Cahier des charges Gestion Horizons

Sommaire

1. Présentation du projet

1.1 Contexte

Le cabinet « Gestion Horizons », spécialisé dans le conseil financier, souhaite moderniser et sécuriser son infrastructure informatique afin de protéger efficacement ses données sensibles.

Les associés sont conscients des risques liés à la cybersécurité et se demandent comment sécuriser leurs informations contre les cyberattaques, les pertes de données et les accès non autorisés.
Ils souhaitent également mettre en place un système de sauvegarde fiable afin d'éviter toute perte d'informations critiques en cas d'incident.

Par ailleurs, ils expriment le besoin d'une accessibilité fluide et sécurisée : leurs données doivent être consultables aussi bien sur PC que sur téléphone, que ce soit au bureau ou à distance.

Enfin, les associés envisagent d'encadrer l'utilisation de leur infrastructure informatique, mais ne savent pas par où commencer. Ils recherchent donc des conseils pour établir des règles d'usage et des contrôles efficaces afin d'assurer un cadre sécurisé et conforme aux bonnes pratiques.

1.2 Objectifs

L'objectif principal de ce projet est de mettre en place une architecture réseau sécurisée et performante pour le cabinet « Gestions Horizons », en répondant aux besoins spécifiques des associés en matière de sécurité, accessibilité et gestion informatique.

Objectifs généraux :

- Sécuriser les données sensibles du cabinet contre les cyberattaques et les accès non autorisés.
- Garantir la disponibilité des informations, que ce soit en local ou à distance, sur PC comme sur mobile.
- Mettre en place un système de sauvegarde fiable pour prévenir toute perte de données.
- Encadrer et structurer l'usage de l'informatique en définissant des règles et des bonnes pratiques.

Objectifs techniques :

- Implémenter un réseau sécurisé, segmenté et protégé par un pare-feu adapté
- Configurer des accès sécurisés (VPN, authentification multi-facteurs, contrôle des droits d'accès) pour permettre le travail à distance en toute sûreté.
- Déployer une solution de sauvegarde automatisée, locale et sur un cloud sécurisé, avec des restaurations rapides en cas d'incident.
- Mettre en place des outils de supervision et de monitoring pour détecter et prévenir les menaces.
- Élaborer une politique informatique claire, incluant des règles d'utilisation et des restrictions adaptées aux besoins des associés.

Ces actions permettront au cabinet d'améliorer la sécurité, la flexibilité et l'efficacité de son infrastructure informatique tout en assurant une gestion simplifiée.

2. Périmètre fonctionnel

Le périmètre fonctionnel définit les fonctionnalités et services couverts par le projet de mise en place de l'architecture réseau sécurisée du cabinet « Gestion Horizons ».

2.1 Fonctionnalités principales

Infrastructure réseau

- Mise en place d'un pare-feu Pfsense pour la gestion du réseau et la sécurisation des accès.*Voir annexe 1 schéma réseau*.
- Déploiement et renouvellement de l'antivirus CrowdStrike pour 10 postes.
- Mise en place d'un serveur AD DS pour :
    - La gestion du domaine et des authentifications.
    - La création et gestion des utilisateurs.
    - Le stockage et partage des fichiers via un serveur dédié.
- Mise en place de Mailinblack pour sécuriser la messagerie contre le spam, le phishing et les malwares.

Sauvegarde et stockage

- Mise en place d'un serveur de sauvegarde avec :
    - Next cloud pour la synchronisation et l'accès aux fichiers.
    - Un script de sauvegarde automatisé.

- Plan de sauvegarde :
    - Sauvegarde complète chaque dimanche.
    - Sauvegarde incrémentale du lundi au samedi.

Accès distant et mobilité

- Mise en place d'un VPN OpenVPN pour un accès sécurisé à distance via PC et mobile.
- Configuration du Wi-Fi invité (Guest) avec un réseau isolé des ressources internes.

Formation et sensibilisation

- Organisation de stages de sensibilisation aux bonnes pratiques en cybersécurité.
- Formation des employés sur l'utilisation de la nouvelle infrastructure (VPN, stockage, AD DS).

2.2 Contraintes et exclusions

Inclus dans le périmètre :

- Installation, configuration d'open vpn via Pfsense.
- Déploiement des serveurs et solutions de sauvegarde.
- Configuration et sécurisation du VPN et des emails.
- Formation et sensibilisation des employés.

Exclus du périmètre :

- Gestion des connexions personnelles et appareils non sécurisés.
- Développement d'outils ou logiciels sur mesure (hors paramétrage des solutions existantes).

3. Contraintes techniques

L'architecture réseau doit intégrer et optimiser l'infrastructure existante tout en assurant une meilleure sécurisation et gestion des ressources.

Matériel et infrastructure actuelle :

- 1 routeur (box Internet) → Doit être intégré derrière le pare-feu Pfsense pour sécuriser l'ensemble du réseau.
- 5 PC portables → Sécurisés avec Antivirus CrowdStrike.

- 5 téléphones portables → Accès via VPN OpenVPN pour la connexion à distance et via le Wi-Fi sécurisé en local.

- 1 imprimante

- Antivirus CrowdStrike à déployer ou renouveler sur les 5 PC et téléphones pour protéger contre les menaces.

- Mise en place d'un serveur Active Directory (AD DS) pour gérer les comptes utilisateurs et les droits d'accès.

- Authentification multi-facteurs (MFA) pour renforcer la sécurité des accès distants et sensibles.

- Sécurisation de la messagerie avec Mailinblack pour bloquer le phishing et les malwares.

Sauvegarde et stockage :

- Next cloud pour un accès distant aux fichiers depuis PC et mobile.
- Serveur de sauvegarde avec script :
    - Sauvegarde complète tous les dimanches.
    - Sauvegarde incrémentale du lundi au samedi.

Accès distant et mobilité :

- VPN OpenVPN pour un accès sécurisé aux ressources internes depuis les PC et mobiles des employés.
- Borne Wi-Fi Guest pour les visiteurs, isolée du réseau interne.

4. Exigences de performance

Temps de réponse du réseau : inférieur à 2 secondes pour l'accès aux fichiers et services internes.
Capacité réseau : doit pouvoir gérer jusqu'à 100 utilisateurs simultanés sans ralentissement.
Stockage : support de 10 000 fichiers et accès fluide via Next cloud.
Disponibilité :

- Service accessible 24/7 avec une tolérance aux pannes grâce aux sauvegardes régulières.
- Supervision du réseau pour détecter toute anomalie ou tentative d'intrusion.

5. Planning prévisionnel

Puisque certains équipements sont déjà en place, le projet se concentrera principalement sur la sécurisation, l'optimisation et la formation. Voici un planning adapté :

Phase	**Durée**	**Description**
Analyse des besoins	2 semaines	Audit du réseau actuel, validation des équipements existants et identification des mises à jour nécessaires.
Développement	6 semaines	Installation et configuration des nouvelles solutions : **pare-feu Pfsense, AD DS, VPN, Mailinblack, Next cloud**.
Tests et corrections	3 semaines	Vérification des performances, tests de **sécurité, VPN, sauvegarde et accès distant**.
Déploiement et formation	2 semaines	Mise en production et **formation des employés** sur la nouvelle infrastructure et les bonnes pratiques en cybersécurité.

(Voir Annexe 2)

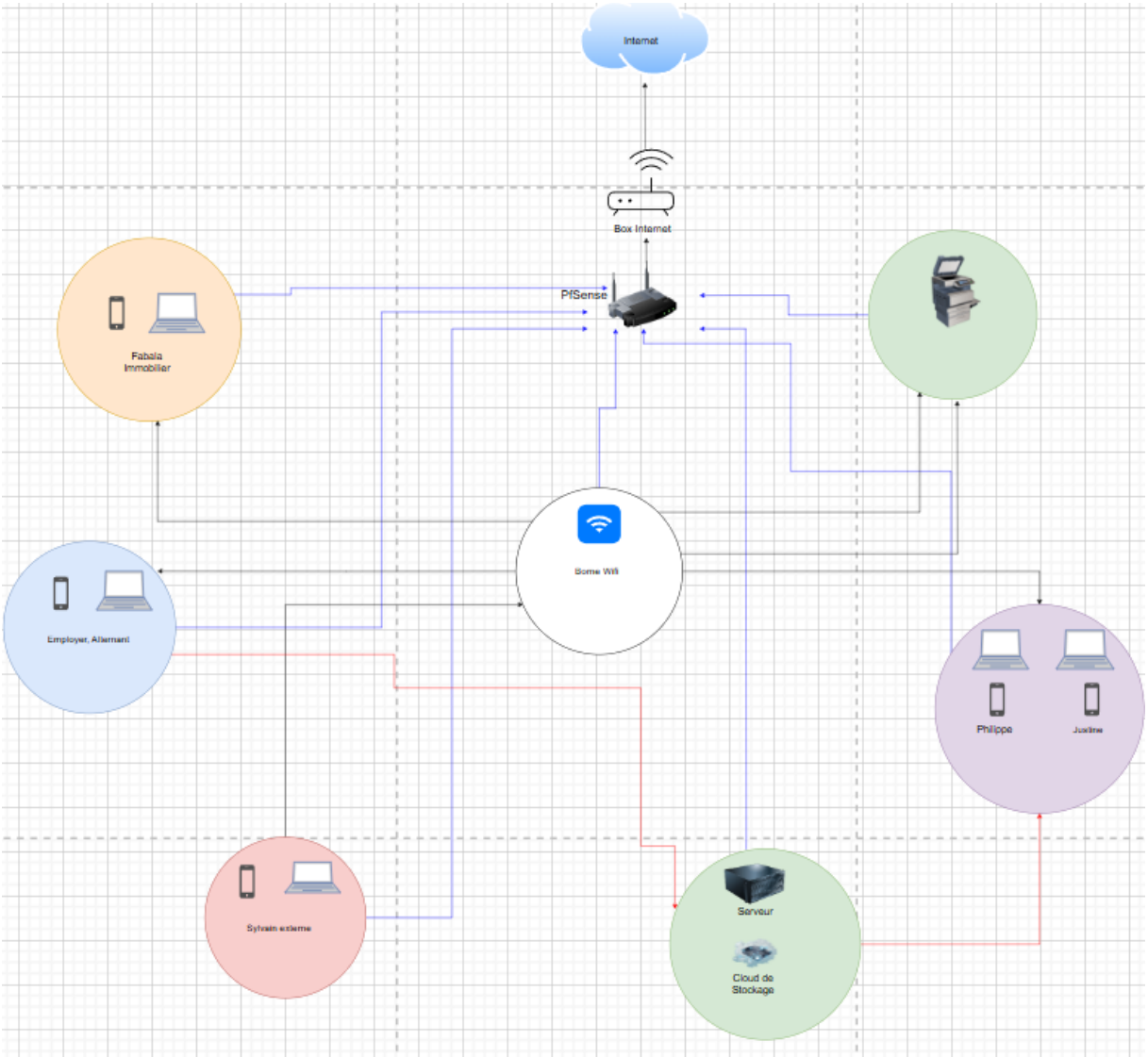
6. Budget prévisionnel

Devis :

Produits / Services	Quantité	Prix TTC	Marge appliquée (%)	Prix final
Matériel et licences				
Disque dur SATA Seagate	3	570 €	15%	655.50 €
Borne Wifi (Guest)	1	179 €	15%	205.85 €
Serveur	1	1,499.00 €	15%	1,723.85 €
Antivirus Crowdstrike	10	572.60 €	15%	658.49 €
VPN SonicWall	10	380 €	15%	436.43 €
Mailinblack	10	30 €	15%	**34.50 €**
Sous-total Matériel et Logiciels				3,714.62 €
Prestations de service				
Stages de sensibilisation	2H	192 €	-	192 €
Formation	1H	96 €	-	**96.00 €**
			Total =	4,002.62 €

Annexe

Annexe 1 Schéma Réseau :



Annexe 2 Diagramme de Gantt :