Randall ETZWEILER A1
Bastien HELEC A1

TP3 - Filtrage par proxy et proxy inverse

1 Questions préliminaires

Rappelez quel est le rôle d'un proxy direct ?

Un proxy direct agit comme un intermédiaire entre l'utilisateur et Internet. Il sert à gérer le trafic sortant, c'est-à-dire les requêtes envoyées par les utilisateurs vers les serveurs externes. Les principaux rôles d'un proxy direct incluent l'amélioration de la sécurité en filtrant les contenus malveillants, la gestion de la confidentialité en masquant les adresses IP des utilisateurs, et parfois la mise en cache de contenu pour améliorer la vitesse de chargement des pages**.**

Quelle différence faites-vous avec le proxy inverse ?

À l'inverse, un proxy inverse (ou reverse proxy) agit principalement côté serveur, en acceptant les requêtes entrantes d'Internet qui sont destinées à un ou plusieurs serveurs internes. Il peut servir à distribuer la charge (load balancing), à augmenter la sécurité en agissant comme un pare-feu pour les attaques ciblant les serveurs internes, et à améliorer les performances en cachant le contenu statique. En gros, le proxy inverse fait office de façade pour un ou plusieurs serveurs de l'arrière-plan.

Citez quelques exemples de solutions permettant de réaliser ces fonctions.

<u>Exemples de solutions pour les proxies directs :</u>

- Squid: C'est un des proxy caches les plus populaires pour les connexions Web. Il est souvent utilisé pour les proxy directs grâce à ses capacités de filtrage et de mise en cache.
- Privoxy: Focalisé sur la protection de la vie privée, Privoxy permet de filtrer les contenus et d'améliorer l'anonymat des requêtes.

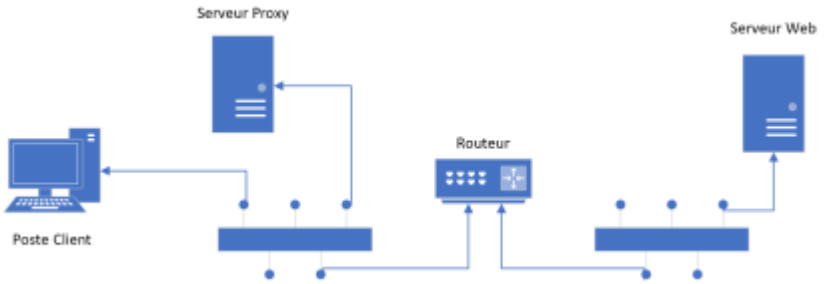
<u>Exemples de solutions pour les proxies inverses :</u>

- Nginx: Très utilisé comme serveur web et proxy inverse, Nginx permet de gérer le load balancing, la mise en cache, et les connexions SSL/TLS.
- Apache HTTP Server: Bien qu'originellement un serveur web, Apache peut être configuré pour fonctionner comme un proxy inverse.
- HAProxy: Spécifiquement conçu pour le load balancing et la haute disponibilité, il est fréquemment utilisé comme proxy inverse pour des applications nécessitant une grande stabilité et une répartition efficace du trafic.

2 Proxy direct

Dans un premier temps, il s'agit de réaliser l'architecture matérielle. Vous câblerez le réseau présenté en figure 1. On a volontairement simplifié l'architecture pour ne tester que la fonctionnalité du proxy. Pour le poste client, vous prendrez une machine avec une interface graphique pour pouvoir configurer le proxy sur le navigateur web.

Nous réaliserons cette infrastructure virtuellement afin d'accroître nos connaissances dans ce domaine.



Pour la partie routeur <-> web :
Routeur (côté serveur web) : 192.168.80.254/24
Routeur (côté réseau interne) : 10.202.50.254/24
Serveur web : 192.168.80.1/24

partie proxy <-> routeur
Réseau interne : 192.168.1.0/24
routeur : 192.168.1.254/24

Réseau interne :

Poste client :
Configuration de l'IP statique :

sudo nano /etc/network/interfaces (fichier de configuration)

Ajout des lignes suivantes :

```
auto enp0s3
iface enp0s3 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    gateway 192.168.1.254
    dns-nameservers 8.8.8.8
```

Redémarrage du réseau pour appliquer les changements :

sudo systemctl restart networking.service

Serveur Proxy :
Configuration de l'IP statique (même démarche que pour le client) :

sudo nano /etc/network/interfaces

Ajout des lignes suivantes :

```
auto enp0s3
iface enp0s3 inet static
    address 192.168.1.3
    netmask 255.255.255.0
    gateway 192.168.1.254
    dns-nameservers 8.8.8.8
```

Redémarrage du réseau pour appliquer les changements :

sudo systemctl restart networking.service

Exercice 5 Installer squid sur le serveur proxy. Le fichier de configuration est dans /etc/squid/squid.conf. Faire une copie de sauvegarde de ce fichier (/etc/squid/squid.conf.bak) avant de le modifier.

Installation de Squid :

sudo apt update
sudo apt install squid

Copie de sauvegarde du fichier Squid :

sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.bak

Exercice 6 :

Au niveau du réseau coté proxy il faudra configurer l'adresse ip et la route directement sur l'interface adapté :

ip a a 10.202.50.2/16 [ou] 10.202.50.3/16 dev [interface]
ip r a default via 10.202.50.254 dev [interface]

idem coté web :

ip a a 192.168.80.1/24 dev [interface]
ip r a default via 192.168.80.254 dev [interface]

au niveau de la passerelle la regle initial est celle-ci :

iptables -t nat -A POSTROUTING -s 192.168.80.254/24 -o [interface internet] -j MASQUERADE
iptables -t nat -A POSTROUTING -s 10.202.5.254/16 -o [interface internet] -j MASQUERADE

Exercice 7 Modifier le fichier de configuration de squid pour que le trafic de votre réseau local soit seulement capté par le serveur proxy. Squid permet également de mettre en cache les pages web visitées. On pourra modifier la valeur par défaut.

sudo nano /etc/squid/squid.conf

Spécification du réseau local pour permettre l'accès au proxy uniquement à ce réseau :

acl localnet src 192.168.1.0/24
http_access allow localnet
http_access deny all

Modification de la taille de la mise en cache :
cache_dir ufs /var/spool/squid 500 16 256

L'espace de cache est ici augmenté à 500 MB au lieu de 100 MB par défaut.

On sauvegarde et redémarrons le service Squid pour appliquer les changements :

sudo systemctl restart squid

Exercice 8 Configurez le navigateur du client web pour qu'il utilise le serveur proxy que vous avez configuré (adresse IP et port d'écoute).

Exercice 9 : Une fois la configuration opérationnelle, on bloquera tout autre trafic. Prévoir la règle nftable ou la politique par défaut qui permet de réaliser cela.

La regle par defaut sera : celle ci

sudo nft add table ip filter
sudo nft add chain ip filter input { type filter hook input priority 0\; }
sudo nft add rule ip filter input ip saddr 192.168.80.0/24 ip daddr 10.202.5.254/16 accept

```
sudo nft add rule ip filter input drop
sudo nft add chain ip filter output { type filter hook output priority 0\; }
sudo nft add rule ip filter output ip saddr 192.168.80.0/24 accept
sudo nft add rule ip filter output ip saddr 10.202.5.254/16 accept
sudo nft add rule ip filter output drop
```

Exercice 12 Quel peut-être, à votre avis, une des difficultés rencontrée avec squid pour la navigation sur le WEB ?

Une difficulté majeure rencontrée avec Squid est la gestion du trafic HTTPS, car Squid peut avoir du mal à cacher efficacement ce trafic chiffré sans configurations complexes, ce qui pose également des problèmes de confidentialité.

Exercice 13 Afin que la sécurité soit assurée (utilisation du proxy obligatoire pour sortir) que faudrait il prévoir au niveau de la configuration des postes client ?

Pour garantir une utilisation obligatoire du proxy, il faudrait prévoir un pare-feu ou routeur pour bloquer tout trafic direct vers Internet sauf celui passant par le serveur proxy, et utiliser des politiques de configuration des postes clients pour imposer les paramètres du proxy.

Exercice 14 : Dans un premier temps, on va monter l'infrastructure réseau simplifiée pour tester notre proxy inverse. Réaliser le montage de la figure 2.

Exercice 15 : Installer Nginx sur le serveur proxy inverse et tester son fonctionnement. Attention si vous avez un apache2 qui tourne sur la même machine, il risque d'y avoir des conflits.

Exercice 16 : Installer un serveur web sur les 2 machines qui font office de serveur web (apache ou Nginx) on différenciera les 2 page web pour bien arriver à faire la différence au moment de l'accès à ces pages web

Exercice 17 : On se servira d'une machine avec une interface graphique pour faire le client. Configurer le plan d'adressage du schéma pour que cela fonctionne. Configurer le fichier /etc/hosts sur le client web pour que le nom de domaine que vous choisirez soit associé à votre serveur proxy inverse (cela remplacera le fonctionnement du DNS). Par exemple : 192.168.1.1 www.monsite.fr

Exercice 18 : Configurer le serveur proxy inverse pour que tout le trafic provenant du client web à destination du nom de site que vous avez renseigné dans le /etc/hosts soit redirigé alternativement vers l'un ou l'autre des serveurs web. Vous pourrez vous inspirer de cette configuration (issu de https ://doc.ubuntu-fr.org/nginx) pour réaliser cela :