TP2 : PAREFEU

OBJECTIF

Le but de ce TP est de concevoir une zone démilitarisée (DMZ) permettant à une entreprise de rendre accessible un serveur web à partir d'Internet. Ce serveur web est placé sur une zone neutre (DMZ), indépendante du réseau local de l'entreprise. En cas d'attaque venant d'Internet, seul le serveur web sera accessible.

Le schéma suivant présente l'architecture du réseau à monter :

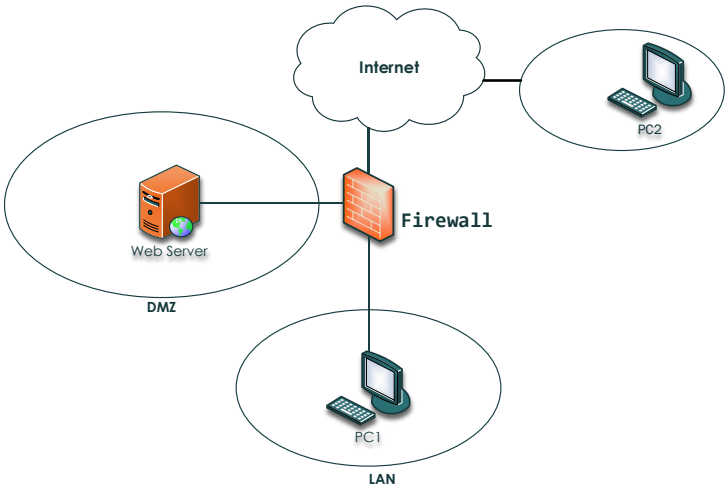

FIGURE 1 : MAQUETTE DU RESEAU A MONTER

Le PC2 sur le schéma représente une machine externe au réseau de l'entreprise (une VM ou votre machine hôte) et sert à tester les règles d'accès depuis l'extérieur.

TRAVAIL À FAIRE:

1. Monter la maquette de la figure1 en proposant un plan d'adressage de votre choix.
2. Ecrire les règles du parefeu pour satisfaire les contraintes suivantes :
   - **a)** Il doit permettre l'accès à Internet des utilisateurs, mais uniquement vers un serveur http ou https (n'oublier pas d'autoriser DNS).
   - **b)** Il doit permettre le ping d'une machine interne vers un serveur sur Internet. L'inverse est interdit.
   - **c)** Les machines du réseau LAN ne doivent pas être visible d'Internet (SNAT)
   - **d)** Le serveur WEB dans la DMZ est accessible depuis le réseau LAN.
   - **e)** Le serveur WEB dans la DMZ n'est pas accessible directement depuis Internet (Utiliser le *port forwarding*).
   - **f)** Le parefeu est accessible en utilisant SSH.
3. Configurer le parefeu pour qu'il puisse détecter et bloquer les scan réseau (nmap).

4. Ajouter les règles qui permettent de protéger le parefeu et les services internes des attaques DoS. Plusieurs solutions sont possibles. Faites une recherche et implémenter celle qui vous parait la plus pertinente.
5. Ecrire des règles de protection contre les attaques par usurpation (spoofing).
6. Le parefeu est accessible par SSH. Faites le nécessaire afin de bloquer une adresse IP pour une heure après 5 tentatives de connexions SSH échouées.