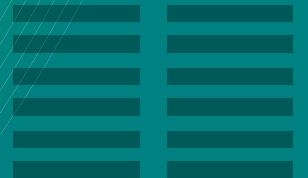


Proxy et reverse proxy

Serveurs mandataires et relais inverses



PORTAIL DE LA FORMATION PROFESSIONNELLE AU MAROC

Télécharger tous les modules de toutes les filières de l'OFPPT sur le site dédié à la formation professionnelle au Maroc : www.marocetude.com

Pour cela visiter notre site www.marocetude.com et choisissez la rubrique :

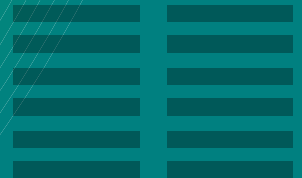
MODULES ISTA



The screenshot shows the homepage of the website *Maroc Etude.Com*. The header features a navigation bar with links: HOME, LIVRES, **MODULES ISTA**, ANNUAIRE ECOLES, DOCTORAT, LETTRE DE MOTIVATION, NOUS CONTACTER, and SE CONNECTER. Below the navigation bar is a large banner with the site's logo and the tagline "Connaissance - Métier - Technique". Underneath the banner are several service links: Annonces Google, Emploi Maroc, Messagerie, Télécharger Un Jeu, and Maroc Annonces. A search bar is located on the right side of the header. The main content area is divided into three columns. The left column contains a login section with fields for "Identifiant" (containing "sniper") and "Mot de passe", a "Connexion" button, and links for "Mot de passe oublié ?" and "Identifiant oublié ?". The middle column features a promotional banner for "MacKeeper" with a "-20%" discount, a coupon code, and a "Apply Discount Automatically" button. The right column displays a list of services under the heading "Annonces Google", including "Jeu De Jeux", "Jeux Sur Internet", "Ecole Ingénieur", and a section for "Dépanner et configurer votre réseau à domicile" with sub-links for "Outil de Diagnostic", "Wi-Fi / Ethernet", "Console de jeu", "Imprimante", and "Messagerie". At the bottom of the page, a quote reads: "On ne jouit bien que de ce qu'on partage" [Madame de Genlis].

Proxy et reverse proxy

- Qu'est-ce qu'un proxy ?
 - Proxy = mandataire (traduction)
 - Un proxy est un service mandataire pour une application donnée.
 - C'est à dire qu'il sert d'intermédiaire dans une connexion entre le client et le serveur pour relayer la requête qui est faite.
 - Ainsi, le client s'adresse toujours au proxy, et c'est lui qui s'adresse ensuite au serveur.



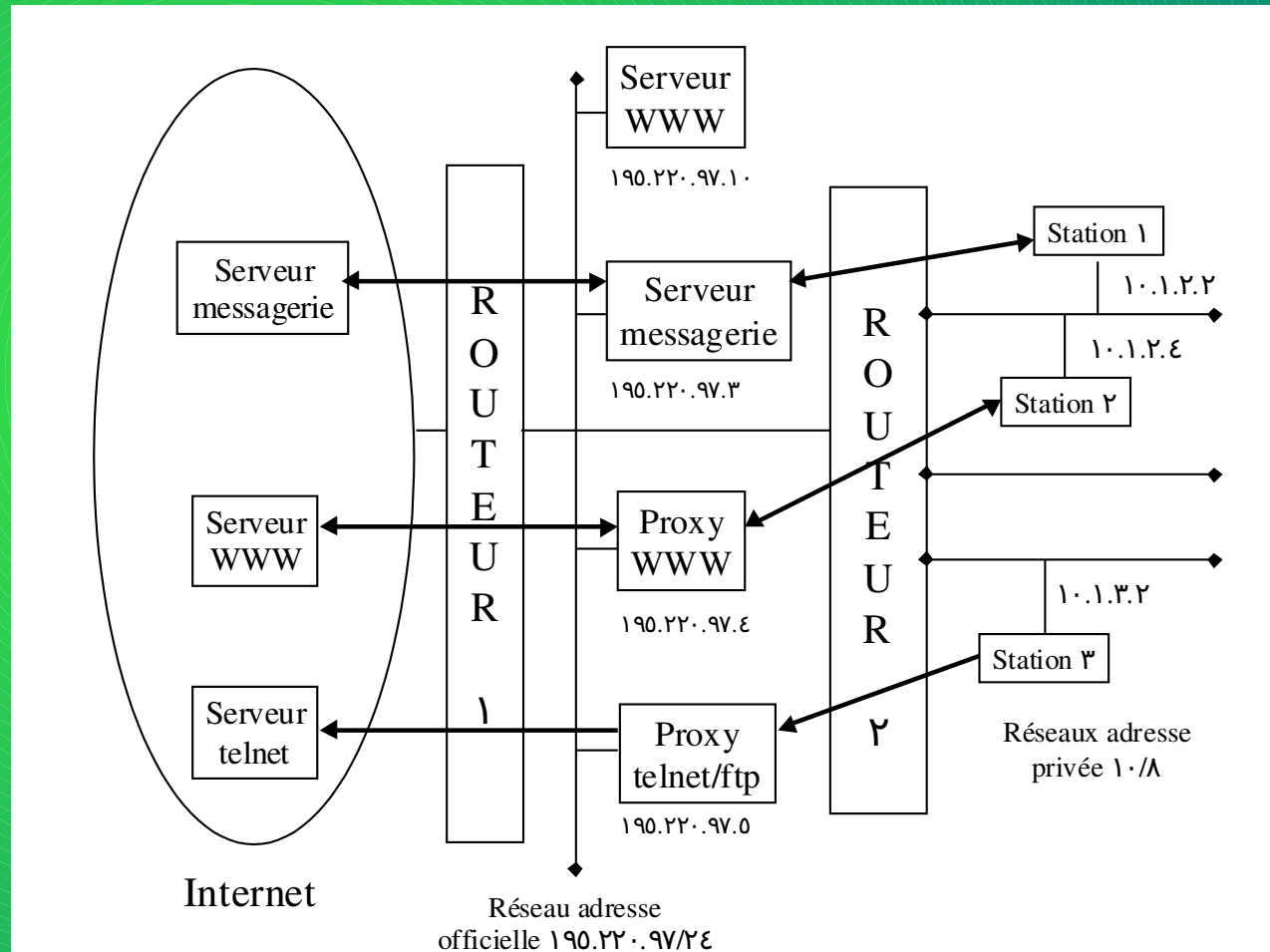
Proxy et reverse proxy

- Permet de casser complètement la connectivité directe à l 'internet des machines internes => possibilité de fermer tous les ports entre les machines internes et l 'internet
- Ne peuvent être utilisé que les applications supportées par un relais applicatif
- Exemples :
 - telnet ftp vers une machine relais puis vers l 'internet
 - cache Web (squid)
 - serveur relais de messagerie
 - existence de relais transparents pour certaines applications
 - socks

Proxy et reverse proxy

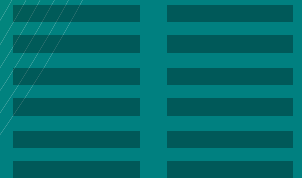
- Fonctionnement
 - Pour une application donnée, http, ftp, smtp, etc, il peut donc modifier les informations à envoyer au serveur, ainsi que celles renvoyées par celui-ci.
 - La contrepartie est qu'il faut un proxy par application.
 - Cependant, beaucoup de proxy sont en fait des multi-proxy qui sont capables de comprendre la plupart des applications courantes

Proxy et reverse proxy



Proxy et reverse proxy

- Fonctionnalités des serveurs
 - Fonctions de cache
 - Fonction de d'enregistrement
 - Fonction de filtre
 - Fonction de sécurité
 - Autres fonctions

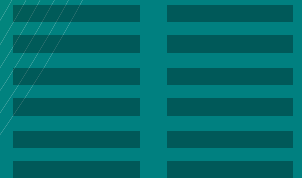


Proxy et reverse proxy

- Fonction de cache
 - Le client conserve en mémoire toutes les requêtes effectuées par le client
 - Permet de conserver localement les informations afin d'être réutilisées ultérieurement
 - Conséquence
 - le cache accélère les consultations des informations déjà demandée,
 - le trafic réseau en est diminué
 - Réduit les malveillances

Proxy et reverse proxy

- Fonction d'enregistrement
 - Le serveur garde une trace détaillée de toutes les informations qui le traversent
 - Génère un fichier journal (fichier de log).
 - enregistre la trace des requêtes effectuées par tous les clients utilisant le proxy.
 - L'identification du client,
 - les dates et heures de connexion,
 - Les URL des ressources consultés,
 - les taille et temps de téléchargement, etc.

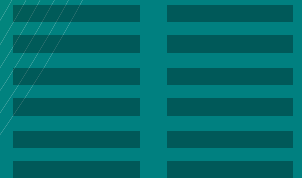


Proxy et reverse proxy

- Fonction de filtre
 - Mise en place de filtre au niveau des requêtes
 - Analyse des paquets qu'il reçoit et agit ainsi en fonction de la politique de sécurité choisie
- Fonction de sécurité
 - Serveur permettant de protéger les postes clients d'agressions extérieures
 - Protège des attaques via des accès directs
 - Attention ce n'est pas un firewall !

Proxy et reverse proxy

- Autres fonctions
 - Fonction d'anonymat
 - Les requêtes relayées par un serveur peuvent ne pas contenir d'adresse du client, de manière à protéger leur anonymat
 - Fonction de traduction d'adresse (NAT)
 - Permet à des réseaux privés de sortir vers l'Internet



Proxy et reverse proxy

- Avantages du proxy
 - Il est capable d'interpréter le trafic et notamment de cacher les informations. On diminue ainsi le trafic et augmente la bande passante de la même occasion.
 - On peut aussi autoriser ou non l'accès à certaines parties d'un site, à certaines fonctionnalités, etc.
 - On a donc un bon contrôle de ce qui transite sur le réseau, et on sait quels protocoles peuvent circuler.

Proxy et reverse proxy

- Proxy transparent

- Le principe :

- Le réseau est configuré avec une passerelle par défaut et un serveur DNS.
 - Chaque requête est automatiquement , et de manière invisible renvoyée vers le proxy par le routeur/firewall.
 - Le serveur proxy relaye la requete sur le serveur Internet et stocke l'information dans son cache.
 - Le client croit ainsi dialoguer avec le serveur internet , mais en réalité, elle ne dialogue qu'avec le serveur proxy.

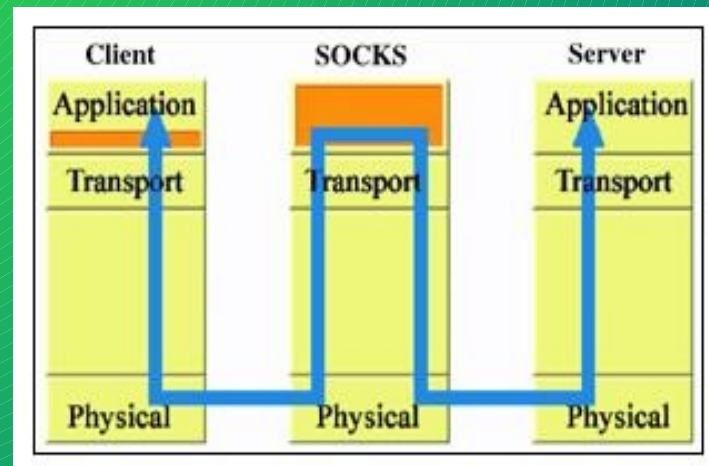


Proxy et reverse proxy

- Proxy transparent
 - Fonctions :
 - Mettre en cache les pages les plus visitées, afin d'éviter de recharger une page qui a déjà été visitée
 - Forcer les utilisateurs du réseau à utiliser un proxy, qu'ils le veuillent ou non.
 - Faire utiliser un proxy à toutes les machines d'un réseau sans avoir à configurer chaque application.
 - Bloquer des applications internet (comme les utilitaires de chat, ou de peer2peer)
 - sécuriser un réseau qui accède à internet en limitant l'accès à certaines pages.

Proxy et reverse proxy

- Proxy socks
 - Socks est un protocole proxy générique pour TCP/IP
 - Standard IETF, RFC 1928
 - Fonctionne en mode client-serveur
 - Agit au niveau des couches transport et application



Proxy et reverse proxy

- Proxy socks
 - Accès réseau transparent au travers de multiples serveurs proxy
 - Pour chaque canal de communication TCP ou UDP que le protocole SOCKS établit, il
 - Transfert les informations utilisateurs du client SOCKS au serveur SOCKS pour l'authentification des utilisateurs
 - Authentifie l'utilisateur et le canal
 - Garantit l'intégrité des canaux TCP et UDP

Proxy et reverse proxy

- Proxy socks

- Serveur socks linux (socks.conf) sur le port 1080/Tcp
- Permet l'implémentation de proxy dans des applications (programme java etc..)
- l'avantage de ce cette méthode c'est que l'on n'a pas besoin de connaître le protocole de communication des deux machines donc pas d'intervention sur les paquets qu'ils se transmettent (gain de temps)
- Inconvénient nécessite son implémentation dans les applications (clients)

Proxy et reverse proxy

- Squid

- C'est un serveur proxy cache haute performance, qui supporte les protocoles HTTP, FTP
- Il prend en compte toutes les requêtes demandées un seul processus qui est non-bloquant.
- Il conserve les données génériques et spécialement les objets très demandés en RAM
 - il met en cache les requêtes DNS,
 - et implémente le cache négatif lors les requêtes demandées ont échoué.



Proxy et reverse proxy

- Squid
 - Il support
 - le cryptage SSL,
 - une gestion des accès évoluée,
 - une journalisation complète des requêtes
 - Utilisation du protocole ICP (Internet Cache Protocol)
 - les caches de squid peuvent être référencés :
 - Par hiérarchie,
 - Par sites visités pour minimiser la bande passante utilisée

Proxy et reverse proxy

- Squid
 - Le package squid contient:
 - un programme principal nommé Squid ,
 - un système de DNS,
 - des outils de réécriture de requêtes et d'authentification,
 - et des outils de gestion.
 - Utiliser Iptables pour utiliser SQUID en tant que proxy transparent



Proxy et reverse proxy

- Squid

- Configuration de squid

- `http_port 3128` : c'est le port sur lequel travaille le cache, 3128 par défaut, certains déplacent ce port en 8080
 - `icp_port 3128` : c'est le port sur lequel le cache peut être interrogé par un autre serveur
 - `cache_mgr admin@formation.jussieu.fr` : c'est le nom de l'administrateur du serveur de cache
 - `cache_effective_user nobody nobody` : donne des droits à un utilisateur et un groupe pour squid (éviter root)
 - `visible_hostname cache.formation.jussieu.fr` : c'est le nom du serveur squid depuis les réseaux externes
 - `cache_mem 64 MB` : c'est la mémoire que l'on alloue à un serveur Squid

Proxy et reverse proxy

- Squid

- Configuration de squid:

- `cache_dir /var/cache 3200 16 256` : indique le répertoire devant accueillir les informations, avec en paramètre la taille disque, le nombre de répertoires niveau et sous niveau pour le cache
 - `cache_access_log /var/log/squid/access.log` : indique à le fichier log des requêtes appelées
 - `cache_log /var/log/squid/cache.log` : fichier journal de squid
 - `cache_store_log none` : pour ne pas enregistrer dans un fichier de log les écritures et effacements d'informations (très verbeux)

Proxy et reverse proxy

- Squid
 - Configuration de squid:
 - Règles d'accès au service
 - `acl HOST_AUTHORISE src 10.1.0.0/255.255.0.0` : on définit les réseaux ou les machines autorisées
 - `http_access allow CLIENTS` : on autorise les accès http aux machines définies dans l'`acl HOST_AUTHORISE`
 - `http_access deny all` : on interdit toutes les autres
 - Mise en place d'une hiérarchie de cache
 - `icp_access allow 192.168.1.10` : on autorise les accès icp aux machines définies dans l'`acl HOST_AUTHORISE`
 - `icp_access deny all` : on interdit toutes les autres

Proxy et reverse proxy

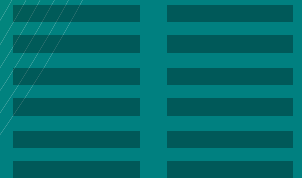
- Proxy transparent avec squid
 - Squid et iptables sur la même machine
 - Elle est moins sécurisée car le serveur proxy est accessible directement via le port TCP 3128
 - pour activer le proxy transparent il suffit de taper la ligne suivante :
 - `iptables -t nat -A PREROUTING -i eth0 -p tcp -s 192.168.1.0/24 --dport 80 -j REDIRECT --to-port 3128`

Proxy et reverse proxy

- Proxy transparent avec squid
 - Iptables et Squid sur deux machines différentes :
 - Les paquets ne provenant pas du proxy mais étant a destination du port 80 seront redirigés vers le proxy ; que les paquets revenant depuis le proxy, passeront par le routeur ; et que nous autorisons les paquets provenant du réseau local à être redirigés vers le proxy
 - iptables -t nat -A PREROUTING -i eth0 -s ! 10.1.0.1 -p tcp --dport 80 -j DNAT --to 172.20.0.1:3128
 - iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.0/24 -d 10.1.0.1 -j SNAT --to 172.20.0.4
 - iptables -A FORWARD -s 192.168.1.0/24 -d 10.1.0.1 -i eth0 -o eth1 -p tcp --dport 3128 -j ACCEPT

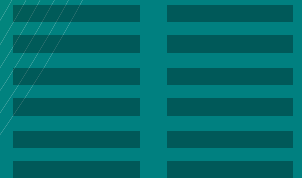
Proxy et reverse proxy

- Proxy transparent avec squid
 - Iptables et Squid sur deux machines différentes :
 - Modification du fichier squid.conf
 - `acl machines_locales src 10.1.0.0/16`
 - `http_access allow machines_locales`
 - `http_access deny machines_locales`
 - Et
 - `acl machines_locales src 192.168.1.0/24`
 - `http_access allow machines_locales`
 - `http_access deny !machines_locales`



Proxy et reverse proxy

- Reverse proxy
 - proxy à l'envers
 - Permettre à des clients externes d'utiliser un service interne
 - achemine des requêtes extérieures vers le serveur du réseau interne
 - garde les propriétés d'un proxy
 - Utilise SSL (avec l'accélération hardware)
 - amélioration des performances réseau via les caches ou/et un load balancing



Proxy et reverse proxy

- Reverse proxy
 - proxy à l'envers
 - Un relais inverse n'est utile que s'il apporte des fonctionnalités
 - d'authentification par mots de passe ou forte par certificats,
 - de chiffrement,
 - de filtrage applicatif
 - Pour protéger des scripts vulnérables, il faut que le relais inverse soit capable de filtrer les données envoyées par l'utilisateur dans URL