

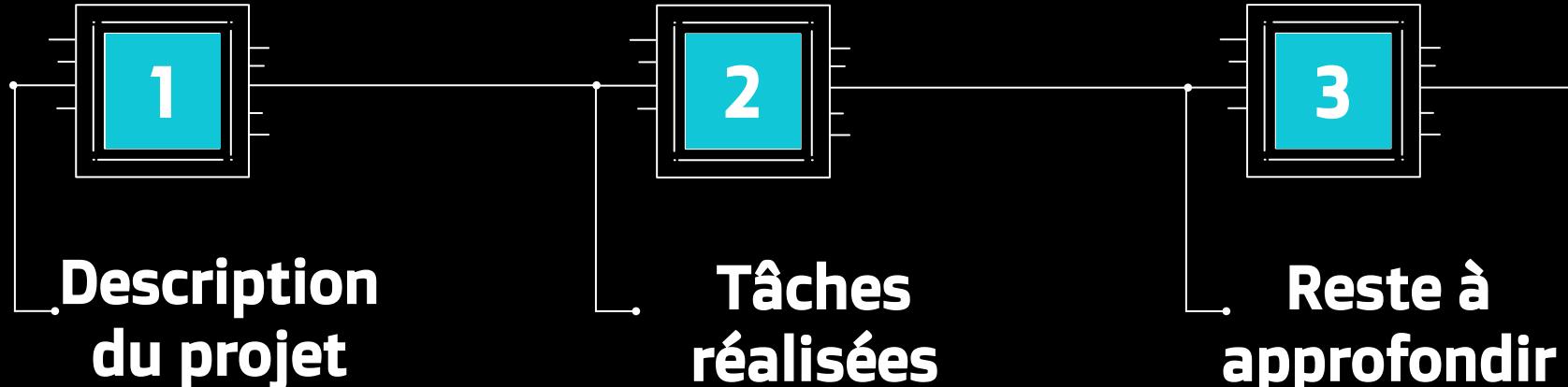


Mise en réseaux de deux cliniques

Rendu final

ECOTIERE Léo
HIMMI Adam
HIRSCH Matéo
DEUSCHER Lucas
LOUREIRO Hugo

Sommaire



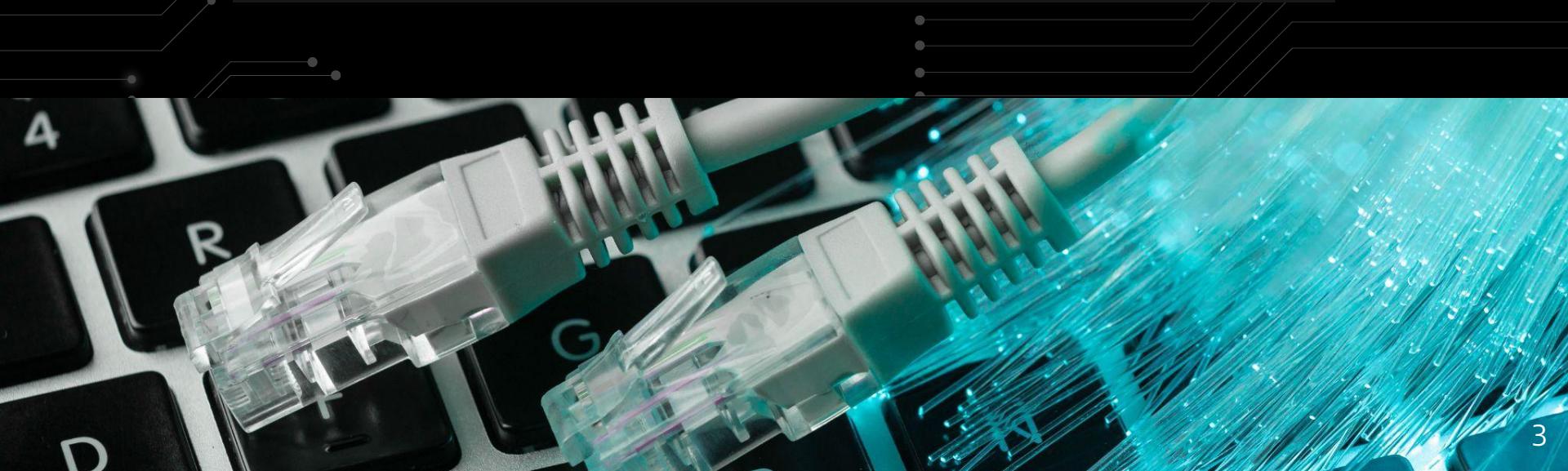
- Présentation du projet
- Déroulement du projet
- Organisation

- Schéma de la solution technique
- Différentes captures des réalisations
- Problèmes rencontrés

- Points améliorations

01

Description du projet





Projet proposé :

Sécuriser au mieux le système informatique d'un hôpital :

1. Organiser la mise en place d'un réseau sécurisé afin de protéger le matériel et les données médicales d'un hôpital.
2. L'architecture du réseau doit définir 4 espaces séparés : la direction, l'administration de l'hôpital et la gestion des données médicales.
3. L'accès sur le réseau de l'hôpital sera sécurisé avec la norme 802.1X sur les parties filaire et sans fil afin d'identifier les droits de chaque utilisateur dans le réseau.
4. Un accès par VPN sur un site secondaire tout en respectant les différentes normes de sécurité.

Déroulement du projet

Intitulé	Objectif	Lun	Mar	Mer	Jeu	Ven	Sam	Dim	Lun	Mar	Mer	Jeu	Ven
Organisation	Lecture du projet et création d'un Trello												
Création des documentations	Créer différents documents pour le projet												
Création des bases de données	Création des bases de données et communication avec les badges												
Configuration des équipements réseaux	Configuration des serveurs, routeurs et switchs + cœur de réseau sur gns3												
Gestion des badges	Gestion des badges et communication avec les bases de données												
Stormshield	Configuration du pare-feux + VPN												

Organisation

SAE501

Tâches à faire

- Codage application Android
- Configuration Caméras

+ Ajouter une carte

Tâches en cours

- Codage application web
- Configuration réseau
- Sprints
- Install & Config serveurs

+ Ajouter une carte

Tâches réalisées

- Plan IP
- Document de formation
- Rapport de Sécurité
- Schéma d'architecture
- Base de Données

+ Ajouter une carte

Partagés avec moi > SAE 501 - Piloter un proj... ▾

Type Contacts Date de modification

Nom	Propriétaire	D
Capture écran	Mateo	16
Codes	Mateo	16
Documents	Mateo	16

Création d'un Trello et d'un drive :

- Chacun à des tâches attribuées
- Suivi continu de l'avancement du projet
- Permet de faire des tâches en parallèles
- Permet l'archivage et le versionning.
- Permet la gestion des accès

02 Tâches réalisées

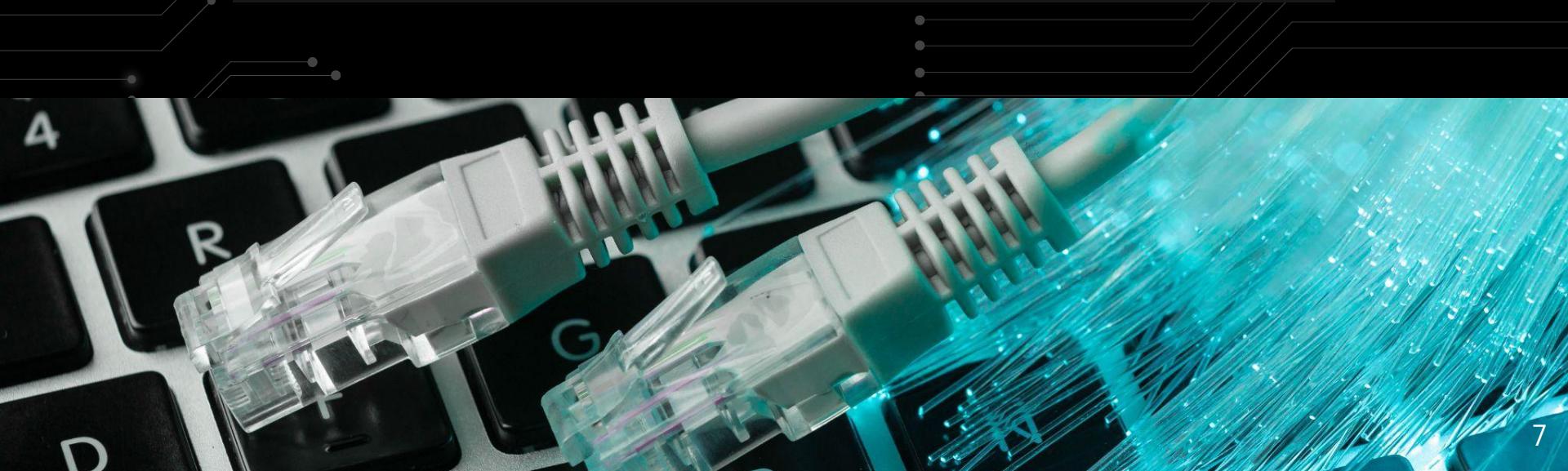
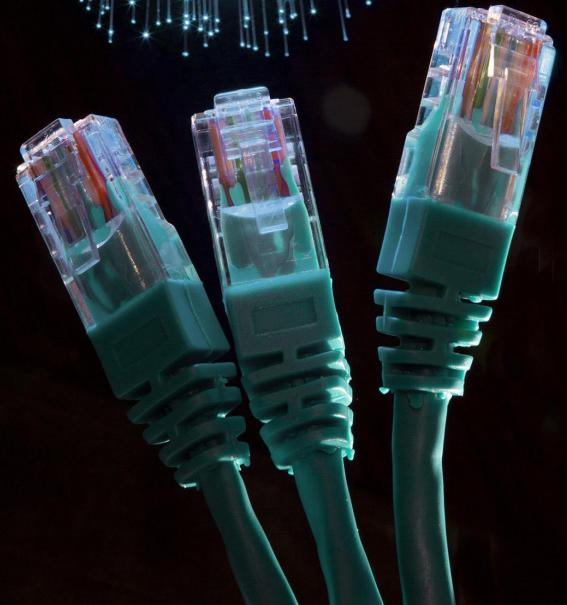
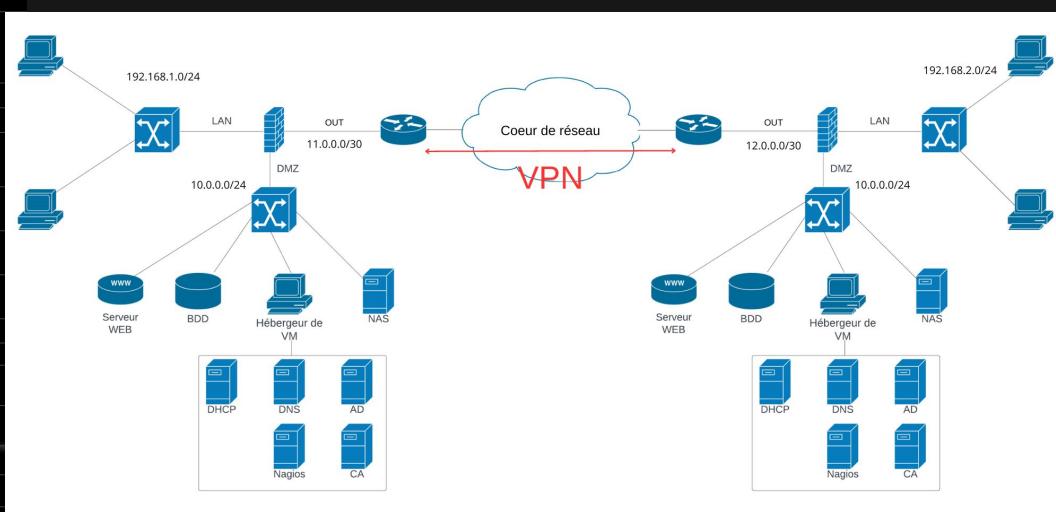


Schéma de la solution proposée



Configuration des routers

```
interface GigabitEthernet0/0
 ip address 11.0.0.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 13.0.0.1 255.255.255.252
 duplex auto
 speed auto
!
```

Configuration IP

```
router ospf 10
 redistribute connected subnets
 network 11.0.0.0 0.0.0.3 area 0
 network 13.0.0.0 0.0.0.3 area 0
!
```

Configuration OSPF

```
ip ssh time-out 60
ip ssh logging events
ip ssh version 2
```

Activation SSH

Configuration des switchs

101	administration	active	Gi2/0/1, Gi2/0/2, Gi2/0/3 Gi2/0/4, Gi2/0/5
102	gestion	active	Gi2/0/6, Gi2/0/7, Gi2/0/8 Gi2/0/9, Gi2/0/10
103	medical	active	Gi2/0/11, Gi2/0/12, Gi2/0/13 Gi2/0/14, Gi2/0/15
1002	fdci-default		

Configuration des 3 VLANs

```
interface GigabitEthernet2/0/23
switchport mode trunk
```

Configuration du trunk

Configuration des Firewalls

DHCP

PLAGE D'ADRESSES

Rechercher...	Ajouter
Plage d'adresses	Passerelle
dhcp_wifi	Firewall_AP_CLINIQUE_B
dhcp_lan	Firewall_in

RÉSERVATION

Rechercher...	Ajouter
Réservation	Passerelle
SRV_WEB	default

FILTRAGE ET NAT

Filtrage

(10) SAE Activer cette politique | Éditer | Exporter | Allez-n

Etat	Trafic original (avant translation)			Trafic après translation			Protocole	Opt
	Source	Destination	Port dest.	Source	Port src.	Protocole		
on	Any interface: AP_CLINIQUE	Firewall_AP_CLI	https	Firewall_bric	ephemeral_fw	S	h	
on	Any interface: AP_CLINIQUE	Firewall_AP_CLI	http	Firewall_bric	ephemeral_tw	S	h	
on	Any interface: AP_CLINIQUE	Any	Any	Firewall_AP_	ephemeral_tw	A		
on	PC-client	Any interface: out	Any	ARP	Firewall_			
on	Any interface: out	ARP	Firewall_out	Any			P	

CONFIGURATION DE L'INTERFACE

Nom du réseau : AP_CLINIQUE_B
Authentification : WPA 2
Clé de sécurité : Isolation AP

Plan d'adressage

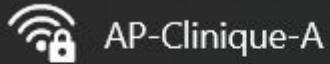
Aucun (interface désactivée)
IP fixe (statique)
Plan d'adressage hérité du bridge

Sélectionnez un bridge

Ajouter Supprimer

Adresse IP	Masque réseau
192.168.0.254	255.255.255.0

Configuration des FireWalls



AP-Clinique-A



Wifi activé

Authentification Interne

nom.prenom

Mot de passe

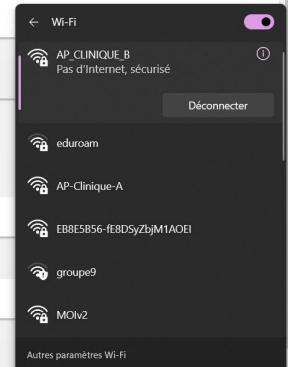
Connexion

Authentification Externe

nom.prenom

Mot de passe

Connexion
©DataSafe Systems 2023



Accès à l'application WEB depuis le wifi du FW

Capture relations phpMyAdmin

The screenshot shows the phpMyAdmin interface for managing database relations. On the left, the database structure is visible with two main databases: SAE501_privée and SAE501_publique. Under SAE501_privée, there are four tables: operations, personnels, matériaux, and salles. Under SAE501_publique, there are three tables: patient, personnel, and salle. The current view is on the 'operations' table's relations page. It displays four foreign key constraints being defined:

- Constraint 1: Relates 'operations' to 'matériel'. It has an ON DELETE RESTRICT clause.
- Constraint 2: Relates 'operations' to 'patient'. It has an ON DELETE RESTRICT clause.
- Constraint 3: Relates 'operations' to 'personnel'. It has an ON DELETE RESTRICT clause.
- Constraint 4: Relates 'operations' to 'salle'. It has an ON DELETE RESTRICT clause.

The interface includes tabs for Parcourir, Structure, SQL, Rechercher, Insertion, Exporter, Importer, Privileges, and Plus. A bottom navigation bar shows links to navigation.php, requetes.php, and index.php.

- Installation de phpMyAdmin (MariaDB), Apache2 & PHP7 sur le serveur Web
- Création des deux bases (publique et privée)
- Création des différentes tables dans les bases
- Mise en place des relations entre les tables

The screenshot shows a Mozilla Firefox browser window with multiple tabs open. The active tab is titled "Page d'Accueil". The page content is an internal authentication form titled "Authentification Interne". It contains fields for "nom.prenom" and "Mot de passe". Below the form, a note says "Connexion". Further down, another section titled "Authentification Externe" is visible, also with "nom.prenom" and "Mot de passe" fields. The browser status bar at the bottom right shows "©DataSafe Systems 2023".

Page authentication

Création de différentes page Web :

- Accueil
- Ajout/Suppression d'un personnel/patient/matériel/salle
- Authentification
- Consultation par le personnel/patient

Capture script Active Directory

```
@echo off
REM Configure la page de code de la console en UTF-8 pour les caractères spéciaux
chcp 65001 > nul

REM Crée une unité d'organisation (OU) nommée "Qualite" dans Le domaine "GSB.COM"
dsadd ou OU=Qualite,DC=GSB,DC=COM

REM Crée des groupes à partir des noms dans le fichier "groupe.txt"
FOR /F %%i in (groupe.txt) do (
    dsadd group "CN=%%i,OU=Qualite,DC=GSB,DC=COM"
)

REM Lit le fichier "utilqualite.txt" et effectue des actions pour chaque ligne
FOR /F "tokens=1,2,3 skip=1" %%i in (utilqualite.txt) DO (
    REM Crée un nouvel utilisateur avec divers paramètres
    dsadd user -loscr login=Qualite.bat "CN=%%i,OU=Qualite,DC=GSB,DC=COM" -memberof "CN=%%i,OU=Qualite,DC=GSB,DC=COM" -disabled no -pwd Test1234 -hmdir M: -profile \\SRVCLINIQUE-A\Perso\%%i
    REM Configure les autorisations sur le répertoire "C:\Travail\%%i"
    icacls C:\Travail\%%i /grant %%i:M
    icacls C:\Travail\%%i /grant administrateur:F
    icacls C:\Travail\%%i /inheritaunce:R
    REM Partage le répertoire "%%i" via le réseau
    net share %%i=C:\Travail\%%i
)

REM Crée des répertoires en fonction des informations dans "utilqualite.txt"
FOR /F "tokens=1,2,3 skip=1" %%i in (utilqualite.txt) do (
    mkdir C:\Perso\%%i\%%i
)

REM Configure les autorisations sur les répertoires créés
FOR /F "tokens=1,2,3 skip=1" %%i IN (utilqualite.txt) DO (
    icacls C:\Perso\%%i /grant %%i:M
    icacls "C:\Perso\%%i\%%i" /grant "%%i:M"
    icacls "C:\Perso\%%i\%%i" /inheritaunce:R
    REM Met en pause le script
)
```

Permet de déployer l'Active Directory sur un Windows Server 2019

Capture script DHCP

```
Import-Module DhcpsServer

# Ajout DHCP nommée "Administration" pour des adresses de gestion
Add-DhcpServerv4Scope -Name "Administration" -StartRange "192.168.1.10" -EndRange "192.168.1.200" -SubnetMask "255.255.255.0" -State Active

# Ajout DHCP nommée "DMZ" pour des adresses de La zone démilitarisée
Add-DhcpServerv4Scope -Name "DMZ" -StartRange "10.0.0.40" -EndRange "10.0.0.200" -SubnetMask "255.255.255.0" -State Active

# Ajout DHCP nommée "Gestion" pour des adresses de gestion
Add-DhcpServerv4Scope -Name "Gestion" -StartRange "192.168.10.10" -EndRange "192.168.10.200" -SubnetMask "255.255.255.0" -State Active

# Ajout DHCP nommée "Medical" pour des adresses médicales
Add-DhcpServerv4Scope -Name "Medical" -StartRange "192.168.12.10" -EndRange "192.168.12.200" -SubnetMask "255.255.255.0" -State Active

# Assignment de La route par défaut à chaque étendue
Set-DhcpServerv4OptionValue -OptionID 003 -ScopeId 192.168.1.0 -Value "192.168.1.254"
Set-DhcpServerv4OptionValue -OptionID 003 -ScopeId 192.168.10.0 -Value "192.168.10.254"
Set-DhcpServerv4OptionValue -OptionID 003 -ScopeId 192.168.12.0 -Value "192.168.12.254"
```

Permet de déployer un serveur DHCP sur un Windows Server 2019

Zabbix

Global view

Tous les tableaux de bord / Global view

HOME ZABBIX SRVA SRVBACKUP STORMSHIELD

Disponibilité de l'hôte

2 Disponible	0 Non disponible	0 Inconnu	2 Total
--------------	------------------	-----------	---------

Problems by severity

0 Désastre	0 Haut	0 Moyen	2 Avertissement	0 Information	0 Non classé
------------	--------	---------	-----------------	---------------	--------------

Current problems

Temps	Info	Hôte	Problème + Sévérité	Durée	Actualiser	Actions	Tags
11:11:37	SRVBACKUP	KUP	Windows: Host has been restarted. (uptime < 10m)	11m 3s	Actualiser	class: os component: system	scope: notice ...
11:00	SERVCLINIQUE-A		Windows: System time is out of sync. (diff with Zabbix server > 60s)	56m 18s	Actualiser	class: os component: system	scope: notice ...

Top hosts by CPU utilization

NAME	CPU USE	SPACE USE
SRVBACKUP	3.1 %	86 %
SERVCLINIQUE-A	0.9 %	53 %

Zabbix server problems

Temps	Moment de la récupération	Etat	Info	Hôte	Problème + Sévérité	Durée	Actualiser	Actions
Aucune donnée trouvée.								

UPTIME

2023-10-27 11:23:00

02:07:08↑

CPU USE

SPACE USE

RAM USE

```

69 void loop()
70 {
71     uint8_t success;
72     uint8_t uidLength;
73     uint8_t uid[] = {0, 0, 0, 0, 0, 0, 0, 0};
74
75     success = nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A, uid, &uidLength);
76
77     if (success)
78     {
79         Serial.println("Carte détectée !");
80         digitalWrite(LED_BUILTIN, HIGH); // Allume la LED intégrée
81         delay(1000); // Attend une seconde
82         digitalWrite(LED_BUILTIN, LOW); // Éteint la LED intégrée
83
84         Serial.print("Longueur UID: ");
85         Serial.print(uidLength, DEC);
86         Serial.println(" octets");
87         Serial.print("Valeur UID: ");
88
89         for (uint8_t i = 0; i < uidLength; i++)
90         {
91             Serial.print("0x");
92             Serial.print(uid[i], HEX);
93             Serial.print(" ");
94         }
95         Serial.println("");
96
97         // Transforme l'UID en décimal et l'affiche
98         String decimalUID = byteArrayToString(uid, uidLength);
99         Serial.print("Valeur UID (décimal): ");
100        Serial.println(decimalUID);
101
102        // Prépare la requête HTTP
103        HttpClient http;
104        String url = (String)serverAddress + "?uid=" + decimalUID; // Inclut l'UID dans l'URL de la requête
105
106        Serial.print("URL de la requête : ");
107        Serial.println(url); // Affiche l'URL de la requête
108
109        WiFiClient client;
110        http.begin(client, url);
111

```

Code du Lecteur RFID :

- Initialisation du lecteur/graveur RFID
- Détection d'un badge RFID
- Remonté de l'identifiant RFID à la BdD

```
Carte détectée !
Longueur UID: 4 octets
Valeur UID: 0xD0 0xAB 0x1 0x9C
Valeur UID (décimal): 2081711156
URL de la requête : http://10.0.0.10/check_badge.php?uid=2081711156
Réponse du serveur :
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <link rel="stylesheet" href="style.css"/>
    </head>
    <body>
        yes      </body>
</html>

Accès autorisé
```

```
Carte détectée !
Longueur UID: 4 octets
Valeur UID: 0x29 0xD6 0x96 0xC4
Valeur UID (décimal): 41214150196
URL de la requête : http://10.0.0.10/check_badge.php?uid=41214150196
Réponse du serveur :
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <link rel="stylesheet" href="style.css"/>
    </head>
    <body>
        no      </body>
</html>

Accès non autorisé
```

Exemple lecteur RFID :

- Exemple lecteur de badge
- Autorisation des accès
- Ajout d'ID badge RFID dans la BDD

Fait !

[Deconnexion](#)

Numéro :

231568765413

Propriétaire :

Bichon Joseph

Envoyer

Budget

Hôpital de campagne

Décomposition de prix globale et forfaitaire

PRÉSTATION MATERIEL, LOGICIEL et D'INTEGRATION				
Désignation	Qté	Unité	Prix Unitaire HT	Prix HT
Système de communication et applications				
Serveur de communication	1	Ensemble	14 760,00 €	14 760,00 €
Serveur de communication de secours	1	Ensemble	7 570,80 €	7 570,80 €
Poste IP	30	Unité(s)	129,60 €	3 888,00 €
Poste sans fil DECT	11	Unité(s)	70,70 €	777,70 €
Applications de téléphonie	1	Ensemble	5 300,00 €	5 300,00 €
Application de Téléphonie sur PC	1	Ensemble	5 300,00 €	5 300,00 €
Application de distribution d'appels pour la gestion de crise	1	Ensemble	9 068,90 €	9 068,90 €
Serveurs et commutateur	1	Ensemble	176,70 €	176,70 €
Infrastructure de réseau LAN et WLAN				
Serveur de gestion des données	4	Unité(s)	2 650,00 €	10 600,00 €
1 VLAN pour les données administratives	1	Unité(s)	265,00 €	265,00 €
1 VLAN pour les données médicales	1	Unité(s)	265,00 €	265,00 €
1 VLAN de direction	1	Unité(s)	265,00 €	265,00 €
Routeur Cisco 1841/900	1	Unité(s)	463,80 €	463,80 €
Switch 24 ports Niveau 3 100/1000Base T PoE 802.3af	2	Unité(s)	596,30 €	1 192,60 €
Module de stack 10 Gigabit pour switch 24 ports	2	Unité(s)	145,80 €	291,60 €
Module 1000Base LX	4	Unité(s)	112,70 €	450,80 €
Point d'accès Wifi 802.11n / 1 port 1000Base T avec support mural	2	Unité(s)	165,70 €	331,40 €
Port Wifi 802.11abg avec supports et mat de fixation	2	Unité(s)	1 060,00 €	2 120,00 €
Sécurité des accès Internet				
Firewall Stormshield	1	Unité(s)	1 817,20 €	1 817,20 €
Filtrage Firewalls avec une année de mise à jour	1	Unité(s)	454,30 €	454,30 €
Prévention des intrusions avec une année de mise à jour	1	Unité(s)	302,90 €	302,90 €
Tracabilité des accès visiteurs				
Application de tracabilité des accès	1	Ensemble	3 785,80 €	3 785,80 €
Sauvegarde des alimentations électriques				
Onduleur SKVA + batterie et câblage	1	Ensemble	3 445,00 €	3 445,00 €
Infrastructures de câblage				
Local Technique et câblage hôpital	1	Ensemble	1 590,00 €	1 590,00 €
Prestation d'intégration				
Collecte de données	1,5	Jour(s)	1 040,00 €	1 560,00 €
Prise en charge et mise en service systèmes, applications et réSEAUNES	12,9	Jours(s)	320,00 €	4 128,00 €

Création d'une DPGF (Décomposition du Prix Global Forfaitaire) :

- Permet de déterminer le prix de chaque produits/services
- Calculer la marge dégagée
- Calculer le prix de revient commercial et le prix de revient pour le client

	Prix d'achat	Prix de revient commercial unitaire	Prix de revient commercial total	Marge
12 532,00 €	13 283,92 €	13 283,92 €	10%	
6 428,00 €	6 813,68 €	6 813,68 €	10%	
110,00 €	116,60 €	1 632,40 €	10%	
60,00 €	63,60 €	63,60 €	10%	
4 500,00 €	4 770,00 €	4 770,00 €	10%	
4 500,00 €	4 770,00 €	4 770,00 €	10%	
7 700,00 €	8 162,00 €	8 162,00 €	10%	
150,00 €	159,00 €	159,00 €	10%	

Exemple devis client

La campagne

Décomposition de prix globale et

PRESTATION MATERIEL, LOGICIEL et D'INTEGRATION				
Désignation	Qté	Unité	Prix Unitaire HT	Prix HT
Système de communication et applications				
Serveur de communication	1	Ensemble	14 760,00 €	14 760,00 €
Serveur de communication de secours	1	Ensemble	7 570,80 €	7 570,80 €
Poste IP	30	Unité(s)	129,60 €	3 888,00 €
Poste sans fil DECT	11	Unité(s)	70,70 €	777,70 €
Applications de téléphonie	1	Ensemble	5 300,00 €	5 300,00 €
Application de Téléphonie sur PC	1	Ensemble	5 300,00 €	5 300,00 €
Application de distribution d'appels pour la gestion de crise	1	Ensemble	9 068,90 €	9 068,90 €
Serveurs et commutateur	1	Ensemble	176,70 €	176,70 €
Infrastructure de réseau LAN et WLAN				
Serveur de gestion des données	4	Unité(s)	2 650,00 €	10 600,00 €
1 VLAN pour les données administratives	1	Unité(s)	265,00 €	265,00 €
1 VLAN pour les données médicales	1	Unité(s)	265,00 €	265,00 €

PRESTATION DE SERVICES				
Désignation	Qté	Unité	Prix HT annuel	Prix HT annuel
Service de maintenance	1	Ensemble	1 300,00 €	1 300,00 €
Service d'assistance utilisateurs	1	Ensemble		
Service de mise à jour software système téléphonique	1	Ensemble		
			TOTAL HT Annuel	1 300,00 €
			TVA 20%	260,00 €
			TOTAL TTC Annuel	1 560,00 €

OPTIONS SERVICE DE FILTRAGE URL ET PREVENTION DES INTRUSIONS				
Désignation	Qté	Unité	Prix HT annuel	
Service de mise à jour filtrage URL et sonde de prévention des intrusions	1	Année		0,00 €
			TOTAL HT	0,00 €
			TVA 20%	0,00 €
			TOTAL TTC	0,00 €

PRIX	Qté	Unité	Prix TTC annuel
PRESTATION MATERIEL, LOGICIEL et D'INTEGRATION	1	Ensemble	97 644,60 €
PRESTATION DE SERVICES	1	Ensemble	1 560,00 €
OPTIONS SERVICE DE FILTRAGE URL ET PREVENTION DES INTRUSIONS	1	Ensemble	0,00 €
			TOTAL TTC
			99 204,60 €

24.29%

Marge dégagée de l'entreprise

61 607.20 €

Prix de revient commercial total

81 370.50 €

Côut total (HT)

Bilan économique	
Détail économique (PRC)	61 607,20 €
Prix de revient commercial total	81 370,50 €
Prix de vente total	19 763,30 €
Marge brut	24,29%
Taux de marge	

Marge	
Téléphonie	10,0%
Réseaux	20,0%
Sécurité accès internet + traçabilité	30,0%
Alimentation câblage	20,0%

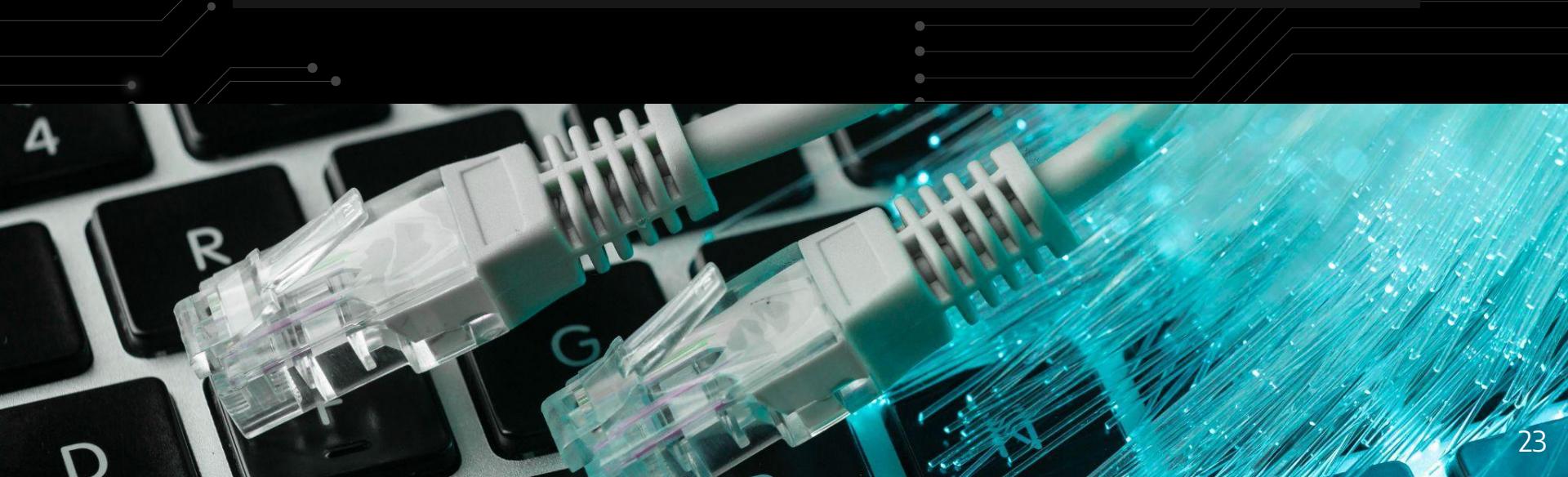
Les problèmes rencontrés

- Temps dédié inégalement réparti et insuffisant
- Pas de droit “root” sur les PCs dans les salles -> Utilisation de PCs portables
- Mauvais adressage mémoire dans les configurations des routeurs Cisco
- Défaillance matérielle de certains portables
- Comportement totalement imprévisible des firewalls Stormshield
- Cahier des charges extrêmement changeant



03

Reste à approfondir



Les points d'améliorations

- Implémentation d'un VPN site à site entre les cliniques
- Mise en place de MPLS et de VRF pour le coeur de réseau
- Haute Disponibilité
- Ajout de serveur d'authentification dédié (Radius)
- Ajout de caméra de surveillance
- Ajout de différents capteurs (température, hydrométrie...)
- Ajout d'un système de téléphonie IP
- Mise en place de suite ELK (ElasticSearch, Kibana, Beats & Logstash)
- Monitorer toute l'infra à l'aide de Zabbix (Via SNMP)
- Avoir un seul script
- Association salle <--> badge d'accès



Merci

**Nous sommes prêt à répondre à vos
questions.**

