Sécurisation de l'interconnexion de réseaux

Il est devenu très rare que le réseau local de l'entreprise soit isolé. Son interconnexion avec Internet, ou tout autre réseau, est devenue chose courante. Il est donc nécessaire de protéger les entrées et sorties sur le réseau interne privé. Différents équipements peuvent être mis en place pour réaliser cette sécurisation.

1. Routeur filtrant

Les mécanismes de filtrage qui peuvent être associés à l'équipement routeur autorisent des analyses de la couche 3 (Réseau) du modèle OSI.

L'examen des paquets entrants ou sortants porte ainsi, par exemple, sur l'en-tête IP, ce qui permet des actions comme :

- Le blocage d'adresses IP (source et destination).
- L'interdiction de transmission de protocoles de couche Réseau ou Transport utilisés (UDP, TCP ou ICMP)...

Certains équipements comprennent les en-têtes de couche 4 (Transport). Ils peuvent ainsi, entre autres, exercer un filtrage au niveau des ports TCP ou UDP et même aller jusqu'à l'analyse des données applicatives (couche 7).

2. Translateur d'adresse

Dans des entreprises de grande taille, différents réseaux interconnectés peuvent utiliser les mêmes adresses IP. Pour que la communication soit possible entre nœuds des deux côtés, il est nécessaire de modifier les références de l'émetteur du paquet, afin qu'il n'y ait pas de conflit et que la transmission soit fiable.

Des équipements de translation d'adresse (NAT - *Network Address Translation*) sont chargés d'apporter cette fonctionnalité. Ils permettent le changement d'une adresse IP par une autre.

Trois types de translation d'adresse sont possibles :

- La translation de port (PAT - *Port Address Translation*), joue sur une allocation dynamique des ports TCP ou UDP, en conservant l'adresse IP d'origine.
- La conversion dynamique d'adresse change à la volée l'adresse IP, par rapport à une externe disponible dans une liste.
- La conversion statique d'adresse, effectue également un changement d'adresse IP, mais une table est maintenue, permettant à une adresse IP interne de toujours être remplacée par la même adresse IP externe.

On peut remarquer que la conversion dynamique d'adresse permet de disposer de moins d'adresses externes que d'adresses internes, ce qui n'est pas le cas de la version statique.

Une translation de l'adresse IP peut également être réalisée en sortie du réseau local. Elle permet de masquer l'adresse interne privée. Un tel fonctionnement est prévu de longue date et la RFC 1918 définit les plages d'adresses exploitables dans les réseaux privés. Les trois espaces réservés sont :

- 10.0.0.0, avec un masque sur 8 bits (255.0.0.0).
- 172.16.0.0, avec un masque sur 12 bits (de 172.16.255.254 à 172.31.255.254).
- 192.168.0.0, dont le masque est sur 16 bits (255.255.0.0).

Nous pouvons remarquer que seule la première plage d'adresses respecte la notion de classe initiale, en l'occurrence ici A.

Toutes les autres adresses sont qualifiées de publiques et peuvent être utilisées sur le réseau Internet.

Ainsi, par exemple, un poste de travail du réseau local effectuant une demande de site web sur Internet, verra son adresse IP d'émetteur translatée vers une adresse publique en sortie du LAN.

3. Pare-feu

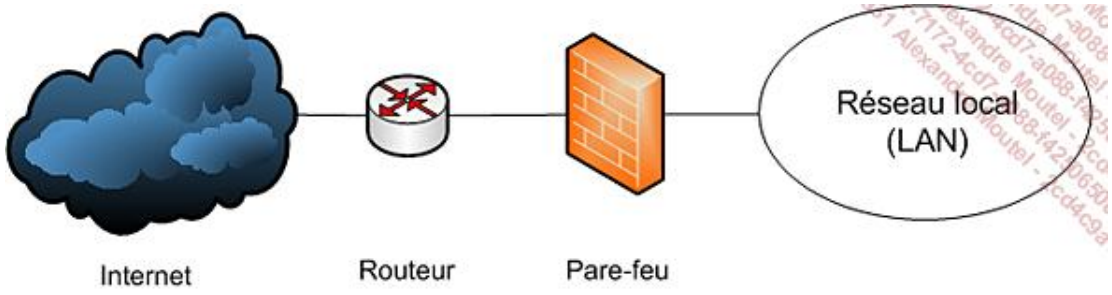
Un équipement de pare-feu (firewall) rend indépendant les différents réseaux auxquels il est connecté. Contrairement au routeur, il ne se contente pas de transmettre la demande. Ainsi, un pare-feu segmente les flux en prenant en charge lui-même les demandes. Il établit pour cela deux connexions et peut exercer une action d'authentification.

Une telle segmentation permet également le changement de l'adresse du demandeur, comme un mécanisme de translation d'adresse.

La première génération de ces équipements autorise différents examens sur les en-têtes de paquets, actions similaires à ceux des routeurs filtrants. Le pare-feu à table d'état (*statefull inspection*), plus récent, conserve en mémoire une table des connexions établies. Ainsi, les communications entre clients, autorisés après authentification, continuent sans rupture.

La nouvelle génération de pare-feu, dite applicative, devient capable d'analyser certains corps de paquets, tels que ceux des protocoles SMTP, HTTP... Un tel niveau d'analyse permet de pallier aux nouvelles formes d'attaques, qui profitent de failles sur ces applicatifs standard.

Le pare-feu d'infrastructure est même régulièrement complété par un pare-feu personnel, installé sur les postes de travail. Ce dernier est ainsi protégé d'attaques qui pourraient provenir de l'intérieur même du réseau local.

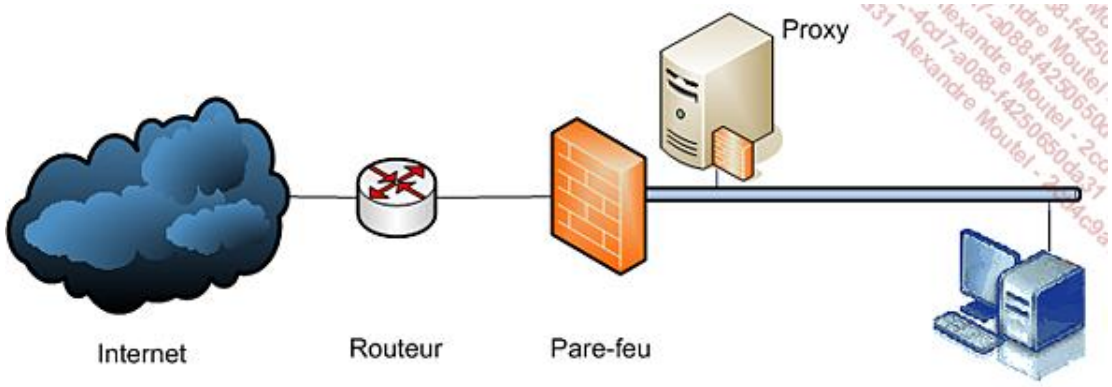


4. Proxy

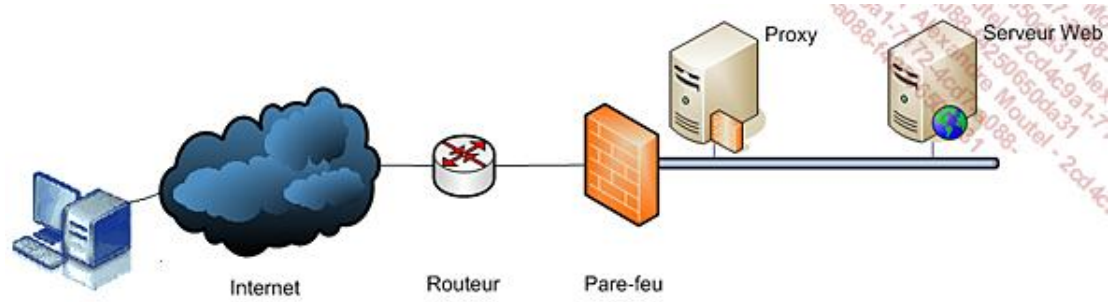
Le serveur mandataire, ou proxy, est particulièrement utilisé dans le cadre de trafics *Hyper Text Transfer Protocol* (HTTP), voire *File Transfer Protocol* (FTP) entre le réseau LAN et l'Internet. On peut considérer qu'il complète l'équipement pare-feu.

Interceptant une demande vers l'extérieur, le proxy la fait en son propre nom, puis stocke les données renvoyées. Ensuite, il les retransmet au demandeur initial. L'intérêt du proxy est double. Tout d'abord, il camoufle les adresses IP internes, puisque la demande n'est pas prolongée jusqu'à l'Internet. Ensuite, il autorise des filtrages, par exemple pour interdire l'accès à certains sites web.

Un troisième avantage du proxy est sa capacité à gérer une mémoire cache. Ainsi, il est possible d'éviter de redemander un fichier ou un site sur Internet. Au niveau Web, une telle fonction est à relativiser. En effet, un site dynamique change tellement régulièrement qu'on peut souvent considérer qu'il est rechargé à chaque demande.



Un équipement de serveur mandataire inverse (*reverse proxy*) intercepte une demande, par exemple de site web, provenant de l'extérieur, vers un serveur interne. Il permet ainsi d'éviter que de telles requêtes arrivent sur un serveur plus sensible.

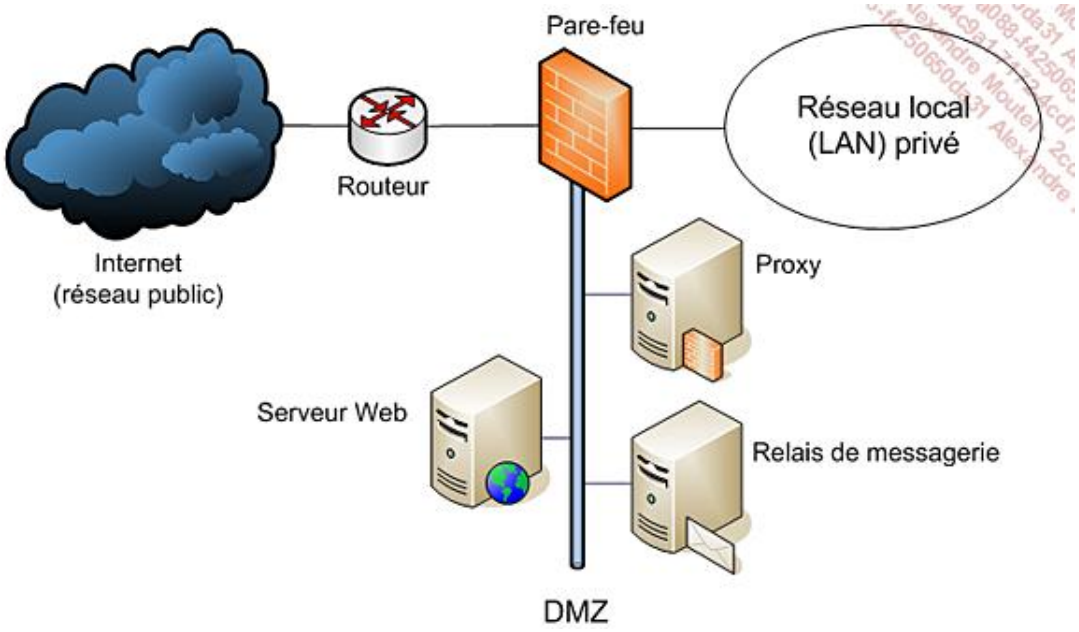


5. Zone démilitarisée

L'interconnexion entre le réseau public Internet et le LAN utilise très souvent une zone publique tampon, hébergée dans l'entreprise. Ce sas est nommé zone démilitarisé ou *DeMilitarized Zone* (DMZ). Elle héberge différents serveurs accessibles depuis l'Internet, tels que :

- Le serveur proxy.
- Le serveur web hébergeant le site de l'entreprise.
- Le relais de messagerie, chargé de réaliser un tri des messages...

La frontière de cette DMZ est concrétisée par au moins un pare-feu. Dans des infrastructures de petite taille, il est souvent unique. Dans ce cas, il est qualifié de tri résident.



Des infrastructures de plus grande taille hébergent une DMZ protégée par deux pare-feu dos à dos. Ils sont configurés dans ce cas de manière complémentaire et sont généralement de marques différentes, pour ne pas présenter les mêmes failles.