EXPOSÉE SUR LE PARE-FEU

Groupe 2

MEMBRES

-GBEGNON Komi Sedegnon Rodrigue
-SIBI Khalil
-BANGWABO SHABURWA Joyce
-ZIME

Professeur
Mr BOUKLINAM

Lomé Business School

SOMMAIRE

1. Introduction

Dans un monde où les échanges de données sont omniprésents et où la cybersécurité devient une préoccupation majeure, les pare-feu jouent un rôle fondamental dans la protection des systèmes informatiques. Un pare-feu, en anglais *"firewall"*, est un dispositif de sécurité réseau qui surveille et contrôle le trafic entrant et sortant d'un réseau informatique. Il agit comme une barrière entre un réseau sécurisé, souvent privé (comme un réseau d'entreprise ou un réseau domestique), et des réseaux extérieurs, tels qu'Internet, afin de filtrer les communications et d'empêcher les connexions non autorisées.

Les pare-feu sont essentiels dans la défense contre une variété de menaces informatiques, y compris les attaques malveillantes, les intrusions, les virus, les chevaux de Troie, ainsi que les tentatives d'accès non autorisé. En filtrant le trafic en fonction de critères prédéfinis (comme les adresses IP, les ports, les protocoles), ils permettent d'isoler les systèmes internes des menaces extérieures, tout en assurant la continuité des échanges légitimes de données.

Au-delà de leur rôle de prévention des intrusions, les pare-feu sont également un élément clé dans le contrôle des communications au sein d'un réseau. Ils peuvent être configurés pour bloquer ou autoriser l'accès à certaines ressources, limiter la bande passante, ou encore détecter des comportements suspects en temps réel. Dans un contexte de cybersécurité toujours plus complexe, les pare-feu évoluent constamment pour faire face aux nouvelles menaces, avec des technologies avancées telles que l'inspection approfondie des paquets (DPI), le filtrage des applications, et l'intégration d'analyses comportementales.

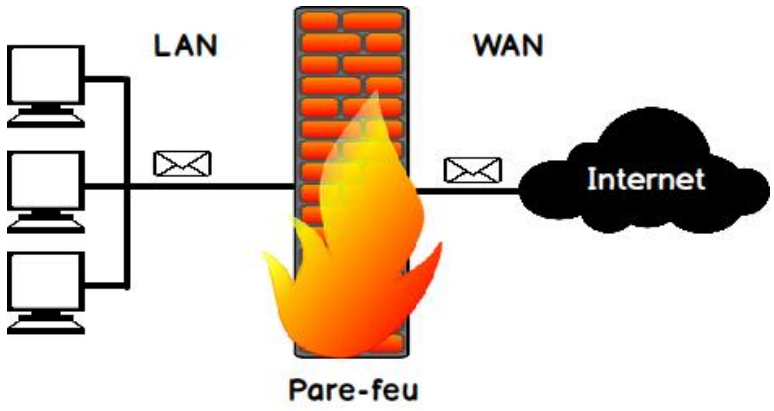
En somme, les pare-feu sont bien plus qu'un simple outil de filtrage : ils forment la première ligne de défense dans la sécurisation des réseaux informatiques modernes. À mesure que les menaces deviennent plus sophistiquées, les pare-feu continuent de jouer un rôle essentiel dans la protection des données et la préservation de la confidentialité des utilisateurs à travers le monde.

2. Qu'est-ce qu'un pare-feu ?

Un **pare-feu** (ou firewall en anglais) est un dispositif de sécurité réseau utilisé pour contrôler et filtrer les flux de données entre un réseau interne (par exemple, un réseau d'entreprise ou un réseau domestique) et un réseau externe, tel qu'Internet. Il sert de barrière de protection afin de prévenir les intrusions non autorisées, les attaques malveillantes, et autres menaces provenant de l'extérieur, tout en permettant les communications légitimes et nécessaires entre les différentes parties du réseau.

Le pare-feu fonctionne en surveillant et en analysant les paquets de données qui traversent le réseau. Selon un ensemble de règles définies par un administrateur, il décide si un paquet doit être autorisé à passer ou s'il doit être bloqué. Ces règles peuvent se baser sur différents critères, tels que l'adresse IP, le protocole de communication (TCP, UDP, ICMP, etc.), le port de destination ou l'état de la connexion.

Il existe plusieurs types de pare-feu, dont les pare-feu **matériels** (qui sont des appareils physiques dédiés) et les pare-feu **logiciels** (qui sont installés sur un ordinateur ou un serveur). Les pare-feu modernes vont au-delà du simple filtrage de paquets en intégrant des technologies avancées, telles que l'inspection approfondie des paquets (DPI), la détection d'intrusions et le filtrage des applications, pour renforcer la sécurité et contrer des menaces plus complexes.



3. Comment fonctionne un pare-feu ?

Un pare-feu décide quel trafic réseau est autorisé à passer et quel trafic est jugé dangereux. Essentiellement, il fonctionne en filtrant le bon du mauvais, ou le fiable du non fiable. Toutefois, avant d'entrer dans les détails, il est utile de comprendre la structure des réseaux sur Internet.

Les pare-feu sont destinés à sécuriser les réseaux privés et les dispositifs terminaux qu'ils contiennent, appelés hôtes réseau. Les hôtes réseau sont des dispositifs qui « communiquent » avec d'autres hôtes sur le réseau. Ils envoient et reçoivent des données entre les réseaux internes, ainsi que des données sortantes et entrantes entre les réseaux externes.

Les ordinateurs et autres dispositifs terminaux utilisent des réseaux pour accéder à Internet et aux autres équipements. Toutefois, Internet est segmenté en sous-réseaux pour des raisons de sécurité et de confidentialité. Les segments de sous-réseau de base sont les suivants :

- **Les réseaux publics externes** font généralement référence à l'Internet public/global ou à divers extranets.
- **Le réseau privé interne** définit un réseau domestique, des Intranets d'entreprise et d'autres réseaux « fermés ».
- **Les réseaux périphériques** désignent les réseaux frontaliers constitués d'hôtes bastion : des hôtes informatiques dédiés à la sécurité renforcée capables de résister à une attaque externe. En tant que tampon sécurisé entre les réseaux internes et externes, ils peuvent également être utilisés pour héberger tous les services tournés vers l'extérieur fournis par le réseau interne (c'est-à-dire les serveurs pour le Web, le courrier, le FTP, la VoIP, etc.) Ils sont plus sûrs que les réseaux externes mais moins que les réseaux internes. Ils ne sont pas toujours présents dans les réseaux plus simples comme les réseaux domestiques mais peuvent souvent être utilisés dans les Intranets d'entreprise ou nationaux.

Les routeurs de filtrage sont des ordinateurs passerelles spécialisés placés sur un réseau pour le segmenter. Ils sont connus comme des pare-feu domestiques au niveau du réseau. Les deux modèles de segmentation les plus courants sont le pare-feu d'hôte filtré et le pare-feu de sous-réseau filtré :

- **Les pare-feu d'hôte filtrés** utilisent un routeur de filtrage unique entre les réseaux externe et interne. Ces réseaux constituent les deux sous-réseaux de ce modèle.
- **Les pare-feu de sous-réseau filtrés** utilisent deux routeurs de filtrage : un connu sous le nom de *routeur d'accès* entre le réseau externe et le réseau périphérique, et un autre connu sous le nom de *routeur de rétention (ou « choke »)* entre le réseau périphérique et le réseau interne. Cela crée trois sous-réseaux, respectivement.

Tant le périmètre du réseau que les machines hôtes elles-mêmes peuvent abriter un pare-feu. Pour ce faire, celui-ci est placé entre un seul ordinateur et sa connexion à un réseau privé.

- **Les pare-feu réseau** impliquent l'application d'un ou plusieurs pare-feu entre les réseaux externes et les réseaux privés internes. Ils régulent le trafic réseau entrant et sortant, en séparant les réseaux publics externes, comme l'Internet mondial, des réseaux internes comme les réseaux Wi-Fi domestiques, les Intranets d'entreprise ou les Intranets nationaux. Les pare-feu réseau peuvent se présenter sous la forme de l'un des types d'appareils suivants : matériel dédié, logiciel et virtuel.
- **Les pare-feu basés sur l'hôte** ou « pare-feu logiciels » impliquent l'utilisation de pare-feu sur des appareils individuels d'utilisateurs et d'autres terminaux de réseaux privés comme barrière entre les appareils du réseau. Ces dispositifs, ou hôtes, reçoivent une régulation personnalisée du trafic à destination et en provenance d'applications informatiques spécifiques. Les pare-feu basés sur l’hôte peuvent s'exécuter sur des dispositifs locaux en tant que service du système d'exploitation ou en tant qu'application de sécurité de terminaux. Les pare-feu basés sur l’hôte peuvent également s'intéresser de plus près au trafic Web, en filtrant sur la base du protocole HTTP et d'autres protocoles réseau, ce qui permet de gérer le contenu qui arrive sur votre machine, plutôt que sa provenance.

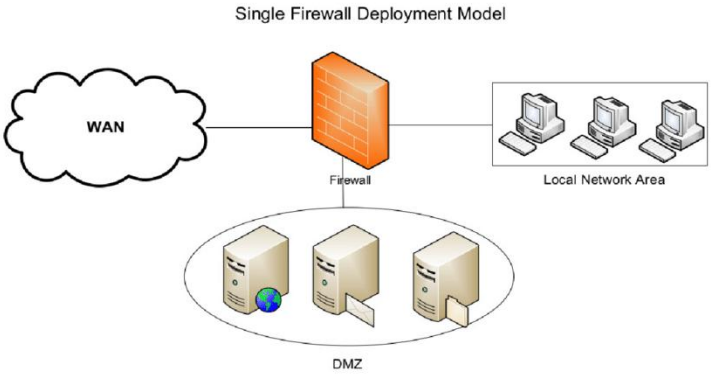
Un pare-feu réseau nécessite une configuration pour accommoder un large éventail de connexions, alors qu'un pare-feu basé sur l’hôte peut être adapté aux besoins de chaque machine. Cependant, les pare-feu basés sur l’hôte demandent plus d'efforts de personnalisation, ce qui signifie que les pare-feu réseau sont idéaux pour une solution de contrôle complète. Mais l'utilisation des deux types de pare-feu dans les deux sites simultanément est idéale pour un système de sécurité multicouche.

Le filtrage du trafic via un pare-feu fait appel à des règles préétablies ou apprises dynamiquement pour autoriser et refuser les tentatives de connexion. Ces règles contrôlent la manière dont un pare-feu régule le flux du trafic Web à travers votre réseau privé et vos périphériques informatiques privés. Quel que soit leur type, tous les pare-feu peuvent filtrer par une combinaison des éléments suivants :

- **La source :** d'où provient une tentative de connexion.
- **La destination :** où une tentative de connexion est censée aller.
- **Le contenu :** ce qu'une tentative de connexion essaie d'envoyer.
- **Protocoles par paquets :** Le « langage » utilisé par une tentative de connexion pour transmettre son message. Parmi les protocoles réseau que les hôtes utilisent pour « parler » entre eux, les protocoles TCP/IP sont principalement utilisés pour communiquer sur Internet et au sein des Intranets/sous-réseaux.
- **Les protocoles d'application :** les protocoles courants comprennent HTTP, Telnet, FTP, DNS et SSH.

La source et la destination sont communiquées par des adresses de protocole Internet (IP) et des ports. Les adresses IP sont des noms de périphériques uniques pour chaque hôte. *Les ports* sont un sous-niveau de tout périphérique hôte source et destination donné ; ils s'apparentent aux différentes salles d'un grand bâtiment par exemple. Les ports sont généralement affectés à des fins spécifiques, de sorte que certains protocoles et adresses IP utilisant des ports peu communs ou des ports désactivés peuvent s'avérer problématiques.

En utilisant ces identifiants, un pare-feu peut décider si un paquet de données tentant de se connecter doit être rejeté, silencieusement ou avec une réponse d'erreur à l'expéditeur, ou transféré.



4.**Types de pare-feu**

Les différents types de pare-feu intègrent des méthodes de filtrage variées. Bien que chaque type ait été développé pour dépasser les générations précédentes de pare-feu, une grande part de la technologie de base a été transmise de génération en génération.

Les types de pare-feu se distinguent par leur approche des éléments suivants :

- Suivi des connexions
- Règles de filtrage
- Journaux d'audit.

Chaque type fonctionne à un niveau différent du modèle de communication normalisé, le modèle d'interconnexion des systèmes ouverts (OSI). Ce modèle permet de mieux visualiser la manière dont chaque pare-feu interagit avec les connexions.

4.1. *Pare-feu statique de filtrage de paquets*

Les pare-feu statiques de filtrage de paquets, également appelés pare-feu d'inspection sans état, fonctionnent au niveau de la couche réseau OSI (couche 3). Ils offrent un filtrage de base en vérifiant tous les paquets de données individuels envoyés sur un réseau, en fonction de leur provenance et de leur destination. Notamment, les connexions précédemment acceptées ne sont pas suivies. Cela signifie que chaque connexion doit être réapprouvée avec chaque paquet de données envoyé.

Le filtrage est basé sur les adresses IP, les ports et les protocoles de paquets. Ces pare-feu, au minimum, empêchent deux réseaux de se connecter directement sans autorisations.

Les règles de filtrage sont définies sur la base d'une liste de contrôle d'accès créée manuellement. Elles sont très rigides et il est difficile de couvrir le trafic indésirable de manière appropriée sans compromettre la convivialité du réseau. Le filtrage statique nécessite une révision manuelle permanente pour être efficace. Cela peut être envisageable sur les petits réseaux mais peut rapidement devenir difficile sur les plus grands.

L'impossibilité de lire les protocoles d'application signifie que le contenu d'un message livré dans un paquet ne peut être lu. Sans lecture du contenu, les pare-feu de filtrage de paquets présentent une qualité de protection limitée.

4.2. Pare-feu de passerelle au niveau du circuit

Les passerelles au niveau du circuit fonctionnent au niveau de la session (couche 5). Ces pare-feu vérifient si les paquets sont fonctionnels lors d'une tentative de connexion et, s'ils fonctionnent bien, ils permettent une connexion ouverte permanente entre les deux réseaux. Le pare-feu cesse alors de superviser la connexion.

En dehors de son approche des connexions, la passerelle au niveau du circuit peut être similaire aux pare-feu proxy.

La connexion permanente non surveillée est dangereuse, car des moyens légitimes pourraient ouvrir la connexion et permettre ensuite à un acteur malveillant d'entrer sans encombre.

4.3. Pare-feu à inspection dynamique

Les pare-feu à inspection dynamique, également appelés pare-feu à filtrage dynamique des paquets, se distinguent du filtrage statique par leur capacité à surveiller les connexions en cours et à se souvenir des connexions passées. Ils ont commencé par fonctionner sur la couche transport (couche 4) mais aujourd'hui, ces pare-feu peuvent surveiller de nombreuses couches, y compris la couche application (couche 7).

À l'instar du pare-feu à filtrage statique, les pare-feu à inspection dynamique autorisent ou bloquent le trafic en fonction de propriétés techniques, telles que des protocoles de paquets, des adresses IP ou des ports spécifiques. Cependant, ces pare-feu suivent également de manière unique et filtrent en fonction de l'état des connexions à l'aide d'une table d'état.

Ce pare-feu met à jour les règles de filtrage en fonction des événements de connexion passés enregistrés dans la table d'état par le routeur de filtrage.

En général, les décisions de filtrage sont souvent basées sur les règles de l'administrateur lors de la configuration de l'ordinateur et du pare-feu. Toutefois, la table d'état permet à ces pare-feu dynamiques de prendre leurs propres décisions en fonction des interactions précédentes qu'ils ont « apprises ». Par exemple, les types de trafic qui ont causé des perturbations dans le passé seront filtrés à l'avenir. La souplesse de l'inspection dynamique en a fait l'un des types de protection les plus répandus.

4.4. Pare-feu proxy

Les pare-feu à proxy, également appelés pare-feu au niveau des applications (couche 7), ont la particularité de lire et de filtrer les protocoles d'application. Ils combinent l'inspection au niveau des applications, ou « inspection approfondie des paquets (IAP) », et l'inspection dynamique.

Un pare-feu proxy est aussi proche d'une véritable barrière physique qu'il est possible de l'être. Contrairement à d'autres types de pare-feu, il agit comme deux hôtes supplémentaires entre les réseaux externes et les ordinateurs hôtes internes, l'un d'entre eux servant de représentant (ou « proxy ») pour chaque réseau.

Le filtrage est basé sur les données au niveau des applications plutôt que sur les adresses IP, les ports et les protocoles de base des paquets (UDP, ICMP) comme dans les pare-feu basés sur les paquets. La lecture et la compréhension des protocoles FTP, HTTP, DNS et autres permettent une investigation plus approfondie et un filtrage croisé pour de nombreuses caractéristiques de données différentes.

À l'instar d'un vigile à l'entrée d'un bâtiment, il examine et évalue essentiellement les données entrantes. Si aucun problème n'est détecté, les données sont autorisées à être transmises à l'utilisateur.

L'inconvénient de ce type de sécurité renforcée est qu'elle interfère parfois avec des données entrantes qui ne constituent pas une menace, ce qui entraîne des retards de fonctionnement.

4.5. Pare-feu de nouvelle génération (NGFW)

L'évolution des menaces continue d'exiger des solutions plus intenses, et les pare-feu de nouvelle génération restent à la pointe de ce problème en combinant les fonctionnalités d'un pare-feu traditionnel avec des systèmes de prévention des intrusions dans le réseau.

Les pare-feu de nouvelle génération spécifiques aux menaces sont conçus pour examiner et identifier des menaces spécifiques, telles que les programmes malveillants avancés, à un niveau plus fin. Plus fréquemment utilisés par les entreprises et les réseaux sophistiqués, ils offrent une solution complète pour filtrer les menaces.

4.6. Pare-feu hybride

Comme son nom l'indique, le pare-feu hybride utilise deux types de pare-feu ou plus dans un seul réseau privé.

5.Les critères de configuration d'un pare-feu

5.1. Filtrage de paquets

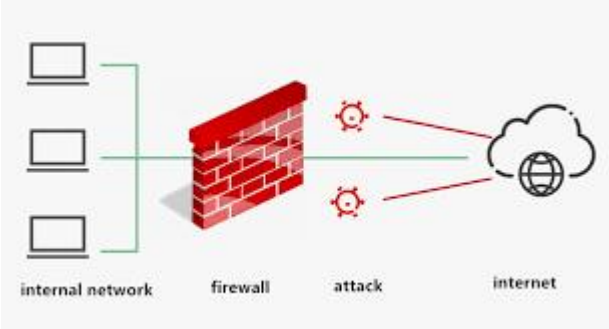
Le filtrage de paquets est la méthode la plus basique et la plus utilisée pour sécuriser un réseau à l'aide d'un pare-feu. Il consiste à examiner chaque paquet de données entrant ou sortant du réseau et à appliquer des règles de filtrage pour déterminer si le paquet doit être autorisé ou bloqué. Ces règles peuvent être basées sur diverses informations présentes dans les en-têtes des paquets, telles que l'adresse IP source, l'adresse IP de destination, le protocole utilisé, ainsi que le port d'origine et de destination.

5.2. Inspection approfondie des paquets (Deep Packet Inspection - DPI)

L'inspection approfondie des paquets va au-delà du simple filtrage de paquets. Elle consiste à examiner non seulement les en-têtes des paquets, mais aussi leur contenu. Cela permet au pare-feu de détecter des menaces plus complexes, comme les malwares ou les intrusions, en analysant les données qui transitent dans les paquets. DPI permet également de vérifier les protocoles de communication et d'identifier des anomalies comportementales ou des tentatives d'attaque.

5.3. Filtrage d'applications et de contenu

Ce type de filtrage va encore plus loin que le filtrage de paquets traditionnel. Il consiste à analyser les applications qui communiquent à travers le pare-feu, ainsi que le contenu des messages ou des fichiers échangés. Cela permet de bloquer l'accès à certaines applications ou services, comme les réseaux sociaux, les services de messagerie instantanée ou les applications de partage de fichiers, tout en autorisant le passage des applications jugées sûres. Le filtrage de contenu peut également être utilisé pour bloquer des sites web malveillants ou inappropriés en fonction de leur contenu.



6. L'Importance des Pare-feu dans la Cybersécurité

6.1. Protection contre les intrusions

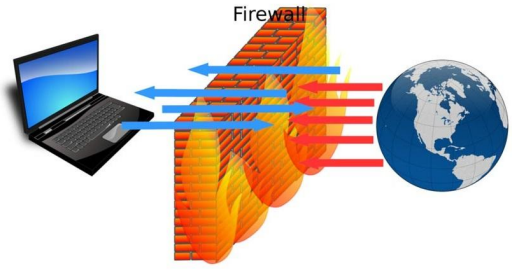
Les pare-feu jouent un rôle fondamental dans la protection contre les intrusions malveillantes. En contrôlant et filtrant le trafic réseau, ils empêchent l'accès non autorisé aux systèmes et réseaux. Ils permettent de détecter des tentatives d'intrusion, telles que des scans de ports ou des attaques par déni de service (DoS), et d'agir rapidement pour les bloquer avant qu'elles n'atteignent leur cible.

6.2. Sécurisation des communications et des échanges de données

Les pare-feu sont également essentiels pour garantir la confidentialité et l'intégrité des données échangées sur un réseau. Ils permettent de sécuriser les communications entre les appareils en empêchant l'accès aux données sensibles par des acteurs malveillants. En bloquant les connexions non autorisées et en filtrant le contenu des échanges, les pare-feu minimisent le risque d'interception ou de manipulation des informations.

6.3. Contrôle d'accès et prévention des attaques

Les pare-feu sont utilisés pour appliquer des politiques de contrôle d'accès rigoureuses en fonction de l'adresse IP, du port ou du protocole. Cela permet de s'assurer que seuls les utilisateurs et applications autorisés peuvent accéder aux ressources critiques. De plus, ils empêchent les attaques par usurpation d'identité, les attaques par injection ou les tentatives d'exploitation des vulnérabilités connues.



7. Limitations et Défis des Pare-feu

7.1. Risque d'erreurs de configuration

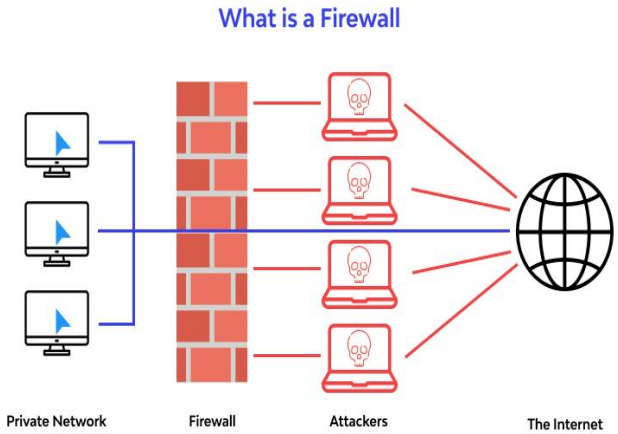
Les pare-feu sont puissants, mais leur efficacité dépend en grande partie de la manière dont ils sont configurés. Une mauvaise configuration peut entraîner des failles de sécurité, permettant aux attaquants de contourner les règles établies. Par exemple, une règle trop permissive ou mal définie peut ouvrir une porte d'entrée pour les cybercriminels. Il est donc essentiel de procéder à une configuration soignée et de réévaluer régulièrement les règles de sécurité.

7.2. Impact sur la performance du réseau

Un pare-feu, particulièrement s'il effectue une inspection approfondie des paquets ou un filtrage de contenu complexe, peut introduire un certain ralentissement du trafic réseau. L'analyse en temps réel des paquets et des applications peut nécessiter des ressources systèmes considérables, impactant ainsi la vitesse de transmission des données. Ce problème est particulièrement pertinent dans les grandes entreprises ou les réseaux avec un trafic élevé.

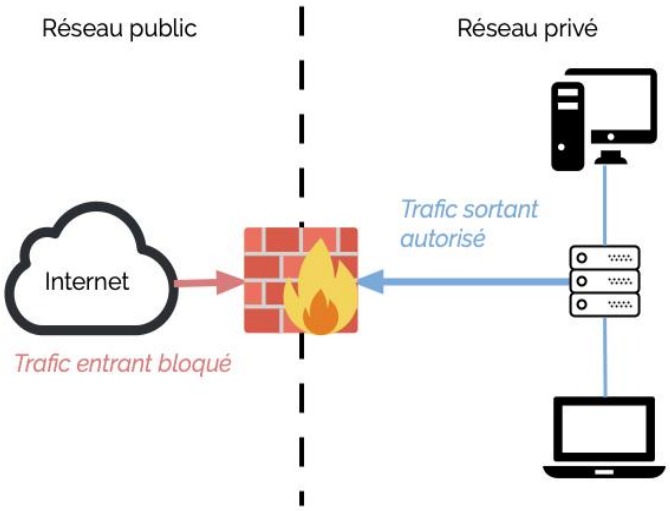
7.3. Gestion des menaces évolutives

Les cybermenaces évoluent constamment, avec de nouvelles méthodes d'attaque et des techniques de contournement de sécurité régulièrement mises au point. Les pare-feu doivent être mis à jour en permanence pour contrer ces nouvelles menaces. Cependant, certains pare-feu peuvent être vulnérables face aux attaques zero-day (inconnues) ou aux méthodes sophistiquées d'intrusion, nécessitant une gestion proactive des menaces.



8. Conclusion

Les pare-feu sont un élément indispensable de la cybersécurité moderne. Ils offrent une protection essentielle contre les menaces internes et externes, garantissant ainsi la sécurité des systèmes et des données. Cependant, ils ne sont pas infaillibles et doivent être utilisés en complément d'autres solutions de sécurité, telles que les systèmes de détection d'intrusions, la gestion des identités, et la formation continue des utilisateurs. En dépit de leurs limitations, une bonne configuration et une surveillance constante des pare-feu peuvent considérablement réduire les risques de sécurité.



9. BIOGRAPHIE

Le terme "pare-feu" (ou *firewall* en anglais) fait référence à un dispositif de sécurité réseau conçu pour surveiller et contrôler le trafic entrant et sortant d'un réseau informatique. Cela permet de protéger les systèmes informatiques des attaques externes ou non autorisées en filtrant les communications. Le pare-feu peut être matériel ou logiciel et joue un rôle crucial dans la protection des réseaux, notamment en entreprise, mais aussi à l'échelle personnelle.

Cependant, vous semblez demander la "biographie complète" du pare-feu, ce qui pourrait être interprété comme une explication de son évolution, de son invention et de son développement au fil du temps. Voici donc un aperçu de l'histoire du pare-feu :

❖ Les premières protections réseau

Avant l'invention du pare-feu tel que nous le connaissons aujourd'hui, les premières méthodes de sécurisation des réseaux étaient rudimentaires et se concentraient sur des contrôles d'accès physiques et des systèmes de sécurité sur des systèmes isolés. Dans les années 1970 et 1980, alors que les réseaux informatiques commençaient à se développer (notamment avec ARPANET), la sécurité réseau est devenue une préoccupation croissante.

❖ L'apparition des premiers pare-feu

Les premiers pare-feu ont vu le jour dans les années 1980. L'un des pionniers dans le domaine est **William Cheswick** (célèbre pour ses travaux sur la sécurité réseau) qui, en 1988, a écrit un document sur la sécurité des réseaux et les pare-feu. Il a proposé l'idée de séparer un réseau interne d'un réseau externe en utilisant des techniques de filtrage de paquets.

❖ Le développement des pare-feu à filtrage de paquets

Au début des années 1990, les entreprises ont commencé à adopter des pare-feu de plus en plus sophistiqués. Un pare-feu à filtrage de paquets examine chaque paquet de données entrant ou sortant d'un réseau pour déterminer s'il est légitime ou non, basé sur des règles préconfigurées (par exemple, l'adresse IP, le numéro de port, ou le protocole utilisé). Ce système a été une avancée significative, notamment avec le développement de systèmes de filtrage plus complexes et plus adaptables.

❖ Les pare-feu à inspection d'état

En 1994, l'invention du pare-feu à inspection d'état (stateful inspection) a représenté une avancée majeure. Ce type de pare-feu permet de suivre l'état des connexions réseau (par exemple, les connexions TCP) et de filtrer non seulement les paquets mais aussi leur contexte. Il garde une trace des connexions ouvertes et veille à ce que seules les connexions valides et suivies soient autorisées.

❖ L'émergence des pare-feu applicatifs (proxy et filtrage des applications)

Dans les années 2000, avec la multiplication des menaces et des vulnérabilités sur Internet, les pare-feu ont évolué pour intégrer des fonctions plus avancées, telles que le filtrage des applications (application-level gateway ou proxy). Ces pare-feu sont capables de filtrer le trafic en fonction du type d'application (par exemple, HTTP, FTP) et d'inspecter plus profondément les données transmises. Cela permet de mieux se défendre contre des attaques spécifiques, comme les injections SQL ou les malwares.

❖ Les pare-feu de nouvelle génération

Les "pare-feu de nouvelle génération" (NGFW - Next-Generation Firewalls) ont vu le jour au milieu des années 2000 et intègrent plusieurs fonctionnalités avancées, telles que :

- **Inspections profondes de paquets** (DPI : Deep Packet Inspection)
- **Filtrage des applications en temps réel**
- **Détection des intrusions (IDS) et prévention des intrusions (IPS)**
- **VPN et sécurité des réseaux mobiles**

Ces pare-feu modernes sont capables de détecter et de prévenir les menaces en temps réel tout en permettant une gestion centralisée et une adaptation constante aux nouvelles vulnérabilités.

❖ Le pare-feu dans l'ère du Cloud et de la mobilité

Avec la montée du Cloud Computing et la popularité des appareils mobiles connectés, le pare-feu a continué à évoluer pour s'adapter à des environnements de plus en plus décentralisés. Les pare-feu modernes, souvent appelés **pare-feu Cloud**, sont capables de sécuriser des infrastructures réparties sur plusieurs sites, incluant les applications basées sur le Cloud.

En parallèle, l'intégration de la gestion de la sécurité dans des environnements complexes et hybrides a conduit à la conception de solutions comme les pare-feu **Zéro-Trust**, qui s'assurent que chaque demande d'accès à un réseau ou une ressource est systématiquement vérifiée avant d'être autorisée.

10. REFERENCES

https://www.kaspersky.fr/resource-center/definitions/firewall

https://fr.wikipedia.org/wiki/Pare-feu_(informatique)

https://datascientest.com/pare-feu-tout-savoir

https://www.checkpoint.com/fr/cyber-hub/network-security/what-is-firewall/

https://www.cisco.com/c/fr_fr/products/security/firewalls/what-is-a-firewall.html

https://www.futura-sciences.com/maison/definitions/maison-pare-feu-10814/

https://www.cloudflare.com/fr-fr/learning/security/what-is-a-firewall/

Lomé Business School