Les Firewall

Définition

Définition

Firewall

Un firewall, ou pare-feu, est un programme ou matériel destiné à protéger un réseau local contre les menaces provenant de l'extérieur en : - Contrôlant les connexions sortantes. - Sécurisant le réseau interne contre les intrusions externes. - Surveillant et traçant le trafic réseau.

Filtrage Statique vs Dynamique

Filtrage statique (Stateless) :

Analyse chaque paquet de manière indépendante.

Critères : IP source/destination, port source/destination, protocole.

Exemples : `iptables`, `nftables`, `ACL`.

Avantages : Peu de ressources nécessaires, transparent pour les utilisateurs.

Inconvénients : Trop restrictif, inefficace contre certaines attaques comme les chevaux de Troie.

Filtrage dynamique (Stateful) :

Suivi de l'état des connexions (SYN, ACK, etc.).

Exemples : `Netfilter`, `iptables masquerade`, `CBAC` de Cisco.

Avantages : Plus sécurisé, efficace contre les attaques DOS, suivi des connexions.

Inconvénients : Plus gourmand en ressources, peut ralentir le réseau.

Localisation des outils de Firewalling

Le filtrage peut être réalisé sur :

Hôtes/serveurs : PC, smartphones, consoles.

Systèmes d'interconnexion : Box, routeurs, points d'accès WiFi.

ACL (Access Control List) : Filtrage Stateless

Les ACL permettent de filtrer des paquets selon différents critères (IP, ports, protocoles) en fonction des informations dans les en-têtes IP, TCP ou UDP.

Types d'ACL :

- **Standard** : Basé uniquement sur l'IP source.
- **Étendue** : Basé sur plusieurs champs (IP, ports, protocoles).

Critères de filtrage :

- IP source et/ou destination.
- Ports source et/ou destination.
- Protocole (TCP, UDP, ICMP, etc.).

Séquence de traitement :

- Les paquets sont vérifiés successivement par rapport aux critères d'une ACL.
- Action : `permit` ou `deny`.

Exemple 1 : Filtrer tous les paquets de l'IP 172.16.3.10

access-list 1 deny 172.16.3.10 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255

Recommandations sur l'utilisation des ACL

- Placer les **ACL étendues** près de la source des paquets.
- Placer les **ACL standard** près de la destination.
- Optimiser les listes d'accès en plaçant les règles les plus précises en premier.
- Éviter les ACL trop complexes pour ne pas ralentir le routage.

Faiblesses du filtrage ACL :

- Vulnérabilité au **spoofing IP**.
- Permet le **hacking fragmenté** en raison des paquets courts (RFC 791).

Les ACL doivent être utilisées en complément d'autres mesures de sécurité, mais ne suffisent pas comme solution de pare-feu complète.