Analyse des besoins

Projet APPLI-FRAIS

Elaboré par

Yann Duffay & Louis Gautier

Promotion

2 TSSIOSR

Année scolaire

2024-2025

SOMMAIRE

I. Introduction

L'objectif de ce projet est de mettre en place une architecture technique et des fonctions de sécurisation pour une application web destinée au suivi des comptes rendus et des frais de remboursement.

Cette application sera utilisée par les visiteurs, délégués et responsables de secteur, et sera accessible en ligne via Internet ou depuis les différents sites du réseau GSB.

Les principales exigences sont l'accessibilité restreinte aux acteurs de l'entreprise via une authentification préalable et le chiffrement des échanges entre les utilisateurs et le serveur.

L'architecture réseau devra inclure des périmètres de sécurité avec cloisonnement des réseaux, filtrage des accès publics, et sécurisation des bases de données.

Le projet doit aboutir à une solution technique fonctionnelle intégrée au réseau de l'entreprise, avec des serveurs sécurisés, en DMZ ou sur le LAN, et des mécanismes de protection comme le firewall et l'authentification.

II. Analyse des Besoins et Proposition de Solutions Techniques Adaptées

Le laboratoire désire mettre à disposition des visiteurs médicaux une application Web permettant de centraliser les comptes-rendus de visite.

L'entreprise a choisi d'héberger en interne les serveurs exécutant l'application. L'achat de nouveaux équipements peut être envisagé si le besoin le justifie.

2.1. Authentification et accès sécurisé

Besoin	*Mise en place d'un service sécurisé pour la mise à jour des pages Web, accessible uniquement aux développeurs internes et restreint à l'accès interne de l'entreprise.*

Contraintes	☐ **Authentification** : Accès via une méthode sécurisée. ☐ **Accès Interne** : Limité réseau interne, inaccessible de l'extérieur. ☐ **Sécurité** : Protection contre les accès non autorisés.

Solution	Type de Serveur	Web
	Système d'exploitation	Linux
	Module	Apache

Justification	Linux	Système d'exploitation robuste, sécurisé et largement utilisé pour les serveurs Web. Il offre une stabilité élevée, une gestion efficace des ressources et une grande flexibilité.
	Apache	Serveur Web open-source très populaire et éprouvé. Il est connu pour sa stabilité, sa flexibilité et sa richesse en fonctionnalités.

Cybersécurité	Authentification et accès sécurisé
	Contrôle d'accès : Limiter l'accès aux utilisateurs autorisés seulement. *Gestion des identités et des accès (IAM) : Mise en place d'un système d'authentification centralisée, comme un annuaire Active Directory (AD).* *Multi-factor authentication (MFA) : Pour ajouter une couche supplémentaire de sécurité en plus des mots de passe.*

2.2. Chiffrement des données

Besoin	*Le chiffrement des données est essentiel pour garantir la **confidentialité** et l'**intégrité** des informations échangées dans un Système d'Information (SI). Il permet de protéger les données sensibles contre les cyber-attaques, les accès non autorisés et toute tentative de compromission.*

Contraintes	☐ **Confidentialité** : Les données sensibles doivent être protégées contre toute interception, qu'elles soient en transit ou au repos. ☐ **Intégrité** : Il est nécessaire de garantir que les données ne soient ni altérées ni modifiées lors de leur transmission ou lorsqu'elles sont stockées. ☐ **Gestion des clés de chiffrement** : Les clés utilisées pour le chiffrement doivent être stockées et gérées de manière sécurisée, avec des processus de rotation et de révocation adaptés. ☐ **Authentification des parties** : Les utilisateurs et systèmes doivent pouvoir vérifier l'identité des entités avec lesquelles ils échangent des informations.

Solution	TLS	**TLS (Transport Layer Security)** : Protéger toutes les communications entre clients et serveurs pour garantir la confidentialité des données en transit.
	Chiffrement des données	**AES-256** : Chiffrement des bases de données et des systèmes de stockage (disques, sauvegardes) pour protéger les données sensibles stockées.
	Contrôle d'accès	**A2F :** L'authentification à 2 facteurs est un solution fiable pour contrôler les accès.

Cybersécurité	Authentification et accès sécurisé
	Les données seront entièrement cryptées, transiteront en toute sécuritée et seules les personnes autorisées à accéder à ces données pourront y accéder.

2.3. Filtrage des accès et segmentation

Besoin	*Les accès aux serveurs doivent être filtrés, et plusieurs périmètres de sécurité doivent être mis en place (LAN, VLAN).*

Contraintes	☐ **Complexité de gestion** : La segmentation doit rester flexible pour permettre une gestion efficace tout en maintenant la sécurité. ☐ Garantir que les segments peuvent communiquer sans compromettre la sécurité.

Solution	Routeur pare-feu

Justification	Routeur pare-feu	**Contrôle centralisé** : Les routeurs permettent un contrôle centralisé et granulaire du trafic réseau, garantissant que seules les connexions autorisées passent entre les segments.

Cybersécurité	Filtrage des accès et segmentation
	Segmentation du réseau *: Utilisation de VLAN pour séparer les différents départements (R&D, marketing, packaging) et réduire la surface d'attaque.* ***Pare-feu et Listes de contrôle d'accès*** *: Configuration des pare-feu et des ACL pour restreindre les flux réseau uniquement aux connexions nécessaires.*

2.4. Serveur de temps et Synchronisation

Besoin	*Synchroniser toutes les machines sur le même fuseau horaire.*

Contraintes	*Si les serveurs ne sont pas synchronisés sur l'heure, il se peut qu'il y ait des soucis de communication et diverses erreurs.*

Solution	NTP

Justification	Simple	L'installation d'un serveur NTP via Windows serveur est simple.
	Suffisant	Le serveur NTP du gestionnaire de serveur Windows est amplement suffisant pour maintenir une synchronisation.

Cybersécurité	Serveur NTP
	Mettre en place un serveur NTP pour synchroniser l'horloge des serveurs, évitant ainsi la corruption des données lors des sauvegardes et des synchronisations

2.5. Sauvegarde et reprise après incident

Besoin	*Sauvegarder l'ensemble des données pour prévenir leur perte en cas de panne ou d'attaque.*

Contraintes	☐ **Fréquence des sauvegardes** : Il est crucial de définir une fréquence de sauvegarde adaptée. ☐ **Stockage sécurisé** : Les sauvegardes doivent être conservées en toute sécurité..

Solution	Sauvegarde 3-2-1 / MySQLdump

Justification	Sauvegarde 3-2-1	**Résilience accrue** : Conserver plusieurs copies sur différents supports et en incluant une sauvegarde hors site (clou), => réduit le risque de perte de données en cas de sinistre.
	MySQLDump	**Sauvegarde par script**, automatisée pour la base de données

Cybersécurité	Sauvegarde/ Reprise incident
	Mettre en place des stratégies de sauvegarde pour garantir la récupération rapide des données en cas d'incident. (Différentielle/ Incrémentielle/ Complète) **Redondance** : Mise en œuvre de systèmes de RAID, alimentation redondante, et clustering pour la continuité de service.

2.6. Intrusion Detection System (IDS/IPS)

Besoin	*Intégrer un système de détection et de prévention des intrusions (IDS/IPS).*

Contraintes	**Performance du réseau** : Le système doit être capable de fonctionner sans nuire à la performance globale du réseau. **Faux positifs** : Minimiser les alertes inutiles pour ne pas surcharger l'équipe de sécurité.

Solution	IDS/IPS

Justification	IDS	**Système IDS** : Utiliser un IDS pour surveiller le trafic réseau en temps réel et alerter sur les activités suspectes.
	IPS	**Système IPS** : Compléter avec un IPS pour non seulement détecter mais aussi bloquer les attaques en cours.

Cybersécurité	IDS/IPS
	Surveillance et détection d'intrusions : Un IDS permet de surveiller les anomalies et les tentatives d'intrusion sur le réseau. **Réaction proactive aux attaques** : L'IPS bloque automatiquement les menaces détectées avant qu'elles n'affectent les systèmes.

2.7. Accès VPN pour les visiteurs médicaux

Besoin	*Les visiteurs médicaux doivent accéder au réseau interne via un VPN sécurisé.*

Contraintes	**Sécurité des données** : Garantir que les données médicales restent protégées pendant la transmission. **Facilité d'utilisation** : L'accès VPN doit être simple à configurer et à utiliser pour les visiteurs médicaux, qui peuvent ne pas être familiarisés avec la technologie.

Solution	OpenVPN

Justification	OpenVPN	créer un tunnel sécurisé entre les dispositifs des visiteurs médicaux et le réseau de l'entreprise.

Cybersécurité	Accès VPN
	Autorisations via VPN : Le VPN limite l'accès à des services spécifiques selon les rôles des utilisateurs, et réduit la surface d'attaque externe.

2.8. Gestion des droits d'accès à la base de données

Besoin	*Permettre une gestion des accès à la base de données, avec différents niveaux de permissions selon les utilisateurs.*

Contraintes	☐ **Principes du moindre privilège** : Les utilisateurs ne doivent avoir que les droits nécessaires pour effectuer leurs tâches. ☐ **Conformité réglementaire** : Respecter les normes et réglementations sur la protection des données (ex. RGPD).

Solution	**Authentification multifactorielle** (MFA) : Exiger une validation supplémentaire (ex: A2F) pour accéder à la base de données.

Justification	MFA	**Renforcement de la sécurité** : L'ajout d'une couche d'authentification supplémentaire réduit considérablement les risques d'accès non autorisé, même si un mot de passe est compromis.

Cybersécurité	Continuité de service
	Contrôle d'accès basé sur les rôles : Accorder des permissions spécifiques aux utilisateurs en fonction de leur rôle.

2.9. Continuité de service

Besoin	*Proposer une solution pour garantir la continuité des services en cas de panne.*

Contraintes	☐ **Temps de récupération** : Minimiser le temps nécessaire pour rétablir les services après un incident.

Solution	**Plan de reprise d'activité (PRA)** : Élaborer un PRA détaillant les étapes à suivre en cas d'incident majeur pour rétablir les services rapidement. **Redondance des systèmes** : Mettre en place des systèmes redondants pour assurer un basculement en cas de défaillance.

Justification	PRA	**Préparation proactive** : Avoir un plan en place permet de réagir rapidement face à des incidents, réduisant ainsi les temps d'arrêt et les pertes financières.
	Redondance	**Disponibilité continue** : Les systèmes redondants assurent que, même en cas de défaillance d'un composant, les services restent disponibles, garantissant ainsi une expérience utilisateur fluide.

Cybersécurité	Continuité de service
	***Haute disponibilité** : Utilisation de mécanismes de répartition de charge et de redondance des systèmes serveurs pour éviter les interruptions de service*

2.10. Protection contre les attaques externes

Besoin	*Protéger l'application contre les attaques malveillantes venant de l'extérieur.*

Contraintes	☐ **Impact sur la performance** : Les solutions de sécurité ne doivent pas nuire aux performances des systèmes.

Solution	Solutions anti-DDoS

Justification	Solutions anti-DDoS	**Continuité des services** : En utilisant des solutions anti-DDoS, l'entreprise peut maintenir la disponibilité de ses services même en cas d'attaques massives, protégeant ainsi sa réputation et ses revenus.

Cybersécurité	Attaques externes
	Protection DDoS *: Mise en place de stratégies pour atténuer les attaques par déni de service distribué (DDoS).* ***Segmentation du réseau*** *: Diviser le réseau en segments pour limiter l'impact potentiel d'une attaque.*

2.11. Mise à jour des systèmes

Besoin	*Assurer que les systèmes et applications soient régulièrement mis à jour pour corriger les vulnérabilités.*

Contraintes	☐ **Planification des mises à jour** : Les mises à jour doivent être planifiées pour minimiser l'impact sur les utilisateurs et les opérations. ☐ **Tests préalables** : Tester les nouvelles versions dans un environnement de développement pour éviter les dysfonctionnements en production.

Solution	Type de Serveur	WSUS
	Système d'exploitation	Windows

Justification	Windows	**Compatibilité** : WSUS est conçu pour les environnements Windows, assurant une intégration fluide. **Support** : Windows offre un support continu et des mises à jour régulières, garantissant la stabilité et la sécurité.
	WSUS	**Centralisation des mises à jour** : WSUS permet de gérer les mises à jour à partir d'un point unique. **Contrôle du déploiement** : Les administrateurs peuvent planifier et tester les mises à jour avant déploiement, garantissant ainsi une application cohérente.

Cybersécurité	Mise à jour des systèmes
	Surveillance des vulnérabilités : Utiliser des outils de surveillance pour détecter les vulnérabilités et les mises à jour critiques nécessaires. *Automatisation des mises à jour => Gain de sécurité si Urgence*