Cahier des charges - Projet d'interconnexion de deux cliniques

1. Introduction

Ce document présente le cahier des charges pour le projet d'interconnexion de deux cliniques chirurgicales, ainsi que la mise en place de réseaux privés virtuels (VPN) et de mesures de sécurité pour garantir la confidentialité des données médicales, administratives et de direction.

2. Objectifs du Projet

Les objectifs principaux du projet sont les suivants :

1. Interconnecter deux cliniques chirurgicales distantes au moyen d'une connexion VPN sécurisée.
2. Séparer les données en trois catégories distinctes : données administratives, données médicales et données de direction, au sein de chaque clinique. (VLAN)
3. Mettre en place une base de données sécurisée pour le stockage des informations des patients.
4. Installer des équipements de sécurité, notamment des lecteurs de badge, pour contrôler l'accès aux zones sensibles.
5. Garantir la conformité aux réglementations de protection des données et la sécurité des données des patients.

3. Contexte

Le contexte de ce projet est la mise en place d'une infrastructure informatique pour une clinique de campagne, avec un accent sur la sécurité et la gestion des données médicales. Voici les éléments clés du projet :

Base de données médicale : Le projet vise à créer une base de données médicale pour stocker les informations des patients. Cela implique de gérer l'accès aux données de manière sécurisée.

Architecture réseau : L'architecture réseau est basée sur la norme 802.1 et comprend la création de VLAN distincts. Il y a un VLAN dédié aux données administratives (pilpro), un autre VLAN pour les données médicales. De plus, un troisième VLAN de direction est établi, permettant un accès aux deux autres VLAN à partir de points spécifiques.

Infrastructure réseau : Il est nécessaire de construire et configurer une infrastructure réseau robuste pour prendre en charge la communication et la gestion des données au sein de la clinique.

Tests de pénétration : Des audits de sécurité seront réalisés pour évaluer la sécurité du réseau et identifier les vulnérabilités potentielles. Cette étape est cruciale pour s'assurer que le réseau est résistant aux attaques.

Gestion des Patients et Données Sensibles : Le projet inclut la création d'un tableau de patients contenant des informations telles que le nom, prénom, âge, et adresse. De plus, il y aura une liste de données sensibles, y compris des informations sur les opérations ou les traitements réels ou imaginaires, qu'ils soient passés, en cours, ou futurs.

VPN entre différents sites : Le projet prévoit la mise en place d'un VPN pour permettre le transfert sécurisé de patients ou de données entre différents sites. Cela implique de garantir la confidentialité et la sécurité des données pendant leur transfert.

L'objectif global est de mettre en place une infrastructure informatique sécurisée pour la clinique de campagne, en garantissant la sécurité des données médicales, la communication efficace, et la disponibilité des services, tout en prenant des mesures pour faire face aux situations imprévues.

4. Portée du Projet

Le projet englobe les éléments suivants :

1. Configuration de deux réseaux VPN pour l'interconnexion des deux cliniques.
2. Mise en place de VLAN pour la séparation des données au sein de chaque clinique.
3. Installation d'une base de données sécurisée pour stocker les informations des patients.
4. Intégration d'équipements de sécurité, tels que des lecteurs de badge, des caméras de sécurité et des systèmes de détection d'intrusion.
5. Formation du personnel aux protocoles de sécurité et aux bonnes pratiques de gestion des données.
6. Conformité aux réglementations de protection des données (le cas échéant).

7. Mise en place de stratégies de sauvegarde des données et de plan de reprise d'activité.

5. Exigences Techniques

5.1 Interconnexion VPN

- Configuration de VPN sécurisés entre les deux cliniques.
- Utilisation de chiffrement fort pour les communications VPN (par exemple, AES-256).
- Mise en place de pare-feu pour filtrer le trafic entrant et sortant.

5.2 Séparation des Données

- Création de 3 VLAN distincts pour les données administratives, médicales et de direction.
- Configuration de règles de pare-feu pour contrôler le trafic entre les VLAN.
- Mise en place de mécanismes de contrôle d'accès pour limiter l'accès aux données sensibles.

5.3 Stockage des Données des Patients

- Installation d'une base de données sécurisée pour le stockage des données des patients.
- Chiffrement des données sensibles dans la base de données.
- Mise en place de contrôles d'accès stricts à la base de données.

5.4 Équipements de Sécurité

- Installation de lecteurs de badge pour contrôler l'accès aux zones sensibles.
- Mise en place de caméras de sécurité pour la surveillance des locaux.
- Mise en place de capteur intelligent pour la sécurité de l’installation.
- Configuration de systèmes de détection d'intrusion pour alerter en cas d'intrusions non autorisées. (Décidément on en a prévu des choses mdr)

5.5 Conformité Légale

- Assurer la conformité aux réglementations locales de protection des données, le cas échéant.
- Gestion appropriée de l'accès aux données médicales conformément à la réglementation applicable.

5.6 Formation du Personnel

- Formation du personnel à l'utilisation des VPN, à la sécurité des données et à l'accès sécurisé aux zones sensibles.

5.7 Sauvegarde

- Élaboration d'une stratégie de sauvegarde régulière des données critiques.

6. Calendrier

Le projet devra être achevé dans un délai de deux semaines.

7. Équipe de Projet

- Himmi Adam - Chef de Projet
- Ecotiere Léo - Administrateur réseaux
- Hirsch Matéo - Administrateur réseaux
- Loureiro Hugo - Administrateur réseaux
- Deuscher Lucas - Responsables de la mise en œuvre technique