**Compte Rendu Détaille du Projet : Mise en œuvre d'un Système de Réseau d'Entreprise**

**Introduction**

Le projet de mise en œuvre du système de réseau sécurisé pour @Tech Innovation Ltd est un projet majeur visant à garantir l'intégrité, la sécurité, la performance et la résilience du réseau de l'entreprise dans son nouveau bâtiment. Ce projet a pour objectif de répondre aux besoins de connectivité des différentes équipes et départements tout en assurant une gestion efficace des ressources réseau et une sécurité maximale.

L'entreprise, qui se spécialise dans les solutions cloud, opère dans un environnement à la fois dynamique et international, nécessitant des solutions robustes et évolutives pour soutenir son activité. Le réseau conçu a été conçu pour être hautement disponible, sécurisé et facilement extensible pour répondre aux besoins futurs de croissance de l'entreprise.

**Objectifs et Exigences du Projet**

Les principaux objectifs de ce projet étaient :

* Concevoir une infrastructure réseau robuste, sécurisée et évolutive pour le nouveau bâtiment de trois étages.
* Garantir une communication fluide entre les différents départements tout en maintenant un contrôle strict sur l'accès aux ressources sensibles.
* Mettre en place un réseau performant et fiable, capable de supporter des services critiques tels que la téléphonie VOIP, le cloud computing, les applications internes et les ressources partagées.
* Assurer une gestion centralisée du réseau sans fil pour les employés, invités et utilisateurs externes.

**Défis rencontrés :**

* Assurer une sécurité optimale face aux menaces internes et externes tout en maintenant une accessibilité simple et fluide pour les utilisateurs.
* Gérer la redondance des services critiques pour garantir la disponibilité constante des applications essentielles à l'activité de l'entreprise.
* Implémenter des solutions de virtualisation pour améliorer l'efficacité du matériel et réduire les coûts opérationnels.

**Conception du Réseau**

**1. Architecture du Réseau**

La conception du réseau a suivi un modèle hiérarchique classique en trois couches : Accès, Distribution et Cœur. Chaque niveau joue un rôle spécifique dans la gestion du trafic et des services réseau.

**1.1 Couche d'Accès**

La couche d'accès est responsable de la connectivité des utilisateurs finaux et des périphériques réseau (ordinateurs, imprimantes, téléphones IP, etc.). Chaque service et département dispose de son propre VLAN pour isoler le trafic et améliorer la sécurité. La segmentation est réalisée à l’aide de VLANs, afin d’assurer une gestion optimisée du réseau et de prévenir les risques de congestion.

**1.2 Couche de Distribution**

Les commutateurs de distribution gèrent le routage entre les VLANs. Ces commutateurs multicouches permettent la communication entre les différents segments du réseau (par exemple, entre le LAN et le WLAN). Les fonctions de routage sont également intégrées dans cette couche, assurant une gestion efficace du trafic entre les différents sous-réseaux.

**1.3 Couche de Cœur**

Le cœur du réseau est constitué de commutateurs de haute performance qui gèrent l’acheminement du trafic entre les différentes parties du réseau. Ces commutateurs sont configurés pour offrir une redondance élevée grâce à l'utilisation du protocole **HSRP** (Hot Standby Router Protocol), garantissant ainsi une haute disponibilité des services.

**2. Sécurité du Réseau**

**2.1 Pare-feu Cisco ASA 5500-X**

Les pare-feu Cisco ASA 5500-X sont placés en différentes zones du réseau pour sécuriser les accès internes et externes. Le réseau est segmenté en plusieurs zones de sécurité, à savoir :

* **Zone extérieure** : Zone dédiée aux connexions externes, protégée par des règles strictes pour empêcher l'accès non autorisé.
* **Zone interne** : Zone protégée où les ressources sensibles et les serveurs critiques (comme Active Directory, DNS, DHCP, etc.) sont hébergés.
* **Zone DMZ (Démilitarisée)** : Zone où les serveurs accessibles depuis l'extérieur (FTP, Web, Email, etc.) sont hébergés, mais isolée du reste du réseau interne pour réduire les risques en cas d'attaque.

**2.2 VLAN et ACLs**

Les VLANs sont utilisés pour séparer logiquement les différentes sections du réseau et limiter l'accès en fonction des besoins. Par exemple, un VLAN dédié pour la gestion des serveurs est créé, tandis que le VLAN 50 est dédié aux utilisateurs sans fil (WLAN). Les **Listes de Contrôle d'Accès (ACL)** sont appliquées pour restreindre l'accès à certaines ressources sensibles du réseau. Un exemple spécifique est l'ACL standard configurée sur la ligne VTY, permettant l'accès SSH uniquement à partir de l'IP de l'ingénieur principal en sécurité réseau.

**2.3 Portfast et BPDU Guard**

Le protocole **STP (Spanning Tree Protocol)** est utilisé pour éviter les boucles dans le réseau. Cependant, pour améliorer la vitesse de convergence du réseau, **Portfast** et **BPDU Guard** sont activés sur les ports connectés à des périphériques finaux. Cela permet de passer rapidement à l'état de transfert et d'éviter les boucles en cas de problème.

**3. Infrastructures Sans Fil et VOIP**

**3.1 Infrastructure Sans Fil**

Deux **Contrôleurs LAN Sans Fil (WLC)** sont déployés pour gérer l'ensemble des points d'accès sans fil répartis dans les différents départements du bâtiment. Cette gestion centralisée permet de configurer, surveiller et maintenir l'infrastructure sans fil avec une efficacité maximale. Les employés, les invités et les utilisateurs externes peuvent se connecter à un réseau sans fil sécurisé avec des identifiants d'accès appropriés, garantissant ainsi un contrôle rigoureux de l'accès.

**3.2 Téléphonie VOIP**

Des **Téléphones IP** sont déployés dans chaque service pour permettre une communication via **VOIP (Voice over IP)**. Une **Passerelle Vocale Cisco** est utilisée pour garantir la qualité des appels et assurer la connectivité avec les systèmes téléphoniques externes. La solution VOIP permet de réduire les coûts de télécommunication tout en offrant des fonctionnalités avancées comme la messagerie vocale, les conférences et les appels en attente.

**4. Routage et Résilience**

**4.1 Routage Inter-VLAN**

Le routage entre les VLANs est géré par des **commutateurs multicouches**, permettant aux différents départements de communiquer de manière transparente tout en maintenant les isolations nécessaires. Le protocole **OSPF (Open Shortest Path First)** est utilisé comme protocole de routage afin d'assurer une communication dynamique et redondante entre les différents équipements réseau (pare-feu, routeurs et commutateurs multicouches).

**4.2 Redondance et Haute Disponibilité**

Pour garantir la redondance, les **serveurs DHCP**, **DNS** et autres services critiques sont configurés pour fonctionner en mode actif-actif, avec des serveurs redondants prêts à prendre le relais en cas de panne d'un serveur. En complément, le protocole **HSRP** est mis en place pour assurer la haute disponibilité des routeurs et un équilibrage de charge entre plusieurs routeurs.

**5. Virtualisation et Gestion des Ressources Serveurs**

**5.1 Virtualisation des Serveurs**

La virtualisation est mise en œuvre avec **deux serveurs physiques** fonctionnant sous un hyperviseur, permettant de créer plusieurs machines virtuelles pour différents services (serveurs DNS, DHCP, FTP, etc.). Cela permet de maximiser l'utilisation des ressources tout en offrant une plus grande flexibilité et une gestion simplifiée des serveurs.

**5.2 Redondance Serveurs**

Les serveurs critiques comme **Active Directory (AD)** et **Radius** sont placés dans la zone interne du pare-feu, et des **serveurs DHCP** sont configurés pour fournir des adresses IP de manière dynamique et assurer une redondance.

**6. Tests et Validation**

Une série de tests a été menée pour valider la configuration du réseau :

* **Tests de connectivité** : Vérification de la capacité de communication entre les différents services et départements grâce à des tests de ping, de routage et de transfert de fichiers.
* **Tests de sécurité** : Validation des règles de pare-feu, des ACL et des configurations SSH pour s'assurer qu'aucune brèche de sécurité n'existe.
* **Tests de performance** : Test de la gestion du trafic inter-VLAN, des performances des points d'accès sans fil et de la bande passante sur les liens de connexion FAI.

**Conclusion**

Le réseau conçu répond pleinement aux exigences de sécurité, de performance, de redondance et d'évolutivité. Grâce à l'intégration de technologies de pointe, telles que la virtualisation, le routage dynamique et la gestion centralisée du sans fil, l'infrastructure réseau est prête à soutenir la croissance future de l'entreprise tout en garantissant une connectivité fiable et sécurisée. Ce projet a été un succès, offrant une solution réseau moderne et flexible pour les employés, les clients et les partenaires de l'entreprise.

Schéma :

