Pour garantir une disponibilité élevée et une tolérance aux erreurs, il est important que tous les éléments de l'architecture réseau soient redondants. Le diagramme ci-dessous montre cette redondance au niveau des liens et des commutateurs modulaires, mais il reste quelques SPOF (Single Point Of Failure) qui ont été conservés afin de simplifier l'architecture. Cela signifie que, même si certaines parties de l'architecture ne sont pas redondantes, elles ont été maintenues afin de rendre l'ensemble de l'architecture plus facile à comprendre.

Pour tirer parti de toutes les ressources disponibles dans un réseau redondant, il est recommandé d'utiliser des technologies comme l'agrégation de liens (Etherchannel), le protocole de redondance HSRP et le protocole Spanning Tree (STP). Ces technologies permettent de garantir la disponibilité et la tolérance aux erreurs dans le réseau en s'assurant que les différentes parties du réseau peuvent travailler de manière transparente et efficace.

Selon les informations fournies dans l'énoncé, l'architecture décrite est une architecture en forme de HUB et de rayons, dans laquelle le centre de l'architecture (le HUB) est le siège social qui est connecté aux différentes villes par des liens câblés ou sans fil. Chaque ville dispose également d'une connexion Internet et de connexions vers d'autres succursales en plus de sa liaison avec le HUB. Voici l'architecture du siège social et ses liens avec les différentes villes, avec les spécifications suivantes :

- Le siège a une architecture en trois couches, qui peuvent être distinguées sur le diagramme : la couche d'accès, la couche de distribution et la couche de cœur.
- Le siège qui est le point central de l'architecture doit avoir une connexion redondante vers Internet à travers deux ISP différents de 2 fournisseurs d'accès Internet, si le premier tombe en panne le second prendra la relève le temps pour l'administrateur de le réparer
- On a installé un Pare-feu et un VPN qui permettent l'interconnexion des sites distants avec le siège. Ce type de pare-feu et de VPN sont de type "site à site", ce qui signifie qu'elles sont transparentes pour les utilisateurs, elles utilisent le protocole IPsec et SSH pour chiffrer les données qui traversent le tunnel de connexion.
- Ensuite on a mis en place le IDS et le ASA pour protéger les réseaux et les systèmes contre les menaces de sécurité en fournissant une alerte en temps réel lorsqu'une activité anormale est détectée.
- Puis après Email security Appliance (ESA) pour filtrer les messages entrants et sortants pour éviter les menaces de messagerie électronique et pour la prévention des pertes de données (DLP) et la gestion de la conformité réglementaire.

Pour la couche coeur qui gère le transport de données à travers le réseau :

- On a installé un NAC qui vas devoir vérifier que les utilisateurs et les appareils qui tentent de se connecter au réseau respectent les politiques de sécurité définies par l'administrateur du réseau.
- Par la suite on a installé WLC contrôle qui va venir gérer et contrôler un réseau sans fil local (WLAN, pour Wireless Local Area Network) en centralisant la gestion des points d'accès sans fil (AP, pour Access Point).
- Ensuite on a installé WSA (Web Security Appliance) de Cisco qui est une application de sécurité Web qui permet de protéger les réseaux contre les menaces en ligne telles que les sites Web malveillants, les logiciels espions et les virus, c'est une solution de sécurité en ligne qui peut être installée en tant que périphérique de réseau ou en tant que logiciel sur un serveur.
- On a aussi mis en place Le Cisco ACS pour authentifier les utilisateurs qui tentent de se connecter au réseau, en utilisant des protocoles tels que RADIUS (Remote Authentication Dial-In User Service) ou TACACS+ (Terminal Access Controller Access Control System Plus), ainsi pour vérifier que les appareils qui tentent de se connecter au réseau respectent les exigences de sécurité définies par l'administrateur du réseau.
- Et pour répondre au besoin de la banque en termes de BYOD, on a décidé d'implémenter la solution cisco ACS qui va nous permettre de contrôler les appareils des utilisateurs, vérifier leurs conformités aux politiques de sécurité appliquées et prendre les décision adéquates pour protéger le réseau. Par exemple, pour un client qui utilise son propre laptop qui n'a pas été mise à jour et qui n'a aucun antivirus installé, Cisco ACS ou ISE peut mettre cet utilisateur dans un VLAN isolé et lui donner un accès restreint aux ressources de l'entreprise (accès Internet seulement par exemple).

Pour la Zone Protégée qui est une zone d'un réseau informatique protégée par des mesures de sécurité pour empêcher l'accès non autorisé ou non sécurisé, elle peut être utilisée pour protéger des données sensibles ou pour séparer différentes parties d'un réseau afin de gérer de manière plus efficace l'accès et l'utilisation de ses ressources, et c'est la partie de l'architecture la plus sensible, c'est pour cette raison qu'on a ajouté :

- On a dupliqué la distribution layer pour la redondance et la disponibilité en cas de panne
- Par la suite on a mis en place Cisco VSM afin de fournir une interface centralisée pour la gestion et la visualisation des images de vidéosurveillance capturées par les caméras de surveillance de l'entreprise.
- Puis après Cisco Unified Communication Manager qui permet de gérer et de contrôler les communications vocales, vidéo et de données dans les entreprises et les organisations de toutes tailles.
- On suite on a dupliquer la base de donner et serveur d'application si un des deux tombe en pagne l'autre le remplace

Pour la zone DMZ qui est une zone d'un réseau séparée du reste du réseau qui permet d'accueillir des serveurs et des services accessibles depuis Internet :

- On a mis en place le NTP qui permet de synchroniser l'heure sur les ordinateurs d'un réseau en se basant sur un serveur de temps de référence pour les transactions de change et d'autre
- Puis le serveur Web, le serveur mail, Email Security pour la protection contre les attaques liées au serveur mail, le serveur DNS, DHCP et un serveur d'authentification lié à l'application Web (transaction bancaire).
- Par la suite on a dupliqué la distribution layer pour la redondance et la disponibilité en cas de panne car c'est la place le plus visiter dans la compagnie

Pour la Zone Mobilité ou télétravail là ou les utilisateurs mobiles devront utiliser un VPN (joue un rôle important pour les travailleurs à distance, car il permet de sécuriser les connexions à distance à un réseau privé, lorsqu'un utilisateur se connecte à un réseau privé via un VPN, toutes les données qu'il envoie et reçoit sont cryptées, ce qui les protège contre les interceptions et les cyberattaques) accès distant comme cisco annyconnect pour se connecter au cœur du reseau après s'être authentifiés :

- On a mis en place un NAT qui va permettre à plusieurs appareils de partager une connexion Internet unique. NAT permet de masquer l'adresse IP privée de l'appareil derrière une adresse IP publique, ce qui permet d'économiser des adresses IP publiques.

- Puis un WAN : qui va permettre de connecter des appareils et des ordinateurs situés dans différentes régions géographiques, voire dans des pays différents, le terme "WAN" fait référence à la couverture géographique étendue du réseau, qui peut couvrir de vastes distances et inclure de nombreux sites distants.

- Par la suite une liaison VPN site to site sera déployé pour connecter chaque ville au siège.

- Un pare-feu est obligatoire à l'entrée du siège et à chaque sortie d'une ville. Le VPN est limité à l'extérieur du pare-feu pour rendre l'inspection de ce dernier plus facile (trafic non crypté)

La zone site : C'est le réseau d'accès de la banque, Il regroupe les différentes installations réseaux dans les différents sites du siège (commutateurs, points d'accès ...) ainsi qu'un NAC pour l'application de la politique de sécurité, un contrôleur WIFI et un Web Security pour filtrer les sites web malveillants.

Dans la partie site du réseau, Il est important de mettre en place une solution de traduction d'adresses réseau (NAT) avec un adressage privé adéquat et de sécuriser les protocoles réseaux en utilisant, par exemple, OSPF pour le routage, des VLANs par secteur et par technologie (VLAN WIFI, VLAN MANAGEMENT, etc.) pour limiter les domaines de diffusion, NTP pour la synchronisation de l'heure, et SNMP pour la supervision. De plus, Il est nécessaire d'utiliser HTTPS/TLS pour le serveur Web et SSH pour la gestion à distance des équipements réseau. Ces mesures permettent de renforcer la sécurité du réseau et de garantir une bonne performance.