INSA – 5° R.T.

Sujet d’examen
25 janvier 2008

Sécurité des systèmes informatiques

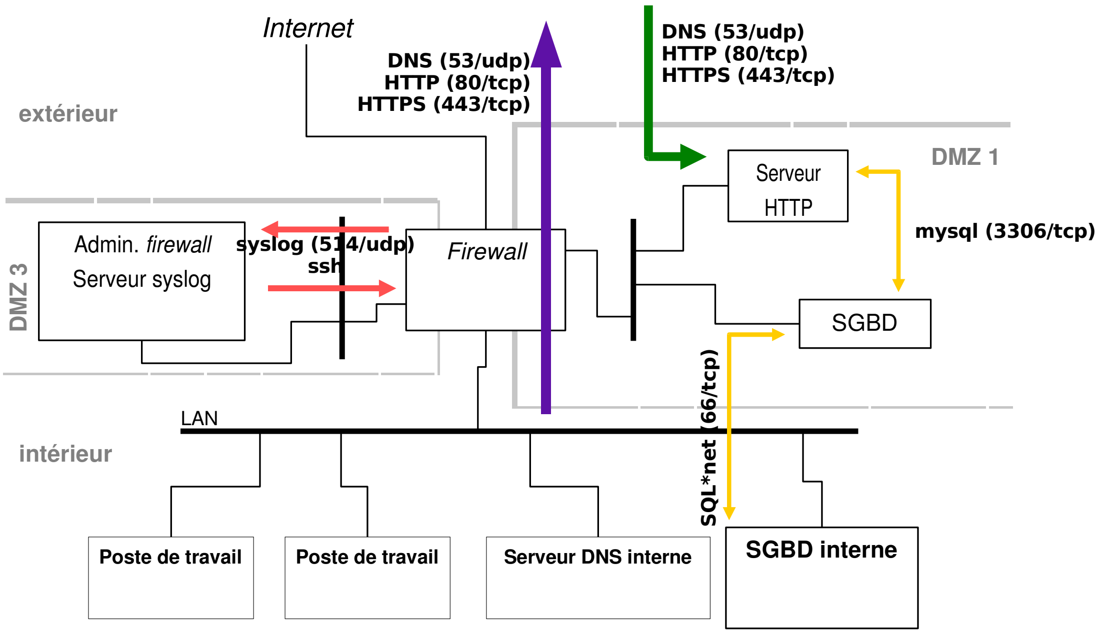
2ème partie

Exercice 1 *(2,5 points)*

Le logiciel d'authentification des systèmes d'exploitation usuels vérifie le mot de passe fourni par un utilisateur à l'aide d'une empreinte de ce mot de passe stockée par le système dans un fichier protégé.

1. Pourquoi stocker des empreintes des mots de passe plutôt que les mots de passe eux-mêmes ?
2. Pourquoi doit-on protéger l'accès à ce fichier contenant les empreintes des mots de passe ?
3. Sous quelle condition cette précaution ne serait pas nécessaire ?

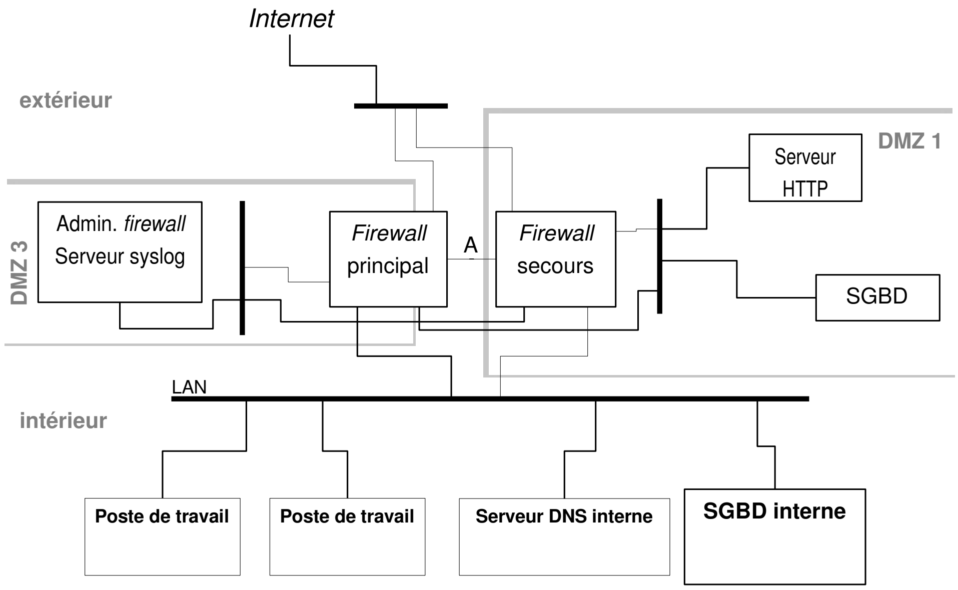
Exercice 2 *(8 points)*
On étudie l'architecture de protection réseau suivante :



Question 1 *(2 points)* : Compte tenu du mode de fonctionnement suggéré par le schéma, expliquez le fonctionnement des différents services réseau fournis à l’organisation utilisant cette architecture. Indiquez les protections offertes par l'architecture.
Question 2 *(1 point)* : Compte tenu des flux identifiés, un autre service réseau devrait figurer en DMZ. Lequel ?

Question 3 *(1 point)* : Certains flux d'administration sont également absents. Indiquez lesquels vous semblent nécessaires et si on peut vraiment envisager de s'en passer dans un cas d'utilisation réaliste.

Pour améliorer la disponibilité de l'architecture, on propose l'évolution suivante visant à introduire de la redondance au niveau du *firewall*. (Il s'agit ici d'une redondance passive où l'équipement de secours ne fonctionne pas en situation normale et ne prend le relais de l'équipement principal qu'en cas de besoin.)



Question 4 *(1 point)* : Certains équipements nécessaires au fonctionnement du système n'apparaissent pas sur la figure. Lesquels ? Quel peut être l'impact de leur choix sur la disponibilité de l'ensemble ?

Question 5 *(1 point)* : Compte tenu de la gestion de la redondance et des informations gérées en interne par un *firewall*, quelles informations transitent sur le lien A ?

Question 6 *(1 point)* : A votre avis, du point de vue d'un utilisateur (ou d'un routeur) sur Internet, quelle est l'adresse IP du *firewall* ? Comment pourrait-on gérer ce type de cas ?

Question 7 *(1 point)* : On envisage de basculer dans une autre configuration où les deux firewall fonctionnent en régime normal en se partageant le trafic. Pointer les difficultés que ce type de fonctionnement peut poser au niveau du fonctionnement habituel d'un réseau ?

<u>Exercice 3</u> *(1,5 points)*

Un employé télécharge de la musique grâce à un logiciel *peer-to-peer* pendant ses heures de travail. Il reçoit et lance malencontreusement une copie d'un virus *VisualBasic* qui se propage automatiquement sous forme de courrier électronique à tous les contacts inscrits dans son carnet d'adresses. Le serveur de messagerie interne étant doté d'un antivirus, la pièce jointe est heureusement automatiquement éliminée. Quels principes de base ne sont pas respectés dans l'architecture informatique de cette entreprise ?