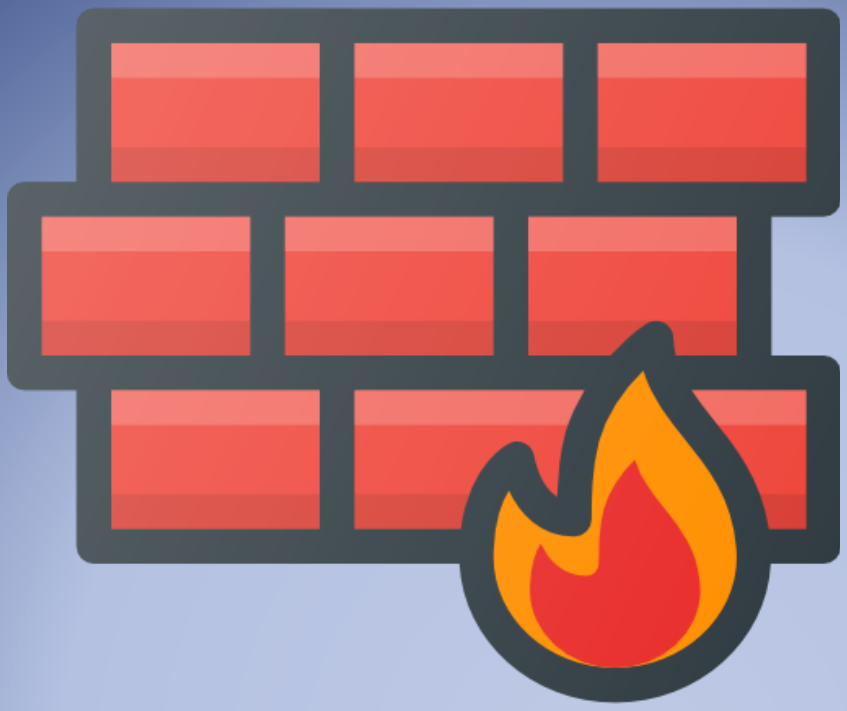


Le Firewall

BTS SiO1 2022-2023 / IZAC Matthieu

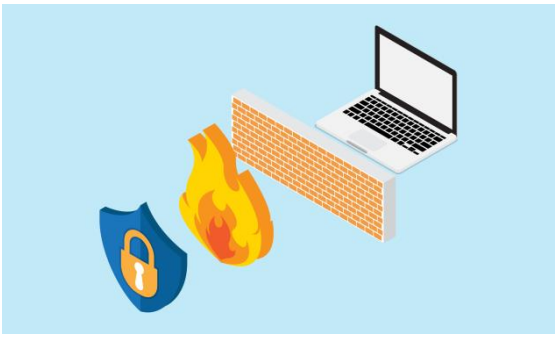
Aussi appelé pare feu en français le firewall est un logiciel informatique d'un ordinateur ou encore d'un modem qui permet la protection des « gateways » communiquant avec l'extérieur de ces appareils. Il permet aussi d'éviter que n'importe qui puisse se connecter et récupérer les données.

-SOMMAIRE

-Qu'est-ce qu'un Firewall et quel est son importance ?

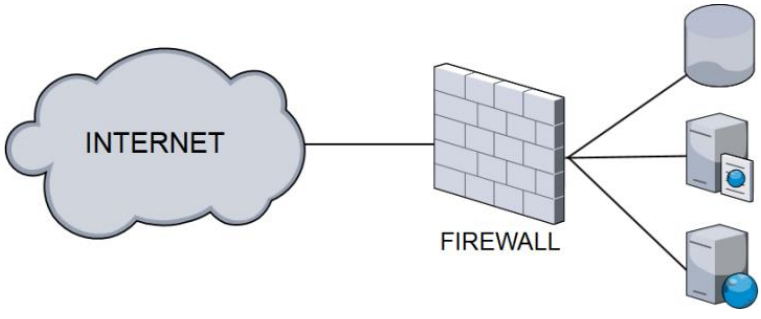
Chaque ordinateur connecté à internet est susceptible d'être victime d'une potentiel attaque informatique. Les pirates informatique pour attaquer les ordinateurs utilise généralement une méthodologie qui consiste à scruter le réseau en envoyant des paquets de données de manière aléatoire a celui-ci dans l'objectif d'y trouvé une machine connectée, puis à y chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant.

Ces menaces sont d'autant plus grande que la machine est connectée en permanence à internet car celle-ci est susceptible d'être connectée sans pour autant être surveillée, la machine est aussi généralement connectée avec une plus grande bande passante et elle ne change pas ou très peu souvent d'adresses IP



https://www.efficiens.com/cloudflare-waf-cest-quoi/

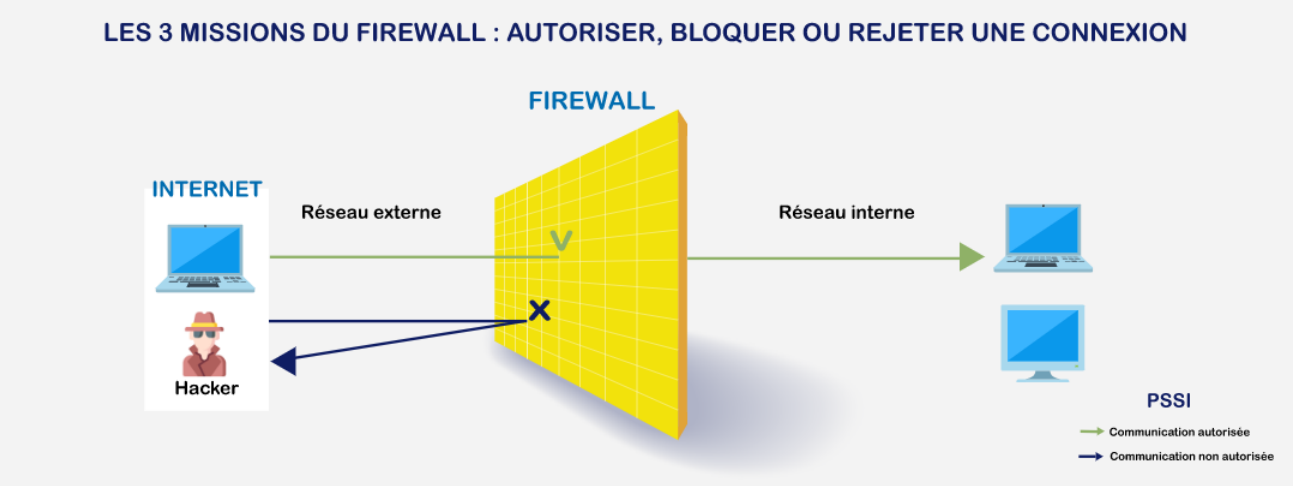
C'est pour toutes ces raisons qu'il est important d'utiliser un firewall que ce soit pour les entreprises ou encore pour les internautes dans l'optique de se protéger des intrusions réseaux.



https://kgrall.wordpress.com/2018/01/09/fridu-

-Comment fonctionne un Firewall

Un système firewall peut faire trois choses ; autoriser une connexion (allow), bloquer une connexion (deny) et rejeter la demande de connexion sans avertir l'émetteur (drop).



https://www.hexatel.fr/firewall-indispensable-de-securite/

Toutes ces possibilités permettent de mettre en œuvre une méthode dites de filtrage dépendant de la politique de sécurité adoptée par l'utilisateur. On distingue habituellement deux types de politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité ;

◆Une permettant d'autoriser uniquement les communications ayant été explicitement autorisées.

◆Une autre pour empêcher les échanges qui ont été explicitement interdits.

La première politique de sécurité est sans nul doute la plus sûre, mais elle impose toutefois une définition précise des besoins en communication.

- Les différents types de firewall

Au cours de ces dernières années le firewall n'a cessé d'évoluer. Le choix de celui-ci dépendra maintenant du besoin comme le nombre de collaborateurs présents dans votre entreprise ou de vos accès internet. Chaque pare feu correspond a un besoin comme :

◆ Le Firewall sans état (Stateless)

Celui-ci se base sur l'adresse IP sources et/ou destination, le numéro de port sources et des protocoles de couche. Il n'inspecte pas l'intégralité du trafic ou des paquets et ne différenciera pas les différents types de trafic tel que le HTTPS, HTTP ou encore le SSH. Chaque paquets sont alors analysés indépendamment des autres.

◆ Le Firewall a état (Stateful)

Celui-ci garde en mémoire les différents attributs de chaque connexion du début a la fin de celle-ci. En plus du traitement de paquet selon les règles défini par l'entité, il peut garder en mémoire et analyser les paquets en fonction de l'état de la session. En plus de son analyse, le firewall a état permet une protection de certaines attaques DDoS

◆ Le Firewall applicatif

Appartenant à la dernière génération des firewall, il est capable d'effectuer une analyse pousser des informations à transiter. Il permet de filtrer les communications applications par applications. Les requêtes sont quant à elle analysées par des processus dédies par exemple une adresse de type http sera analysée par un proxy HTTP.

◆ Le Firewall authentifiant

Ce firewall permet de mettre des règles précises en fonction de l'utilisateur authentifié et non plus seulement en fonction d'un filtrage IP

- Les différents types d'architecture

Pour détecter les attaques extérieures dont vous pourriez être victime et sécuriser vos communications internet, votre Firewall doit être positionné entre votre réseau local et votre routeur. Pour vous protéger des menaces internes, vous pouvez également faire le choix de le positionner directement sur les postes de travail de votre parc informatique.

– L'architecture simple : le Firewall est positionné entre le LAN et le WAN, c'est l'architecture la plus utilisée. Le filtrage s'effectue au niveau des adresses IP et ports TCP/UDP.

– L'architecture proxy : même architecture que la précédente avec l'application d'un filtre en plus au niveau de la couche applicative ce qui permettra de filtrer des protocoles tel que HTTP et FTP.

– La zone démilitarisée (DMZ) : véritable sécurité pour votre réseau local, la DMZ va permettre de rendre votre serveur accessible sur le web tout en sécurisant les ressources de votre réseau LAN des personnes externes.

/ !\ Attention, un Firewall ne bloquera pas les virus, en général, les entreprises installent un Firewall et un antivirus.

- Conclusion

En d'autres termes le firewall est indispensable car celui-ci protège la totalité d'un trafic réseau et a la capacité d'identifier et de bloquer le trafic indésirable. Étant donné que, de nos jours, la plupart des ordinateurs sont connectés à Internet, les attaquants ont de nombreuses opportunités pour trouver des victimes, c'est pour cela que le firewall joue un rôle important dans la sécurisation des réseaux.

Sources

https://www.eficiens.com/cloudflare-waf-cest-quoi/

https://kgrall.wordpress.com/2018/01/09/fridu-firewall/

https://www.hexatel.fr/firewall-indispensable-de-securite/

https://web.maths.unsw.edu.au/~lafaye/CCM/protect/firewall.htm