

Exercices RXI

8-Firewall

Objectifs d'apprentissage

1. Savoir expliquer les principaux objectifs de sécurité réseau
2. Savoir expliquer les fonctions d'un firewall et ses limites
3. Savoir expliquer les fonctions des types d'équipements :
filtre de paquets, passerelle applicative, serveur bastion
4. Savoir expliquer les principales architectures de firewalls et leurs caractéristiques

1 Firewall

a) Expliquez brièvement le concept d'un routeur écran.

Un routeur écran (ou filtre de paquets) filtrent les paquets sur la base des informations contenues dans les en-têtes des paquets (par exemple IP source, IP destination, port source/destination) et des informations sur l'interface d'entrée et de sortie. Les routeurs écran sont un élément essentiel d'une architecture firewall.

b) Comment un routeur écran peut-il interdire, pour des raisons de sécurité, l'accès à certains services (FTP, ...) ?

Les services utilisent des ports connus, par exemple 80 pour le Web, 22 pour le SSH. Afin de rendre un service inaccessible, le routeur écran supprime tous les paquets depuis l'extérieur ayant comme port de destination le port utilisé par le service.

c) Quels sont les avantages de l'utilisation d'un proxy (serveur mandataire) pour les communications des utilisateurs ?

Un serveur mandataire sécurise les communications des utilisateurs de manière presque transparente. La configuration est simple. Il suffit par exemple de configurer le proxy Web dans le navigateur, pour que toutes les connexions Web passent par le proxy.

d) Quels sont les avantages de l'utilisation d'une DMZ ?

Une DMZ permet d'isoler les machines plus vulnérables dans un réseau séparé. Comme vulnérable on considère en particulier les serveurs accessibles à Internet. Un intrus ayant réussi à s'infiltrer sur un tel serveur ne peut pas propager son attaque au réseau interne, comme un routeur écran interne protège ce dernier.

e) Donnez une raison pour laquelle un firewall doit être configuré pour inspecter le trafic entrant, et une autre raison pour le trafic sortant.

Trafic entrant : pour empêcher des attaques venant de l'extérieur (par exemple propagation de vers informatiques)

Trafic sortant : pour empêcher les utilisateurs à accéder des services interdits par la politique de sécurité de l'entreprise

f) Décrivez l'architecture firewall généralement utilisée dans les réseaux d'entreprise.

Les entreprises utilisent généralement un firewall avec une DMZ. Les serveurs vulnérables sont isolés dans la DMZ. Un firewall externe restreint l'accès depuis l'extérieur aux serveurs de la DMZ. Un firewall interne restreint l'accès depuis l'extérieur aux ordinateurs internes et empêche des attaques venant de la DMZ.