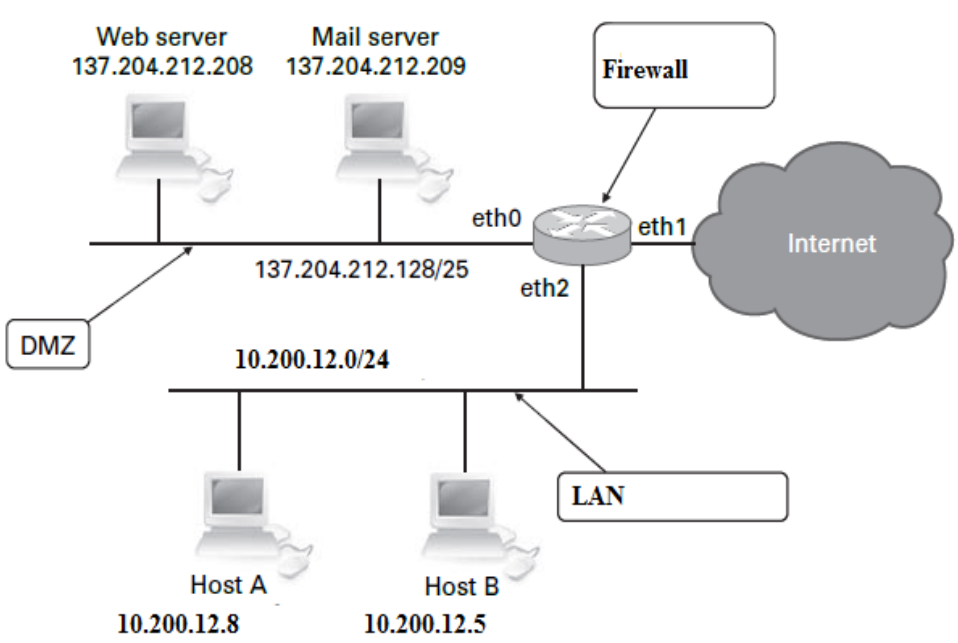
Université Des Sciences et de la Technologie d'Oran Mohamed Boudiaf USTO-MB
Faculté des Mathématiques et Informatique
Département d'informatique

Licence 3 Sécurité Informatique **2020-2021**

TD2 Firewall

Une société dispose de la plage d'adressage suivante 137.204.212.128/25 :

eth0	**137.204.212.129**
eth1	**193.194.88.1**
eth2	**10.200.12.1**



La politique de sécurité de la société requiert deux niveaux de sécurité :

- Les hôtes sur le réseau interne, « LAN », doivent être protégés d'accès non autorisés depuis Internet.
- Les serveurs de la DMZ doivent être accessibles depuis l'extérieur

Donner la configuration du firewall pour que :

Politique de sécurité N°1

1. Chaque connexion initiée de l'extérieur et dirigée vers la DMZ doit être autorisée, si l'adresse IP de destination et le numéro de port correspond a un serveur accessible publiquement.
2. Chaque connexion initiée depuis la DMZ et dirigée vers Internet doit être autorisée.
3. Chaque connexion initiée depuis le réseau interne et dirigée vers la DMZ ou Internet doit être autorisée.
4. tout le reste doit être bloqué.

Politique de sécurité N°2

1. Faire en sorte que le firewall bloque tous les PING vers les machines du réseau interne.
2. Ajouter des règles pour interdire le trafic type SSH et TELNET du réseau interne vers la DMZ.
3. Pour un serveur SSH qui se trouve dans la partie DMZ limiter la demande de la connexion à trois ouvertures par minute.
4. Mettre en place un mécanisme de trace (logs)

Politique de sécurité N°3

1. Partager la connexion internet a partir de l'interface eth0 du firewall avec le réseau interne (Utiliser la table NAT).
2. Par mesure de sécurité l'administrateur de notre serveur web veut camoufler le port de configuration de son serveur le port par défaut est 80 le port camoufler est 8080
   Ecrire la table de nat iptables qui permet de faire cette opération ?
3. Écrire la règle iptables qui permet de faire le NAT sur les deux sorties eth0 et eth1