Mise en œuvre d'un système de réseau d'entreprise sécurisé

Cahier de charges du projet

@Tech Innovation Ltd est une entreprise dynamique et avant-gardiste spécialisée dans la fourniture de solutions cloud innovantes à des clients du monde entier. S'appuyant sur une technologie de pointe et une équipe de professionnels hautement qualifiés, Cytonn Innovation se concentre sur le développement et la mise en œuvre de solutions basées sur le cloud adaptées pour répondre aux besoins changeants des entreprises de divers secteurs. En mettant fortement l'accent sur la créativité, l'agilité et l'orientation client, @Tech Innovation vise à permettre aux organisations d'améliorer leur efficacité opérationnelle, leur évolutivité et leur compétitivité dans le paysage numérique actuel.

Avec un effectif de 600 personnes, @Tech Innovation Ltd s'est récemment agrandie et se prépare à déménager dans un nouveau bâtiment. Le nouveau bâtiment, composé de trois étages, abritera divers départements, notamment les ventes et le marketing, les ressources humaines et la logistique, les finances et la comptabilité, l'administration et les relations publiques, les TIC et une salle de serveurs. Le département TIC accueille en outre des développeurs de logiciels, des ingénieurs cloud, des ingénieurs en cybersécurité, des ingénieurs réseau, des administrateurs système, des spécialistes du support informatique, des analystes commerciaux et des chefs de projet.

Avant le déménagement, un nouveau service réseau doit être conçu et mis en œuvre dans le nouveau bâtiment. Pour garantir une sécurité robuste, @Tech Innovation mettra en œuvre plusieurs mesures de sécurité pour protéger le réseau des menaces internes et externes. Le pare-feu comportera des zones de sécurité extérieures, intérieures et DMZ, avec des serveurs essentiels stratégiquement hébergés dans la zone fortifiée. De plus, les serveurs Active Directory (AD), responsables de la gestion et de l'authentification des utilisateurs, des ordinateurs et des ressources du réseau interne, seront placés dans la zone intérieure du pare-feu. Cela implique que les serveurs tels que DHCP, DNS et Radius seront tous placés dans la zone interne du pare-feu ,tandis que d'autres serveurs tels que le stockage FTP, WEB, Email, APP et NAS seront situés dans la DMZ - la zone peut être attachée à n'importe quel pare-feu dès maintenant. Cette planification méticuleuse et le déploiement de mesures de sécurité protégeront le réseau et garantiront le bon fonctionnement de @Tech Innovation Ltd dans son nouveau bâtiment.

Au cœur de l'infrastructure technologique se trouve le campus principal, qui héberge une ferme de serveurs, souvent appelée zone démilitarisée (DMZ). Au sein de cette zone fortifiée, les serveurs essentiels tels que DHCP, DNS, FTP, WEB, Email et SMTP sont stratégiquement hébergés. Reconnaissant l'importance d'un accès sécurisé aux ressources, les utilisateurs des succursales sont

dotés de la capacité de se connecter et d'utiliser en toute sécurité ces serveurs centralisés. Cette connectivité sécurisée garantit que les ressources éducatives, informationnelles et de communication sont facilement accessibles à tous les utilisateurs, quel que soit leur emplacement physique.

En tant que partie intégrante de l'infrastructure TIC de l'Université, les éléments suivants ont été intégrés :

- Fournisseur de services Internet (FAI) : La Société a établi un abonnement auprès de deux FAI (Free et SFR) pour assurer une connectivité Internet redondante.
- Sécurité du réseau : deux pare-feu Cisco ASA de la série 5500-X ont été acquis pour améliorer la sécurité et la redondance du réseau.
- Routage réseau : les pares-feux et les commutateurs principaux seront utilisés à la place d'un routeur.
- Infrastructure de commutation : le réseau comprend deux commutateurs Catalyst 3850 à 48 ports pour chaque campus et des commutateurs Catalyst 2960 à 48 ports pour garantir une connectivité réseau locale robuste.
- Matériel du serveur et virtualisation : deux serveurs physiques seront utilisés pour la virtualisation via l'hyperviseur afin d'obtenir plusieurs machines virtuelles pour divers services. Pour la redondance ou le basculement, nous aurons deux serveurs DHCP fonctionnant en même temps.
- Infrastructure sans fil : deux contrôleurs LAN sans fil Cisco (WLC) et divers points d'accès légers (LAP) centraliseront la gestion du réseau sans fil.
- Téléphones VOIP ou IP : une passerelle vocale Cisco sera utilisée pour activer le service de téléphonie sur le réseau.

Le CLOUD COMPUTING, en tant que technologie importante, est utilisé pour connecter les clients du monde entier aux services et ressources de l'entreprise. Le réseau proposé devrait donc permettre à l'équipe d'accéder à ces ressources.

Par conséquent, en tant que membre clé de l'équipe Réseaux, vous avez été chargé de concevoir un réseau pour le nouveau bâtiment. À ce stade, une conception logique est requise, qui montre les mesures que vous mettriez en place pour garantir que le nouveau réseau réponde aux besoins commerciaux actuels et soit évolutif.
L'entreprise met fortement l'accent sur l'obtention de performances, de redondance, d'évolutivité et de disponibilité de premier ordre au sein de son infrastructure réseau. En tant que tel, votre tâche consiste à créer une conception de réseau complète et à exécuter sa mise en œuvre. Pour faciliter cet effort, la Société a désigné des plages d'adresses IP spécifiques :

- **Réseau de gestion : Pour la gestion, la plage d'adresses IP de 192.168.10.0/24 a été allouée.**
- **WLAN : le réseau WLAN fonctionnera dans la plage d'adresses IP de 10.20.0.0/16.**
- **LAN : pour le réseau local (LAN), la plage d'adresses IP de 172.16.0.0/16.**
- **VOIP : pour le réseau local (LAN), la plage d'adresses IP de 172.30.0.0/16.**
- **DMZ : la zone démilitarisée (DMZ) se verra attribuer des adresses IP comprises dans la plage 10.11.11.0/27.**
- **Adresses publiques : adresses IP publiques de la plage 105.100.50.0/30 de Free et 197.200.100.0/30 de SFR**

Technologies mises en œuvre

1) **Outil de conception : utilisez Cisco PACKET TRACER pour concevoir et mettre en œuvre la solution réseau. Conception hiérarchique : mettez en œuvre un modèle**
2) **Hiérarchique qui intègre la redondance pour une résilience améliorée du réseau.**
3) **. FAI : établissez la connectivité à un routeur FAI Airtel au sein de l'infrastructure réseau.**
4) **WLC : assurez-vous que chaque service est équipé d'un point d'accès sans fil (WAP) pour fournir un accès Wi-Fi aux employés, aux utilisateurs de l'entreprise, aux auditeurs externes et aux invités, le tout géré de manière centralisée par un contrôleur LAN sans fil (WLC).**
5) **VOIP : déployez des téléphones IP dans chaque service pour prendre en charge la communication voix sur IP (VOIP).**
6) **VLAN : gérez les VLAN avec les ID suivants : 10 pour la gestion, 20 pour le LAN, 50 pour le WLAN, 70 pour la VOIP et enfin 199 pour Garage dans lequel sont placés tous les ports inutilisés.**
7) **ETHERCHANNEL : implémentez le protocole LACP (Link Agrégation Control Protocol) pour la configuration ETHERCHANNEL, améliorant ainsi l'efficacité de l'agrégation de liens.**
8) **STP PORTFAST et BPDUGUARD : configurez PORTFAST et BPDUGUARD du protocole SPANNING TREE (STP) pour accélérer les transitions de port de l'état de blocage à l'état de transfert.**
9) **Sous-réseau : utilisez des techniques de sous-réseau pour attribuer le nombre approprié d'adresses IP à chaque groupe de réseau.**
10) **Paramètres de base : configurez les paramètres fondamentaux de l'appareil, notamment les noms d'hôte et les mots de passe de la console, activez les mots de passe, les messages de bannière, le cryptage des mots de passe et désactivez la recherche de domaine IP.**
11) **Routage inter-VLAN : permettez aux appareils de tous les services de communiquer entre eux en configurant le commutateur multicouche respectif pour le routage inter-VLAN.**
12) **Core Switch : attribuez des adresses IP aux commutateurs multicouches pour activer les fonctionnalités de routage et de commutation.**

13) Serveur DHCP : assurez-vous que tous les appareils du réseau obtiennent des adresses IP de manière dynamique à partir des serveurs situés sur le site de la batterie de serveurs.
14) HSRP : implémentez des protocoles de routeur à haute disponibilité tels que HSRP pour obtenir des capacités de redondance, d'équilibrage de charge et de basculement.
15) Adressage statique : attribuez des adresses IP statiques aux appareils situés dans la salle des serveurs.
16) Protocole de routage : utilisez OSPF (Open SHORTEST Path First) comme protocole de routage pour annoncer les itinéraires sur le pare-feu, les routeurs et les commutateurs multicouches.
17) ACL standard pour SSH : établissez une simple liste de contrôle d'accès (ACL) standard sur la ligne VTY pour autoriser les tâches administratives à distance via SSH uniquement pour le PC de l'ingénieur principal en sécurité réseau.
18) Pare-feu Cisco ASA : configurez les routes statiques par défaut, les paramètres de base, les niveaux de sécurité, les zones et les politiques sur le pare-feu Cisco ASA pour définir le contrôle d'accès et l'utilisation des ressources au sein du réseau.
19) Tests finaux : effectuez des tests approfondis pour vérifier la bonne communication et garantir que tous les éléments configurés fonctionnent comme prévu.