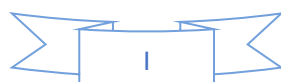




## ***DÉDICACES***

*À ma famille ;*



## **REMERCIEMENTS**

Je tiens tout d'abord à exprimer ma profonde gratitude envers l'École Supérieure d'Industrie de l'Institut National Polytechnique Félix Houphouët Boigny, et plus particulièrement envers *M. OUATTARA Adama*, Directeur de l'ESI, ainsi que notre Directeur des études, *M. KPO Loua Daniel*, pour avoir intégré des modules indispensables, y compris ce stage de fin d'étude, comme parties intégrantes de notre formation. L'accompagnement administratif et académique dont j'ai bénéficié m'a permis de trouver rapidement un stage, dans le but d'affiner mes compétences et de valider mon cycle à travers un projet de fin d'étude.

J'adresse des remerciements particuliers à mon encadreur pédagogique, *M. KONAN N'Dri*, pour son accompagnement magistral. Grâce à lui, j'ai pu maintenir une approche en adéquation avec les fondamentaux pédagogiques et académiques de l'institut.

Je tiens également à exprimer ma sincère reconnaissance envers *M. DIAKITÉ Check Amadou Tidiane*, Directeur Général de DCAT, qui a cru en mon potentiel et m'a accueilli au sein de son entreprise. À cet égard, je souhaite particulièrement remercier *M. BOGNINI Jean Abraham* qui m'a épaulé et conseillé, et qui m'a surtout transmis son expertise dans le domaine des Réseaux Informatiques. Mes remerciements s'adressent également à toute l'équipe de DCAT, notamment *M. KOICHY Don Sylvain*, *Mme. DIALLO Fanta*, *M. KOSSÉRÉ Jean-Jacques*, *M. SIMBORO Mohamed* et *M. DOUMBIA Abdoulaye*.

Ce stage m'a permis de mettre en pratique et d'affiner certaines compétences et connaissances acquises au cours de ces trois dernières années académiques, tout en découvrant les méthodes et moyens utilisés en situation réelle au sein d'une entreprise. Il constitue également l'aboutissement de mon parcours en cycle de Technicien Supérieur 2021-2024.

Je n'oublie surtout pas de remercier mes proches qui m'ont soutenu et aidé tout au long de la période de ce stage, que ce soit financièrement, émotionnellement ou spirituellement.

## AVANT-PROPOS

L'Institut National Polytechnique Félix Houphouët-Boigny (INP-HB) de Yamoussoukro a été créé en septembre 1996 par le décret N°96-678, résultant de la fusion de quatre grandes écoles: l'École Nationale Supérieure d'Agronomie (ENSA), l'École Nationale Supérieure des Travaux Publics (ENSTP), l'Institut Agricole de Bouaké (IAB), et l'Institut National Supérieur de l'Enseignement Technique (INSET). Cette fusion visait à revitaliser ces institutions en vue de former une jeunesse capable de relever les défis du monde professionnel et de faire de Yamoussoukro une technopole.

Aujourd'hui, l'INPHB regroupe neuf écoles :

- l'École Supérieure d'Industrie (ESI),
- l'École Supérieure d'Agronomie (ESA),
- l'École Supérieure de Commerce et d'Administration des Entreprises (ESCAE),
- l'École Supérieure des Travaux Publics (ESTP),
- l'École Supérieure des Mines et de Géologie (ESMG),
- l'École de Formation Continue et de Perfectionnement des Cadres (EFCPC),
- les Classes Préparatoires aux Grandes Écoles (CPGE),
- l'École Doctorale Polytechnique (EDP),
- l'École Supérieure du Pétrole et de l'Énergie (ESPE).

Notre formation en tant que Technicien Supérieur en Informatique se déroule à l'ESI, qui est chargée de former des ingénieurs et des techniciens supérieurs dans les principaux domaines de l'industrie. En fin d'étude, dans le cadre de cette formation, des stages pratiques en entreprise sont organisés pour permettre aux étudiants de mettre en pratique leurs connaissances acquises au cours de leur cycle académique et de les confronter aux réalités du monde professionnel. C'est dans ce cadre que l'entreprise *Data Communications and All Technologies (DCAT)* nous a accueilli du 02 Avril au 07 Juin 2024 pour réaliser le projet présenté dans ce mémoire.

# SOMMAIRE

<b>DÉDICACES</b> .....	I
<b>REMERCIEMENTS</b> .....	II
<b>AVANT-PROPOS</b> .....	III
<b>SOMMAIRE</b> .....	IV
<b>LISTE DES FIGURES, ILLUSTRATIONS ET TABLEAUX</b> .....	V
<b>LISTE DES SIGLES ET ABRÉVIATIONS</b> .....	VI
<b>RÉSUMÉ</b> .....	VIII
<b>INTRODUCTION</b> .....	1
<b>PARTIE I : CADRE ET CONTEXTE DU PROJET</b> .....	2
<b>CHAPITRE I : PRÉSENTATION DE LA STRUCTURE D'ACCUEIL</b> .....	3
<b>CHAPITRE II : DESCRIPTION DU PROJET</b> .....	6
<b>PARTIE II : ÉTUDE CONCEPTUELLE</b> .....	10
<b>CHAPITRE III : ENQUÊTES ET ÉTAT DES LIEUX</b> .....	11
<b>CHAPITRE IV : ÉTUDE DE FAISABILITÉ</b> .....	14
<b>CHAPITRE V : CONCEPTION DU SYSTÈME</b> .....	23
<b>PARTIE III : MISE EN ŒUVRE DU SYSTÈME</b> .....	30
<b>CHAPITRE VI : IMPLÉMENTATION DES TECHNOLOGIES</b> .....	31
<b>CHAPITRE VII : BILAN DE LA MISE EN ŒUVRE DU PROJET</b> .....	64
<b>PARTIE IV : BILAN DU STAGE</b> .....	68
<b>CHAPITRE VIII : DÉROULEMENT DU STAGE</b> .....	69
<b>CONCLUSION</b> .....	73
<b>BIBLIOGRAPHIE</b> .....	IX
<b>WEBOGRAPHIE</b> .....	X
<b>TABLE DES MATIERES</b> .....	XI

# LISTE DES FIGURES, ILLUSTRATIONS ET TABLEAUX

➤ Illustration 1 : Plan de localisation de DCAT.....	3
➤ Figure 1 : Organigramme de DCAT .....	5
➤ Figure 2 : Schéma de l'architecture du réseau interne .....	13
➤ Illustration 2 : Diagramme architectural de la solution d'accès distant .....	23
➤ Illustration 3 : Interface de connexion des techniciens .....	32
➤ Illustration 4 : Interface de connexion des clients .....	33
➤ Illustration 5 : Interface de création de tickets .....	34
➤ Illustration 6 : Tableau de bord ou liste des tickets ouverts .....	35
➤ Illustration 7 : Interface NOC de visualisation des noms de domaines et de sous- domaines .....	37
➤ Illustration 8 : Interface NOC d'activation des certificats SSL/TLS.....	38
➤ Illustration 9 : Interface NOC de gestion des enregistrements .....	39
➤ Illustration 10 : Interface d'installation de Container Manager sur le Synology.....	42
➤ Illustration 11 : Interface du registre de conteneurs de Container Manager .....	43
➤ Illustration 12 : Interface de démarrage des conteneurs de Container Manager.....	44
➤ Illustration 13 : Interface web du tableau de bord du Routeur/firewall UNIFI.....	45
➤ Illustration 14 : Interface de configuration de la règle de redirection http .....	47
➤ Illustration 15 : Interface de configuration de la règle de redirection HTTPS.....	47
➤ Illustration 16 : Barre de menu de l'interface du Nginx Proxy Manager .....	49
➤ Illustration 17 : Interface d'ajout de certificats SSL/TSL du Nginx Proxy Manager	49
➤ Illustration 18 : Interface de création et de visualisation des règles d'accès du serveur Synology .....	51
➤ Illustration 19 : Menu et sous-menu d'accès à l'interface d'ajout des hôtes.....	52
➤ Illustration 20 : Boîte de dialogue des détails du nouvel hôte à ajouter.....	53
➤ Illustration 21 : Boîte de dialogue du certificat SSL du nouvel hôte à ajouter .....	53
➤ Illustration 22 : Liste des hôtes pris en compte par Nginx Proxy Manager.....	54
➤ Illustration 23 : Interface de HELPDESK DCAT sur le navigateur d'un ordinateur portable .....	55
➤ Illustration 24 : Caractéristiques du réseau sur lequel est connecté l'ordinateur....	56
➤ Illustration 25 : Interface de HELPDESK DCAT sur le navigateur d'un téléphone portable .....	57
➤ Illustration 26 : Caractéristiques du réseau mobile sur lequel est connecté le téléphone .....	58
➤ Illustration 27 : Basculement automatique en "https" dans la barre d'adresse.....	59
➤ Illustration 28 : Page d'accueil d'HELPDESK DCAT .....	62
➤ Tableau 1 : Bilan financier de la mise en œuvre du projet .....	66

## ***LISTE DES SIGLES ET ABRÉVIATIONS***

A
ACL : Access Control List
C
CPGE : Classes Préparatoires aux Grandes Ecoles
D
DCAT : Data Communications & All Technologies DNS : Domain Name System DDoS : Distributed Denial of Service
E
EDP : Ecole Doctorale Polytechnique EFCPC : Ecole de Formation Continue et de Perfectionnement des Cadres ENSA : Ecole Nationale Supérieure d'Agronomie ENSTP : Ecole Nationale Supérieure des Travaux Publics ESA : Ecole Supérieure d'Agronomie ESCAE : Ecole Supérieure de Commerce et d'Administration des Entreprises ESI : Ecole Supérieure d'Industrie ESMG : Ecole Supérieure de Mines et Géologie ESPE : Ecole Supérieure de Pétrole et d'Energie ESTP : Ecole Supérieure des Travaux Publics
H
HTTP : HyperText Transfer Protocol HTTPS : HyperText Transfer Protocol Secure
I
INP-HB : Institut National Polytechnique Houphouët Boigny INSET : Institut National Supérieur de l'Enseignement Technique IP : Internet Protocol
N
NAS : Network Attached Storage

O
OVH: Oles Van Hermann / On Vous Héberge
P
PHP : PHP Hypertext Preprocessor
R
RDS : Remote Desktop Services
S
SSL : Secure Sockets Layer SQL : Structured Query Language
T
TLD : Top-Level Domains TLS : Transport Layer Security
U
URL : Uniform Resource Locator
V
VDI : Virtual Desktop Infrastructure VM : Virtual Machine VoIP : Voice over Internet Protocol VPN : Virtual Private Network

## *RÉSUMÉ*

Ce projet de fin d'études s'inscrit dans le cadre de la modernisation des services informatiques de l'entreprise DCAT, visant à offrir un accès distant sécurisé à son système de gestion de tickets d'interventions. Face à l'évolution des besoins technologiques, DCAT a pris l'initiative de mettre en place une solution permettant aux employés et aux clients d'accéder à distance à l'application de gestion de tickets d'interventions "HELPDESK DCAT" basée sur OsTicket qui fonctionne déjà sur le réseau local.

Pour répondre à cette problématique, notre mission consistait à implémenter une architecture sécurisée pour l'accès distant à l'application, en tenant compte des exigences de performance et de sécurité. Nous avons opté pour une architecture basée sur le HTTPS, utilisant des technologies telles que Nginx Proxy Manager et le SSL/TLS pour assurer la sécurité et la confidentialité des communications.

La mise en œuvre de cette solution a nécessité une analyse approfondie des besoins des utilisateurs, ainsi qu'une conception minutieuse de l'architecture du système. Nous avons également effectué des tests pour garantir la fonctionnalité et la sécurité de la solution, en mettant l'accent sur les bonnes pratiques de sécurité et d'utilisation.

Au terme de ce projet, nous avons réussi à mettre en place une solution fonctionnelle et sécurisée permettant l'accès distant à l'application HELPDESK DCAT. Cette réalisation témoigne de notre capacité à relever les défis technologiques et à proposer des solutions innovantes répondant aux besoins spécifiques de nos clients.

Cependant, des défis ont été rencontrés tout au long du processus, notamment en termes de complexité technique et de contraintes budgétaires. Malgré ces obstacles, nous avons su faire preuve de résilience et d'ingéniosité pour mener à bien ce projet dans les délais impartis.



## *INTRODUCTION*

Dans un monde où les technologies de l'information et de la communication sont devenues indispensables, l'accès à distance aux applications d'entreprise est devenu un enjeu majeur pour assurer la continuité des activités. Cette nécessité s'est accentuée avec l'essor du télétravail, imposant aux entreprises le défi d'offrir un accès sécurisé et efficace à leurs applications, quelles que soient les circonstances.

Dans ce contexte, notre projet de fin d'étude vise à implémenter une solution sécurisée d'accès distant à OsTicket, une application web de gestion de tickets d'interventions déjà fonctionnelle et hébergée sur le serveur local de l'entreprise. Cette application revêt une importance capitale pour notre entreprise, tant pour les employés que pour les clients. Cependant, son accès à distance présente des défis complexes étant donné qu'à la base elle n'est accessible que dans le réseau local.

Le présent rapport détaille notre approche pour relever ces défis, en intégrant les meilleures pratiques en matière de réseau informatique et de sécurité des systèmes d'information, tout en tenant compte des ressources disponibles.

Nous débuterons par une présentation détaillée du cadre et du contexte de ce projet, suivie de l'étude conceptuelle réalisée. Ensuite, nous décrirons les étapes de mise en œuvre du projet, pour enfin faire un tour des réalisations effectuées pendant ce stage de fin d'études et des perspectives pour ce projet au sein de l'entreprise.

## **PARTIE I : CADRE ET CONTEXTE DU PROJET**

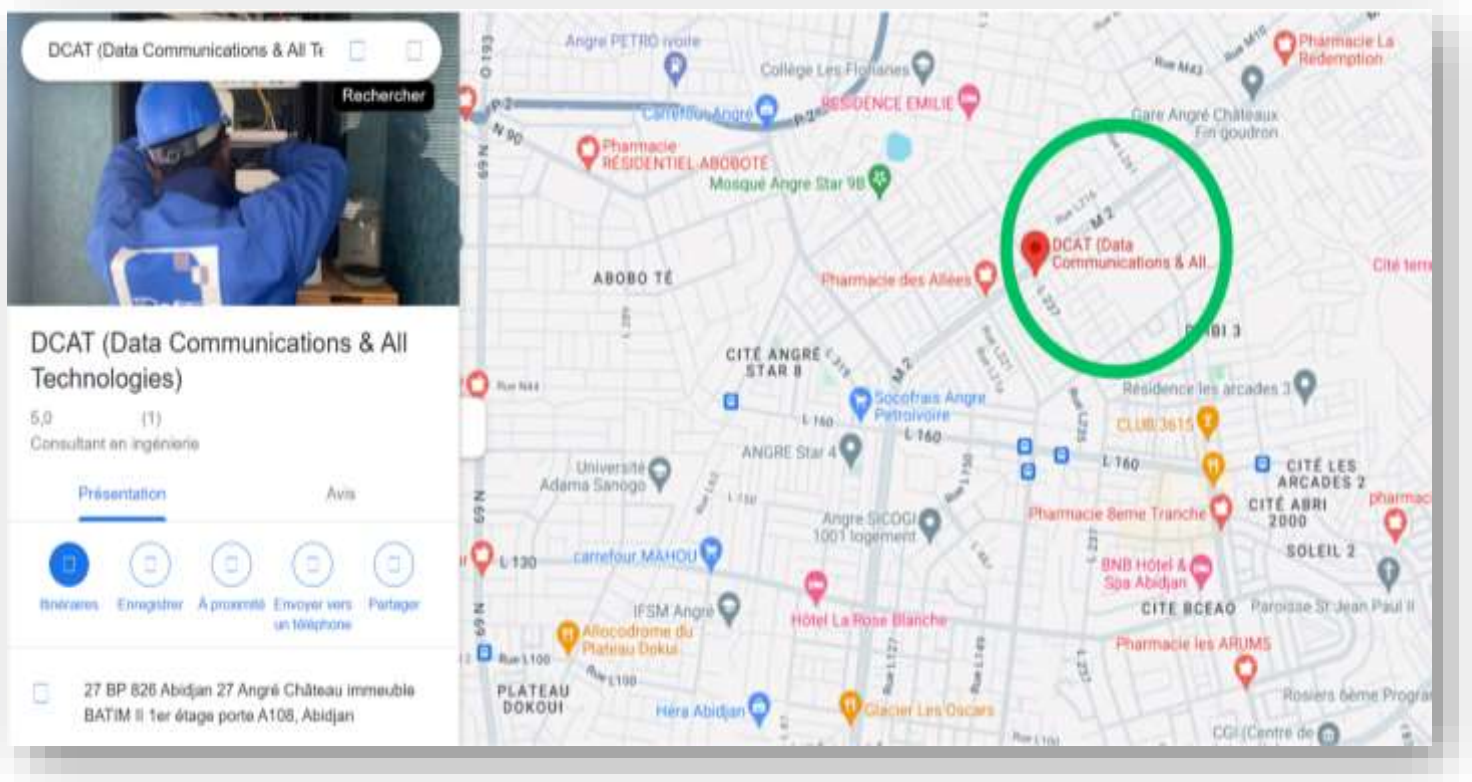
Cette section est dédiée à  
la présentation de l'entreprise d'accueil et du thème qui nous a été confié.

# CHAPITRE I : PRÉSENTATION DE LA STRUCTURE D'ACCUEIL

## I. GÉNÉRALITÉ

**Data Communications and All Technologies (DCAT)** est une entreprise spécialisée dans l'expertise et l'ingénierie techniques en télécommunications, établie en 2004 et située à Abidjan, dans la commune de Cocody, au sein de l'Immeuble BATIM à Angré Château. Cette entreprise regroupe une équipe diversifiée, composée d'ingénieurs et de techniciens provenant de différentes écoles de Côte d'Ivoire et de la sous-région, ainsi que de collaborateurs et consultants dotés d'une vaste expérience dans les systèmes d'information, avec une expertise particulière dans les domaines de l'audiovisuel et de l'informatique. Dans le cadre de ses activités, DCAT capitalise sur la solide expérience de ses collaborateurs pour fournir des solutions innovantes et adaptées aux besoins des télécommunications, à la transmission des données et à la sécurité.

Voici ci-dessous la localisation de l'entreprise présentée par l'illustration 1.



➤ *Illustration 1 : Plan de localisation de DCAT*

## **II. ACTIVITÉS**

Notre mission est de fournir en Afrique des solutions techniques en télécommunications audiovisuelles, en transmission de données et en sécurité électronique. L'expertise de DCAT se déploie autour des trois domaines clés suivants.

### **1. Audiovisuel**

Fort de son expertise en audiovisuel, DCAT se spécialise dans la création de chaînes de télévision et de radio, la production audiovisuelle, ainsi que la mise en place de réseaux de distribution audiovisuelle et de données. Nos compétences incluent la gestion des dossiers techniques pour l'obtention de fréquences d'émission, l'étude technique des sites de production et de diffusion, l'installation d'équipements radio (émetteurs hertziens, MMDS en analogique ou numérique, systèmes de cryptage), la configuration des locaux de production, l'utilisation de logiciels pour le réseau de télédistribution, et la réalisation de câblages pour la réception des chaînes de télévision en collectivité (hôtels, immeubles, cliniques, villas).

### **2. Sécurité électronique**

DCAT met à votre disposition des moyens et des compétences techniques pour protéger vos familles, vos biens et vos entreprises dans un contexte d'insécurité de plus en plus préoccupant. Nos services englobent un audit de votre système de sécurité, la conception et la réalisation de systèmes de sécurité comprenant des dispositifs de portiers et de contrôle d'accès, la vidéosurveillance, ainsi que l'intégration de la vidéosurveillance au réseau de télédistribution. De plus, nous assurons la fourniture, l'installation et la mise en service d'équipements de diffusion tels que platines, combinés audio ou audio-vidéo, et nous proposons également un service après-vente, une maintenance et un dépannage.

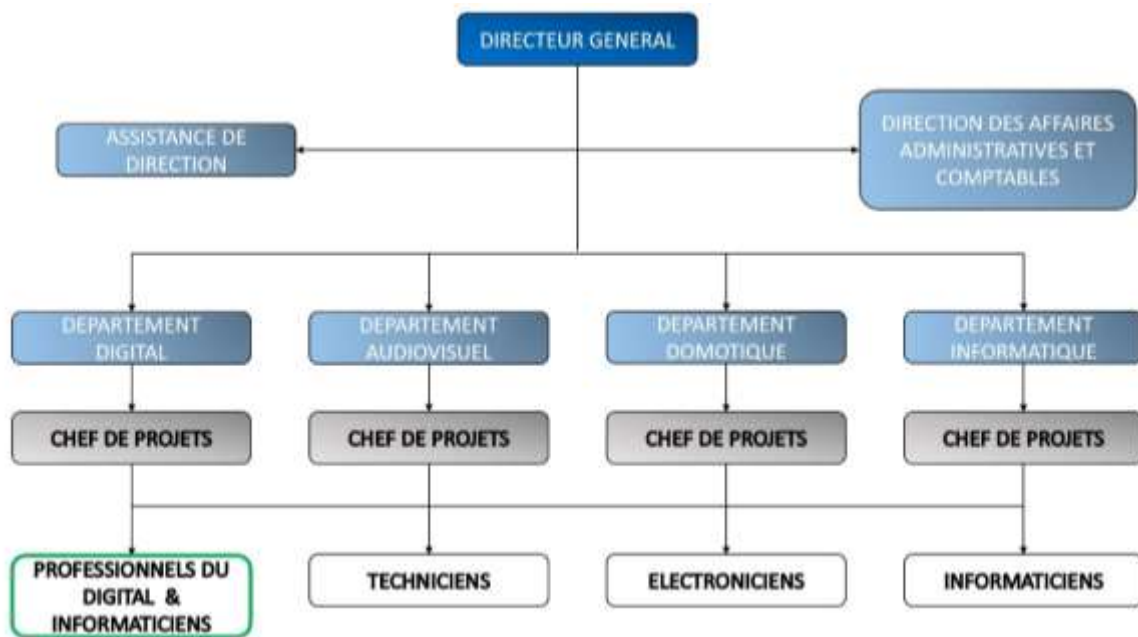
### **3. Solutions intégrées**

DCAT se démarque par son engagement continu dans l'innovation des Nouvelles Technologies de l'Information et de la Communication (NTIC) en Afrique. Notre entreprise a mis en place un réseau de distribution à distance qui intègre de manière complète et harmonieuse divers services essentiels tels que la télévision, la radio, l'accès à Internet, ainsi que la vidéosurveillance. Cette

approche globale nous permet de répondre de manière exhaustive aux besoins de nos clients. Elle leur offre un accès varié et efficace à ces services, tous regroupés au sein d'une unique plateforme de qualité, garantissant ainsi une expérience utilisateur optimale.

### III. ORGANIGRAMME

La structure organisationnelle de DCAT se présente comme suit :



➤ *Figure 1 : Organigramme de DCAT*

## CHAPITRE II : DESCRIPTION DU PROJET

### **I. CONTEXTE DU PROJET**

Notre arrivée au sein de DCAT pour le stage de fin d'étude de trois mois, débuté le 02 avril 2024, a coïncidé avec un moment crucial pour l'entreprise : le lancement d'un projet d'application web de gestion de tickets d'interventions par le service Digital. Dans le cadre de ce projet de digitalisation, nous avons rapidement saisi une opportunité majeure. Nous avons entrepris de faire en sorte que l'application soit installée sur le serveur de l'entreprise et que les utilisateurs puissent l'utiliser à distance.

C'est dans ce contexte stimulant que nous avons été chargés de travailler sur le projet intitulé : ***"Implémentation d'une solution d'accès distant pour la gestion des tickets d'interventions techniques : cas de la société DCAT"***. Ce projet illustre notre engagement à contribuer à la transformation numérique de DCAT, une entreprise de premier plan dans le domaine des Technologies de l'Information et de la Communication en Côte d'Ivoire.

Ce cadre dynamique a favorisé une expérience riche et mémorable, au cours de laquelle nous avons eu l'occasion de mettre en pratique les connaissances et compétences acquises tout au long de notre parcours académique et d'en découvrir les processus en entreprise.

### **II. OBJECTIFS DU PROJET**

#### **1. Objectif général**

L'objectif général de ce projet est de concevoir et de mettre en œuvre une solution sécurisée d'accès distant pour les employés et les clients de l'entreprise à une application web de gestion de tickets d'interventions, hébergée sur un serveur local.

#### **2. Objectifs spécifiques**

Les objectifs spécifiques de ce projet sont les suivants :

- Analyser les besoins des employés et des clients en termes d'accès à distance à l'application de gestion de tickets d'interventions.

- Concevoir une architecture sécurisée pour l'accès distant à l'application, en tenant compte des exigences de sécurité et de performance.
- Mettre en place les composants nécessaires pour permettre cet accès.
- Tester la solution pour s'assurer de sa fonctionnalité et de sa sécurité, en effectuant des tests d'accès à distance.
- Former les employés et les clients à l'utilisation de la solution d'accès distant, en mettant l'accent sur les bonnes pratiques de sécurité et d'utilisation. (Faire un support qui explique le processus)
- Assurer la maintenance et le suivi de la solution après sa mise en œuvre, en effectuant des mises à jour régulières et en surveillant son efficacité et sa sécurité au fil du temps.

En atteignant ces objectifs spécifiques, le projet contribuera à améliorer l'efficacité et la flexibilité des opérations de l'entreprise DCAT en permettant à ses employés et clients d'accéder à distance à une application essentielle, tout en assurant la sécurité et la confidentialité des données.

### **III. CAHIER DES CHARGES**

Le présent cahier des charges énonce les spécifications et les exigences pour l'implémentation d'une solution sécurisée, permettant aux employés et aux clients de l'entreprise DCAT d'accéder à distance à une application web de gestion de tickets d'interventions hébergée sur le serveur de l'entreprise.

#### **1. Description du public ciblé**

Le public ciblé par ce projet comprend :

- Les employés de l'entreprise DCAT
- Les clients de l'entreprise DCAT

Les employés, qu'ils soient situés au siège social ou en télétravail, représentent des utilisateurs internes qui ont besoin d'accéder à l'application pour créer, gérer et suivre les tickets d'interventions.

Les clients, quant à eux, sont des utilisateurs externes qui peuvent avoir besoin d'accéder à l'application pour soumettre des demandes de service ou suivre l'avancement des interventions en cours.

En résumé, le public ciblé comprend à la fois des utilisateurs internes et externes qui ont des besoins spécifiques en matière d'accès à distance à l'application de gestion de tickets d'interventions.

## **2. Spécifications fonctionnelles**

La solution devra :

- Permettre aux employés et aux clients de se connecter à distance à l'application web de gestion de tickets d'interventions à l'aide de leurs informations d'authentification.
- Assurer la confidentialité et l'intégrité des données transmises entre les utilisateurs (employés et clients) et le serveur de l'entreprise lors de l'accès distant à l'application.
- Être capable de gérer un nombre suffisant d'utilisateurs simultanés (à la fois employés et clients) sans compromettre les performances du système, assurant ainsi une expérience utilisateur fluide et réactive.

## **3. Contraintes**

- La solution devra être mise en place dans un délai de deux mois à compter de la date de début du projet fixé pour le 08 avril 2024.
- Les coûts liés à la mise en place de la solution devront être pris en compte et rester dans les limites du budget alloué au projet.
- La solution doit être conforme aux normes de sécurité et de confidentialité des données en vigueur au sein de l'entreprise DCAT, ainsi qu'aux réglementations et directives légales applicables en matière de protection des données.



#### **4. Livrables**

Les livrables attendus à la fin du projet sont les suivants :

- Documentation détaillée de conception et de mise en place de la solution.
- Rapport de test décrivant les résultats des tests de fonctionnalité et de sécurité de la solution.
- Support de formation pour les utilisateurs de l'application, comprenant des instructions d'accès à distance à l'application et des recommandations de sécurité.

#### **5. Validation**

La solution sera validée par les responsables de l'entreprise DCAT, qui vérifieront sa conformité aux spécifications fonctionnelles et techniques définies dans ce cahier des charges.

Ce cahier des charges constitue le cadre de référence pour la réalisation du projet de conception et de déploiement d'une solution sécurisée d'accès distant à une application web de gestion de tickets d'interventions pour l'entreprise DCAT.

## **PARTIE II : ÉTUDE CONCEPTUELLE**

Dans cette partie, nous allons détailler l'analyse conceptuelle du projet, y compris les besoins et les exigences, la faisabilité technique, et la conception préliminaire de la solution.

## CHAPITRE III : ENQUÊTES ET ÉTAT DES LIEUX

### **I. ENQUÊTES SUR LES BESOINS ET EXIGENCES**

#### **1. Identification des besoins spécifiques des utilisateurs**

- Besoin d'accéder à distance à une application hébergée sur le serveur local de l'entreprise.
- Besoin de pouvoir accéder à l'application à partir de différents terminaux, tels que des ordinateurs de bureau, des ordinateurs portables, des smartphones, etc.
- Besoin d'une connexion sécurisée pour protéger les données sensibles tout en accédant à l'application depuis des emplacements externes.
- Besoin d'une disponibilité élevée de l'application pour permettre un accès continu et sans interruption (électricité, internet, etc...).

#### **2. Identification des exigences**

- **Exigence de sécurité :** L'accès à distance à l'application doit être sécurisé pour protéger les données de l'entreprise contre les accès non autorisés.
- **Exigence de performance :** L'application doit être accessible à distance avec des temps de réponse rapides pour assurer une expérience utilisateur satisfaisante.
- **Exigence de compatibilité :** L'application doit être accessible à partir d'une variété de navigateurs web et de terminaux, et être compatible avec différents systèmes d'exploitation.
- **Exigence de disponibilité :** L'application doit être disponible 24 heures sur 24, 7 jours sur 7, avec une disponibilité maximale pour répondre aux besoins opérationnels de l'entreprise.

## II. ÉTAT DES LIEUX DES MOYENS À DISPOSITION

### 1. Identification des moyens mis à disposition

- Serveur hyperviseur
- Serveur Synology
- Commutateurs (switches)
- Routeur/ Pare-feu (firewall) Unifi
- Serveur de téléphonie VoIP
- Accès Internet via Fibre optique
- Electricité ondulée et régulée
- Périphériques et terminaux

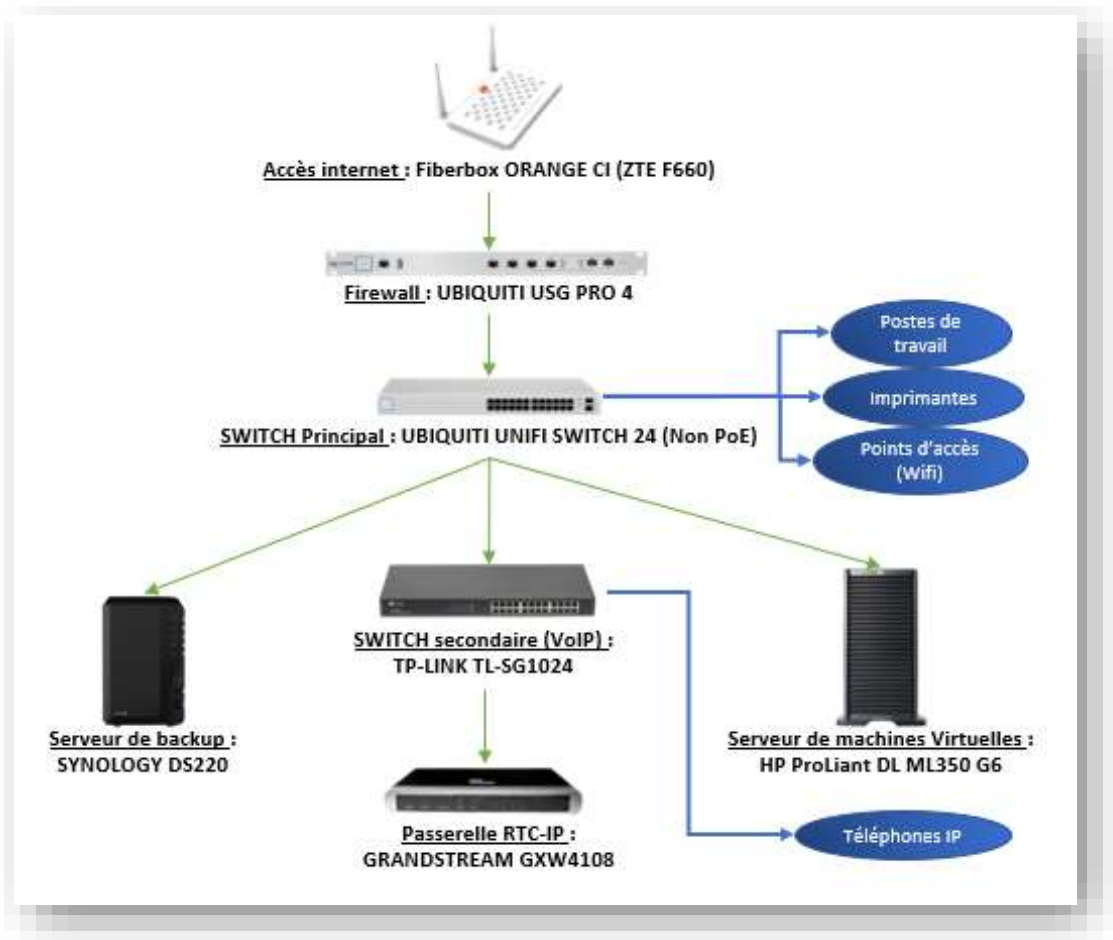
### 2. Rôle des moyens mis à disposition

- **Serveur hyperviseur** : Fournit une plateforme pour la création et la gestion des machines virtuelles, permettant la virtualisation des serveurs et des applications pour une utilisation efficace des ressources matérielles.
- **Serveur Synology** : Assure la sauvegarde et la restauration des données du serveur hyperviseur principal, offrant une solution de stockage sécurisée et fiable pour protéger les données critiques en cas de défaillance du système ou de perte de données.
- **Commutateurs** : Assurent la connectivité des terminaux au sein du réseau local, facilitant le partage des ressources et la communication entre les utilisateurs et les terminaux.
- **Routeur/Pare-feu** : Gère le trafic réseau entre le réseau local et Internet, permettant aux utilisateurs d'accéder à Internet et aux services en ligne. Il protège également le réseau interne en surveillant et en contrôlant le trafic entrant et sortant, prévenant les menaces de sécurité et garantissant la confidentialité des données.
- **Serveur de téléphonie VoIP** : Gère les appels téléphoniques internes, offrant une solution de téléphonie économique et flexible basée sur IP.

- **Accès Internet via Fibre optique** : Fournit l'accès à Internet aux utilisateurs internes, permettant la communication en ligne, la recherche d'informations, l'accès aux services cloud, etc.
- **Électricité ondulée et régulée** : Fournit une alimentation électrique stable et continue, en protégeant les équipements contre les fluctuations de tension, les surtensions et les interruptions de courant, assurant ainsi la fiabilité et la disponibilité constante du réseau et des systèmes informatiques.
- **Périphériques et terminaux** : Facilitent l'accès et l'interaction des utilisateurs avec le système, permettant la saisie, la visualisation et la gestion des données via des dispositifs tels que les ordinateurs, les tablettes et les smartphones.

### 3. Architecture du réseau interne

L'architecture du réseau interne de l'entreprise est représenté par la figure 2 suivante :



➤ Figure 2 : Schéma de l'architecture du réseau interne

## CHAPITRE IV : ÉTUDE DE FAISABILITÉ

### **I. VEILLE TECHNOLOGIQUE**

Cette veille technologique nous permet de faire un tour rapide des principales technologies contemporaines qui permettent d'accéder à une machine distante en faisant ressortir leurs avantages et inconvénients.

#### **1. VPN (Virtual Private Network)**

Un VPN (Virtual Private Network) crée un tunnel sécurisé sur Internet, permettant aux utilisateurs distants de se connecter au réseau interne de l'entreprise de manière sécurisée.

##### **Fonctionnement :**

- **Tunnel sécurisé :** Un VPN utilise un protocole de chiffrement pour créer un tunnel sécurisé entre l'appareil de l'utilisateur et le réseau interne de l'entreprise.
- **Accès distant :** Les utilisateurs distants peuvent se connecter au réseau interne de l'entreprise comme s'ils étaient physiquement présents dans les locaux de l'entreprise.
- **Chiffrement des données :** Toutes les données transmises via le VPN sont cryptées, assurant ainsi la confidentialité et la sécurité des informations échangées.

##### **Avantages du VPN :**

- **Sécurité renforcée :** Le chiffrement des données offre une protection contre l'interception ou la manipulation des informations sensibles lors de la transmission sur Internet.
- **Accès universel :** Les utilisateurs peuvent accéder au réseau interne de l'entreprise depuis n'importe où avec une connexion Internet, offrant ainsi une flexibilité maximale en termes de mobilité.
- **Gestion centralisée :** Les administrateurs système peuvent gérer les autorisations d'accès et les politiques de sécurité du VPN de manière centralisée, assurant ainsi un contrôle total sur les connexions distantes.

### Inconvénients du VPN :

- **Complexité** : La configuration et la gestion d'un VPN peuvent être complexes, nécessitant des compétences techniques avancées et des ressources dédiées.
- **Coût** : La mise en place et la maintenance d'un VPN peuvent entraîner des coûts initiaux et continus en termes de matériel, de logiciel et de bande passante.
- **Débit internet affecté** : L'utilisation d'un VPN peut réduire la vitesse de connexion en raison du chiffrement des données et du routage supplémentaire, entraînant une latence accrue et une diminution de la performance réseau, surtout si le serveur VPN est situé loin géographiquement.

## 2. Accès distant via HTTPS

L'accès distant via HTTPS utilise le protocole HTTP sécurisé (HTTPS) pour permettre aux utilisateurs d'accéder à une application web à distance de manière sécurisée.

### Fonctionnement :

- **Chiffrement SSL/TLS** : HTTPS utilise SSL/TLS pour chiffrer les données échangées entre le navigateur de l'utilisateur et le serveur web.
- **Authentification** : Le serveur web utilise un certificat SSL/TLS pour prouver son identité aux utilisateurs distants et établir une connexion sécurisée.
- **Transmission sécurisée** : Toutes les données échangées entre le navigateur de l'utilisateur et le serveur web sont cryptées, assurant ainsi la confidentialité et l'intégrité des informations.

### Avantages de l'accès distant via HTTPS :

- **Sécurité renforcée** : Le chiffrement SSL/TLS offre une protection robuste contre les attaques de type interception et permet de garantir la confidentialité des données sensibles.
- **Facilité d'utilisation** : L'accès distant via HTTPS ne nécessite pas l'installation de logiciels supplémentaires et peut être réalisé à partir de n'importe quel navigateur web compatible.

- **Compatibilité** : Le protocole HTTPS est largement pris en charge par les navigateurs web et est une norme de facto pour assurer la sécurité des communications en ligne.

#### **Inconvénients de l'accès distant via HTTPS :**

- **Dépendance au serveur web** : L'accès distant via HTTPS nécessite un serveur web sécurisé avec un certificat SSL/TLS valide, ce qui peut impliquer des coûts supplémentaires pour l'acquisition et le renouvellement des certificats.
- **Gestion des certificats** : La gestion des certificats SSL/TLS peut être complexe, nécessitant des connaissances techniques pour installer, configurer et renouveler les certificats de manière appropriée.
- **Performance** : Le chiffrement des données peut entraîner une légère surcharge sur le serveur web, ce qui peut affecter les performances globales de l'application, en particulier lors de la transmission de grandes quantités de données.

### **3. Terminal Server / Remote Desktop Services (RDS)**

Les services de Terminal Server, également connus sous le nom de Remote Desktop Services (RDS) dans l'environnement Windows, permettent aux utilisateurs d'accéder à distance à un environnement de bureau complet hébergé sur un serveur central.

#### **Fonctionnement :**

- **Environnement de bureau à distance** : Les utilisateurs se connectent à un serveur central à l'aide d'un client RDS, établissant ainsi une session de bureau à distance.
- **Interaction utilisateur** : Les utilisateurs peuvent interagir avec l'environnement de bureau distant de manière similaire à celle d'un ordinateur local, en exécutant des applications, en manipulant des fichiers, etc.
- **Transmission des données** : Les données de la session de bureau à distance sont transférées entre le serveur et le client via le protocole RDP (Remote Desktop Protocol), assurant ainsi la fluidité et la réactivité de l'expérience utilisateur.



### Avantages des services de Terminal Server / RDS :

- **Expérience utilisateur familière :** Les utilisateurs bénéficient d'une expérience utilisateur familière, similaire à celle d'un ordinateur local, ce qui réduit la courbe d'apprentissage et favorise une adoption rapide.
- **Centralisation des ressources :** Les ressources informatiques sont centralisées sur le serveur, ce qui facilite la gestion, la maintenance et la mise à jour des logiciels et des données.
- **Flexibilité :** Les utilisateurs peuvent accéder à leur environnement de bureau depuis n'importe quel appareil avec une connexion Internet, offrant ainsi une flexibilité maximale en termes de mobilité.

### Inconvénients des services de Terminal Server / RDS :

- **Coût initial :** La mise en place d'une infrastructure RDS peut entraîner des coûts initiaux élevés en termes de matériel serveur, de licences logicielles et de configuration.
- **Complexité :** La configuration et la gestion d'une infrastructure RDS peuvent être complexes, nécessitant des compétences techniques avancées et une planification minutieuse.
- **Dépendance à Internet :** La qualité et la disponibilité de la connexion Internet peuvent avoir un impact sur les performances et la fiabilité de l'expérience utilisateur, en particulier pour les applications gourmandes en bande passante.

## 4. Protocoles de bureau virtuel (VDI)

Les solutions de bureau virtuel, également connues sous le nom de VDI (Virtual Desktop Infrastructure), permettent aux utilisateurs d'accéder à des environnements de bureau complets hébergés sur des serveurs centraux à partir de n'importe quel appareil.

### Fonctionnement :

- **Création de machines virtuelles (VM) :** Les administrateurs système créent des machines virtuelles sur des serveurs centraux, chacune représentant un environnement de bureau complet pour un utilisateur.

- **Connexion à distance :** Les utilisateurs se connectent à leur bureau virtuel à distance via un client VDI, généralement à l'aide d'un navigateur web ou d'une application dédiée.
- **Utilisation de l'environnement de bureau :** Une fois connectés, les utilisateurs ont accès à un environnement de bureau familier, avec la possibilité d'exécuter des applications, de manipuler des fichiers, etc.

#### **Avantages des protocoles de bureau virtuel (VDI) :**

- **Flexibilité :** Les utilisateurs peuvent accéder à leur environnement de bureau depuis n'importe quel appareil avec une connexion Internet, offrant ainsi une flexibilité maximale en termes de mobilité.
- **Gestion centralisée :** Les administrateurs système peuvent gérer les environnements de bureau virtuel de manière centralisée, ce qui facilite la gestion des logiciels, des mises à jour et des politiques de sécurité.
- **Sécurité renforcée :** Les données et les applications sont hébergées de manière centralisée sur des serveurs sécurisés, réduisant ainsi les risques de perte ou de vol de données sur les terminaux des utilisateurs.

#### **Inconvénients des protocoles de bureau virtuel (VDI) :**

- **Coût :** La mise en place et la maintenance d'une infrastructure VDI peuvent entraîner des coûts initiaux élevés en termes de matériel serveur, de licences logicielles et de bande passante réseau.
- **Complexité :** La configuration et la gestion d'une infrastructure VDI peuvent être complexes, nécessitant des compétences techniques avancées et une planification minutieuse.
- **Dépendance au réseau :** Comme les utilisateurs dépendent d'une connexion réseau pour accéder à leur bureau virtuel, la qualité et la fiabilité de la connexion Internet peuvent avoir un impact sur l'expérience utilisateur.

## 5. Applications de collaboration et de partage d'écran

Les applications de collaboration et de partage d'écran permettent aux utilisateurs de travailler ensemble à distance en partageant leur écran et en collaborant sur des projets en temps réel. Voici plus de détails sur leur fonctionnement, leurs avantages et leurs inconvénients :

### Fonctionnement :

- **Partage d'écran :** Les utilisateurs peuvent partager leur écran avec d'autres participants, leur permettant de voir en temps réel ce qui se passe sur l'écran de l'utilisateur partageant.
- **Collaboration en temps réel :** Les participants peuvent collaborer sur des documents, des présentations ou d'autres contenus directement depuis leur propre navigateur web.
- **Communication audio et vidéo :** La plupart des applications de collaboration incluent des fonctionnalités de communication audio et vidéo, permettant aux participants de discuter en temps réel pendant la collaboration.

### Avantages des applications de collaboration et de partage d'écran :

- **Collaboration efficace :** Les participants peuvent travailler ensemble à distance en temps réel, ce qui améliore l'efficacité et la productivité du travail d'équipe.
- **Facilité d'utilisation :** Les applications de collaboration sont généralement faciles à utiliser et n'exigent souvent aucune installation de logiciel supplémentaire.
- **Interaction visuelle :** Le partage d'écran permet une interaction visuelle directe, ce qui facilite la compréhension et la communication entre les participants.

### Inconvénients des applications de collaboration et de partage d'écran :

- **Dépendance à Internet :** Comme ces applications fonctionnent via Internet, la qualité et la stabilité de la connexion Internet peuvent influencer l'expérience utilisateur.
- **Sécurité :** Le partage d'écran peut potentiellement compromettre la confidentialité des informations si les participants ne sont pas correctement authentifiés ou si les paramètres de partage ne sont pas correctement configurés.

- **Limitations fonctionnelles :** Certaines fonctionnalités avancées disponibles dans des logiciels spécifiques peuvent manquer dans les applications de collaboration en ligne, ce qui peut limiter les possibilités de certains projets.

En dehors de ces technologies, il existe d'autres technologies permettant d'accéder à distance à une machine et par conséquent à ses applications.

## II. SELECTION DES TECHNOLOGIES

Au terme de l'analyse des technologies existantes que nous avons effectuée plus tôt, nous retenons que les différentes technologies répertoriées plus haut en dehors de l'Accès distant via HTTPS ne nous conviennent pas. La raison est qu'elles demandent une certaine installation chez les utilisateurs, alors que nous recherchons une solution qui ne nécessite aucune installation ou configuration chez les utilisateurs. Nous voulons une solution prête à l'emploi une fois mise en place, permettant à chacun d'accéder à notre application web OsTicket facilement peu importe leur emplacement. En d'autres termes, nous souhaitons une solution sur mesure qui offre une accessibilité directe à l'application se basant sur l'Accès distant via HTTPS. Pour se faire, nous utiliserons les technologies et notions suivantes : nom de domaine et sous-domaine, redirection DNS, port forwarding, serveur reverse proxy...

### 1. Nom de domaine et sous-domaine

Un nom de domaine est une adresse unique sur Internet permettant d'identifier un site web. Un sous-domaine est une partie d'un domaine principal qui peut être utilisée pour différencier des sections ou des services spécifiques d'un site web.

**Pertinence pour le projet :** L'utilisation d'un nom de domaine et de sous-domaines permettra d'attribuer des adresses distinctes à notre application web de gestion des tickets d'interventions, offrant ainsi une accessibilité facile et intuitive pour les utilisateurs internes et externes. Cela simplifiera également la gestion et la configuration des accès à l'application.

## 2. Redirection DNS

La redirection DNS permet de rediriger le trafic d'une adresse URL vers une autre adresse IP. Cela peut être utilisé pour rediriger les demandes d'accès à un domaine ou un sous-domaine vers une adresse spécifique.

**Pertinence pour le projet :** En configurant une redirection DNS, nous pouvons diriger le trafic des utilisateurs vers l'adresse IP de notre serveur local hébergeant l'application web, assurant ainsi que les utilisateurs accèdent directement à l'application sans avoir besoin de connaître l'adresse IP spécifique.

## 3. Port forwarding

Le port forwarding consiste à rediriger le trafic réseau entrant d'un port spécifique d'un routeur ou d'un pare-feu vers un appareil ou un service particulier sur le réseau interne.

**Pertinence pour le projet :** En configurant le port forwarding sur notre routeur, nous pouvons rediriger le trafic HTTP/HTTPS entrant vers le serveur hébergeant notre application web. Cela permettra aux utilisateurs d'accéder à l'application via un navigateur web, peu importe leur emplacement.

## 4. Serveur Reverse Proxy

Un Serveur Reverse Proxy est un type de serveur proxy, habituellement placé du côté des serveurs web, qui permet de relayer des requêtes web provenant de l'extérieur vers les serveurs internes. Il peut filtrer, accélérer ou sécuriser le trafic réseau.

**Pertinence pour le projet :** En déployant un serveur reverse proxy, nous pouvons sécuriser les communications entre les utilisateurs et notre application web en filtrant le trafic et en appliquant des politiques de sécurité. Cela renforce la confidentialité des données et protège l'application contre les menaces potentielles. De plus, un reverse proxy peut équilibrer la charge du trafic réseau, améliorer les performances et la disponibilité de l'application en distribuant les demandes entrantes sur plusieurs serveurs internes.

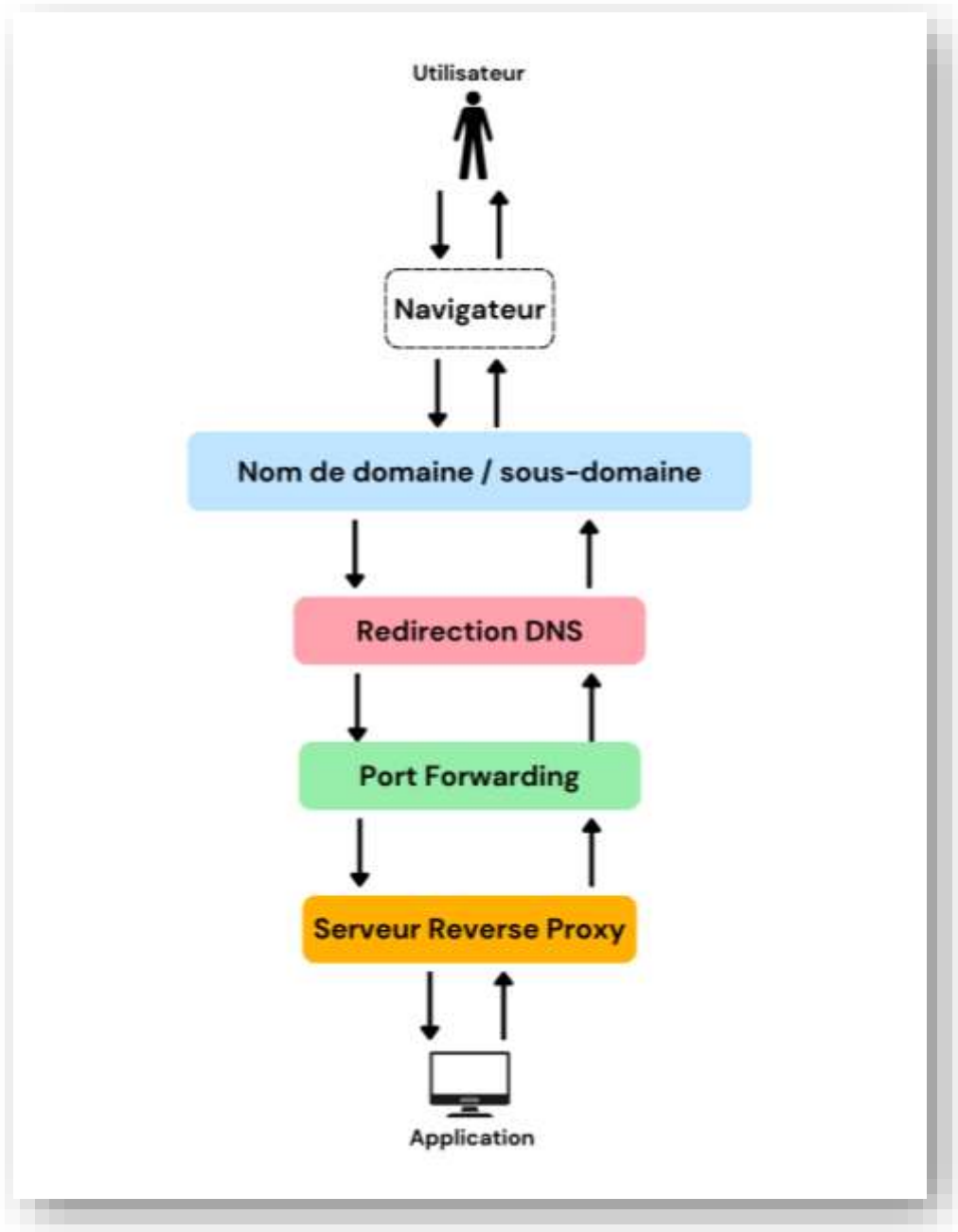


En utilisant ces technologies, nous pouvons mettre en place une solution robuste et sécurisée pour permettre un accès distant à notre application web de gestion des tickets d'interventions, offrant ainsi une expérience utilisateur transparente et fiable pour les employés et les clients, sans nécessiter d'installations ou de configurations complexes de leur part.

## CHAPITRE V : CONCEPTION DU SYSTÈME

### I. ARCHITECTURE DU SYSTÈME

L'association des principales technologies que nous avons choisies peut se résumer tel que représentée sur l'illustration 2 suivante :



➤ *Illustration 2 : Diagramme architectural de la solution d'accès distant*

## **1. Nom de Domaine et Sous-Domaine**

Le nom de domaine et les sous-domaines constituent le point d'entrée principal pour accéder à l'application à distance.

Ils permettent aux utilisateurs d'identifier facilement l'emplacement de l'application sur Internet.

Le lien logique avec la redirection DNS réside dans le fait que ces domaines sont associés à une adresse IP publique, permettant aux utilisateurs d'accéder au serveur local via Internet.

## **2. Redirection DNS**

Le DNS est responsable de la traduction des noms de domaine en adresses IP.

La redirection DNS permet de rediriger les demandes des utilisateurs vers l'adresse IP publique du serveur local où est hébergée l'application.

Le lien logique avec le port forwarding réside dans le fait que la redirection DNS dirige les demandes vers l'adresse IP publique du serveur, et le port forwarding redirige ensuite le trafic entrant vers le port spécifique de ce serveur.

## **3. Port Forwarding**

Le port forwarding est implicite dans la redirection DNS car il nous permet de rediriger le trafic entrant d'un port spécifique (principalement les ports HTTP et HTTPS) vers le serveur reverse proxy. Cela garantit que les requêtes des utilisateurs sont correctement acheminées vers le serveur approprié, facilitant ainsi une communication efficace avec l'application hébergée.

## **4. Serveur Reverse Proxy**

Le serveur reverse proxy agit comme un intermédiaire entre l'application et les utilisateurs.

Il assure la sécurité et la confidentialité des communications en filtrant et en redirigeant le trafic réseau. Placé entre les utilisateurs et le serveur local, il permet de contrôler et de gérer les demandes des utilisateurs, améliorant ainsi la sécurité et les performances du système. Contrairement à un proxy classique, un reverse proxy gère les demandes de connexion entrantes en les distribuant à plusieurs serveurs internes, ce qui peut également équilibrer la charge et fournir une couche supplémentaire de sécurité.



## **II. ÉLABORATION DU PLAN DE DÉPLOIEMENT**

### **1. Présentation de l'Application Locale**

Avant de procéder à toute configuration réseau, nous commencerons par présenter l'application existante en locale. Cela inclut l'explication de son fonctionnement et la documentation de ses configurations actuelles.

### **2. Création du Nom de Domaine et Sous-Domaine**

Pour la configuration du nom de domaine et des sous-domaines, nous allons sélectionner un fournisseur de noms de domaine et enregistrer notre nom de domaine principal. Ensuite, nous allons créer un sous-domaine nécessaire pour l'accès à distance à notre application.

### **3. Configuration de la Redirection DNS**

Pour la configuration de la redirection DNS, nous allons accéder à l'interface d'administration de notre hébergeur web. Ensuite, nous configurerons les paramètres DNS pour faire pointer le sous-domaine vers l'adresse IP publique de notre serveur local.

### **4. Configuration du Reverse Proxy**

Pour la configuration du reverse proxy, nous commencerons par sélectionner un serveur proxy adapté à nos besoins spécifiques. Ensuite, nous installerons et configurerons ce reverse proxy sur un serveur local.

## **5. Configuration du Port Forwarding**

Pour la configuration du port forwarding, nous accéderons à l'interface d'administration de notre routeur/firewall. Ensuite, nous configurerons les règles de redirection de port pour rediriger les trafics HTTP et HTTPS entrants vers le serveur reverse proxy.

## **6. Ajout des Certificats SSL/TLS**

Pour sécuriser les communications entre les utilisateurs et notre application, nous ajouterons des certificats SSL sur les URL dans les paramètres du reverse proxy. Nous générerons et installerons ces certificats sur le reverse proxy, cela assurera la confidentialité des données échangées et renforcera la confiance des utilisateurs.

## **7. Configuration des ACL (Access Lists)**

Nous allons créer sur le serveur physique hébergeant le reverse proxy des règles sur certains ports et adresses IP pour filtrer l'accès à notre application web. Cela ajoutera une couche de sécurité supplémentaire sur le serveur physique hébergeant le reverse proxy en plus de celles déjà configurées sur le firewall.

## **8. Indexation de l'hôte**

Nous mettrons en relation le Nom de domaine/sous-domaine et l'application web en utilisant l'adresse IP et le port local dans les paramètres du reverse proxy.

## **9. Tests et Vérifications**

Pour les tests et les vérifications, nous commencerons par vérifier l'accès à distance à l'application en utilisant le nom de domaine/sous-domaine que nous avons configuré. Ensuite, nous évaluerons la sécurité du déploiement en testant les mesures de sécurité mises en place. Nous vérifierons également le bon fonctionnement des certificats SSL/TLS dans les navigateurs web.

### III. ÉVALUATION DES RISQUES

#### 1. Vulnérabilités de Sécurité

Des failles de sécurité dans notre système pourraient permettre à des individus malveillants d'accéder à nos données sensibles ou de compromettre le fonctionnement de notre application.

- **Impact : Élevé**

Une exploitation réussie de ces vulnérabilités pourrait compromettre la confidentialité, l'intégrité ou la disponibilité de nos données, entraînant ainsi des conséquences financières et une perte de confiance de la part des utilisateurs.

- **Probabilité : Élevée**

Les menaces de sécurité sont omniprésentes dans le monde numérique d'aujourd'hui, et il est probable que des acteurs malveillants cherchent à exploiter les vulnérabilités de notre système.

#### 2. Panne du Serveur

Des pannes matérielles ou des problèmes logiciels sur notre serveur local pourraient entraîner une interruption de service, affectant ainsi la disponibilité de notre application pour les utilisateurs distants.

- **Impact : Moyen à Élevé**

Une panne du serveur pourrait entraîner une interruption de service, ce qui pourrait avoir un impact sur la productivité des utilisateurs et causer des pertes financières, en fonction de la durée de l'indisponibilité.

- **Probabilité : Moyenne**

Les pannes de serveur peuvent survenir en raison de divers facteurs tels que des défaillances matérielles, des erreurs de configuration ou des mises à jour logicielles, mais elles sont moins fréquentes que les menaces de sécurité.

### 3. Problèmes de Connectivité Internet

Des problèmes avec notre connexion Internet, tels que des pannes ou des ralentissements, pourraient rendre difficile voire impossible l'accès à distance à notre application.

- **Impact : Moyen à Élevé**

Des problèmes de connectivité pourraient empêcher les utilisateurs d'accéder à notre application, ce qui pourrait entraîner des perturbations dans les opérations quotidiennes et nuire à la satisfaction des clients.

- **Probabilité : Moyenne**

Les problèmes de connectivité Internet peuvent survenir en raison de pannes réseau, de problèmes avec les fournisseurs de services Internet, ou même de facteurs environnementaux tels que les conditions météorologiques.

### 4. Erreurs de Configuration

Des erreurs humaines dans la configuration des composantes clés de notre système, comme le nom de domaine, la redirection DNS ou le port forwarding, pourraient entraîner des dysfonctionnements ou des vulnérabilités de sécurité.

- **Impact : Moyen**

Des erreurs de configuration pourraient entraîner des dysfonctionnements temporaires de notre système, mais ils pourraient être corrigés rapidement avec un suivi attentif.

- **Probabilité : Moyenne**

Les erreurs de configuration peuvent se produire en raison de la complexité du déploiement de notre système et de la possibilité d'erreurs humaines lors de la configuration initiale ou des mises à jour ultérieures

## 5. Attaques DDoS

Des attaques par déni de service distribué (DDoS) pourraient surcharger notre infrastructure réseau, rendant ainsi notre application inaccessible pour tous les utilisateurs.

- **Impact : Moyen à Élevé**

Les attaques DDoS pourraient entraîner une interruption prolongée de notre service, ce qui pourrait avoir un impact significatif sur nos activités et notre réputation.

- **Probabilité : Faible à Moyenne**

Les attaques DDoS sont moins fréquentes que d'autres formes d'attaques, mais elles restent une menace potentielle, surtout si notre application devient une cible attrayante pour des attaquants.

### **PARTIE III : MISE EN ŒUVRE DU SYSTÈME**

Dans cette partie nous présenterons l'agencement des différents composants qui nous ont permis d'aboutir à une solution fonctionnelle répondant aux besoins spécifiés.

## CHAPITRE VI : IMPLÉMENTATION DES TECHNOLOGIES

### **I. PRÉSENTATION DE L'APPLICATION LOCALE**

L'application de gestion des tickets d'intervention que nous souhaitons rendre accessible sur internet et qui tourne déjà localement est "**OsTicket**" comme mentionné plus tôt. Il s'agit d'un logiciel open source de système de tickets permettant de gérer les demandes de support client. OsTicket est largement utilisé par les entreprises pour gérer efficacement leur service client.

#### **1. Fonctionnement de l'application existante en local**

Le service digital de DCAT a procédé à une personnalisation de OsTicket afin d'avoir les fonctionnalités nécessaires à l'entreprise en termes de gestion des tickets d'interventions. Le logiciel offre donc des fonctionnalités telles que la création et le suivi de tickets, la gestion des files d'attente, la personnalisation des formulaires de ticket, la gestion des utilisateurs et des groupes, etc. Suite à la personnalisation faite par le service digital, notre OsTicket porte désormais le nom "**HELPDESK DCAT**".

#### **2. Configurations actuelles de l'application**

Pour faire tourner OsTicket, un serveur web a été installé sur un système d'exploitation, ainsi que PHP et MySQL pour la gestion de la base de données.

- **Système d'exploitation de la machine hôte :** Ubuntu server
- **Serveur web :** Apache 2
- **Autres Dépendances :** PHP 8.2, MySQL 8.0, Composer...

### 3. Interfaces de l'application

- **Interface de connexion (technicien) :** Cette première interface permet aux techniciens de se connecter à l'application web. Une fois connectés, ils peuvent accéder à leurs outils et ressources nécessaires pour mener à bien leurs activités de gestion et de résolution de tickets.

L'illustration 3 suivante nous permet de visualiser cette interface.



➤ *Illustration 3 : Interface de connexion des techniciens*



- **Interface de connexion (client) :** Cette interface permet aux clients de se connecter à l'application web. Elle leur donne accès à leurs comptes pour soumettre des tickets, suivre leur progression, et communiquer avec les techniciens.

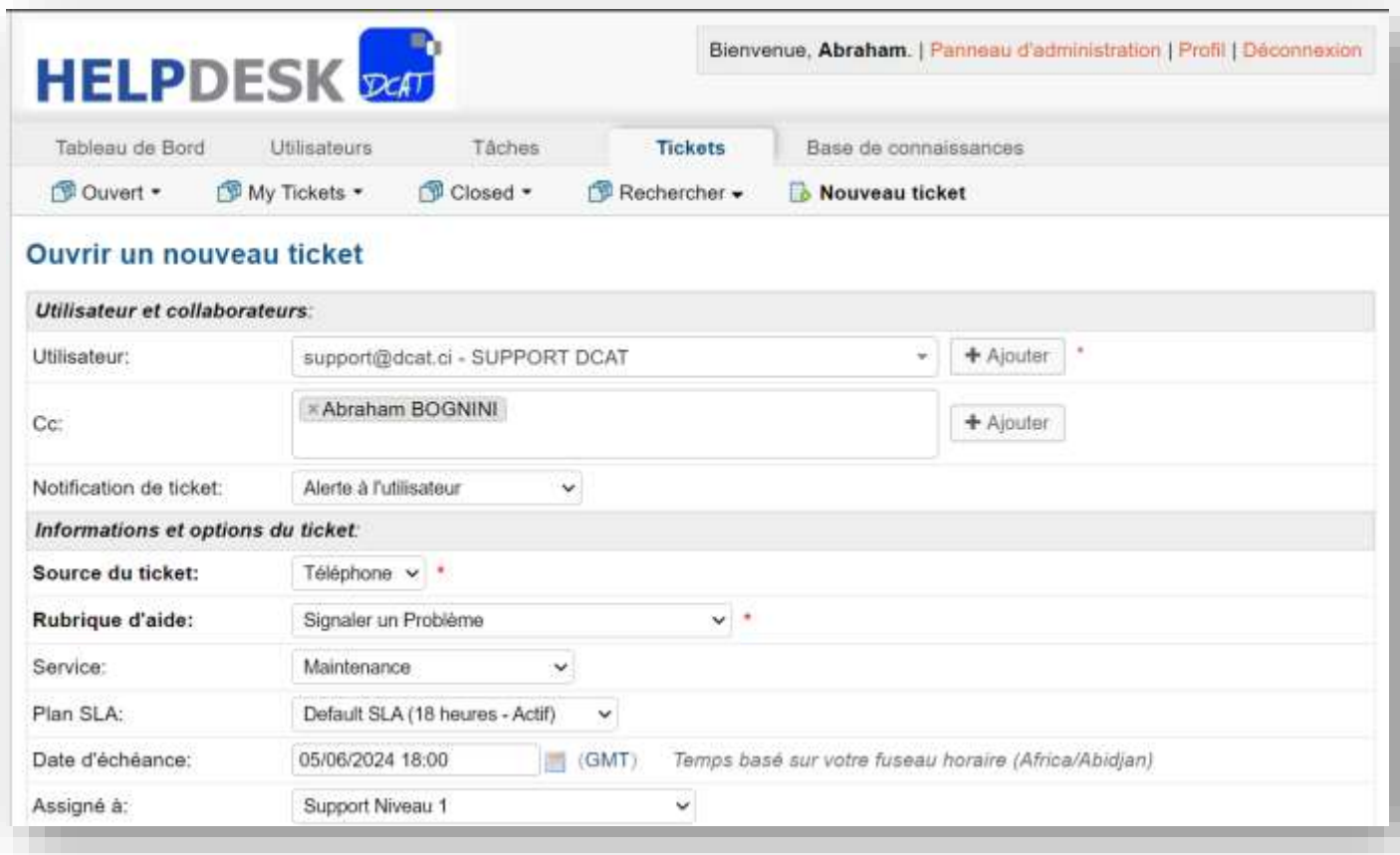
Nous pouvons constater ces points grâce à l'illustration 4 suivante :



➤ *Illustration 4 : Interface de connexion des clients*

- **Interface de création de tickets (technicien et client) :** Cette interface permet aux techniciens et aux clients de créer de nouveaux tickets d'intervention. Les utilisateurs peuvent détailler les problèmes rencontrés, joindre des fichiers, et définir la priorité des tickets, facilitant ainsi la communication et la prise en charge des incidents.

Voici ci-dessous l'illustration 5 qui nous permet de visualiser cette interface :



**HELPDESK DCAT**

Bienvenue, **Abraham.** | [Panneau d'administration](#) | [Profil](#) | [Déconnexion](#)

Tableau de Bord Utilisateurs Tâches **Tickets** Base de connaissances

Ouvert My Tickets Closed Rechercher Nouveau ticket

### Ouvrir un nouveau ticket

**Utilisateur et collaborateurs:**

Utilisateur: support@dcate.ci - SUPPORT DCAT + Ajouter \*

Cc: Abraham BOGNINI + Ajouter

Notification de ticket: Alerte à l'utilisateur

**Informations et options du ticket:**

Source du ticket: Téléphone \*

Rubrique d'aide: Signaler un Problème \*

Service: Maintenance

Plan SLA: Default SLA (18 heures - Actif)

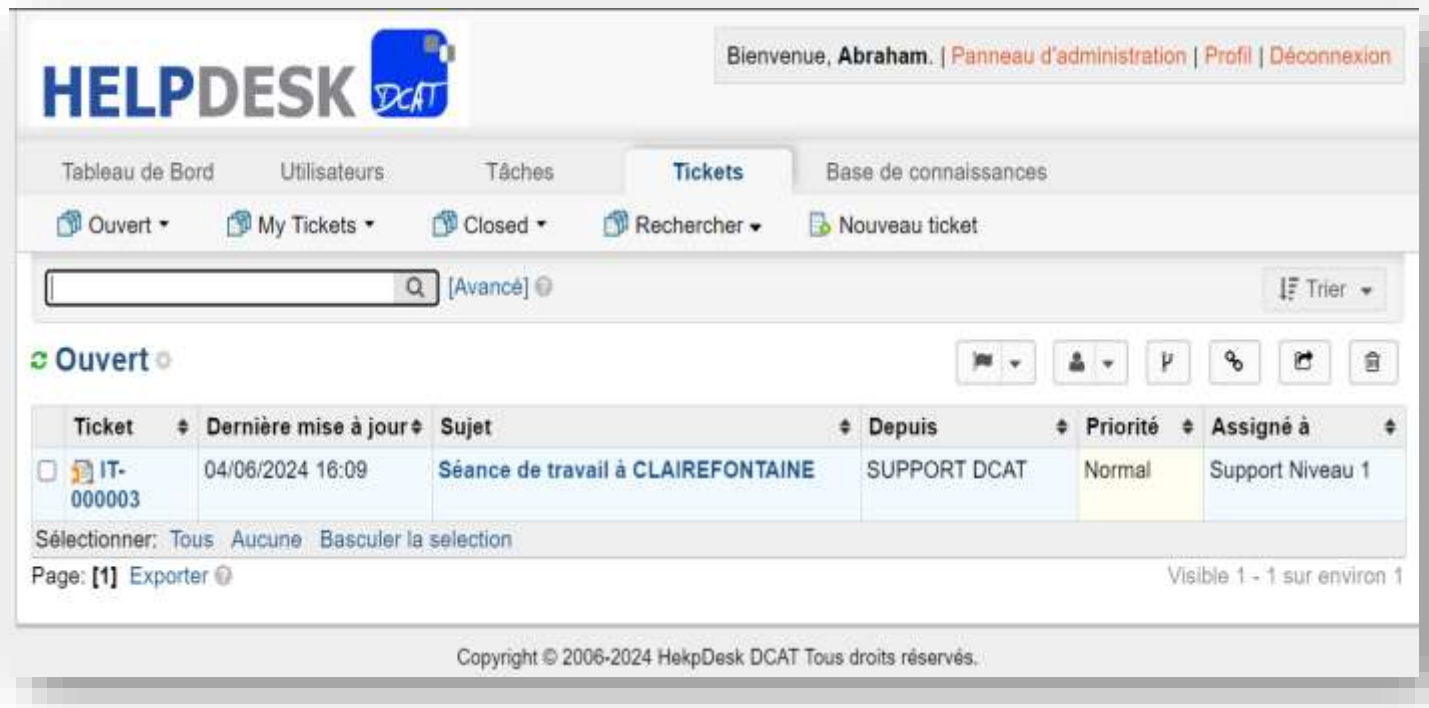
Date d'échéance: 05/06/2024 18:00 (GMT) Temps basé sur votre fuseau horaire (Africa/Abidjan)

Assigné à: Support Niveau 1

➤ *Illustration 5 : Interface de création de tickets*

- **Tableau de bord ou liste des tickets ouverts (technicien) :** Cette interface offre aux techniciens une vue d'ensemble des tickets ouverts. Elle affiche une liste des tickets en cours de traitement, avec des informations clés telles que les délais, les priorités, et les détails des incidents, permettant une gestion efficace et rapide des interventions.

Cette interface est visible sur l'illustration 6 suivante :



HELPDESK DCAT

Bienvenue, **Abraham**. | [Panneau d'administration](#) | [Profil](#) | [Déconnexion](#)

Tableau de Bord Utilisateurs Tâches **Tickets** Base de connaissances

[Ouvert](#) [My Tickets](#) [Closed](#) [Rechercher](#) [Nouveau ticket](#)

[Avancé] [Trier](#)

**Ouvert**

Ticket	Dernière mise à jour	Sujet	Depuis	Priorité	Assigné à
<input type="checkbox"/> IT-000003	04/06/2024 16:09	Séance de travail à CLAIREFONTAINE	SUPPORT DCAT	Normal	Support Niveau 1

Sélectionner: [Tous](#) [Aucune](#) [Basculer la selection](#)

Page: **[1]** [Exporter](#)

Visible 1 - 1 sur environ 1

Copyright © 2006-2024 HekpDesk DCAT Tous droits réservés.

➤ Illustration 6 : Tableau de bord ou liste des tickets ouverts

## II. CONFIGURATION DU NOM DE DOMAINE ET SOUS-DOMAIN

### 1. Sélection d'un fournisseur et enregistrement du nom de domaine principal

Parmi les fournisseurs de noms de domaine que nous avons la possibilité de choisir, nous pouvons citer les suivants :

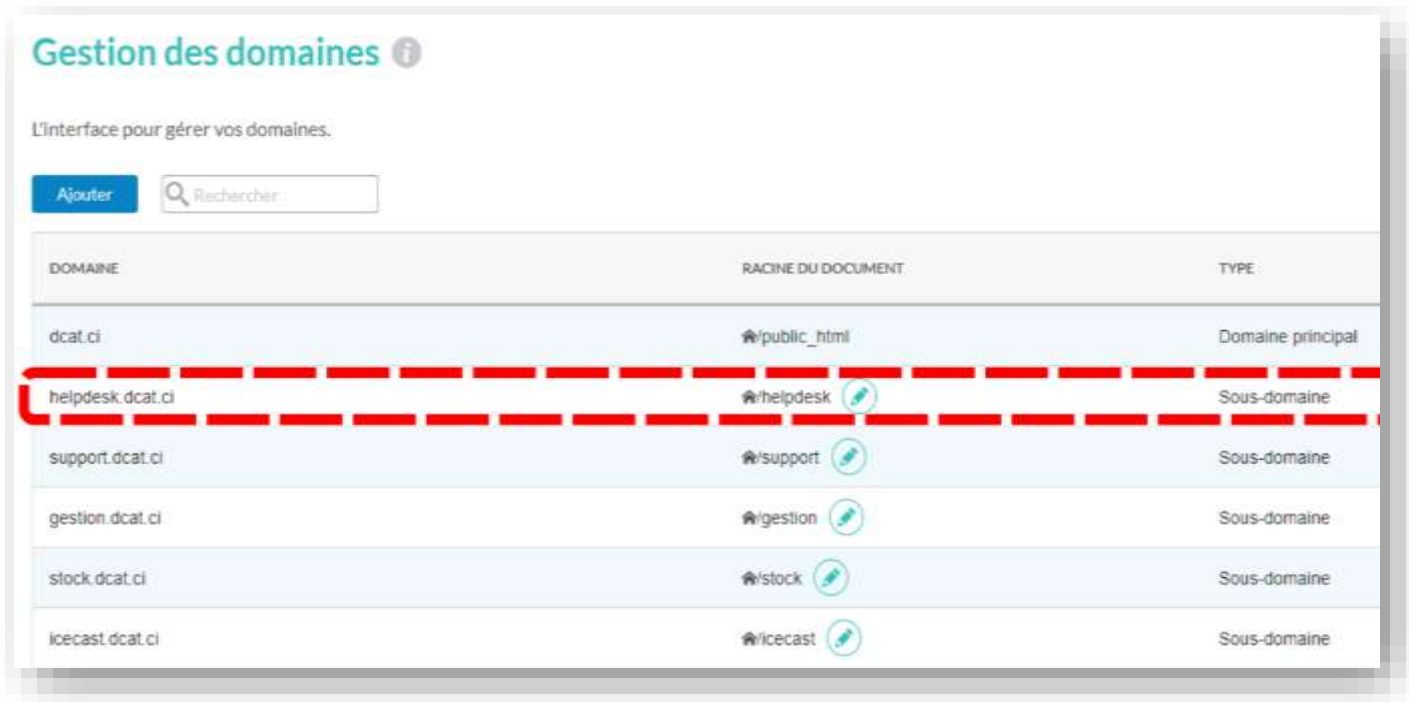
- **PlanetHoster** offre de bonnes performances et une disponibilité élevée de ses serveurs, avec un support technique réactif. En tant que fournisseur de noms de domaine, ils proposent une gestion facile des DNS et des options de protection de la vie privée. Cependant, leurs services peuvent être légèrement plus chers que ceux de certains autres hébergeurs.
- **Assist Web** offre une interface utilisateur intuitive et un excellent support client, facilitant la gestion de vos noms de domaine en ligne. Leur processus d'enregistrement de domaine est simple et efficace. Cependant, leur couverture géographique peut être limitée par rapport à certains autres fournisseurs, ce qui peut impacter les temps de réponse dans certaines régions.
- **MTN Cloud for Africa** fournit une infrastructure robuste et des solutions adaptées aux besoins des entreprises africaines, avec une forte présence régionale. En tant que fournisseur de noms de domaine, ils offrent des services d'enregistrement fiables et une gestion simplifiée des DNS. Toutefois, les services peuvent être coûteux et la disponibilité de certaines fonctionnalités avancées peut être limitée en comparaison avec des fournisseurs mondiaux.
- **OVH** propose une large gamme de services d'hébergement et de cloud computing avec des prix compétitifs et une infrastructure mondiale. En tant que fournisseur de noms de domaine, OVH offre un large choix de TLD (top-level domains) et des outils de gestion avancés. Leur support technique est réputé pour être rapide et efficace. Néanmoins, certains utilisateurs peuvent trouver leur interface de gestion de domaine complexe et moins conviviale par rapport à d'autres fournisseurs.






Étant donné que nous avons actuellement un hébergement chez PlanetHoster chez lequel nous avons déjà transféré le nom de domaine principal « **dcat.ci** », notre choix se porte sur ce fournisseur en particulier qui nous permet de gérer nos domaines via son interface N0C.

## 2. Création du sous-domaine approprié pour l'accès à distance à l'application

Le nom final de notre application étant "HELPDESK DCAT" nous allons créer le nom de sous-domaine « **helpdesk.dcat.ci** » pour suivre la logique.

Le nom de domaine que nous avons créé est visible sur l'illustration 7 ci-dessous :



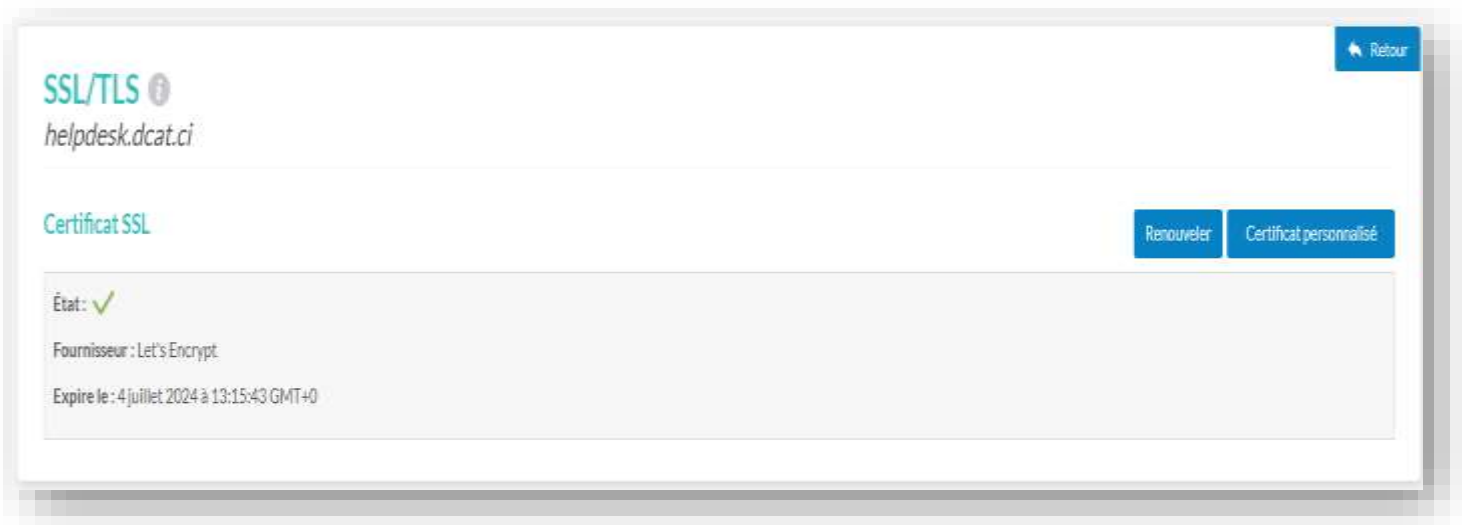
DOMAINE	RACINE DU DOCUMENT	TYPE
dcat.ci	📁/public_html	Domaine principal
helpdesk.dcat.ci	📁/helpdesk 	Sous-domaine
support.dcat.ci	📁/support 	Sous-domaine
gestion.dcat.ci	📁/gestion 	Sous-domaine
stock.dcat.ci	📁/stock 	Sous-domaine
icecast.dcat.ci	📁/icecast 	Sous-domaine

➤ *Illustration 7 : Interface N0C de visualisation des noms de domaines et de sous-domaines*

### 3. Activation du certificat SSL/TLS sur le nom de sous-domaine

Ici nous activons les certificats SSL/TLS du fournisseur Let's Encrypt sur le nom de sous-domaine pour forcer la connexion en https à chaque fois que celui-ci sera saisi dans un navigateur.

L'illustration 8 suivante nous donne les informations relatives au certificat SSL/TLS que nous avons activé.

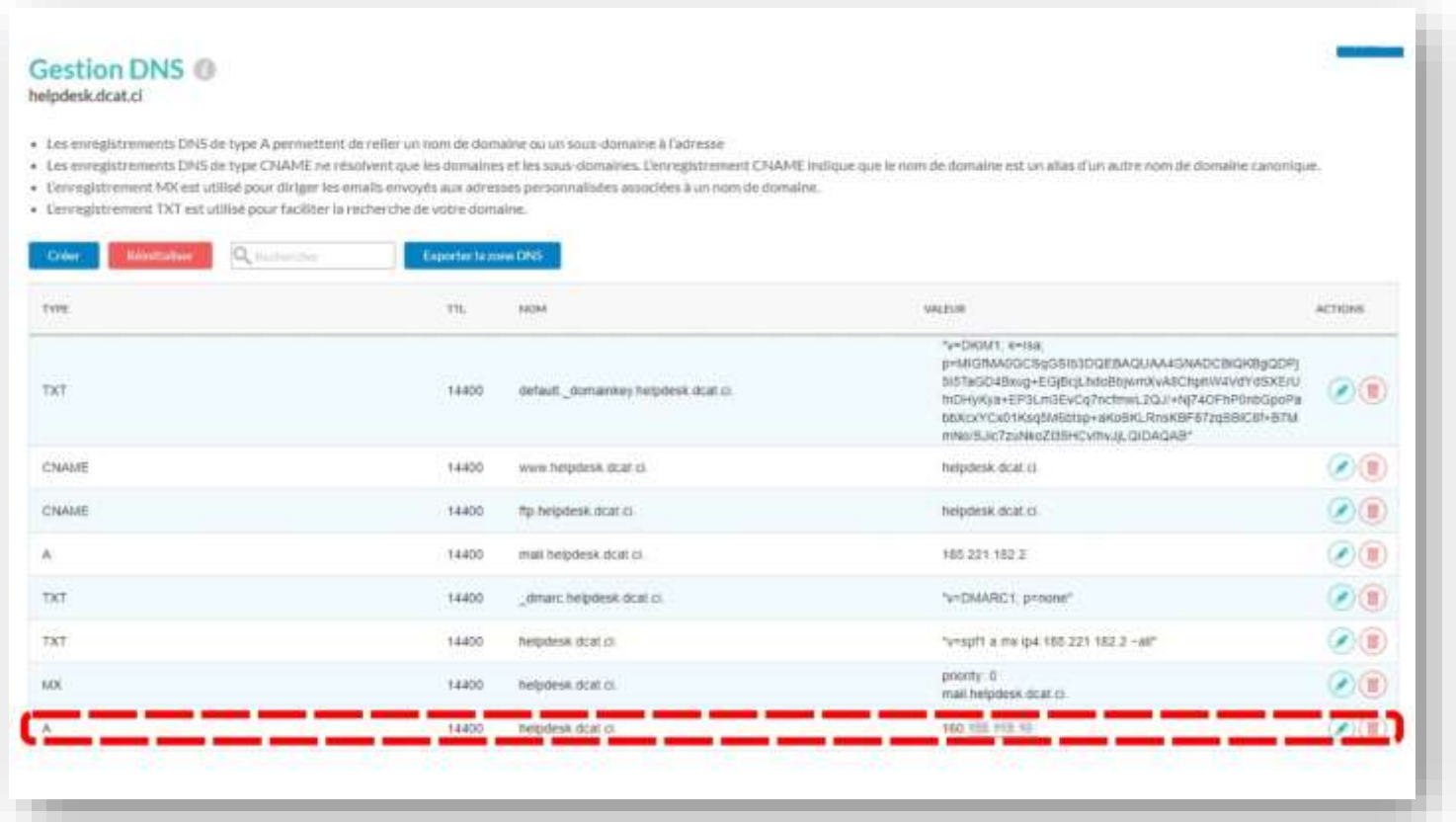


➤ Illustration 8 : Interface NOC d'activation des certificats SSL/TLS

### III. CONFIGURATION DE LA REDIRECTION DNS

Ici nous allons juste modifier l'enregistrement DNS de type A qui permet de relier le nom de sous domaine à l'adresse. Cette opération consiste à remplacer l'adresse IP de l'hébergeur par notre adresse IP publique statique attribuée par notre fournisseur d'accès internet.

















L'illustration 9 ci-dessous nous permet de visualiser cette étape.



**Gestion DNS**  
helpdesk.dcat.ci

- Les enregistrements DNS de type A permettent de relier un nom de domaine ou un sous-domaine à l'adresse.
- Les enregistrements DNS de type CNAME ne résolvent que les domaines et les sous-domaines. L'enregistrement CNAME indique que le nom de domaine est un alias d'un autre nom de domaine canonique.
- L'enregistrement MX est utilisé pour diriger les emails envoyés aux adresses personnalisées associées à un nom de domaine.
- L'enregistrement TXT est utilisé pour faciliter la recherche de votre domaine.

Créer Réinitialiser Rechercher Exporter la zone DNS

TYPE	TTL	NOM	VALUE	ACTIONS
TXT	14400	default._domainkey.helpdesk.dcat.ci.	"v=DIGMT, e=138, p=MIGfMAAGCISqG5t3DQEEBAQUAA4SNADCBIGK8gGDPj5t5taGQ4Bxug+EgBicLhfcBtjwmXvA8ChnW4VdyesXEJUthDHykja+EP3LmGEvCq7nctmwL2QJl+Nj74OFhP0nbGpoPa b6XcYCx01KsqM6cttp+aKoSKLRnsKBF67zqSBICB+BTM mN6/SJic7zuN6oZB5HCvnyJLQIDAQAB"	 
CNAME	14400	www.helpdesk.dcat.ci.	helpdesk.dcat.ci.	 
CNAME	14400	ftp.helpdesk.dcat.ci.	helpdesk.dcat.ci.	 
A	14400	mail.helpdesk.dcat.ci.	165.221.182.2	 
TXT	14400	_dmarc.helpdesk.dcat.ci.	"v=DMARC1; p=none"	 
TXT	14400	helpdesk.dcat.ci.	"v=spf1 a mx ip4 165.221.182.2 -all"	 
MX	14400	helpdesk.dcat.ci.	priority: 0 mail.helpdesk.dcat.ci.	 
A	14400	helpdesk.dcat.ci.	160.155.152.58	 

➤ Illustration 9 : Interface NOC de gestion des enregistrements

## IV. CONFIGURATION DU SERVEUR REVERSE PROXY

### 1. Choix du serveur reverse proxy

Parmi les serveurs reverse proxy les plus connus que nous avons la possibilité de choisir, nous pouvons citer les suivants :

- **Nginx Proxy Manager** : C'est une solution libre de droits populaire pour la gestion des proxies inverses, offrant une interface utilisateur simple et intuitive. Il permet de configurer facilement des proxies pour plusieurs domaines et sous-domaines, et supporte les certificats SSL/TLS pour sécuriser les connexions. En outre, Nginx Proxy Manager propose des options de redirection et de filtrage avancées pour une gestion fine du trafic. Cependant, bien qu'il soit convivial pour les débutants, ses capacités peuvent être limitées par rapport aux configurations avancées possibles avec Nginx standard.
- **Squid** : C'est un serveur proxy cache très performant, largement utilisé pour optimiser la livraison des contenus web en stockant les copies des pages fréquemment consultées. Il offre de nombreuses fonctionnalités pour la gestion du trafic web, y compris le filtrage des URL, l'authentification des utilisateurs et la mise en cache dynamique. Squid est hautement configurable et peut être adapté à des besoins très spécifiques. Cependant, sa configuration peut être complexe et nécessite une bonne compréhension des fichiers de configuration et des concepts réseau.
- **HAProxy** : C'est un reverse proxy et un load balancer open-source réputé pour sa performance et sa fiabilité. Il est couramment utilisé dans les environnements à haute disponibilité pour équilibrer la charge entre plusieurs serveurs backend, améliorant ainsi la disponibilité et la performance des applications. HAProxy supporte une large gamme de protocoles et offre des fonctionnalités avancées telles que la gestion des sessions et des règles de routage dynamiques. Malgré ses nombreux avantages, HAProxy peut être complexe à configurer et à maintenir, nécessitant des compétences techniques avancées.



Pour le serveur reverse proxy, nous avons opté pour **Nginx Proxy Manager** en raison de ses fonctionnalités répondant à nos besoins, notamment la gestion du trafic associé à nos noms de domaine et sous-domaines. De plus, son niveau de complexité est adapté à nos compétences actuelles, car nous sommes déjà familiers avec son utilisation.

## 2. Installation du serveur reverse proxy sur le serveur Synology NAS

- **Choix de l'Environnement**

Nous avons choisi d'installer Nginx Proxy Manager sur notre serveur secondaire Synology NAS DS218+ en raison de ses fonctionnalités robustes et de notre familiarité avec cette technologie.

- **Étapes d'Installation**

- **Préparation de l'Environnement**

- **Sélection du Gestionnaire de Conteneurs** : Nous avons décidé d'utiliser "Container Manager", disponible dans le Package Center de Synology, pour gérer notre conteneur Nginx Proxy Manager.
- **Installation du Container Manager** : Nous accédons au Package Center sur notre Synology NAS puis nous recherchons et installons "Container Manager".

Nous pouvons voir les informations relatives au Container Manager que nous venons d'installer sur l'illustration 10 juste en bas.

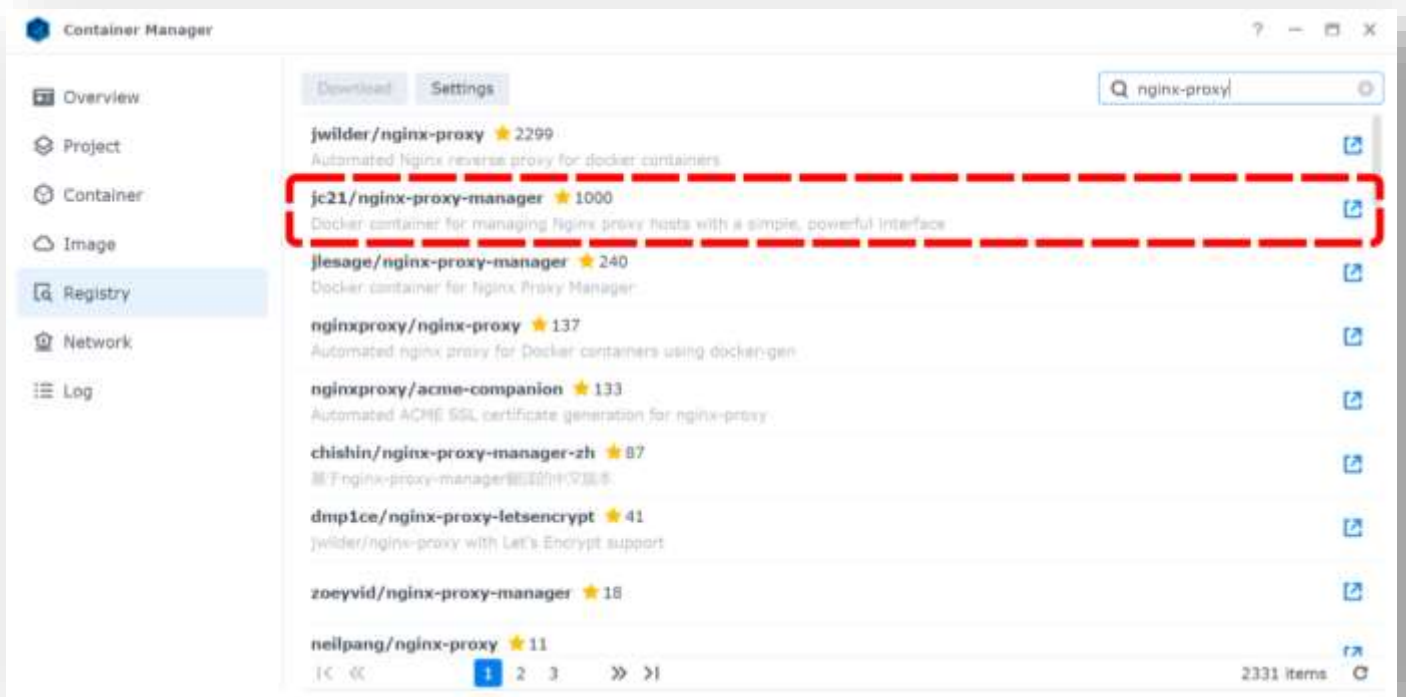


➤ *Illustration 10 : Interface d'installation de Container Manager sur le Synology*

- **Téléchargement de l'Image du Conteneur**

- **Accès au Registre du Container Manager** : Nous ouvrons le Container Manager puis nous naviguons vers l'onglet "Registry" pour accéder au registre des conteneurs.
- **Téléchargement de l'Image Nginx Proxy Manager** : Nous recherchons "Nginx Proxy Manager" dans le registre et nous téléchargeons l'image « jc21/nginx-proxy-manager » du conteneur.

La liste dans laquelle nous avons trouvé l'image que nous avons téléchargé et installé est visible dans l'illustration 11 ci-dessous.

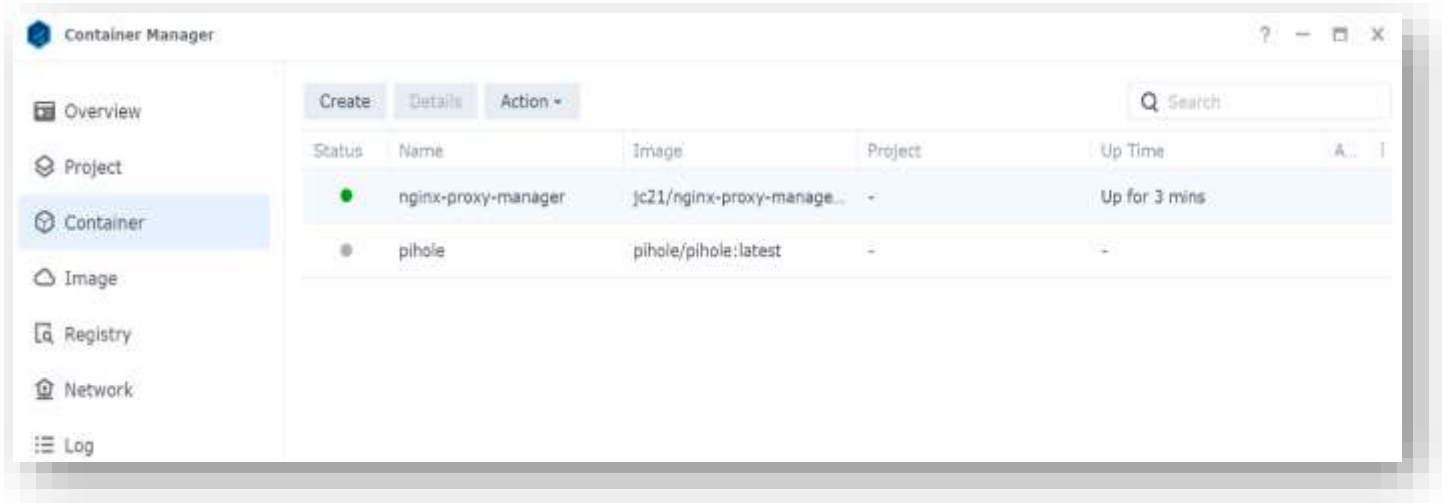


➤ *Illustration 11 : Interface du registre de conteneurs de Container Manager*

## • Installation et Exécution du Conteneur

- **Installation de l'Image** : Une fois l'image téléchargée, nous allons dans l'onglet "Image" du Container Manager puis nous sélectionnons l'image téléchargée et cliquons sur "Launch" pour lancer l'installation.
- **Configuration Initiale du Conteneur** : Nous configurons les paramètres de base nécessaires à l'exécution du conteneur, tels que les ports réseau et les volumes.
- **Mise en Service du Conteneur** : Nous démarrons le conteneur Nginx Proxy Manager pour le mettre en service.

Nous voyons dans l'illustration 12 juste en bas, la liste des conteneurs.



➤ *Illustration 12 : Interface de démarrage des conteneurs de Container Manager*

- **Accès et Configuration élémentaire de Nginx Proxy Manager**

- **Accès à l'Interface Web** : Nous accédons à l'interface web de Nginx Proxy Manager via l'adresse IP de notre NAS et le port configuré.
- **Configurations Initiales** : Nous nous connectons à l'interface et commençons les configurations élémentaires nécessaires pour faciliter son interaction avec notre réseau local.

En suivant ces étapes, nous assurons une installation fluide et fonctionnelle du Nginx Proxy Manager sur notre serveur Synology NAS DS218+, nous permettant ainsi d'insérer notre Serveur reverse proxy dans le réseau interne de notre entreprise.

## V. CONFIGURATION DU PORT FORWARDING

### 1. Accès à l'interface d'administration du routeur/firewall

- **Accès au Routeur/Firewall** : Nous ouvrons un navigateur web et saisissons l'adresse IP de notre routeur/firewall UNIFI dans la barre d'adresse.
- **Connexion** : Nous entrons nos identifiants de connexion (nom d'utilisateur et mot de passe) pour accéder à l'interface d'administration.
- **Interface d'Administration**: Une fois connectés, nous accédons au tableau de bord de l'interface d'administration, où nous pouvons configurer les paramètres réseau et de sécurité

L'illustration 13 nous présente l'interface que nous devons voir juste après la connexion.



➤ Illustration 13 : Interface web du tableau de bord du Routeur/firewall UNIFI

## 2. Configuration des règles de redirection de port

- **Accès aux Paramètres de Redirection de Port**

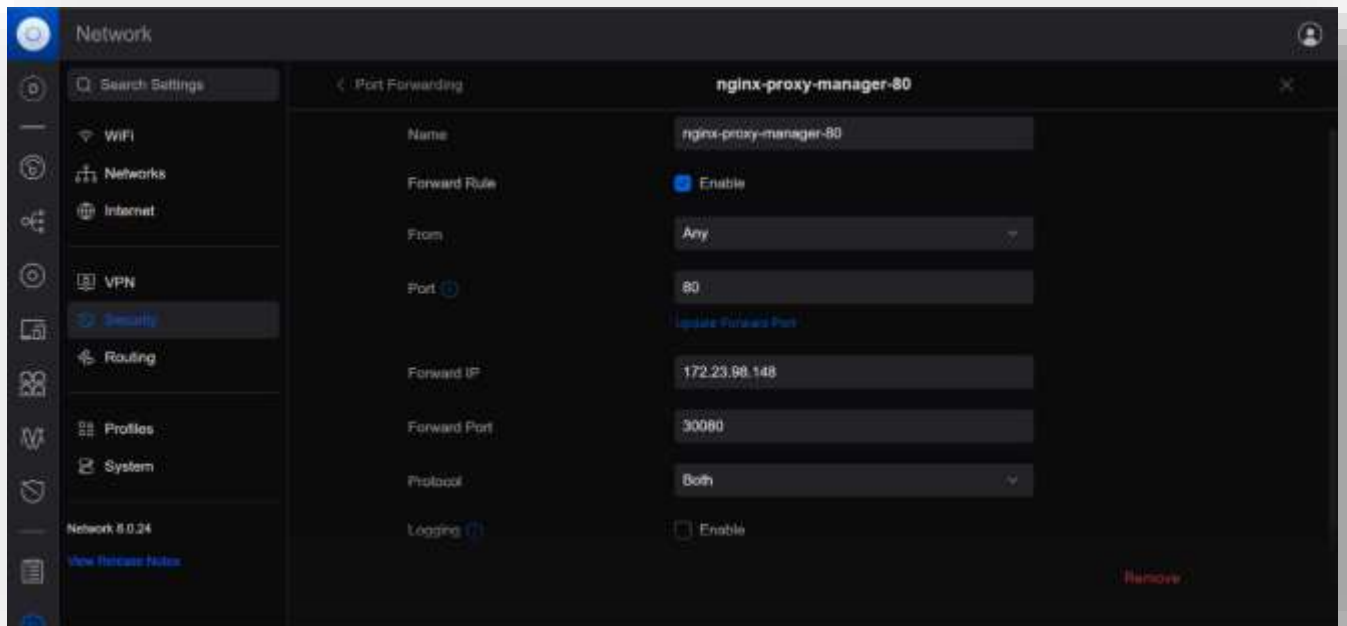
- **Navigation vers les Paramètres Avancés** : Dans l'interface d'administration, nous naviguons vers la section des paramètres avancés "Security", dans la zone "Port Forwarding".
- **Ajout d'une Nouvelle Règle**: Nous sélectionnons l'option pour ajouter une nouvelle règle de redirection de port.

- **Configuration des Détails de la Redirection**

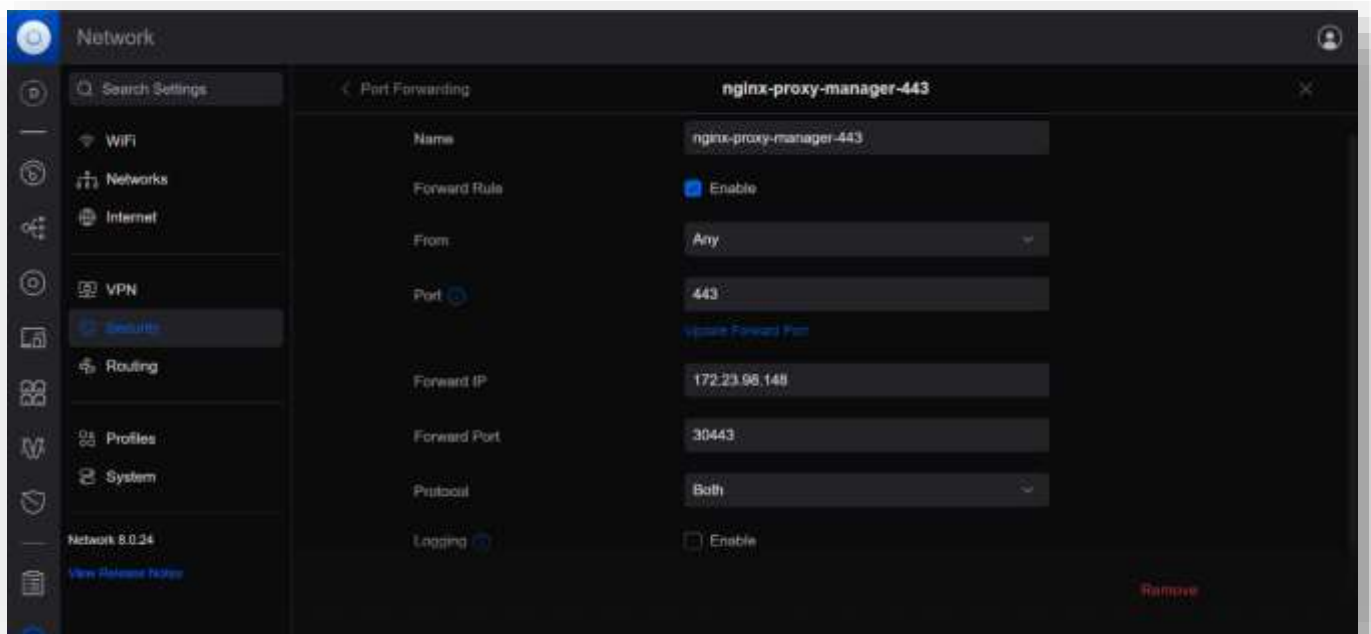
Nous définissons une règle pour chacun de nos deux ports à gérer mais le processus reste le même.

- **Nom de la Règle** : Nous donnons un nom descriptif à la règle, "nginx-proxy-manager-80" dans un premier temps pour le HTTP et "nginx-proxy-manager-443" dans un second temps pour le HTTPS.
- **Adresse IP Locale** : Nous saisissons l'adresse IP locale du Synology NAS où Nginx Proxy Manager est installé.
- **Ports Externes** : Pour HTTP, nous spécifions le port externe "80" et pour HTTPS, nous spécifions le port externe "443".
- **Ports Internes** : Pour HTTP, nous redirigeons le port externe "80" vers le port interne utilisé par Nginx Proxy Manager "30080". Quant à HTTPS, nous redirigeons le port externe "443" vers le port interne utilisé par Nginx Proxy Manager "30443".
- **Protocole** : Nous sélectionnons "both" afin de prendre en charge les protocoles UDP et TCP à la fois pour chaque règle.

Nous pouvons avoir un aperçu de la configuration des règles de redirection pour les ports http et https respectivement avec les illustrations 14 et 15 ci-dessous :



➤ Illustration 14 : Interface de configuration de la règle de redirection http



➤ Illustration 15 : Interface de configuration de la règle de redirection HTTPS

- **Enregistrement et Application des Modifications**

Nous enregistrons la nouvelle règle en cliquant sur le bouton dédié et attendons que les modifications soient prises en compte. Si nécessaire, nous redémarrons le routeur/firewall pour appliquer les modifications.

En suivant ces étapes détaillées, nous configurons efficacement le port forwarding pour rediriger le trafic HTTP/HTTPS entrant vers le port correspondant du Synology NAS, assurant ainsi un accès fluide et sécurisé à notre Nginx Proxy Manager.

## **VI. AJOUT DES CERTIFICATS SSL/TLS**

### **1. Accès à l'interface du Nginx Proxy Manager**

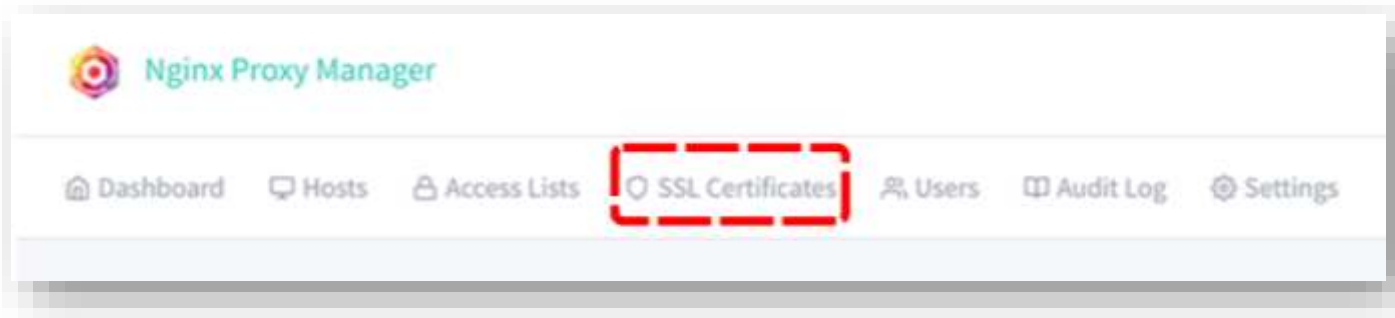
À ce niveau, en tapant le nom de sous-domaine "helpdes.dcat.ci" nous pouvons être reconduits vers l'interface web de notre Nginx Proxy Manager à laquelle nous nous connectons en utilisant les informations d'identification administratives ; ce qui nous permet d'accéder à l'interface utilisateur qui est intuitive et qui permet une gestion facile des configurations proxy, des certificats SSL, et de bien d'autres paramètres de redirection.

### **2. Ajout des certificats SSL/TLS au Nginx Proxy Manager**

Nous avons précédemment activé et acquis des certificats SSL/TLS lors de la création du nom de sous-domaine. Ces certificats sont essentiels pour sécuriser les communications entre les utilisateurs et notre application web en assurant un chiffrement des données.



- **Accès à la Section SSL** : Nous naviguons vers la section "SSL Certificates" de l'interface du Nginx Proxy Manager comme indiqué dans l'illustration 16.

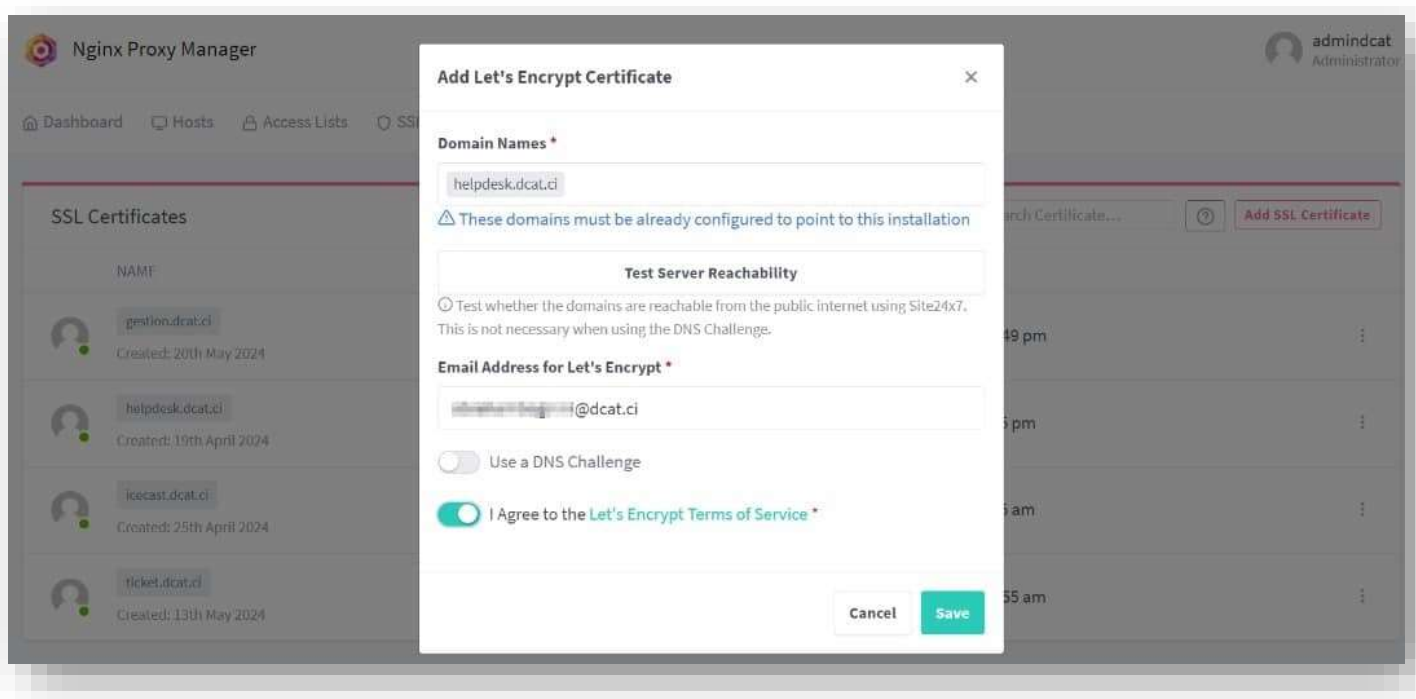


➤ *Illustration 16 : Barre de menu de l'interface du Nginx Proxy Manager*

- **Ajout des Certificats** :

En appuyant sur le bouton "Add SSL Certificate", nous remplissons les informations requises telles que le nom de domaine auquel nous voulons ajouter le certificat et l'adresse email pour Let's Encrypt. Le nom de domaine spécifie pour quel domaine le certificat SSL sera utilisé, assurant ainsi que les communications vers ce domaine seront sécurisées. L'adresse email est nécessaire pour Let's Encrypt afin de recevoir des notifications importantes concernant le certificat, telles que les rappels de renouvellement. Après avoir entré ces informations, nous enregistrons les modifications.

Nous pouvons voir comment cette procédure se déroule à travers l'illustration 17.



➤ *Illustration 17 : Interface d'ajout de certificats SSL/TSL du Nginx Proxy Manager*

## **VII. CONFIGURATION DES ACL (ACCESS LISTS)**

Nous créons des règles sur le serveur Synology hébergeant le reverse proxy pour filtrer l'accès à notre application web. Ces règles ajoutent une couche de sécurité supplémentaire au-delà de celles déjà configurées sur le firewall. Voici les règles mises en place :

### **1. Autorisation des applications locales**

Nous autorisons l'accès aux applications hébergées sur notre serveur depuis toutes les adresses IP sources, permettant ainsi un accès global tout en appliquant les autres règles de filtrage pour une sécurité accrue.

### **2. Autorisation des adresses privées de classe A**

Nous permettons l'accès aux adresses IP privées de classe A (10.0.0.0/8), ce qui couvre une large gamme d'adresses privées utilisées couramment dans les réseaux internes.

### **3. Autorisation des adresses privées de classe B**

Nous autorisons également l'accès aux adresses IP privées de classe B (172.16.0.0/12), couvrant une autre plage de réseaux privés utilisés pour les sous-réseaux moyens à grands.

### **4. Autorisation des adresses privées de classe C**

Les adresses IP privées de classe C (192.168.0.0/16) sont également autorisées, couvrant la plage de réseaux privés couramment utilisés dans les petites et moyennes entreprises ainsi que dans les réseaux domestiques.

### **5. Autorisation des adresses publiques provenant de la Côte d'Ivoire**

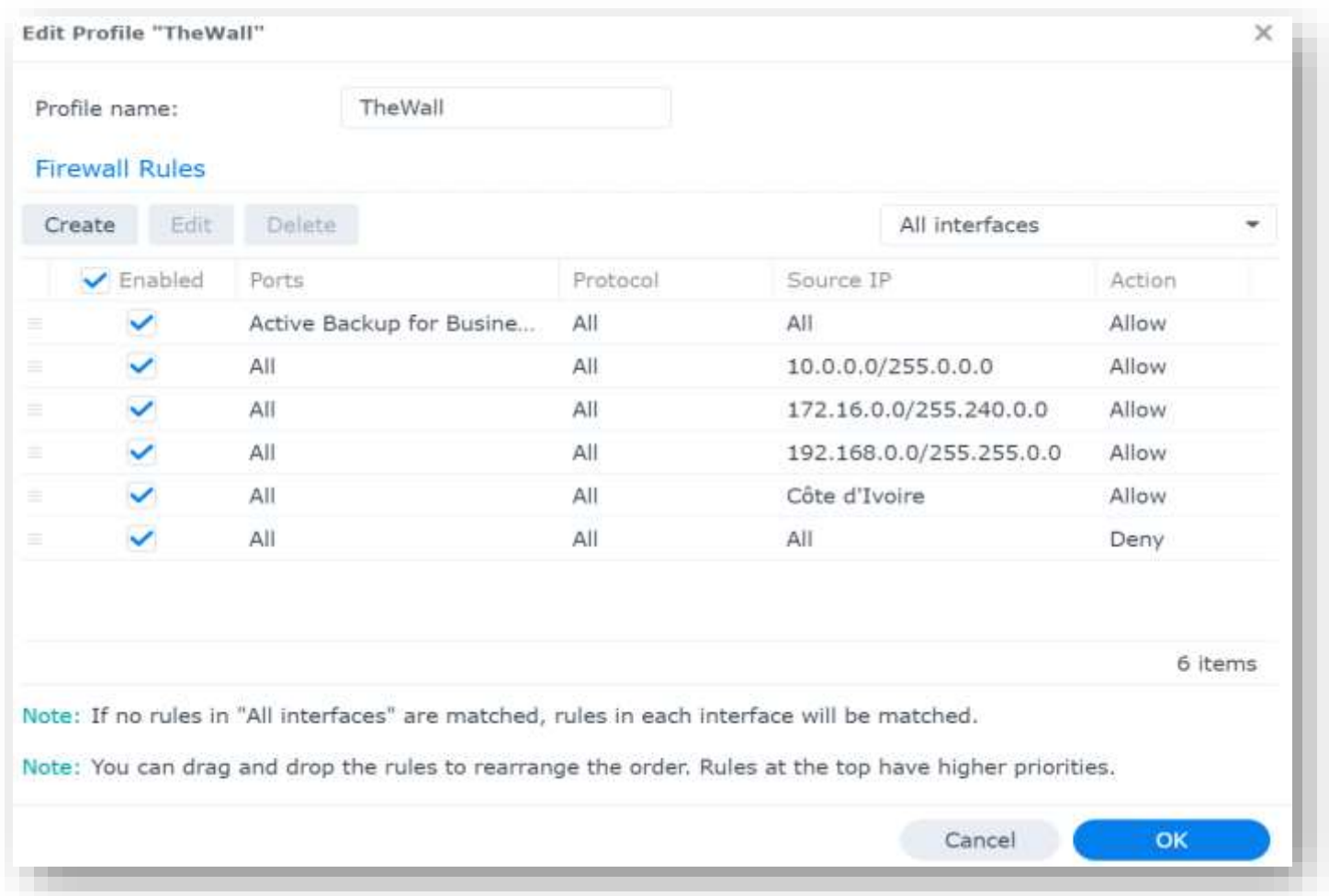
Nous configurons des règles pour autoriser les adresses IP publiques provenant de la Côte d'Ivoire, permettant ainsi aux utilisateurs situés dans le pays d'accéder à notre application web.

## 6. Non Autorisation des adresses ne respectant aucune des règles déjà énoncées

Toutes les autres adresses IP qui ne sont pas couvertes par les règles précédentes seront bloquées, ajoutant ainsi une couche de sécurité pour empêcher l'accès non autorisé.

Ces mesures permettent de contrôler et de restreindre l'accès à notre application web, en assurant une sécurité renforcée contre les accès non autorisés tout en permettant un accès approprié pour les utilisateurs autorisés.

Voici donc comment ces règles sont représentées dans l'illustration 18 :



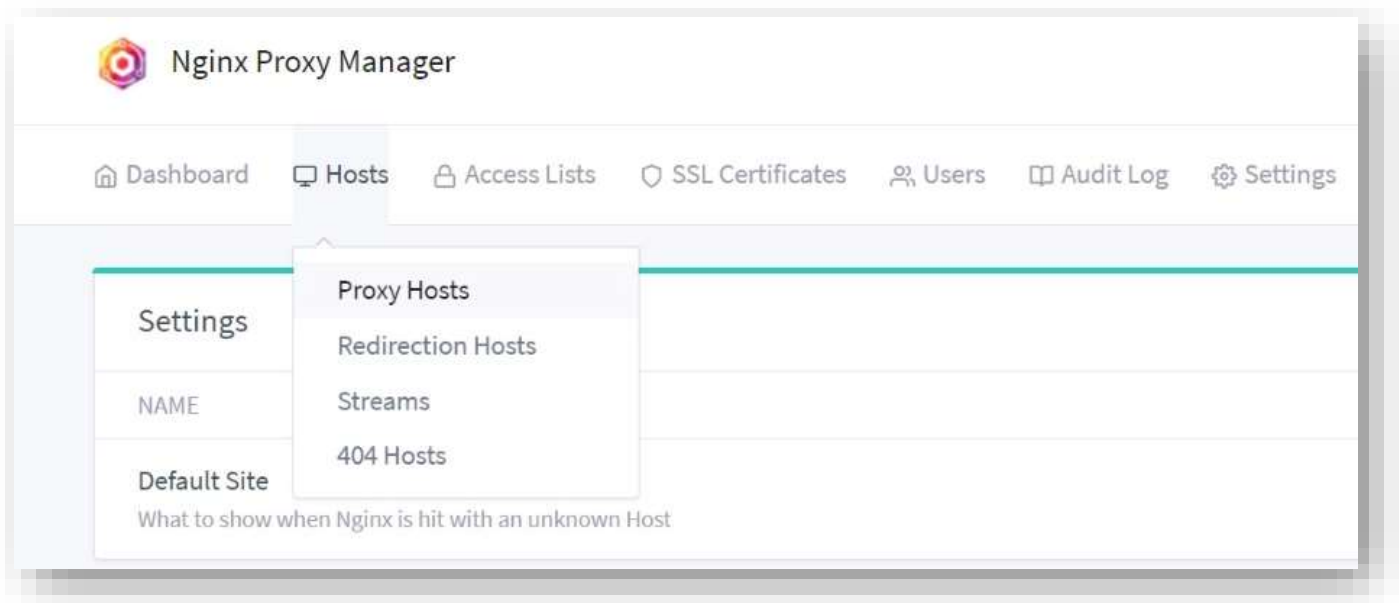
➤ Illustration 18 : Interface de création et de visualisation des règles d'accès du serveur Synology

## VIII. INDEXATION DE L'HÔTE

Nous finalisons notre processus en mettant en relation le nom de sous-domaine et l'application web. Cela se fait en utilisant l'adresse IP et le port local dans les paramètres du reverse proxy. Cette étape assure que le trafic dirigé vers notre sous-domaine est correctement acheminé vers l'application web hébergée sur le serveur local.

### 1. Accès à l'interface d'ajout des hôtes

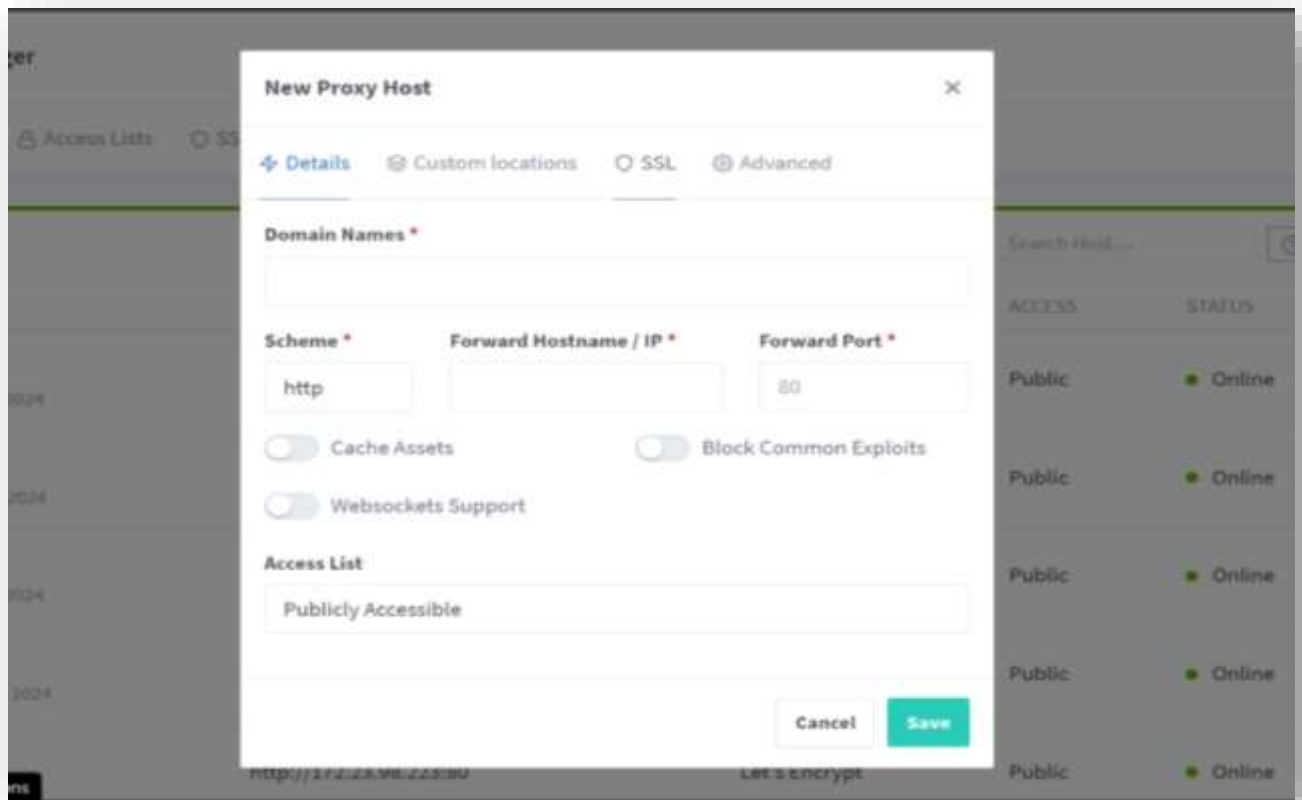
Ayant déjà accès à l'interface de notre Nginx Proxy Manager, il nous faut cliquer sur le champ "Hosts" du menu puis sur le champ "Proxy Hosts" du sous-menu comme indiqué sur l'illustration 19.



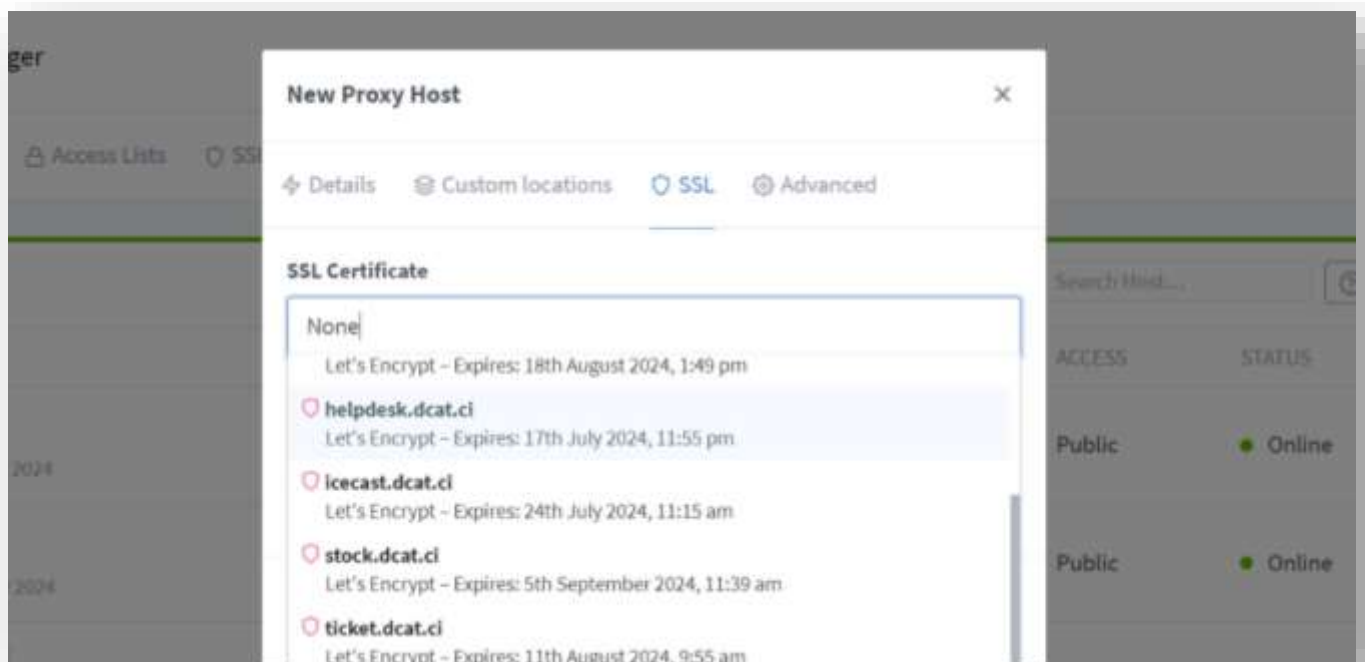
➤ Illustration 19 : Menu et sous-menu d'accès à l'interface d'ajout des hôtes

### 2. Liaison de l'hôte au nom de sous-domaine

Une fois sur l'interface d'ajouts des hôtes, nous sélectionnons l'option "Add Proxy Host" qui nous ouvrira une boîte de dialogue dans laquelle nous aurons à remplir les informations nécessaires pour la mise en relation du nom de domaine et de la machine hôte. Il s'agit d'informations tels que le nom du sous-domaine en question, l'adresse IP de la machine hôte sur laquelle tourne notre HELPDESK DCAT comme le montre les illustrations 20 et 21 suivantes :

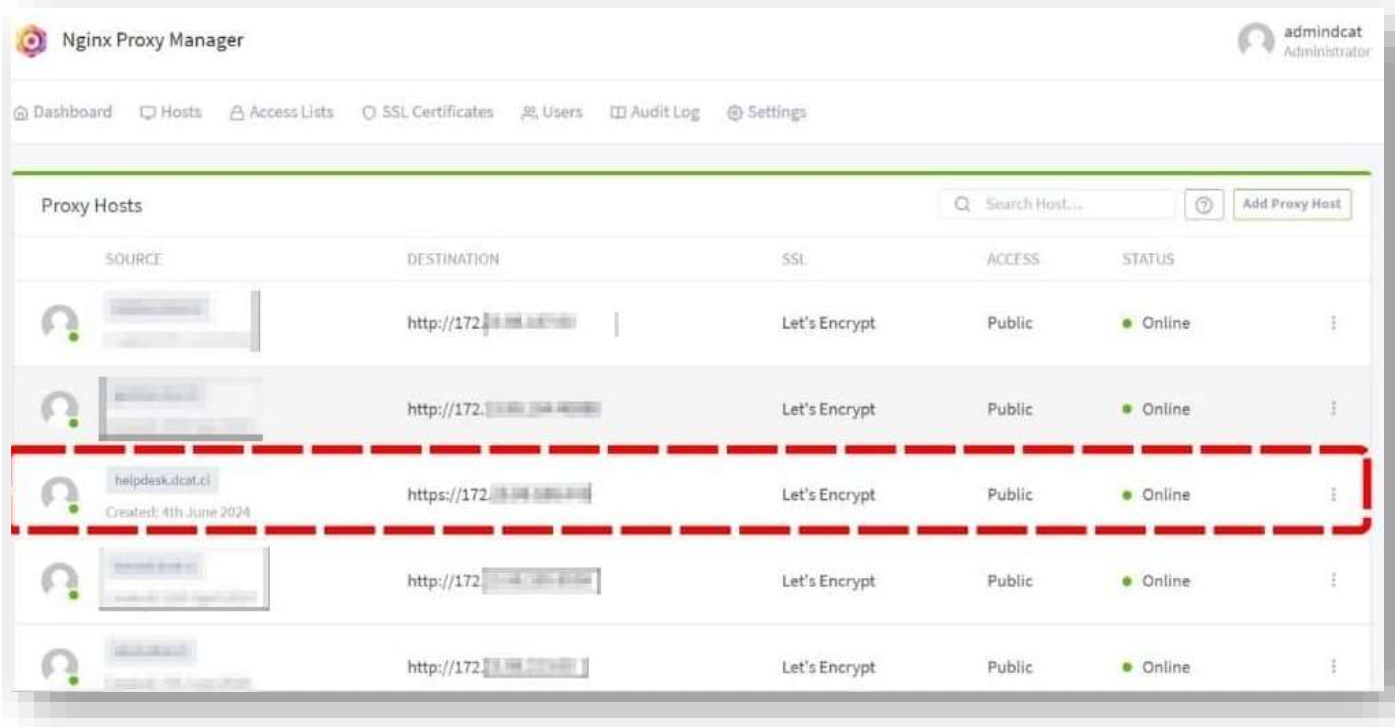







➤ Illustration 20 : Boîte de dialogue des détails du nouvel hôte à ajouter



➤ Illustration 21 : Boîte de dialogue du certificat SSL du nouvel hôte à ajouter

Nous pouvons constater dans l'illustration 22 ci-dessous que notre nouvel hôte a bel et bien été ajouté à la liste des hotes gérés par notre serveur reverse proxy.



SOURCE	DESTINATION	SSL	ACCESS	STATUS
 [redacted]	http://172.[redacted]	Let's Encrypt	Public	Online
 [redacted]	http://172.[redacted]	Let's Encrypt	Public	Online
 helpdesk.dcat.ci Created: 4th June 2024	https://172.[redacted]	Let's Encrypt	Public	Online
 [redacted]	http://172.[redacted]	Let's Encrypt	Public	Online
 [redacted]	http://172.[redacted]	Let's Encrypt	Public	Online

➤ Illustration 22 : Liste des hôtes pris en compte par Nginx Proxy Manager

La réalisation de ces étapes aura pour conséquence d'afficher dorénavant notre application web de gestion de tickets HELPDESK DCAT lorsque le nom de sous-domaine "helpdesk.dcat.ci" sera consulté via internet dans un navigateur web.

## IX. TESTS ET VÉRIFICATIONS

### 1. Vérification du fonctionnement correct de l'application à distance

Nous testons l'accès à l'application web en utilisant le nom de sous-domaine depuis différents réseaux internet pour nous assurer que l'application est accessible et fonctionne correctement pour tous les utilisateurs distants et sur des terminaux différents.

- Accès depuis un Ordinateur portable connecté sur le réseau "(((K•T•S•C)))" comme le montrent les illustrations 23 et 24



➤ *Illustration 23 : Interface de HELPDESK DCAT sur le navigateur d'un ordinateur portable*

## Network & internet > Wi-Fi > (((K•T•S•C)))

Help protect your privacy by making it harder for people to track your device location when you connect to this network. The setting takes effect the next time you connect to this network.

Off

IP assignment: Automatic (DHCP)

Edit

DNS server assignment: Automatic (DHCP)

Edit

SSID: (((K•T•S•C)))

Copy

Protocol: Wi-Fi 4 (802.11n)

Security type: WPA2-Personal

Manufacturer: Intel Corporation

Description: Intel(R) Wi-Fi 6 AX201 160MHz

Driver version: 22.250.1.2

Network band: 2.4 GHz

Network channel: 10

Link speed (Receive/Transmit): 72/72 (Mbps)

Link-local IPv6 address: fe80::fa64:284e:5461:bce9%3

IPv4 address: 192.168.161.3

IPv4 DNS servers: 192.168.161.27 (Unencrypted)

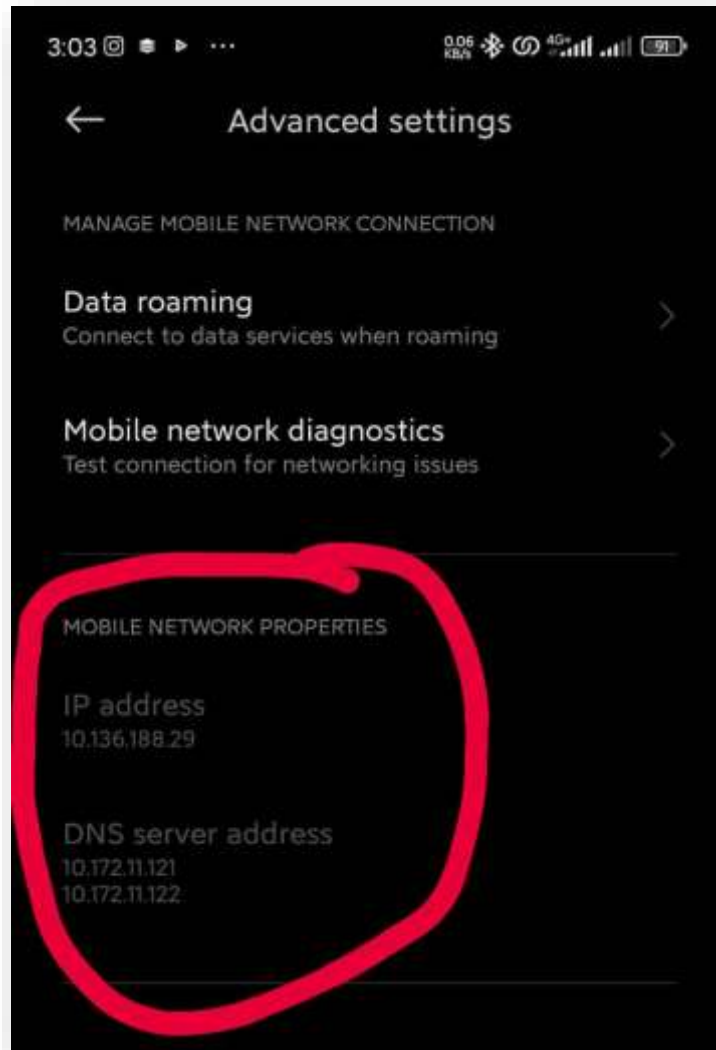
➤ *Illustration 24 : Caractéristiques du réseau sur lequel est connecté l'ordinateur*



- Accès depuis un téléphone portable connecté via les données mobiles comme le montrent les illustrations 25 et 26



➤ Illustration 25 : Interface de HELPDESK DCAT sur le navigateur d'un téléphone portable



➤ *Illustration 26 : Caractéristiques du réseau mobile sur lequel est connecté le téléphone*

Nous pouvons constater que notre application web "HELPDESK DCAT" est effectivement accessible à distance simplement grâce à un navigateur et une connexion internet quel que soit le périphérique (Ordinateur ou téléphone).

## 2. Évaluation de la sécurité du déploiement

Nous testons les mesures de sécurité mises en place, telles que les configurations du serveur reverse proxy, les règles de filtrage IP, et les certificats SSL/TLS.

- **Configurations du serveur reverse proxy**

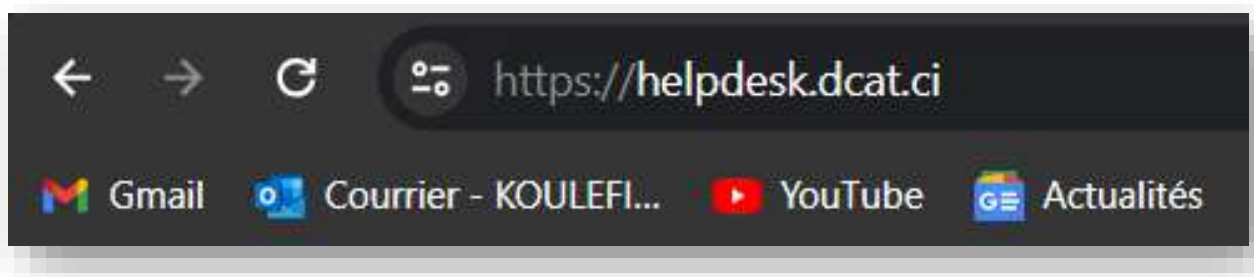
Nous parvenons à voir l'interface HELPDESK DCAT, ce qui confirme que les configurations de notre serveur reverse proxy ont été correctement appliquées. Sinon, nous n'aurions accès qu'à l'interface de notre Nginx Proxy Manager. Donc nous pouvons être sûrs que les configurations sont prises en compte.

- **Règles de filtrage IP**

Nous parvenons à accéder à l'application dès lors que nous avons une adresse IP de classe A, B, C, ou répertoriée en Côte d'Ivoire. Cela démontre que nos réglages ont été correctement pris en compte, car sans ces configurations, l'accès n'aurait pas été possible.

- **Certificats SSL/TLS**

Lorsque nous saisissons le nom de sous-domaine « helpdesk.dcat.ci » dans le navigateur, la connexion bascule automatiquement en "https", même si nous spécifions "http://helpdesk.dcat.ci/". Cela démontre que notre certificat SSL est actif et que son utilisation est forcée pour sécuriser la communication entre le navigateur et le serveur de notre application. L'illustration 27 nous fait constater ce phénomène.



➤ *Illustration 27 : Basculement automatique en "https" dans la barre d'adresse*

## **X. FORMATION ET SUPPORT DES UTILISATEURS**

Notre système étant à présent fonctionnel et permettant l'accès distant à HELPDESK DCAT sur internet, nous allons procéder à une campagne de formation et nous rendre disponibles pour le support afin de garantir une utilisation optimale par le personnel et les clients. Nous mettrons également au point un support de formation qui résume les différentes étapes d'utilisation de l'application.

NB : Il y a une différence entre le support de formation (qui est un document) et le support (qui consiste à apporter des solutions aux utilisateurs en cas de problèmes).

### **1. Formation du personnel**

Pour former le personnel :

- Nous informons le personnel de la disponibilité d'HELPDESK DCAT en ligne.
- Nous leur expliquons comment se connecter à la plateforme avec leurs différents terminaux (ordinateurs, tablettes, smartphones).
- Des sessions de formation pratiques seront organisées pour familiariser le personnel avec les fonctionnalités et l'interface de l'application.

### **2. Formation des clients**

Pour former les clients :

- Nous informons les clients de l'existence de ce nouvel outil qu'est HELPDESK DCAT.
- Nous les guidons sur la manière de se connecter à la plateforme et d'utiliser leurs terminaux pour y accéder.
- Nous leur expliquons comment demander et suivre des interventions techniques via cette plateforme.

### 3. Support aux utilisateurs

Pour assurer le support à tous les utilisateurs :

- Nous restons à l'écoute du personnel et des clients pour résoudre d'éventuels problèmes d'accès ou d'utilisation d'HELPDESK DCAT.
- Un système de support technique sera mis en place pour répondre aux questions et résoudre les problèmes rapidement et efficacement.
- Nous collectons les retours d'expérience des utilisateurs pour améliorer continuellement l'expérience d'accès distant et la fonctionnalité de l'application.

#### 4. Support de Formation

Ce présent support de formation à l'utilisation d'HELPDESK DCAT s'adresse au personnel technique et aux clients de DCAT afin de leur expliquer les usages de bases. Ils pourront par la suite découvrir l'application par eux même et contacter l'équipe si besoin.

- **Accès à l'interface d'accueil**

- Ouvrez un navigateur web sur votre ordinateur, tablette ou téléphone
- Saisissez le nom de sous-domaine « helpdesk.dcat.ci » dans la barre d'adresse de votre navigateur et validez.
- Vous êtes à présent sur la page d'accueil d'HELPDESK DCAT comme représenté sur l'illustration 25 juste en bas.



➤ *Illustration 28 : Page d'accueil d'HELPDESK DCAT*

- **Connexion à HELPDESK DCAT**

- Une fois sur la page d'accueil, en choisissant les options "Connexion", "Ouvrir un nouveau ticket" ou "Vérifier le statut d'un ticket", vous êtes directement invité à vous connecter sur l'interface de connexion des clients comme vous pouvez le voir sur l'illustration 4.

- Si vous êtes plutôt un technicien choisissez l'option "Je suis un Technicien — Connectez-vous ici" pour accéder à l'interface de connexion des techniciens représentée par l'illustration 3 qui se trouve plus haut.
- Une fois sur l'interface de connexion qui vous concerne, entrez vos informations d'authentification (Courriel / nom d'utilisateur et mot de passe) qui vous ont été fourni par l'administrateur.
- Si vous n'en avez pas contactez l'administrateur au « +225 07 49 825 050 » ou à l'adresse « support@dcatt.ci » pour qu'il vous en attribue et vous pourrez alors vous connecter.

**NB :** En tant que personnel ou client de DCAT, vous avez automatiquement droit à un compte sur HELPDESK DCAT. N'hésitez donc pas à réclamer vos informations d'authentification auprès des administrateurs.

- **Utilisation des fonctionnalités d'HELPDESK DCAT**

- Une fois connecté vous pouvez créer des tickets d'intervention et les suivre via l'interface à laquelle vous avez accès en fonction de si vous êtes un technicien ou un client comme on peut le constater sur les illustrations 5 et 6.
- N'hésitez pas à explorer HELPDESK DCAT en suivant les instructions.
- Si besoin contactez l'administrateur au « +225 07 49 825 050 » ou à l'adresse « support@dcatt.ci »

## CHAPITRE VII : BILAN DE LA MISE EN ŒUVRE DU PROJET

### **I. ETAT D'AVANCEMENT DU PROJET**

#### **1. Présentation des Objectifs Atteints**

Nous pouvons retenir que tous les objectifs que nous nous sommes fixés lors de la description du projet ont été atteints, notamment :

- **Analyse des besoins :** Nous avons mené une enquête détaillée auprès des employés et des clients pour comprendre leurs besoins spécifiques en matière d'accès distant à l'application de gestion de tickets. Les résultats ont été utilisés pour guider la conception de notre solution.
- **Conception de l'architecture sécurisée :** Nous avons conçu une architecture qui intègre un serveur reverse proxy, un nom de sous-domaine, une configuration DNS et un port forwarding appropriés pour garantir la sécurité et la performance de l'accès distant.
- **Mise en place des composants :** Tous les composants nécessaires, y compris le serveur reverse proxy (Nginx Proxy Manager), les règles de port forwarding et les certificats SSL, ont été mis en place avec succès.
- **Tests de la solution :** Nous avons effectué des tests pour vérifier la fonctionnalité et la sécurité de la solution. Ces tests incluaient des essais d'accès distant depuis différentes localisations et des vérifications de sécurité.
- **Formation des utilisateurs :** Nous avons élaboré des supports de formation détaillés et organisés des sessions de formation pour les employés et les clients. Ces formations ont couvert l'utilisation de la solution d'accès distant ainsi que les bonnes pratiques de sécurité.
- **Maintenance et suivi :** Nous avons mis en place un plan de maintenance qui inclut des mises à jour régulières de la solution et une surveillance continue de son efficacité et de sa sécurité.



## 2. Problèmes Rencontrés et Solutions Apportées

Durant tout le processus de réalisation de ce projet, nous avons fait face à des problèmes que nous avons dû régler pour pouvoir avancer.

- **Manque de connaissances techniques** : Certains concepts nécessaires à la mise en œuvre du projet nous faisaient défaut au début. Pour surmonter cet obstacle, nous avons utilisé des ressources autodidactes pour combler nos lacunes en matière de compétences techniques.
- **Technologies payantes** : Certaines technologies initialement envisagées pour le projet étaient payantes et dépassaient notre budget. Pour résoudre ce problème, nous avons recherché des alternatives gratuites aux technologies payantes initialement envisagées, ce qui nous a permis de respecter notre budget tout en atteignant nos objectifs de sécurité et de fonctionnalité.

## II. BILAN FINANCIER DE LA MISE EN ŒUVRE DU PROJET

Les couts initiaux et les couts opérationnels présentés dans cette partie sont les coûts normaux de différents éléments cités si l'on est sensé lancer le projet en partant de zéro.

### 1. Coûts Initiaux (CAPEX)

- **Coût d'acquisition des équipements (environ 3.350.000 FCFA)**
  - Serveur hyperviseur HP (ProLiant DL ML350 G6) : 1.900.000 FCFA
  - Serveur NAS Synology (DS220) : 250.000 FCFA
  - Routeur/Firewall UBIQUITI UNIFI (USG PRO 4) : 500.000 FCFA
  - Switch UBIQUITI UNIFI (24 Non-PoE) : 650.000 FCFA
  - Box internet Orange (ZTE F6600P) : 50.000 FCFA
- **Coût des licences et des logiciels (0 FCFA)**
  - Proxmox : 0 FCFA (libre de droit et gratuit)
  - Nginx Proxy Manager : 0 FCFA (libre de droit et gratuit)
  - Container Manager : 0 FCFA (libre de droit et gratuit)

- **Coût de formation du personnel (environ 20.000 FCFA)**

## 2. Coûts Opérationnels (OPEX)

- **Coûts de maintenance et de support technique (environ 175.000 FCFA)**
  - Mise à jour régulière des logiciels utilisés (Proxmox, Nginx Proxy Manager, Container Manager) et des systèmes d'exploitation des serveurs : estimé à 25.000 FCFA maximum par an.
  - Assistance technique pour la résolution des problèmes techniques rencontrés et la gestion des incidents : estimé à 150.000 FCFA par an.
- **Coûts d'hébergement et de bande passante (environ 350.000 FCFA)**
  - Hébergement du nom de domaine chez PlanetHoster : estimé à 50.000 FCFA par an.
  - Bande passante de l'abonnement internet : estimé à 300.000 FCFA par an.
- **Coûts liés à la sécurité (environ 150.000 FCFA)**
  - Renouvellement des Certificats SSL de Let's Encrypt : estimé à 0 FCFA par an.
  - Surveillance et audits de l'infrastructure : estimé à 150.000 FCFA par an.

## 3. Conclusion Financière

Le tableau 1 suivant fait un récapitulatif des coûts théoriques que nous avons présentés plus haut tout en les comparant à ce que l'entreprise DCAT a réellement déboursé dans le cadre de la réalisation de ce projet.

CLASSIFICATION	CATEGORIE	MONTANT R.A.Z	MONTANT DCAT
Coûts Initiaux (CAPEX)	Coût d'acquisition des équipements	3 350 000 CFA	0 CFA
	Coût des licences et des logiciels	0 CFA	0 CFA
	Coût de formation du personnel	20 000 CFA	20 000 CFA
	<b>TOTAL CAPEX</b>	<b>3 370 000 CFA</b>	<b>20 000 CFA</b>
Coûts Opérationnels (OPEX)	Coûts de maintenance et de support technique	175 000 CFA	0 CFA
	Coûts d'hébergement et de bande passante	350 000 CFA	0 CFA
	Coûts liés à la sécurité	150 000 CFA	0 CFA
	<b>TOTAL OPEX</b>	<b>675 000 CFA</b>	<b>0 CFA</b>
<b>CAPEX + OPEX</b>	<b>TOTAUX</b>	<b>4 045 000 CFA</b>	<b>20 000 CFA</b>

➤ *Tableau 1 : Bilan financier de la mise en œuvre du projet*

Nous remarquons que plusieurs coûts théoriques (Montant R.A.Z) se sont annulés au niveau de DCAT. En effet, cela est dû au fait que l'entreprise a déjà fait ces dépenses dans le cadre de projets antérieurs. De ce fait, ces dépenses ne peuvent donc pas être attribuées à notre projet d'accès distant.

Nous avons donc réussi cette manœuvre qui ne fait dépenser que 20.000 FCFA à l'entreprise au lieu de plus de 4.000.000 FCFA en utilisant majoritairement les moyens mis à disposition par DCAT. Ce qui nous permet de faire des économies de plus de 4.000.000 FCFA et même mieux ; ceci nous permet de rentabiliser les investissements de DCAT en ce sens qu'ils sont utilisés pour potentiellement faire gagner de l'argent à l'entreprise ou apporter de la valeur ajoutée à ses services.

## **PARTIE IV : BILAN DU STAGE**

Cette partie fait un récapitulatif des activités menées pendant le stage de façon générale, les compétences que nous avons pu en tirer ainsi que nos suggestions à l'entreprise d'accueil.

## CHAPITRE VIII : DÉROULEMENT DU STAGE

### **I. ACTIVITÉS RÉALISÉES**

#### **1. Réalisation effective du Projet de fin d'étude**

- **Description** : Nous avons implémenté une solution d'accès distant pour la gestion des tickets d'interventions techniques au sein de la société DCAT.
- **Résultat** : La solution est pleinement opérationnelle, permettant aux techniciens et aux clients de créer et suivre des tickets d'intervention en ligne de manière efficace et sécurisée.
- **Impact** : Cette réalisation a significativement amélioré la gestion des interventions techniques, optimisant les délais de réponse et la satisfaction des clients.

#### **2. Participations aux projets internes**

- **Description** : Nous avons collaboré à divers projets internes du service digital de DCAT, notamment la mise en place d'un système interne de gestion de stock, de gestion financière et administrative.
- **Résultat** : Ces systèmes ont été déployés avec succès, apportant une meilleure organisation et un suivi plus rigoureux des stocks, des finances et de l'administratif de l'entreprise.
- **Impact** : Ces projets ont contribué à améliorer l'efficacité opérationnelle et à rationaliser les processus internes de l'entreprise.

#### **3. Participation à certains projets externes sur chantiers**

- **Description** : Nous avons participé à des missions techniques chez certains clients de DCAT, notamment la mise en réseau de plusieurs postes de travail dans une régie de radio.
- **Résultat** : Les projets clients ont été menés à bien, répondant aux besoins spécifiques des clients et améliorant leur infrastructure technique.
- **Impact** : Ces interventions ont démontré notre capacité satisfaire nos clients et à fournir des solutions techniques fiables et efficaces.

#### 4. Participation à une formation en Audiovisuel (MAirList)

- **Description** : Nous avons suivi une formation sur l'utilisation de la suite logicielle MAirList, spécialisée dans la gestion informatisée des programmes de radio.
- **Résultat** : Nous avons acquis une connaissance de MAirList, permettant une gestion efficace des programmes et des émissions de radio.
- **Impact** : Cette compétence supplémentaire nous permet de contribuer de manière significative aux projets audiovisuels de l'entreprise, offrant une valeur ajoutée aux services de DCAT.

## II. COMPÉTENCES ACQUISES

Grâce aux activités réalisées et aux expériences vécues durant ce stage, nous avons développé des compétences essentielles, tant sur le plan technique que personnel :

### 1. Compétences techniques

- **Gestion de projet** : Capacité à planifier, exécuter et finaliser des projets techniques, en respectant les délais et les objectifs fixés.
- **Administration réseau** : Maîtrise des concepts et des outils de gestion des réseaux informatiques, y compris la configuration de routeurs, de pare-feux et de serveurs.
- **Déploiement de solutions web** : Expérience dans la mise en place de solutions web sécurisées, incluant l'utilisation de reverse proxy, le port forwarding et les certificats SSL.
- **Support technique** : Compétence dans la résolution de problèmes techniques et l'assistance aux utilisateurs, améliorant ainsi leur expérience avec les systèmes déployés.
- **Familiarisation avec la notion de conteneurisation** : Apprentissage des concepts de conteneurisation et de virtualisation légère avec Docker. Compréhension des avantages et des principes de fonctionnement des conteneurs pour le déploiement et la gestion d'applications.
- **Familiarisation à certaines notions de comptabilité** : Apprentissage des concepts de coûts d'acquisition, de coûts d'exploitation, d'amortissement des investissements qui sont très importants pour le contrôle du volet financier d'une entreprise.

## 2. Compétences personnelles

- **Communication** : Amélioration de la capacité à expliquer des concepts techniques à des utilisateurs non techniques, facilitant leur compréhension et leur adoption des nouvelles solutions.
- **Travail en équipe** : Expérience de collaboration efficace avec différents départements et équipes de projet, renforçant la cohésion et la productivité.
- **Gestion du temps** : Développement de la capacité à gérer efficacement plusieurs projets et tâches simultanément, en respectant les délais imposés.
- **Adaptabilité** : Capacité à s'adapter rapidement à de nouveaux environnements et technologies, et à résoudre les défis imprévus de manière proactive.

## III. SUGGESTIONS À L'ENTREPRISE

### 1. Renforcer les investissements

Nous recommandons d'augmenter les investissements dans l'hébergement et l'accès à distance pour les autres applications web de DCAT actuellement en développement. Des investissements supplémentaires permettront d'améliorer la performance et la sécurité de ces systèmes, garantissant une meilleure expérience utilisateur et une protection accrue des données.

### 2. Impliquer davantage le personnel

Une implication accrue du personnel de DCAT dans les projets d'hébergement et d'accès à distance est essentielle. En formant et en sensibilisant les employés aux bonnes pratiques de sécurité et aux technologies utilisées, l'entreprise peut maximiser l'efficacité et la fiabilité de ses systèmes.

### **3. Améliorer la disponibilité et la sécurité**

Bien que les solutions d'hébergement et d'accès à distance mises en place par DCAT soient satisfaisantes, il est crucial de viser une amélioration continue. En investissant dans des infrastructures plus robustes et en adoptant des technologies de pointe, DCAT peut augmenter la disponibilité et la sécurité de ses services.

### **4. Devenir un hébergeur local de premier plan**

Avec des investissements et des améliorations continues, DCAT pourrait envisager de devenir l'un des meilleurs hébergeurs locaux. Si l'entreprise souhaite offrir des services d'hébergement à des particuliers, elle devra se concentrer sur l'optimisation de la performance, de la sécurité et de la fiabilité de ses solutions. Cela pourrait ouvrir de nouvelles opportunités de marché et renforcer la position de DCAT dans le secteur des technologies de l'information.



## CONCLUSION

La problématique initiale de ce projet était de permettre un accès distant sécurisé à l'application déjà existante de gestion des tickets d'interventions techniques de la société DCAT. Nous avons entrepris ce projet avec l'objectif de répondre aux besoins des employés et des clients en termes de connectivité et de sécurité, tout en garantissant une utilisation optimale de l'application web HELPDESK DCAT.

Pour concevoir et implémenter le système, nous avons suivi une méthodologie rigoureuse, en commençant par une analyse détaillée des besoins. Cette analyse nous a conduits à choisir des technologies adaptées à notre infrastructure, notamment l'utilisation de Nginx Proxy Manager pour le reverse proxy. La configuration des règles de sécurité, la mise en place de certificats SSL/TLS, ainsi que l'optimisation du port forwarding ont été des étapes cruciales pour garantir la sécurité et l'efficacité du système d'accès distant. Nous avons également assuré la formation et le support des utilisateurs pour faciliter l'adoption de cette nouvelle solution.

Le bilan de ce projet est très positif. Nous avons atteint tous les objectifs fixés : l'application est désormais accessible à distance sur le net, sécurisée, et utilisable par les employés et les clients. Les problèmes rencontrés ont été surmontés grâce à une approche proactive et une adaptation continue aux défis techniques. Cependant, ce projet ouvre également des perspectives pour l'avenir. Nous recommandons de renforcer les investissements ainsi que l'implication du personnel de DCAT dans l'hébergement et l'accès à distance des autres applications web. Certes l'hébergement et l'accès à distance mis en place par l'entreprise ne sont pas les meilleures du monde en matière de disponibilité et de sécurité mais ils sont déjà satisfaisants. Plus d'investissements dans ce sens pourraient propulser DCAT parmi les meilleurs hébergeurs locaux si jamais ils souhaitent offrir ce service à des particuliers.

En conclusion, ce projet a non seulement répondu à la problématique initiale, mais a également posé les bases pour des améliorations continues, assurant ainsi la pérennité et l'efficacité des systèmes informatiques en particulier web de la société DCAT.

## ***BIBLIOGRAPHIE***

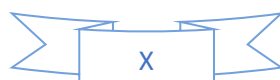
### ***Mémoires et Rapports***

- ***DIALLO Azise Oumar, TALL Hamadoun***, (2019). « Etude et mise en place d'un réseau informatique sécurisé à l'hôpital de jour du centre hospitalier universitaire Sanou Souro de Bobo-Dioulasso ». Mémoire de fin de cycle, Bobo-Dioulasso, UPB: Ecole Supérieure d'Informatique, 2009-2010, 75 pages ;
- ***OUEDRAOGO Souleymane***, « Réalisation d'une solution de bascule automatique du secours audio pour une station de radiodiffusion : cas de la radio AL HIKMAH ». Mémoire de fin de cycle, Yamoussoukro, INP-HB : ESI, 2018 – 2019, 64 pages ;
- ***Ezan TAHI***, « Conception des API d'une application de gestion scolaire ». Mémoire de fin de cycle, Yamoussoukro, INP-HB : ESI, 2021-2022, 64 pages ;
- ***KOMBO Madou Hope Othniel***, « Conception et réalisation d'une application de gestion des paiements : cas de l'église saint-joseph ». Mémoire de fin de cycle, Yamoussoukro, INP-HB : ESI, 2022-2023, 127 pages ;



## WEBOGRAPHIE

- <https://www.youtube.com/watch?v=QxH9DNWY4yo> | importer conteneur sur mon Synology | consulté le 24/05/2024 à 17h14
- <https://www.youtube.com/watch?v=QxH9DNWY4yo> | Docker avec Synology: Container Manager | consulté le 24/05/2024 à 15h34
- <https://www.docker.com> | Documentation Docker | consulté le 24/05/2024 à 10h32
- <https://www.proxmox.com/en> | Documentation Proxmox | consulté le 19/05/2024 à 11h13
- <https://www.youtube.com/watch?v=Bw4akxSfnCM> | Proxmox à moindre coût: J'installe un serveur Puissant pour 40 EUR | consulté le 19/05/2024 à 10h42
- <https://www.youtube.com/watch?v=okm29mVf0nM> | Formation Docker - Les bases en moins de 20 minutes | consulté le 18/05/2024 à 17h22
- <https://www.youtube.com/watch?v=4LyyLURi544> | Installer Nginx Proxy Manager - Exposer vos services | consulté le 10/05/2024 à 14h57
- [https://www.youtube.com/results?search\\_query=nginx+proxy+manager](https://www.youtube.com/results?search_query=nginx+proxy+manager) | Nginx proxy manager | consulté le 10/05/2024 à 14h12
- <https://www.youtube.com/watch?v=IDD2K7qmYhw&list=PPSV> | Les Tutos - Proxmox No 1 : Installation, configuration, création stockage et VM - (CE\*) | consulté le 09/05/2024 à 22h12
- <https://nginxproxymanager.com> | Documentation Nginx Proxy Manager | consulté le 08/05/2024 à 16h43



# TABLE DES MATIERES

<b>DÉDICACES</b> .....	I
<b>REMERCIEMENTS</b> .....	II
<b>AVANT-PROPOS</b> .....	III
<b>SOMMAIRE</b> .....	IV
<b>LISTE DES FIGURES, ILLUSTRATIONS ET TABLEAUX</b> .....	V
<b>LISTE DES SIGLES ET ABRÉVIATIONS</b> .....	VI
<b>RÉSUMÉ</b> .....	VIII
<b>INTRODUCTION</b> .....	1
<b>PARTIE I : CADRE ET CONTEXTE DU PROJET</b> .....	2
<b>CHAPITRE I : PRÉSENTATION DE LA STRUCTURE D'ACCUEIL</b> .....	3
<b>I. GÉNÉRALITÉ</b> .....	3
➤ <i>Illustration 1 : Plan de localisation de DCAT</i> .....	3
<b>II. ACTIVITÉS</b> .....	4
1. Audiovisuel .....	4
2. Sécurité électronique .....	4
3. Solutions intégrées .....	4
<b>III. ORGANIGRAMME</b> .....	5
➤ <i>Figure 1 : Organigramme de DCAT</i> .....	5
<b>CHAPITRE II : DESCRIPTION DU PROJET</b> .....	6
<b>I. CONTEXTE DU PROJET</b> .....	6
<b>II. OBJECTIFS DU PROJET</b> .....	6
1. Objectif général .....	6
2. Objectifs spécifiques .....	6
<b>III. CAHIER DES CHARGES</b> .....	7
1. Description du public ciblé .....	7
2. Spécifications fonctionnelles .....	8
3. Contraintes .....	8
4. Livrables .....	9
5. Validation .....	9
<b>PARTIE II : ÉTUDE CONCEPTUELLE</b> .....	10
<b>CHAPITRE III : ENQUÊTES ET ÉTAT DES LIEUX</b> .....	11
<b>I. ENQUÊTES SUR LES BESOINS ET EXIGENCES</b> .....	11
1. Identification des besoins spécifiques des utilisateurs .....	11
2. Identification des exigences .....	11

<b>II.</b>	<b>ÉTAT DES LIEUX DES MOYENS À DISPOSITION .....</b>	<b>12</b>
1.	Identification des moyens mis à disposition .....	12
2.	Rôle des moyens mis à disposition .....	12
3.	Architecture du réseau interne.....	13
	➤ <i>Figure 2 : Schéma de l'architecture du réseau interne</i> .....	13
<b>CHAPITRE IV : ÉTUDE DE FAISABILITÉ .....</b>		<b>14</b>
<b>I.</b>	<b>VEILLE TECHNOLOGIQUE.....</b>	<b>14</b>
1.	VPN (Virtual Private Network).....	14
2.	Accès distant via HTTPS .....	15
3.	Terminal Server / Remote Desktop Services (RDS) .....	16
4.	Protocoles de bureau virtuel (VDI).....	17
5.	Applications de collaboration et de partage d'écran .....	19
<b>II.</b>	<b>SELECTION DES TECHNOLOGIES .....</b>	<b>20</b>
1.	Nom de domaine et sous-domaine.....	20
2.	Redirection DNS .....	21
3.	Port forwarding .....	21
4.	Serveur Reverse Proxy .....	21
<b>CHAPITRE V : CONCEPTION DU SYSTÈME .....</b>		<b>23</b>
<b>I.</b>	<b>ARCHITECTURE DU SYSTÈME.....</b>	<b>23</b>
	➤ <i>Illustration 2 : Diagramme architectural de la solution d'accès distant</i> .....	23
1.	Nom de Domaine et Sous-Domaine.....	24
2.	Redirection DNS .....	24
3.	Port Forwarding.....	24
4.	Serveur Reverse Proxy .....	24
<b>II.</b>	<b>ÉLABORATION DU PLAN DE DÉPLOIEMENT.....</b>	<b>25</b>
1.	Présentation de l'Application Locale .....	25
2.	Création du Nom de Domaine et Sous-Domaine .....	25
3.	Configuration de la Redirection DNS .....	25
4.	Configuration du Reverse Proxy .....	25
5.	Configuration du Port Forwarding .....	26
6.	Ajout des Certificats SSL/TLS .....	26
7.	Configuration des ACL (Access Lists).....	26
8.	Indexation de l'hôte.....	26
9.	Tests et Vérifications .....	26
<b>III.</b>	<b>ÉVALUATION DES RISQUES .....</b>	<b>27</b>
1.	Vulnérabilités de Sécurité.....	27

2. Panne du Serveur .....	27
3. Problèmes de Connectivité Internet.....	28
4. Erreurs de Configuration .....	28
5. Attaques DDoS.....	29
<b>PARTIE III : MISE EN ŒUVRE DU SYSTÈME .....</b>	<b>30</b>
<b>CHAPITRE VI : IMPLÉMENTATION DES TECHNOLOGIES.....</b>	<b>31</b>
<b>I. PRÉSENTATION DE L'APPLICATION LOCALE .....</b>	<b>31</b>
1. Fonctionnement de l'application existante en local .....	31
2. Configurations actuelles de l'application .....	31
3. Interfaces de l'application .....	32
➤ Illustration 3 : Interface de connexion des techniciens .....	32
➤ Illustration 4 : Interface de connexion des clients .....	33
➤ Illustration 5 : Interface de création de tickets .....	34
➤ Illustration 6 : Tableau de bord ou liste des tickets ouverts .....	35
<b>II. CONFIGURATION DU NOM DE DOMAINE ET SOUS-DOMAIN .....</b>	<b>36</b>
1. Sélection d'un fournisseur et enregistrement du nom de domaine principal.....	36
2. Création du sous-domaine approprié pour l'accès à distance à l'application.....	37
➤ Illustration 7 : Interface N0C de visualisation des noms de domaines et de sous-domaines .....	37
3. Activation du certificat SSL/TLS sur le nom de sous-domaine.....	38
➤ Illustration 8 : Interface N0C d'activation des certificats SSL/TLS.....	38
<b>III. CONFIGURATION DE LA REDIRECTION DNS .....</b>	<b>39</b>
➤ Illustration 9 : Interface N0C de gestion des enregistrements .....	39
<b>IV. CONFIGURATION DU SERVEUR REVERSE PROXY .....</b>	<b>40</b>
1. Choix du serveur reverse proxy .....	40
2. Installation du serveur reverse proxy sur le serveur Synology NAS .....	41
➤ Illustration 10 : Interface d'installation de Container Manager sur le Synology.....	42
➤ Illustration 11 : Interface du registre de conteneurs de Container Manager .....	43
➤ Illustration 12 : Interface de démarrage des conteneurs de Container Manager.....	44
<b>V. CONFIGURATION DU PORT FORWARDING.....</b>	<b>45</b>
1. Accès à l'interface d'administration du routeur/firewall.....	45
➤ Illustration 13 : Interface web du tableau de bord du Routeur/firewall UNIFI.....	45
2. Configuration des règles de redirection de port .....	46
➤ Illustration 14 : Interface de configuration de la règle de redirection http .....	47
➤ Illustration 15 : Interface de configuration de la règle de redirection HTTPS.....	47
<b>VI. AJOUT DES CERTIFICATS SSL/TLS .....</b>	<b>48</b>
1. Accès à l'interface du Nginx Proxy Manager .....	48

2. Ajout des certificats SSL/TLS au Nginx Proxy Manager .....	48
➤ Illustration 16 : Barre de menu de l'interface du Nginx Proxy Manager .....	49
➤ Illustration 17 : Interface d'ajout de certificats SSL/TSL du Nginx Proxy Manager .....	49
<b>VII. CONFIGURATION DES ACL (ACCESS LISTS) .....</b>	<b>50</b>
1. Autorisation des applications locales .....	50
2. Autorisation des adresses privées de classe A .....	50
3. Autorisation des adresses privées de classe B .....	50
4. Autorisation des adresses privées de classe C .....	50
5. Autorisation des adresses publiques provenant de la Côte d'Ivoire .....	50
6. Non Autorisation des adresses ne respectant aucune des règles déjà énoncées .....	51
➤ Illustration 18 : Interface de création et de visualisation des règles d'accès du serveur Synology .....	51
<b>VIII. INDEXATION DE L'HÔTE .....</b>	<b>52</b>
1. Accès à l'interface d'ajout des hôtes .....	52
➤ Illustration 19 : Menu et sous-menu d'accès à l'interface d'ajout des hôtes .....	52
2. Liaison de l'hôte au nom de sous-domaine .....	52
➤ Illustration 20 : Boîte de dialogue des détails du nouvel hôte à ajouter .....	53
➤ Illustration 21 : Boîte de dialogue du certificat SSL du nouvel hôte à ajouter .....	53
➤ Illustration 22 : Liste des hôtes pris en compte par Nginx Proxy Manager .....	54
<b>IX. TESTS ET VÉRIFICATIONS .....</b>	<b>55</b>
1. Vérification du fonctionnement correct de l'application à distance .....	55
➤ Illustration 23 : Interface de HELPDESK DCAT sur le navigateur d'un ordinateur portable .....	55
➤ Illustration 24 : Caractéristiques du réseau sur lequel est connecté l'ordinateur ....	56
➤ Illustration 25 : Interface de HELPDESK DCAT sur le navigateur d'un téléphone portable .....	57
➤ Illustration 26 : Caractéristiques du réseau mobile sur lequel est connecté le téléphone .....	58
2. Évaluation de la sécurité du déploiement .....	59
➤ Illustration 27 : Basculement automatique en "https" dans la barre d'adresse .....	59
<b>X. FORMATION ET SUPPORT DES UTILISATEURS .....</b>	<b>60</b>
1. Formation du personnel .....	60
2. Formation des clients .....	60
3. Support aux utilisateurs .....	61
4. Support de Formation .....	62
➤ Illustration 28 : Page d'accueil d'HELPDESK DCAT .....	62
<b>CHAPITRE VII : BILAN DE LA MISE EN ŒUVRE DU PROJET .....</b>	<b>64</b>
<b>I. ETAT D'AVANCEMENT DU PROJET .....</b>	<b>64</b>

1. Présentation des Objectifs Atteints.....	64
2. Problèmes Rencontrés et Solutions Apportées .....	65
II. BILAN FINANCIER DE LA MISE EN ŒUVRE DU PROJET.....	65
1. Coûts Initiaux (CAPEX) .....	65
2. Coûts Opérationnels (OPEX) .....	66
3. Conclusion Financière.....	66
➤ Tableau 1 : Bilan financier de la mise en œuvre du projet .....	66
<b>PARTIE IV : BILAN DU STAGE .....</b>	<b>68</b>
<b>CHAPITRE VIII : DÉROULEMENT DU STAGE.....</b>	<b>69</b>
I. ACTIVITÉS RÉALISÉES.....	69
1. Réalisation effective du Projet de fin d'étude .....	69
2. Participations aux projets internes .....	69
3. Participation à certains projets externes sur chantiers.....	69
4. Participation à une formation en Audiovisuel (MAirList) .....	70
III. COMPÉTENCES ACQUISES .....	70
1. Compétences techniques .....	70
2. Compétences personnelles .....	71
IV. SUGGESTIONS À L'ENTREPRISE.....	71
1. Renforcer les investissements .....	71
2. Impliquer davantage le personnel.....	71
3. Améliorer la disponibilité et la sécurité.....	72
4. Devenir un hébergeur local de premier plan .....	72
<b>CONCLUSION .....</b>	<b>73</b>
<b>BIBLIOGRAPHIE .....</b>	<b>IX</b>
<b>WEBOGRAPHIE .....</b>	<b>X</b>
<b>TABLE DES MATIERES .....</b>	<b>XI</b>