

Projet Final JobInTech Cybersécurité : Infrastructure Réseau et Sécurité

1. Introduction et Contexte

AtlasTech Solutions est une entreprise fictive en pleine croissance opérant spécialisée dans les services numériques et le développement web. L'entreprise propose des packs de développement web (sites vitrines, e-commerce, maintenance, hébergement) à destination de PME.

Face à l'augmentation du nombre de clients et à la sensibilité croissante des données manipulées (données clients, ressources humaines, informations financières et code source des applications web), la direction a décidé de revoir entièrement son infrastructure informatique.

Face à la croissance de l'activité commerciale et à l'augmentation des exigences de sécurité, la direction a décidé de revoir l'infrastructure réseau et applicative afin d'améliorer la sécurité, la disponibilité et la fiabilité des services.

Présentation de l'Entreprise

- **Nom de l'entreprise : AtlasTech Solutions**
- **Secteur d'activité : Services numériques et développement web**
- **Effectif total : 25 employés**
- **Objectif principal : Mise en place d'une infrastructure sécurisée, fiable et évolutive**

2. Objectifs du Projet

Les objectifs principaux de ce projet sont :

- **Héberger une application web principale de vente de packs de développement web.**
- **Déployer une application web CRUD dédiée au département RH.**
- **Sécuriser les communications web via HTTPS (Apache + TLS).**
- **Mettre en place une gestion de code avec GitHub ou GitLab.**
- **Introduire des pratiques DevOps (CI, versioning).**
- **Identifier les faiblesses de sécurité initiales.**
- **Proposer une infrastructure améliorée.**

AtlasTech Solutions fournit des solutions web à des PME (Petites et Moyennes Entreprises) et gère des données sensibles nécessitant un haut niveau de sécurité et de disponibilité.

Organisation de l'Entreprise

Répartition des Départements

Département	Nombre d'employés	Rôle principal
Direction Générale	1	Pilotage stratégique
Informatique (IT)	3	Administration systèmes et réseaux
Développement	6	Développement et maintenance applicative
Ressources Humaines	3	Gestion du personnel
Finance / Comptabilité	3	Gestion financière et facturation
Commercial & Marketing	8	Gestion clients et activités commerciales

Rôles et Accès aux Systèmes

Rôle	Type de poste	Accès serveurs Linux	Accès application web	Accès application CRUD	Accès documentation IT
Directeur Général (CEO)	Windows	Non	Oui	Oui (Accès limité)	Non
Administrateurs IT	Windows / Linux	Oui (SSH)	Oui	Oui	Oui (IP restreinte)
Développeurs	Windows	Non	Oui	Non	Oui (accès limité)
Ressources Humaines	Windows	Non	Oui	Oui	Non
Comptabilité	Windows	Non	Oui	Non	Non
Commercial / Marketing	Windows	Non	Oui	non	Non

3. Services Applicatifs de l'Entreprise

L'infrastructure héberge **deux applications web principales** :

1. Application Web Commerciale (Application principale)

Cette application permet :

- **La présentation des services de l'entreprise**
- **La vente de packs de développement web**
- **La prise de contact avec les clients**
- **La gestion basique des commandes**

Technologies utilisées :

- **Linux**
- **Apache**
- **PHP**
- **Base de données MariaDB / MySQL**
- **Accès public via Internet**
- **Communication sécurisée via HTTPS**

2. Application Web CRUD – Ressources Humaines

Cette application est réservée au département RH et permet :

- **Ajouter un employé**
- **Modifier les informations d'un employé**
- **Supprimer un employé**
- **Consulter la liste des employés**

Technologies utilisées :

- **Linux**
- **Apache**
- **PHP**
- **MariaDB / MySQL**

Cette application est interne à l'entreprise et ne doit pas être accessible depuis Internet.

4. Infrastructure Réseau Initiale (État Actuel)

L'infrastructure initiale repose sur une architecture simple et centralisée.

Composants principaux

- Accès Internet
- Routeur jouant le rôle de pare-feu
- Switch central (Core Switch)
- Un réseau local unique (LAN)
- Serveur Linux hébergeant :
 - Apache
 - Application web commerciale
 - Application web CRUD RH
 - Base de données clients
 - Base de données RH
- Serveur de sauvegarde
- Postes clients Windows pour les différents départements

5. Sécurisation Web – HTTPS (Apache)

Le serveur web Apache est configuré pour utiliser le protocole **HTTPS** afin de garantir :

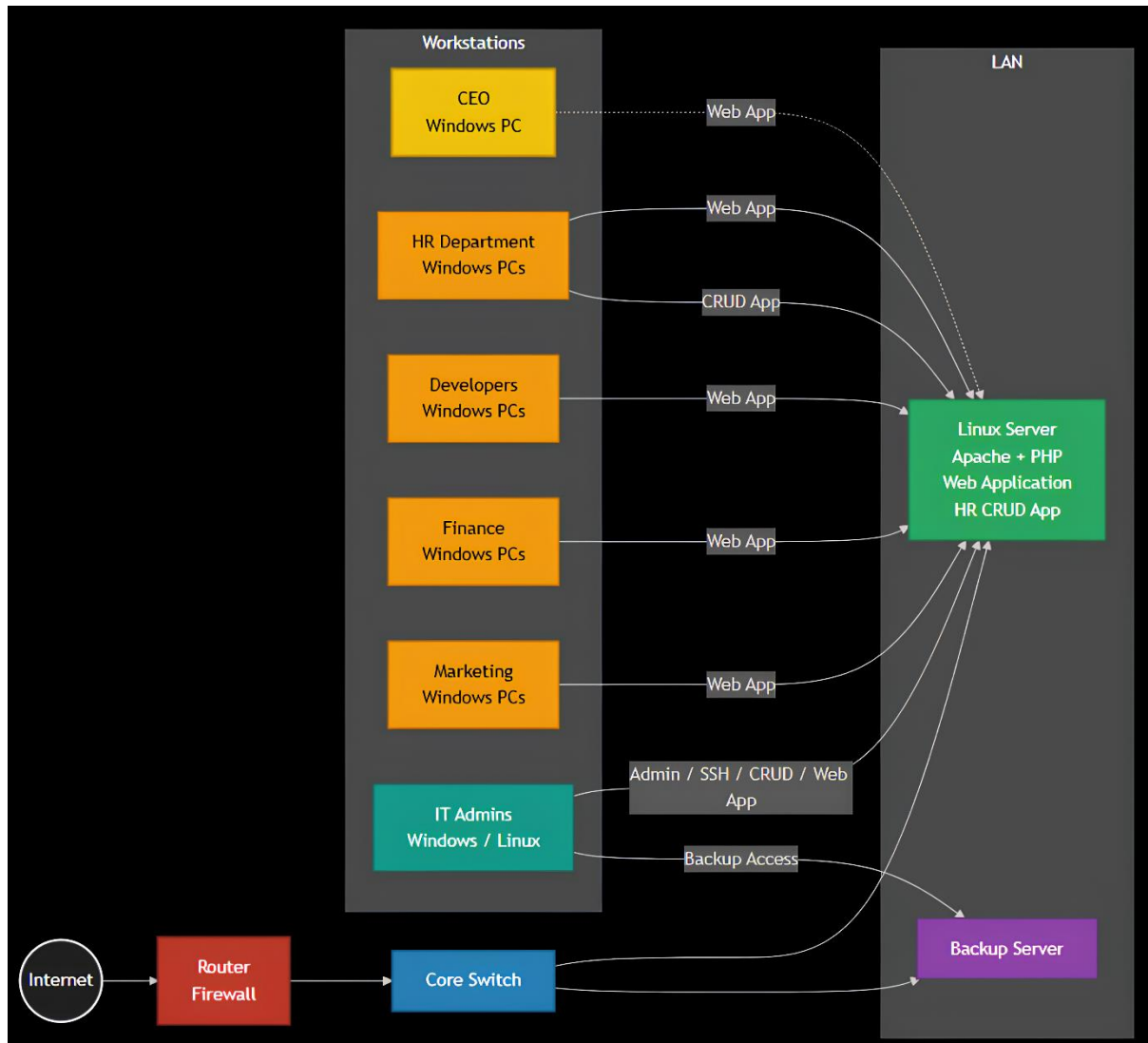
- La confidentialité des échanges
- L'intégrité des données
- L'authentification du serveur

Mesures mises en place (niveau initial)

- Certificat TLS (auto-signé ou Let's Encrypt)
- Redirection HTTP → HTTPS
- Chiffrement des communications web

Cette configuration constitue une **première étape de sécurisation**, mais reste perfectible.

6. Schéma de l'Infrastructure Initiale



Ce schéma représente l'infrastructure initiale avant toute amélioration de sécurité avancée.

7. Analyse de l'Infrastructure Initiale (Travail Demandé)

À partir du schéma de l'infrastructure initiale et de la description technique fournie, les étudiants devront analyser l'architecture existante et identifier les faiblesses et les risques de sécurité.

Cette analyse devra porter notamment sur :

- L'organisation du réseau
- La gestion des accès
- L'exposition des services
- L'hébergement des applications web

- La protection des données
- La configuration des services web (Apache / HTTPS)

Les étudiants devront :

- Identifier les **failles potentielles** de l'infrastructure initiale
- Expliquer les **risques associés** (confidentialité, intégrité, disponibilité)
- Illustrer les problèmes identifiés à l'aide de schémas ou d'exemples
- Justifier leurs observations de manière argumentée

8. Gestion du Code et DevOps (GitHub / GitLab)

L'application web principale doit être gérée via un dépôt GitHub ou GitLab.

Contenu du dépôt

- Code source de l'application commerciale
- Documentation
- Fichier README.md

9. Évolution de l'Infrastructure (Travail Demandé)

Les étudiants devront proposer une **infrastructure améliorée**, incluant, mais pas limité à :

- Segmentation réseau par VLAN
- Mise en place d'une DMZ pour l'application web commerciale
- Isolation de l'application RH
- Accès restreint à la base de données
- Règles de pare-feu strictes
- Durcissement HTTPS (TLS, headers de sécurité)
- Application du principe du moindre privilège

Objectif Global du Projet

Ce projet vise à démontrer la capacité des étudiants à :

- Mettre en place une infrastructure réseau fonctionnelle
- Appliquer des mesures de sécurité réalistes
- S'aligner sur les principes de la norme ISO/IEC 2700X
- Documenter et justifier chaque choix technique