**Projet : Sécurisez le réseau d'une grande entreprise**

**Table des matières**

[**Plan-Projet : Sécurisation de l'Architecture Réseau pour une PME** 2](#_Toc177602517)

[**1.** **Introduction** 2](#_Toc177602518)

[**2.** **Étape 1 : Identification des Failles de l’Architecture Actuelle** 2](#_Toc177602519)

[**3.** **Étape 2 : Répertorier les Équipements de Sécurisation** 3](#_Toc177602520)

[**4.** **Étape 4 : Chiffrage et Planification de la Sécurisation** 3](#_Toc177602521)

[**5.** **Chiffrage des Équipements** 4](#_Toc177602522)

[**6.** **Planification de la Sécurisation** 5](#_Toc177602523)

[**a.** **Chronologie du projet** 5](#_Toc177602524)

[**b.** **Le diagramme de GANTT** 5](#_Toc177602525)

[**7.** **Conclusion** 6](#_Toc177602526)

# **Plan-Projet : Sécurisation de l'Architecture Réseau pour une PME**

## **Introduction**

Ce plan vise à sécuriser l'architecture du système d'information (SI) de l’entreprise **Open Pharma** en identifiant les failles existantes, en répertoriant les équipements nécessaires pour les combler, puis en chiffrant et en planifiant la mise en œuvre. L’objectif est de renforcer la résilience et la sécurité globale du réseau en réduisant les risques de cyberattaques, tout en assurant une continuité des services.

**Contexte :**

* PME d'environ 11 personnes.
* Budget : 10 000 €, avec l'assistance de l’équipe technique interne pour l’installation.
* Objectif : Renforcer la sécurité du réseau en réutilisant des équipements existants et en achetant des nouveaux équipements.

## **Étape 1 : Identification des Failles de l’Architecture Actuelle**

Une analyse approfondie de l'architecture actuelle a révélé plusieurs vulnérabilités et faiblesses qui nécessitent des solutions adaptées. Les failles identifiées incluent :

1. **Manque de pare-feu de nouvelle génération (NGFW)** : La sécurité périmétrique repose sur un pare-feu standard qui n’offre pas une inspection approfondie des flux applicatifs.
2. **Absence de contrôle d'accès réseau (NAC)** : Aucun dispositif ne permet de vérifier les équipements se connectant au réseau interne.
3. **Absence de VPN**: Aucune connexion sécurisée entre différents réseaux via internet.
4. **Absence de segmentation réseau** : Pas de segmentation réseau via VLANs.
5. **Absence de séparation de la couche core et la couche d’accès** : Aucun dispositif ne permet de fournir des services de routage et de sécurité avant de transmettre le trafic à la couche cœur (core) ou à l'extérieur du réseau.
6. **Manque de proxy** : Absence d’intermédiaire entre les utilisateurs et Internet, ni de filtrage pour les requêtes.
7. **L’utilisation de systèmes d’exploitation obsolètes comme Windows Server 2012 R2 et Debian 8 :** peut entraîner plusieurs vulnérabilités et risques de sécurité

## **Étape 2 : Répertorier les Équipements de Sécurisation**

Pour sécuriser notre architecture, nous avons identifié les équipements suivants pour combler les failles :



## **Étape 4 : Chiffrage et Planification de la Sécurisation**

La main d’œuvre sera facturée à hauteur de 1729 euros ce qui correspond à 133 heures de travail pour 13 euros de l’heure.

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

## **Chiffrage des Équipements**



**Coût total du projet : 9 848,88 €**

## **Planification du projet de sécurisation**

### **Chronologie du projet**

**Une image contenant texte, ligne, reçu, diagramme

Description générée automatiquement**

### **Le diagramme de GANTT**



## **Conclusion**

Ce plan de sécurisation permettra de combler les failles de l'architecture actuelle et de renforcer la sécurité globale du système d'information. Grâce à l'acquisition de nouveaux équipements et à leur mise en œuvre planifiée, nous réduirons considérablement les risques de cyberattaques et assurerons une protection continue du réseau et des données critiques. Le projet est estimé à 9 848,88 €, avec une mise en œuvre complète d’ici novembre 2024.