Réponse 1 : **AUTOMNE 2021**

Selon les informations fournies dans l'énoncé, l'architecture mise en place est une architecture HUB and SPOKE. Dans cette configuration, le hub (le siège social) est connecté aux différentes villes via des liaisons câblées ou sans fil. Chaque ville dispose, en plus de cette liaison avec le hub, d'une connexion à Internet et d'autres liaisons vers ses succursales. Voici un aperçu de l'architecture du siège social et de ses liaisons avec les différentes villes, en respectant les spécifications suivantes :

- Le siège, qui représente le point central de l'architecture, doit avoir une connexion redondante vers Internet en utilisant deux fournisseurs d'accès (ISP) différentes et deux technologies d'accès distinctes. Par exemple, on peut envisager une connexion principale en fibre optique et une connexion de secours via faisceaux hertziens ou LTE/5G.

- Comme mentionné dans l'énoncé, le siège repose sur une architecture trois tiers. On distingue dans le diagramme les trois couches suivantes : Accès, Distribution et Cœur.
Un pare-feu combiné à un IPS est nécessaire pour sécuriser les services présents dans la DMZ.

- La zone DMZ inclut : un serveur Web, un serveur mail, une solution Email Security pour se prémunir des attaques sur le serveur mail, un serveur DNS et DHCP, ainsi qu'un serveur d'authentification lié à l'application Web (transactions bancaires).

- L'application Web, de son côté, suit une architecture trois tiers. Afin d'assurer un niveau de sécurité renforcé, un second pare-feu est ajouté entre le serveur Web et le serveur d'application. Un Web Security Appliance a également été intégré pour bloquer les connexions malveillantes.

- Une autre couche de sécurité (pare-feu et IPS) est mise en place pour protéger le réseau interne de la banque en cas de compromission du serveur d'application.
Le réseau interne du siège est divisé en trois blocs :
= WAN : Une liaison VPN site-to-site est configurée pour relier chaque ville au siège. Un pare-feu est obligatoire à l'entrée du siège et à la sortie de chaque ville. Le VPN est placé en dehors du pare-feu pour faciliter son inspection (trafic non crypté).
= Data Center : Cette partie est particulièrement sensible, d'où l'ajout d'un pare-feu et IPS supplémentaire pour se prémunir des attaques internes. Cette section comprend plusieurs serveurs, notamment : le serveur d'authentification couplé à Active Directory, le serveur de base de données, le serveur de fichiers et des outils de surveillance.
= Campus : Ce segment constitue le réseau d'accès de la banque. Il englobe les installations réseau situées dans les différents sites du siège (commutateurs, points d'accès, etc.), un NAC pour l'application des politiques de sécurité, un contrôleur Wi-Fi et une solution Web Security pour filtrer les sites malveillants.

- Pour répondre aux besoins BYOD de la banque, la solution Cisco ISE a été mise en place. Elle permet de contrôler les appareils des utilisateurs, de vérifier leur conformité avec les politiques de sécurité, et d'appliquer des décisions adaptées pour protéger le réseau. Par exemple, si un utilisateur utilise un laptop non mis à jour sans antivirus, Cisco ISE peut isoler cet appareil dans un VLAN restreint, avec un accès limité (par exemple, uniquement à Internet).

- Pour garantir une haute disponibilité et une tolérance aux pannes, tous les éléments du réseau sont redondants. Cette redondance est illustrée dans le diagramme au niveau des liaisons et des commutateurs modulaires, bien que certains SPOF (Single Point of Failure) aient été conservés pour simplifier l'architecture. Pour maximiser l'utilisation des ressources, des technologies telles que l'agrégation de liens (EtherChannel), le protocole HSRP et le protocole Spanning Tree (STP) sont indispensables.

- Dans la section Campus, la solution NAT doit être appliquée avec un adressage privé approprié, et des protocoles réseau sécurisés comme OSPF pour le routage, des VLANs sectorisés (VLAN WIFI, VLAN MANAGEMENT, etc.) pour limiter les domaines de broadcast, NTP pour la synchronisation horaire, et SNMP pour la supervision.

- Enfin, l'utilisation de HTTPS/TLS est obligatoire sur le serveur Web, tandis que le protocole SSH doit être employé pour la gestion à distance des équipements réseau.

Architecture des villes et succursales

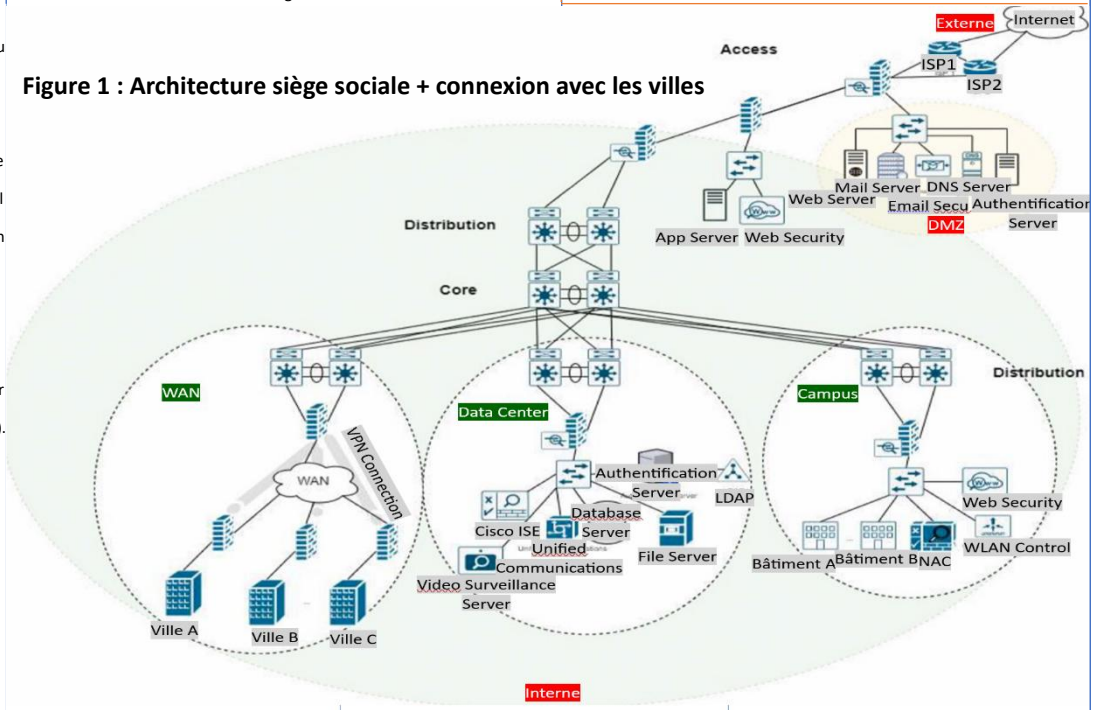
D'après l'énoncé, chaque ville comprend plusieurs succursales, dispose d'une connexion Internet et possède un serveur avec base de données centralisée. Le diagramme ci-dessous illustre cette architecture avec une succursale unique. Les principes et choix techniques énoncés pour le siège s'appliquent également ici, avec des ajustements mineurs concernant les équipements déployés (serveurs, connexions entre villes et succursales, etc.).

Question 1 : **AUTOMNE 2021**
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.
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 1 Quels sont les types d'attaques d'ingénierie sociale ?
i. Social, Physique, Technique, Sociotechnique ✓
ii. E-mail, cloud, website, physique
iii. Logiciel, humain, VoIP, message
iv. Social, technique, website, humain
Question 2 Parmi les attaques suivantes lequel est un type d'attaque de 'DNS spoofing'?
a. Réinstallation d'une clé chez le serveur DNS
b. Une attaque de déni de service sur le serveur DNS
c. Attaque sur la réponse du serveur DNS vers le client ✓
d. Attaque KRACK sur le réseau wifi
Question 3 : Avec quel algorithme Flask encode les données des cookies ?
a. Base64 ✓
b. AES
c. MD5
d. sha-256
Question 4 Lors d'une attaque de déni de service du type 'SYN flood', quel protocole est-on en train d'utiliser pour réaliser l'attaque ?
a. TCP ✓
b. IP
c. UDP
d. HTTP
Question 5 La résilience d'un réseau informatique est liée aux suivants concepts :
a. Contrôle d'accès, authentification
b. Disponibilité, fiabilité, sûreté ✓
c. Pare-feu, routeur
d. Protocoles réseau
Question 6 Quelle est la définition qui s'ajuste plus à la fiabilité d'un réseau
a. Un événement (ou une série d'événements) non planifiés qui peut entraîner des conséquences
b. La mesure dans laquelle un système est en état de rendre son service (état opérationnel) ✓
c. La probabilité que les conditions qui peuvent causer des accidents ne surviennent pas
d. La probabilité pour qu'un système soit continûment en fonctionnement non catastrophique sur une période donnée

Figure 1 : Architecture siège sociale + connexion avec les villes



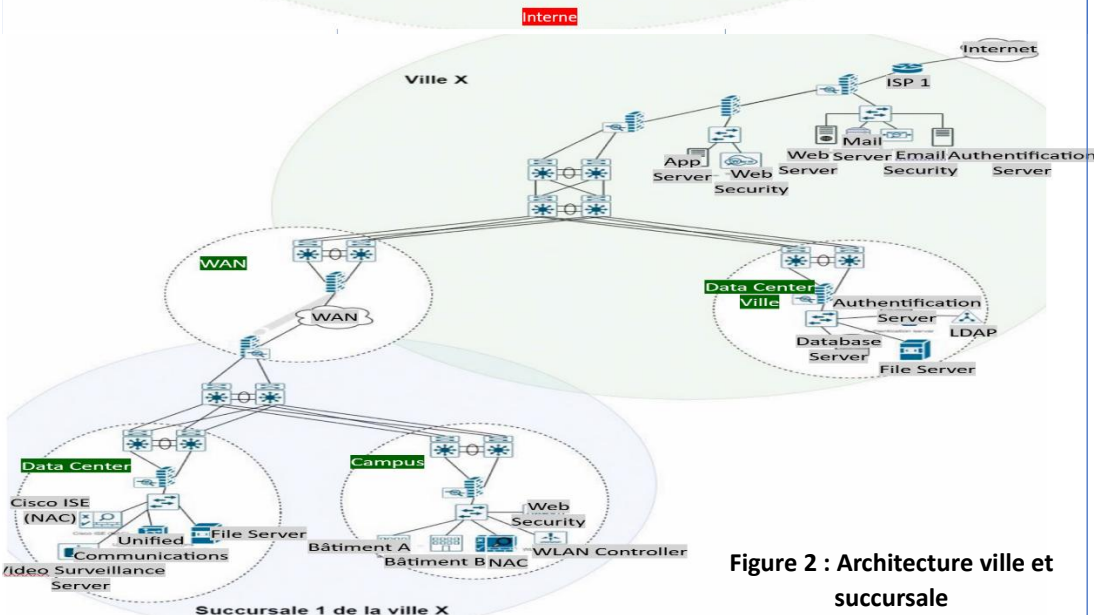
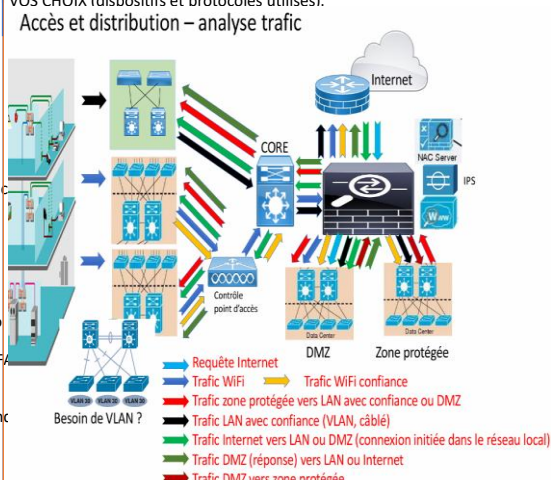


Figure 2 : Architecture ville et succursale

1. WPA2 Wi-Fi Password Cracking
Vulnerability: Weaknesses in WPA2 encryption allow password interception through a four-way handshake.
Method: Monitor mode → Capture handshake → Force reconnection → Crack using wordlists. Tools: airmon-ng, airodump-ng, aircrack-ng.
Key Takeaway: Migrating to WPA3 and using strong, complex passwords significantly reduces this risk.
2. SQL Injection Exploit Vulnerability: Exploitation of poorly validated user input allows access or disruption of databases.
Impact: Unauthorized access to data, admin privileges, and system control. Defense: Prepared statements, input validation, and regular security audits. Key Takeaway: SQL injection can cripple databases; proactive protections like input filtering are crucial.
3. ProxyLogon (CVE-2021-26855) Vulnerability: Microsoft Exchange allows unauthenticated remote access via SSRF.
Method: Exploit vulnerability to gain access, combine with other CVEs for chain attacks. Impact: Data theft, Web Shell deployment, complete server compromise. Defense: Immediate patching of Exchange servers and proactive monitoring. Key Takeaway: Rapid patching of critical vulnerabilities is vital to avoid catastrophic breaches.
4. CUPS Print Service Exploit Vulnerability: Command injection via PPD files exploiting cupsFilter2. Method: Fake printer setup → Inject payload → Execute commands on user attempts to print.
Impact: Remote Code Execution (RCE) and privilege escalation. Defense: Update cups to patched versions, disable unused services, secure network print services.
Key Takeaway: Network printers are often overlooked and can be exploited for critical system breaches5. Phishing with GoPhish
Method: Use tools like GoPhish and OSINT to craft convincing phishing campaigns.Impact: Stolen credentials, identity theft, and access to sensitive company resources.Defense: User awareness training, email filtering, and verification of sender addresses/URLs.Key Takeaway: Effective phishing simulations demonstrate the need for improved user awareness and security configurations.
5. Starvation and SpoofingVulnerabilities: Lack of DHCP protections allows denial of service (DoS) and man-in-the-middle (MITM) attacks.
Method: Exhaust IP addresses (Starvation) or set rogue DHCP server (Spoofing).Defense: Enable DHCP Snooping, trust ports, and segment networks with VLANs.Key Takeaway: DHCP services are critical but vulnerable; protections like Snooping and segmentation are essential.
6. MicrosE (CVE-2024-21413)
Vulnerability: Exploit hyperlinked resources to execute remote code via NTLM authentication.Method: Malicious email with file:// links → SMB protocol → Steal NTLMv2 hashes.Impact: Compromise Windows accounts, system access, and potential ransomware.Defense: Regular updates, disable auto-hyperlink execution, and limit user privileges.Key Takeaway: User awareness and software updates are key to mitigating modern phishing-based RCE attacks.
7. Password Cracking
Vulnerability: Weak passwords and insecure systems that rely on hashed credentials (NTLMv2) which can be exploited.
Method: Capture NTLMv2 hash using tools like Responder → Crack hashes via dictionaries (hashcat with rockyou.txt).
Impact: Credential theft and remote access (via xfreerdp).
Defense: Use strong passwords, avoid NTLM, and monitor SMB traffic for anomalies.Key Takeaway: Weak passwords are easily cracked; strong authentication policies and monitoring are critical.
8. Vulnerability in Evilginx Phishing (AiTM)
Vulnerability: Evilginx is a tool that facilitates advanced phishing attacks by bypassing MFA via session cookie interception.
Method: Setup a phishing site using Evilginx → Send phishing link to target → Capture victim's cookies and session tokens → Use them to bypass MFA.Impact: Identity theft, access to sensitive company information, and possible ransomware deployment.Defense: Use MFA with hardware tokens, awareness training, and ensure users verify links manually. Key Takeaway: Awareness and proper security configurations, including strong MFA methods, are essential to defend against sophisticated phishing attacks like Evilginx.

Question 1 : **AUTOMNE 2022**
L'entreprise LA MODE fait affaire au Canada depuis l'année 2000. Son siège social se trouve à Montréal où se trouve le centre des données globales de la compagnie. Elle est établie dans 15 villes canadiennes. Dans chacune de ces villes, elle possède 10 succursales. La communication entre les succursales et le siège social se fait à travers Internet. Également, l'entreprise effectue des ventes en ligne. L'infrastructure informatique de toutes les succursales est identique (Figure 1). Les réseaux physiques des succursales sont sans fil.
Depuis la COVID, 50% des employés travaillent de la maison.
Les ingénieurs qu'elle a engagés pour développer le système ont proposé une architecture répartie basée sur le modèle client/serveur.
Dans cette architecture, chaque succursale possède son propre serveur, cependant la base de données est centralisée et elle est localisée au centre de données du siège social.
L'architecture pour l'application, 3-tiers, de transactions en ligne est schématisée dans la figure 2. L'architecture de cette application est basée sur les notions de client/serveur (C/S).
Sachant que vous êtes des ingénieurs avisés en sécurité, LA MODE 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 détaillée qui tient compte de la sécurité pour chaque succursale, pour le siège social, le centre de données du siège social, pour la communication des travailleurs à distance, ainsi que pour le système réparti (pour les transactions en ligne) 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.
• Redondance.
• Système de détection d'intrusion IDS ('Intrusion Detection System').
• Mécanisme d'authentification.
• Pare-feu (`firewall').
• Mécanismes de protection WiFi.
• Chaque succursale possède une connexion à Internet.
• Les succursales ont des réseaux sans fil.
• Les succursales permettent aux employés d'utiliser leurs dispositifs pour se connecter au réseau (BYOD : 'bring your own device').
• Montrer un schème avec l'analyse du trafic.
VOUS DEVEZ JUSTIFIER CLAIREMENT VOTRE ARCHITECTURE PROPOSÉE ET VOS CHOIX (dispositifs et protocoles utilisés).



Reponse 1 : **AUTOMNE 2022**
Dans l'ensemble, l'entreprise communique via Internet avec ses différentes succursales, ses employés en télétravail, ainsi que des réseaux de partenaires, comme ceux utilisés pour les processus de paiement.

Pour sécuriser les communications entre le siège social et les succursales, il est essentiel d'installer des dispositifs de sécurité à chaque point d'accès à Internet. Cela inclut notamment un pare-feu externe et un système IDS/IPS.

Concernant les échanges entre le siège social, les employés distants et les partenaires, il est recommandé de chiffrer les communications, par exemple en utilisant un VPN. Par ailleurs, pour renforcer la sécurité des réseaux internes au sein de l'infrastructure, l'usage de NATs est conseillé, surtout dans le cas des réseaux sans fil des succursales.

Les succursales devront accéder à la base de données située au siège, car elles ne disposent pas d'une copie locale. Pour garantir la sécurité de cette communication, il est primordial de chiffrer les échanges de données.

Pour l'implémentation de l'architecture logicielle en trois tiers de l'application, des réseaux locaux virtuels (VLAN) seront mis en place et protégés à l'aide de pare-feu virtuels.

Afin d'assurer la mobilité des utilisateurs, un réseau de points d'accès (routeurs) sera déployé à travers les bâtiments de l'entreprise, incluant le siège et les succursales. Quant aux utilisateurs distants, ils pourront accéder aux services de l'entreprise soit via le siège, soit via les succursales. Cela permettra de réduire les délais liés à de potentiels sauts de nœuds réseaux, en particulier si le siège est éloigné de l'utilisateur.

Enfin, pour garantir la résilience du réseau, l'infrastructure intègre une duplication des composants critiques.

Le schéma ci-dessous illustre l'architecture proposée pour l'entreprise LA MODE, en intégrant les dispositifs nécessaires à la sécurisation des communications.
- Firewall entre DMZ et inside : DMZ est accessible depuis l'extérieur donc on ne peut pas être sûr que les requêtes provenant de cette zone ne sont pas malveillantes.
- Firewall entre BD et app : données de la banque sont sensibles donc il faut les protéger au maximum. On peut mettre par exemple comme règle de n'accepter que des les requêtes provenant des serveurs internes (App)
- Lier le LAN au firewall aussi pour sécuriser car il est possible d'avoir des attaques du réseau intérieur.
- Pas de NAT pour DMZ car ça doit être visible de l'extérieur. Mais NAT pour inside et d'autres modules comme le LAN.
- VPN : s'arrête au firewall à l'entrée pour que le firewall puisse analyser les paquets ; mettre VPN sur les communications entre villes et siège social
- IPS après firewall pour éviter les faux positifs
succursales : pas de dmz etc et communique en réseau privé avec les couches core et distribution