Année : 2022/2023

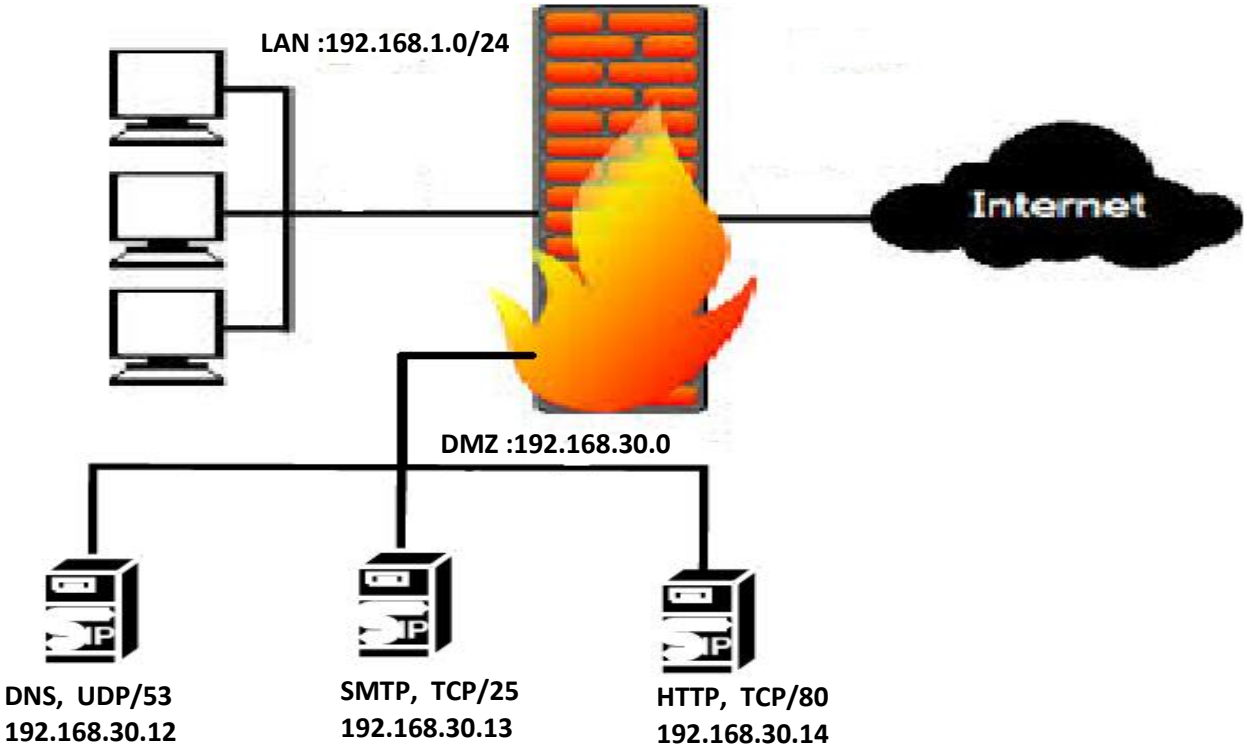
Centre universitaire Abdalhafid Boussouf Mila
Institut des sciences et technologies
3ème Année informatique
Module: Sécurité informatique

Série TD N° 02

Exercice1:

Une entreprise dispose d'un pare-feu pour limiter l'accès depuis et vers les machines de son réseau interne. L'architecture du réseau de l'entreprise comprend également une zone démilitarisée (DMZ) pour le déploiement des serveurs SMTP, HTTP et DNS propres à l'entreprise.

- Le réseau de l'entreprise est représenté par le schéma suivant :

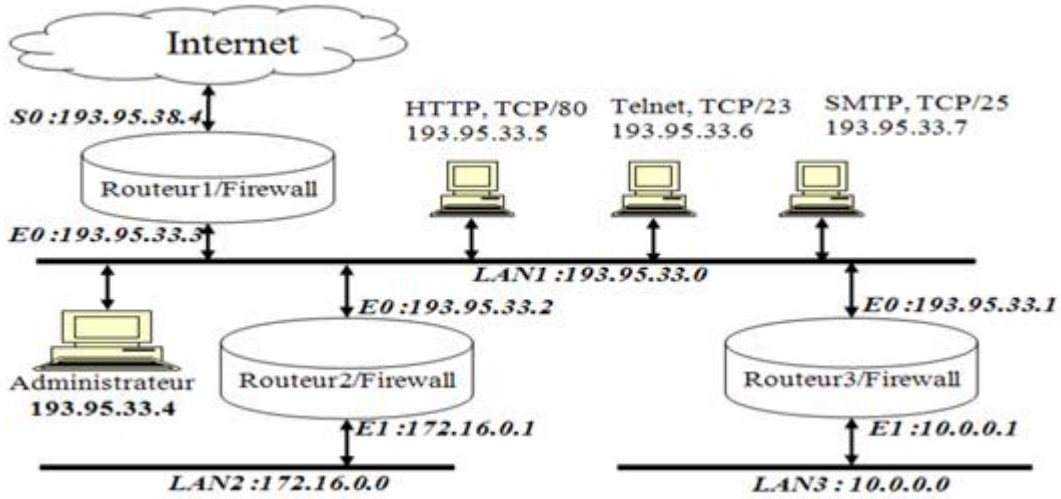


Ecrire les règles de filtrage pour le pare feu correspondant aux politique suivantes :

1- Permettre aux utilisateurs externes d'accéder aux serveurs DNS du Réseau local.
2- Permettre aux utilisateurs internes d'accéder aux serveurs HTTP du Réseau local.
3- Permettre aux utilisateurs internes d'accéder aux serveurs SMTP sur Internet.
4- Tout autre type de communication doit être refusé.

Exercice 2 :

Soit l'architecture du réseau indiqué dans la figure suivante, où LAN1 est le réseau des serveurs accessibles de l'extérieur et de l'intérieur de l'entreprise.



1. Dans quels routeurs doit-on implémenter des règles de filtrage dans chacun des cas suivants (répondre par oui ou non):

	Routeur1	Routeur2	Routeur3
Permettre aux utilisateurs internes et externes d'accéder aux serveursHTTP, FTP et SMTP du LAN1.			
Permettre à la machine administrateur d'accéder aux différents LAN.			
Permettre aux utilisateurs du LAN1 d'accéder à Internet.			

2. Compléter le tableau suivant (règles de filtrage au niveau du Routeur1) permettant aux utilisateurs externes d'accéder au serveur HTTP du LAN1 et permettant aux utilisateurs du LAN1 d'accéder aux serveurs web externes :

@IP source	@IP dest	Port source	Port destination	Protocole	Action