

## EXAMEN DE RESEAU

(Documents et calculatrices autorisés, durée : 2 heures. 2 pts/question)

1. Citez les trois principaux principes de base qui guident à la fois la mise en oeuvre et l'évaluation de la sécurité des systèmes d'information.
2. Lors de la mise en oeuvre d'une PSSI, le débat autour de l'échelle convenable pour caractériser des critères de sécurité s'éternise. Proposez 4 niveaux pour la confidentialité et 3 niveaux pour l'intégrité.
3. Citez deux avantages et deux inconvénients liés à l'externalisation des applicatifs d'une Entreprise de son infrastructure locale vers une solution d'hébergement dans le Cloud.
4. La mise en oeuvre de la sécurité sur le critère de la disponibilité repose en grande partie sur la protection de l'accès aux ressources via le réseaux aux seuls terminaux, utilisateurs et trafics légitimes. Il s'agit donc en général de spécifier très clairement tous les accès autorisés et d'interdire par défaut tous les autres. Dans un contexte d'infrastructure locale, le pare-feu est placé à l'entrée du réseau de l'Entreprise. Dans un contexte d'externalisation, les postes de travail sont éparpillés entre l'Entreprise, les employés mobiles et les télé-travailleurs. Dans ces conditions, où doit être implémenté le pare-feu matérialisant la politique propre de l'Entreprise ?
5. Dans un réseau local basé sur une architecture classique reliant le routeur à deux commutateurs principaux (un par bâtiment), tous les commutateurs secondaires sont directement reliés au commutateur principal du bâtiment dans lequel ils se trouvent et chaque poste de travail est obligatoirement connecté à un de ces commutateurs secondaires. Si on suppose que le taux de perte est uniforme pour toutes les liaisons, alors peut-on dire que le taux de perte estimé pour tout trafic allant d'un poste de travail vers Internet est à peu près le quadruple du taux de perte d'une liaison élémentaire ?
6. Discutez l'utilisation de la cryptographie (asymétrique vs symétrique) dans le cadre d'une application sécurisée impliquant des flux à contraintes temps réel (communications trains-infrastructure ferroviaire, outil de visio sécurisé tel que Tixeo, etc). Décrivez comment vous mettriez en oeuvre cette sécurité dans les grandes lignes.
7. La validité du certificat électronique est assurée par la présence d'un Hash des informations sur le détenteur chiffré avec la clé privée de l'autorité de certification (sceau signé). Décrivez la procédure suivie par le navigateur d'un client C pour vérifier la validité d'un certificat CA présenté par le serveur S et signé par l'autorité de certification AC.
8. Citez sans les détailler trois nouveaux paradigmes des réseaux fortement impliqués soit dans l'organisation des futurs clouds, soit dans la mise en oeuvre de la 5G, au choix.
9. Le pare-feu applicatif est un dispositif intrusif qui accède aux messages transmis dans un réseau IP et en analyse le contenu, y compris dans les sections autres que les en-têtes, afin de détecter des séquences interdites ou malicieuses. A ce titre, sa présence dans un réseau doit être explicitement notifié aux utilisateurs au même titre que la vidéo-surveillance. Qu'en pensez-vous ?
10. Donnez au moins un élément manquant dans les étapes ci-après lors de la mise en oeuvre d'une PSSI dans une Entreprise comprenant un grand nombre de salariés divers :
  - Détermination des critères et des échelles relatifs
  - Analyse des événements redoutés et des scénarios de menaces
  - Analyse et qualification des risques
  - Évaluation des mesures en place et réduction des risques