Cahier des Charges Fonctionnel

Infrastructure Système et Réseau Sécurisée

Entreprise ITWay SAS

28 novembre 2024

Table des matières

1 Introduction

1.1 Contexte

L'entreprise ITWay souhaite mettre en place une infrastructure système et réseau sécurisée pour répondre à ses besoins opérationnels actuels et futurs. Cette infrastructure est destinée à remplacer l'infrastructure actuelle qui n'est pas optimisée et ne respecte pas l'état de l'art en termes d'efficacité, d'accessibilité et de sécurité en environnement professionnel.

1.2 Objectifs du Projet

- **Concevoir une infrastructure sécurisée** intégrant des services essentiels pour l'entreprise.
- **Assurer la sécurité** des données, des communications et des accès.
- **Faciliter le déploiement, la maintenance et l'évolution** de l'infrastructure grâce à des solutions modernes.
- **Adopter une approche écoresponsable** en privilégiant des solutions légères, efficaces et économes en ressources.
- **Intégrer des technologies innovantes** pour anticiper les besoins futurs et améliorer continuellement la sécurité.
- **Prendre en compte le handicap** en garantissant l'accessibilité des éléments destinés au public.

2 Présentation Générale du Projet

2.1 Architecture Générale

L'architecture réseau se compose à minima de trois segments principaux :

- **Réseau SRV** : héberge les serveurs internes sensibles, non accessibles directement depuis l'extérieur.
- **Réseau DMZ** : zone tampon qui héberge les serveurs devant être accessibles depuis l'extérieur, avec des contrôles de sécurité stricts.
- **Réseau LAN** : réseau local interne pour les postes clients et les utilisateurs finaux.

Chaque segment réseau dispose de sa propre plage d'adresses IP pour faciliter la gestion, renforcer la sécurité et assurer une segmentation efficace.

3 Exigences Fonctionnelles

3.1 Composants de l'Infrastructure

3.1.1 Gestion des Identités et des Accès

Gestion des Utilisateurs et des Groupes

- **Gestion centralisée des accès** : L'entreprise a besoin d'un système permettant de créer, gérer et supprimer les comptes utilisateurs de manière centralisée. Ce système doit offrir une gestion fine des droits d'accès en fonction des rôles et des départements au sein de l'organisation.
  - **Équipe informatique** : Doit disposer des permissions nécessaires pour administrer l'ensemble de l'infrastructure.
  - **Personnel interne** : Les employés doivent avoir accès aux ressources nécessaires à leur travail, tout en respectant le principe du moindre privilège.
  - **Partenaires et prestataires** : Des accès temporaires ou restreints doivent être possibles pour des utilisateurs externes, avec des droits limités aux seules ressources nécessaires.
- **Itinérance des profils** : Les utilisateurs doivent pouvoir se connecter depuis n'importe quel poste de travail de l'entreprise et retrouver leurs paramètres personnalisés, leurs documents et leurs applications.
- **Politiques de sécurité des mots de passe** : Le système doit appliquer des politiques de mots de passe robustes (complexité, expiration, historique) pour garantir la sécurité des comptes utilisateurs.

Partage et Gestion des Fichiers

- **Stockage centralisé** : Les documents et fichiers de l'entreprise doivent être stockés de manière centralisée pour faciliter l'accès, la sauvegarde et la gestion des droits.
- **Contrôle d'accès** : L'accès aux documents doit être contrôlé en fonction des droits des utilisateurs, avec la possibilité de définir des dossiers partagés entre plusieurs équipes ou départements.
- **Gestion des quotas** : Il doit être possible de définir des quotas de stockage pour chaque utilisateur ou groupe afin de gérer efficacement l'espace disque disponible.
- **Sécurité des fichiers** : Le système doit prévenir le stockage de fichiers potentiellement dangereux (par exemple, fichiers contenant des malwares) et assurer l'intégrité des données.

Sécurité des Communications

- **Chiffrement des données** : Toutes les communications internes de l'entreprise doivent être sécurisées par chiffrement pour protéger les informations sensibles.
- **Authentification sécurisée** : Les méthodes d'authentification doivent garantir l'identité des utilisateurs et prévenir les accès non autorisés.
- **Intégrité des données** : Assurer que les données ne peuvent pas être altérées ou interceptées lors des transmissions.

3.1.2 Accès Distant et Mobilité

Accès Sécurisé depuis l'Extérieur

- **Télétravail** : Les employés doivent pouvoir accéder aux ressources de l'entreprise depuis l'extérieur de manière sécurisée, tout en respectant les politiques de sécurité internes.
- **Accès pour les partenaires** : Permettre à des utilisateurs externes (prestataires, clients) d'accéder à certaines ressources spécifiques de l'entreprise de manière contrôlée et sécurisée.
- **Contrôle des connexions** : Le système doit être capable de gérer et de surveiller les connexions à distance pour assurer la sécurité et la conformité.

Authentification Unifiée

- **Gestion unique des identifiants** : Les utilisateurs doivent pouvoir utiliser un seul jeu d'identifiants pour accéder à l'ensemble des services et applications de l'entreprise, réduisant ainsi la complexité et améliorant la sécurité.
- **Synchronisation des droits** : Toute modification des droits d'un utilisateur doit être répercutée automatiquement sur l'ensemble des services et applications.

3.1.3 Services de Communication Internes et Externes

Messagerie Électronique

- **Communication efficace** : Mettre en place un système de messagerie performant pour faciliter les communications internes et externes de l'entreprise.
- **Sécurité des e-mails** : Protéger les communications par e-mail contre les spams, les logiciels malveillants et les tentatives d'hameçonnage.
- **Accès à la messagerie** : Offrir aux utilisateurs la possibilité d'accéder à leur messagerie via différents moyens, y compris une interface web sécurisée accessible de l'intérieur comme de l'extérieur.

Site Internet et Intranet

- **Présence en ligne** : L'entreprise souhaite disposer d'un site web public pour présenter ses activités, ses produits et services.
- **Intranet pour les employés** : Mettre en place un intranet pour partager des informations aux employés, cet intranet ne sera accessible qu'aux salariés de l'entreprise.
- **Sécurité et fiabilité** : Les sites web doivent être sécurisés, disponibles et performants, tout en offrant une expérience utilisateur de qualité.

3.1.4 Gestion de l'Infrastructure

Gestion des Configurations

- **Automatisation des déploiements** : Automatiser le déploiement et la configuration des systèmes pour assurer la cohérence, réduire les erreurs humaines et gagner en efficacité.
- **Gestion des changements** : Mettre en place des processus formalisés pour gérer les modifications de l'infrastructure, avec des approbations et des validations appropriées.
- **Documentation** : Maintenir une documentation à jour des configurations et des procédures pour faciliter la maintenance et les futures évolutions.

3.1.5 Résolution de Noms et Gestion des Certificats

Service de Résolution de Noms

- **Gestion des domaines** : Assurer la résolution des noms de domaine internes et externes de l'entreprise pour le bon fonctionnement des services.

— **Fiabilité et performance** : Le service de résolution de noms doit être hautement disponible et offrir des temps de réponse optimisés.
— **Sécurité** : Protéger le service contre les attaques et assurer l'intégrité des informations fournies.

Gestion des Certificats

— **Sécurisation des communications** : Chiffrer les communications entre les utilisateurs et les services de l'entreprise.
— **Autorité de certification interne** : Mettre en place une autorité de certification interne pour délivrer et gérer les certificats nécessaires aux services et applications internes.
— **Gestion du cycle de vie des certificats** : Assurer l'émission, le renouvellement et la révocation des certificats de manière efficace et sécurisée.

3.2 Exigences de Performance et de Disponibilité

— **Disponibilité des services** : Les services critiques de l'entreprise doivent être disponibles en permanence, avec un objectif de temps d'indisponibilité minimal.
— **Performances optimales** : Les systèmes doivent offrir des performances adaptées aux besoins, avec des temps de réponse rapides et une capacité à gérer les charges de travail prévues.
— **Évolutivité** : L'infrastructure doit pouvoir évoluer pour supporter une augmentation du nombre d'utilisateurs, de données ou de services sans nécessiter une refonte complète.
— **Redondance et tolérance aux pannes** : Mettre en place des mécanismes de redondance pour assurer la continuité des services en cas de défaillance matérielle ou logicielle.

3.3 Conformité et Éthique

— **Conformité réglementaire** : L'infrastructure doit respecter les lois et réglementations en vigueur, notamment en matière de protection des données personnelles (par exemple, RGPD).
— **Respect de la vie privée** : Garantir la confidentialité et l'intégrité des données des utilisateurs et de l'entreprise.
— **Approche écoresponsable** : Privilégier des solutions respectueuses de l'environnement, en optimisant l'utilisation des ressources énergétiques et matérielles.

4 Phases du Projet et Évaluations

Le projet est divisé en trois phases majeures, chacune avec des objectifs précis, des livrables attendus et des critères d'évaluation spécifiques. Ces phases sont conçues pour vous guider à travers un processus complet de conception, de mise en œuvre et d'amélioration d'une infrastructure système et réseau sécurisée. Chaque phase dispose d'une deadline qui vous sera communiquée en cours.

4.1 Phase 1 : Analyse du Cahier des Charges

4.1.1 Objectifs

- **Compréhension du Cahier des Charges** : Lire attentivement et comprendre les besoins et les contraintes exprimés.
- **Étude des Solutions** :
  - Comparer les avantages et inconvénients des technologies d'automatisation, de virtualisation et de conteneurisation par rapport à une infrastructure classique en considérant les aspects réglementaires, de conformité et d'impact environnemental.
  - Mettre en avant les avantages écologiques et d'évolutivité des solutions légères.
  - Prendre en compte le handicap en proposant des solutions permettant l'accessibilité des services fournis.
- **Identification des Risques** :
  - Identifier les menaces et vulnérabilités potentielles.
  - Évaluer les risques associés à chaque composant de l'infrastructure.
- **Conception Préliminaire** :
  - Proposer une maquette répondant aux besoins fonctionnels en démontrant la mise en œuvre d'une infrastructure permettant de commencer à produire des conteneurs et des machines virtuelles, en assurant une communication sécurisée entre les différents éléments, respectant les bonnes pratiques en termes de sécurité.
- **Plan de Sécurité** :
  - Élaborer un plan de sécurisation intégrant les principes de "Security by Design".
  - Préconiser des évolutions du cahier des charges si nécessaire pour améliorer la sécurité.
- **Gestion de Projet** :
  - Mettre en place des outils collaboratifs (par exemple, gestion de versions, tableaux de bord).
  - Définir les rôles et responsabilités de chaque membre de l'équipe.
  - Établir un calendrier réaliste avec des jalons et des livrables.

4.1.2 Livrables

- **Rapport d'Analyse** :
  - Document détaillant l'étude des solutions, l'analyse des risques, la conception préliminaire et le plan de sécurité.
- **Plan de Gestion de Projet** :
  - Document présentant l'organisation de l'équipe, le calendrier, les outils utilisés, etc.

4.1.3 Évaluation

- **Travail en Équipe** :
  - Capacité à collaborer efficacement, à communiquer et à gérer les conflits.
- **Contribution Individuelle** :
  - Implication personnelle, qualité des tâches réalisées, respect des délais.
- **Qualité des Livrables** :
  - Clarté, précision et exhaustivité de la documentation.
- **Présentation Orale** :
  - Capacité à présenter le travail de manière structurée, à répondre aux questions du jury.

4.2 Phase 2 : Conception, Développement, Déploiement et Maintenance

4.2.1 Objectifs

- **Choix des Technologies** :
  - Sélectionner les outils, technologies et langages appropriés pour chaque composant (par exemple, choix du serveur web, du SGBD, etc.).
- **Développement des Services** :
  - Concevoir et implémenter les services requis, en respectant les bonnes pratiques de conception et de développement.
- **Sécurité Intégrée** :
  - Appliquer les principes de sécurité dès la phase de conception (par exemple, compartimentage des réseaux, gestion des droits d'accès).
- **Tests et Recettes** :
  - Élaborer des plans de tests couvrant les aspects fonctionnels et non fonctionnels.
  - Réaliser des tests unitaires, d'intégration et des tests de sécurité (par exemple, tests de vulnérabilité).
- **Déploiement en Production** :
  - Mettre en place l'environnement de production en respectant les procédures établies.
  - Documenter le processus de déploiement pour faciliter les futures opérations.
- **Maintenance** :
  - Établir des procédures pour la maintenance corrective et évolutive.
  - Prévoir des mécanismes de sauvegarde et de restauration.

4.2.2 Livrables

- **Documentation Technique** :
  - Spécifications détaillées, manuels d'installation, guides d'utilisation.
- **Codes Sources et Configurations** :
  - Fournir tous les scripts, configurations et codes nécessaires à la reproduction de l'infrastructure.
- **Plans de Tests et Rapports** :
  - Documentation des tests effectués, des résultats et des actions correctives.
- **Procédures de Maintenance** :
  - Guides détaillés pour la maintenance quotidienne et les mises à jour.

4.2.3 Évaluation

- **Travail en Équipe** :
  - Coordination efficace, respect des rôles et responsabilités.
- **Contribution Individuelle** :
  - Qualité du travail fourni, capacité à résoudre les problèmes rencontrés.
- **Qualité des Livrables** :
  - Fonctionnalité des services, conformité aux spécifications, qualité du code.
- **Présentation Orale** :
  - Capacité à expliquer les choix techniques, à démontrer le fonctionnement des services.

4.3 Phase 3 : Modernisation et Sécurisation de la Solution

4.3.1 Objectifs

- **Étude des Technologies Innovantes** :
  - Rechercher et analyser des solutions de sécurité avancées (par exemple, SIEM, centralisation des journaux, solutions de surveillance en temps réel).
- **Adaptation de l'Architecture** :
  - Intégrer les nouveaux éléments de sécurité de manière cohérente avec l'architecture existante.
  - S'assurer que les modifications respectent les réglementations et bonnes pratiques de sécurité.
- **Renforcement de la Sécurité** :
  - Mettre en œuvre des mesures supplémentaires (par exemple, durcissement des configurations, surveillance active).
- **Sensibilisation des Utilisateurs** :
  - Créer du matériel éducatif pour informer les utilisateurs et les équipes techniques sur les bonnes pratiques de sécurité et les raisons des mesures mises en place.

4.3.2 Livrables

- **Rapport d'Étude** :
  - Document détaillant les technologies étudiées, les critères de sélection, les avantages attendus.
- **Documentation Technique Mise à Jour** :
  - Décrire les modifications apportées, les nouvelles configurations, les procédures associées.
- **Matériel de Sensibilisation** :
  - Guides, notes, présentations pour les utilisateurs finaux et les équipes techniques.

4.3.3 Évaluation

- **Travail en Équipe** :
  - Capacité à intégrer les contributions de chacun, à innover collectivement.
- **Contribution Individuelle** :
  - Implication dans la recherche, la mise en œuvre et la documentation.
- **Qualité des Livrables** :
  - Pertinence des solutions proposées, clarté de la documentation.
- **Présentation Orale** :
  - Capacité à convaincre de la valeur ajoutée des améliorations, à communiquer efficacement en sachant vulgariser les technologies mises en œuvre.

5 Consignes Générales

— N'attendez pas les regroupements pour commencer le travail ; il sera largement trop tard !
— Prenez le temps de définir un rétroplanning.
— Les séances au centre sont dédiées à assembler toutes les pièces du projet entre elles, à organiser des réunions d'équipe et à décortiquer les éventuelles problématiques techniques avec l'enseignant.
— Ce projet n'est pas réalisable facilement seul, mais est relativement facilement réalisable si l'ensemble des tâches est défini, que chaque tâche est affectée à l'un d'entre vous, et que vous communiquez très régulièrement (en tenant trace des échanges) sur l'avancée du projet.
— Ce projet nécessite des recherches, de l'expérimentation, et doit débuter en travail personnel dès distribution du sujet.
— Je ne m'attends pas à ce que tout fonctionne parfaitement le jour J.
— Je m'attends à ce que vos livrables prouvent que vous avez cerné le sujet, que vous savez ce que vous faites, ce qui est différent de "ça fonctionne grâce à un tuto, mais je n'ai pas idée de ce que je suis en train de faire".