**Réponse à l'appel d'offre EcoDeli**

**Mission 3 : Infrastructure Système, Réseau et Sécurité**

**1. Compréhension du besoin**

**Suite à l'analyse de votre cahier des charges, nous avons identifié les besoins suivants pour votre infrastructure système, réseau et sécurité :**

**Objectifs principaux :**

* **Connecter et assurer une haute disponibilité de service sur l'ensemble des sites (Paris, Marseille, Lyon, Lille)**
* **Mettre en place un réseau propriétaire (EDN - EcoDeli Network) pour gérer les connexions intersites**
* **Sécuriser l'ensemble des données et communications de l'entreprise**
* **Permettre l'accès distant sécurisé pour les collaborateurs en mobilité**

**Contraintes identifiées :**

* **Nécessité de maintenir les missions 1 et 2 (applications de gestion et services supplémentaires) en production sur cette nouvelle infrastructure**
* **Segmentation précise des accès selon les profils utilisateurs**
* **Protection des données sensibles, notamment celles concernant la RGPD**
* **Haute disponibilité des services critiques avec solutions de backup**

**2. Solution proposée**

**Notre solution répond à l'ensemble des exigences décrites dans le cahier des charges et s'articule autour de quatre sites principaux :**

**2.1. Site de Paris (Siège principal)**

**Infrastructure serveurs :**

* **Serveur Active Directory sous Windows Server 2022 avec gestion de l'ensemble des utilisateurs (80 collaborateurs)**
* **Baie de stockage centralisée pour toutes les données de l'entreprise**
* **DMZ sécurisée hébergeant le serveur mail Postfix sous Linux**

**Segmentation réseau :**

* **LAN segmenté en 5 VLAN distincts (Direction, Marketing, Commercial, RH, Informatique)**
* **DMZ isolée pour les services accessibles depuis l'extérieur**
* **Double firewall OPNSense en haute disponibilité**

**Accès :**

* **Accès externe sécurisé pour clients et prestataires via la DMZ**
* **Accès interne pour les collaborateurs sur site**
* **Solution VPN pour les collaborateurs en télétravail**

**Supervision :**

* **GLPI pour la gestion des tickets et inventaire**
* **Zabbix pour la supervision des équipements et services**

**2.2. Site de Marseille (Backup mail)**

* **Serveur mail de secours sous Linux en réplication avec le serveur principal**
* **Double connectivité réseau pour assurer la redondance**
* **VPN site-to-site avec Paris**
* **Solution VPN pour accès distant des collaborateurs**

**2.3. Site de Lyon (Backup serveurs)**

* **Serveur DHCP sous Linux**
* **Serveur DNS sous Linux**
* **Solution de backup programmée :** 
  + **Quotidienne (23h)**
  + **Mensuelle (jour 30)**
* **Double firewall OPNSense en haute disponibilité**

**2.4. Site de Lille (RODC et RGPD)**

* **Contrôleur de domaine en lecture seule (RODC)**
* **Stockage sécurisé et chiffré pour les données sensibles de la direction**
* **Double firewall OPNSense**
* **Solution VPN pour accès distant**

**2.5. Réseau EDN (EcoDeli Network)**

* **Configuration du protocole RIP v2 pour le routage entre sites**
* **Tunnels VPN IPSec over GRE pour la communication sécurisée intersites**
* **ACL spécifiques pour le contrôle des flux**
* **HSRP pour la redondance des routeurs**

**2.6. Sécurité globale**

* **Certificats SSL/TLS pour les communications web**
* **Chiffrement des données sensibles**
* **Politiques de sécurité strictes**
* **Système de sauvegarde multi-sites**

**3. Méthodologie de déploiement**

**Notre déploiement suivra une méthodologie en 5 phases :**

1. **Phase de préparation (2 semaines)**
   * **Validation des plans d'adressage**
   * **Finalisation des schémas réseau**
   * **Préparation des environnements virtuels**
2. **Phase de mise en place de l'infrastructure cœur (4 semaines)**
   * **Déploiement des routeurs et firewalls**
   * **Configuration du réseau EDN**
   * **Mise en place des tunnels VPN intersites**
3. **Phase de déploiement des services (3 semaines)**
   * **Installation des serveurs**
   * **Configuration Active Directory**
   * **Mise en place des solutions de stockage**
4. **Phase d'intégration des missions 1 et 2 (2 semaines)**
   * **Migration des applications**
   * **Tests de performance et de disponibilité**
   * **Configuration des conteneurs Docker**
5. **Phase de tests et validation (1 semaine)**
   * **Tests de charge**
   * **Tests de failover**
   * **Formation des équipes**

**4. Avantages de notre solution**

* **Haute disponibilité : Redondance à tous les niveaux critiques**
* **Évolutivité : Architecture modulaire permettant l'ajout futur des sites de Rennes et Montpellier**
* **Sécurité renforcée : Segmentation, chiffrement et contrôle d'accès stricts**
* **Maintenance simplifiée : Documentation complète et outils de supervision**
* **Conformité RGPD : Isolation des données sensibles**

**5. Livrables**

* **Document d'Architecture Technique (DAT) complet**
* **Schémas réseau détaillés (physiques et logiques)**
* **Procédures d'installation et de configuration**
* **Documentation utilisateur**
* **Rapports de tests et de validation**
* **Conteneurisation des applications des missions 1 et 2**