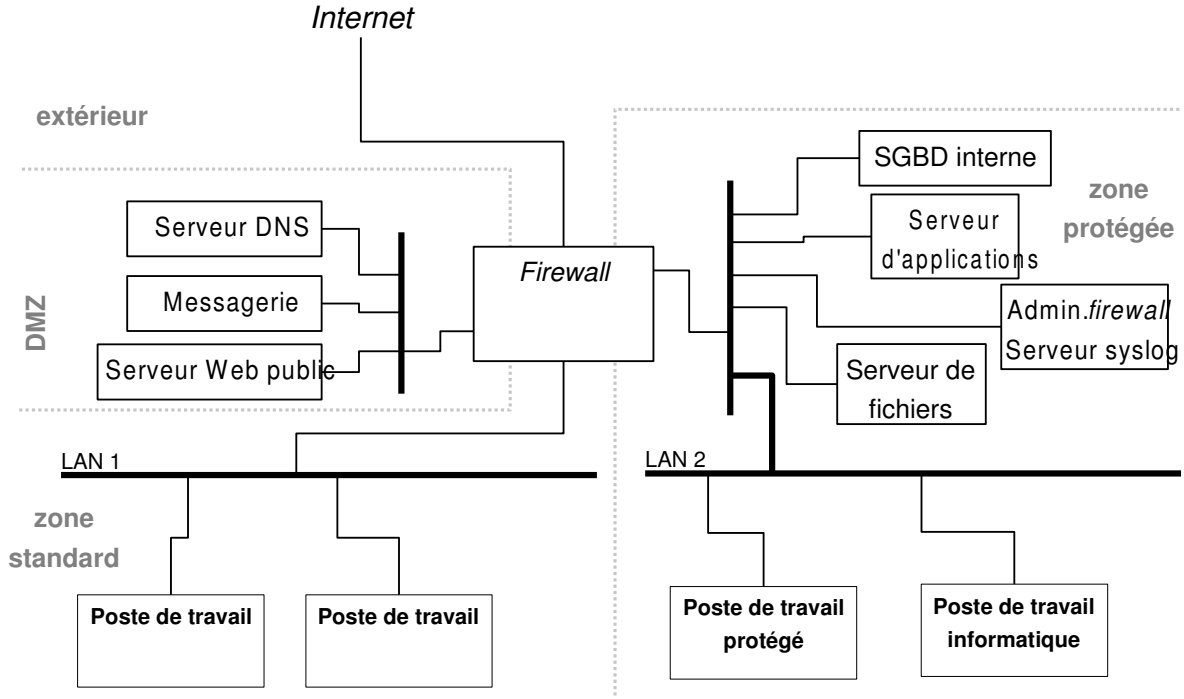
INSA – 5° R.T.

CORRIGÉ
Examen du 23 janvier 2009

Sécurité des systèmes informatiques

2ème partie

Exercice 1 *(6,5 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)* : D'un point de vue organisationnel, que pensez-vous de l'impact que va avoir cette architecture, notamment au niveau de la situation du service informatique ?
Question 3 (2 *points*) : Indiquez quels sont, à votre avis, les avantages et les inconvénients d'une telle architecture, notamment en regard des 3 axes : disponibilité, intégrité, confidentialité ?
Question 4 *(1 point)* : Proposez une option d'amélioration *technique* de cette architecture ?
Question 5 *(0,5 point)* : Nécessairement présent pour une simple connexion à ce système d'information, un serveur primordial n'apparaît pas. Lequel ?

Description du fonctionnement (question 1) :
Les machines situées dans la zone DMZ hébergent des services nécessitant généralement des accès depuis ou vers Internet.

- *Tout d'abord, le serveur DNS permet d'assurer la résolution des noms appartenant à TEG auprès des autres serveurs DNS d'Internet (flux entrant depuis l'extérieur). Il*

permet également de consulter les serveurs DNS d'Internet afin d'effectuer la résolution des noms demandés par les différents réseaux internes de TEG.

- *Les flux de messagerie (Internet) de l'entreprise entrent ou sortent de son réseau via la passerelle de messagerie située dans cette DMZ. Cette passerelle doit également être accédée depuis le LAN1 ou le LAN2 afin de permettre aux utilisateurs de relever leur boite de messagerie ou d'envoyer des messages.*
- *Enfin, un serveur Web est présent dans cette zone, certainement principalement à l'usage d'Internet. (Des accès en mise à jour sont également sans doute possible depuis un des deux LAN.)*

Les machines recensées dans le réseau LAN1 sont seulement des postes de travail. Le LAN1 compte probablement la majorité des postes de travail du système d'information. Ce réseau, associé à une zone « standard » du point de vue de la sécurité, correspond aux postes de travail généralistes, est a été isolé dans cette architecture. Ces postes de travail sont notamment isolés de tous les serveurs.

Les machines situées dans la zone « protégée » sont de 2 catégories : des serveurs et des postes de travail.

- *Les serveurs correspondent à des services à usage essentiellement interne: SGBD, serveur de fichiers, serveur d'applications. Ces services sont certainement accédés depuis le LAN1 pour permettre aux postes de travail de la zone standard de fonctionner normalement. Toutefois, l'ensemble des serveurs est isolé de la majorité des postes de travail qui ne peuvent y accéder qu'au travers des contrôles effectués par le firewall (types de services réseau utilisés, adresses source et destination, etc.)*
  Un serveur spécifique est plus particulièrement associé aux fonctions de sécurité (administration du firewall, rétention des traces). Celui-ci doit être d'accès restreint (limité à la zone protégée et probablement inaccessible depuis le LAN1).
- *La zone protégée comporte également un LAN. Ce LAN2 connecte des postes de travail, identifiés comme « protégé » ou « informatique ». Ces postes de travail peuvent accéder directement aux serveurs internes.*
  Cette zone vise apparemment à offrir un niveau de sécurité élevé, du même niveau que celui associé aux principaux serveurs internes, dont bénéficie les postes de travail protégés ou à vocation informatique.

On n'identifie pas de postes de travail « informatique » sur le LAN1, il est donc probable que tous les informaticiens disposent de postes de travail dans le LAN2.

<u>Impact organisationnel</u> (question 2) :
Techniquement parlant, les postes de travail des informaticiens sont isolés des postes de travail normaux, mais ils sont aussi notablement privilégiés car directement connectés aux ressources internes du système d'information. Par ailleurs, pour une mise en oeuvre efficace, cette architecture suppose que le service informatique soit entièrement regroupé physiquement et distinct des autres services de TEG.
D'un point de vue organisationnel, cette architecture va donc probablement avoir un impact en conduisant à sanctuariser, non seulement les ressources informatiques, mais également le service informatique dans son ensemble. Cette séparation entre utilisateurs normaux et informaticiens (ou utilisateurs protégés) peut conduire à un éloignement entre les préoccupations des uns et des autres.

On peut envisager que l'autorité du service informatique s'en trouve dans un premier temps renforcée. Néanmoins, surtout dans un contexte civil, la vocation d'un service informatique est avant tout d'offrir des services aux autres utilisateurs et l'éloignement entre les utilisateurs finaux et le service informatique peut aussi conduire à un déficit de collaboration, voire des dysfonctionnements.

<u>Avantages/Inconvénients</u> (question 3) :
Avantages :
Les serveurs internes de l'entreprise sont protégés des accès de la majorité des postes de travail, hors les utilisateurs protégés ou les informaticiens (qui ont de toute manière généralement accès à des droits étendus sur ces systèmes). L'intégrité de ces systèmes est donc renforcée par le contrôle d'accès plus précis au niveau réseau.
L'existence d'un LAN protégé, plus étendu qu'une DMZ classique, permet de disposer d'une zone de travail sécurisée. Ceci peut permettre d'envisager d'aborder des projets nécessitant un niveau de sécurité élevé (par exemple des projets confidentiels) en dotant les équipes concernées d'un poste de travail protégé ; et en assurant également la sécurité physique de la zone.
Les services en interaction avec l'extérieur sont situés dans leur propre zone de sécurité (la DMZ) et bénéficient de la protection du firewall à la fois vis à vis d'Internet mais également des utilisateurs internes. L'intégrité de ces services est améliorée.

Inconvénients :
Le firewall est situé à un point névralgique du réseau, à la fois pour les communications avec l'extérieur mais également pour les communications réseaux internes. Ainsi, si le firewall est indisponible, non seulement les postes de travail ne peuvent plus accéder aux ressources extérieures (par exemple Internet), mais ils sont également dans l'incapacité d'accéder aux applications locales de TEG ou à ses serveurs de fichiers. Ceci constitue un risque important vis à vis de la disponibilité.
Les postes de travail des informaticiens et les postes de travail protégés sont situés au même niveau de sécurité. Dans le cas de projets confidentiels ou sensibles, il faudra donc prendre en compte le fait que tous les informaticiens vont également être concernés par les contraintes de sécurité du projet.
Le firewall se trouve situé dans la position d'un coeur de réseau ; il devra donc être en mesure de gérer un volume de trafic très important (notamment par rapport au seul trafic sortant/entrant de l'entreprise dans une architecture plus classique).
Le système d'administration du firewall est situé dans la même DMZ que les serveurs de l'entreprise. Certes il est ainsi dans une zone protégée, mais il est aussi placé au même niveau de sécurité que ces serveurs (alors qu'il assure lui la gestion des équipements de protection). Il est donc potentiellement accessible à tous les postes de travail du LAN2 (même si on suppose qu'une authentification spéciale est nécessaire pour accéder à cette administration de sécurité).

<u>Amélioration(s)</u> (question 4) :
Compte tenu de la remarque précédente vis à vis de la disponibilité, l'introduction de redondance au niveau du firewall avec la mise en place d'un équipement de secours semble tout à fait souhaitable. Pour ce type d'architecture, une redondance permettant la mise en ligne très rapide de l'équipement de secours semble même recommandée afin de ne pas

perturber les accès aux applications et aux données internes en cas de défaillance du firewall principal.

Isoler le serveur d'administration du firewall dans une DMZ dédié pourrait également permettre de mieux contrôler l'accès à l'administration du firewall lui-même.

Enfin, séparer le LAN2 en 2 zones, soit par l'introduction d'un autre équipement de sécurité, soit par l'ajout d'une DMZ dédiée, permettrait de séparer les postes de travail « protégés » des postes de travail informatiques. Ceux-ci peuvent en effet nécessiter tous deux des niveaux de sécurité plus élevé que les postes de travail standard ; mais malgré tout, ils correspondent à des besoins différents. Un cloisonnement entre ces deux types de besoin de sécurité permettrait de faciliter la prise en compte d'éventuels conflits d'intérêts entre les 2 catégories.

<u>Complétude de la description</u> *(question 5) :*
Visiblement, le système d'information fonctionne avec des ressources réseau centralisées situées sur les serveurs internes : serveur de fichiers partagés, serveur d'application, SGBD backoffice. Pour accéder initialement au système d'information et à ses ressources, les utilisateurs doivent donc s'authentifier auprès d'un service d'authentification disposant d'une base des différents utilisateurs autorisés. Ce serveur essentiel[1], notamment du point de la sécurité, qui manque au niveau des serveurs internes de la zone protégée.

<u>Exercice 2</u> *(1 point)*
WEP&WPA (sécurité WiFi), SSL/TLS (utilisé par exemple dans HTTPS), IPsec et PGP (logiciel de chiffrement de fichiers ou de messages) sont tous des moyens de sécuriser des échanges de données. Pour chacune de ces techniques, indiquez comment elle se positionne par rapport au modèle en couches TCP/IP (qui distingue les 4 niveaux suivants : application, transport, réseau et accès réseau).

Les différents protocoles correspondent à la répartition suivante :
- *accès réseau : WEP&WPA*
- *réseau :IPSEC*
- *transport : SSL/TLS*
- *application :PGP*

<u>Exercice 3</u> *(2,5 points)*
L'entreprise TrucsEnGros (TEG) est une société disposant d'un centre informatique central situé au siège de l'entreprise et de plusieurs succursales réparties sur le territoire national. Elle sous-traite à l'opérateur de télécommunications AlloYaKkun (AIK) la mise en place d'un réseau privé entre son siège et ses succursales. AIK prend en charge tout le réseau WAN, jusqu'aux points d'accès Ethernet offerts au niveau du réseau LAN de TEG. Le système d'information de TEG est constitué de matériels et de logiciels commerciaux courants.
Dernièrement, le comité de sécurité de TEG a élaboré une charte de sécurité du système d'information à destination de ses utilisateurs et la direction vient de décider de la mettre en application (avec l'aval du conseil d'administration). Cette charte explicite les principes généraux de l'utilisation du système d'information et des moyens de communication de l'entreprise (usage à vocation professionnelle, respect de la vie privée, protection des données,

[1] Actuellement, souvent un contrôleur de domaine Active Directory.

existence de moyens de protection et de contrôle, usage de la messagerie, d'Internet, des clefs USB, etc.). La question se pose désormais de savoir à qui la diffuser précisément.
La plupart des employés de TEG disposent d'un micro-ordinateur et utilisent le système d'information dans leur travail quotidien.

1. Imaginez des exemples concrets (Pierre, Paul, Jacques, Alice, etc.) d'employés ou de collaborateurs amenés à interagir avec le système d'information de TEG et appartenant à des catégories différentes d'intervenants (parmi toutes celles que l'on peut rencontrer dans la vie quotidienne d'une entreprise).
2. Par rapport aux différents exemples d'intervenants que l'on peut identifier, indiquez comment on peut envisager de *formaliser ou contractualiser* la diffusion de la charte auprès des différents types d'utilisateur.
3. Indiquez en le justifiant des catégories d'utilisateurs (notamment dans le domaine technique) qui peuvent nécessiter des aménagements spécifiques du *contenu* d'une telle charte de sécurité (par exemple parce qu'ils révèlents des droits ou des besoins particuliers).
4. La charte est inscrite dans le serveur Web interne de TEG. Donnez des exemples d'intervenants ou de personnels qui ne sont pas touchés par cette publication.

Notez que les exemples identifiés (et les catégories d'intervenants dans une entreprise) sont à prendre en compte vis à vis de différents aspects : existence d'un contrat de travail direct ou d'un équivalent, existence d'une relation client/fournisseur (le contrat commercial est alors entre les personnes morales employant les personnes physiques), aspects techniques (notamment pour l'informatique : développeur, administrateur, utilisateur ou réseau, système, application, etc.)

Exemples d'intervenants :

- *José, salarié de TEG en CDI.*
- *Paul, salarié de TEG en CDD de 6 mois.*
- *Jean, stagiaire d'un établissement d'enseignement au service comptabilité*
- *Alice, intérimaire sur un poste de secrétariat RH.*
- *Maxime, administrateur réseau de AIK, chargé de la maintenance routeurs du siège de TEG.*
- *Francis, technicien réseau de EFGH, sous-traitant de AIK, chargé par ce dernier de l'installation d'un point d'accès réseau dans une succursale de TEG en province.*
- *Stéphanie, administrateur système chez TEG (salarié en CDI).*
- *René, administrateur réseau chez TEG (salarié en CDD).*
- *Nicole, développeur d'une application métier chez TEG (salarié en CDI).*
- *Didier, consultant de la société IJKL participant à un projet de développement d'application de TEG.*
- *Vincent, stagiaire d'une école d'ingénieur chargé d'un projet expérimental de déploiement de VPN via Internet pour le réseau TEG.*
- *Pierre, livreur de la société ABCD, amenant du matériel informatique chez TEG.*
- *Isidore, membre du conseil d'administration de TEG.*

Formalisation :

Vis à vis des personnels dont le lieu de travail habituel est l'entreprise TEG, la délivrance de la charte peut s'effectuer au travers du service RH. Dans ce cas, la formalisation de sa délivrance peut être effectuée via la signature d'un accusé de réception.
On touche généralement ainsi les catégories suivantes : celle des personnes ayant un contrat de travail conclu directement avec TEG (qu'ils soient CDI ou CDD), et celle des personnes

travaillant dans l'entreprise suite à une convention particulière (convention de stage, contrat d'intérim[2]).

En ce qui concerne les personnes intervenants dans un cadre contractuel de type commercial (la plupart des sous-traitants), l'engagement personnel n'a pas directement lieu d'être. La formalisation du respect de la charte de sécurité (ou des objectifs de sécurité de TEG) doit être prévue dans le contrat liant TEG avec son sous-traitant. Ces clauses contractuelles doivent aussi prévoir la répercussion de cette obligation vers d'éventuels sous-traitants secondaires (ou interdire de faire appel à d'autres sous-traitants).

Notez qu'il reste certaines catégories manquantes (livreurs, membres du conseil d'administration) pour lesquelles ce type de formalisation semble difficile à mettre en place.

Exceptions et aménagements :
Les administrateurs réseaux et les administrateurs système[3] bénéficient de droits étendus sur le système d'information de part leur activité. Ils peuvent donc nécessiter des aménagements concernant la charte de sécurité afin de pouvoir exercer leur métier sans violer certaines de leurs obligations (par exemple pour capturer du trafic en ce qui concerne un technicien réseau).

Diffusion intranet :
Ne touche pas ceux n'ayant pas d'accès au niveau applicatif, notamment les sous-traitants intervenant ponctuellement (comme l'opérateur réseau par exemple).
Rq: Ne touche pas non plus les salariés de l'entreprise en absence de longue durée au moment de la publication.

[2] Point à vérifier, mais si le contrat de travail d'un intérimaire reste avec la société d'intérim, un changement de lieu de travail est, d'après mes sources, très certainement inscrits pour chaque mission d'intérim.
[3] Les administrateurs de sécurité également bien entendu ; mais aussi les techniciens RH, les juristes, les auditeurs, les comptables...