**Plan de l'Architecture Réseau**

**1. Introduction**

L'objectif de ce document est de présenter le plan de l'architecture réseau illustré dans le schéma Packet Tracer. Ce réseau est composé de plusieurs segments interconnectés, incluant des postes clients, des serveurs, des routeurs, des switchs et des dispositifs de sécurité. La topologie adoptée vise à assurer la connectivité, la sécurité et la performance du système d'information.

**2. Description des Différents Éléments**

**2.1. Infrastructure Principale**

* **Routeurs** : Gestion de l'interconnexion des différents réseaux et répartition du trafic.
* **Switchs** : Distribution locale du trafic réseau pour les postes clients et les serveurs.
* **Pare-feu (Firewall)** : Protection du réseau contre les menaces externes et internes.

**2.2. Segments du Réseau**

* **Réseau de l'administration** : Contient les postes des administrateurs avec un VLAN dédié.
* **Réseau des collaborateurs** : Segment destiné aux postes de travail des employés avec un VLAN dédié.
* **Réseau des invités** : Isolation des connexions des visiteurs pour renforcer la sécurité avec un VLAN dédié.
* **Réseau commercial** : Intègre les postes qui sont dans un réseau externe à l’entreprise (télétravail) liés aux activités commerciales de l'entreprise.
* **Réseau d'hébergement cloud** : Infrastructure décentralisée permettant de faire des backups des sauvegardes de l’entreprise.
* **DMZ (Zone Démilitarisée)** : Espace intermédiaire pour les serveurs accessibles depuis Internet, tels que DNS et VPN.

**2.3. Adressage et Interconnexion**

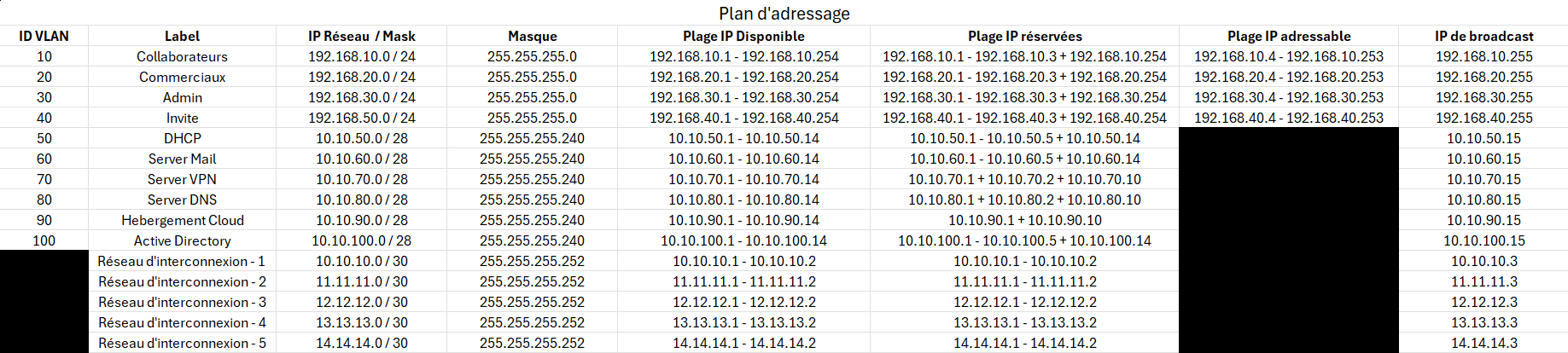
* Différents sous-réseaux sont utilisés pour segmenter le trafic.
* VLANs configurés pour optimiser la sécurité et la gestion des flux.
* Liens redondants pour assurer la continuité de service.

**3. Objectifs de l'Architecture**

* **Performance** : Facilité d’accès aux ressources de l’entreprise y compris depuis chez soi grâce au VPN.
* **Sécurité** : Mise en place de redondance sur le réseau (+ STP), d'une segmentation réseau et de filtrage de paquets.
* **Scalabilité** : Capacité d'évoluer avec les besoins de l'entreprise.

**4. Conclusion**

Cette architecture réseau permet une gestion efficace des flux de données, tout en garantissant la sécurité et la performance des communications internes et externes grâce à plusieurs dispositifs comme la segmentation par VLANs et sous réseau, l’accès aux ressources depuis un VPN ou encore les backups disponibles sur le cloud.

**Plan d’adressage IP**

**Gestion des ACL**

**1. Introduction**

Les listes de contrôle d'accès (ACL) sont des règles de filtrage utilisées sur les pare-feu et routeurs pour sécuriser le réseau en régulant le trafic autorisé ou interdit. Dans ce document, nous allons définir les ACL nécessaires à la protection des services et données du projet.

**2. Types d’ACL**

Il existe deux types d’ACL :  
- \*\*ACL standard\*\* : filtrent uniquement sur l’adresse IP source.  
- \*\*ACL étendues\*\* : permettent un contrôle plus précis en filtrant sur plusieurs critères (adresse source/destination, protocole, ports…).  
  
Dans notre projet, nous utiliserons principalement des ACL étendues pour une meilleure sécurité.

**3. Règles ACL définies**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Règle | Source | Destination | Protocole | Port | Action |
| 1 | Internet (0.0.0.0/0) | Serveur Web | TCP | 443 (HTTPS) | Autoriser |
| 2 | Internet (0.0.0.0/0) | Réseau interne | Tout | Tout | Refuser |
| 3 | Réseau interne | Internet | TCP/UDP | 80, 443 | Autoriser |
| 4 | VPN (collaborateurs) | Réseau interne | Tout | Tout | Autoriser |
| 5 | Réseau interne | Serveur de fichiers | SMB | 445 | Autoriser |
| 6 | Réseau interne | DNS interne | UDP | 53 | Autoriser |
| 7 | Tout | Tout | Tout | Tout | Refuser (par défaut) |

**4. Exemple de configuration d’ACL sur un pare-feu Cisco**

Voici un exemple de configuration des ACL sur un pare-feu Cisco :

! Autoriser l’accès HTTPS au serveur web

access-list 100 permit tcp any host 192.168.1.10 eq 443

! Interdire tout autre trafic venant d’Internet vers le réseau interne

access-list 100 deny ip any 192.168.0.0 0.0.255.255

! Bloquer l'accès du réseau DMZ (192.168.2.0/24) au réseau local

access-list 100 deny ip 192.168.2.0 0.0.0.255 192.168.0.0 0.0.255.255

! Autoriser les connexions sortantes vers Internet (web)

access-list 100 permit tcp 192.168.0.0 0.0.255.255 any eq 443

! Autoriser uniquement SSH (port 22, TCP) et HTTPS (port 443, TCP et UDP) depuis le VPN

access-list 100 permit tcp 10.0.0.0 0.0.0.255 192.168.0.0 0.0.255.255 eq 22

access-list 100 permit tcp 10.0.0.0 0.0.0.255 192.168.0.0 0.0.255.255 eq 443

access-list 100 permit udp 10.0.0.0 0.0.0.255 192.168.0.0 0.0.255.255 eq 443

! Bloquer tout le reste

access-list 100 deny ip any any

! Application des ACL sur l’interface du pare-feu

interface GigabitEthernet0/1

ip access-group 100 in

**5. Conclusion**

La mise en place des ACL permet d'assurer une segmentation efficace du réseau et de limiter les accès non autorisés. En appliquant une politique de sécurité stricte, nous réduisons les risques d’attaques et assurons la protection des données et services du projet.

**Justificatif des Choix Effectués**

**1. Introduction**

L'architecture réseau mise en place repose sur des choix techniques visant à assurer la sécurité, la disponibilité et la performance des communications au sein de l'entreprise. Ce document justifie les décisions prises en expliquant leurs avantages et inconvénients, ainsi que l'utilisation de solutions open source ou propriétaires.

**2. Justification des Choix**

**2.1 Redondance et Sécurité des Switchs**

**Choix :** Mise en place d'une infrastructure redondante avec le protocole STP (Spanning Tree Protocol).

* **Avantages :**
  + Évite les boucles réseau et assure la stabilité du réseau local.
  + Améliore la disponibilité en cas de défaillance d’un switch ou d’un lien réseau.
  + Permet une meilleure gestion de la topologie dynamique.
* **Inconvénients :**
  + Augmente la complexité de configuration et de maintenance.
  + Peut engendrer un temps de convergence en cas de panne.

**2.2 Segmentation Réseau avec VLANs**

**Choix :** Utilisation de VLANs pour segmenter le réseau en sous-réseaux isolés.

* **Avantages :**
  + Améliore la sécurité en isolant les différents services et départements.
  + Réduit la congestion en limitant la propagation du trafic de broadcast.
  + Facilite l’administration et l’application de politiques de sécurité.
* **Inconvénients :**
  + Complexifie la configuration initiale et la gestion.
  + Peut nécessiter des équipements compatibles avec les VLANs.

**2.3 Attribution Dynamique des Adresses IP**

**Choix :** Mise en place d’un serveur DHCP pour la gestion automatique des adresses IP.

* **Avantages :**
  + Simplifie l’administration réseau en évitant l’attribution manuelle des adresses IP.
  + Permet une gestion centralisée et efficace du plan d’adressage IP.
  + Réduit le risque d’erreurs de configuration.
* **Inconvénients :**
  + Dépendance au serveur DHCP : une panne peut empêcher les nouveaux appareils de se connecter.
  + Risque de saturation de la table d’adresses en cas de mauvaise gestion.

**2.4 Routage Dynamique avec EIGRP**

**Choix :** Utilisation du protocole EIGRP (Enhanced Interior Gateway Routing Protocol), propriétaire Cisco.

* **Avantages :**
  + Temps de convergence rapide par rapport à d’autres protocoles comme RIP.
  + Utilisation efficace de la bande passante avec mise à jour incrémentielle des routes.
  + Possibilité de faire du load balancing avancé.
* **Inconvénients :**
  + Protocole propriétaire, limité aux équipements Cisco.
  + Configuration plus complexe que RIP.

**2.5 Hébergement des Services Critiques en DMZ**

**Choix :** Hébergement du serveur DNS et VPN dans une DMZ pour des raisons de sécurité.

* **Avantages :**
  + Renforce la protection contre les attaques extérieures en isolant les services exposés.
  + Permet un contrôle strict des flux de données entre Internet et le réseau interne.
  + Assure la disponibilité des services critiques même en cas d’attaque.
* **Inconvénients :**
  + Complexité accrue dans la gestion des règles de pare-feu.
  + Peut nécessiter une infrastructure matérielle plus robuste.

**2.6 Intégration du Cloud pour les Backups**

**Choix :** Utilisation d’un cloud privé ou hybride pour les sauvegardes de l’entreprise.

* **Avantages :**
  + Protection contre la perte de données en cas de panne matérielle.
  + Accessibilité des sauvegardes depuis différents sites.
  + Réduction des coûts liés à l’infrastructure locale de stockage.
* **Inconvénients :**
  + Dépendance à une connexion Internet stable pour accéder aux sauvegardes.
  + Risque de sécurité si le stockage cloud n'est pas correctement protégé.

**3. Conclusion**

L’architecture réseau adoptée repose sur des solutions techniques équilibrant performance, sécurité et évolutivité. L’utilisation de technologies propriétaires comme EIGRP et d’équipements Cisco assure une compatibilité et un support optimal, bien que cela implique des coûts plus élevés. En parallèle, l’intégration de mécanismes standards comme STP, VLANs et DHCP facilite la gestion et la maintenance du réseau. Enfin, l’hébergement des services critiques en DMZ et l’usage du cloud garantissent une protection accrue des ressources de l’entreprise.

# Planning et Répartition des Tâches

## **1. Introduction**

Ce document présente la répartition des tâches au sein de l'équipe de trois personnes travaillant sur l'architecture réseau. Chaque membre est assigné à des responsabilités spécifiques pour assurer une gestion efficace du projet.

## **2. Répartition des Tâches**

|  |  |  |
| --- | --- | --- |
| Membre | Tâches principales | Détails |
| Thomas | Description de l’architecture | - Configuration des commutateurs (Switchs) et VLANs - Routage et protocole EIGRP - Configuration de l'Active Directory |
| Christophe | Justification des choix techniques | - Explication des avantages et inconvénients des technologies choisies (Open Source vs Commercial) - Sécurité (Pare-feu, DMZ, VPN)  - Préparation des tests et validation des configurations |
| Axel | Organisation, documentation et tests | - Élaboration du planning du projet  - Configuration du pare-feu et des ACL - Documentation du projet et rédaction du rapport |
| Tous | Tâches communes | - Création du schéma réseau - Configuration du fichier Packet Tracer  - Plan d’adressage IP |

## **3. Échéancier**

|  |  |  |  |
| --- | --- | --- | --- |
| Phase | Tâche | Responsable | Date de rendu |
| Phase 1 | Mise en place de l’architecture réseau | Thomas | 11/12/2024 |
| Phase 2 | Rédaction de la justification des choix | Christophe | 11/12/2024 |
| Phase 3 | Test et validation des configurations | Axel | 04/01/2024 |
| Phase 4 | Finalisation du rapport et démonstration | Tous | 16/01/2024 |

## **4. Conclusion**

Ce planning permet une organisation claire des tâches et assure que chaque membre contribue efficacement au projet. La collaboration et le respect des délais seront essentiels pour mener à bien cette mission.