On considère le réseau de la société IMMO-DO qui est constitué des éléments suivants :
Serveurs internes :
- Serveur Proxy ; Linux Debian ; adresse 172.30.32.11 / 255.255.255.0
- Serveur de fichiers ; Windows serveur 2003 ; adresse 172.30.32.12 / 255.255.255.0
- Serveur WEB intranet Linux Debian & Apache ; adresse 172.30.32.13 / 255.255.255.0
- Serveur DHCP ; Linux Debian ; adresse 172.30.32.14 / 255.255.255.0
- commutateur 3com

Postes de travail
- Poste de travail 1 : secrétaire : Windows seven pro
- Poste de travail 2 : directeur : Windows seven pro
- Poste de travail 3 : comptable : Windows seven pro
- commutateur 3com

serveurs accessibles de l'extérieur :
- Serveur DNS ; Windows serveur 2003 ;adresse 172.30.32.3 / 255.255.255.0
- Serveur WEB internet Linux Debian & Apache ;adresse 172.30.32.4 / 255.255.255.0
- Serveur Messagerie Exchange ;Windows serveur 2003 ;adresse 172.30.32.5 / 255.255.255.0
  - Routeur accès internet
  -

Votre travail :
- décrire le rôle de chacun des ces éléments
- critiquer l'architecture réseau de l'entreprise
- proposer une architecture réseau plus conforme à l'état de l'art en matière de sécurité

éléments de correction :

- décrire le rôle de chacun des ces éléments

cf cours

- critiquer l'architecture réseau de l'entreprise

un masque de 255.255.255.0, cela veut dire que la partie réseau de l'adresse des machines est constituée des 3 premiers nombres. On se rend compte que toutes les machines sont sur le même réseau 172.30.32.0/24.
Ce n'est pas une bonne pratique d'un point de vue sécurité car cela veut dire que les machines de l'entreprise peut communiquer directement entre elles. Si l'une d'elle est corrompue, l'attaquant (ou le virus) aura ensuite un accès libre aux autres machines de l'entreprise.

Les machines directement accessibles depuis l'extérieur de l'entreprise (machines bastion) sont des machines exposées. Elles devraient être placées dans une DMZ, réseau spécifique isolé du réseau interne de l'entreprise.

Aucun coupe feu ne filtre l'accès entrant ou sortant de l'entreprise.

- proposer une architecture réseau plus conforme à l'état de l'art en matière de sécurité

La proposition faite en TP consistait en :

- positionner un routeur coupe feu en entrée de l'entreprise
- créer 3 réseaux internes distincts
  - DMZ 172.30.34.0/24 pour les machines bastions accessibles depuis internet
  - serveurs pour les serveurs internes : 172.30.33.0.24
  - réseau interne pour les postes de travail : 172.30.32.0/24
- et ajouter des régles de filtrage (non détaillées) sur le coupe feu pour n'autoriser que le trafic utile au bon fonctionnement des services et interdire le reste.