

TP CISCO ACL- Conception et déploiement d'une infrastructure réseau d'entreprise

Contexte

Vous êtes ingénieur réseau pour la société MultiTech qui vient d'acquérir de nouveaux locaux. On vous confie la responsabilité de concevoir et déployer l'architecture réseau complète entre les différents services de l'entreprise, répartis sur 3 bâtiments distincts.

La société emploie environ 220 collaborateurs et prévoit une croissance dans les années à venir. L'infrastructure doit être évolutive, sécurisée et permettre la mise en place de qualité de service pour les applications critiques.

Cahier des charges

Organisation physique

- 3 bâtiments séparés d'environ 300m chacun
- Interconnexion par fibre optique (20 Gbps)
- Chaque bâtiment possède sa propre salle serveur

Organisation logique

- **Bâtiment A (Siège)** : Direction générale, Service finance, Service RH
 - Une DMZ pour héberger les serveurs web et mail accessibles depuis l'extérieur
 - Connexion Internet principale (liaison fibre 1 Gbps)
- **Bâtiment B (Production)** : Équipes de développement, Ingénierie
 - Applications gourmandes en bande passante (visioconférence HD, transfert de fichiers volumineux)
 - Système de téléphonie IP
 - Connexion Internet secondaire (liaison fibre 500 Mbps) pour redondance
- **Bâtiment C (Support)** : Service client, Marketing
 - Accès aux bases de données clients
 - Système de téléphonie IP
 - Streaming vidéo pour les communications marketing

Étape 1 : Conception de l'architecture (5 points)

1. Établir un plan d'adressage IP complet pour l'ensemble des réseaux avec un minimum de 6 VLANs en utilisant uniquement des adresses privées
2. Créer un schéma du réseau identifiant tous les équipements nécessaires
3. Prévoir des plages d'adressage permettant une expansion future (30% de croissance minimum)
4. Planifier la redondance des liens critiques et l'équilibrage de charge

Étape 2 : Mise en place de l'infrastructure sous Packet Tracer (10 points)

1. Placer et configurer les équipements principaux (routeurs, commutateurs, pare-feu)
2. Configurer les VLANs et le routage inter-VLAN
3. Mettre en place le protocole de routage EIGRP avec authentification
4. Configurer la DMZ avec NAT/PAT pour les serveurs accessibles depuis l'extérieur
5. Configurer la téléphonie IP avec un minimum de 4 téléphones

Étape 3 : Mise en place des politiques de sécurité (5 points)

1. Configurer des ACL pour :
 - Interdire l'accès SSH aux équipements réseau depuis le réseau des utilisateurs
 - Bloquer tout accès au réseau de la Direction générale depuis les autres départements
 - Autoriser uniquement les ports 80, 443 et 25 sur les serveurs de la DMZ
 - Empêcher le service marketing d'accéder aux serveurs de développement
2. Mettre en place un mécanisme d'inspection de paquets stateful entre la DMZ et le réseau interne

Bonus (+2 points)

Mettre en place un poste d'administration réseau capable de se connecter à tous les équipements via un VLAN d'administration dédié, avec configuration d'un tunnel VPN pour accès à distance sécurisé.

Livrables attendus

1. Document plan d'adressage
2. Fichier de configuration Packet Tracer (.pkt)