Cahier des charges

Infrastructure Réseaux et Sécurité

Projet EcoDeli – 2024-2025

EcoDelie

110, rue de Flandre

75019 Paris

EcoDeli
CROWDSHIPPING DELIVERY SERVICE

Sommaire

Introduction

EcoDeli souhaite moderniser son infrastructure réseau afin d'améliorer la disponibilité, la sécurité et la performance de ses services. L'objectif est de garantir une communication fiable entre les différents sites et d'assurer la protection des données sensibles.

1.1 Objectifs

Dans le cadre de son expansion et de l'optimisation de ses services, **EcoDeli** souhaite moderniser son infrastructure réseau et sécuriser l'ensemble de ses communications inter-sites. Ce projet vise à mettre en place un réseau fiable, sécurisé et évolutif, garantissant une **haute disponibilité des services** et une **gestion optimale des flux de données**.

L'objectif principal est d'assurer une **connectivité fluide** entre les différents sites de l'entreprise, tout en **renforçant la sécurité des accès et la protection des données sensibles**. Une **segmentation réseau efficace**, une **virtualisation des ressources** et une **politique de sécurité stricte** seront mises en place pour garantir une infrastructure stable et performante.

2. Périmètre du projet

Le projet couvre l'ensemble des **sites d'exploitation** de l'entreprise :

- **Paris (Siège & Datacenter principal)** : Gestion de l'Active Directory, stockage centralisé, messagerie et supervision du réseau.
- **Marseille (Backup Mail)** : Serveur de secours pour la messagerie, assurant une continuité de service en cas de panne du site principal.
- **Lyon (Backup des serveurs, DHCP, DNS)** : Administration des IPs, gestion des noms de domaine et sauvegarde journalière de l'infrastructure.
- **Lille (Stockage sécurisé, RODC, RGPD)** : Serveur dédié à la gestion des données sensibles, avec un stockage chiffré et un contrôleur de domaine en lecture seule.

- **Rennes et Montpellier** : Sites non encore déployés, prévus dans une **phase 2** du projet.

3. Architecture Réseau

3.1 Topologie et segmentation

L'architecture réseau sera basée sur une segmentation en **VLANs** afin de garantir **une meilleure organisation des flux et une séparation logique des services**. Chaque département (Direction, RH, Marketing, Informatique, etc.) disposera de son propre VLAN, avec des règles d'accès spécifiques.

Les connexions entre les différents sites seront assurées par un **réseau privé EDN (EcoDeli Network)**, utilisant le **protocole RIP v2** pour le routage interne. Ce choix permettra une **mise à jour dynamique des routes** et une **répartition efficace du trafic**.

Un **schéma d'architecture détaillé** sera élaboré pour illustrer la répartition des équipements, la segmentation des réseaux et les règles de communication entre les différents sites.

3.2 Connectivité et accès distant

Pour assurer une communication fluide entre les agences, une **infrastructure VPN** sera déployée :

- **VPN Site-to-Site** : Relie les différentes agences entre elles, garantissant un accès sécurisé aux services hébergés à Paris et Lyon.
- **VPN Client-to-Site** : Permet aux employés en télétravail de se connecter au réseau interne via une **authentification renforcée (MFA)**.

Deux **firewalls OPNsense** seront installés sur chaque site pour assurer une **redondance et une protection avancée contre les intrusions**.

3.3 Répartition des services réseau par site

Site	Rôles principaux
Paris (Siège)	Active Directory, stockage central, DMZ, serveur mail principal, monitoring

Marseille	Backup du serveur mail, connexion VPN site-to-site
Lyon	Serveur DHCP & DNS, Backup des serveurs, gestion des IPs
Lille	RODC (Read-Only Domain Controller), stockage sécurisé pour la direction
Rennes / Montpellier	Déploiement prévu en phase 2

4. Sécurité & Supervision

4.1 Sécurisation des accès

La **sécurité** étant un enjeu majeur du projet, plusieurs **mesures de protection** seront mises en place :

- **Filtrage avancé des flux** via **firewalls OPNsense** (interdiction des accès non autorisés).
- **Segmentation VLAN** stricte pour limiter les risques de propagation des menaces.
- **VPN sécurisé** avec **authentification multi-facteurs (MFA)**.
- **Chiffrement des données sensibles** sur les serveurs et bases de données.
- **Gestion centralisée des identités et des droits d'accès** via Active Directory et RADIUS.

4.2 Monitoring & Alerting

Un **système de supervision** sera mis en place afin de **garantir la disponibilité et la performance** des équipements réseau et des serveurs.

- **Zabbix / Nagios** : Supervision en temps réel des infrastructures, remontée des alertes en cas de panne.
- **GLPI** : Gestion des incidents et suivi des équipements.
- **ELK Stack** : Centralisation des logs pour une analyse approfondie des événements de sécurité.

5. Déploiement & Virtualisation

5.1 Virtualisation des services

Tous les services critiques seront **virtualisés** afin de maximiser leur **disponibilité et leur évolutivité**.

- **VMware vSphere ESXi / Proxmox / Eve-NG / GNS3** pour l'hébergement des serveurs.
- **Docker & Kubernetes** pour **l'isolation et l'orchestration des applications**.
- **Backup journalier** des serveurs sur **Lyon** et **sauvegarde mensuelle** sur un stockage externe.

5.2 Plan de secours et reprise après incident

Un **plan de continuité d'activité (PCA)** sera défini afin d'assurer la **récupération rapide des services en cas de panne**. Il inclura :

- Des **serveurs de secours** (Backup Mail, DNS, Active Directory).
- Une **réplication des données** entre Paris et Lyon.
- Des **tests de reprise réguliers** pour garantir l'efficacité des procédures.

6. Livrables attendus

Pour assurer le suivi et la bonne exécution du projet, les **livrables suivants** devront être produits :

- **Schéma détaillé de l'architecture réseau**
- **Plan d'adressage IP (LAN, DMZ, WAN)**
- **Documentation de configuration (firewalls, routeurs, serveurs, VPNs)**
- **Plan de sécurisation des accès et gestion des droits**
- **Procédure de sauvegarde et de reprise après incident**
- **Rapports de supervision et d'audit de sécurité**

7. Contraintes & Exigences

- Respect strict des **normes de sécurité et de protection des données (RGPD)**.
- Limitation du budget d'hébergement cloud externe à **40-50€/mois**.
- Documentation détaillée et mise à jour régulièrement.
- **Tests de montée en charge et de failover** avant la mise en production.

8. Planning prévisionnel

Phase	Tâches	Durée estimée
1. Conception	Définition de l'architecture, choix des outils	2 semaines
2. Installation	Déploiement des serveurs, configuration réseau	3 semaines
3. Sécurisation	Firewalling, VPN, ACL, tests de sécurité	2 semaines
4. Virtualisation	Mise en place des machines virtuelles	2 semaines
5. Supervision	Déploiement des outils de monitoring et alerting	1 semaine
6. Tests & validation	Vérifications finales, correction des erreurs	1 semaine

9. Conclusion

Ce cahier des charges définit une **infrastructure réseau robuste et évolutive** pour EcoDeli, garantissant **sécurité, performance et continuité de service** face à sa croissance rapide.