IUT Béziers
Département Réseaux et Télécoms
Bachelor R&T

2022/2023
R401
F.C.

R401 – Architectures sécurisées

Filtrage par proxy et proxy inverse

TP 3

Consignes

Dans une architecture réseau classique, il est indispensable de mettre en place une zone particulière, appelée passerelle Internet sécurisée par l'ANSSI. Le rôle de cette zone est d'isoler le réseau interne de l'Internet et de protéger également les accès aux ressources exposées de l'entreprise. Dans ce TP nous allons nous intéresser à la fonctionnalité de Proxy filtrant (Direct et inverse). Ce travail est à réaliser en binôme avec un seul compte rendu par groupe.

1 Questions préliminaires

Exercice 1 Rappelez quel est le rôle d'un proxy direct

Exercice 2 Quelle différence faites-vous avec le proxy inverse ?

Exercice 3 Citez quelques exemples de solutions permettant de réaliser ces fonctions.

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.

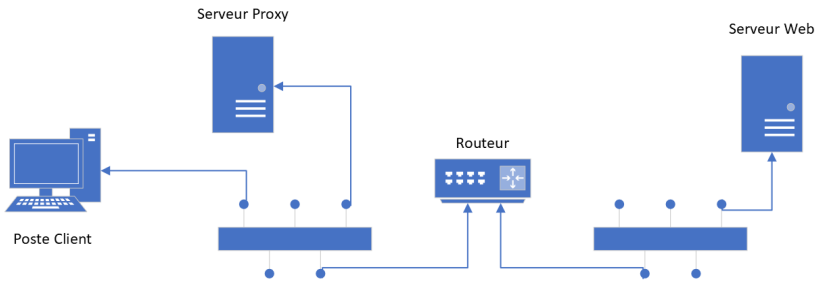

FIGURE 1 – Architecture réseau simplifiée pour mise en place d'un proxy.

Exercice 4 Installer le paquet apache2 sur le serveur web. On gardera la configuration de base du serveur.

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.

Version du document
31 mars 2023

Exercice 6 Déterminer le plan d'adressage pour que le montage soit fonctionnel. Configurer les routes et les règles nftables pour que le poste client puisse joindre le serveur web et vice-versa. On s'arrangera pour que le serveur WEB soit sur le plan d'adressage de la salle de TP. Le serveur Proxy et le client Web pourront être des machines virtuelles. Attention, il faut que le client web ait une interface graphique pour pouvoir utiliser un navigateur Web.

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

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.

Exercice 10 Vérifier le fonctionnement de la mise en cache en proposant des captures de trames judicieuses.

Exercice 11 Prévoir une procédure de test pour illustrer que le trafic est bien capturé par le serveur proxy. Vous analyserez également les logs qui sont situés dans /var/log/squid/. Une description des logs possibles se trouve ici : https ://wiki.squid-cache.org/SquidFaq/SquidLogs.

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

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 ?

En annexe !

Vous rendrez en annexe un résumé du fichier de configuration de votre serveur proxy. Celui-ci ne comprendra que les éléments que vous avez modifiés.

3 Proxy reverse

On va mettre en place un proxy reverse avec NginX. Une des fonctionnalités de ce proxy inverse est de faire bien sûr proxy, mais aussi de pouvoir faire de l'équilibrage de charge. Un article ici explique les avantages du proxy inverse https ://kinsta.com/fr/blog/proxy-inverse/.

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.

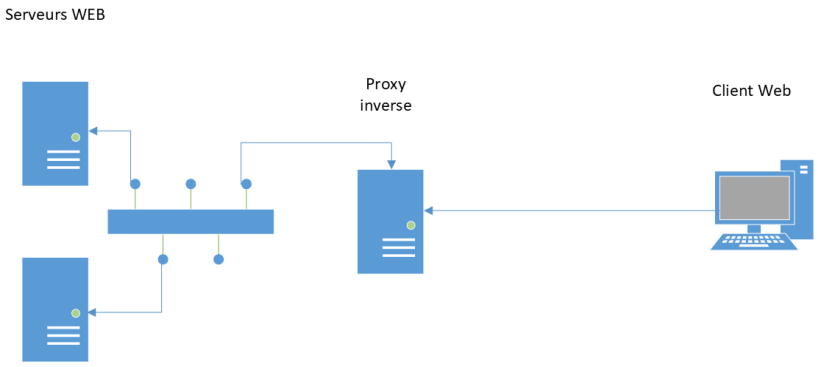

FIGURE 2 – Architecture réseau simplifiée pour mise en place d'un proxy inverse.

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 :

```
# partie de la configuration de nginx
    upstream backend {
        server 192.168.1.1 weight=1;
        server 192.168.1.2 weight=1;
    }

    server {
        listen 80;
        server_name www.monsite.fr monsite.fr;
        location / {
            proxy_pass  backend;
        }
    }
```

En annexe !

Vous rendrez en annexe les fichiers de configuration de votre serveur proxy inverse.