**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.

# Définissez une politique de sécurité

## Une politique de sécurité c’est quoi ?

Une politique de sécurité c’est le fait d’exposer les besoins de l’entreprise (son utilisation d’Internet) et d’en déduire les règles qui lui permettent son bon fonctionnement, tout en sécurisant au maximum l’entreprise.

C’est donc en concertation avec d’autres membres de l’entreprise que sera créée la politique de sécurité. L’administrateur système et cloud ne peut pas le faire seul. Il doit se concerter avec tous les services de l’entreprise afin d’établir les services utilisés par l’entreprise sur le web et sur les serveurs de l’entreprise.

## Bloquez tout et autorisez petit à petit

Votre politique de sécurité commence donc comme ceci : tout est interdit !

Vous autoriserez petit à petit ce qui est sorti des réunions avec les différents services de l’entreprise. Par exemple, si une réunion a conclu que :

* Les utilisateurs ont besoin d’accéder au Web = ouverture port HTTP.
* Les utilisateurs ont besoin d’accéder à leurs mails = ouverture port POP ou IMAP.
* Le serveur doit être accessible depuis Internet = ouverture port HTTP.

La politique de sécurité consistera donc à interdire tout sauf les protocoles :

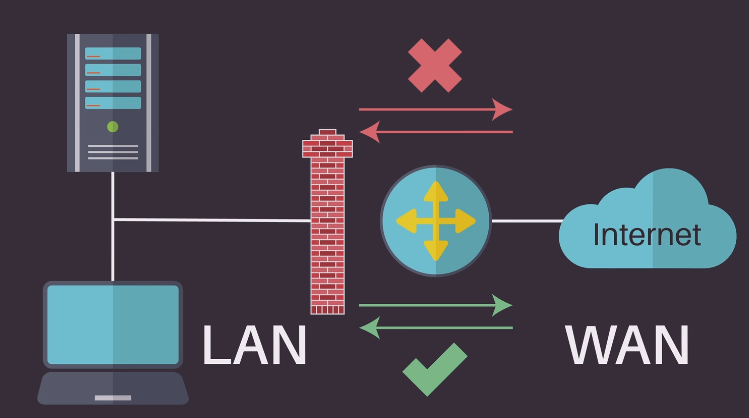
* HTTP
* POP
* IMAP

Il est évidemment possible d'affiner cela, en définissant sur quels sites les utilisateurs ont le droit d’aller, ou plutôt leur interdire certains sites. Définir des utilisateurs avec des droits différents, si par exemple l’équipe R&D a besoin de télécharger certains fichiers, vous les regrouperez et leurs autoriserez le téléchargement FTP, mais il restera bloqué pour les autres utilisateurs.

# Choisissez la bonne architecture

## L’architecture simple (couche réseau et transport)

Le firewall est simplement positionné entre le LAN et le WAN.



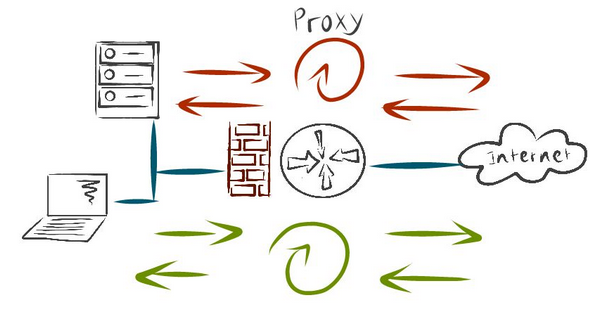
C’est l’architecture la plus connue et la plus utilisée :

* On filtre au niveau des adresses IP (couche 3) et des ports TCP/UDP (couche 4).
* On autorise les règles définies dans la politique de sécurité.
* Cette solution est peu coûteuse, un hardware peu puissant combiné à un firewall open source est suffisant.
* Il faut que l’administrateur cloud et infrastructure ait une bonne connaissance des règles à appliquer.
* Elle ne permet pas de filtrage sur les services tels que HTTP ou FTP (il est impossible d'empêcher du peer-to-peer par exemple).

Je vous conseille d’utiliser cette architecture lorsque le client ne possède pas de serveur interne ouvert sur l’extérieur.

## L’architecture proxy (couche application)

Il s’agit en fait, de la même architecture mais on ajoute un filtre, au niveau de la couche applicative. On va donc pouvoir filtrer des protocoles tel que HTTP et non pas le port HTTP (80, 443). Ceci va par exemple vous permettre d'empêcher l’utilisation du peer-to-peer.



Pour résumer cette architecture :

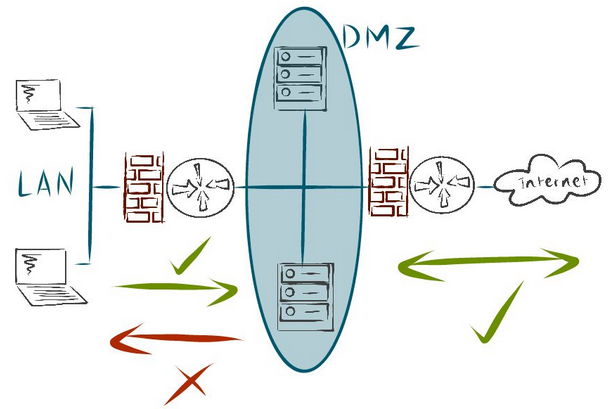
* Filtre la couche applicative et donc les protocoles HTTP et autre.
* Contrôle le réseau par utilisateur et donc permet de garder un historique.
* Permet de faire circuler le trafic HTTP et FTP via le proxy, en cas d’attaque, l’attaque se ferait sur le proxy et non sur le poste utilisateur.
* Permet de voir les attaques potentielles (IDS).
* Est très coûteux, plus vous avez d’utilisateurs et plus votre connexion Internet est puissante, plus vous devrez avoir un firewall puissant. Il faudra dans ce cas un investissement beaucoup plus conséquent que pour firewall de couches 3 et 4.

Je vous conseille d’utiliser cette architecture pour un client ayant besoin de contrôler l’utilisation de son réseau, comme une école par exemple ou un réseau wifi libre-service. C’est dans ces cas-là que l’on trouve le plus souvent des utilisateurs dangereux (pirates), imprudents (téléchargements) ou dans l'illégalité (peer-to-peer).

## La zone démilitarisée (DMZ)

La DMZ est une architecture qui permet de sécuriser votre réseau local, alors même que vous voulez le rendre accessible sur Internet.

Imaginez que votre client souhaite vendre ses produits sur le Web, vous configurerez le PAT (cours CISCO) sur le routeur relié à Internet. Mais en rendant son serveur accessible depuis Internet, vous rendez son LAN vulnérable aux attaques venues de l’extérieur.



La DMZ vous permet de rendre votre serveur accessible sur le Web tout en sécurisant votre LAN. Ceci est possible grâce à l’ajout d’un deuxième firewall entre le LAN et les serveurs. L’idée est la suivante :

* une règle permet au Web de se rendre sur le serveur, par le routeur/firewall externe. L’accès est autorisé selon le protocole voulu (HTTP par exemple). Tous les autres services doivent être désactivés et la connexion ssh ne doit pas pouvoir se faire depuis le WAN.
* Une autre règle permet au LAN de se rendre sur le serveur (par SSH par exemple), tout en empêchant le serveur de se rendre sur le LAN. Ainsi, même s’il venait à se faire pirater, le serveur ne pourrait pas contaminer le LAN.

Notez qu’il est encore une fois possible d’y ajouter les concepts des deux premières architectures.

Vous l’avez compris, mais je vous le redis quand même, c’est cette architecture que je vous conseille d’utiliser si votre client dispose d’un serveur accessible depuis le WEB.

Vous pouvez ajouter à toutes ces architectures l’architecture NAT. Le NAT, en cachant les adresses IP du LAN, protège les utilisateurs contre les attaques directes et contre l’écoute du réseau depuis l’extérieur.

# Comment fonctionne un pare-feu ?

## Filtrer les IP, les ports

Nous l’avons déjà dit, mais un tel firewall se base sur la couche réseau et la couche transport. Regardons comment se schématise l’entrée d’un paquet dans un firewall Iptable.

Iptables est un module du noyau Linux depuis la version 2.4. Au 12 avril 2018, nous sommes à la version 4.16.2

**Fonctionnement**

Lorsque le paquet arrive sur votre firewall, après avoir été routé vers sa destination par le routeur, il peut prendre deux chemins, appelés **chaînes** :

* INPUT, si le paquet lui est destiné.
* ou FORWARD, si le paquet ne fait que traverser le firewall vers un autre terminal.

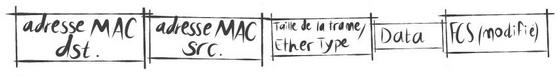
Un paquet émis par votre firewall va quant à lui passer par la chaîne OUTPUT.

**Filtrage**

Ipatbles, pour filtrer ses paquets, se base sur plusieurs propriétés du paquet :

* L’entête IP
* Le TCP ou UDP header

Voilà un petit rappel du format d’un datagramme IP.



Iptables se basant sur ce datagramme, vous pouvez filtrer les paquets sur tout ce qui compose la structure du datagramme.

Vous vous intéresserez sûrement plus particulièrement :

* Pour l’entête IP :
  + Aux flags, pour la fragmentation
  + Aux Protocol (en général TCP, UDP ou ICMP)
  + A l’Adresse source et destination
* Pour l’entête source ou destination :
  + Aux ports source et destination.
  + Aux flags pour le protocole TCP (nous y reviendrons dans un prochain chapitre)

Une règle de filtrage pourra donc par exemple être :

* Interdire les paquets avec adresses source X.X.X.X
* Interdire les paquets avec adresses destination X.X.X.X
* Interdire les paquets TCP
* Interdire les paquets UDP
* Interdire les paquets avec port de destination 22 (pour la connexion SSH)

**Lisez les règles, une par une**

Ces règles sont séquentielles, c’est-à-dire qu’elles sont lues dans l’ordre, l’une après l’autre.

Si un paquet tombe sur une règle qui le concerne, qu’il l’accepte ou le refuse, l’acceptant ou le refusant, la lecture s’arrête.

C’est pour cette raison que les règles les plus globales doivent être placées à la fin, alors que les règles les plus fines, elles, doivent être placées au début.

Le risque majeur est qu’une règle globale englobe justement une règle plus fine qui ne sera jamais lue.

## Filtrer une application

Filtrer une application, que vous trouverez sous le nom de Deep packet inspection (DPI), vous permet donc de lire le livre, c’est-à-dire de filtrer au niveau de la couche **application** du modèle OSI. C’est le rôle d’une **architecture proxy.**

Cela veut dire qu’en tant qu’administrateur infrastructure et cloud, vous pourrez voir si un virus est téléchargé, ou si un utilisateur utilise du peer-to-peer et donc, si nécessaire, le lui interdire.

Le constructeur du DPI analyse des attaques, comme les spams, les virus, ou des types de trafic, comme celui de Facebook, YouTube ou des logiciels de peer-to-peer. Cette analyse lui permet d’établir une empreinte (une signature) pour chaque type de trafic.

Il enregistre ensuite ses empreintes dans sa base de données, que vous possédez dans votre firewall. Votre firewall est donc en mesure de savoir ce qui se passe sur votre réseau en analysant le trafic et en le comparant aux empreintes fournies par le constructeur.

L’avantage de cette technique est que cela vous facilite énormément le travail. Analyser le trafic pour un administrateur est simplement impossible, surtout lorsque la bande passante augmente en permanence.

# Vérifiez les protocoles à risque

## Ne bloquez pas tous les accès

Vous vous demandez sûrement pourquoi je ne vous fais pas une liste de services et de ports dangereux, que vous bloqueriez dès l’installation de votre firewall.

La raison est simple, ces services sont utilisés par les utilisateurs de votre réseau. Vous ne pouvez donc pas les interdire, car ils sont nécessaires au bon fonctionnement de l’entreprise. Ils devraient donc apparaître dans la politique de sécurité si celle-ci a été bien conçue.

Ceci est très paradoxal, mais vous allez devoir ouvrir des services susceptibles de laisser entrer une attaque.

Il faut ajouter à cela deux choses, la première, qui n'est pas une fatalité, est qu'il n'existe pas de sécurité absolue. La seule sécurité absolue serait de fermer votre LAN de l'accès Internet, ce que vous ne voulez évidemment pas. La deuxième est qu'il existe, en plus des architectures que nous avons vues, des solutions pour sécuriser ces services laissés ouverts.

Voyons cela, service par service.

## Autorisez et sécurisez vos accès

**SMTP (Simple Mail Transfert Protocol)**

C'est le protocole qui permet à vos utilisateurs d'envoyer et recevoir des mails. Il est donc fort probable que vous soyez amené à devoir l’ouvrir.

Si vous hébergez un serveur SMTP, vous devrez donc ouvrir les différents ports qu’il utilise (25, 465, 587).

Pour sécuriser ce protocole, vous avez néanmoins quelques solutions :

* Utilisez une architecture proxy, ce qui vous permet de vérifier le service SMTP.
* Utilisez des connexions chiffrées et sécurisées avec TLS ou SSL.
* Configurez votre serveur de mail, pour qu’il ne relaie que vos mails, et ce afin que les spammeurs n’utilisent pas votre serveur pour envoyer des mails (problème assez courant).
* Protégez-vous contre les attaques DoS (déni de service), qui vous empêche d’utiliser votre serveur mail, en configurant fail2ban (https://openclassrooms.com/courses/proteger-son-serveur-avec-fail2ban).
* Configurez l’authentification, afin qu’un utilisateur sans login et mot de passe ne puisse utiliser le serveur SMTP.
* Mettez à jour vos listes noires grâce aux DNSBL (Domain Name System Blacklists). Il s’agit de liste de nom de domaine reconnue comme spammeur.
* Utilisez un antispam comme SpamAssassin.

**HTTP**

Sans ce protocole, pas de navigation Internet. Aucun doute que vos utilisateurs en aient besoin.

Pour le sécuriser :

* Utiliser une architecture proxy, avec firewall type DPI.

**Accès à distance**

Il s’agit des méthodes de connexion à vos serveurs et autres appareils :

* N’autorisez que SSH et indiquez les adresses IP sources ayant le droit de se connecter.

**Le transfert de fichier**

Si vos utilisateurs en ont le besoin, ou s’y un de vos serveurs utilise FTP, il vous faudra :

* Utilisez FTPS qui est une combinaison de FTP et de SSL ou TLS
* Utilisez une architecture proxy
* Si seulement certaines personnes ou serveurs ont accès au serveur FTP, configurez les adresses sources dans vos règles firewall. Ainsi, aucune personne non autorisée n'y aura accès.

Avec cette petite liste des services les plus utilisés en entreprise, et certaines des solutions à mettre en œuvre pour vous défendre, vous avez déjà un bon aperçu de ce qui vous attend le jour où vous serez amené à configurer un firewall. Vous serez sûrement amené à en configurer d’autres selon les utilisations de l’entreprise.

Dans le prochain chapitre, vous apprendrez à écrire ces règles en prenant en exemple Iptables.

## Ce qu’il faut retenir

* La seule façon de se prémunir de toute attaque est de fermer tous les accès. Dans la majorité des cas, cela n’est pas envisageable.
* Il n’y a pas de sécurité garantie à 100 %.
* Vous devrez ouvrir les protocoles utilisés par vos utilisateurs et serveurs. Ceux-ci devraient coïncider avec la politique de sécurité.
* Afin de sécuriser les accès laissés ouverts, vous avez plusieurs façons de procéder :
  + Sécuriser les accès serveur.
  + Utiliser une architecture proxy.
  + Utiliser des antispams.
  + Configurer les adresses IP source ayant le droit de se connecter.
  + Utiliser fail2ban, pour les attaques DoS.

1