Administration des Systèmes et Réseaux

LES PROXY

Auteur: Bernard GIACOMONI - Autoentreprise GIACOMONI Bernard

Version	Date	Objet
1.0	21/10/2019	Version initiale

Table des matières

I.DÉFINITION:

Le mot anglais "proxy" peut se traduire par procuration ou mandat). Un PROXY est un élément informatique qui joue le rôle d'intermédiaire (ou de mandataire entre un CLIENT et un SERVEUR. Son rôle peut être décrit comme suit ;

- il va prendre à son compte les demandes du client et les diriger vers le serveur en MASQUANT à ce serveur les éléments d'identification du client (son adresse IP);
- En retour, il va rediriger la réponse du serveur vers le client.

Du point de vue du logiciel, un proxy est un SERVEUR installé sur une machine dédiée. L'appellation française officielle est SERVEUR MANDATAIRE.

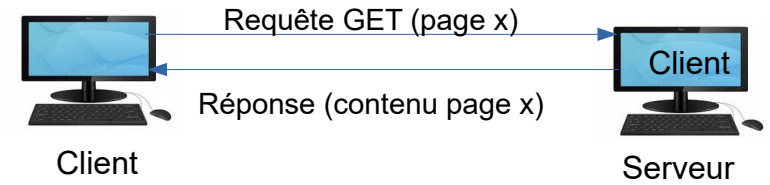
Un PROXY est un élément qui agit au niveau de la couche réseau APPLICATION: de ce fait, il n'apparaît pas au niveau de commandes comme TRACEROUTE (linux) ou TRACERT (windows), qui travaillent au niveau 3 de l'OSI.

Un PROXY permet l'accès à une ou plusieurs catégories de serveurs (serveurs HTTP, FTP, SSH, etc.). Les PROXY les plus courants sont les proxy dits "HTTP", qui permettent d'interroger les serveurs web (sites web).

II.FONCTIONNEMENT:

II.1.INTERROGATION DIRECTE D'UN SERVEUR PAR UN CLIENT:

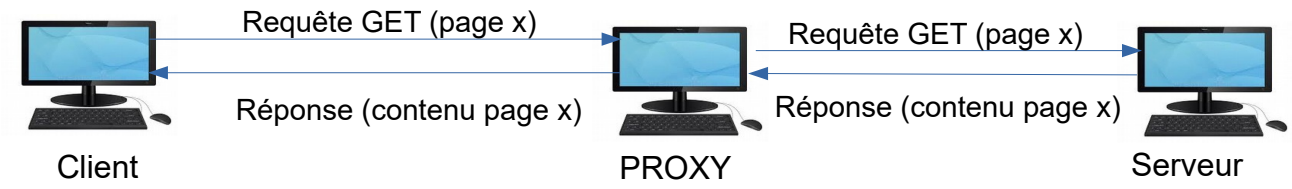
Lorsqu'un client interroge un site web sans utiliser de proxy, il saisit l'URL de ce site et l'envoie directement au serveur, grâce à une requête HTTP de type GET ou POST. Le serveur répond à la requête en renvoyant directement la réponse au client. Le serveur est donc informé de l'adresse IP du client (qui est contenue dans la couche réseau des messages), du moins si ce client n'est pas connecté par l'intermédiaire un serveur web utilisant un NAT (une BOX par exemple). Dans le cas contraire, il ne connaîtra que l'adresse IP externe du routeur :



II.2.INTERROGATION D'UN SERVEUR PAR UN CLIENT VIA UN PROXY:

Lorsqu'un client utilise un PROXY, les requêtes émises par le client sont envoyées au

proxy qui prend cette requête à son compte et la relaie vers le serveur. La réponse du serveur est alors adressée au proxy qui la relaie vers le client :



Le serveur ne connaît donc que l'adresse IP du proxy et pas celle du client: le client est MASQUÉ par le proxy.

III.UTILISATION:

Un proxy peut remplir les fonctions suivantes:

- FONCTION MASQUAGE: Permettre à un client situé dans un LAN de se connecter à l'extérieur du LAN tout en interdisant aux ordinateurs extérieurs de venir se connecter à lui. Cette fonction de protection qui consiste à masquer le client vis à vis de l'extérieur est souvent incluse dans les PARE-FEUX;
- FONCTION ANONYMISATION: l'utilisation d'un PROXY peut avoir pour résultat de masquer les informations concernant l'ordinateur client en empêchant les sites HTTP ou FTP de connaître certains renseignements contenus dans ses requêtes: site de provenance, navigateur utilisé, système d'exploitation utilisé, adresse IP du client, etc. Ceci permet d'anonymiser le client vis à vis des serveurs utilisés. Les proxy qui masquent ces informations sont dits PROXY ANONYMES;
- FONCTION CACHE: Le PROXY peut mémoriser les pages web consultées par le client. Dans ce cas, si le proxy a déjà mémorisé la page web que le client demande, il la lui renverra immédiatement sans aller la chercher sur le site en question. On l'appelle alors un PROXY-CACHE.

IV.DANGERS LIES A L'UTILISATION D'UN PROXY:

IV.1.PERTE DE CONFIDENTIALITÉ:

Le proxy "connaît" tous les sites visités par le client: pour des utilisations "sensibles" (comme la consultation de sites interdits par la législation locale), il convient donc de choisir un proxy non atteignable par les autorités du pays (Ic'est à dire localisé dans un pays qui ne se montre pas coopératif avec le pays où le client est localisé).

IV.2.DIVULGATION DE MOTS DE PASSE:

Certains sites Web nécessitent des mots de passe. Le proxy "connaît" donc les mots de passe du client, sauf en cas d'utilisation de sites utilisant HTTPS/SSL.

IV.3.MANIPULATION DES CONTENUS:

Le proxy a, bien sûr, la possibilité de modifier à la volée les pages web avant de les renvoyer à ses clients. Ceci peut lui permettre de manipuler l'information: c'est un cas certes rare, mais dans le domaine du possible. Il faut donc choisir un proxy de bonne réputation.

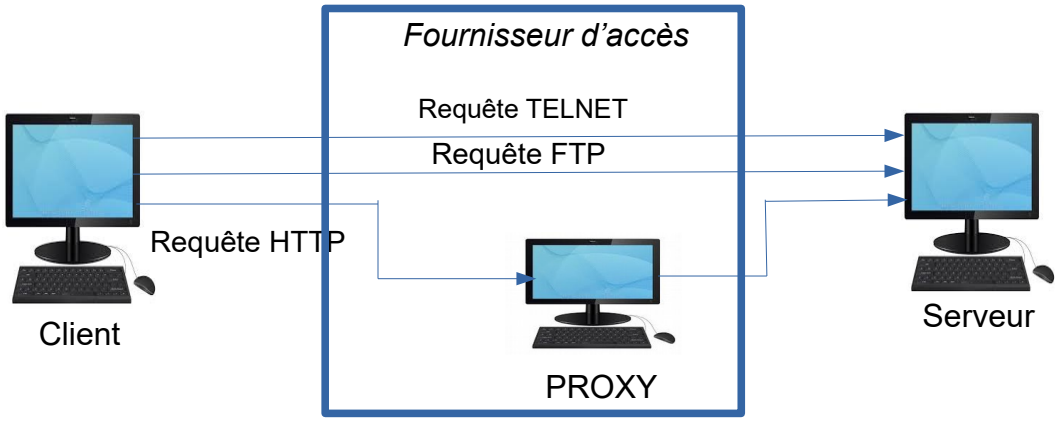
IV.4.CENSURE DE CERTAINS ACCÈS:

Certains proxy peuvent être configurés pour censurer des sites. C'est un cas assez fréquent dans certains pays qui restreignent la liberté d'information.

IV.5.PROXY "TRANSPARENTS":

IV.5.1.PRINCIPE:

Certains fournisseurs d'accès détournent les requêtes HTTP vers leurs serveurs proxy selon le mécanisme suivant, sans en informer leurs utilisateurs:



Ce mécanisme ne modifie pas les requêtes envoyées par le client, ni les réponses obtenues: de ce fait, ce type de proxy est dit "transparent". Cependant, le fournisseur d'accès peut en retire des bénéfices:

- Il peut ainsi effectuer des statistiques sur les habitudes de navigation des internautes afin de les vendre aux sociétés de marketing ;
- Cela peut lui permettre d'économiser de la bande passante pour réduire la quantité de données reçues d'Internet, en compressant les données clients. Cependant, ce procédé ne peut que dégrader la définition des images reçues par le client et la

rapidité d'affichage.

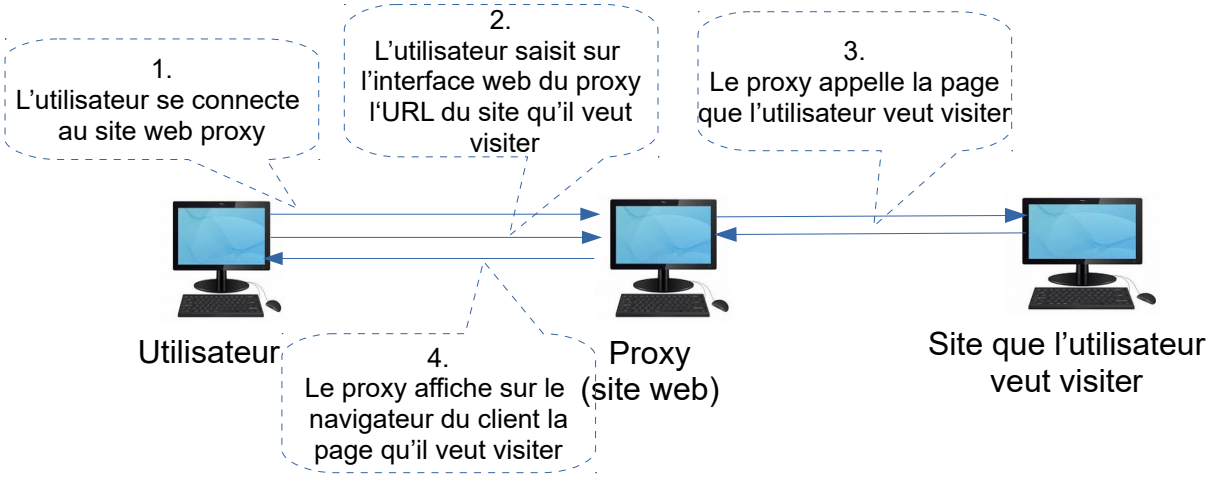
IV.5.2.COMMENT DÉTECTER UN PROXY TRANSPARENT:

Il suffit de comparer l'adresse IP du client avec celle vue par le serveur Web (dans les réponses aux requêtes ou, en PHP, dans la variable globale REMOTE_ADDR. Si les deux valeurs sont différentes, c'est que le fournisseur d'accès utilise un proxy transparent.

V.PRODUITS DISPONIBLES:

V.1.LES SITES WEB PROXY:

Certains proxy se présentent comme des sites web classiques: l'utilisateur se connecte à eux par l'intermédiaire de son navigateur, puis saisit sur leur IHM l'adresse du site qu'il désire visiter. Le proxy interroge ce site à la place de l'utilisateur, puis renvoie les réponses (pages web) au navigateur de l'utilisateur comme si cette réponse venait de lui:



REMARQUE: Ce type de proxy est évidemment le plus facile à utiliser, mais il possède forcément des capacités limitées:

- Il se limite en général à l'interrogation de sites web;
- Ce type de site effectue souvent des compressions non réversibles des éléments graphiques ou audio, dégradant la qualité du rendu ;
- Les codes flash ou javascript attachés aux pages web renvoyées au client sont souvent inactivés;

V.2.LES PROXY HTTP:

Dans ce cas, la machine du client redirige systématiquement les requêtes HTTP issue des navigateurs vers le proxy :

- La requête émise par le navigateur vers le site qu'il désire consulter est interceptée,

puis "encapsulée" dans une requête adressée au proxy (tunnelisation);
- Celui-ci récupère la requête d'origine, puis l'émet vers le site ciblé, puis redirige la réponse vers le client.

L'installation de ce mécanisme n'exige en général qu'un paramétrage du navigateur qui consiste à saisir l'URL et le numéro de port du serveur proxy, puis à autoriser l'interception des requêtes. Sous chrome, par exemple, faire:
paramètres→système→ouvrir les paramètres proxy→ Paramètres réseau → Utiliser un serveur Proxy → Saisir l'url et le port du proxy).

V.3.LES PROXY "SYSTÈMES":

Il est possible d'installer le mécanisme de redirection au niveau du système d'exploitation: dans ce cas, ce sont toutes les communications réseau sortantes de la machine cliente qui sont redirigées vers le proxy. L'installation se fait par paramétrage du système d'exploitation (saisie de l'URL et du numéro de port du serveur proxy et autorisation de la redirection).

- Sous windows: paramètres→ Reseau et internet→ Proxy→ Configuration manuelle/Configuration automatique.
- Sous Linux: export http_proxy=http://"ip_proxy":"port_proxy".

VI.CONCLUSION:

- Il est important d'avoir confiance en l'administrateur du proxy que l'on utilise, qu'il s'agisse de celui que vous avez choisi ou de celui de votre entreprise (70% des entreprises américaines examineraient les accès des employés aux proxy).
- Il est recommandé de désactiver le proxy quand on accède à des sites nécessitant des mots de passe (ce n'est pas toujours possible…).