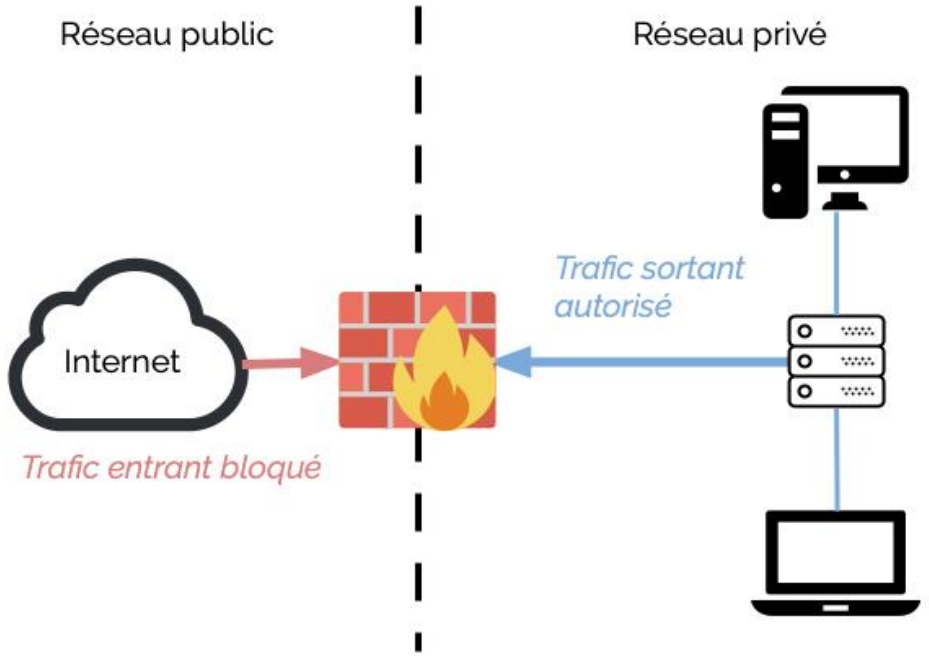
FIREWALL & PROXY

PRESENTATION

Table des matières :

1. Principe du pare-feu :

- **Un pare-feu (firewall) est un logiciel et/ou un matériel permettant de faire respecter la stratégie de sécurité du réseau, il définit quels sont les types de communication autorisés sur ce réseau informatique, il surveille et contrôle les applications et les flux de données (paquets).**
- Le filtrage peut se fait selon divers critères. Les plus courants sont :
  - L'origine ou la destination des paquets (adresse IP, ports TCP ou UDP, interface réseau, etc.).
  - Les options contenues dans les données (fragmentation, validité, etc.).
  - Les données elles-mêmes (taille, correspondance à un motif, etc.).
  - Les utilisateurs pour les plus récents.



2. Les différents firewall :

Firewall logiciel :

- **Avantages** :

Coût réduit aucun matériel supplémentaire à investir.

Facilité de mise en place (Windows Defender est déjà préconfiguré).

- **Inconvénients :**

Consomme des ressources matérielles au sein du système d'exploitation et est soumis aux failles de sécurité de ce dernier.

Firewall matériel :

- **Avantages** :

Moins de failles de sécurité.

Meilleures performances car l'équipement est dédié seulement à cette tâche.

- **Inconvénients :**

Coûts de l'appareil.

Mise en place plus conséquente.

3. Fonctionnement :

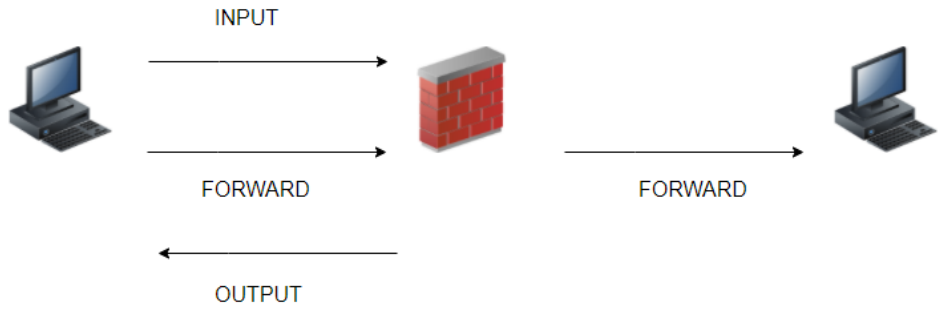
- Afin que le pare-feu puisse correctement assurer son rôle de sécurisation d'un réseau par rapport à un autre réseau, ce dernier doit être obligatoirement placer derrière un routeur.
- Ce placement garanti aussi que le pare-feu est un passage obligatoire pour le flux de données entrant ou sortant depuis votre réseau.
- Le par feu est un élément de sécurité important, il contribue grâce à son travail en synergie avec un antivirus et les mises à jour du système à réduire les menaces informatiques.
- Un pare-feu ne vous protège aucunement d'une menace présente à l'intérieur de votre réseau.

3. Fonctionnement :

- Afin de sécuriser le réseau, le pare-feu peut filtrer des paquets en se basant sur :
  - La couche 3 du modèle OSI (Réseau) : contrôle des adresses IP sources et destinataires.
  - La couche 4 du modèle OSI (Transport) : contrôle des ports (exemple TCP, UDP).
  - La couche 7 du modèle OSI (Application) : contrôle d'une application (par exemple blocage d'un logiciel de peer-to-peer) car le pare-feu peut agir sur des protocoles (exemple http).

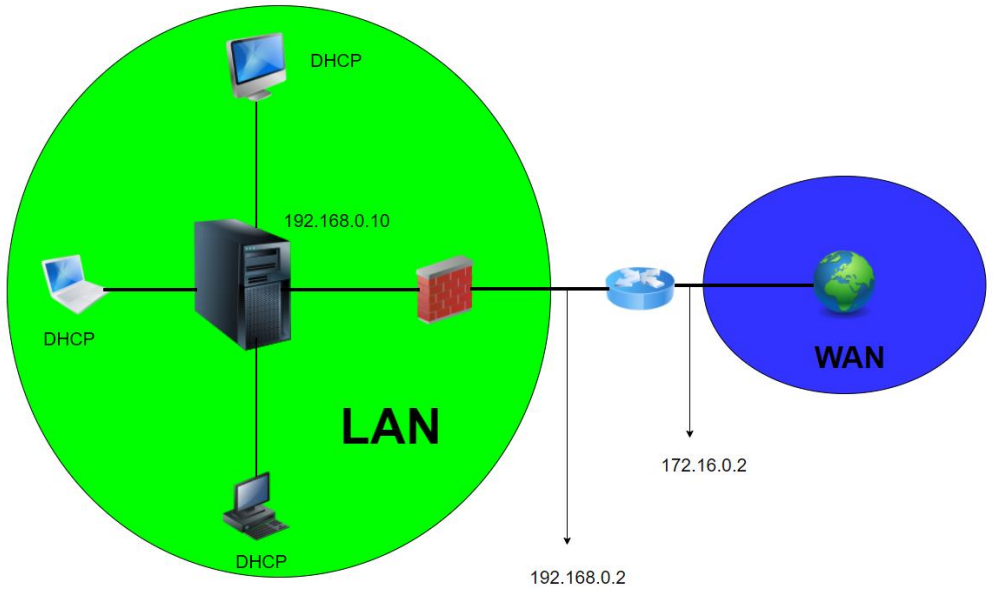
3. Fonctionnement :

- Après avoir été routé, un paquet arrive sur le firewall, il pourra prendre deux chemins (chaînes) :
- **Input** : le paquet est destiné au firewall.
- **Forward** : le paquet traverse le firewall car il est destiné à un autre terminal.
- **Output** : le paquet est émis par le firewall.



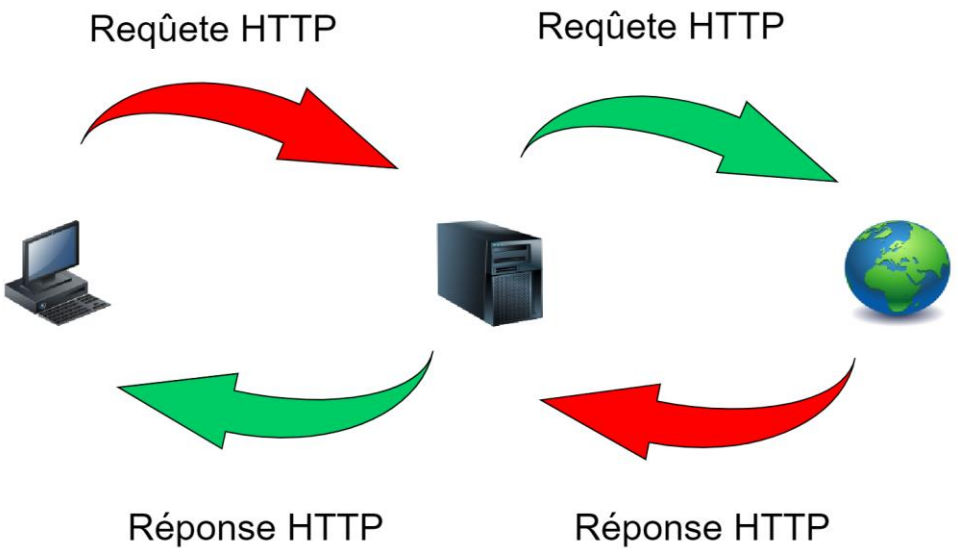
4. L'architecture simple :

- Le pare-feu se positionne entre le réseau LAN et le réseau WAN :
  - Filtrage au niveau de la couche 3 (IP) et 4 (ports).
  - Mise en place d'une politique de sécurité par des règles.
  - Coût réduit : logiciel open source couplé à un matériel peu puissant.
  - Impossibilité de filtrer des applications ou des services (peer-to-peer).
- Utilisation recommandée lorsque les serveurs internes ne sont ouverts vers le WAN.



5. L'architecture proxy :

- Cette architecture est semblable à l'architecture simple mais elle permet en plus de filtrer les applications (couche 7).
- Permet de filtrer des protocoles (http) et non pas les ports (http) afin d'empêcher un logiciel de peer-to-peer.
- Le proxy agit comme un intermédiaire entre deux réseaux, cette solution peut devenir coûteuse en fonction du nombre d'utilisateur.
- Adapté au réseaux publics, écoles, etc.
- En cas d'attaque, le proxy sera ciblé au lieu du poste client.



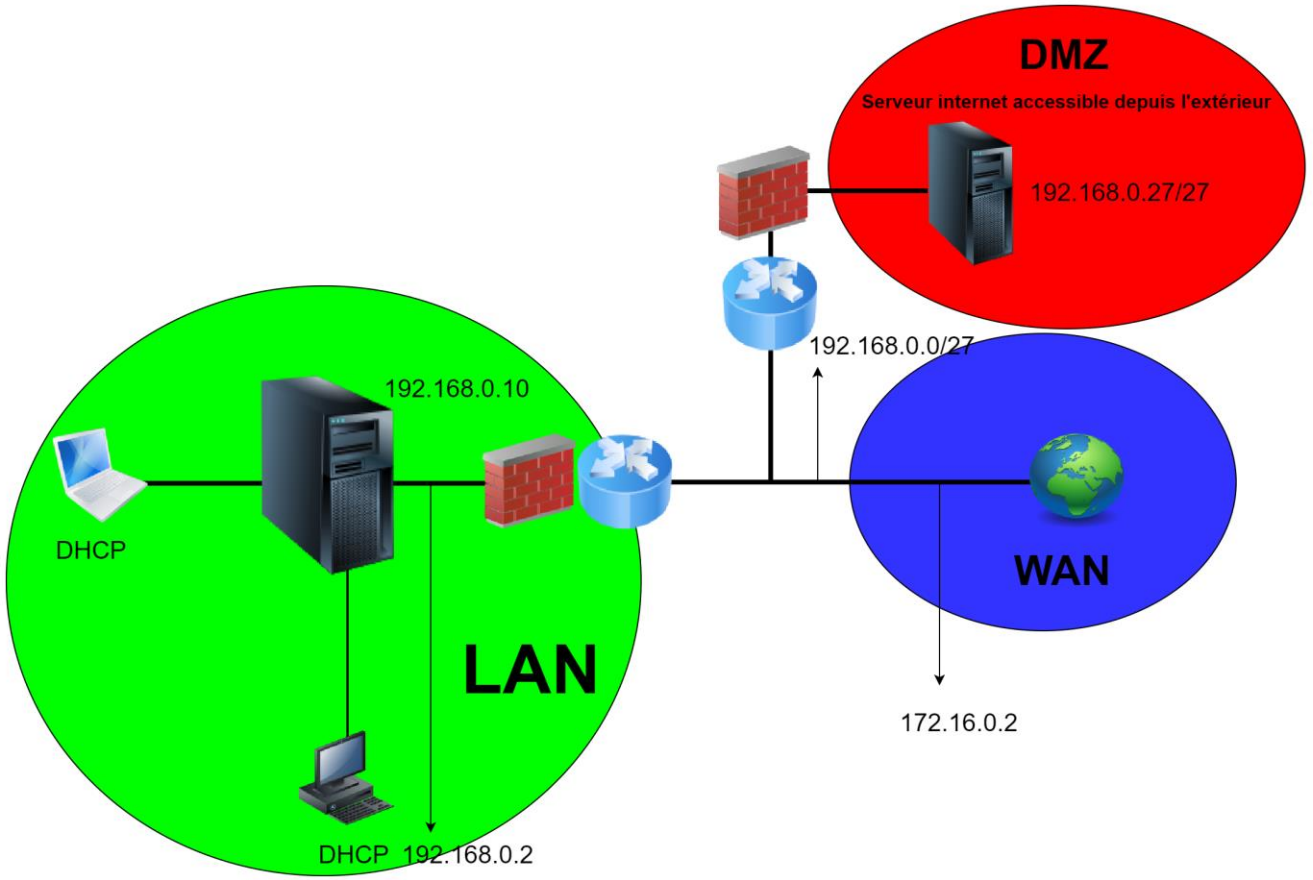
6. La zone démilitarisée (DMZ) :

- Une DMZ permet de rendre accessible un serveur sur le Web tout en sécurisant le réseau local (LAN) de l'entreprise grâce à l'ajout d'un deuxième firewall entre le LAN et les serveurs en établissant deux règles :
  - une règle permettant au WAN de se rendre sur le serveur, par le routeur/firewall externe en autorisant l'accès selon un protocole défini (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 permettant au LAN de se rendre sur le serveur (via SSH notamment), mais en empêchant le serveur de se rendre sur le LAN. De cette façon si le serveur était compromis, ce dernier ne pourrait pas contaminer le LAN en cas de piratage.

6. La zone démilitarisée (DMZ) :

- Cette architecture est particulièrement recommandée dès lors que vous disposez d'un serveur qui doit être accessible sur le Web (serveur IIS ou Apache, formulaire client en php, etc.).
- Dans ce type d'architecture les règles de base sont :
  - La DMZ doit être accessible depuis Internet.
  - Le LAN ne doit pas être accessible depuis Internet.
  - Le LAN peut accéder à Internet (pas obligatoire non plus).
  - Le Lan peut accéder à la DMZ (pas obligatoire non plus).
  - La DMZ ne doit pas avoir accès au LAN.

6. La zone démilitarisée (DMZ) :



7. Les règles :

- Les règles doivent être définies par rapport à la **politique de sécurité** qui a été mise en place par le direction et le service informatique.
- Il existe deux possibilités pour sa stratégie de sécurité :
  - Tout autoriser puis bloquer au fur et à mesure les flux inutiles.
  - Tout bloquer puis autoriser au fur et à mesure suivant les besoins les flux nécessaires au fonctionnement de l'entreprise (procédure recommandée).
- Les règles se composent de la même manière peu importe le logiciel ou matériel pare-feu utilisé.

7. Les règles :

- La sémantique des règles est souvent la suivante :
  - Choix de la règle : autoriser ou interdire le trafic.
  - Spécification des adresses sources et destination qui seront soumises à cette règle.
  - Définition des ports sources et destinations concernant le flux soumis à cette règle.
- Les règles étant appliquées de **manière séquentielle**, il est impératif de placer en tête les règles les plus fines afin qu'elles soient appliquées (les règles générales doivent se placer en fin de liste).

7. Les règles :

- Les entreprises ne peuvent plus se permettre de bloquer complètement le trafic entrant et sortant, certains protocoles et applications sont nécessaires au bon fonctionnement économique de l'entreprise.
- Les protocoles suivants sont nécessaires, mais ils deviennent des points d'entrées qui peuvent se transformer en faille de sécurité :
  - HTTP/HTTPS
  - SMTP
  - Accès à distance
  - Transfert de fichiers

7. Les règles :

- Il est donc nécessaire d'établir quelques règles de base sur ces différents protocoles qui seront systématiquement utilisés par les sociétés.
- **HTTP/HTTPS** : de nombreux sites utilisent maintenant le protocole https, le protocole http peut être bloqué si il n'est pas nécessaire. L'utilisation d'un proxy peut permettre de filtrer le trafic internet.
- **SMTP** étant nécessaire pour la messagerie, l'utilisation de connexions chiffrées et sécurisées avec TLS ou SSL permet de renforcer la sécurité. La messagerie est un service qui est fréquemment la cible d'attaque DDoS, il est possible de diminuer les risques en empêchant de relayer les mails étrangers et en obligeant les utilisateurs à s'authentifier pour utiliser la messagerie.

7. Les règles :

- **Accès à distance** peut aussi devenir une faille de sécurité, il est préférable de n'utiliser que des connexions sécurisées SSH en spécifiant si possible les adresses IP autorisées à se connecter.
- **FTP** peut être renforcé en utilisant uniquement le protocole FTPS qui combine les protocoles FTP et SSL (TLS). Il est aussi possible de définir les adresses sources autorisées à utiliser ce protocole et d'en interdire les autres afin de contrôler un peu plus l'accès.
- Cette liste est loin d'être exhaustive et le risque zéro n'existant pas, d'autant plus que le pare-feu est à double tranchant car la multiplication des règles autorisées créent des points d'entrées sur le réseau.