

Anisse FOUKA ; Mourad AMGHAR ;  
Mehdi BERRADA ; Altay CEVIK

## Rapport technique :

Réseau d'hôpital de HealthCare



# SECURELINK

Professeurs : Messieurs Canalda et Spies

## I.Table des matières

<b>II.</b>	<b><i>Introduction .....</i></b>	<b>4</b>
A.	Contexte et objectifs du projet .....	4
B.	Enjeux de la sécurité et besoins en infrastructure réseau .....	4
C.	Cahier des charges initial .....	4
D.	Méthodologie de travail et choix technologiques .....	4
<b>III.</b>	<b><i>Conception de l'architecture réseau.....</i></b>	<b>5</b>
A.	Diagramme de l'architecture réseau et segmentation par VLAN .....	5
B.	Organisation des sous-réseaux pour les différents services (administration, médical, IoT, etc.) .....	6
C.	Choix des équipements et logiciels .....	7
D.	Routeurs, switchs, points d'accès (ex : borne Linksys), et serveurs.....	7
E.	Solutions logicielles pour la gestion des droits, des accès et de la sécurité réseau .....	7
<b>IV.</b>	<b><i>Configuration réseau : VLAN, DHCP, VPN et sécurité.....</i></b>	<b>8</b>
A.	<b>VLANs et segmentation du réseau .....</b>	<b>8</b>
1.	Création des VLANs (ex : VLAN médical, administratif, IoT, Wi-Fi) et définition des adresses IP .....	8
2.	Configuration des VLANs sur le Switch .....	8
3.	Définition des adresses IP .....	9
B.	<b>Configuration du DHCP et gestion des adresses IP .....</b>	<b>9</b>
1.	Configuration du serveur DHCP pour l'attribution automatique d'adresses IP .....	9
2.	Attribution dynamique des adresses IP selon les VLANs .....	10
C.	<b>Sécurité du réseau avec Stormshield .....</b>	<b>10</b>
D.	<b>Règles de sécurité pour l'accès au réseau interne selon les rôles des utilisateurs.....</b>	<b>10</b>
E.	<b>Portail captif Wi-Fi et authentification .....</b>	<b>11</b>
1.	Configuration d'un annuaire sur Stormshield .....	11
2.	Configuration portail captif avec règle de redirection .....	12
F.	<b>Configuration du VPN pour accès vers un autre hôpital .....</b>	<b>12</b>
1.	Configuration du VPN pour accès vers un autre hôpital .....	12
2.	Configuration de la règle de routage sur Stormshield et Autorisations pour les utilisateurs .....	13
<b>V.</b>	<b><i>Développement et intégration de l'application web .....</i></b>	<b>14</b>
A.	<b>Présentation des objectifs de l'application .....</b>	<b>14</b>
1.	Rôle de l'application pour la gestion des patients, des imprimantes, et des consultations .....	14
B.	<b>Architecture de l'application en Node.js, HTML, CSS et JavaScript .....</b>	<b>14</b>
1.	Structure en Node.js pour le serveur back-end et gestion des requêtes http .....	14
2.	Utilisation de HTML et CSS pour la structure et le design des pages web .....	15
3.	Intégration de JavaScript pour la dynamique des pages et interactions utilisateur .....	15
C.	<b>Gestion des utilisateurs et sécurité de l'application .....</b>	<b>15</b>
1.	Middleware de sécurité et authentification pour l'accès (ex : express-session, JWT).....	15
2.	Chiffrement des données dans la base de données et gestion des rôles (admin, personnel médical) .....	15
3.	Protection des pages sensibles selon le rôle de l'utilisateur.....	16
D.	<b>Fonctionnalités principales de l'application .....</b>	<b>16</b>
1.	Gestion des patients : ajout, modification, consultation .....	16
2.	Gestion des imprimantes et suivi des stocks d'encre .....	17

<b>E.</b>	<b>Interaction avec les services réseaux et IoT .....</b>	<b>17</b>
1.	Intégration des données de l'IoT pour le suivi en temps réel des salles (température, CO2) .....	17
2.	Communication avec le serveur Apache pour récupérer et afficher les données MQTT .....	17
<b>VI.</b>	<b>Infrastructure IoT et gestion des données environnementales .....</b>	<b>18</b>
<b>A.</b>	<b>Déploiement et configuration des capteurs IoT (température, mouvement, etc.) .....</b>	<b>18</b>
1.	Capteurs utilisés : .....	18
2.	Choix des microcontrôleurs : .....	18
3.	Configuration des capteurs : .....	19
<b>B.</b>	<b>Installation des capteurs et configuration avec le broker MQTT sur Raspberry Pi .....</b>	<b>19</b>
1.	Configuration du broker MQTT : .....	19
2.	Exemple de code MQTT : .....	19
<b>C.</b>	<b>Suivi des données en temps réel et visualisation pour la gestion des environnements hospitaliers..</b>	<b>20</b>
1.	Application web de suivi en temps réel : .....	20
2.	Communication avec le serveur Apache : .....	20
3.	Collecte et interprétation des données avec Apache .....	20
4.	Badge RFID pour l'accès restreint aux zones sensibles .....	20
5.	Programmation de l'accès via MQTT : .....	20
6.	Messages d'autorisation et de refus : .....	21
<b>VII.</b>	<b>Tests et validations.....</b>	<b>22</b>
<b>A.</b>	<b>Résultats et validation des fonctionnalités de l'application web .....</b>	<b>22</b>
<b>B.</b>	<b>Tests de gestion des utilisateurs et de l'accès sécurisé aux données .....</b>	<b>22</b>
<b>C.</b>	<b>Vérification de la consultation et de l'intégration des données IoT .....</b>	<b>22</b>
<b>VIII.</b>	<b>Coût total du projet.....</b>	<b>22</b>
<b>A.</b>	<b>Coûts des équipements et infrastructures réseau .....</b>	<b>22</b>
<b>B.</b>	<b>Routeurs, switchs, bornes Wi-Fi, serveurs, capteurs, etc.....</b>	<b>22</b>
<b>C.</b>	<b>Coûts logiciels et licences .....</b>	<b>23</b>
<b>D.</b>	<b>Coûts de développement de l'application.....</b>	<b>23</b>
<b>E.</b>	<b>Coûts d'installation et de formation .....</b>	<b>23</b>
1.	Installation des équipements, configuration des VLANs.....	23
2.	Formation des utilisateurs .....	23
<b>F.</b>	<b>Coût total estimé .....</b>	<b>24</b>
<b>IX.</b>	<b>Améliorations potentielles.....</b>	<b>24</b>
<b>A.</b>	<b>Optimisation de l'application web .....</b>	<b>24</b>
1.	Ajout de nouvelles fonctionnalités .....	24
2.	Ajout de la téléphonie.....	24
3.	Ajout de Radius et d'Active Directory pour une authentification sans mot de passe.....	24
4.	Amélioration de l'interface utilisateur pour plus de convivialité .....	25
<b>B.</b>	<b>Extension de l'IoT et collecte de nouvelles données .....</b>	<b>25</b>
1.	Intégration de nouveaux capteurs et dispositifs de sécurité .....	25
2.	Développement d'un site de gestion IoT pour l'hôpital.....	26
<b>X.</b>	<b>Conclusion .....</b>	<b>26</b>
<b>A.</b>	<b>Bilan du projet et atteinte des objectifs .....</b>	<b>26</b>
<b>B.</b>	<b>Perspectives futures et retours sur expérience .....</b>	<b>26</b>

## II. Introduction

### A. Contexte et objectifs du projet

L'évolution rapide des technologies numériques a transformé de nombreux secteurs, y compris le domaine de la santé. Les hôpitaux, en particulier, sont désormais confrontés à des défis technologiques importants pour offrir des soins de qualité tout en assurant la sécurité des données médicales. La digitalisation des établissements de santé, combinée à l'essor des objets connectés (IoT), exige une infrastructure réseau fiable et sécurisée pour gérer les informations sensibles et les dispositifs médicaux.

Ce projet a pour objectif de moderniser l'infrastructure réseau d'un établissement hospitalier, en renforçant la sécurité des systèmes d'information et en intégrant des dispositifs IoT pour améliorer la gestion et la surveillance des données. Plus précisément, il s'agit de mettre en place une architecture réseau robuste, d'assurer la sécurité des communications internes et externes, et d'implémenter une solution de maintenance qui garantit la disponibilité des systèmes critiques. Le projet vise à répondre aux besoins actuels de l'hôpital tout en anticipant les évolutions futures des technologies de santé.

### B. Enjeux de la sécurité et besoins en infrastructure réseau

La sécurité des données de santé est un enjeu crucial pour les établissements hospitaliers. Les informations médicales sont sensibles et doivent être protégées contre les accès non autorisés et les cyberattaques. En outre, l'infrastructure réseau doit être capable de gérer des flux de données importants et d'assurer une connectivité continue entre les différents services de l'hôpital.

Les principaux enjeux de sécurité pour cet hôpital sont :

- **Protection des données patients** : Assurer la confidentialité et l'intégrité des informations médicales.
- **Sécurité des dispositifs IoT** : Mettre en place des mesures de sécurité pour les objets connectés, tels que les capteurs et badges d'accès, afin de limiter les risques de piratage.
- **Contrôle des accès** : définir des règles strictes pour limiter l'accès aux informations sensibles aux seuls membres autorisés du personnel.
- **Continuité de service** : Garantir une disponibilité constante des systèmes pour éviter tout risque d'interruption des soins.

Pour répondre à ces enjeux, l'hôpital a besoin d'une infrastructure réseau modernisée et sécurisée, avec des dispositifs de cybersécurité avancés, une gestion des accès par badge RFID, un monitoring en temps réel, et un support de maintenance pour répondre aux incidents dans des délais rapides.

### C. Cahier des charges initial

### D. Méthodologie de travail et choix technologiques

Pour mener à bien ce projet, une **méthodologie Agile** a été adoptée, avec des sprints hebdomadaires permettant une planification, un suivi et un ajustement continu en fonction des retours. Cette méthodologie a

permis une grande flexibilité, essentielle pour un projet impliquant des parties variées et des infrastructures complexes. Chaque sprint comprenait une phase de planification, de développement, de tests, et de validation, garantissant ainsi une progression contrôlée et un ajustement rapide en cas d'imprévus.

Les **choix technologiques** ont été faits en fonction des exigences de sécurité, de performance et de durabilité. Parmi les principaux éléments technologiques retenus figurent :

- **Switches Cisco Catalyst et routeur Stormshield** : Choix pour leur robustesse et leur capacité à supporter un trafic important tout en offrant des fonctionnalités de segmentation et de filtrage des données.
- **Serveurs DELL et dispositifs IoT** : Utilisés pour la gestion des données et la surveillance en temps réel des conditions environnementales dans les salles.
- **Système de gestion des accès par badge RFID** : Permettant une gestion fine des autorisations et une traçabilité des accès pour renforcer la sécurité.
- **Dispositifs de cybersécurité** : Pare-feu et IDS/IPS pour la protection en temps réel contre les intrusions et les cybermenaces, assurant un haut niveau de sécurité pour les données critiques.
- **Logiciels de surveillance et de maintenance** : Intégration d'outils de suivi pour surveiller l'état des dispositifs en temps réel et intervenir rapidement en cas de problème.

Ce choix technologique, combiné à une méthodologie de gestion de projet Agile, a permis de garantir une infrastructure sécurisée, évolutive, et capable de répondre aux besoins présents et futurs de l'établissement hospitalier.

### III. Conception de l'architecture réseau

#### A. Diagramme de l'architecture réseau et segmentation par VLAN

L'architecture réseau de l'hôpital est conçue pour répondre aux exigences de sécurité, de performance et de fiabilité, sans utiliser de segmentation VLAN. À la place, chaque type de réseau est configuré de manière isolée avec des sous-réseaux distincts pour chaque fonction. Cette configuration permet d'assurer un niveau de sécurité élevé et une séparation stricte des différents flux de données.

Les réseaux principaux incluent :

- **Réseau Wi-Fi Administratif** : pour le personnel administratif, offrant un accès aux ressources de gestion et de support.
- **Réseau IoT** : pour connecter et surveiller les dispositifs IoT (capteurs de température, humidité, mouvements, etc.) déployés dans les différentes zones de l'hôpital.
- **Réseau Serveurs** : réservé aux serveurs centraux de l'hôpital, hébergeant des applications critiques comme la gestion des dossiers patients et les bases de données médicales.
- **Réseau Administration** : pour les postes de travail de l'administration de l'hôpital, incluant des services financiers et de gestion des ressources humaines.
- **Réseau Médical** : dédié au personnel médical avec un accès aux informations sur les patients et aux dispositifs de diagnostic connectés.
- **Réseau IT** : utilisé par l'équipe informatique pour la gestion, la maintenance et la surveillance du réseau

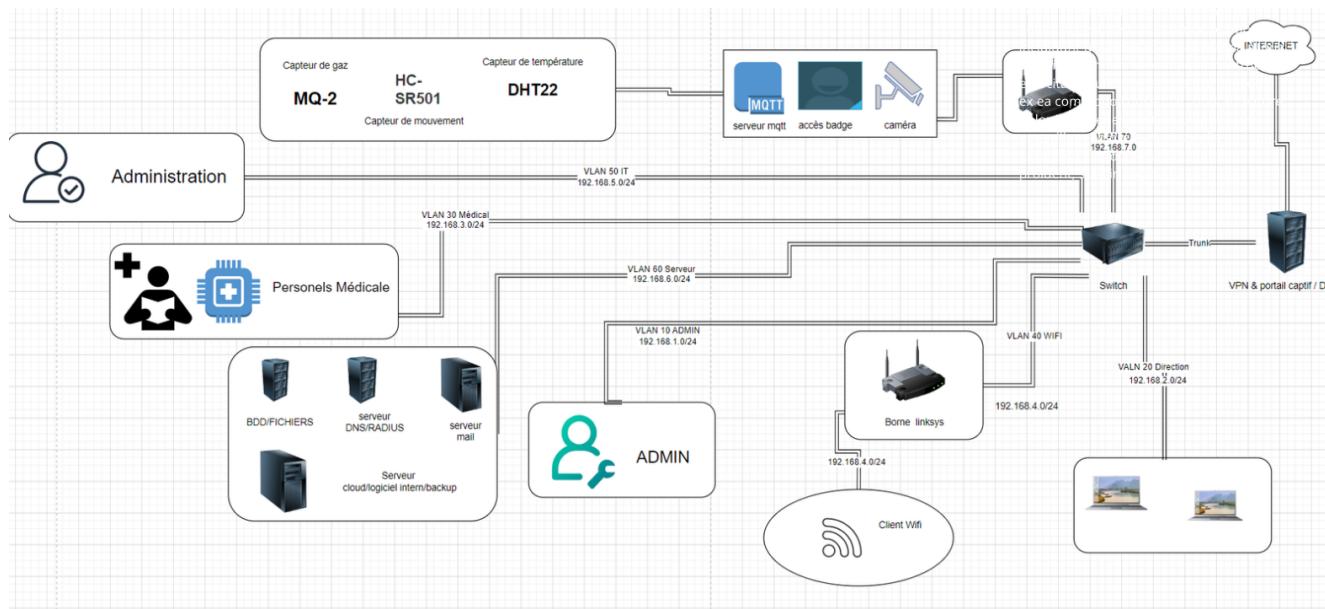


Figure 1 - Schéma du réseau

## B. Organisation des sous-réseaux pour les différents services (administration, médical, IoT, etc.)

Chaque réseau est configuré avec sa propre plage d'adresses IP, permettant une gestion des accès plus sécurisée et une isolation des flux de données. Voici comment chaque sous-réseau est organisé :

- **Sous-réseau Wi-Fi Administratif** : Ce réseau est configuré pour le personnel administratif qui a besoin d'une connexion Wi-Fi sécurisée pour accéder aux ressources internes de gestion et aux documents administratifs.
- **Sous-réseau IoT** : Ce réseau regroupe l'ensemble des dispositifs IoT qui surveillent l'environnement hospitalier. Les données sont envoyées aux serveurs pour traitement, mais les dispositifs IoT sont isolés des autres réseaux pour limiter les risques d'attaques et protéger les autres ressources critiques.
- **Sous-réseau Serveurs** : Ce réseau héberge les serveurs principaux de l'hôpital, offrant un accès direct aux bases de données et aux applications critiques. L'accès est strictement contrôlé et limité aux utilisateurs autorisés.
- **Sous-réseau Administration** : Ce réseau est utilisé par le personnel administratif de l'hôpital, permettant un accès sécurisé aux applications de gestion et aux informations administratives sans interférence avec le réseau médical.
- **Sous-réseau Médical** : Utilisé par le personnel médical, ce réseau fournit un accès rapide et sécurisé aux informations patients et aux applications de diagnostic en temps réel.
- **Sous-réseau IT** : Ce réseau est réservé à l'équipe informatique pour la surveillance du réseau, la configuration des équipements, et la gestion de la sécurité.
- **Sous-réseau Direction** : Utilisé pour les directions et crée une séparation entre les autres sous-réseau.

### C. Choix des équipements et logiciels

L'infrastructure réseau est équipée de matériels de haute qualité et de logiciels spécialisés pour garantir une gestion efficace et sécurisée des différents sous-réseaux.

- **Pare-feu Stormshield** : Utilisé pour segmenter les différents sous-réseaux et gérer les flux de données. Il assure la protection contre les menaces externes et permet un contrôle précis des autorisations d'accès entre les réseaux.
- **Switchs managés** : Ces switchs permettent une configuration avancée et facilitent la gestion de la bande passante entre les différents sous-réseaux pour une performance optimale.
- **Points d'accès Linksys** : Les bornes Wi-Fi Linksys fournissent une connexion Wi-Fi sécurisée pour le personnel administratif. Elles sont configurées pour séparer les réseaux invités et administratifs, assurant une couverture fiable et un accès restreint.
- **Serveurs dédiés** : Les serveurs de l'hôpital sont isolés dans le sous-réseau Serveurs et hébergent des applications critiques comme les bases de données de gestion des patients. Ils sont configurés pour des sauvegardes automatiques et une haute disponibilité.

### D. Routeurs, switchs, points d'accès (ex : borne Linksys), et serveurs

- **Routeur Stormshield** : Les routeurs permettent de gérer le trafic entre les sous-réseaux et assurent la connectivité internet sécurisée pour les utilisateurs autorisés.
- **Switchs managés** : Ils sont utilisés pour la gestion des connexions entre les sous-réseaux, permettant une configuration et un contrôle avancés de la répartition du trafic.
- **Points d'accès Linksys** : Les bornes Wi-Fi Linksys offrent une connexion sécurisée pour le réseau administratif sans interférer avec les autres sous-réseaux.
- **Serveurs** : Les serveurs sont protégés au sein du sous-réseau Serveurs, garantissant un accès limité aux ressources critiques de l'hôpital et une protection renforcée des données des patients.

### E. Solutions logicielles pour la gestion des droits, des accès et de la sécurité réseau

Le pare-feu **Stormshield** gère la sécurité des sous-réseaux, les droits d'accès, et la journalisation des activités, assurant ainsi une sécurité globale de l'infrastructure.

- **Stormshield pour la gestion des accès** : Stormshield est configuré pour appliquer des règles strictes de filtrage de trafic, permettant uniquement aux utilisateurs autorisés d'accéder aux ressources nécessaires dans chaque sous-réseau. Chaque règle est adaptée aux besoins de chaque réseau, garantissant une isolation stricte des données sensibles.
- **Stormshield pour la sécurité réseau** : Stormshield inclut des fonctionnalités de détection d'intrusions (IDS) et de prévention (IPS) pour surveiller le trafic en temps réel et bloquer les menaces potentielles. Cette solution protège les sous-réseaux critiques, comme ceux des serveurs et du réseau médical.
- **Journalisation des activités par Stormshield** : Toutes les activités réseau sont enregistrées directement par Stormshield, permettant une surveillance continue et une gestion des incidents en cas de

comportement suspect. Ce système de journalisation aide à détecter toute anomalie et facilite les audits de sécurité pour assurer la conformité et la sécurité des données.

En s'appuyant sur Stormshield pour la gestion des droits, la sécurité, et la journalisation, l'architecture réseau de l'hôpital bénéficie d'une protection renforcée et d'un contrôle précis des accès, garantissant ainsi la confidentialité et la disponibilité des ressources critiques.

## IV. Configuration réseau : VLAN, DHCP, VPN et sécurité

### A. VLANs et segmentation du réseau

#### 1. **Création des VLANs (ex : VLAN médical, administratif, IoT, Wi-Fi) et définition des adresses IP**

La segmentation du réseau de l'hôpital est réalisée en créant plusieurs **VLANs** pour isoler les différents services et flux de données. Chaque VLAN est associé à un sous-réseau spécifique, avec une plage d'adresses IP dédiée, ce qui permet une gestion plus précise des accès et une meilleure sécurité.

Les VLANs créés sont les suivants :

- **VLAN Médical** : réservé au personnel médical avec accès aux dossiers patients et aux dispositifs de diagnostic.
- **VLAN Administratif** : dédié au personnel administratif pour les opérations de gestion et de support.
- **VLAN IoT** : utilisé pour les dispositifs IoT (capteurs de température, d'humidité, etc.) qui surveillent l'environnement hospitalier.
- **VLAN Wi-Fi** : fournit un accès sans fil pour le personnel et les invités, avec des restrictions spécifiques pour garantir la sécurité.
- **VLAN Médical** : Utilisé par le personnel médical, ce réseau fournit un accès rapide et sécurisé aux informations patients et aux applications de diagnostic en temps réel.
- **VLAN IT** : Ce réseau est réservé à l'équipe informatique pour la surveillance du réseau, la configuration des équipements, et la gestion de la sécurité.
- **VLAN Direction** : Utilisé pour les directions et crée une séparation entre les autres vlan.

SYSTÈME		RESEAU			
VLAN-10	Direction	AN-10	AN-20	2 Ethernet, 1 Gb/s	172.16.0.254/24
Type: VLAN, 1 Gb/s, Protégée	État: Activée, Connectée	AN-30	AN-40	2 VLAN, Identifiant 10, 1 Gb/s	192.168.1.254/24
Nom physique: In (Ethernet)		AN-50	AN-60	2 VLAN, Identifiant 20, 1 Gb/s	192.168.2.254/24
Port: 2		AN-70	AN-80	2 VLAN, Identifiant 30, 1 Gb/s	192.168.3.254/24
Identifiant: 10		AN-90	AN-99	2 VLAN, Identifiant 40, 1 Gb/s	192.168.4.254/24
Nom système: wlan0		AN-100	AN-111	2 VLAN, Identifiant 50, 1 Gb/s	192.168.5.254/24
Adresses IPv4: 192.168.1.254/24				2 VLAN, Identifiant 60, 1 Gb/s	192.168.6.254/24
				2 VLAN, Identifiant 70, 1 Gb/s	192.168.7.254/24
				2 VLAN, Identifiant 99, 1 Gb/s	192.168.99.254/24
				Bridge	10.0.0.254/8
				3 Ethernet, 1 Gb/s	
				1 Ethernet	
				Activée, Non connectée	192.168.33.103/24 (DHCP)

Figure 2 - Vlan configuration

#### 2. Configuration des VLANs sur le Switch

Les VLANs sont configurés sur un **switch managé** qui prend en charge le routage inter-VLAN. Chaque port du switch est associé à un VLAN particulier en mode **access** pour les appareils finaux (ordinateurs, imprimantes, dispositifs IoT) afin d'assurer qu'ils ne peuvent accéder qu'à leur VLAN respectif.

Un port du switch est configuré en mode **trunk** et connecté au pare-feu **Stormshield**. Le mode trunk permet de transmettre le trafic de tous les VLANs via un seul lien entre le switch et le pare-feu, ce qui permet à Stormshield de gérer le filtrage et les règles de sécurité pour chaque VLAN.

### 3. Définition des adresses IP

Chaque VLAN dispose d'une plage d'adresses IP dédiée pour organiser le réseau de manière structurée et faciliter la gestion des accès.

- VLAN Médical** : 192.168.3.0/24
- VLAN Administratif** : 192.168.1.0/24
- VLAN IoT** : 192.168.7.0/24
- VLAN Wi-Fi** : 192.168.4.0/24
- VLAN Direction** : 192.168.2.0/24
- VLAN IT** : 192.168.5.0/24
- VLAN Serveur** : 192.168.6.0/24

Ces plages d'adresses IP permettent de segmenter efficacement les flux de données et de maintenir une isolation stricte entre les différents services.

SYSTÈME		in				
<b>VLAN-10</b>		AN-10	2 Ethernet, 1 Gb/s	172.16.0.254/24		
Direction		AN-20	2 VLAN, Identifiant 10, 1 Gb/s	192.168.1.254/24	Direction	
		AN-30	2 VLAN, Identifiant 20, 1 Gb/s	192.168.2.254/24	Administration	
Type:	VLAN, 1 Gb/s, Protégée	AN-40	2 VLAN, Identifiant 30, 1 Gb/s	192.168.3.254/24	Medical	
État:	Activée, Connectée	AN-50	2 VLAN, Identifiant 40, 1 Gb/s	192.168.4.254/24	Informatique	
Nom physique:	in (Ethernet)	AN-60	2 VLAN, Identifiant 50, 1 Gb/s	192.168.5.254/24	it	
Port:	2	AN-70	2 VLAN, Identifiant 60, 1 Gb/s	192.168.6.254/24	Serveurs	
Identifiant:	10	AN-99	2 VLAN, Identifiant 70, 1 Gb/s	192.168.7.254/24	IOT	
Nom système:	vlan0	Bridge	2 VLAN, Identifiant 99, 1 Gb/s	192.168.99.254/24	Gestion	
Adresses IPv4:	192.168.1.254/24		3 Ethernet, 1 Gb/s	10.0.0.254/8		
			1 Ethernet	192.168.33.103/24 (DHCP)		

Figure 3 - VLAN sur Stormshield

## B. Configuration du DHCP et gestion des adresses IP

### 1. Configuration du serveur DHCP pour l'attribution automatique d'adresses IP

Le serveur DHCP (Dynamic Host Configuration Protocol) est configuré pour attribuer automatiquement des adresses IP aux périphériques des différents VLANs par notre Pare-feu. Cette configuration facilite la gestion des adresses IP, éliminant le besoin d'attribution manuelle tout en assurant que chaque dispositif connecté obtienne une adresse unique.

La configuration du serveur DHCP inclut :

- Plages d'adresses IP pour chaque VLAN** : Le serveur DHCP attribue des adresses en fonction du VLAN de

chaque dispositif. Par exemple, le VLAN Médical utilise la plage 192.168.3.0/24, tandis que le VLAN IoT utilise la plage 192.168.7.0/24.

- Attribution de passerelles et de serveurs DNS :** Le serveur DHCP fournit également des informations de passerelle et de serveur DNS pour chaque dispositif connecté, facilitant leur accès aux ressources internes et externes du réseau.

#### PLAGE D'ADRESSES

Rechercher...		+ Ajouter	X Supprimer	
Plage d'adresses	Passerelle	DNS primaire	DNS secondaire	Nom de domaine
dhcp_range	Firewall_bridge	serveurdns	default	hopital3.local
DHCP_10	Firewall_VLAN-10	serveurdns	default	hopital3.local
DHCP_99			default	hopital3.local
DHCP_50		DHCP_10	default	hopital3.local
DHCP_40		Plage d'adresses IPv4	192.168.1.1 à 192.168.1.100	hopital3.local

#### RÉSERVATION

Figure 4 - DHCP Stormshield

## 2. Attribution dynamique des adresses IP selon les VLANs

Chaque VLAN dispose de sa propre plage d'adresses IP, configurée dans le serveur DHCP. Cette attribution dynamique assure que les dispositifs sont segmentés et peuvent être facilement identifiés et gérés en fonction de leur VLAN d'origine. Cela permet aussi d'appliquer des politiques de sécurité spécifiques en fonction de l'adresse IP de chaque dispositif.

### C. Sécurité du réseau avec Stormshield

Le pare-feu Stormshield est au cœur de la stratégie de sécurité du réseau. Il permet de filtrer le trafic, d'appliquer des politiques de sécurité strictes et d'isoler les différents VLANs pour une meilleure protection des données.

- Inspection des paquets :** Stormshield inspecte en profondeur les paquets entrants et sortants pour détecter des menaces potentielles, comme les virus et les intrusions.
- Segmentation du réseau :** Chaque VLAN est isolé, et Stormshield assure que le trafic entre les VLANs est strictement contrôlé selon des règles prédéfinies. Par exemple, le VLAN IoT est limité pour éviter toute communication non autorisée avec les autres VLANs.
- Journalisation des activités :** Stormshield enregistre toutes les activités réseau, permettant une analyse approfondie des accès et facilitant la détection de comportements anormaux.

### D. Règles de sécurité pour l'accès au réseau interne selon les rôles des utilisateurs

Les règles de sécurité sur Stormshield sont configurées pour contrôler l'accès au réseau en fonction des rôles des utilisateurs. Cela garantit que chaque utilisateur dispose uniquement des accès nécessaires pour ses tâches.

- Accès restreint pour le personnel invité :** Les invités n'ont accès qu'au Wi-Fi et sont limités au VLAN Wi-Fi, sans possibilité d'accéder aux ressources internes sensibles.
- Accès dédié pour le personnel médical :** Le personnel médical a accès au VLAN Médical et aux ressources

partagées du réseau médical, mais ne peut accéder au réseau administratif.

- Accès complet pour l'administration :** Les administrateurs disposent d'un accès complet au réseau interne, y compris aux serveurs de gestion et aux dossiers patients.

Ces règles de sécurité sont définies pour chaque VLAN et appliquées sur Stormshield afin d'assurer une gestion rigoureuse des accès.

The screenshot shows the Stormshield firewall's rule configuration interface. It displays a list of rules categorized by source and destination VLANs. Key details include:

- Rule 1:** Source: 'tout le monde vers le portail DNS' (contains 1 rule, from 1 to 1). Action: 'passer'. Destination: Any. Protocols: dns, dns-tcp, dns-udp. Type: IPS. Created on 2024-10-18 10:26:11.
- Rule 2:** Source: 'redirection vers portail captif + accès à l'application' (contains 1 rule, from 2 to 2). Action: 'on'. Port: unknown @ Portail d'authtk. Destination: Network\_VLAN-1 (Any). Protocols: http, https, http\_proxy. Type: IPS. Created on 2024-10-15 13:58:57.
- Rule 3-6:** Source: 'qui doit passer ou ?' (contains 4 rules, from 3 to 6). Action: 'bloquer'. Destination: Firewall\_VLAN-30 (Any). Protocols: Any. Type: IPS. Created on 2024-10-18 10:13:52.
- Rule 7:** Source: 'tout passe' (contains 1 rule, from 7 to 7). Action: 'bloquer'. Destination: Any. Protocols: Any. Type: IPS. Created on 2024-10-18 10:13:52.

Figure 5 - Règle Stormshield

## E. Portail captif Wi-Fi et authentification

### 1. Configuration d'un annuaire sur Stormshield

Un annuaire d'utilisateurs est configuré sur Stormshield pour faciliter l'authentification sur le réseau Wi-Fi. Cet annuaire répertorie les identifiants et les rôles des utilisateurs autorisés à se connecter, permettant à Stormshield de contrôler et d'authentifier chaque utilisateur avant de lui accorder l'accès au réseau.

The screenshot shows the Stormshield user configuration interface for a user named 'H1'. The user details are as follows:

- General Information:**
  - Émis le: Oct 9 13:54:17 2024 GMT
  - Expiration: Oct 14 13:54:17 2024 GMT
- Emis pour:**
  - Sujet: C=FR,ST=Franch-comté,L=Montbéliard,O=hôpital1,OU=hôpital1,CN=H1
  - Nom (CN): H1
  - Nom de l'organisation (O): hôpital1
  - Nom de l'unité (OU): hôpital1
  - Nom du lieu (L): Montbéliard
  - Nom de l'état ou de la province (ST): Franch-comté
  - Pays (C): FR
  - E-mail: 873f54e2
- Emetteur:**
  - Émetteur: C=FR,ST=Franch-comté,L=Montbéliard,O=hôpital1,OU=hôpital1,CN=H1
  - Nom (CN): H1
  - Nom de l'organisation (O): hôpital1
  - Nom de l'unité (OU): hôpital1
  - Nom du lieu (L): Montbéliard

Figure 6 - Configuration hôpital

## 2. Configuration portail captif avec règle de redirection

Un portail captif est mis en place pour gérer les accès au Wi-Fi. Lorsque les utilisateurs tentent de se connecter au Wi-Fi, ils sont redirigés vers une page d'authentification où ils doivent entrer leurs identifiants. Le portail captif est configuré pour :

- Rediriger automatiquement les utilisateurs non authentifiés vers la page d'authentification.**



Figure 7 - Règle authentification

- Limiter l'accès des utilisateurs invités au seul VLAN Wi-Fi, leur interdisant l'accès aux autres ressources réseau.**

Le portail captif offre une couche de sécurité supplémentaire pour contrôler les connexions au Wi-Fi et garantir que seules les personnes autorisées peuvent accéder aux ressources internes.

The screenshot shows a list of network rules in a configuration interface. The rules are organized into several sections:

- "tout le monde vers le portail DNS (contient 1 règles, de 1 à 1)": Rule 1 (entry 1) passes all traffic ("passer") to destination "Any" on ports "dns, dns\_tcp, dns\_udp" (Protocol Type "IPS").
- "redirection vers portail captif + accès à l'application (contient 1 règles, de 2 à 2)": Rule 2 (entry 2) has "on" action, "Portail d'auth: Hormis : authentica", destination "Any", protocols "http, https, http\_proxy" (Protocol Type "IPS").
- "qui doit passer ou ? (contient 4 règles, de 3 à 6)": Rules 3, 4, 5, 6 (entries 3-6) block traffic ("bloquer") from source "Firewall\_VLAN-30" to destination "Firewall\_VLAN-20" and "Firewall\_VLAN-10" on any ports (Protocol Type "IPS").
- "tout passe (contient 1 règles, de 7 à 7)": Rule 7 (entry 7) blocks traffic ("bloquer") from source "Any" to destination "Any" on any ports (Protocol Type "IPS").

## F. Configuration du VPN pour accès vers un autre hôpital

Pour configurer le VPN et la règle de routage sur Stormshield pour une connexion sécurisée entre deux hôpitaux, voici une explication détaillée de la configuration VPN et des règles de routage.

### 1. Configuration du VPN pour accès vers un autre hôpital

La mise en place du VPN permet au personnel de l'hôpital d'échanger des informations sensibles avec un autre établissement de santé de manière sécurisée. Stormshield est utilisé pour établir le tunnel VPN et gérer les règles de routage nécessaires pour que seuls les utilisateurs autorisés puissent accéder aux ressources distantes.

#### Configuration du tunnel VPN sécurisé

Le tunnel VPN est configuré pour créer un canal chiffré entre les deux hôpitaux. Ce tunnel utilise des protocoles de chiffrement robustes (par exemple, IPsec ou SSL) pour garantir la confidentialité des données transmises.

- **Protocole de chiffrement** : IPsec est souvent utilisé pour ce type de connexion, car il assure l'intégrité et la confidentialité des données. Le VPN utilise également un chiffrement AES pour renforcer la sécurité du tunnel.
- **Authentification** : Les hôpitaux utilisent des certificats numériques pour authentifier chaque point de connexion, assurant que seules les parties autorisées peuvent établir la connexion.

## 2. Configuration de la règle de routage sur Stormshield et Autorisations pour les utilisateurs

Une règle de routage spécifique est ajoutée sur Stormshield pour diriger le trafic approprié à travers le tunnel VPN. Cette règle assure que seules certaines adresses IP et réseaux locaux sont autorisés à utiliser le tunnel VPN pour accéder aux ressources de l'autre hôpital.

- **Définition des réseaux sources et cibles** : La règle de routage identifie les plages d'adresses IP internes des deux hôpitaux qui sont autorisées à communiquer via le VPN. Par exemple :
  - Réseau source (hôpital local) : 192.168.3.0/24
  - Réseau cible (serveur hôpital distant) : 192.168.70.0/24
- **Route statique pour le VPN** : Une route statique est configurée pour diriger tout le trafic destiné au réseau de l'hôpital distant (192.168.70.0/24) vers le tunnel VPN. Cette route garantit que les paquets atteignent le réseau distant uniquement via le VPN.

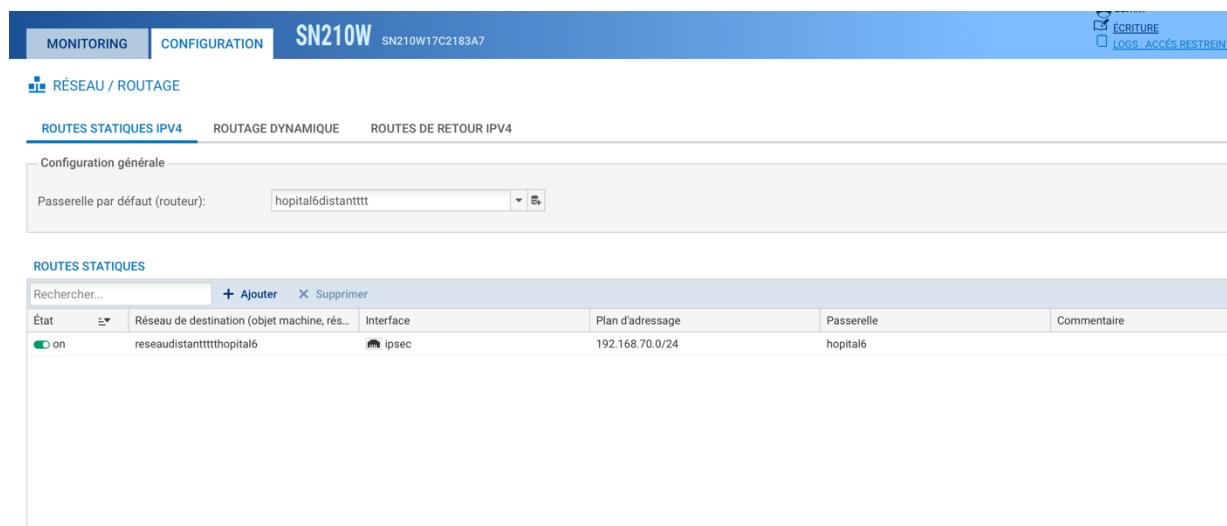


Figure 8 - règle de routage

- **Règles de filtrage et d'accès** : Stormshield applique des règles de filtrage pour s'assurer que seuls les utilisateurs et les appareils autorisés peuvent transmettre des données via le VPN. Par exemple :
  - Autorisation du trafic en provenance du réseau administratif et médical.
  - Restriction de l'accès au VPN pour les utilisateurs invités et IoT.

### Autorisations spécifiques pour les utilisateurs

Stormshield est configuré pour appliquer des autorisations spécifiques, garantissant que seuls les utilisateurs autorisés (comme le personnel administratif et les médecins) peuvent accéder aux ressources de l'autre hôpital via le VPN. Cela se fait en créant des groupes d'utilisateurs et en définissant des règles d'accès en fonction des besoins de chaque groupe.

- **Groupes d'utilisateurs** : Création de groupes distincts pour le personnel administratif et médical. Chaque groupe est associé à des règles d'accès définissant ce qu'ils peuvent voir et faire sur le réseau distant.
- **Règle de filtrage sur Stormshield** : La règle de filtrage vérifie l'appartenance au groupe d'utilisateurs

autorisés avant de permettre l'accès via le tunnel VPN. Les utilisateurs non autorisés sont automatiquement bloqués.

## V. Développement et intégration de l'application web

### A. Présentation des objectifs de l'application

#### 1. **Rôle de l'application pour la gestion des patients, des imprimantes, et des consultations**

L'application web développée dans le cadre de ce projet vise à centraliser la gestion des données des patients, des consultations et des imprimantes de l'hôpital. Elle permet de simplifier les opérations quotidiennes, en donnant accès en temps réel aux informations essentielles pour le personnel hospitalier, et en assurant le suivi des équipements critiques comme les imprimantes. Grâce à cette application, les administrateurs peuvent ajouter, consulter et mettre à jour les dossiers des patients ainsi que gérer les consommables des imprimantes.

L'application distingue deux types de profils utilisateurs : **administrateur** et **utilisateur standard**.

- **Administrateur** : Possède des priviléges étendus lui permettant non seulement de gérer les patients et les imprimantes, mais aussi de créer et de gérer les comptes d'autres utilisateurs (comme les salariés de l'hôpital). Cette fonctionnalité est cruciale pour garantir un accès contrôlé aux informations sensibles et pour organiser les accès en fonction des responsabilités des employés.
- **Utilisateur standard (salarié de l'hôpital)** : Accède aux fonctionnalités de base de l'application pour la gestion des patients et des consultations, mais sans droits pour ajouter ou gérer d'autres utilisateurs.

### B. Architecture de l'application en Node.js, HTML, CSS et JavaScript

#### 1. **Structure en Node.js pour le serveur back-end et gestion des requêtes http**

Le Framework javascript Node.js constitue le cœur du serveur de l'application, responsable de la gestion des requêtes HTTP et de la communication avec la base de données. Express, un Framework minimaliste pour Node.js, est utilisé pour structurer les routes et gérer le routage des requêtes. Les routes sont essentielles pour organiser les différentes fonctionnalités de l'application en regroupant les requêtes associées à une fonctionnalité spécifique, comme la gestion des patients ou des imprimantes.

**Définition des routes :** Chaque fonctionnalité est associée à une route distincte. Par exemple :

- /patients : pour afficher, ajouter, modifier ou supprimer des informations sur les patients.
- /consultations : pour gérer les consultations associées aux patients.
- /imprimantes : pour suivre l'état des imprimantes et gérer les consommables.
- /utilisateurs : uniquement accessible par les administrateurs, cette route permet de gérer les comptes des utilisateurs (ajout, modification, suppression).

**Méthodes HTTP :** Les routes utilisent des méthodes HTTP pour indiquer l'action souhaitée :

- GET : pour récupérer des informations (par exemple, obtenir la liste des patients).
- POST : pour envoyer de nouvelles données (par exemple, ajouter un nouveau patient ou créer un compte utilisateur).
- PUT : pour mettre à jour des données existantes (par exemple, mettre à jour les informations d'un patient ou d'un utilisateur).
- DELETE : pour supprimer des données (par exemple, supprimer un dossier patient ou désactiver un compte utilisateur).

## 2. Utilisation de HTML et CSS pour la structure et le design des pages web

L'interface utilisateur est construite en **HTML** pour structurer le contenu des pages et en **CSS** pour styliser l'application et assurer une expérience utilisateur agréable. Les pages sont conçues pour être intuitives et permettre une navigation fluide entre les différentes fonctionnalités. Le CSS est utilisé pour uniformiser les éléments de design, avec des boutons, des formulaires et des tableaux bien agencés pour afficher les informations essentielles sans surcharge visuelle.

## 3. Intégration de JavaScript pour la dynamique des pages et interactions utilisateur

**JavaScript** joue un rôle important pour enrichir l'interactivité et la dynamique des pages. Grâce à JavaScript, l'application permet de valider les données côté client avant l'envoi au serveur, d'actualiser des sections de la page sans recharger toute la page (via **AJAX**), et de fournir une réponse immédiate aux actions de l'utilisateur. Par exemple, lorsqu'un utilisateur ajoute un nouveau patient, JavaScript envoie les données au serveur sans recharger la page, permettant ainsi une expérience utilisateur fluide.

### C. Gestion des utilisateurs et sécurité de l'application

#### 1. Middleware de sécurité et authentification pour l'accès (ex : express-session, JWT)

La sécurité de l'application est une priorité, étant donné la nature sensible des données manipulées (informations patients, consultations, etc.). Pour garantir un accès sécurisé, plusieurs middleware de sécurité ont été mis en place.

- **Express-session** : Ce middleware permet de gérer les sessions utilisateurs en stockant des informations temporaires sur l'état de connexion de l'utilisateur. Lorsqu'un utilisateur se connecte, une session est créée et identifiée par un identifiant de session unique, qui est stocké côté serveur. Cette session persiste tant que l'utilisateur reste connecté, et elle est détruite lorsqu'il se déconnecte, garantissant ainsi que seuls les utilisateurs authentifiés peuvent accéder aux fonctionnalités protégées.
- **JWT (JSON Web Tokens)** : Les JSON Web Tokens sont utilisés pour gérer l'authentification dans une structure sans état. Lorsqu'un utilisateur se connecte, un JWT est généré, signé et envoyé au client. Ce token inclut des informations d'authentification (par exemple, l'ID utilisateur et le rôle) et peut être stocké localement sur le client. Pour chaque requête, le client renvoie le token au serveur dans l'en-tête d'autorisation. Le serveur décode et vérifie le token pour authentifier l'utilisateur. Cette approche permet de sécuriser les échanges tout en réduisant la dépendance aux sessions stockées sur le serveur.

L'utilisation combinée de **express-session** pour la gestion des sessions de courte durée et de **JWT** pour les échanges asynchrones renforce la sécurité et la flexibilité de l'authentification dans l'application.

#### 2. Chiffrement des données dans la base de données et gestion des rôles (admin, personnel médical)

Pour renforcer la sécurité des données, toutes les informations sensibles stockées dans la base de données sont chiffrées. Les mots de passe des utilisateurs sont chiffrés à l'aide d'un algorithme de hachage sécurisé (par exemple, **bcrypt**), empêchant ainsi toute récupération en cas d'accès non autorisé à la base de données.

- **Gestion des rôles (admin, personnel médical)** : Lors de la création d'un utilisateur, un rôle est attribué pour définir ses privilèges dans l'application :
  - **Admin** : Les administrateurs ont des privilèges étendus qui leur permettent non seulement de

gérer les patients et les imprimantes, mais aussi de créer et de gérer les comptes des autres utilisateurs. Ils ont la capacité d'ajouter, de modifier et de supprimer des comptes en fonction des besoins de l'hôpital.

- **Personnel médical (utilisateur standard)** : Ce rôle est réservé aux utilisateurs ayant besoin d'accéder aux dossiers patients et aux consultations. Les utilisateurs standard peuvent consulter, ajouter et modifier les informations liées aux patients, mais ils n'ont pas accès aux fonctions de gestion des utilisateurs.

La gestion des rôles est appliquée côté serveur en chiffrant les informations de chaque utilisateur et en s'assurant que seules les personnes disposant des priviléges requis peuvent accéder aux données sensibles.

### **3. Protection des pages sensibles selon le rôle de l'utilisateur**

L'application utilise un système de contrôle d'accès pour restreindre l'accès aux pages sensibles selon le rôle de chaque utilisateur. Ce contrôle est géré par des middlewares et des vérifications côté serveur.

- **Middleware de vérification de rôle** : Avant de permettre l'accès à certaines routes, un middleware analyse les informations de session ou le JWT pour vérifier le rôle de l'utilisateur. Par exemple, seules les routes de gestion des utilisateurs sont accessibles aux administrateurs. Si l'utilisateur ne dispose pas des droits requis, il est redirigé vers une page d'erreur ou reçoit un message d'accès refusé.
- **Protection des pages côté client** : En complément de la protection côté serveur, l'interface utilisateur masque également les options non autorisées en fonction du rôle de l'utilisateur. Par exemple, les boutons pour gérer les utilisateurs ne sont visibles que pour les administrateurs. Cette protection double (client et serveur) empêche les utilisateurs d'accéder ou de voir des éléments qu'ils ne sont pas autorisés à utiliser.
- **Chiffrement des données sensibles** : Outre le chiffrement des mots de passe, toute autre information sensible (comme les données médicales) est également chiffrée dans la base de données. Cela garantit que même si un utilisateur malveillant accède aux données brutes, les informations demeurent protégées par un chiffrement fort.

En combinant authentification par JWT, sessions sécurisées avec express-session, et chiffrement des données, l'application garantit un haut niveau de sécurité pour la gestion des utilisateurs et la protection des informations sensibles.

## D. Fonctionnalités principales de l'application

### **1. Gestion des patients : ajout, modification, consultation**

La gestion des patients est une fonctionnalité centrale de l'application, permettant au personnel médical de traiter et de suivre les informations essentielles des patients de manière sécurisée et organisée.

- **Ajout de patients** : Cette fonctionnalité permet au personnel médical d'ajouter de nouveaux patients dans la base de données en remplissant un formulaire dédié. Les informations incluent les données personnelles (nom, prénom, date de naissance, numéro de sécurité sociale, etc.) et les détails médicaux essentiels. Ces données sont enregistrées de manière sécurisée et chiffrée dans la base de données pour garantir la confidentialité des informations sensibles.
- **Modification des informations des patients** : Les utilisateurs autorisés peuvent mettre à jour les informations des patients en cas de changement de données personnelles ou d'évolution du dossier médical. Cette fonctionnalité garantit que les informations sur chaque patient restent à jour et que tout le personnel médical accède aux données les plus récentes.
- **Consultation des dossiers** : Le personnel médical peut consulter les dossiers patients via une interface de

recherche rapide, facilitant l'accès aux informations en fonction des besoins du moment. La consultation inclut l'historique des consultations et des traitements, permettant aux médecins et infirmiers d'avoir un aperçu complet du parcours de soins de chaque patient.

Cette gestion centralisée des données patients simplifie l'organisation des informations médicales et assure une meilleure coordination des soins, tout en respectant les normes de sécurité pour la confidentialité des données médicales.

## 2. **Gestion des imprimantes et suivi des stocks d'encre**

La gestion des imprimantes est une autre fonctionnalité clé de l'application, spécialement conçue pour optimiser les ressources matérielles de l'hôpital et garantir la disponibilité des imprimantes.

- **Suivi des imprimantes** : L'application permet de surveiller l'état des imprimantes utilisées dans différents services de l'hôpital. Chaque imprimante est enregistrée dans le système avec ses caractéristiques (modèle, emplacement, état) pour un suivi facile. En cas de panne ou d'erreur, le personnel peut signaler le problème, et l'équipe technique peut intervenir rapidement pour résoudre l'incident.
- **Suivi des stocks d'encre** : Cette fonctionnalité assure un suivi précis des niveaux d'encre pour chaque imprimante. Lorsque le niveau d'encre est bas, le système peut déclencher une alerte pour prévenir l'équipe de maintenance, évitant ainsi les interruptions dans l'impression des documents importants. Un suivi proactif des stocks d'encre permet également de commander les consommables à temps, améliorant ainsi l'efficacité des opérations et minimisant les temps d'arrêt des imprimantes.

En intégrant ces fonctionnalités, l'application permet une gestion efficace et optimisée des imprimantes et des stocks d'encre, ce qui réduit les interruptions dans les activités hospitalières et améliore la continuité des soins.

## E. Interaction avec les services réseaux et IoT

### 1. **Intégration des données de l'IoT pour le suivi en temps réel des salles (température, CO2)**

Les capteurs IoT déployés dans différentes zones de l'hôpital mesurent des paramètres critiques comme la **température** et la **qualité de l'air (CO2)**. Les données sont transmises en temps réel au réseau via un broker MQTT, permettant au personnel hospitalier de surveiller et réagir rapidement aux fluctuations environnementales. Cette intégration assure le maintien des conditions optimales dans les salles de soins et les zones sensibles.

- **Capteurs et configuration** : Chaque capteur IoT est configuré pour transmettre ses lectures à intervalles réguliers en utilisant des topics MQTT spécifiques.
- **Fonctionnement en temps réel** : Les données environnementales sont accessibles en temps réel dans le site, permettant de visualiser les niveaux actuels de température et de CO2 pour chaque salle.

### 2. **Communication avec le serveur Apache pour récupérer et afficher les données MQTT**

Le serveur **Apache** joue un rôle clé dans la collecte et la visualisation des données IoT en s'interfaisant avec le broker MQTT. Ce serveur intercepte les données provenant des capteurs et les rend accessibles pour l'application web, garantissant un affichage fluide des données en temps réel pour le personnel autorisé.

- **Configuration Apache et MQTT** : Le serveur Apache utilise des scripts pour interroger le broker MQTT et mettre à jour les informations sur l'application, facilitant ainsi un suivi en temps réel des paramètres

environnementaux dans les espaces hospitaliers.

- **Affichage des données IoT** : Les données transmises sont organisées en tableaux sur l'application web, où les utilisateurs peuvent visualiser les historiques de température et de CO<sub>2</sub>, ainsi que les niveaux actuels.

## VI. Infrastructure IoT et gestion des données environnementales

Dans cette section, nous allons détailler l'infrastructure IoT mise en place, couvrant les composants matériels et logiciels, leur configuration, et leur intégration dans le réseau hospitalier et l'application web pour surveiller et optimiser l'environnement hospitalier.

### A. Déploiement et configuration des capteurs IoT (température, mouvement, etc.)

#### 1. **Capteurs utilisés :**

- **DHT22** : Capteur de température et d'humidité, choisi pour sa précision et sa faible latence, qui permet une surveillance en temps réel des salles critiques (par exemple, salle de stockage de médicaments).
- **MQ135** : Capteur de qualité de l'air, essentiel pour assurer des conditions optimales dans les environnements sensibles aux agents pathogènes.
- **Capteur de mouvement** : Permet de détecter les activités dans les zones restreintes et peut être associé à des alertes automatiques pour renforcer la sécurité.

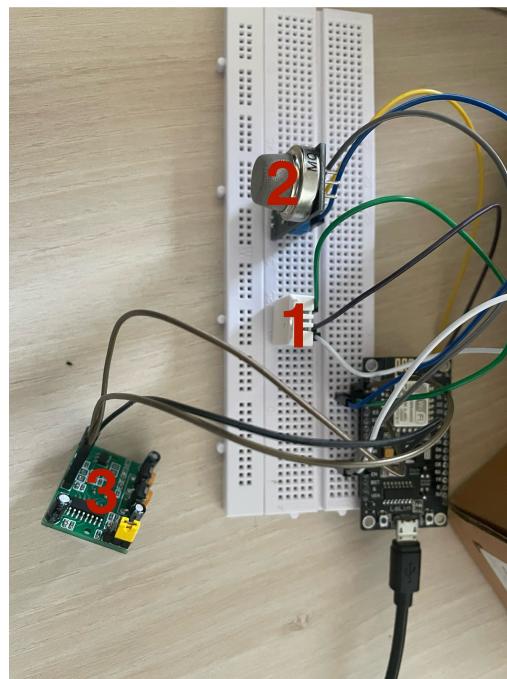


Figure 9 - Capteur IOT

1 = DHT22

2= MQ135

3= Capteur de mouvement

#### 2. **Choix des microcontrôleurs :**

L'**ESP8266** a été retenu pour sa connectivité Wi-Fi, essentielle dans des applications IoT sans fil. Ce microcontrôleur simplifie l'intégration des capteurs au réseau hospitalier via MQTT en assurant un envoi fiable et en temps réel des données mesurées par les capteurs.

### **3. Configuration des capteurs :**

**Installation physique** : Les capteurs sont installés dans des emplacements stratégiques de l'hôpital : le DHT22 est situé dans les salles sensibles à la température, le MQ135 dans les espaces de stockage et le capteur de mouvement à proximité des zones sécurisées.

**Code de collecte des données** : Le code ESP8266, utilisé pour chaque capteur, envoie périodiquement des données au broker MQTT. Le programme configure les capteurs pour mesurer les valeurs à intervalles réguliers (e.g., toutes les 10 secondes), formate les données, puis les publie via Wi-Fi sur un topic MQTT spécifique à chaque type de mesure.

## B. Installation des capteurs et configuration avec le broker MQTT sur Raspberry Pi

### **1. Configuration du broker MQTT :**

Le **Raspberry Pi** est configuré en tant que serveur MQTT pour centraliser les données IoT. Mosquitto est installé pour gérer les échanges MQTT entre les capteurs et le serveur Apache.



Figure 10 - Raspberry pi

**Paramétrage réseau** : Chaque capteur se voit assigner une adresse IP spécifique au sein du réseau hospitalier, en utilisant le protocole DHCP pour l'assignation automatique des adresses. Les ports de communication MQTT sont configurés et ouverts uniquement pour les capteurs pour limiter les accès extérieurs.

### **2. Exemple de code MQTT :**

Le code sur l'ESP8266 publie les données sur des topics structurés de manière logique, par exemple sensors/dht22/humidity pour l'humidité et sensors/mq135/value pour la qualité de l'air. Cette organisation permet une récupération ciblée des données par le serveur central et facilite la gestion des flux de données par catégorie.

Suivi des données en temps réel et visualisation pour la gestion des environnements hospitaliers

C. Suivi des données en temps réel et visualisation pour la gestion des environnements hospitaliers

**1. Application web de suivi en temps réel :**

Les données sont intégrées dans une application web en utilisant Flask en backend et Apache pour héberger le service. Les valeurs en temps réel des capteurs sont récupérées et traitées pour la visualisation dans des tableaux de bord accessibles au personnel hospitalier autorisé.

**2. Communication avec le serveur Apache :**

Le serveur Apache est configuré pour recevoir les données des capteurs via MQTT et les acheminer vers Flask, qui les rend disponibles pour l'application web. Cela permet un suivi instantané des paramètres environnementaux (température, humidité, etc.) sur une interface intuitive, accessible aux équipes de maintenance et de gestion des infrastructures.

**3. Collecte et interprétation des données avec Apache**

Apache intercepte les messages MQTT publiés par les capteurs pour les stocker temporairement dans une base de données. Un processus de polling permet de maintenir une mise à jour régulière des données sur le backend Flask, qui présente ensuite ces informations sous forme de graphique sur l'application web.

**4. Badge RFID pour l'accès restreint aux zones sensibles**

**Capteur et intégration du badge RFID :**

Un **lecteur NFC/RFID PN532** est déployé à l'entrée de certaines zones pour restreindre l'accès aux personnes autorisées. Le badge administrateur est enregistré dans le système au démarrage ; lors de chaque scan, l'UID du badge est comparé avec l'UID administrateur stocké.

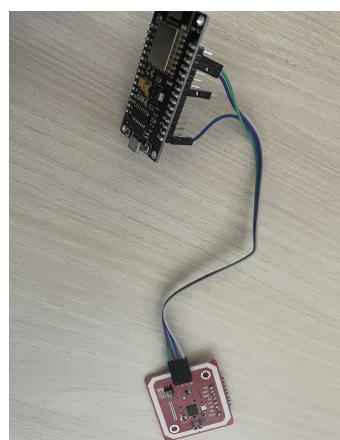


Figure 11 - Capteur du badge RFID

**5. Programmation de l'accès via MQTT :**

Lorsqu'un badge est scanné, l'ESP8266 envoie les informations au broker MQTT, qui publie un message d'accès sur un topic dédié (e.g., access/rfid). Les contrôles permettent de bloquer les accès non autorisés et de notifier le personnel en cas de badge non reconnu.

### 6. Messages d'autorisation et de refus :

En fonction de la reconnaissance du badge, le système MQTT envoie un message pour accorder ou refuser l'accès. Ces événements sont journalisés dans l'application web pour un suivi de l'accès sécurisé.

#### Accès autorisé :

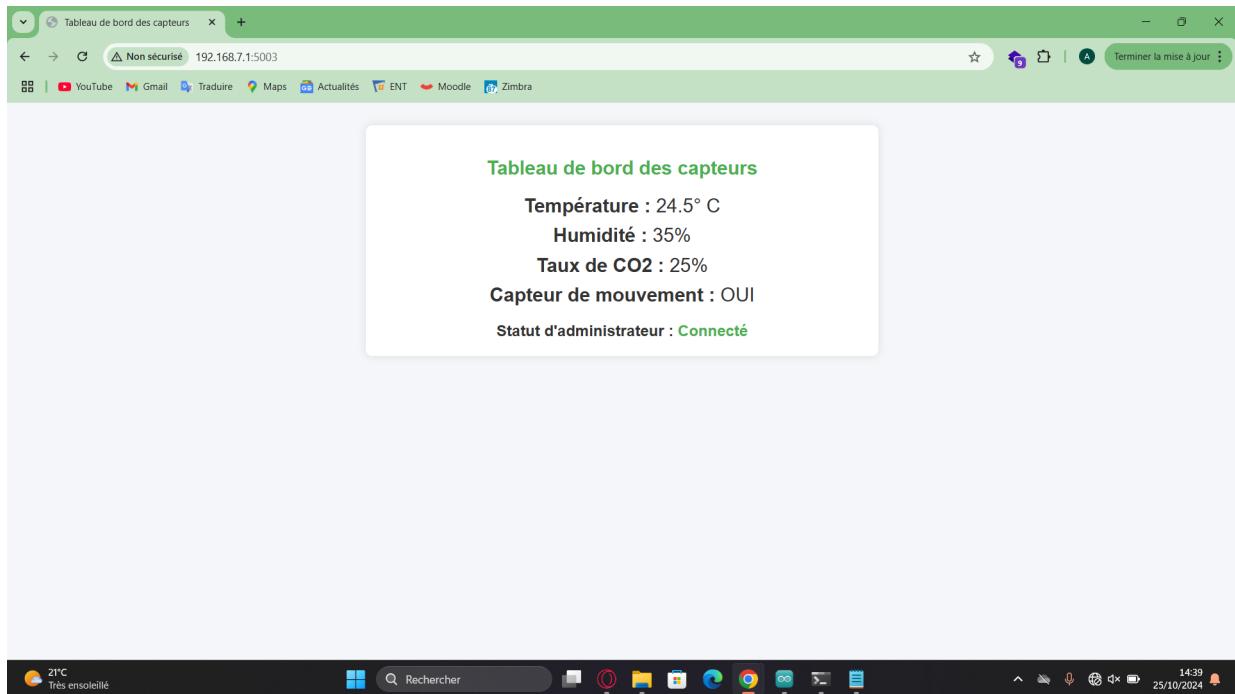


Figure 12 - Accès autorisé IOT

#### Accès non autorisé :

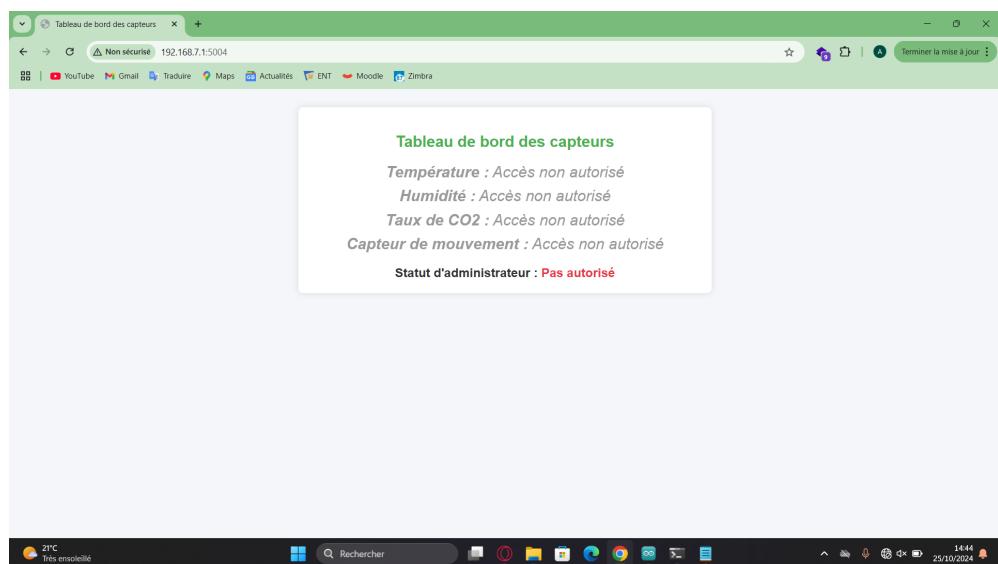


Figure 13 - Accès non autorisé IOT

## VII. Tests et validations

- A. Résultats et validation des fonctionnalités de l'application web
- B. Tests de gestion des utilisateurs et de l'accès sécurisé aux données
- C. Vérification de la consultation et de l'intégration des données IoT

## VIII. Coût total du projet

- A. Coûts des équipements et infrastructures réseau

Pour mener à bien ce projet d'infrastructure réseau sécurisée au sein de l'hôpital, il a été nécessaire de prévoir un budget conséquent pour les équipements matériels. Ces équipements constituant le socle de l'infrastructure réseau, permettant de garantir une connectivité fiable, une performance élevée et une sécurité optimale. Les éléments matériels achetés incluent des switchs, des routeurs, des serveurs et des dispositifs IoT, chacun étant sélectionné pour ses caractéristiques de sécurité et de performance adaptées aux besoins hospitaliers.

Le budget pour les équipements comprend :

- **Switches Cisco Catalyst** : Ces switchs permettent la gestion des VLAN et assurent une segmentation réseau fiable pour isoler les différents services de l'hôpital, intervenant ainsi les risques d'intrusion.
- **Routeur Stormshield** : Choisi pour ses fonctionnalités avancées de sécurité et de filtrage, ce routeur assure une protection efficace des flux de données entrants et sortants.
- **Serveurs DELL** : Utilisés pour la centralisation des données médicales et la gestion des dispositifs connectés, les serveurs sont dimensionnés pour assurer une haute disponibilité et des performances optimales.
- **Capteurs IoT et dispositifs de contrôle d'accès** : Divers capteurs (température, CO2, mouvements) et des badges RFID ont été intégrés pour la surveillance de l'environnement hospitalier et le contrôle des accès, garantissant la sécurité physique des installations.

- B. Routeurs, switchs, bornes Wi-Fi, serveurs, capteurs, etc.

Les équipements suivants ont été nécessaires pour l'infrastructure réseau :

- **Bornes Wi-Fi** : Pour garantir une connectivité mobile sécurisée dans tout l'établissement, plusieurs bornes Wi-Fi ont été installées, offrant une couverture sans fil complète et supportant un grand nombre de connexions simultanées. Les bornes sont configurées pour restreindre l'accès aux utilisateurs autorisés et respecter les règles de confidentialité.
- **Dispositifs de surveillance et de contrôle** : Des caméras connectées, des capteurs de mouvements, et des capteurs de température et de CO2 sont installés pour surveiller les conditions de sécurité dans l'hôpital

Ces équipements sont dimensionnés pour répondre aux besoins actuels de l'hôpital et sont évolutifs afin d'accompagner de futures extensions. Les coûts associés à ces équipements représentent une part importante du budget, mais ils sont indispensables pour assurer une infrastructure sécurisée, performante et adaptée aux exigences de l'hôpital.

### C. Coûts logiciels et licences

- **Stormshield** : Pour la sécurisation du réseau, la solution de pare-feu Stormshield a été choisie pour ses capacités avancées en matière de détection et de prévention des intrusions. Stormshield offre des fonctionnalités de filtrage des contenus, de protection contre les malwares, et de gestion des accès, garantissant une protection continue de l'infrastructure réseau.
- **Logiciels de monitoring** : Des logiciels de monitoring ont été intégrés pour surveiller les performances du réseau et des dispositifs IoT en temps réel. Ces logiciels permettent de détecter toute anomalie, d'alerter les administrateurs en cas de problème, et de prendre des mesures correctives rapides pour éviter les interruptions de service.

Ces solutions logicielles nécessitent des licences payantes, mais elles offrent des fonctionnalités critiques pour la protection et le suivi de l'infrastructure réseau, justifiant ainsi leur coût dans le budget total.

### D. Coûts de développement de l'application

Le développement d'une application pour la gestion et la surveillance des infrastructures a été réalisé en interne, en utilisant des technologies adaptées aux besoins spécifiques de l'hôpital. L'application a été développée en utilisant **Node.js, HTML, CSS et JavaScript**.

**Temps de développement** : Le temps de développement a été amélioré en fonction des fonctionnalités spécifiques de l'application, notamment la gestion des accès par badge RFID, le suivi des capteurs IoT, et la création de rapports pour le personnel hospitalier. Chaque fonctionnalité nécessite plusieurs cycles de développement et de tests pour garantir une interface utilisateur intuitive et une intégration parfaite avec le réseau de l'hôpital.

Le coût de développement représente principalement le temps de travail des développeurs, leur expertise en cybersécurité, et les tests nécessaires pour garantir une application fiable et sécurisée.

### E. Coûts d'installation et de formation

#### **1. Installation des équipements, configuration des VLANs**

L'installation des équipements a été réalisée par une équipe de techniciens spécialisés. Elle comprenait la configuration des switchs et des routeurs, le déploiement des VLAN pour la segmentation du réseau, et l'intégration des dispositifs de contrôle d'accès et des capteurs IoT. Ces installations ont été réalisées selon une planification rigoureuse pour minimiser les interruptions de service au sein de l'hôpital.

#### **2. Formation des utilisateurs**

Une formation a été dispensée au personnel hospitalier pour s'assurer qu'ils maîtrisent les nouvelles technologies mises en place. Cette formation inclut l'utilisation de l'application développée, la gestion des accès par badge RFID, et les bonnes pratiques de sécurité pour réduire les risques d'erreurs humaines.

Ces coûts d'installation et de formation sont essentiels pour assurer la pérennité du projet. Ils garantissent que les utilisateurs finaux sont autonomes dans l'utilisation de l'infrastructure et qu'ils peuvent répondre aux exigences de sécurité de l'hôpital.

#### F. Coût total estimé

**Estimation totale :** Le budget total pour ce projet a été coûté à **80 506,60 € TTC**, incluant la marge pour les imprévus. Ce montant couvre l'ensemble des équipements, des licences logicielles, du développement de l'application, ainsi que les coûts d'installation et de formation. La répartition est la suivante :

- Équipements matériels : 48 738,83 €
- Main-d'œuvre et installation : 18 350 €
- Marge de sécurité (20 %) : 13 417,77 €

### IX. Améliorations potentielles

#### A. Optimisation de l'application web

##### **1. Ajout de nouvelles fonctionnalités**

- **Gestion des rendez-vous** : Intégration d'une fonctionnalité de gestion des rendez-vous, permettant aux utilisateurs de planifier et de consulter les créneaux des patients. Cette fonctionnalité inclut des rappels et des notifications pour assurer une meilleure organisation.
- **Alertes et notifications** : Mise en place d'un système d'alertes qui avertit automatiquement le personnel en cas d'urgence ou de besoin de suivi pour un patient.

##### **2. Ajout de la téléphonie**

La fonctionnalité de téléphonie a été intégrée à l'application web pour permettre des appels internes entre les utilisateurs de l'hôpital, facilitant ainsi la communication entre les services (administration, médical, etc.). Cette solution utilise des simulateurs de téléphones directement sur les ordinateurs du personnel, permettant d'effectuer et de recevoir des appels sans nécessiter de téléphones physiques supplémentaires.

**Téléphonie sur PC** : La téléphonie est accessible via une interface PC, où les utilisateurs peuvent composer des numéros internes ou répondre aux appels entrants. Les simulateurs de téléphones permettent une expérience fluide, avec des fonctionnalités telles que le transfert d'appels, la mise en attente et le suivi des appels.

##### **3. Ajout de Radius et d'Active Directory pour une authentification sans mot de passe**

Un système d'authentification sans mot de passe a été mis en place en intégrant **RADIUS** et **Active Directory**. Cette configuration permet aux utilisateurs de s'authentifier de manière sécurisée sans entrer de mot de passe, simplifiant ainsi l'accès tout en renforçant la sécurité.

- **RADIUS (Remote Authentication Dial-In User Service)** : RADIUS est utilisé pour centraliser

l'authentification des utilisateurs, offrant une solution sécurisée et uniforme pour gérer les accès au réseau et à l'application.

- **Intégration avec Active Directory** : Active Directory stocke les informations d'identification des utilisateurs, permettant un contrôle d'accès basé sur les identités. Cela facilite la gestion des droits d'accès et renforce la sécurité en permettant une authentification sans mot de passe pour les utilisateurs internes.
- **Simplification de l'accès** : Les utilisateurs peuvent se connecter de manière transparente en fonction de leur identité dans Active Directory, ce qui réduit la charge administrative liée à la gestion des mots de passe et offre une expérience d'accès plus fluide.

#### **4. Amélioration de l'interface utilisateur pour plus de convivialité**

Une refonte complète de l'interface utilisateur a été réalisée pour la rendre plus intuitive et conviviale. Cette amélioration se concentre sur l'esthétique, la simplicité de navigation et l'expérience utilisateur, en utilisant des animations pour rendre l'application plus engageante et réactive.

- **Navigation simplifiée et design moderne** : L'interface a été réorganisée avec des menus clairs et une hiérarchie visuelle améliorée, permettant aux utilisateurs de trouver plus facilement les fonctionnalités. Le design moderne utilise des couleurs et des typographies uniformes pour offrir un aspect plus professionnel.
- **Animations et transitions fluides** : En intégrant des frameworks JavaScript comme **Vue.js** ou **React** et des bibliothèques CSS comme **Animate.css** ou **Bootstrap**, des animations ont été ajoutées pour améliorer l'interactivité. Par exemple :
  - **Transitions de page fluides** lors de la navigation entre différentes sections de l'application, offrant une expérience de navigation sans coupure.
  - **Animations sur les boutons et les éléments interactifs** pour donner un retour visuel immédiat lorsque les utilisateurs cliquent ou survolent des éléments.
  - **Effets de chargement et de transition** lors de l'affichage des données, pour indiquer que le contenu est en cours de chargement et pour éviter des changements brusques à l'écran.

#### B. Extension de l'IoT et collecte de nouvelles données

##### **1. Intégration de nouveaux capteurs et dispositifs de sécurité**

Pour une gestion plus fine de l'environnement et de la sécurité, de nouveaux dispositifs IoT sont intégrés dans l'infrastructure de l'hôpital. Ces dispositifs permettent de collecter des données supplémentaires et d'améliorer la surveillance en temps réel.

- **Caméras de surveillance** : Des caméras connectées sont installées dans les zones clés de l'hôpital pour surveiller les activités et renforcer la sécurité. Elles permettent une surveillance en temps réel des entrées et sorties, ainsi que des zones sensibles. Les flux vidéo sont accessibles via une interface dédiée, avec des options d'enregistrement pour l'archivage et la consultation.
- **Alarmes de sécurité** : Des systèmes d'alarme IoT sont intégrés pour détecter des intrusions, des incendies ou d'autres situations d'urgence. Ces alarmes sont connectées à l'infrastructure IoT de l'hôpital et peuvent envoyer des notifications instantanées au personnel de sécurité. L'interface de gestion permet également de tester et de réinitialiser les alarmes en cas de fausses alertes.

- **Capteurs environnementaux avancés** : Outre les capteurs de température, d'humidité et de CO<sub>2</sub>, de nouveaux capteurs de qualité de l'air, de détection de bruit et de luminosité sont ajoutés pour obtenir une surveillance complète de l'environnement hospitalier. Ces données permettent de maintenir un environnement optimal pour les patients et le personnel.

## 2. Développement d'un site de gestion IoT pour l'hôpital

Un site web dédié est développé pour centraliser la gestion de tous les objets connectés de l'hôpital. Cette interface permet au personnel technique de surveiller, contrôler et configurer chaque dispositif IoT en temps réel.

- **Tableau de bord de gestion** : Le site web offre un tableau de bord centralisé où les utilisateurs peuvent visualiser l'état de tous les dispositifs IoT (caméras, alarmes, capteurs). Chaque dispositif est représenté avec son statut actuel, et les alertes ou anomalies sont mises en évidence pour une réponse rapide.
- **Contrôle des caméras et alarmes** : Depuis l'interface, le personnel de sécurité peut accéder aux flux des caméras en temps réel, ajuster l'angle de certaines caméras, ou encore déclencher des alarmes manuellement si nécessaire. Ils peuvent également configurer les paramètres des alarmes pour adapter les seuils de déclenchement en fonction des besoins.
- **Notifications et alertes** : Le site de gestion IoT inclut un système de notifications qui informe automatiquement le personnel en cas de détection d'une anomalie (par exemple, un niveau de CO<sub>2</sub> élevé ou une intrusion détectée par les caméras). Les alertes peuvent être envoyées par email ou SMS, selon la configuration.

Grâce à l'extension de l'IoT avec de nouveaux capteurs, des caméras et des alarmes, ainsi qu'à la mise en place d'une interface de gestion centralisée, l'hôpital peut désormais assurer une surveillance plus fine de l'environnement et une sécurité renforcée, contribuant ainsi à un environnement plus sûr et mieux contrôlé pour le personnel et les patients.

## X. Conclusion

### A. Bilan du projet et atteinte des objectifs

Le projet Secure Links a permis de répondre aux objectifs initiaux en concevant une infrastructure réseau sécurisée et une application adaptée aux besoins de l'hôpital HealthCare 24/7. Grâce à la segmentation en VLANs, l'intégration de capteurs IoT avec une communication sécurisée par MQTT, et la gestion des accès utilisateurs via badges RFID, l'équipe a réussi à créer un environnement sécurisé et fonctionnel pour la gestion des données hospitalières. L'application de gestion des patients et des imprimantes offre une interface intuitive pour le personnel médical, et le système de monitoring des conditions environnementales améliore la réactivité face aux variations d'environnement dans les salles sensibles. Les tests finaux ont démontré la fiabilité et la robustesse de l'infrastructure mise en place, assurant ainsi une conformité avec les exigences de sécurité et de continuité des opérations.

### B. Perspectives futures et retours sur expérience

À travers ce projet, l'équipe de Secure Links a pu approfondir ses connaissances en cybersécurité, en gestion de réseaux IoT, et en développement d'applications dans un contexte critique. Plusieurs pistes d'améliorations ont été identifiées pour de futurs développements, notamment l'intégration de notifications en temps réel pour les incidents de sécurité, l'ajout d'analyses de données pour détecter les anomalies, et l'optimisation de l'interface utilisateur pour une meilleure ergonomie. En termes de retour d'expérience, le projet

a renforcé la capacité de l'équipe à collaborer sur des problématiques techniques complexes et à adopter une approche méthodique dans la résolution des défis liés à la sécurité des données sensibles. L'équipe envisage d'appliquer ces compétences dans des projets futurs, tout en restant à l'écoute des avancées technologiques dans le domaine de la cybersécurité et de l'IoT.

<i>Figure 1 - Schéma du réseau.....</i>	6
<i>Figure 2 - Vlan configuration .....</i>	8
<i>Figure 3 - VLAN sur Stormshield .....</i>	9
<i>Figure 4 - DHCP Stormshield.....</i>	10
<i>Figure 5 - Règle Stormshield .....</i>	11
<i>Figure 6 - Configuration hôpital.....</i>	11
<i>Figure 7 - Règle authentification .....</i>	12
<i>Figure 8 - règle de routage .....</i>	13
<i>Figure 9 - Capteur IOT.....</i>	18
<i>Figure 10 - Rasberry pi.....</i>	19
<i>Figure 11 - Capteur du badge RFID.....</i>	20
<i>Figure 12 - Accès autorisé IOT .....</i>	21
<i>Figure 13 - Accès non autorisé IOT .....</i>	21