Services et serveurs

Un serveur web est, soit un logiciel de service de ressources web, soit un serveur informatique qui répond à des requêtes du World Wide Web sur un réseau public ou privé, en utilisant principalement le protocole HTTP.

Le serveur FTP permet de transférer des fichiers par Internet ou par le biais d'un réseau informatique local. Toute personne en ayant l'autorisation, peut télécharger et envoyer des fichiers sur un ordinateur distant faisant fonctionner un tel serveur. Le port par défaut et le plus souvent utilisé est le port 21.

Serveur de messagerie électronique Un serveur de messagerie électronique est un logiciel serveur de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie installé sur son terminal (ordinateur ou smartphone), soit une messagerie web, qui se charge de contacter le serveur pour envoyer ou recevoir les messages. On parle dans le premier cas de client lourd, dans le deuxième cas de client léger.

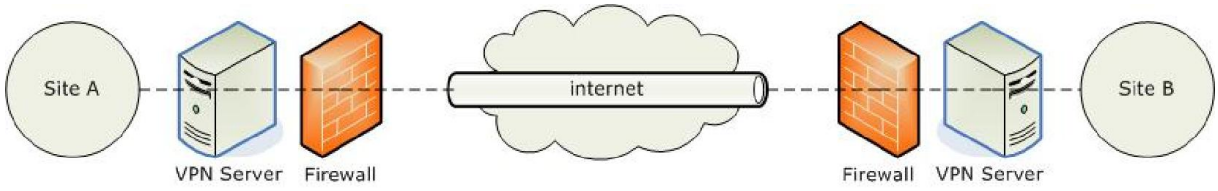
Telnet (***te**rminal **net**work* ou ***tel**ecommunication **net**work*, ou encore ***tel**etype **net**work*) est un protocole utilisé sur tout réseau TCP/IP, permettant de communiquer avec un serveur distant en échangeant des lignes de texte et en recevant des réponses également sous forme de texte.

Créé en 1969, telnet est un moyen de communication très généraliste et bi-directionnel. Il appartient à la couche application du modèle OSI .

Il était notamment utilisé pour administrer des serveurs UNIX distant ou de l'équipement réseau, avant de tomber en désuétude par défaut de sécurisation (le texte étant échangé en clair) et l'adoption de SSH.

VPN

réseau privé virtuel(**RPV**) ou **réseau virtuel privé** (**RVP**), plus communément abrégé en **VPN** (de l'anglais : *Virtual Private Network*), est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.



Principe d'un VPN simple

HTTPS HyperText Transfer Protocol Secure

L'**HyperText Transfer Protocol Secure** (**HTTPS**, littéralement « protocole de transfert hypertextuel sécurisé ») est la combinaison du HTTP avec une couche de chiffrement comme SSL ou TLS.

HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis par une autorité tierce, réputée fiable (et faisant généralement partie de la liste blanche des navigateurs internet). Il garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans les formulaires) et reçues du serveur. Il peut permettre de valider l'identité du visiteur, si celui-ci utilise également un certificat d'authentification client.

HTTPS était initialement surtout utilisé pour les transactions financières en ligne : commerce électronique, banque en ligne, courtage en ligne, etc. Il est aussi utilisé pour la consultation de données privées, comme les courriers électroniques, par exemple.

Un **serveur d'applications** est un logiciel d'infrastructure offrant un contexte d'exécution pour des composants applicatifs. Le terme est apparu dans le domaine des applications web. Au sens strict les composants hébergés par le serveur d'applications ne sont pas de simples procédures ou scripts mais de réels composants logiciels conformes à un modèle de composants (COM, Fractal, etc.).

Les clients des serveurs d'application sont : des programmes autonomes sont des applets ou d'autres composants.

Un **serveur d'impression** est un serveur qui permet de partager une ou plusieurs imprimantes entre plusieurs utilisateurs (ou ordinateurs) situés sur un même réseau informatique.

Le serveur dispose donc :

- d'une connexion réseau (par exemple, un port RJ45 pour un réseau ethernet) gérant les protocoles réseaux (par exemple, TCP/IP, NetBEUI, AppleTalk);
- d'une ou plusieurs connexions à des imprimantes. La plupart des serveurs d'impression disposent de connexions USB ; certains disposent également de ports parallèles. Certains serveurs d'impressions ne sont pas connectés directement par leur câble d'interface aux imprimantes. Ces dernières sont connectées via le réseau, en effet, les imprimantes professionnelles sont généralement connectées directement sur le réseau pour permettre une répartition au sein des locaux de l'entreprise.

Le serveur d'impression peut être constitué d'un ordinateur qui partage une imprimante qui lui est directement connectée (ou à travers le réseau), ce peut également être un petit appareil spécialisé dédié. L'avantage de cette dernière solution est son faible prix. Un serveur d'impression doit toujours rester sous tension et il est préférable qu'il ait une adresse IP fixe.

Il peut être situé sur un poste client : à partir du moment où l'imprimante est connectée sur un ordinateur et que celle-ci est partagée, ce poste devient ce que l'on nomme un serveur d'impression.

Les documents à imprimer sont placés sur des files d'attente (*spool*) puis envoyés petit à petit à l'imprimante.

Le système d'impression qui est le plus utilisé aujourd'hui sous Linux et Unix est CUPS (Common Unix Printing System).

Pour communiquer avec les imprimantes et les clients, les serveurs d'impressions utilisent une grande variété de protocoles tels LPD/LPR, IPP utilisé par CUPS, NetBIOS, AppSocket utilisé par les serveurs d'impression JetDirect ou encore IPX/SPX.

Network address translation

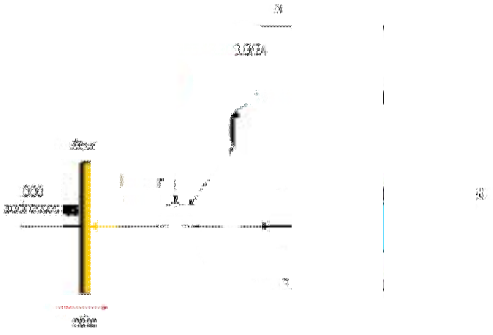
on dit qu'un routeur fait du ***network address translation*** (NAT) (« traduction d'adresse réseau » ou « translation d'adresse réseau ») lorsqu'il fait correspondre des adresses IP à d'autres adresses IP. En particulier, un cas courant est de permettre à des machines disposant d'adresses privées qui font partie d'un intranet et ne sont ni uniques ni routables à l'échelle d'Internet, de communiquer avec le reste d'Internet en utilisant vers l'extérieur des adresses externes publiques, uniques et routables.

Ainsi, il est possible de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, afin de pallier l'épuisement des adresses IPv4.

La fonction NAT dans un routeur de service intégré (ISR) traduit une adresse IP source interne en adresse IP globale.

Ce procédé est très largement utilisé par les box internet (ou modem routeur) des fournisseurs d'accès pour cacher les ordinateurs personnels derrière une seule identification publique. Il est également utilisé de façon similaire dans des réseaux privés virtuels.

Exemple



Réseau sans NAT : les adresses des hôtes sont des adresses uniques et routées sur Internet.

Réseau avec NAT : les adresses des hôtes sont des adresses réutilisables. Le routeur de bordure fait la traduction d'adresse. La modification du plan d'adressage alloue désormais un réseau /16 par sous-réseau, s'affranchissant de la limite des 254 adresses possibles avec un /24.

Un campus est composé de 1000 hôtes (ordinateurs, imprimantes, etc.), répartis dans 4 sous-réseaux. Sans utilisation du NAT, un tel campus nécessiterait l'attribution de presque 1 000 adresses IPv4 uniques et routées.

En connectant un tel campus à Internet via un routeur qui implémente NAT, il est possible de changer le plan d'adressage interne et d'utiliser des adresses non uniques (utilisées ailleurs dans le monde) et non routables sur Internet (voir RFC 1918[1]). On parle aussi d'adresses *publiques* (uniques au monde) et *privées* (uniques seulement dans le réseau privé). Un des buts du NAT est de rendre les adresses privées invisibles depuis Internet.

On n'assignera que quelques centaines d'adresses à l'ensemble des adresses externes du NAT.

implémentation du NAT

Les correspondances entre les adresses privées (internes) et publiques (externes) sont stockées dans une table sous forme de paires (*adresse interne*, *adresse externe*). Lorsqu'une trame est émise depuis une adresse interne vers l'extérieur, elle traverse le routeur NAT qui remplace, dans l'en-tête du paquet TCP/IP, l'adresse de l'émetteur par l'adresse IP externe. Le remplacement inverse est fait lorsqu'une trame correspondant à cette connexion doit être routée vers l'adresse interne. Aussi, on peut réutiliser une entrée dans la table de correspondance du NAT si aucun trafic avec ces adresses n'a traversé le routeur pendant un certain temps (paramétrable).

IP interne	IP externe	Durée (s)	Réutilisable ?
10.101.10.20	193.48.100.174	1 200	non
10.100.54.251	193.48.101.8	3 601	oui
10.100.0.89	193.48.100.46	0	non

Voici par exemple une table de NAT simplifiée. On supposera qu'une entrée pourra être réclamée si la traduction n'a pas été utilisée depuis plus de 3 600 secondes.

La première ligne indique que la machine interne, possédant l'adresse IP 10.101.10.20 est traduite en 193.48.100.174 quand elle converse avec le monde extérieur. Elle n'a pas émis de paquet depuis 1 200 secondes, mais la limite étant 3 600, cette entrée dans la table lui est toujours assignée. La seconde machine est restée inactive pendant plus de 3 600 secondes, elle est peut-être éteinte, une autre machine peut reprendre cette entrée (en modifiant la première colonne puisqu'elle n'aura pas la même IP interne). Enfin, la dernière machine est actuellement en conversation avec l'extérieur, le champ de *Durée* étant 0.

La plupart des pare-feu et routeurs implémentent le NAT pour permettre à plusieurs machines de partager une seule adresse IP publique.

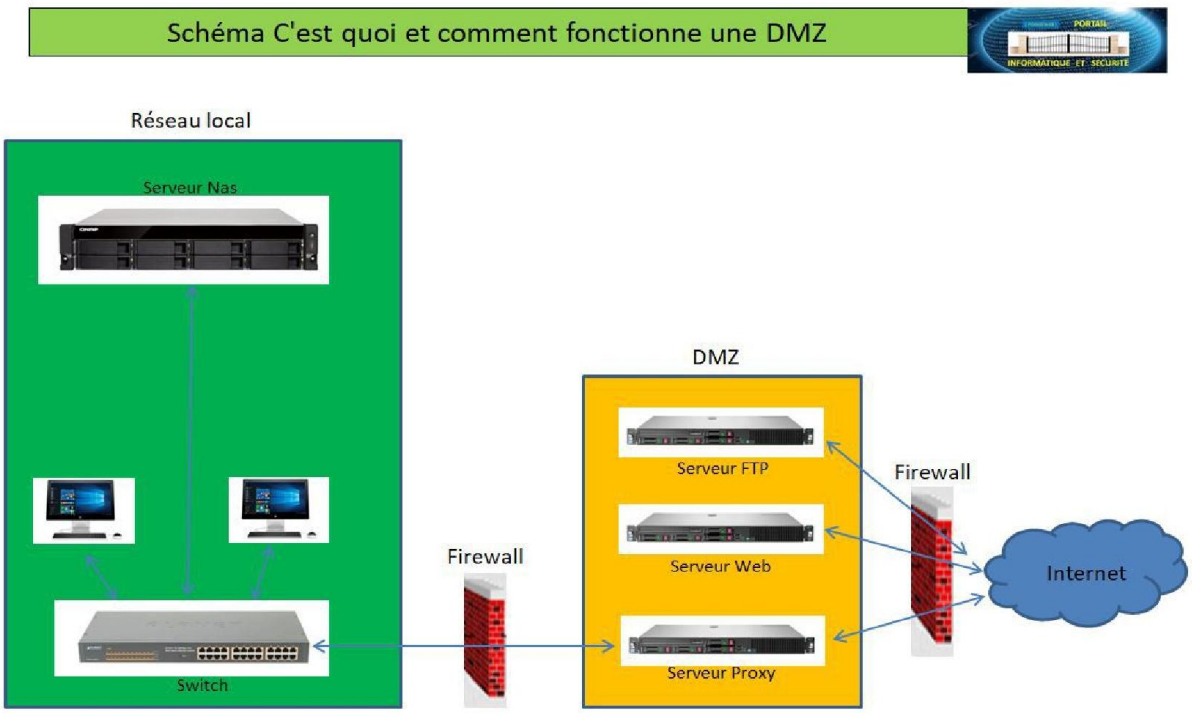
Bénéfices du NAT

- **Optimisation @ IP :**
  plusieurs sites peuvent avoir le même adressage interne et communiquer entre eux en utilisant ce mécanisme. Étant donné que les adresses internes sont réutilisées, on économise des adresses IP publiques, dont l'occupation, en IPv4, arrive à saturation.
- **Sécurité :**
  @ IP sont cachées et invisibles.

Zone démilitarisée

Une **zone démilitarisée**, ou **DMZ** (en anglais, *demilitarized zone*) est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local.

On entend par une zone démilitarisée un réseau d'ordinateur qui sert de zone tampon entre deux réseaux et qui dispose de sa propre adresse IP. Leurs règles d'accès sont clairement délimitées. Les serveurs qui se trouvent à l'intérieur d'une DMZ sont encore physiquement dans l'entreprise mais ne sont pas directement liés aux machines connectées au réseau local. La fonction de protection la plus performante a une architecture où la zone démilitarisée fait écran aux réseaux voisins entre le LAN et Internet via un pare-feu séparé. En revanche, les architectures de réseaux, où tout est relié à un seul pare-feu accompagné de trois terminaux distincts, sont plus avantageuses. On parle alors d'un DMZ protégé (soit DMZ protected en anglais).



Un data center est un ensemble d'éléments. Un **centre de données basique regroupe des serveurs, des sous-systèmes de stockage, des commutateurs de réseau, des routeurs, des firewalls, et bien entendu des câbles et des racks physiques permettant d'organiser et d'interconnecter tout cet équipement informatique**.
Pour fonctionner correctement, **un Data Center doit aussi abriter l'infrastructure adéquate : un système distribution d'énergie, un commutateur électriques, des réserves d'énergie, des générateurs dédiés au backup, un système de ventilation et de refroidissement, et une puissante connexion internet**. Une telle infrastructure nécessite un espace physique suffisamment vaste et sécurisé pour contenir tout cet équipement.

Data center

Qu'est-ce qu'un pare-feu?

Un **pare-feu** (appelé aussi *coupe-feu*, *garde-barrière* ou **firewall** en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant **de filtrer les paquets** de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne) ;
- une interface pour le réseau externe.

Fonctionnement d'un système pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (*allow*) ;
- De bloquer la connexion (*deny*) ;
- De rejeter la demande de connexion sans avertir l'émetteur (*drop*).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la **politique de sécurité** adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- soit d'autoriser uniquement les communications ayant été explicitement autorisées (c'est le Principe du moindre privilège) ;
- soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

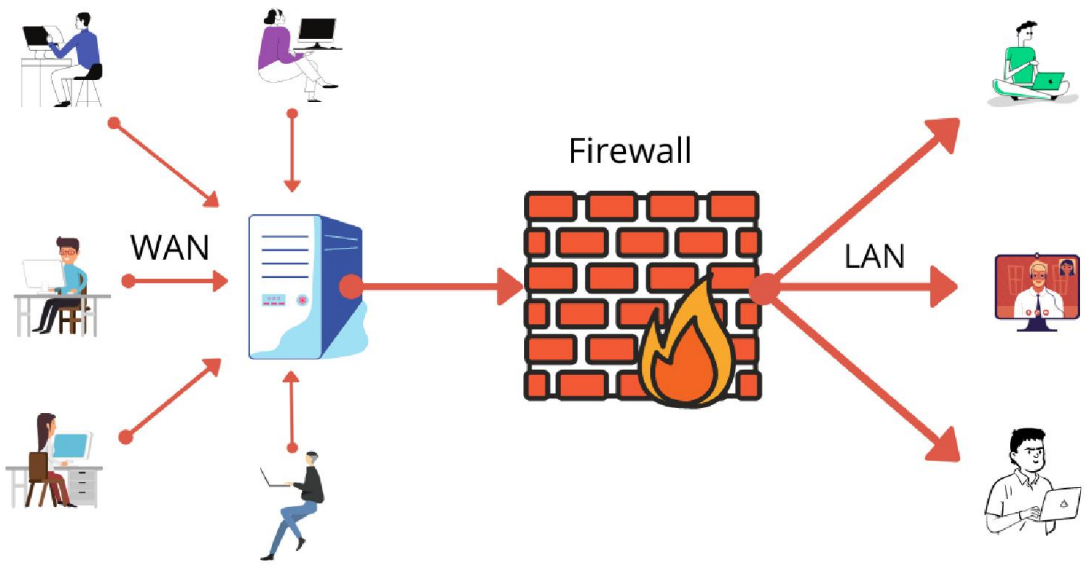
Le filtrage simple de paquets

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « *stateless packet filtering* »). Il analyse les en-têtes de chaque paquet de données (*datagramme*) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- adresse IP de la machine émettrice ;
- adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;
- numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé (ex port 80 Web).



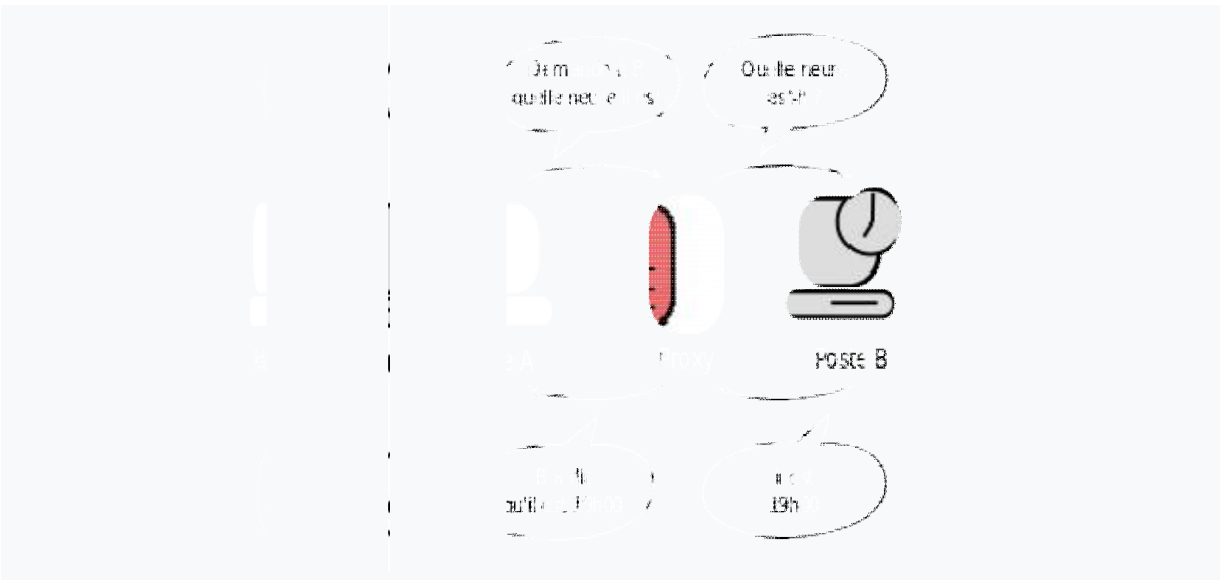
Proxy

Un **proxy** est un composant logiciel informatique qui joue le rôle **d'intermédiaire** en se plaçant entre deux hôtes pour faciliter **ou surveiller leurs** échanges.

Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement Internet. Par extension, on appelle aussi « proxy » un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services.

Attention : le proxy se situe au niveau **de la couche application** (HTTP, FTP, SSH, etc. de niveau 7).

Proxy réseau



Principe du proxy réseau.

Dans l'environnement plus particulier des réseaux, un serveur proxy, serveur mandataire[1] ou mandataire[1], est une fonction informatique client-serveur qui a pour fonction de relayer des requêtes entre une fonction cliente et une fonction serveur (couches 5 à 7 du modèle OSI).

Les serveurs proxys sont notamment utilisés pour assurer les fonctions suivantes :

- accélération de la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds (Java, Flash) ;
- la journalisation des requêtes (historique) ;
- la sécurité du réseau local ;
- le filtrage et l'anonymat.

Dans le cadre de la sécurité

L'utilité des serveurs proxys est importante, notamment dans le cadre de la sécurisation des systèmes d'information.

1. Par exemple, un site interdit >> un message d'erreur : un tel proxy est appelé proxy filtrant.
2. boite de dialogue s'ouvre et demande un identifiant et un mot de passe avant de pouvoir surfer sur Internet.
3. Ex : Le proxy web Glype ne permet pas de consulter des sites comme Facebook ou YouTube