



Université Mohammed Premier Oujda
École Nationale des Sciences Appliquées
Département : Électronique, Télécommunications et Informatique
Filière : GI/GSEIR / Niveau : GI5/GSEIR5
Module : sécurité des réseaux



TP5 Security :

Configuration et administration d'un proxy SQUID

Enseignant : Mohammed SABER

Année Universitaire : 2017/2018

Objectifs pédagogiques de TP :

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

Partie 1 : Configuration des périphériques et vérification de la connectivité de la topologie

- Configurez l'équipement pour qu'il corresponde à la topologie du réseau.
- Attribuez une adresse IP statique aux PC.
- Vérifiez la connectivité entre les périphériques par les ping.
- Vérifiez la connectivité entre les périphériques par accès web.

Partie 2 : Configuration et vérification de Proxy Squid

- Configurez, appliquez et vérifiez de Proxy Squid.

Partie 3 : Filtrage par Proxy Squid

- Configurez, appliquez et vérifiez des règles de filtrage de Proxy Squid.

Scénarios

L'objectif de ce TP est d'étudier la configuration d'un serveur mandataire (appelé "proxy" en anglais) ainsi que le filtrage des accès à travers l'outil **Squid** et quelques autres utilitaires (**Squish**, **SquidGuard**).

Remarque : Assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre enseignant.

Ressources requises

Ressources nécessaires :

1. Trois ordinateurs Linux Debian 7 (mot de passe : **ensao (ATTENTION : NE MODIFIER PAS LE MOT DE PASSE)**) ;
2. Cinq câbles Ethernet directs (2 de couleur rouge, 2 de couleur verte, 1 de couleur blanche) ;
3. Accès à l'invite de commandes des hôtes PC1, PC2 et PC3 ;
4. Accès à la configuration TCP/IP du réseau des hôtes PC1, PC2 et PC3.
5. Deux commutateurs (Switch) ;

Consignes pour le TP

1. Suivez les instructions pour chaque étape.
2. Ne déplacez pas le matériel.
3. **N'utilisez pas les Clés USB sur les machines.**
4. A la fin de TP, SVP réorganiser votre table :

- Éteindre toutes les machines.
 - Réorganiser les chaises à ces places avant de sortir.
 - MERCI d'avance.
5. Un rapport de TP individuel est rendu sur la plateforme Moodle à la fin de TP (en format PDF ou DOC).
 6. **Chaque étudiant ne respect pas les consignes de TP sera sanctionné.**

Commandes utiles pour ces travaux pratiques

Configuration des adresses IP des interfaces par la commande ifconfig

- Chaque interface est identifiée par un nom :
 - **ethX** : première carte réseau de type Ethernet, avec **X** le numéro de l'interface ($0 \leq X \leq N$).
 - **lo** : loopback ou interface de bouclage.
- Liste des interfaces réseau configurées : `ifconfig`.
- Pour configurer une interface réseau : `ifconfig interface AdresseIP netmask MasqueRéseau up/down`

Configuration de la table de routage : la commande route

- Pour afficher la table de routage : `route -n`
- Pour ajouter une entrée de réseau à la table de routage : `route add -net AdresseRéseau(A.B.C.D) netmask MasqueRéseau(A.B.C.D) gw AdressePasserelle(A.B.C.D)`
- Pour supprimer une entrée de réseau dans la table de routage : `route del -net AdresseRéseau(A.B.C.D) netmask MasqueRéseau(A.B.C.D) gw AdressePasserelle(A.B.C.D)`
- Pour ajouter une route (un routeur) par défaut à la table de routage : `route add default gw AdressePasserelle(A.B.C.D)` Pour ajouter la route par défaut à la table de routage : `route add default`

Tester la connectivité la commande ping

La commande ping permet de vérifier l'accessibilité de l'hôte ou de la passerelle (gateway) dont le nom ou l'adresse IP est spécifié en argument.

La commande (`ping AdresseIP`) permet donc :

- Tester la connectivité du système local ;
- Identifier les couches d'où provient le problème ;
- Tests supplémentaires à réaliser pour en déterminer la cause et ainsi compléter le diagnostic.

Adresse MAC et Adresse IP

- En TCP/IP, chaque machine du réseau est identifiée par une adresse codée sur 32 bits (4 octets), son adresse IP.
- Chaque carte réseau dispose d'une adresse codée sur 48 bits (6 octets), son adresse MAC.

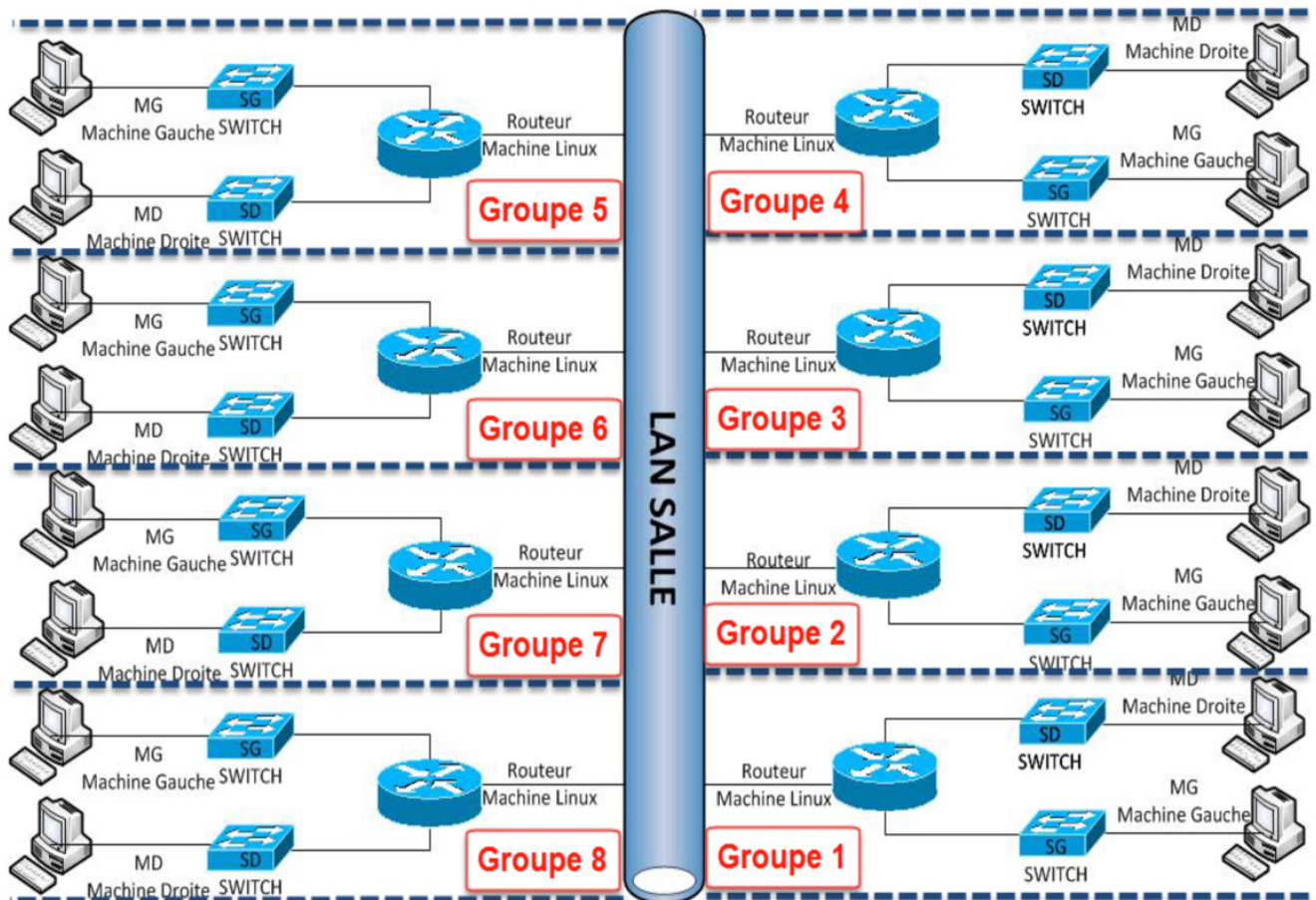
Les machines utilisent leurs adresses IP pour communiquer entre elles, mais au niveau du réseau physique sous-jacent (dans notre cas ETHERNET), c'est l'adresse MAC qui est utilisée dans les trames échangées.

PARTIE 1 : Configuration des périphériques et vérification de la connectivité de la topologie

Atelier du réseau pour ces travaux pratiques

Atelier de TP

L'architecture de l'atelier est la suivante :



Plan d'adressage de l'atelier de TP

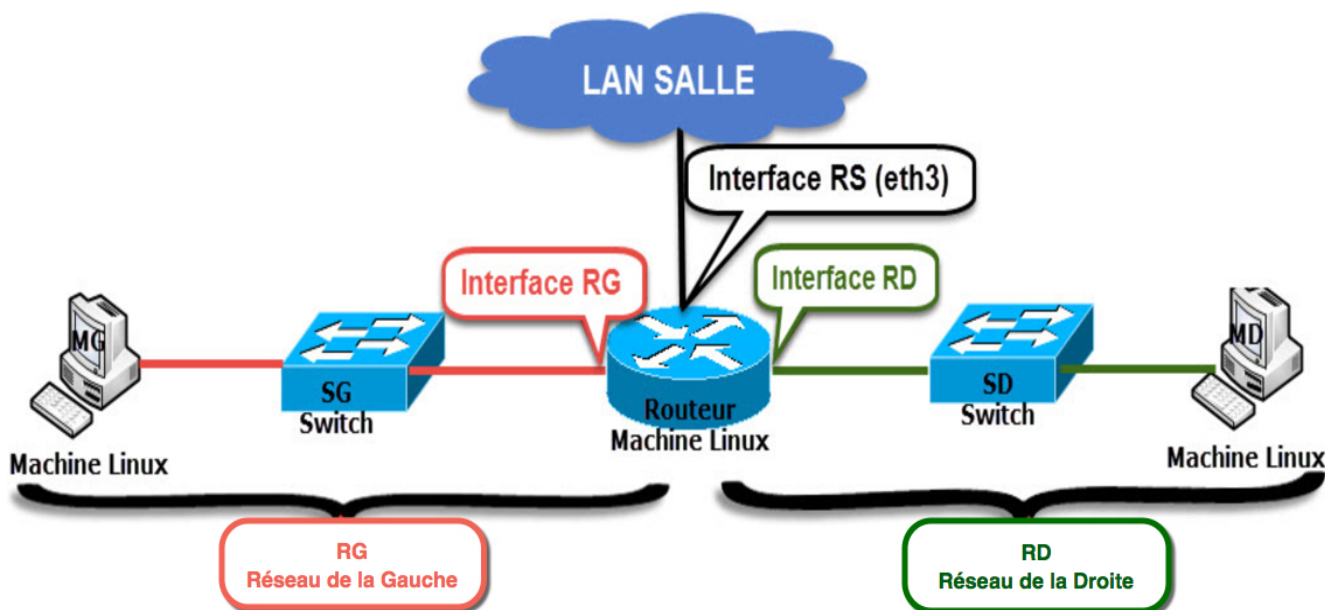
Le plan d'adressage des groupes pour ces travaux pratiques sont présentées sur le tableau suivant :

Groupe	Réseau Gauche	Réseau Droite	Réseau Salle
GR1	192.168.1.0/24	172.21.0.0/16	10.3.0.0/8
GR2	192.168.2.0/24	172.22.0.0/16	10.3.0.0/8
GR3	192.168.3.0/24	172.23.0.0/16	10.3.0.0/8
GR4	192.168.4.0/24	172.24.0.0/16	10.3.0.0/8
GR5	192.168.5.0/24	172.25.0.0/16	10.3.0.0/8
GR6	192.168.6.0/24	172.26.0.0/16	10.3.0.0/8
GR7	192.168.7.0/24	172.27.0.0/16	10.3.0.0/8
GR8	192.168.8.0/24	172.28.0.0/16	10.3.0.0/8

Étape 1 : Câblage des équipements réseau de l'atelier groupe

Tâche 1 : Connexion des périphériques réseau de l'atelier groupe

L'architecture de l'atelier réseau de chaque groupe est la suivante :



Suivez les instructions suivantes pour connecter les périphériques :

- Câblage du réseau gauche :
 1. À l'aide d'un câble droit Ethernet (**câble verte**), connectez la machine gauche **MG** au port de switch **SWG**.
 2. À l'aide d'un câble droit Ethernet (**câble verte**), connectez l'interface de type Ethernet **RG** du routeur au port de switch **SWG**.
- Câblage du réseau droite :
 1. À l'aide d'un câble droit Ethernet (**câble rouge**), connectez la machine droite **MD** au port de switch **SWD**.
 2. À l'aide d'un câble droit Ethernet (**câble rouge**), connectez l'interface de type Ethernet **RD** du routeur au port de switch **SWD**.

- Câblage du réseau vers le réseau de la salle :
 1. À l'aide d'un câble droit Ethernet (**câble blanc**), connectez l'interface de type Ethernet Rs du routeur au **port (prise) de la goulotte**.

Tâche 2 : Démarrage des machines réseau de l'atelier groupe

Démarrer les trois machines, avec les informations suivantes :

- **Compte administrateur** : login (**root**), mot de passe (**ensao**).
- **Compte utilisateur** : login (**ensao**), mot de passe (**ensao**).
- **ATTENTION!!!!** : **NE CHANGER PAS LES MOTS DE PASSE**.

Étape 2 : Configuration des équipements réseau de l'atelier groupe

Soit le plan d'adressage détaillé suivant :

Groupe	Périphérique	Adresse IP	Masque sous-réseau	Passerelle	Interface
GR1	Host MD	172.21.0.2	255.255.0.0	172.21.0.1	eth0
	Interface RD	172.21.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.1.2	255.255.255.0	192.168.1.1	eth0
	Interface RG	192.168.1.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR2	Host MD	172.22.0.2	255.255.0.0	172.22.0.1	eth0
	Interface RD	172.22.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.2.2	255.255.255.0	192.168.2.1	eth0
	Interface RG	192.168.2.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR3	Host MD	172.23.0.2	255.255.0.0	172.23.0.1	eth0
	Interface RD	172.23.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.3.2	255.255.255.0	192.168.3.1	eth0
	Interface RG	192.168.3.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR4	Host MD	172.24.0.2	255.255.0.0	172.24.0.1	eth0
	Interface RD	172.24.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.4.2	255.255.255.0	192.168.4.1	eth0
	Interface RG	192.168.4.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3

GR5	Host MD	172.25.0.2	255.255.0.0	172.25.0.1	eth0
	Interface RD	172.25.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.5.2	255.255.255.0	192.168.5.1	eth0
	Interface RG	192.168.5.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR6	Host MD	172.26.0.2	255.255.0.0	172.26.0.1	eth0
	Interface RD	172.26.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.6.2	255.255.255.0	192.168.6.1	eth0
	Interface RG	192.168.6.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR7	Host MD	172.27.0.2	255.255.0.0	172.27.0.1	eth0
	Interface RD	172.27.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.7.2	255.255.255.0	192.168.7.1	eth0
	Interface RG	192.168.7.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3
GR8	Host MD	172.28.0.2	255.255.0.0	172.28.0.1	eth0
	Interface RD	172.28.0.1	255.255.0.0	ND	eth0/eth1
	Host MG	192.168.8.2	255.255.255.0	192.168.8.1	eth0
	Interface RG	192.168.8.1	255.255.255.0	ND	eth0/eth1
	Interface RS	10.3.x.y	255.0.0.0	ND	eth3

Tâche 1 : Configuration des équipements réseau gauche de l'atelier groupe

1. Configurez l'interface Ethernet **eth0** de la machine **MG** avec l'adresse IP statique à l'aide des paramètres de votre groupe du tableau précédent. (**utilisation de la commande ifconfig**).
2. Pour éviter le problème de désactivation de l'interface. Créez un script pour la configuration de l'interface Ethernet **eth0** de la machine **MG**. Pour cela :
3. Affichez la table de routage de la machine. **route -n**).
4. Ajoutez la route par défaut pour la machine **MG** avec l'adresse IP passerelle indiqué dans le tableau précédent. (**utilisation de la commande route add default gw 192.168.x.1**).
5. Affichez la table de routage de la machine. **route -n**).
6. Configurez l'interface Ethernet gauche du routeur **RG** avec l'adresse IP statique à l'aide des paramètres du tableau précédent. (**utilisation de la commande ifconfig**).

Tâche 2 : Test de connectivité/configuration des équipements réseau gauche de l'atelier groupe

1. Ouvrir un terminal sur la machine **MG**.

2. Lancer la commande **ping** pour tester la connectivité de l'interface Ethernet de la machine **MG** avec l'interface Ethernet gauche du routeur **RG**. À partir de l'hôte **MG**, envoyez une requête **ping** à l'interface de type Ethernet du routeur **RG**.
3. La requête **ping** a-t-elle abouti ?
4. À partir du routeur, envoyez une requête **ping** à l'interface Ethernet de la machine **MG**.
5. La requête **ping** a-t-elle abouti ?
6. Si la réponse à l'une des deux questions est non, vérifiez les configurations de routeur pour identifier l'erreur. Ensuite, relancez des requêtes **ping** jusqu'à ce que la réponse aux deux questions soit oui.
7. Ouvrez un navigateur Web sur la machine **MG** et accédez à Internet. Les requêtes **WEB** ont-elles abouti ? Doivent échouer. Pourquoi ?

Tâche 3 : Configuration des équipements réseau droite de l'atelier groupe

1. Configurez l'interface Ethernet **eth0** de la machine **MD** avec l'adresse IP statique à l'aide des paramètres de votre groupe du tableau précédent. (**utilisation de la commande ifconfig**).
2. Pour éviter le problème de désactivation de l'interface. Créez un script pour la configuration de l'interface Ethernet **eth0** de la machine **MD**. Pour cela :
3. Affichez la table de routage de la machine. **route -n**).
4. Ajoutez la route par défaut pour la machine **MD** avec l'adresse IP passerelle indiqué dans le tableau précédent. (**utilisation de la commande (utilisation de la commande route add default gw 172.x.0.1)**).
5. Affichez la table de routage de la machine. **route -n**).
6. Configurez l'interface Ethernet droite du routeur **RD** avec l'adresse IP statique à l'aide des paramètres du tableau précédent. (**utilisation de la commande ifconfig**).

Tâche 4 : Test de connectivité/configuration des équipements réseau droite de l'atelier groupe

1. Ouvrir un terminal sur la machine **MD**.
2. Lancer la commande **ping** pour tester la connectivité de l'interface Ethernet de la machine **MD** avec l'interface Ethernet gauche du routeur **RD**. À partir de l'hôte **MD**, envoyez une requête **ping** à l'interface de type Ethernet du routeur **RD**.
3. La requête **ping** a-t-elle abouti ?
4. À partir du routeur, envoyez une requête **ping** à l'interface Ethernet de la machine **MD**.
5. La requête **ping** a-t-elle abouti ?
6. Si la réponse à l'une des deux questions est non, vérifiez les configurations de routeur pour identifier l'erreur. Ensuite, relancez des requêtes **ping** jusqu'à ce que la réponse aux deux questions soit oui.
7. Ouvrez un navigateur Web sur la machine **MD** et accédez à Internet. Les requêtes **WEB** ont-elles abouti ? Doivent échouer. Pourquoi ?

Tâche 5 : Configuration des équipements réseau salle de l'atelier groupe

1. L'interface Ethernet salle **eth3** du routeur **RS** est déjà configurée par une adresse IP automatique à l'aide DHCP.
2. A l'aide la commande `ifconfig eth3`, récupérer l'adresse IP de **RS**, elle est sous forme **10.3.x.y/8**.
3. Affichez la table de routage du routeur. `route -n`).

Tâche 6 : Test de connectivité/configuration des équipements réseau Gauche-droite de l'atelier groupe

1. À partir de l'hôte **MD**, envoyez une requête *ping* au hôte **MG**.
2. La requête *ping* a-t-elle abouti ?
3. À partir de l'hôte **MG**, envoyez une requête *ping* au hôte **MD**.
4. La requête *ping* a-t-elle abouti ?
5. Tous ces *ping* doivent échouer. Pourquoi ?

Tâche 7 : Activation de routage sur le routeur de l'atelier groupe

Les machines Linux ne sont pas des routeurs par défaut, il faut activer le routage au niveau des machines jouent le rôle d'une routeur.

1. Ouvrir un terminal sur le routeur.
2. Activez le routage sur le routeur par la commande suivante : `echo 1 > /proc/sys/net/ipv4/ip_forward`.

Tâche 8 : Test de connectivité/configuration des équipements réseau Gauche-droite de l'atelier groupe

1. À partir de l'hôte **MD**, envoyez une requête *ping* au hôte **MG**.
2. La requête *ping* a-t-elle abouti ?
3. À partir de l'hôte **MG**, envoyez une requête *ping* au hôte **MD**.
4. La requête *ping* a-t-elle abouti ?
5. Si la réponse à l'une des deux questions est non, vérifiez les configurations de votre atelier pour identifier l'erreur. Ensuite, relancez des requêtes *ping* jusqu'à ce que la réponse aux deux questions soit oui.

Tâche 9 : Configuration de camouflage (MASQUERADE) des adresses IP pour communiquer vers Internet à partir des réseaux internes

Rappel : Pour autoriser les machines des réseaux internes de communiquées à travers un **NAT**, il faut utiliser la commande `iptables` sous Linux. La règle `iptables -t nat -A POSTROUTING -o Interface -j MASQUERADE` va permettre de **nater** ce qui sort de l'interface Interface de routeur pour que ce soit **camouflé**.

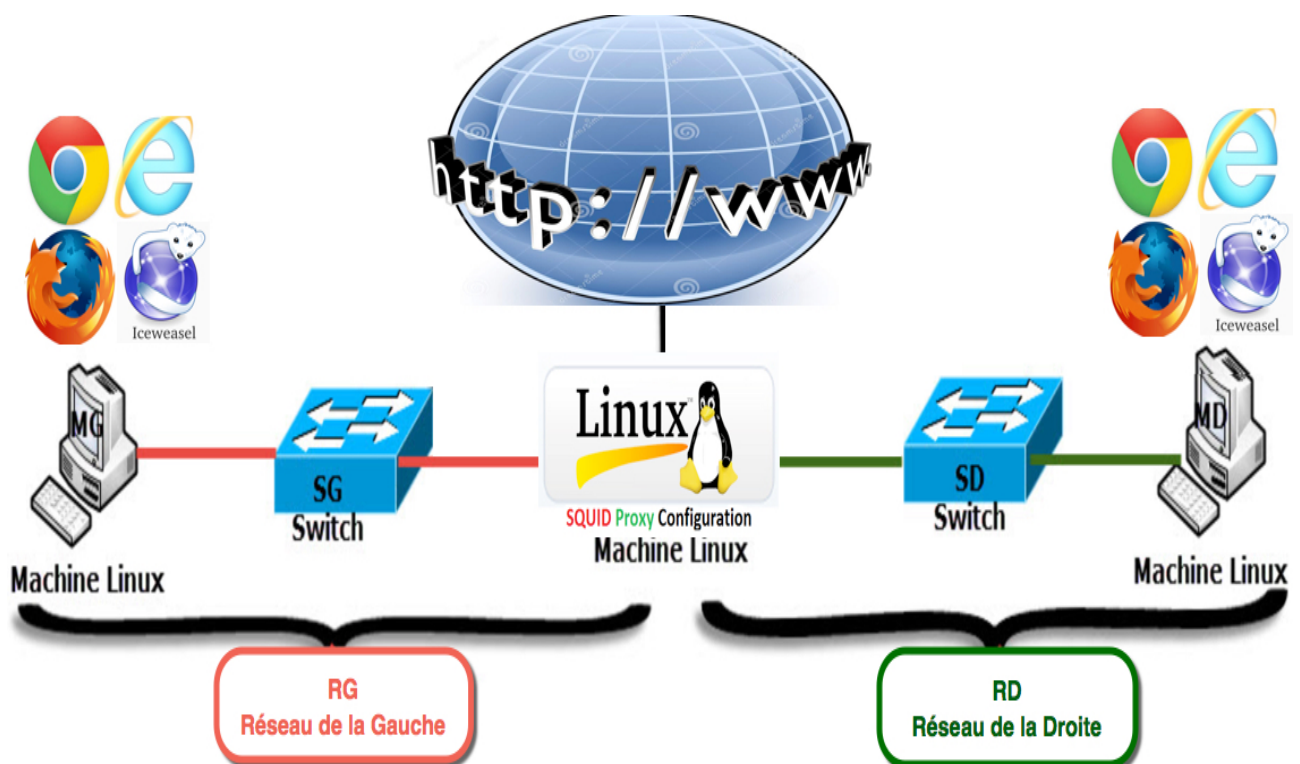
1. À partir de l'hôte **routeur**.
2. Créez la règle suivante pour autoriser la navigation vers Internet. `iptables -t nat -A POSTROUTING -o eth3 -j MASQUERADE`.

Tâche 10 : Test de connectivité des machines des réseaux Gauche-droite vers Internet

1. Ouvrez un navigateur Web sur la machine **MD** et accédez à Internet. Les requêtes WEB ont-elles abouti ?
2. Ouvrez un navigateur Web sur la machine **MG** et accédez à Internet. Les requêtes WEB ont-elles abouti ?

PARTIE 2 : Configuration et vérification de Proxy Squid

Atelier de TP



Étape 3 : Installation de proxy squid3

Tâche 1 : Suppression des configurations de proxy existantes sur le routeur

Il est nécessaire de commencer avec un routeur non configuré en proxy. L'utilisation d'un routeur comportant déjà une configuration peut produire des résultats imprévisibles.

1. A partir la machine serveur proxy squid (routeur).
2. Se connecter en tant que «root» sur une console texte.
3. Supprimer le package squid3, par l'utilisation de la commande suivante : `apt-get --purge remove squid3`. (N.B : Si le squid3 n'est pas installé passer à la tâche suivante).

Tâche 2 : Installation de proxy Squid sur le routeur

1. A partir la machine serveur proxy squid (routeur).

2. Se connecter en tant que «root» sur une console texte.
3. Faire des mises-à-jours du cache du routeur, par la commande suivante : `apt-get update`.
4. Installer le package **SQUID3**, par la commande suivante : `apt-get install squid3`.

Étape 4 : Configuration et vérification de Proxy Squid

Tâche 3 : Configuration de proxy Squid sur le routeur

Rappel : Avant toute modification, nous allons sauvegarder le fichier **squid.conf** qui est le fichier de configuration de **Squid**. On y configure des directives qui permettent notamment de spécifier le port d'écoute de **Squid**, la taille du cache, les chemins d'accès vers les fichiers de **logs**, les restrictions d'accès ou encore les **timeouts**.

1. A partir la machine routeur.
2. Se connecter en tant que «root» sur une console texte.
3. Lancez sur un terminal, la commande suivante : `cp /etc/squid3/squid.conf /etc/squid3/squid.conf.backup`.
4. Configurez le serveur **Squid** /etc/squid3/squid.conf par les informations suivantes :

```
-----
#Configuration de Squid 3 dans le fichier /etc/squid3/squid.conf
```

```
#Identification du serveur proxy
#adresse-ip-du-routeur : 192.168.x.1 (x est le numéro de votre groupe).
http_port adresse-ip-du-routeur:3128
visible_hostname localhost
```

```
#Configuration du cache Proxy
cache_mem 256 MB
cache_mem_low 75
cache_mem_high 90
maximum_object_size 8192 KB
```

```
#Zone Création des ACLs (règles) de filtrage de proxy par la commande acl
```

```
# Soit la dernière dans la liste des règles créées.
acl all src all
```

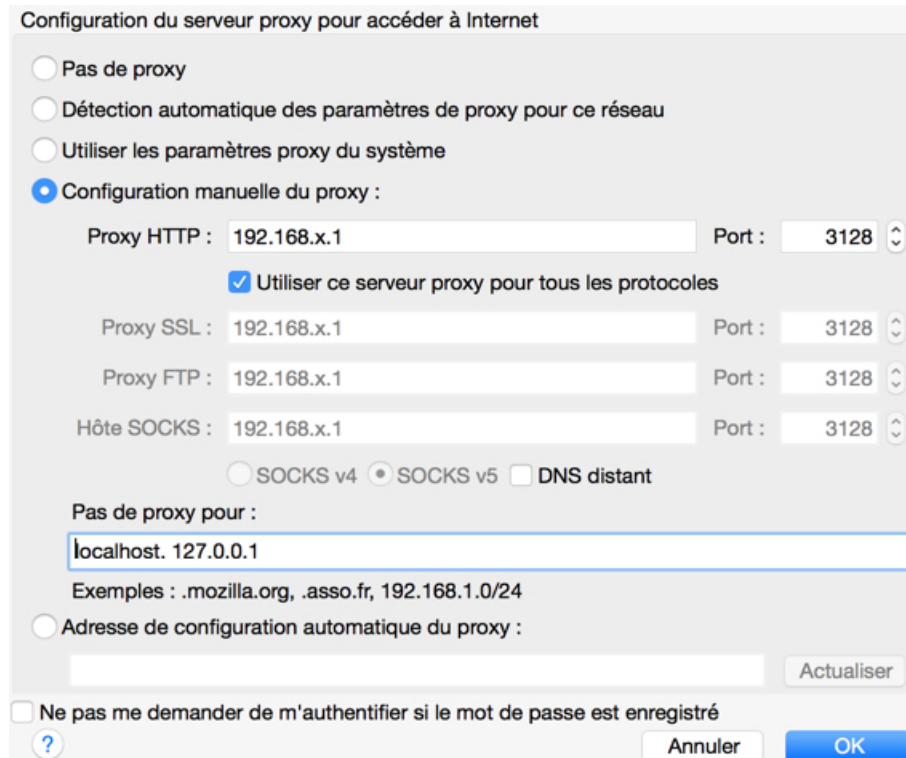
```
# Zone Action sur les ACLs de filtrage par la commande http_access (soit allow pour
```

```
# Soit la dernière dans la liste des actions créées.
http_access allow all
-----
```

5. Une fois vous avez configuré votre proxy, redémarrez ou stoppez le service squid3, par la commande : `service squid3 start|stop|restart` ou `/etc/init.d/squid3 start|stop|restart`.
6. Après le démarrage de proxy Squid, vérifier que le service Squid il est en écoute. (Utilisation de la commande : `netstat -l | grep squid`).

Tâche 4 : Configuration de proxy sur les clients des réseaux internes

1. A partir les machines clientes sur les réseaux droite et gauche.
2. Ouvrez un navigateur Web (Iceweasel) sur les machines **MG** et **MD**.
3. Configurer votre navigateur par les informations de votre proxy, pour cela : dans le menu **Édition** puis **Préférences** puis **Avancé** puis **Réseau** puis **Paramètres** comme montre la figure suivante :



4. Après l'enregistrement, tester maintenant l'accès à Internet.

Tâche 5 : Test de configuration de proxy Squid

1. A partir la machine routeur.
2. Se connecter en tant que «root» sur une console texte.
3. Lancez sur un terminal, la commande suivante : `service squid3 stop` ou `/etc/init.d/squid3 stop`.
4. Ouvrez un navigateur Web (Iceweasel) sur les machines **MG** et **MD** et tester l'accès à Internet. Que remarquez-vous ? Fermer le navigateur sur les machines.
5. Lancez sur un terminal, la commande suivante : `service squid3 start` ou `/etc/init.d/squid3 start`.
6. Ouvrez un navigateur Web (Iceweasel) sur les machines **MG** et **MD** et tester l'accès à Internet. Que remarquez-vous ?

PARTIE 3 : Filtrage par Proxy Squid

Rappel : les syntaxe de **création** et de l'**action** des règles de filtrage par **proxy squid** :

- La **création** d'une règle proxy par la syntaxe suivante : `acl aclname acltype string`.
— `aclname` : Nom de la règle.

- **acltype** : Type de la règle, détermine une adresse IP (**src,dst**), un domaine (**srcdomain,dstdomain**), une **URL**, une partie de l'**URL** etc... Voir les autres type à la fin de type dans l'annexe.
- **string** : Le contenu de la chaîne de caractères identifiant le critère de correspondance.
- L'**action** sur une règle proxy par la syntaxe suivante : **http_access action aclname**.
 - **action=allow** : Autorise la règle **aclname**.
 - **action=deny** : Interdire la règle **aclname**.

Remarque : Il est important que les "**http_access**" soient positionnés après les ACLs dans le fichier **squid.conf** pour qu'ils soient pris en compte. Comme nous avons montré dans l'**étape 4**.

Étape 5 : Filtrage par Proxy Squid

Tâche 1 : Vérification du cache de proxy Squid

Objectifs de cette tâche : Nous désirons visualiser le fonctionnement du cache de proxy Squid.

1. Ouvrez un navigateur Web (Iceweasel) sur la machine **MG** et tester l'accès à Internet sur le site **www.amazon.com**. Que remarquez-vous ?
2. Ouvrez un navigateur Web (Iceweasel) sur la machine **MD** et tester l'accès à Internet sur le site **www.amazon.com**. Que remarquez-vous ?
3. Supprimer le cache de proxy squid. (Utilisation de la commande : **squid** avec une option adéquate).

(a) **Sur la machine MG :**

- i. Fermer le navigateur Web (Iceweasel).
- ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet sur le site **www.amazon.com**.
- iii. Ouvrez une autre page sur le navigateur Web (Iceweasel) et tester l'accès à Internet sur le site **www.amazon.com**. Que remarquez-vous concernant l'accès de la deuxième fois par rapport à la deuxième ? (Tester encore plusieurs fois par l'actualisation des pages web demandées).

(b) **Sur la machine MD :**

- i. Fermer le navigateur Web (Iceweasel).
- ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet sur le site **www.amazon.com**.
- iii. Ouvrez une autre page sur le navigateur Web (Iceweasel) et tester l'accès à Internet sur le site **www.amazon.com**. Que remarquez-vous concernant l'accès de la deuxième fois par rapport à la deuxième ? (Tester encore plusieurs fois par l'actualisation des pages web demandées).

Tâche 2 : Filtrage des adresses IP

Objectifs de cette opération de filtrage : Nous désirons mettre en place une politique d'interdire l'accès à Internet pour des adresses IP et d'autoriser pour des adresses IP.

Remarque : La création des ACLs dans la zone **Création** et les autorisations dans la zone **Action**.

1. Sur le proxy, créer les règles suivantes qui permet d' :
 - (a) Autoriser les machines **MD** du réseau **RD** pour sortir vers Internet ? (utilisation : **acltype = dst/src**).
 - (b) Interdire les machines **MG** du réseau **RG** pour sortir vers Internet ? (utilisation : **acltype = dst/src**).
2. Pour vérifier vos résultats obtenus, utilisez maintenant l'analyseur **wireshark** pour comprendre plus en détail ce qu'il s'est passé :
 - (a) Lancer **wireshark** sur une autre console par la commande **wireshark**, sur les deux machines.
 - (b) Configurer le **wireshark** sur l'interface de type Ethernet sur les deux machines.
 - (c) Démarrer les captures par **wireshark** sur les deux machines.
3. Test de la politique de filtrage des **adresses IP** sur les machines :
 - (a) **Sur la machine MD :**
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet.
 - iii. Que remarquez-vous ?
 - iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**.
 - (b) **Sur la machine MG :**
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet.
 - iii. Que remarquez-vous ?
 - iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient ((**403 forbidden**))).

Tâche 3 : Politique par défaut

Objectifs de cette opération de filtrage : Nous désirons mettre en place une politique d'interdire l'accès à Internet pour tous le mode sauf les deux machines **MD** et **MG**.

Remarque : La création des ACLs dans la zone **Création** et les autorisations dans la zone **Action**.

1. Définir une politique de filtrage, qui bloque tous le monde Autoriser les machines **MD** et **MG** pour sortir vers Internet ?
2. Tester la politique par défaut à partir les machines **MD** et **MG** ? Que remarquez-vous ?
3. Modifier la politique de filtrage par défaut pour autoriser les machines **MD** et **MG** de sortir vers Internet ?
4. Démarrer les captures par **wireshark** sur les deux machines.
5. Tester la politique par défaut à partir les machines :
 - (a) **Sur la machine MD :**
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet.
 - iii. Que remarquez-vous ?

- iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**.
- (b) **Sur la machine MG :**
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet.
 - iii. Que remarquez-vous ?
 - iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**.

Tâche 4 : Filtrage des domaines

Objectifs de cette opération de filtrage : Nous désirons autoriser l'accès aux pages de `.amazon.com`, `.ump.ma` et `.enssup.gov.ma` et interdire l'accès aux pages de type `.hespress.com`, `.facebook.com`, `.youtube.com` et `.net` ?

Remarque : La création des ACLs dans la zone **Création** et les autorisations dans la zone **Action**.

1. Modifier la dernière configuration de la politique de filtrage par défaut effectuée dans la tâche précédente vers autoriser tout le monde.
2. Créer les règles suivantes qui permet d' :
 - (a) Autoriser l'accès aux domaines `.amazon.com`, `.ump.ma` et `.enssup.gov.ma` ? (utilisation : `acltype = dstdomain`).
 - (b) Interdire l'accès aux domaines `.hespress.com`, `.facebook.com` et `.youtube.com` ? (utilisation : `acltype = dstdomain`).
3. Démarrer les captures par **wireshark** sur les deux machines.
4. Test de la politique de **filtrage des domaines** sur les machines :
 - (a) **Sur la machine MD :**
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers les sites autorisés.
 - iii. Que remarquez-vous ?
 - iv. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers les sites interdits.
 - v. Que remarquez-vous ?
 - vi. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient `((403 forbidden))`, vérifier qui sont bien pour les sites interdits).
 - (b) **Sur la machine MG :**
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers les sites autorisés.
 - iii. Que remarquez-vous ?
 - iv. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers les sites interdits.
 - v. Que remarquez-vous ?
 - vi. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient `((403 forbidden))`, vérifier qui sont bien pour les sites interdits).

Tâche 5 : Filtrage des URLs

Objectifs de cette opération de filtrage : Un filtrage judicieux garantit une bonne répartition du trafic, ce en accord avec la politique d'administration de votre serveur. Les ACLs permettent un filtrage sur la base d'expressions rationnelles appliquées aux URL. Pour cela, nous souhaitons mettre en place un filtrage de toutes les images **GIF,TIF,JPG et JPEG**, l'audio **MP3** et des URLs particulières.

Remarque : La création des ACLs dans la zone **Création** et les autorisations dans la zone **Action**.

1. Commenter les règles et les actions de filtrage de la tâche précédente.
2. Créer les règles suivantes qui permet d' :
 - (a) Interdire les images de type `.gif`, `.tif`, `.jpg` et `.jpeg` ? (utilisation : `acltype = urlpath_regex` et `strings = .gif$` avec l'option `-i`).
 - (b) Interdire l'audio de type `.mp3` ? (utilisation : `acltype = urlpath_regex` et `strings = .mp3$` avec l'option `-i`).
 - (c) Autoriser l'accès aux URLs `www.enssup.gov.ma`, `www.youtube.com` et `www.amazon.com` ? (utilisation : `acltype = urlpath_regex`).
3. Démarrer les captures par **wireshark** sur les deux machines.
4. Test de la politique de **filtrage des URL** sur les machines :
 - (a) **Sur la machine MD :**
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers le site autorisé. (Vous pouvez tester sur d'autres qui vous connaissez contient des `.gif`).
 - iii. Que remarquez-vous ?
 - iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient `((403 forbidden))`).
 - (b) **Sur la machine MG :**
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers le site autorisé. (Vous pouvez tester sur d'autres qui vous connaissez contient des `.gif`).
 - iii. Que remarquez-vous ?
 - iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient `((403 forbidden))`).

Tâche 6 : Filtrage une partie des URLs

Objectifs de cette opération de filtrage : Nous souhaitons interdire l'accès vers les sites des jeux.

Remarque : La création des ACLs dans la zone **Création** et les autorisations dans la zone **Action**.

1. Créer la règle suivante qui permet d' :
 - (a) Interdire les sites contient le mot `jeu` dans les URLs ? (utilisation : `acltype = url_regex` et `strings = jeu`).
2. Démarrer les captures par **wireshark** sur les deux machines.

3. Test de la politique de **filtrage une partie des URLs** sur les machines :
 - (a) **Sur la machine MD** :
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers des sites des jeux que vous connaissez.
 - iii. Que remarquez-vous ?
 - iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient ((**403 forbidden**))).
 - (b) **Sur la machine MG** :
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers des sites des jeux que vous connaissez.
 - iii. Que remarquez-vous ?
 - iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient ((**403 forbidden**))).

Tâche 7 : Filtrage par temps d'accès

Objectifs de cette opération de filtrage : Nous souhaitons interdire les accès pendant les plages horaires 8h-12h et 14h-18h en semaine. Pour cela utiliser les informations sur les jours de la semaine «S-Sunday, M-Monday, T-Tuesday, W-Wednesday, H-Thursday, F-Friday, A-Saturday»

Remarque : La création des ACLs dans la zone **Création** et les autorisations dans la zone **Action**.

PARTIE A : Filtrage par des plages de temps

1. Créer les règles suivantes qui permet d' :
 - (a) Interdire les accès à l'Internet pendant la plage horaire **8h-12h** en semaine? (utilisation : `acltype = time` et `strings = Abréviation-de-la-semaine` plage, pour la plage de **08 :00-12 :00**).
 - (b) Interdire les accès à l'Internet pendant la plage horaire **14h-18h** en semaine? (utilisation : `acltype = time` et `strings = Abréviation-de-la-semaine` plage, pour la plage de **14 :00-18 :00**).
2. Démarrer les captures par **wireshark** sur les deux machines.
3. Test de la politique de **filtrage par temps d'accès** sur les machines :
 - (a) **Sur la machine MD** :
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers les sites autorisés dans les tâches précédente.
 - iii. Que remarquez-vous ?
 - iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient ((**403 forbidden**))).
 - (b) **Sur la machine MG** :
 - i. Fermer le navigateur Web (Iceweasel).

- ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers les sites autorisés dans les tâches précédente.
- iii. Que remarquez-vous ?
- iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient ((**403 forbidden**))).

PARTIE B : Filtrage par des plages de temps pour un réseau et non pour l'autre

4. Modifier les règles de la partie A de cet tâche, pour autoriser les machines du réseau droit **RD** et interdire pour les machines du réseau gauche **RG**.
5. Démarrer les captures par **wireshark** sur les deux machines.
6. Test de la politique de **filtrage par des plages de temps pour un réseau et non pour l'autre** sur les machines :
 - (a) **Sur la machine MD :**
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers les sites autorisés dans les tâches précédente.
 - iii. Que remarquez-vous ?
 - iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient ((**403 forbidden**))).
 - (b) **Sur la machine MG :**
 - i. Fermer le navigateur Web (Iceweasel).
 - ii. Ouvrez un navigateur Web (Iceweasel) et tester l'accès à Internet vers les sites autorisés dans les tâches précédente.
 - iii. Que remarquez-vous ?
 - iv. Arrêter les captures et vérifier vos résultats obtenus en détail par **wireshark**. (Voir les trames contient ((**403 forbidden**))).

Tâche 8 : Contrôler les accès par authentification

authentifier les utilisateurs. Cette solution puissante permet de pouvoir gérer efficacement son parc et de pouvoir répondre aux attentes du code des postes et télécommunications en matière de trafic Internet.

Objectifs de cette opération de filtrage : Nous souhaitons faire authentifier les utilisateurs pour obtenir l'accès à Internet. Pour contrôler qui a le droit d'aller sur Internet.

Remarque : La création des ACLs dans la zone **Création** et les autorisations dans la zone **Action**.

1. A partir la machine serveur proxy squid (routeur).
2. Se connecter en tant que «**root**» sur une console texte.
3. Installer le package **apache2-utils**, par la commande suivante : **apt-get install apache2-utils**.
4. Créer l'utilisateur **ensao** avec le mot de passe **ensao**, par l'utilisation de la commande : **htpasswd -cb /etc/squid3/users ensao ensao**.

5. Testez votre fichier de mot de passe en tapant la commande suivante : `/usr/lib/squid3/ncsa_auth /etc/squid3/users`. (Tapez dans le terminal **ensao** puis **Entrer**, normalement il faut voir **OK**).
6. Pour activer l'authentification des utilisateurs par le proxy Squid (c.à.d demander à l'utilisateur d'être authentifié pour pouvoir utiliser le Proxy), vous devez rajouter une acl comme ceci dans **squid.conf** :

```
-----  
auth_param basic program /usr/lib/squid3/ncsa_auth /etc/squid3/users
```

```
# Ajouter cette règle dans la zone Création des ACLs (règles)  
acl restriction proxy_auth REQUIRED
```

```
# Ajouter les deux actions dans la zone Action sur les ACLs  
http_access allow restriction  
http_access deny !restriction  
-----
```

7. Test de la politique de **Contrôle les accès par authentification** sur les machines :
 - (a) **Sur la machine MD** :
 - i. Fermer le navigateur Web (Icweasel).
 - ii. Ouvrez un navigateur Web (Icweasel) et tester l'accès à Internet vers les sites autorisés dans les tâches précédente.
 - iii. Que remarquez-vous ?
 - iv. Un nom d'utilisateur et un mot de passe vous sont demandés. Utilisez **ensao** comme nom d'utilisateur et **ensao** comme mot de passe.
 - (b) **Sur la machine MG** :
 - i. Fermer le navigateur Web (Icweasel).
 - ii. Ouvrez un navigateur Web (Icweasel) et tester l'accès à Internet vers les sites autorisés dans les tâches précédente.
 - iii. Que remarquez-vous ?
 - iv. Un nom d'utilisateur et un mot de passe vous sont demandés. Utilisez **ensao** comme nom d'utilisateur et **ensao** comme mot de passe.

ANNEXE : Rappel sur la création des règles Proxy Squid

Rappel : la création d'une règle par la syntaxe suivante : `acl aclname acltype string`.

La liste pour `aclname` :

- **src** : source (client) IP addresses;
- **dst** : destination (server) IP addresses;
- **myip** : the local IP address of a client's connection;
- **arp** : Ethernet (MAC) address matching;
- **srcdomain** : source (client) domain name;
- **dstdomain** : destination (server) domain name;
- **srcdom_regex** : source (client) regular expression pattern matching;
- **dstdom_regex** : destination (server) regular expression pattern matching;
- **src_as** : source (client) Autonomous System number;
- **dst_as** : destination (server) Autonomous System number;
- **peername** : name tag assigned to the cache_peer where request is expected to be sent;
- **time** : time of day, and day of week;
- **url_regex** : URL regular expression pattern matching;
- **urlpath_regex** : URL-path regular expression pattern matching, leaves out the protocol and hostname;
- **port** : destination (server) port number;
- **myport** : local port number that client connected to;
- **myportname** : name tag assigned to the squid listening port that client connected to;
- **proto** : transfer protocol (http, ftp, etc);
- **method** : HTTP request method (get, post, etc);
- **http_status** : HTTP response status (200 302 404 etc.);
- **browser** : regular expression pattern matching on the request user-agent header;
- **referer_regex** : regular expression pattern matching on the request http-referer header;
- **ident** : string matching on the user's name;
- **ident_regex** : regular expression pattern matching on the user's name;
- **proxy_auth** : user authentication via external processes;
- **proxy_auth_regex** : regular expression pattern matching on user authentication via external processes;
- **snmp_community** : SNMP community string matching;
- **maxconn** : a limit on the maximum number of connections from a single client IP address;
- **max_user_ip** : a limit on the maximum number of IP addresses one user can login from;
- **req_mime_type** : regular expression pattern matching on the request content-type header;
- **req_header** : regular expression pattern matching on a request header content;
- **rep_mime_type** : regular expression pattern matching on the reply (downloaded content); content-type header. This is only usable in the `http_reply_access` directive, not `http_access`;
- **rep_header** : regular expression pattern matching on a reply header content. This is only usable in the `http_reply_access` directive, not `http_access`;
- **external** : lookup via external acl helper defined by `external_acl_type`;
- **user_cert** : match against attributes in a user SSL certificate;
- **ca_cert** : match against attributes a users issuing CA SSL certificate;
- **ext_user** : match on user= field returned by external acl helper defined by `external_acl_type`;
- **ext_user_regex** : regular expression pattern matching on user= field returned by external acl helper defined by `external_acl_type`;