**Sécurisez votre réseaux grâce aux VPN et Firewall**

# Protégez vos données en installant un firewall

## Ne faites pas entrer tout le monde chez vous



Le firewall est comme ta porte d’entrée et ta maison ton réseau informatique. La rue est Internet.

Le firewall, vous l’avez compris, c’est donc votre porte, votre maison correspond à votre réseau privé et la rue, c’est tout simplement Internet.

La raison principale d’un firewall est que, sans lui, toutes les personnes connectées à Internet pourraient se connecter à votre réseau. Mais il vous permet aussi de limiter votre sortie vers l’extérieur. À l’image d’un enfant qui ne pourrait pas sortir seul dans la rue, vous pouvez bloquer ou limiter l’accès de certains utilisateurs ou serveurs vers Internet.

## Placez votre firewall au bon endroit

Il doit être placé entre deux réseaux (donc à côté d’un routeur)  
Il doit être un passage obligatoire entre le réseau que l’on veut protéger et le reste des réseaux.

Ce firewall est soit physique, soit logiciel (il peut être installé sur votre ordinateur) :

Un firewall logiciel est installé sur un OS (Windows, Linux, IOS) et consomme du processeur en plus de l’OS. Il est de plus soumis aux failles de sécurité de l’OS. N’étant qu’un logiciel comme un autre, une faille dans l’OS pourrait par exemple permettre de désactiver le firewall.

Un firewall matériel fonctionne théoriquement de la même façon, mais il n’est dédié qu’à sa tâche et sa charge CPU n’est pas un problème étant donné qu’il est installé sur une machine dédiée.

Pour sécuriser un réseau d’entreprise, on utilise, bien évidemment, un firewall physique, mais on configure aussi les firewalls logiciels de chaque PC et serveur.

## Découvrez le fonctionnement d’un firewall

Pour sécuriser votre réseau, un firewall utilise plusieurs techniques :

Il empêche des intrus d’entrer totalement.   
Il filtre et ne laisse entrer que sous certaines conditions (adresse IP et port).  
Il empêche les utilisateurs de votre réseau de sortir n’importe où, n’importe comment.

Pour réaliser cela, un firewall se base sur les couches 3 (IP) et 4 (TCP/UDP les ports donc) du modèle OSI mais aussi sur la couche 7, la couche applicative, donc sur des protocoles comme HTTP.

Un firewall qui se base sur les couches 3 et 4 vous permet de contrôler les adresses IP et les ports, pour par exemple bloquer ssh ou telnet, alors qu’un firewall qui se base sur la couche 7 vous permet de bloquer l’utilisation d’un logiciel peer-to-peer par exemple.

Attention, un firewall ne permet pas de bloquer les virus ! Pour cela, il vous faut un antivirus. En général, on couple les deux dans une société.

Votre firewall ne vous permet pas non plus de vous protéger contre une personne à l’intérieur de votre réseau !

## Ce qu’il faut retenir

* Un firewall permet de sécuriser un réseau d’un autre réseau, il doit donc être placé entre deux réseaux.
* Le passage par le firewall doit être obligatoire.
* Un firewall peut être physique (matériel) ou logique (logiciel).
* Un firewall ne protège pas contre les virus.
* Un firewall peut soit se baser sur les adresses IP ainsi que les ports, soit sur les applications.
* Un firewall ne protège pas votre réseau d’une personne à l’intérieur du réseau.
* Un firewall ne se configure pas tout seul, mais demande une étude préalable.