INSA – 5° R.T.

Sujet d'examen
21 janvier 2011

Sécurité des systèmes informatiques

2ème partie

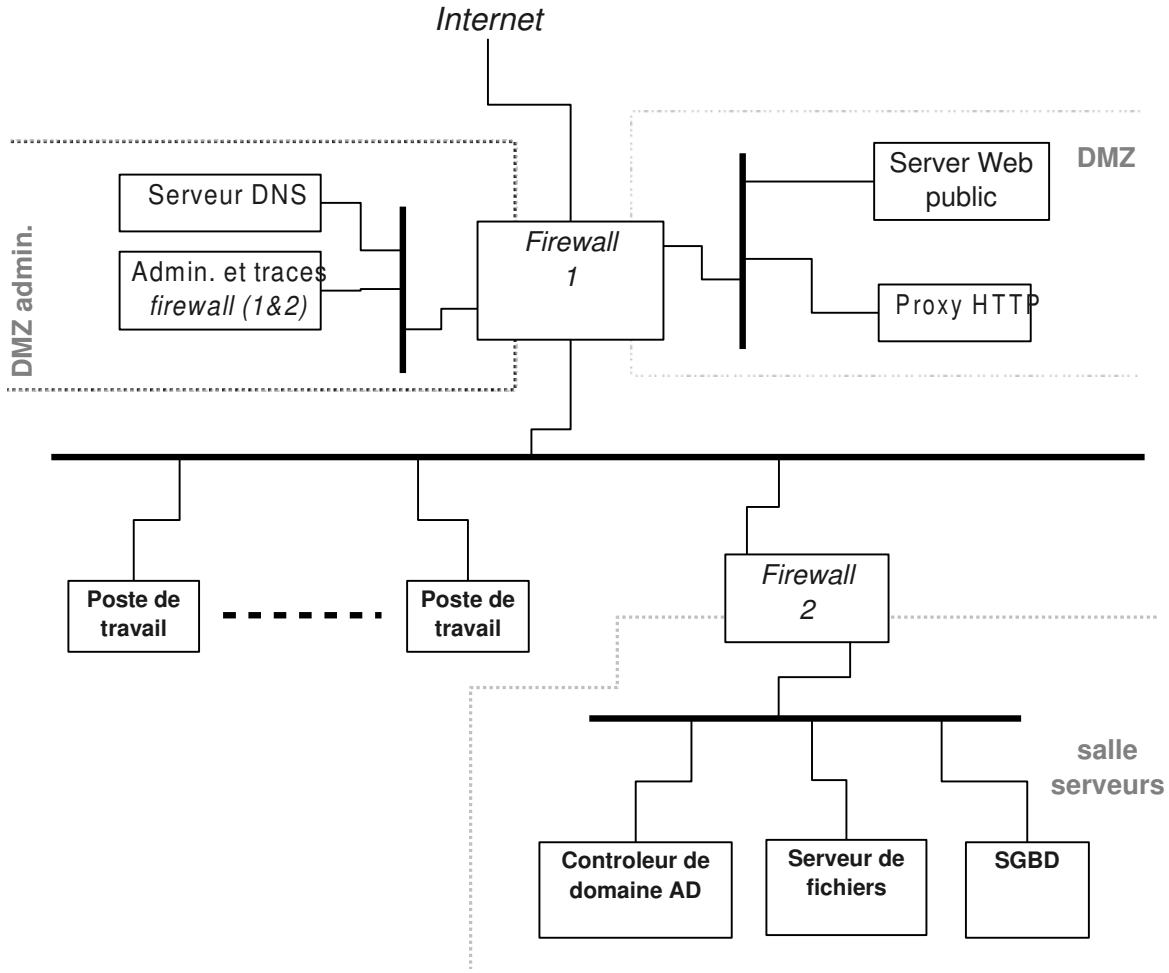
Exercice 1 *(3 points)*

Le protocole HTTPS (HTTP sur SSL/TLS) est couramment utilisé pour sécuriser les communications entre un serveur Web et un navigateur. Pour cela, une session HTTPS s'appuie sur un certificat diffusé par le serveur permettant d'effectuer une session d'authentification initiale et ensuite un chiffrement du canal de communication dans lequel transite l'échange HTTP.

1. Lors de l'authentification, le protocole utilise une clef publique contenu dans un certificat que le serveur détient et diffuse au client à l'établissement de la connexion. Quelles sont les protections offertes par cette utilisation d'un certificat serveur ?
2. Comment l'utilisateur du navigateur peut-il être assuré que cette clef publique correspond bien à l'organisme auquel il souhaite accéder ?
3. Pourquoi de nombreux services Web, utilisant pourtant HTTPS, demandent-ils en plus à l'utilisateur de fournir un nom de compte et un mot de passe pour compléter l'ouverture de session ?
4. Il est possible d'utiliser un certificat client stocké sur le navigateur pour l'échange HTTPS. Quel est l'effet de l'utilisation d'un certificat client sur la protection de l'ensemble du service ?
5. Avec un certificat client, l'utilisateur doit quand même parfois fournir une « *passphrase* »: de quel mot de passe s'agit-il ?
6. Pensez-vous qu'il y ait une « *passphase* » utilisateur sur la partie privée du certificat serveur ? Pourquoi ?

Exercice 2 *(7 points)*

On étudie l'architecture de protection réseau suivante :



Question 1 *(2 points)* : Compte tenu du mode de fonctionnement suggéré par le schéma, présentez les différentes zones de sécurité associées à l'architecture de protection réseau et leurs niveaux de sécurité respectifs.

Question 2 *(1 point)* : Commentez les rôles respectifs du serveur DNS situé en DMZ d'administration et du contrôleur de domaine AD vis à vis du service DNS offert globalement par le système d'information aux utilisateurs internes et externes.

Question 3 *(2 points)* : On a ici une architecture de protection faisant appel à deux équipements distincts, l'un tourné vers Internet et l'autre vers les systèmes serveurs.

Que pensez-vous de ce choix d'architecture en terme de protection, de configuration ?

Quelles seront à votre avis les contraintes de fonctionnement respectives de chacun des deux équipements, en particulier du point de vue des flux réseaux à traiter (nature, débit, etc.). (Mettez notamment en évidence les différences.)

Question 4 (1 *point*) : On suppose que les deux *firewall* sont de technologie identique et que le serveur d'administration et de gestion des traces est unique pour les deux. Commentez cet aspect vis à vis de l'administration et du positionnement de la DMZ d'administration.

Question 5 *(1 point)* : Quel avantage et quel inconvénient pourrait-il y avoir au fait d'avoir deux *firewall* de technologies différentes au lieu de deux équipements similaires?