Question 1. (50%)

La banque **BADABING** fait affaire au Canada depuis 1982. Son siège social se trouve à Montréal (Figure 1). Elle est établie dans 15 villes canadiennes. Dans chacune de ces villes, elle possède 10 succursales et elle exploite 30 guichets automatiques. Un réseau à haut débit relie toutes les succursales du pays entre elles. Le réseau dessert également les transactions effectuées à travers les guichets automatiques. Les réseaux des succursales sont câblés et sans-fil.

Figure 1. Répartition des succursales, des guichets automatiques et du siège social de la banque BADABING.

Elle développe actuellement un nouveau système réparti pour supporter ses transactions bancaires à travers ses succursales et ses guichets automatiques au Canada, ainsi que pour les services de base (DNS, DHCP, courriel, web, …). Les ingénieurs qu'elle a engagés pour développer le système ont proposé une architecture répartie (Figure 2).

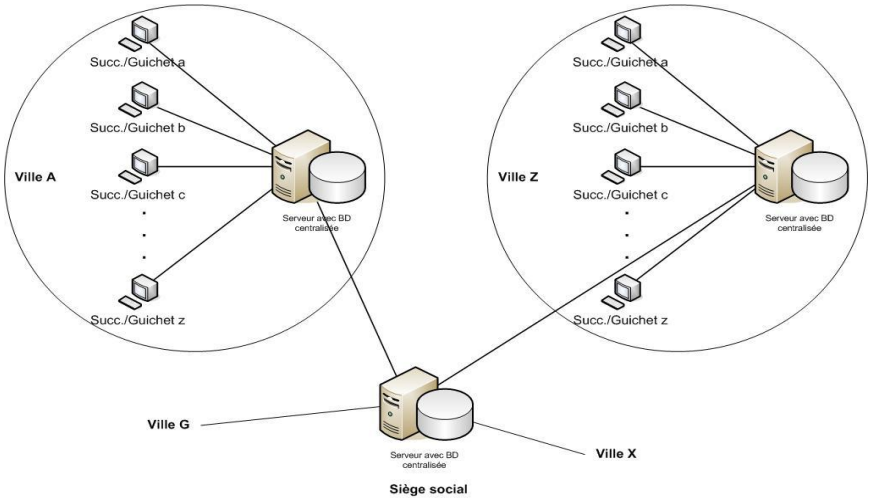

Figure 2. **Architecture client-serveur où chaque ville possède son propre serveur et sa base de données. Les données locales sont mises à jour au serveur du siège social. Les réseaux des succursales sont câblés et sans-fil.**

L'architecture pour l'application 3-tiers de transactions bancaires est montrée dans la figure 3.

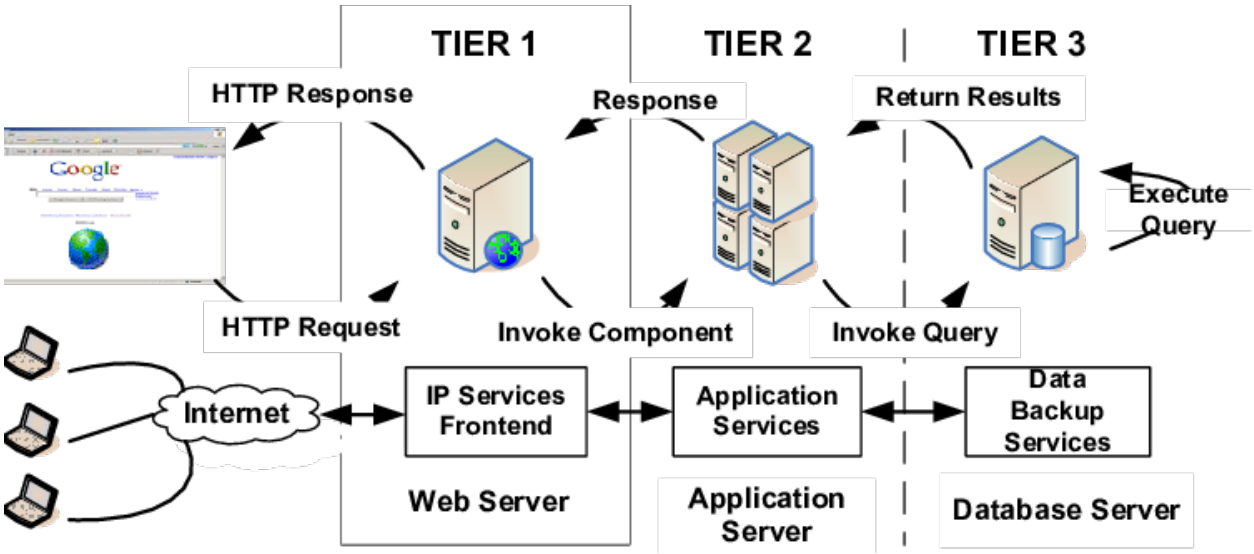

Figure 3 : Architecture de l'application de transactions bancaires.

Sachant que vous êtes des ingénieurs avisés en sécurité, **BADABING** voudrait avoir votre avis sur certaines questions qu'elle se pose à propos de la sécurité du système réparti.

Vous devez proposer une architecture réseau avec sécurité détaillée pour **chaque succursale ainsi que pour le système réparti (pour les transactions bancaires et les services de base)** en tenant compte de l'approche défense en profondeur et des éléments de sécurité suivants :

- L'architecture réseau des villes et du siège social sont 3-tiers,
- Définition des zones de sécurité,
- dispositifs de contrôle d'accès,
- mécanismes d'authentification,
- NAT,
- « Virtual private network » VPN,
- fiabilité,
- mobilité des utilisateurs,
- système de détection d'intrusion IDS ('Intrusion Detection System'),
- mécanisme d'authentification,
- pare-feu (`firewall'),
- mécanismes de protection WiFi,
- utilisation de SSL,
- chaque ville possède une connexion à Internet,
- les succursales ont des réseaux sans-fils,
- au moins une ville permet aux employés d'utiliser leurs dispositifs pour se connecter au réseau (BYOD : 'bring your own device')

EXPLIQUEZ ET JUSTIFIEZ CLAIREMENT CHAQUE CHOIX QUE VOUS FAITES. Il faut ajouter la figure de l'architecture d'une succursale, du siège social ainsi que l'interconnexion entre les villes et le siège social.

Question 2. (50%)

Articles:

[1] Decentralized Self-Enforcing Trust Management System for Social Internet of Things. Muhammad Ajmal Azad, Samiran Bag, Feng Hao,and Andrii Shalaginov, , IEEE Internet Of Things Journal, Vol. 7, No. 4, April 2020.

[2] On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things, Lijun Wei, Jing Wu, Chengnian, IEEE Internet Of Things Journal, Vol. 8, No. 6, March 15, 2021.

[3] A Comprehensive Study on the Trust Management Techniques in the Internet
of Things. Behrouz Pourghebleh, Karzan Wakil, and Nima Jafari Navimipour,
IEEE Internet Of Things Journal, Vol. 6, No. 6, December 2019

1. Les articles [1] (Decentralized Self-Enforcing Trust Management System for Social Internet of Things) et [2] (On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things) présentent deux modèles de confiance (‘trust’) pour SIoT (‘social internet of things’ ou réseau social pour internet des objets).

a. De votre point de vue, lequel de ces deux modèles est le meilleur ? Vous devez justifier clairement votre réponse. Pour le faire, vous devez définir les critères qui pour vous sont importants et ensuite comparer ces deux modèles. **(15%) (Maximum 1 page)**

b. Imaginez qu’on veut développer un SIoT pour les véhicules. Dans ce réseau social, les véhicules vont pouvoir se communiquer entre eux, sans l'intervention des personnes, pour partager l'information sur l’état des routes, du trafic, de la météo, de l'expérience de conduite, etc. Lequel de ces deux modèles est plus adapté selon vous? Justifiez clairement votre réponse en montrant pourquoi le modèle que vous avez choisi s’adapte mieux. **(15%) (Maximum 1 page)**

2. L’article [A Comprehensive Study on the Trust Management Techniques in the Internet of Things] présente un aperçu des différentes techniques/modèles pour la gestion de la confiance dans l’Internet des objets (‘IoT’). Dans la section III-D (page 9328), l’article présente quelques critères qui sont utilisés pour la gestion de la confiance. Est-ce que les modèles de confiance présentés dans les articles [On Designing Context-Aware Trust Model and Service Delegation for Social Internet of Things] et [A Comprehensive Study on the Trust Management Techniques in the Internet of Things] répondent à ces critères ? Justifiez clairement votre réponse. **(20%) (Maximum 2 pages)**