BTS SIO 2

PROJET IFIDE

# REPONSE AU CAHIER DES CHARGES

GROUPE N° 4

BENSALEM Mohamed Abdou

&

AYYADI Aymane

# Table Des Matières :

I. Présentation du Groupe :.....3

II. Rappel des besoins et des objectifs du projet.....4

III. Solutions.....5

A. Étude de solutions et solutions alternatives.....5

B. Tableau comparatif des choix techniques.....6

IV. Diagramme de réseau .....8

V. Budget :.....9

VI. Planning .....10

# I. Présentation du Groupe :

**Abdou** – *Administrateur du site de Mulhouse*

Dans le cadre du projet IFIDE, j'ai pris en charge la configuration complète de l'infrastructure du site de Mulhouse. J'ai mis en place les services réseau indispensables tels qu'Active Directory, DNS, DHCP, DFS, DFS /R et les (GPO) afin d'assurer une gestion centralisée et sécurisée. J'ai également réalisé la réplication et la connexion intersites avec le site de Strasbourg, garantissant ainsi la disponibilité et la fiabilité du système d'information entre les deux serveurs.

**Aymane** – *Administrateur du site de Strasbourg*

Dans le cadre du projet IFIDE, j'ai pris en charge la mise en place et la configuration de l'infrastructure du site de Strasbourg. J'ai installé et configuré les services principaux tels qu'Active Directory, DNS, DHCP, DFS, DFS/R et les stratégies de groupe (GPO), afin d'assurer une administration centralisée et sécurisée. J'ai également configuré la connexion intersites avec le site de Mulhouse, garantissant la redondance, la synchronisation et la continuité des services au sein du domaine IFIDE.LAN.

- Ensemble, nous travaillons en coordination pour assurer le succès du projet, en maintenant la cohérence technique et la haute disponibilité sur les deux sites.

# II. Rappel des besoins et des objectifs du projet :

- Le centre IFIDE nécessite un système d'information hautement disponible et sécurisé interconnectant les sites de Strasbourg et de Mulhouse. Pour y parvenir, le projet se déroulera en deux phases, suivies d'une intégration conjointe :

1. **Phase de déploiement par site**
   - Chaque administrateur est responsable de la mise en place de l'infrastructure de son site attribué (Mulhouse ou Strasbourg).
   - Cela inclut l'installation et la configuration des serveurs (AD, DNS, DHCP, DFS), des routeurs/pare-feu et des postes clients.
   - Les services locaux seront configurés en redondance et sécurisés.
2. **Phase d'intégration inter-sites**
   - Une fois les deux sites opérationnels, nous mettrons en place un **VPN site-à-site** (IPSec ou OpenVPN) entre Strasbourg et Mulhouse.
   - La réplication des données (DFSR) et les systèmes de fichiers distribués seront configurés pour permettre une collaboration fluide.
   - Les politiques de sécurité (pare-feu, authentification, permissions) seront harmonisées entre les deux sites.
3. **Maintenance et continuité**
   - Des sauvegardes régulières, clichés instantanés et l'intégration d'un SAN garantiront la continuité d'activité et la protection des données.
   - Un suivi et une vérification régulière des services seront effectués.
   - La documentation et les présentations accompagneront chaque étape du projet

- **. Le projet devra également respecter les contraintes suivantes :**
  - Durée : 8 semaines (du 11 septembre au 30 novembre 2025).
  - Budget : inférieur à 100 000 € HT.
  - Remise des livrables et soutenances selon le calendrier défini.

# III. Solutions :

## A. Étude de solutions et solutions alternatives :

- Cette étude de solutions présente les différentes options techniques envisagées pour chaque lot du projet. Pour chaque objectif, au moins deux alternatives ont été analysées, avec leurs avantages et inconvénients. Les choix finaux ont été réalisés selon des critères de **sécurité, haute disponibilité, conformité aux recommandations de l'ANSSI, facilité d'administration et fiabilité à long terme**. Les solutions retenues offrent ainsi un équilibre entre robustesse, maîtrise des coûts et simplicité opérationnelle.

| Lot / Objectif | Solutions | Avantages | Inconvénients | Choix retenu |
|---|---|---|---|---|
| **VPN site-à-site** | **Solution 1 : VPN IPSec** | Standard largement utilisé, compatible avec la plupart des routeurs/firewalls, conforme aux recommandations ANSSI | Configuration parfois complexe | **IPSec** (intégré aux équipements réseaux, robuste en contexte professionnel) |
| / | **Solution 2 : OpenVPN** | Open-source, flexible, facile à déployer | Nécessite un serveur supplémentaire et gestion complexe des certificats | + |
| **Serveurs AD/DNS/DHCP** | **Solution 1 : Windows Server 2022 (GUI)** | Administration simplifiée via interface graphique | Consomme plus de ressources, surface d'attaque plus grande | **Mixte (GUI + Core)** (GUI pour principal, Core pour secondaire) |
| / | **Solution 2 : Windows Server 2022 (Core)** | Plus léger, plus sécurisé, recommandé pour redondance | Administration en ligne de commande uniquement (plus complexe) | / |

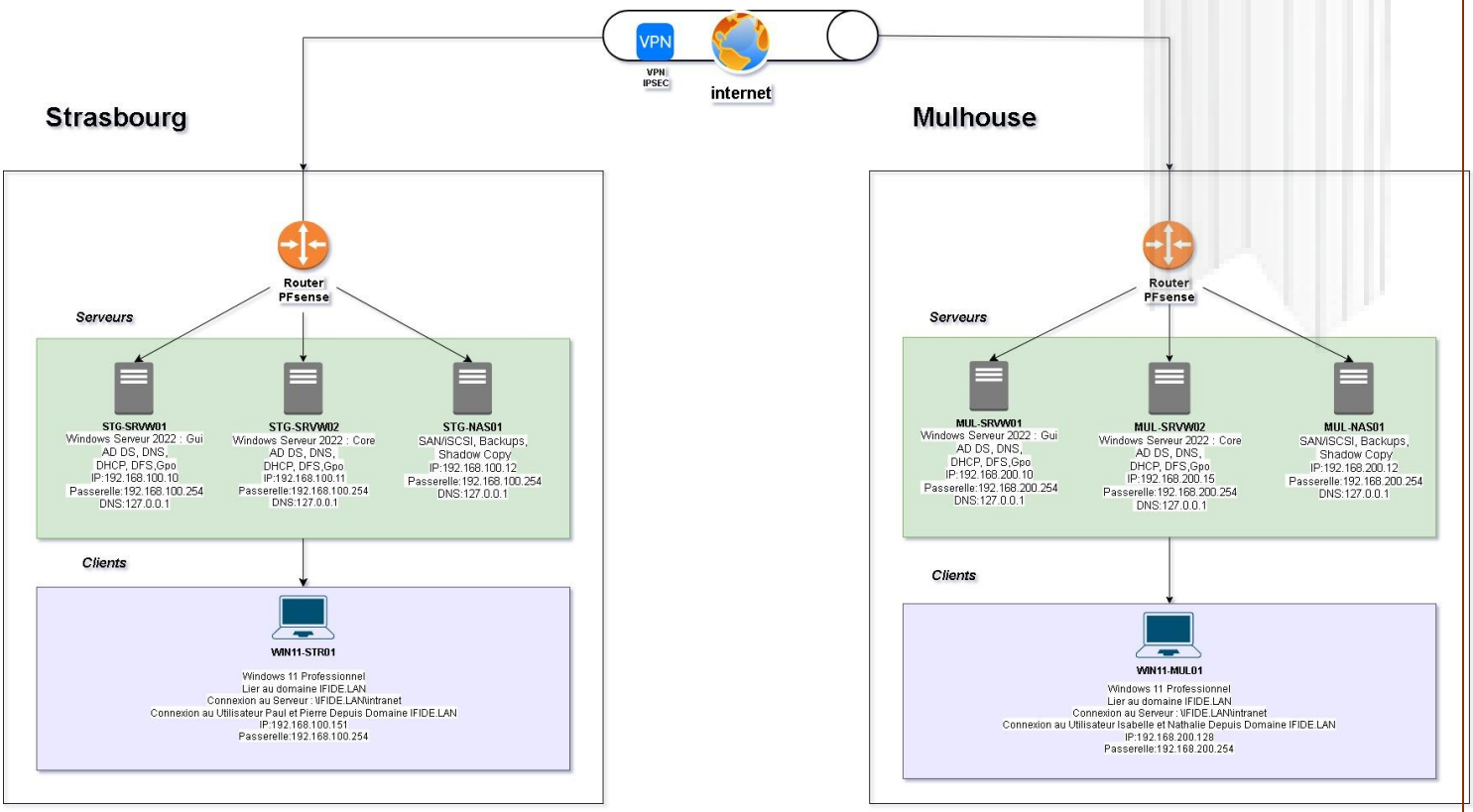
| | | | | |
|---|---|---|---|---|
| **DFS, Réplication et Sauvegardes** | **Solution 1 : SAN avec iSCSI + Shadow Copy** | Haute dispo, snapshots réguliers, centralisation des données | Coût plus élevé | **SAN avec iSCSI + Shadow Copy** (répond aux besoins de PCA et haute dispo) |
| / | **Solution 2 : Stockage local avec sauvegardes manuelles** | Moins cher | Pas de redondance, dépendance aux sauvegardes externes | + |
| **Sécurité et GPO** | **Solution 1 : GPO + règles pare-feu centralisées** | Standardisé, centralisé, conforme ANSSI | Nécessite un suivi constant et documentation | **GPO centralisées + règles pare-feu** (garantissent sécurité et uniformité) |
| / | **Solution 2 : Gestion locale des permissions** | Flexible | Risque élevé d'erreurs, non conforme aux bonnes pratiques | / |

## B. Tableau comparatif des choix techniques :

- Le tableau comparatif offre une vue globale des principaux choix techniques du projet. Il met en évidence les différentes alternatives étudiées et montre clairement les solutions retenues. Cette synthèse permet d'identifier immédiatement les options les plus adaptées en termes de **sécurité, haute disponibilité, conformité et efficacité**, tout en écartant les solutions moins pertinentes.

| Objectif / Composant | Option 1 | Option 2 | Choix retenu |
|---|---|---|---|
| **VPN site-à-site** | IPSec (sécurisé, standard, conforme ANSSI) | OpenVPN + (souple mais plus complexe à gérer) | **IPSec** |
| **Serveurs AD/DNS/DHCP** | Windows Server 2022 GUI (facile à administrer) | Windows Server 2022 Core (léger, sécurisé) | **Mixte GUI + Core** |
| **Stockage & Sauvegardes** | SAN avec iSCSI + Shadow Copy (haute dispo, PCA) | Stockage local + (pas de redondance) | **SAN + Shadow Copy** |
| **Fichiers utilisateurs** | DFS + DFSR (réplication automatique, redondance) | Transfert manuel + (risque d'erreurs, pas fiable) | **DFS + DFSR** |
| **Sécurité & GPO** | GPO centralisées + règles pare-feu (uniformité, sécurité) | Gestion locale + (risques élevés) | **GPO centralisées** |
| **Authentification** | Forêt AD unique (SSO, gestion simplifiée) | Domaines séparés + (complexité accrue) | **Forêt AD unique** |

# IV. Diagramme de réseau :

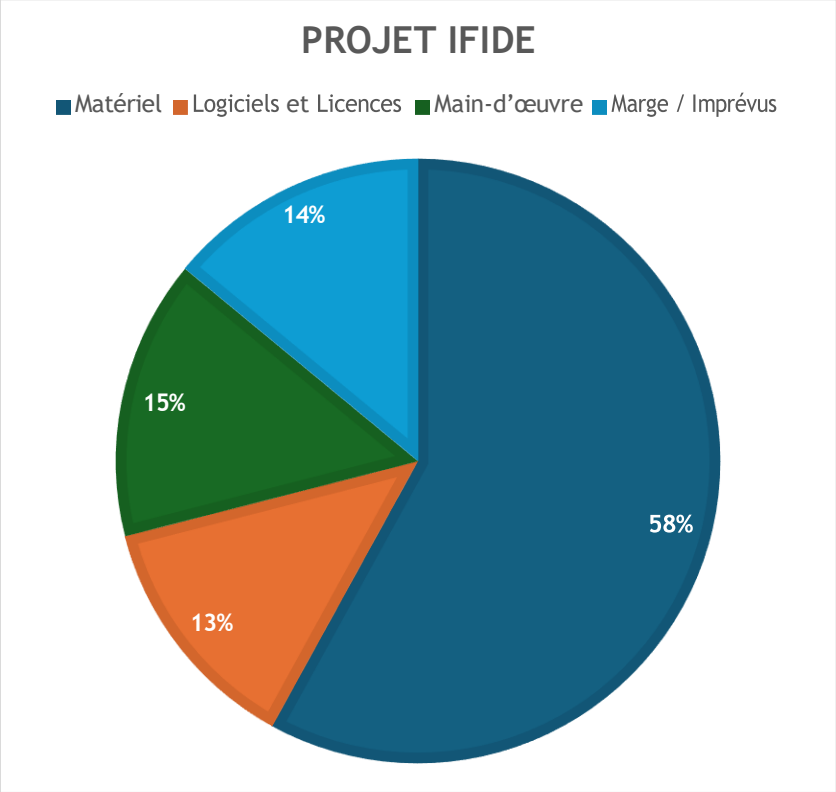



- Le schéma ci-dessus illustre l'architecture proposée pour les sites de **Strasbourg** et **Mulhouse**. Chaque site est équipé d'un **routeur/pare-feu PfSense** assurant la connexion sécurisée au réseau et au **VPN site-à-site IPSec**, garantissant la communication chiffrée entre les deux sites via Internet.
- Dans chaque site, trois serveurs sont déployés :
  - Un **serveur principal** (AD DS, DNS, DHCP, DFS),
  - Un **serveur secondaire** (réplica AD DS, DNS, DHCP failover, DFS),
  - Un **serveur de stockage SAN/iSCSI** dédié aux sauvegardes complètes et aux clichés instantanés (Shadow Copy).

Les **postes clients Windows 11 Pro** sont intégrés au domaine Active Directory et bénéficient d'un accès sécurisé et redondant aux données partagées. Cette infrastructure garantit la **haute disponibilité**, la **sécurité des données** et la **continuité d'activité** pour les utilisateurs des deux sites.

# V. Budget :

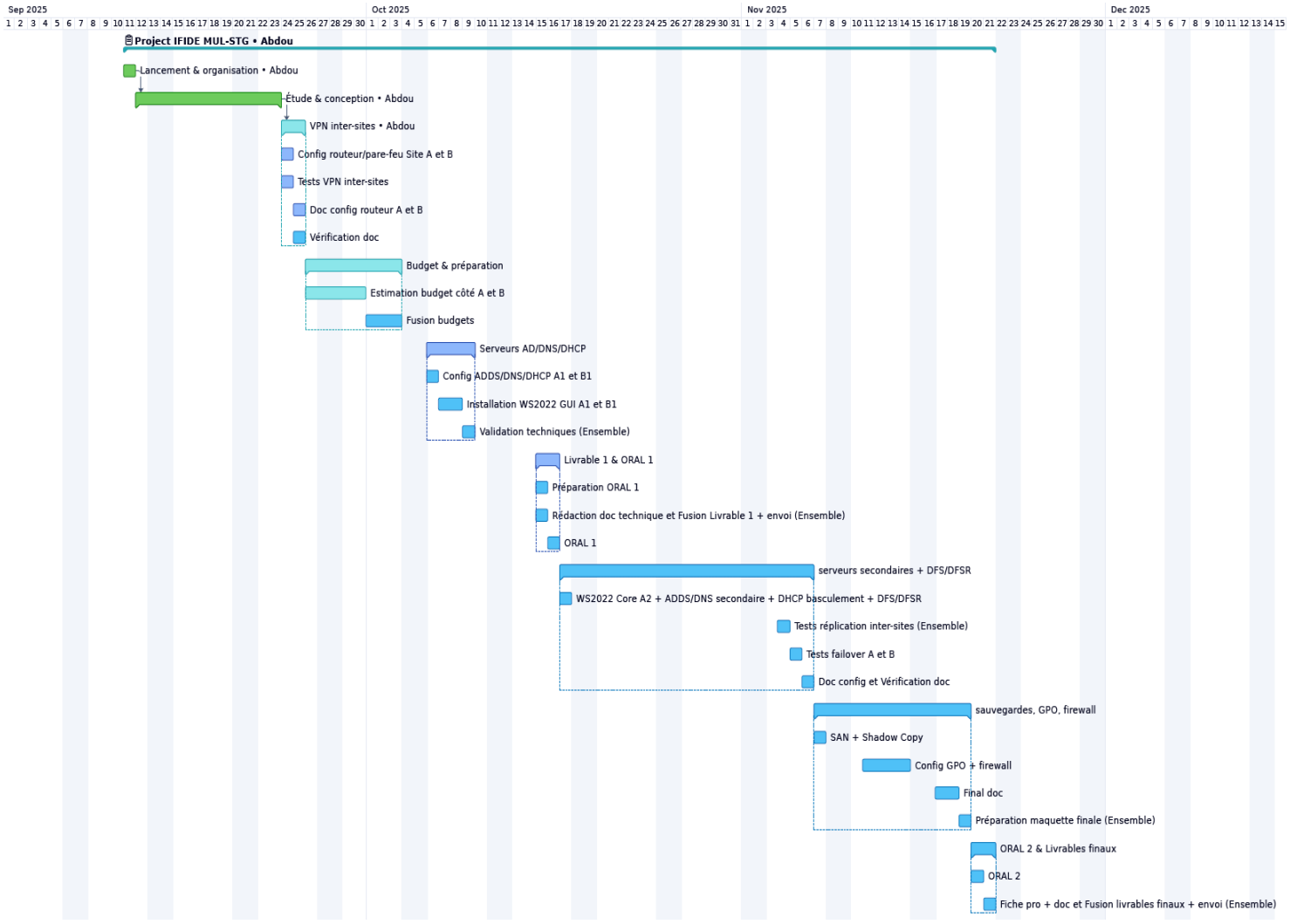
- Le budget prévisionnel du projet est estimé à **67 000 € HT**, ce qui respecte largement la limite de **100 000 € fixée par le cahier des charges**. La plus grande part est consacrée au **matériel (serveurs, SAN, routeurs et postes clients)** afin de garantir une infrastructure robuste et redondante. Les **logiciels et licences** (Windows Server 2022, CALs, solutions VPN/pare-feu) représentent une dépense complémentaire indispensable au bon fonctionnement du système. La **main-d'œuvre** correspond aux heures de travail des deux administrateurs pour l'installation, la configuration, la documentation et les présentations. Enfin, une **marge pour imprévus** a été incluse afin d'anticiper d'éventuels coûts supplémentaires et d'assurer la flexibilité financière du projet.




| Catégorie | Montant (€) | Pourcentage | Explication |
|---|---|---|---|
| **Matériel** | 39 000 | 58 % | 6 serveurs, 2 SAN, 2 routeurs, 2 postes clients – base de l'infrastructure et haute disponibilité |

| | | | |
|---|---|---|---|
| **Logiciels & Licences** | 9 000 | 13 % | Windows Server 2022, CALs, logiciel VPN/pare-feu – nécessaires pour l'exploitation et la sécurité |
| **Main-d'œuvre** | 10 000 | 15 % | ~200h × 50 €/h (2 administrateurs) pour l'installation, la configuration, la documentation et la présentation |
| **Marge / Imprévus** | 9 000 | 14 % | Réserve financière pour couvrir des coûts supplémentaires et assurer la flexibilité du projet |
| **Total** | **67 000** | **100 %** | Respecte la limite fixée à 100 000 € HT |

# VI. Planning :



# VII. Sommaire :

## AD DS (Active Directory Domain Services) :

- Service d'annuaire de Microsoft permettant de gérer les utilisateurs, ordinateurs et ressources du réseau à partir d'un domaine centralisé. Il facilite l'authentification, la gestion des droits d'accès et la sécurité.

## DNS (Domain Name System) :

- Service qui traduit les noms de domaine en adresses IP compréhensibles par les machines, facilitant ainsi l'accès aux ressources du réseau.

## DHCP (Dynamic Host Configuration Protocol) :

- Service qui attribue automatiquement les adresses IP, la passerelle et les paramètres réseau aux postes clients, évitant toute configuration manuelle.

## DFS (Distributed File System) :

- Service permettant de regrouper plusieurs dossiers partagés sur différents serveurs en un seul espace de noms logique, simplifiant ainsi l'accès aux fichiers pour les utilisateurs.

## DFS-R (Distributed File System Replication) :

- Extension du DFS permettant la réplication automatique des données entre plusieurs serveurs afin d'assurer la redondance et la continuité de service.

## GPO (Group Policy Object) :

- Outil de gestion centralisée des stratégies de sécurité et de configuration appliquées aux utilisateurs et ordinateurs d'un domaine Active Directory.

### VPN (Virtual Private Network) :

- Réseau privé virtuel permettant de relier plusieurs sites distants via Internet de manière sécurisée, comme s'ils faisaient partie d'un même réseau local.

### IPSec (Internet Protocol Security) :

- Protocole de sécurité qui chiffre et authentifie les communications entre deux machines ou deux sites dans un VPN, garantissant la confidentialité et l'intégrité des données.

### Pare-feu (Firewall) :

- Système de sécurité qui filtre le trafic réseau entrant et sortant selon des règles définies, protégeant le réseau contre les accès non autorisés et les menaces externes.

*PROJET IFIDE*

***Merci pour votre lecture***