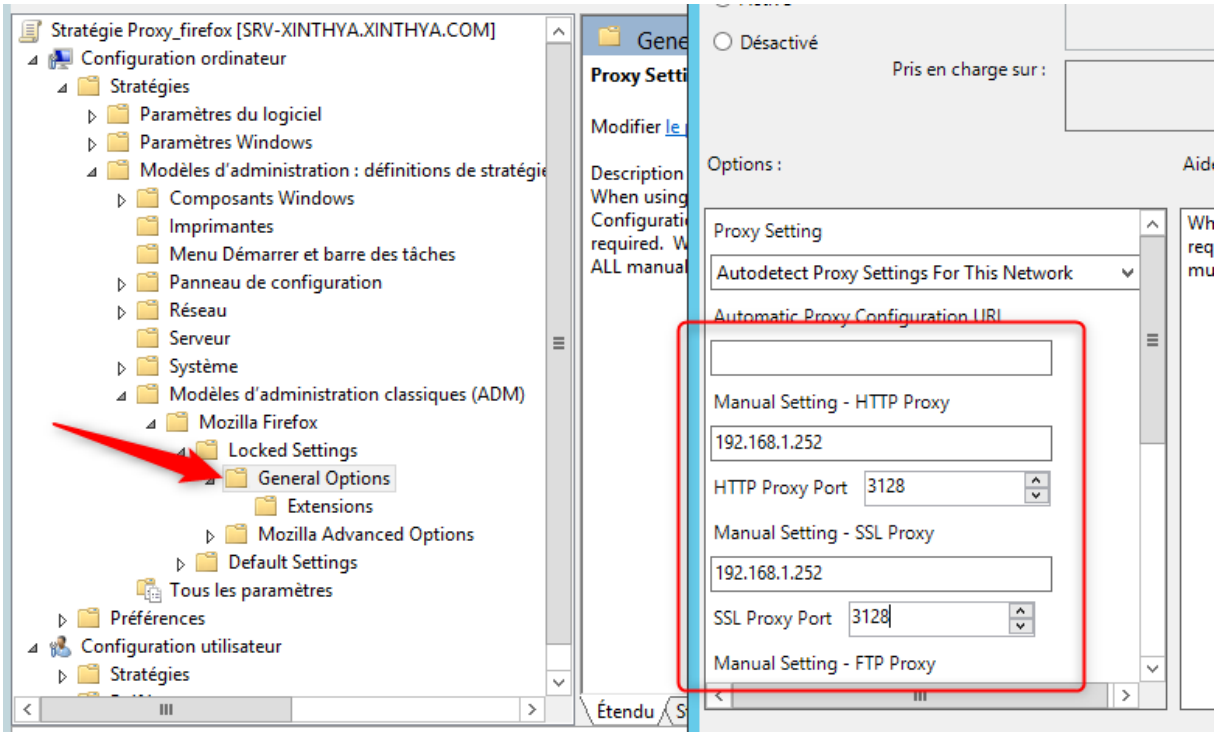
Raphaël Andrieu

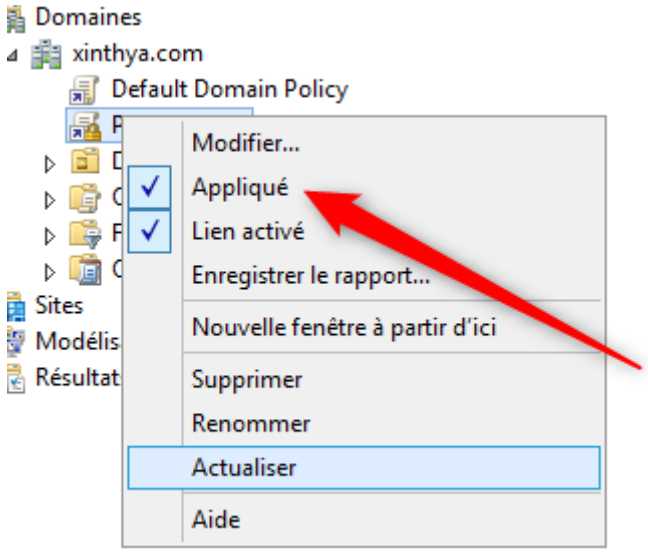






Une fois le modèle ajouté, ouvrir l'arborescence : Locked Settings > General Options, puis modifier le paramétrage du proxy :




Domaines
xinthya.com
Default Domain Policy
Sites
Modélis
Résultat
Modifier...
Appliqué
Lien activé
Enregistrer le rapport...
Nouvelle fenêtre à partir d'ici
Supprimer
Renommer
Actualiser
Aide