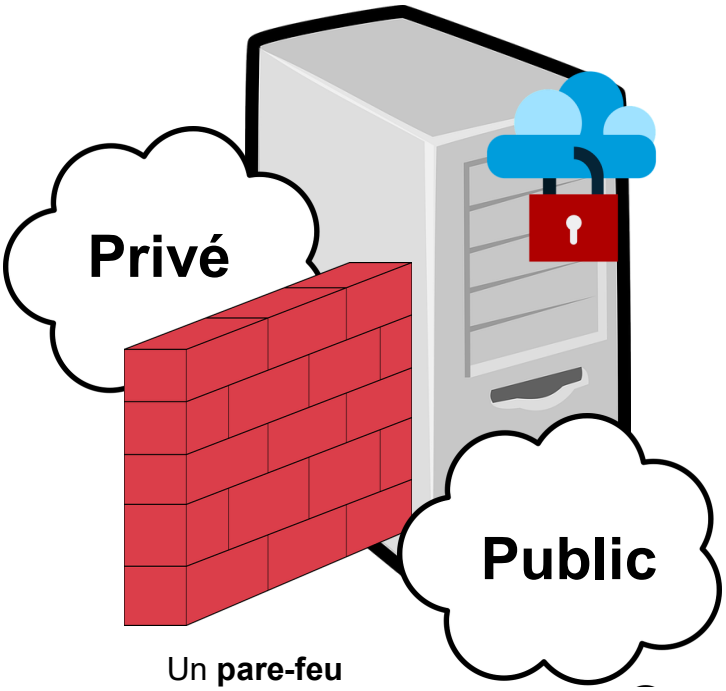
# Pare-feu

(Firewall)

En informatique, l'usage du terme « pare-feu » représente un mur virtuel qui bloque tout ce qui tente d'entrer avec l'intention de nuire dans une machine ou un réseau.

Il établit une barrière de protection contre les intrusions et les contaminations venant de l'extérieur.




Un **pare-feu** représenté par un mur de briques, pour cloisonner le réseau privé.

Fonctionnement :

### Les connexions entrantes

Le pare-feu est **un logiciel qui bloquera les différentes connexions entrantes, susceptibles d'être des attaques** (virus, pirates…).

### Les connexions sortantes

Les connexions sortantes seront elles aussi analysées, ce qui pourra empêcher tel ou tel logiciel (un cheval de Troie par exemple) de s'exécuter et de se connecter à Internet depuis votre ordinateur.
Le trafic sera ainsi régulé mais il vous faudra configurer votre pare-feu correctement pour qu'il ne bloque pas aussi l'accès aux logiciels légitimes.

### Configuration du firewall

Une fois votre firewall installé, chaque fois qu'un programme tentera d'accéder à Internet, un message d'alerte apparaîtra. Vous devrez communiquer au pare-feu votre autorisation ou votre refus de connexion. Pour ne pas avoir à répéter cette opération, vous pourrez demander à votre pare-feu de se souvenir de cette autorisation. Ainsi, petit à petit, vous pourrez faire un tri entre les applications de confiance et les mauvaises surprises qui n'amèneraient que des problèmes sur votre ordinateur.

## En bref

Un pare-feu est parfois appelé coupe-feu, barrière de sécurité ou encore firewall. Il a pour principale tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent. Généralement, les zones de confiance incluent Internet (une zone dont la confiance est nulle) et au moins un réseau interne (une zone dont la confiance est plus importante).