Squid

Squid est un serveur mandataire (proxy) et un mandataire inverse conçu pour relayer les protocoles FTP, HTTP.

1. Installation

```
#apt install squid squidguard
```

2. Configuration de squid

Suppression des commentaires du fichier /etc/squid/squid.conf

```
# cat squid.conf.backup | grep -v ^# | grep -v ^$ > squid.conf
```

Ajout de configurations pour squid dans le fichier /etc/squid/squid.conf :

Ajout des lignes suivantes à la fin du fichier de configuration

```
# Utilisateur faisant les requêtes sur le serveur
cache_effective_user proxy
cache_effective_group proxy

# Emplacement de stockage des données et réglage des niveaux
cache_mem 16 MB
cache_dir ufs /var/spool/squid 120 16 128

# algorithme utilisé pour gérer le remplacement des objets stockés en cache
cache_replacement_policy heap LFUDA

# pourcentage dusage du cache à partir duquel squid commence à supprimer des objets
cache_swap_low 80

# pourcentage dusage du cache à partir duquel squid devient plus agressif
cache_swap_high 90
```

Ajout d'une ACL pour le réseau :

```
acl <NomRéseau> src <Réseau/CIDR>
```

Ajout d'un accès pour le réseau :

```
http_access allow <NomRéseau>
```

Configurations supplémentaires :

```
visible_hostname <hostname>
forwarded_for off
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log
url_rewrite_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf
```

On redémarre le service :

```
# systemctl reload squid
```

3. Configuration de squidguard

Configuration de squidguard:
/etc/squidguard

Installation du paquet SquidGuard

```
apt install squidguard -y
```

Téléchargement de la blacklist

```
cd /var/lib/squidguard/db/
wget cri.univ-tlse1.fr/blacklists/download/blacklists.tar.gz
```

Décompression de la blacklist

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

Configuration de squidguard

```
nano /etc/squidguard/squidguard.conf
```

Configuration du réseau admin

```
src admin {
```

```
      ip    <Réseau/CIDR>
}
```

Configuration du réseau utilisateurs simples

```
src localnet {
      ip    <Réseau/CIDR>
}
```

Blocage de contenu

```
dest <NomListe> {
      domainlist        <NomListe>/domains
      urllist           <NomListe>/urls
}
```

Création d'ACL pour appliquer le blocage de contenu

```
localnet {
                  pass  !<NomListe>  all
                  redirect http://<IpProxy>/<PageWEB>
      }
```

Application des droits à l'utilisateur proxy

```
chown -R proxy:proxy /var/lib/squidguard/
```

Génération des bases de données de SquidGuard

```
squidGuard -C all -d /var/lib/squidguard/db/blacklists
```

Démarrage de squid

```
systemctl reload squid.service
```

Test de configuration :

```
echo "http://www.miniclip.com / - - GET" | squidGuard -d
```

4. Liaison avec un proxy parent

/etc/squid/squid.conf

```
cache_peer <IPproxyParent> parent <PortProxyParent> 0 no-query default
never_direct allow all
```

5. Authentification AD

Configuration de krb5 :
/etc/krb5.conf
Remplacer tout le contenu par :

```
[realms]
      <DOMAINE.DC> = {
                  kdc = <FQDN AD>
                  admin_server = <FQDN AD>
                  default_domain = <DOMAINE.DC>
                  }
[domain_realm]
      .<domaine.dc> = <DOMAINE.CD>
      <domaine.dc> = <DOMAINE.CD>
```

Test de la liaison

```
kinit Administrateur
```

Voir les tickets de Kerberos en cache

```
klist
```

Configuration de samba :
/etc/samba/smb.conf

```
[global]
  workgroup = <DOMAINE>
  realm = <DOMAINE.DC
  security = ads
  encrypt passwords = yes
```

```
  password server = <FQDN AD>

  idmap uid = 10000-20000
  idmap gid = 10000-20000
  winbind offline logon = false
  winbind enum groups = yes
  winbind enum users = yes
  winbind use default domain = yes

[homes]
comment = Home Directories
browseable = no
writable = yes
```

```
nano /etc/nsswitch.conf
passwd:           compat winbind
group:            compat winbind
shadow:           compat winbind
gshadow:          compat winbind
#files winbind

hosts:            files dns
#myhostname
networks:         files

protocols:        db winbind
services:         db winbind
ethers:           db winbind
rpc:              db windbind
#files winbind

netgroup:         nis
```

Démarrage des services Samba et Winbind

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

Rejoindre le domaine

```
net join -U Administrateur
```

Configuration de squid :

/etc/squid/squid.conf

```
visible_hostname PROXY

# Sites bloqués
url_rewrite_program /usr/bin/squidGuard -c
/etc/squidguard/squidGuard.conf

# AD
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

acl ntlm proxy_auth REQUIRED

# ACL pour le réseau
acl lan src <Réseau>
http_access allow ntlm
http_access allow lan
http_access deny all

append_domain .<domaine.dc>

forwarded_for off

# Utilisateur faisant les requêtes sur le serveur
cache_effective_user proxy
cache_effective_group proxy
cache_effective_group winbindd_priv
```

```
msktutil -c -b "CN=COMPUTERS" -s HTTP/proxy.nw07-btsinfogap.org -k
/etc/squid3/PROXY.keytab --computer-name PROXY-K --upn HT
TP/proxy.nw07-btsinfogap.org --server adnwsa.nw07-btsinfogap.org
--verbose
```