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 ?

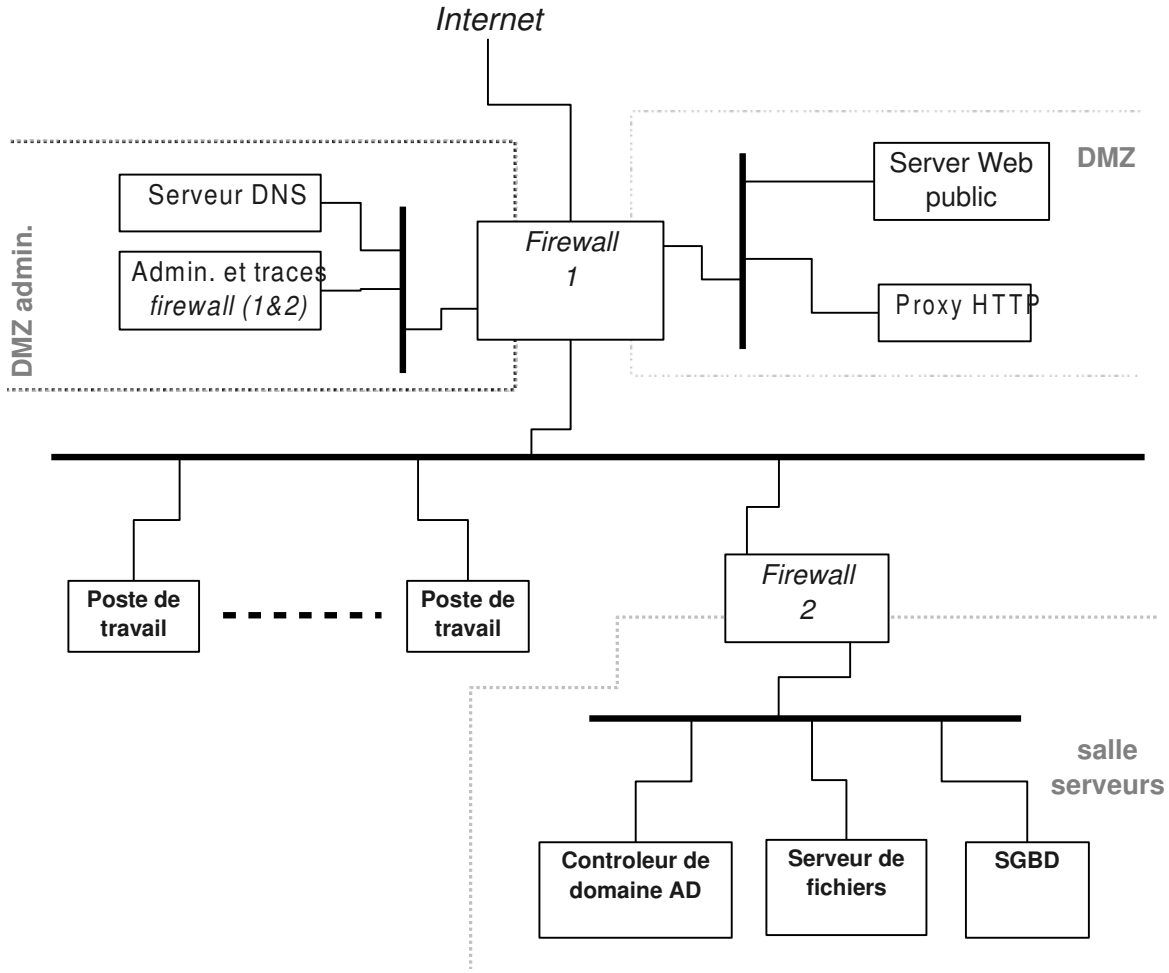
Corrigé

1. *Le protocole SSL avec un certificat serveur offre d'abord une authentification du partenaire accédé par une vérification que ce serveur détient bien la clef privée correspondant à la clef publique diffusée. Ensuite, la communication est chiffrée, on a donc des garanties sur la confidentialité des échanges ainsi que sur l'intégrité de la communication pendant toute sa durée.*
2. *Le certificat n'inclut pas seulement la clef publique, mais également une signature de cette clef publique par un autre certificat. (Celui-ci pouvant également être un certificat intermédiaire.) La racine de cette chaîne de certification doit être un certificat pré-installé sur le navigateur (ou obtenu indépendamment en préalable à la communication). L'utilisateur peut alors être sûr que le certificat diffusé par le serveur appartient bien à l'organisme indiqué s'il vérifie la chaine de certification, s'il a confiance dans le certificat racine et s'il a confiance dans les organismes détenteurs des certificats intermédiaires pour avoir fait les vérifications nécessaires avant de signer les certificats dérivés. (Il s'agit alors de tiers de confiance ou d'autorités de certification.)*

3. *Le certificat serveur n'offre qu'une authentification du serveur. Si le service accédé gère une base de comptes utilisateurs, ceux-ci doivent donc également en plus s'authentifier. Cette authentification du client peut éventuellement s'effectuer via un nom d'utilisateur et un mot de passe. Cette méthode est moins forte qu'une technique faisant appel à des algorithmes de cryptographie asymétriques, mais elle est bénéficie néanmoins via HTTPS de la protection offerte par le canal chiffré et signé de SSL.*
4. *Dans ce cas, l'authentification du client, appuyée sur un certificat et une authentification à clef privée/clef publique offre des garanties bien plus importantes en terme de sécurité. Par contre, il faut alors gérer une procédure de délivrance de ces certificats clients (incluant leur signature par un tiers de confiance, après vérification de l'identité du demandeur par exemple).*
5. *La clef privée associée à un certificat ne doit être que très rarement stockée en clair (notamment sur disque). Elle est protégée par un chiffrement symétrique dont la « passphrase » constitue la clef. C'est donc un mot de passe permettant de déverrouiller l'usage du certificat et de protéger la clef privée de l'utilisateur en cas de vol (par exemple afin de lui laisser le temps de détecter le vol et de révoquer son certificat).*
6. *Si une passphrase est aussi utilisée sur le serveur, à chaque lancement du service Web, il sera nécessaire de la fournir au programme afin qu'il puisse accéder à la clef privée du certificat serveur. Il est peu probable que ceci soit effectué de manière interactive (à chaque redémarrage...). Il est plus probable qu'en pratique, soit la clef privée est effectivement stockée en clair sur le serveur, soit la passphrase en question est stockée dans les paramètres de configuration du serveur (ce qui n'est pas mieux).*
   Ce faisant, les administrateurs Web/système dérogent vis à vis du certificat serveur aux règles de protection qu'ils recommandent à leurs utilisateurs pour les certificats clients. À méditer...

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?

Corrigé

Question 1:

- *La DMZ Admin est une zone d'administration des équipements de sécurité. Elle contient un serveur de gestion des firewall qui stocke également les traces que ces équipements collectent. On trouve également dans cette zone un serveur DNS, probablement placé là car il s'agit d'une zone de haut niveau de sécurité. Ce serveur DNS est alors probablement le serveur principal des zones attribuées à l'entreprise ou l'organisme concerné.*
- *La DMZ contient un serveur Web accessible de l'extérieur. Elle contient également un relais HTTP, qui doit servir à relayer les accès internes vers Internet.*
- *La zone « salle serveurs » est elle aussi placée dans une zone de sécurité spécifique. Ainsi, l'ensemble des serveurs sont logiquement isolés au niveau du réseau des postes de travail et des autres zones de sécurité.*

Question 2:

On peut supposer que le serveur DNS de la DMZ Admin. correspond au serveur DNS visible sur Internet qui gère en propre la zone DNS de l'entreprise. Par contre, le serveur DNS associé au serveur AD situé en interne gère également des zones de nommage (via le DNS) mais qui sont associées aux machines internes du LAN (noms de machines Windows, noms de domaines, etc.). Cette zone n'est a priori pas visible depuis Internet.

Par contre, on entrevoit là une difficulté de fonctionnement. En effet, les postes de travail peuvent avoir besoin d'accéder simultanément aux deux zones de nommage et la configuration respective des deux serveurs sera à étudier plus précisément (notamment si on souhaite éviter que tous les clients n'aient à essayer la résolution de leurs noms auprès des deux serveurs tour à tour, ce qui n'est pas vraiment optimal).

Question 3:

En terme de protection, on dispose ici de deux lignes de défense pour les éléments de l'organisme ayant très probablement le plus de valeur dans le système d'information: ses serveurs internes. C'est certainement positif du point de vue de la sécurité si les firewall sont gérés correctement.

Un point d'administration central est également prévu, qui semble donc ainsi offrir des fonctions de gestion unifiée des 2 équipements afin de faciliter leur configuration. Toutefois, on imagine déjà que cette configuration sera plus compliquée qu'avec un seul équipement faisant face seulement à des flux à la frontière avec Internet.

Le firewall externe est exposé à l'ensemble d'Internet. Il est donc susceptible de faire face à des menaces extrêmement variées. Par contre, les protocoles qui le traversent sont probablement peu nombreux et relativement faciles à préciser et maitriser. C'est finalement un cas assez classique d'utilisation de ce genre d'équipement.

Le firewall interne est essentiellement destiné à assurer une protection des serveurs vis à vis des utilisateurs internes (ou en 2° ligne de protection pour une intrusion externe réussie sur les postes de travail). Or, en interne au LAN, les flux réseaux sont parfois très variés (impression, partage de fichiers, etc.) et la configuration de ce firewall va sans doute être difficile à affiner précisément. On sera même surement amené à faire des compromis sur cette configuration afin d'éviter des dysfonctionnements. Par ailleurs, la volumétrie des flux réseaux concernés sera certainement beaucoup plus importante sur le LAN au niveau du firewall interne que vis à vis d'Internet. La performance de cet équipement sera donc à surveiller.

Question 4:

La DMZ d'administration peut être vue comme la zone de plus haut niveau de sécurité dans l'architecture. Il aurait peut-être été plus logique dans ce cas de la faire elle aussi bénéficier du double niveau de protection réseau (tout comme les serveurs). On aurait donc pu raccorder cette DMZ d'administration sur le 2° firewall interne au lieu de la connecter directement au 1° firewall.

(Par contre, dans ce cas, le positionnement du serveur DNS serait à ré-étudier.)

Peut-être le firewall interne a t'il été installé dans un 2° temps, après que le firewall tourné vers Internet ait été déployé ?

Question 5:
Si les deux firewall sont identiques, on note déjà un risque en cas de faille de sécurité sur l'équipement en question. L'avantage d'avoir deux firewall différents, c'est que même en cas de vulnérabilité grave affectant le firewall en contact avec Internet, le 2° équipement interne pourra assurer une protection des principaux serveurs.
Par contre, en terme de configuration, il sera alors certainement très difficile de disposer d'un moyen de configuration unifié des deux équipements. On aura donc un inconvénient (probablement important) vis à vis de la facilité d'administration de l'architecture.