DEDICATION

To my family ;

ACKNOWLEDGEMENTS

I would like to express my gratitude to the School of Industry at the Félix Houphouët Boigny National Polytechnic Institute, especially to *Mr. OUATTARA Adama*, Director of ESI, and *Mr. KPO Loua Daniel*, Director of Studies, for including this final year internship in our training. Their support helped me quickly find an internship to refine my skills and complete my studies with a final project.

I thank my academic supervisor, *Mr. KONAN N'Dri*, for his guidance in keeping me aligned with the institute's educational principles.

I am also grateful to *Mr. DIAKITÉ Check Amadou Tidiane*, CEO of DCAT, for believing in me and welcoming me into his company. Special thanks to *Mr. BOGNINI Jean Abraham* for his support and advice, as well as for sharing his expertise in Network Computing. My thanks also go to the entire DCAT team, especially *Mr. KOICHY Don Sylvain*, *Ms. DIALLO Fanta*, *Mr. KOSSÉRÉ Jean-Jacques*, *Mr. SIMBORO Mohamed*, and *Mr. DOUMBIA Abdoulaye*.

This internship allowed me to apply and refine the skills and knowledge I acquired over the past three academic years while discovering the methods and means used in the business world. It represents the culmination of my journey in the Advanced Technician cycle from 2021 to 2024.

Finally, I thank my loved ones for their financial, emotional, and spiritual support throughout this period.

FOREWORD

The Félix Houphouët-Boigny National Polytechnic Institute (INP-HB) in Yamoussoukro was established in September 1996 by decree N°96-678, following the fusion of four major schools: the National Higher School of Agronomy (ENSA), the National Higher School of Public Works (ENSTP), the Agricultural Institute of Bouaké (IAB), and the National Higher Institute of Technical Education (INSET). This merger aimed to revitalize these institutions to train a youth capable of meeting professional challenges and to make Yamoussoukro a technopole.

Today, INPHB comprises nine schools:

- *School of Industry (ESI),*
- *School of Agronomy (ESA),*
- *School of Commerce and Business Administration (ESCAE),*
- *School of Public Works (ESTP),*
- *School of Mines and Geology (ESMG),*
- *School of Continuing Education and Executive Training (EFCPC),*
- *Preparatory Classes for the Grandes Écoles (CPGE),*
- *Polytechnic Doctoral School (EDP),*
- *School of Petroleum and Energy (ESPE).*

Our training as Advanced Technicians in Computing takes place at ESI, which trains engineers and advanced technicians in various industrial fields. At the end of the studies, practical internships in companies allow students to apply their knowledge and face the realities of the professional world. This is how the company Data Communications and All Technologies (DCAT) welcomed us from April 2 to June 7, 2024, to carry out the project presented in this report.

TABLE OF CONTENTS

LIST OF FIGURES, ILLUSTRATIONS, AND TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

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

ABSTRACT

This project aims to modernize DCAT's IT services by providing secure remote access to its ticket management system. Facing evolving technological needs, DCAT initiated the implementation of a solution allowing employees and clients to remotely access the "HELPDESK DCAT" ticket management application, which is already operational on the local network.

To address this challenge, our mission was to implement a secure architecture for remote access to the application, considering performance and security requirements. We chose an HTTPS-based architecture, leveraging technologies like Nginx Proxy Manager and SSL/TLS to ensure communication security and privacy.

Implementing this solution required thorough analysis of user needs and meticulous system architecture design. We conducted tests to ensure functionality and security, emphasizing security best practices.

At the end of the project, we successfully established a functional and secure solution for remote access to the HELPDESK DCAT application. This achievement demonstrates our ability to tackle technological challenges and offer innovative solutions meeting specific client needs.

However, challenges arose throughout the process, including technical complexity and budget constraints. Despite these obstacles, we demonstrated resilience and ingenuity to complete the project within the allotted timeframe.

INTRODUCTION

In a world where information and communication technologies are crucial, remote access to business applications is essential for business continuity. This need has been amplified by remote work, forcing companies to offer secure and efficient access to their applications.

Our final year project aims to implement a secure remote access solution for OsTicket, a web-based ticket management application that is already functional and hosted on the company's local server. This application is vital for the company, both for employees and clients. However, its remote access is complex as it is only accessible on the local network.

This report details our approach to addressing these challenges by integrating best practices in computer networking and information system security, considering the available resources.

We will begin with a presentation of the project framework and context, followed by a conceptual study. Then, we will describe the implementation steps of the project and conclude with an overview of the achievements made during this final year internship and the future prospects within the company.

PART I: PROJECT FRAMEWORK AND CONTEXT

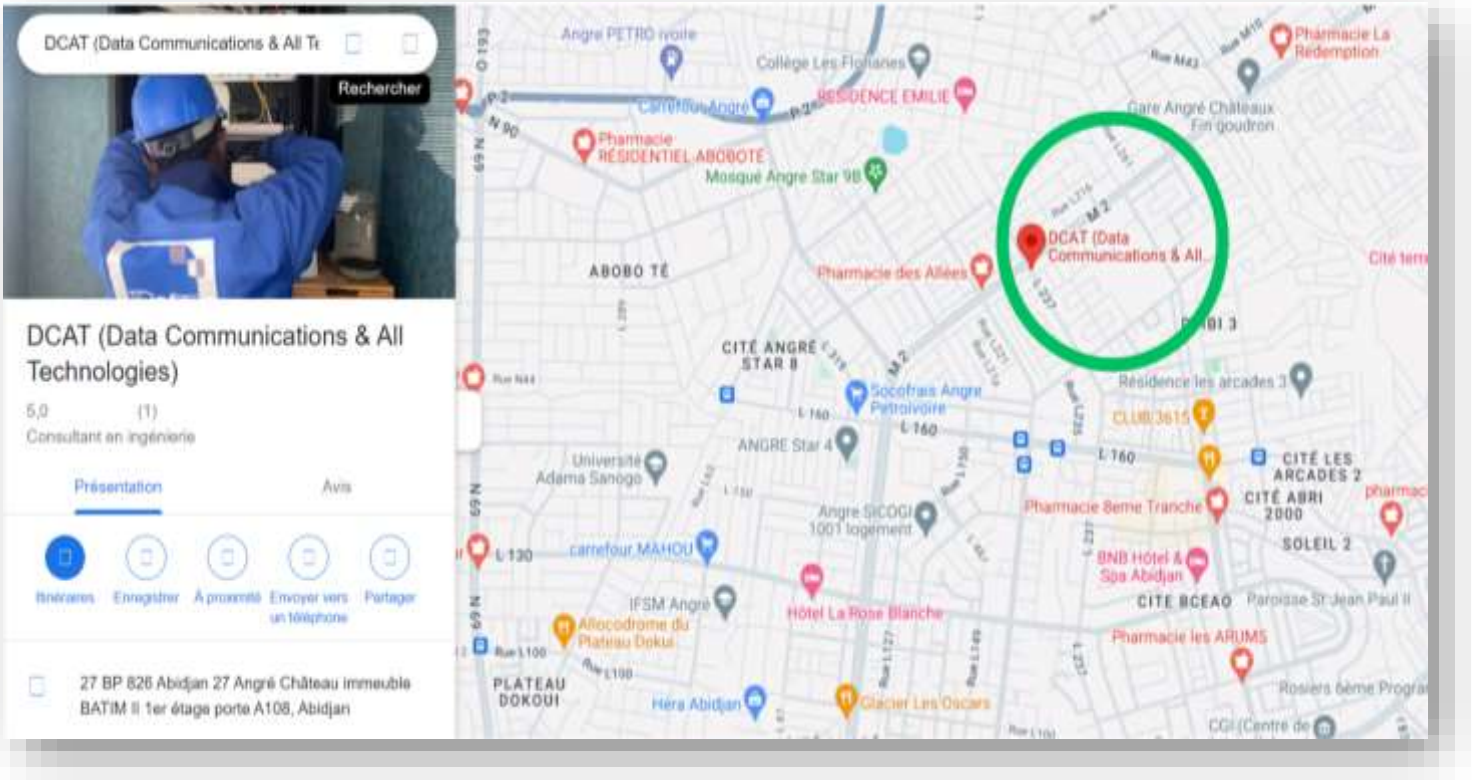
This section presents the host company and the assigned project topic.

CHAPTER I: HOST COMPANY PRESENTATION

I. GENERAL INFORMATIONS

Data Communications and All Technologies (DCAT) is a company specializing in technical expertise and engineering in telecommunications. Established in 2004 and located in Abidjan, Cocody, within the BATIM building in Angré Château, DCAT brings together a diverse team of engineers and technicians from various schools in Côte d'Ivoire and the sub-region, along with experienced collaborators and consultants in information systems, with particular expertise in audiovisual and IT. The company leverages this solid experience to offer innovative solutions tailored to telecommunications, data transmission, and security needs.

Illustration 1 below shows the location of the company.



➢ *Illustration 1: Location map of DCAT*

II. ACTIVITIES

Our mission is to provide technical solutions in audiovisual telecommunications, data transmission, and electronic security in Africa. DCAT's expertise spans three key areas:

1. Audiovisual

DCAT excels in creating TV and radio channels, audiovisual production, and setting up audiovisual and data distribution networks. Our competencies include managing technical files for frequency allocation, technical studies of production and broadcasting sites, installing radio equipment, configuring production premises, and cabling for collective TV channel reception.

2. Electronic Security

We offer solutions to protect families, properties, and businesses in a concerning security context. Our services include auditing your security system, designing and implementing security systems such as intercoms and access control devices, video surveillance, and integrating video surveillance with the telecommunication network. We also provide, install, and maintain broadcasting equipment.

3. Integrated Solutions

DCAT innovates in Information and Communication Technologies (ICT) in Africa. We have established a remote distribution network integrating various services such as TV, radio, internet access, and video surveillance. This comprehensive approach ensures an optimal user experience by providing efficient access to these services within a single quality platform.

CHAPTER II : PROJECT DESCRIPTION

I. PROJECT CONTEXT

Our arrival at DCAT for a three-month final year internship, starting on April 2, 2024, coincided with a crucial moment for the company: the launch of a web application project for ticket management by the Digital service. In this digitization context, we seized the opportunity to make this application accessible remotely on the company's server.

In this stimulating context, we were tasked with working on the project titled: "Implementation of a Remote Access Solution for Technical Ticket Management: The Case of DCAT". This project reflects our commitment to contributing to the digital transformation of DCAT, a major player in Information and Communication Technologies in Côte d'Ivoire. This enriching experience allowed us to apply our academic knowledge and discover corporate processes.

II. PROJECT OBJECTIVES

1. General Objective

The general objective is to design and implement a secure remote access solution for DCAT employees and clients to a web-based ticket management application hosted on a local server.

2. Specific Objectives

The specific objectives are those follow:

- Analyze the needs of employees and clients for remote access to the application.
- Design a secure architecture for remote access to the application, considering security and performance requirements.
- Implement the necessary components to enable this access.
- Test the solution to ensure its functionality and security.
- Train users on how to use the remote access solution.
- Ensure maintenance and follow-up of the solution after implementation.

III. REQUIREMENTS SPECIFICATION

1. Target Audience

The project targets DCAT employees and clients, providing them with remote access to the ticket management application.

2. Functional Specifications

The solution must allow secure connection to the application, ensuring data confidentiality and optimal performance even during simultaneous use by many users.

3. Constraints

- Implementation within two months from the 8th April, 2024
- Adherence to the allocated project budget.
- Compliance with data security and confidentiality standards.

4. Deliverables:

- Design and implementation documentation.
- Test report.
- Training support for users.

5. Validation

The solution will be validated by DCAT managers.

This requirements specification serves as the reference framework for the design and deployment of a secure remote access solution to a web-based ticket management application for DCAT.

PART II : CONCEPTUAL STUDY

In this part, we will detail the conceptual analysis of the project, including needs and requirements, technical feasibility, and the preliminary design of the solution.

CHAPTER III : SURVEYS AND CURRENT STATE

I. NEEDS AND REQUIREMENTS SURVEY

1. Identifying Specific User Needs

- Remote access to a locally hosted application.
- Usage from various devices (computers, smartphones, etc.).
- Data security during remote access.
- Continuous availability of the application.

2. Identifying Requirements

- **Security:** Secure remote access to protect data.
- **Performance:** Fast response times for a satisfactory user experience.
- **Compatibility:** Accessibility from different browsers and operating systems.
- **Availability:** 24/7 access to meet operational needs.

II. CURRENT RESOURCES ASSESSMENT

1. Identifying Available Resources

- Hypervisor server.
- Synology server.
- Switches.
- Unifi router/firewall.
- VoIP telephony server.
- Internet access via fiber optic.

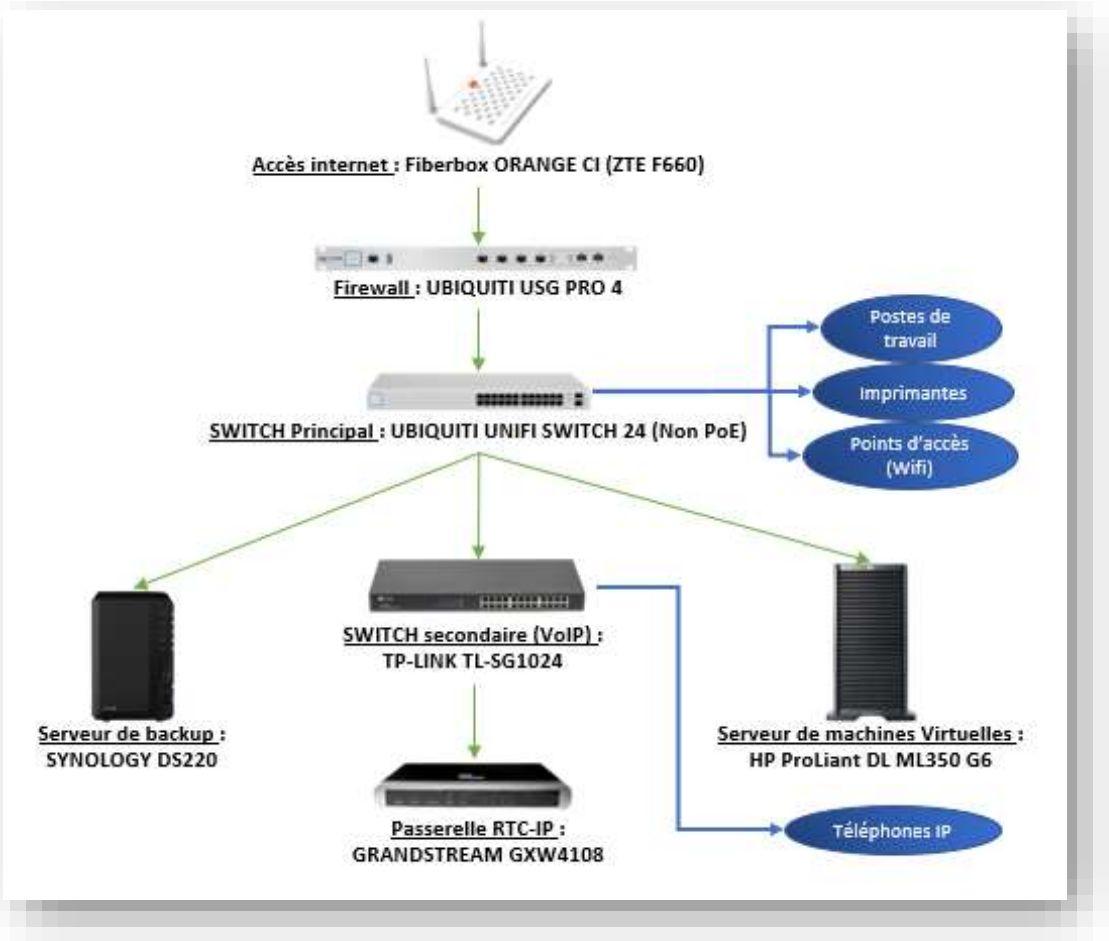
- Regulated power supply.
- Devices and terminals.

2. Role of Available Resources

- **Hypervisor server:** Creates and manages virtual machines for server and application virtualization.
- **Synology server:** Provides data backup and restoration.
- **Switches:** Ensure connectivity within the local network.
- **Router/Firewall:** Manages network traffic and ensures security.
- **VoIP Telephony Server:** Manages internal phone calls.
- **Internet Access via Fiber Optic:** Provides internet connectivity.
- **Regulated Power Supply:** Protects equipment from voltage fluctuations.
- **Devices and Terminals:** Facilitate user interaction with the system.

3. Internal Network Architecture

Figure 1 below presents the internal network architecture of the company.



➢ *Figure 1 : Internal network architecture diagram.*

CHAPTER IV : FEASIBILITY STUDY

I. TECHNOLOGICAL MONITORING

1. VPN (Virtual Private Network)

- **Functioning:** Creates a secure tunnel over the internet for secure remote access to the company's internal network.
- **Advantages:** Enhanced security, universal access, centralized management.
- **Disadvantages:** Complexity, cost, impact on internet speed.

2. Remote Access via HTTPS:

- **Functioning:** Uses HTTPS protocol for secure remote access to a web application.
- **Advantages:** Enhanced security, ease of use, compatibility.
- **Disadvantages:** Dependence on the web server, certificate management, impact on performance.

3. Terminal Server / Remote Desktop Services (RDS):

- **Functioning:** Allows remote access to a complete desktop environment.
- **Advantages:** Familiar user experience, centralized resources, flexibility.
- **Disadvantages:** Initial cost, complexity, internet dependency.

4. Virtual Desktop Infrastructure (VDI) Protocols:

- **Functioning:** Allows access to a virtual desktop hosted on central servers.
- **Advantages:** Flexibility, centralized management, enhanced security.
- **Disadvantages:** Cost, complexity, network dependency.

5. Collaboration and Screen Sharing Applications:

- **Functioning:** Allows real-time collaboration through screen sharing.
- **Advantages:** Effective collaboration, ease of use, visual interaction.
- **Disadvantages:** Internet dependency, security, functional limitations.

II. TECHNOLOGY SELECTION

After analyzing existing technologies, we concluded that the listed technologies, except for remote access via HTTPS, are not suitable for us. The reason is that they require some installation on the users' side, whereas we seek a solution that requires no installation or configuration from users. We want a ready-to-use solution once implemented, allowing everyone to easily access our OsTicket web application from anywhere. In other words, we aim for a tailored solution that provides direct access to the application based on remote access via HTTPS. To achieve this, we will use the following technologies and concepts: domain and subdomain, DNS redirection, port forwarding, reverse proxy server...

1. Domain Name and Subdomain

Assigns distinct addresses for the web application, simplifying access management.

2. DNS Redirection

Directs traffic to the IP address of the local server hosting the application, facilitating direct access.

3. Port Forwarding

Redirects incoming HTTP/HTTPS traffic to the server hosting the application, enabling access from anywhere.

4. Reverse Proxy Server

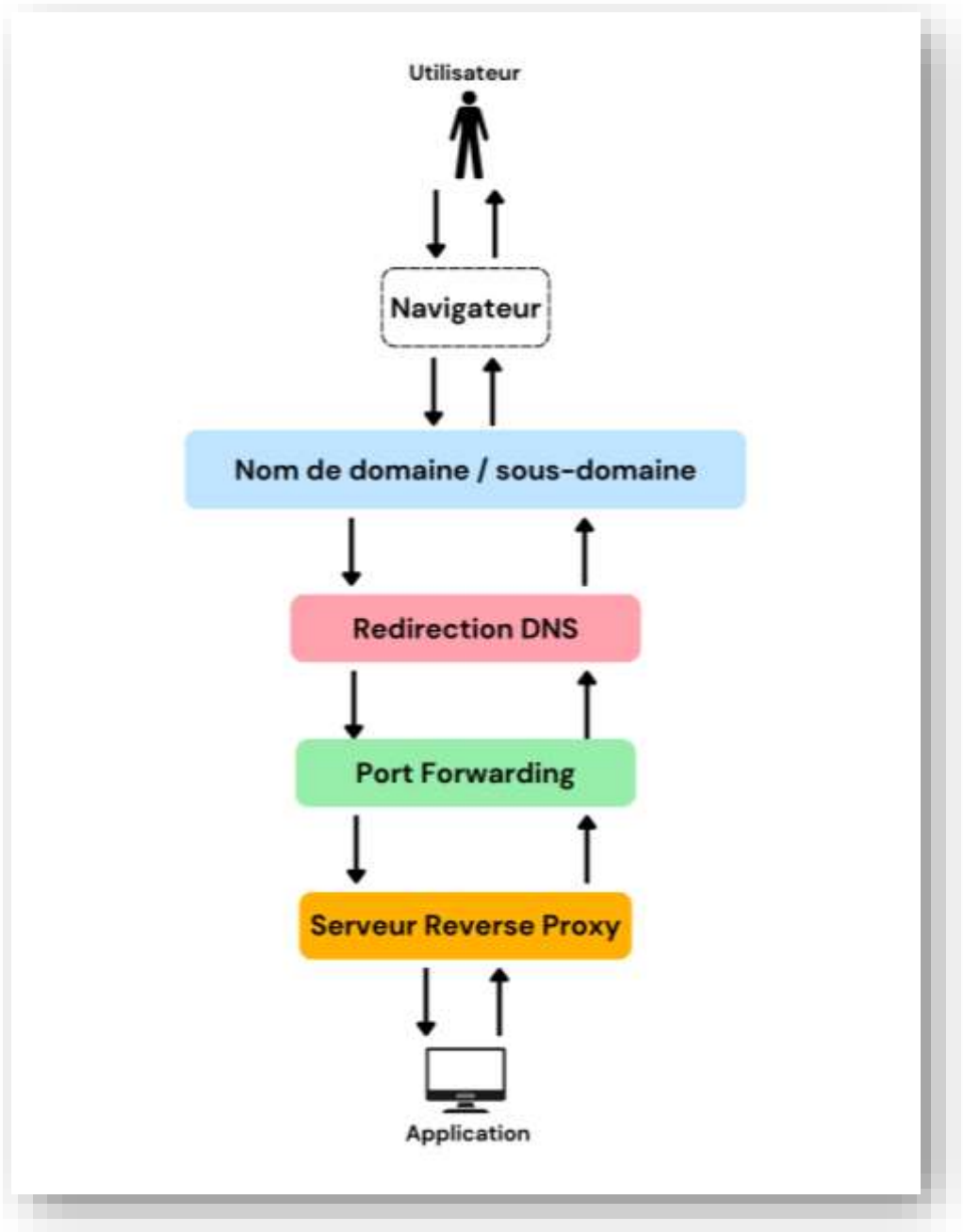
Secures communications, filters traffic, balances load, and improves application performance.

Using these technologies, remote access to the web-based ticket management application can be implemented efficiently and securely, offering a seamless and reliable user experience for employees and clients.

CHAPTER V : SYSTEM DESIGN

I. SYSTEM ARCHITECTURE

The combination of the main technologies we have chosen can be summarized as represented in Illustration 2 below:



➢ *Illustration 2: Architectural Diagram of the Remote Access Solution*

II. DEPLOYMENT PLAN DEVELOPMENT

1. Local Application Presentation

Before any network configuration, we will provide a detailed presentation of the existing local application, including its current functioning and configurations. This will ensure a complete understanding of the infrastructure before proceeding with remote deployment.

2. Creation of Domain Name and Subdomain

We will select a domain name provider and register our main domain name. Subsequently, we will create the necessary subdomain for remote access to our application.

3. DNS Redirection Configuration

Remote access requires DNS redirection configuration to direct user traffic to the public IP address of the local server. We will configure the DNS settings via our web host's administration interface to ensure correct DNS resolution.

4. Reverse Proxy Configuration

We will select and configure a suitable reverse proxy server. This step will involve installing and configuring the reverse proxy on a local server. We will ensure it is properly integrated into the existing infrastructure.

5. Port Forwarding Configuration

Accessing the application via the Internet will require port forwarding configuration on our router/firewall. We will set up port forwarding rules to redirect incoming HTTP/HTTPS traffic to the reverse proxy server.

6. SSL/TLS Certificates Installation

To ensure the security of communications, we will install SSL/TLS certificates on the reverse proxy server. This will enable data encryption and ensure server authenticity, thereby enhancing user trust in our application.

7. Access Control Lists (ACL) Configuration

We will implement access rules on the physical server hosting the reverse proxy to filter incoming traffic. This will add an extra layer of security by restricting access to the application only to authorized IP addresses.

8. Host Indexing

We will associate the domain/subdomain with the local application's IP address and port in the reverse proxy settings. This will ensure seamless communication between the application and remote users.

9. Testing and Verification

Once all configurations are completed, we will conduct thorough tests to verify remote access to the application. We will also assess the deployment's security by testing the security measures implemented. Any issues identified will be resolved before full production deployment.

III. RISK ASSESSMENT

1. Security Vulnerabilities

- **Impact:** High
- **Probability:** High
- **Mitigation:** Implement robust security measures, regular security audits, and user education on security practices.

2. Server Downtime

- **Impact:** Medium to High
- **Probability:** Medium
- **Mitigation:** Regular maintenance, backup power supplies, and failover mechanisms.

3. Internet Connectivity Issues

- **Impact:** Medium to High
- **Probability:** Medium
- **Mitigation:** Ensure multiple ISPs, backup internet connections, and monitor connectivity.

4. Configuration Errors

- **Impact:** Medium
- **Probability:** Medium
- **Mitigation:** Comprehensive testing, configuration backups, and change management processes.

5. DDoS Attacks

- **Impact:** Medium to High
- **Probability:** Low to Medium
- **Mitigation:** Implement DDoS protection services, rate limiting, and regular security updates.

PART III: SYSTEM IMPLEMENTATION

In this part, we will present the arrangement of the various components that allowed us to arrive at a functional solution that meets the specified needs.

CHAPTER VI : TECHNOLOGY IMPLEMENTATION

I. PRESENTATION OF THE LOCAL APPLICATION

The ticket management application we want to make accessible on the internet, which is already running locally, is "OsTicket," as mentioned earlier. OsTicket is an open-source ticketing system software that allows managing customer support requests. It is widely used by companies to efficiently manage their customer service.

1. Functioning of the Existing Application

The digital service team at DCAT has customized OsTicket to include the features necessary for the company to manage intervention tickets. The software now offers functionalities such as ticket creation and tracking, queue management, custom ticket forms, user and group management, etc. Following the customization by the digital service team, our OsTicket is now named "HELPDESK DCAT."

2. Current Configurations

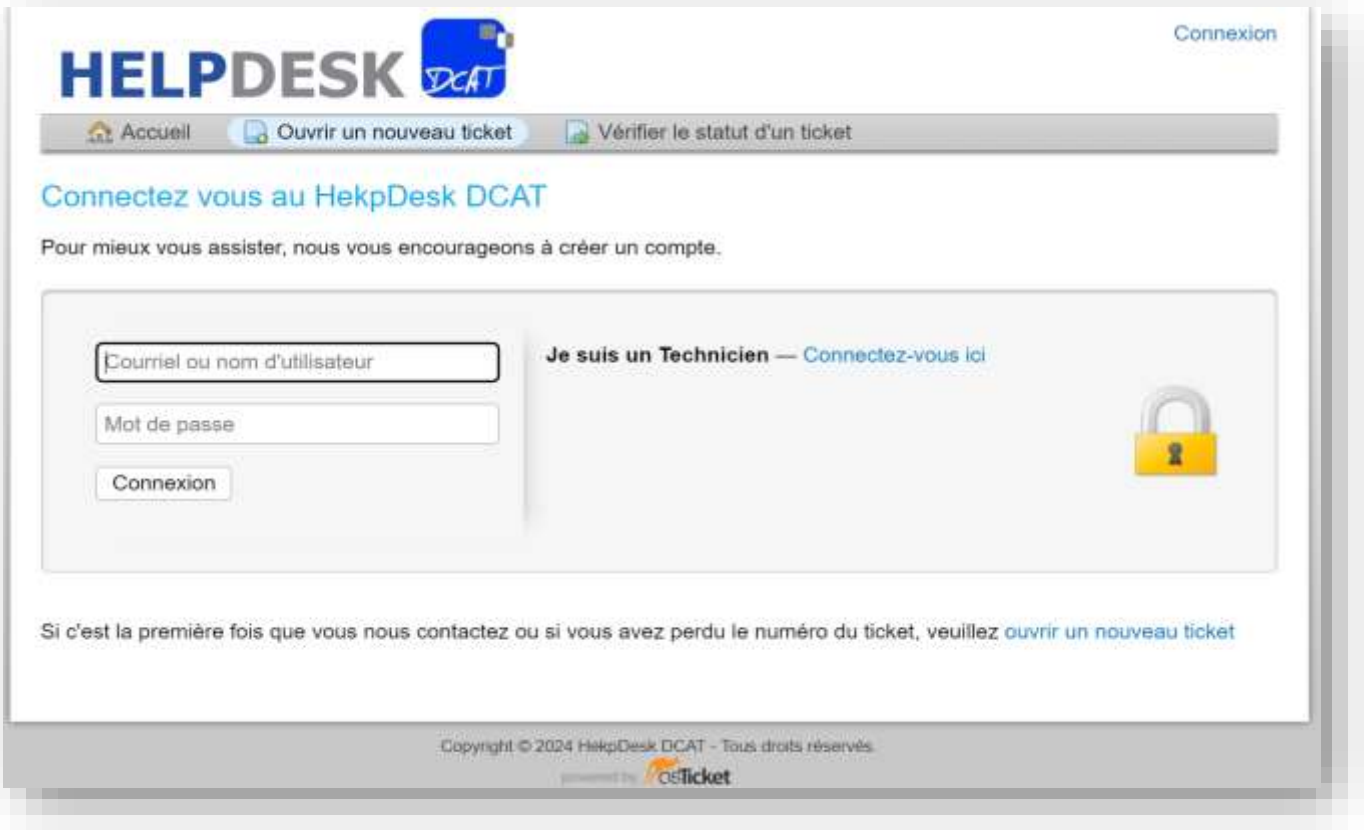
OsTicket operates on a **Ubuntu server** with **Apache 2**, **PHP 8.2**, **MySQL 8.0**, and **Composer**.

3. Application Interfaces

- **Technician Login Interface**: Technicians log in to manage tickets.

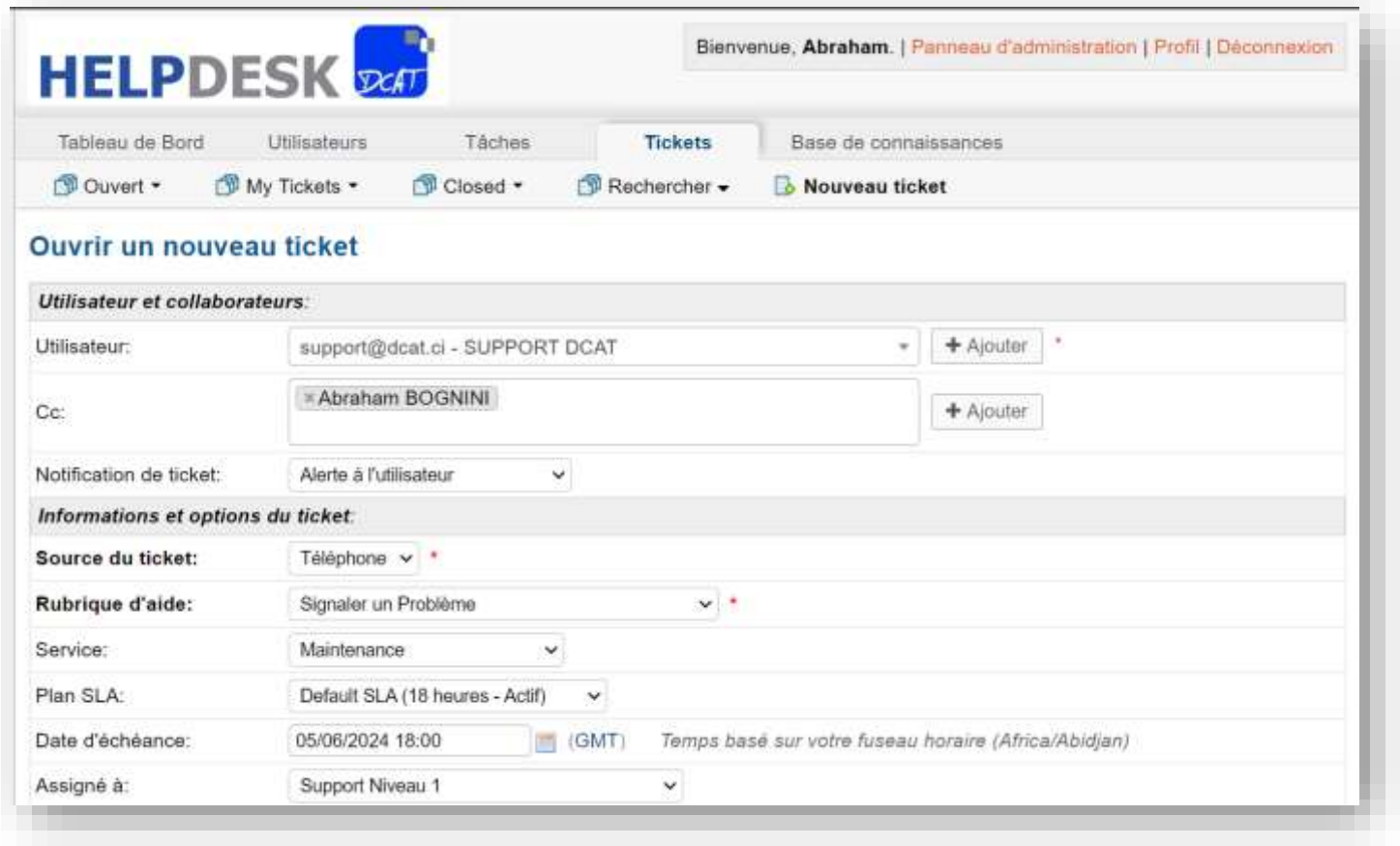
➢ *Illustration 3: Technician Login Interface*

- **Client Login Interface**: Allows clients to log in to the web application to access their accounts, submit tickets, track progress, and communicate with technicians.



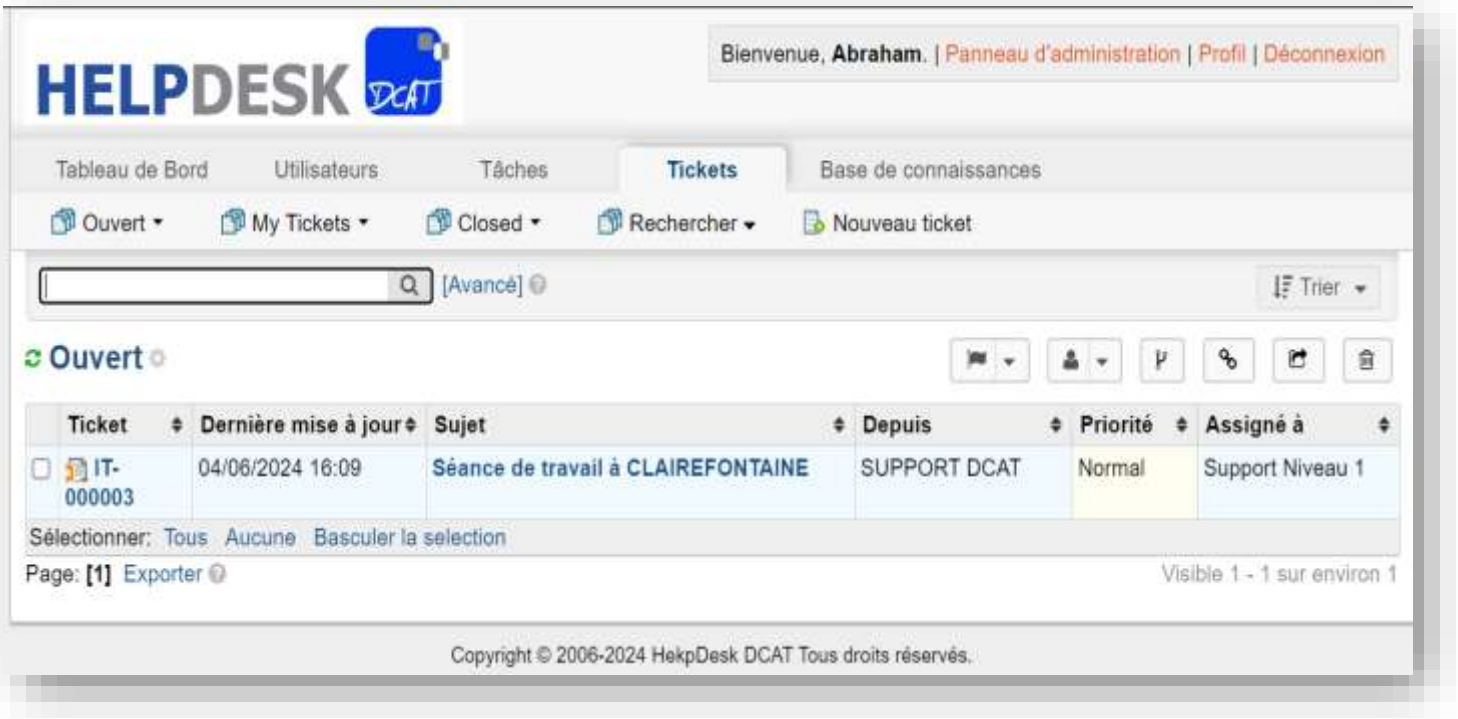
➢ *Illustration 4: Client Login Interface*

- **Ticket Creation Interface**: Allows both technicians and clients to create new intervention tickets. Users can detail issues, attach files, and set ticket priorities, facilitating communication and incident management.



➢ *Illustration 5: Ticket Creation Interface*

- **Dashboard or Open Tickets List (Technician)**: Provides technicians with an overview of ongoing tickets, displaying key information such as deadlines, priorities, and incident details for effective and quick intervention management.



➢ *Illustration 6 : Open Tickets Dashboard*

II. TECHNOLOGY CONFIGURATION

1. Domain Name and Subdomain

We selected the main domain name "**dcat-support.com**" for our ticket management application. For remote access, we created the subdomain "**helpdesk.dcat-support.com**".

2. DNS Redirection

DNS redirection was configured to direct traffic from the subdomain "**helpdesk.dcat-support.com**" to the public IP address of our local server hosting the "HELPDESK DCAT" application.

3. Port Forwarding

Port forwarding rules were established on our router to redirect incoming HTTP/HTTPS traffic to the local server on the appropriate ports (typically 80 for HTTP and 443 for HTTPS).

4. Reverse Proxy Server

We deployed a reverse proxy server (**Nginx**) on our local server to handle incoming requests to our "HELPDESK DCAT" application. The reverse proxy also secures communications via SSL/TLS.

III. TESTING AND VERIFICATION

We conducted thorough testing to verify the proper functioning of remote access to our "HELPDESK DCAT" application. We tested access to the technician login interface and the client user interface using the subdomain "**helpdesk.dcat-support.com**".

We also verified the security of the deployment by testing the SSL/TLS certificates installed on the reverse proxy server and evaluating additional security measures such as Access Control Lists (ACLs).

IV. USER TRAINING AND SUPPORT

1. Staff Training

- Inform staff about the availability of "HELPDESK DCAT" online.
- Explain how to connect to the platform using different devices.
- Organize practical training sessions to familiarize staff with the features and interface.

2. Client Training

- Inform clients about the existence of "HELPDESK DCAT".
- Guide clients on how to connect to the platform and use their devices to access it.
- Explain how to request and track technical interventions through this platform.

3. User Support

- Stay responsive to staff and clients to resolve access or usage issues.
- Establish a technical support system to answer questions and resolve issues quickly and efficiently.
- Collect user feedback to continuously improve the remote access experience and application functionality.

4. Training Support Documentation

This training document explains the basics of using "HELPDESK DCAT" for DCAT's technical staff and clients.

- **Accessing the Home Interface**:
  - Open a web browser and enter the subdomain "helpdesk.dcat.ci" in the address bar.
  - The "HELPDESK DCAT" home page will be displayed.
- **Logging into "HELPDESK DCAT":**
  - Log in using the available options for clients or technicians.
  - Enter the authentication information provided by the administrator. If not received, contact the administrator.
- **Using "HELPDESK DCAT" Features:**
  - Create and track intervention tickets through the corresponding interface.
  - Explore "HELPDESK DCAT" following the instructions.
  - For any assistance, contact the administrator.

CHAPTER VII : PROJECT IMPLEMENTATION SUMMARY

I. PROJECT PROGRESS

1. Achieved Objectives

- **Needs Analysis**: We conducted surveys with employees and clients to understand their specific needs for remote access to the ticket management application.
- **Design of a Secure Architecture**: We designed a secure architecture that includes a reverse proxy server, a subdomain name, DNS configuration, and appropriate port forwarding.
- **Component Setup**: We successfully installed the reverse proxy server, set up port forwarding rules, and installed SSL certificates.
- **Solution Testing**: We performed thorough tests to verify the functionality and security of the solution.
- **User Training**: Training materials were created, and training sessions were organized for staff and clients to familiarize them with the new solution.
- **Maintenance and Monitoring**: We established a maintenance plan to ensure regular updates and continuous monitoring of the solution.

2. Problems Encountered and Solutions

- **Lack of Technical Knowledge**: We used self-study resources (online tutorials, forums, technical documentation) to fill in the gaps in technical skills.
- **Paid Technologies**: To stay within budget, we searched for and used free alternatives to paid technologies.

II. FINANCIAL SUMMARY OF THE PROJECT IMPLEMENTATION

1. Initial Costs (CAPEX)

- **Equipment Purchase Costs**: About 3,350,000 FCFA were spent on acquiring the necessary equipment.
- **Software and License Costs**: 0 FCFA, thanks to the use of free and open-source software.
- **Staff Training Costs**: About 20,000 FCFA for organizing training sessions.

2. Operating Costs (OPEX)

- **Maintenance and Technical Support Costs**: About 175,000 FCFA for regular maintenance and technical support.
- **Hosting and Bandwidth Costs**: About 350,000 FCFA for the necessary hosting and bandwidth to ensure the application's availability.
- **Security Costs**: About 150,000 FCFA for additional security measures such as SSL/TLS certificates and security monitoring solutions.

3. Financial Conclusion

CLASSIFICATION	CATEGORY	R.A.Z AMOUNT	DCAT AMOUNT
Initial Costs (CAPEX)	Equipment Purchase Costs	3 350 000 CFA	0 CFA
	Software and License Costs	0 CFA	0 CFA
	Staff Training Costs	20 000 CFA	20 000 CFA
	TOTAL CAPEX	**3 370 000 CFA**	**20 000 CFA**
Operating Costs (OPEX)	Maintenance and Technical Support Costs	175 000 CFA	0 CFA
	Hosting and Bandwidth Costs	350 000 CFA	0 CFA
	Security Costs	150 000 CFA	0 CFA
	TOTAL OPEX	**675 000 CFA**	**0 CFA**
CAPEX + OPEX	**TOTAL**	**4 045 000 CFA**	**20 000 CFA**

➢ *Table 1: Financial Summary of the Project Implementation*

We noticed that several theoretical costs (R.A.Z amounts) were offset at DCAT. This is because the company had already incurred these expenses in previous projects. Therefore, these expenses cannot be attributed to our remote access project.

We successfully managed to execute this project, costing the company only 20,000 FCFA instead of over 4,000,000 FCFA by primarily using resources already available at DCAT. This allowed us to save more than 4,000,000 FCFA and, even better, it enabled us to make DCAT's investments profitable by using them to potentially generate revenue for the company or add value to its services.

PART IV: INTERNSHIP SUMMARY

This section provides a summary of the activities carried out during the internship, the skills acquired, and our suggestions for the host company.

CHAPTER VIII : INTERNSHIP PROGRESS

1. ACTIVITIES UNDERTAKEN

1. Successful Completion of Final Project

- **Description**: Implementation of a remote access solution for technical intervention ticket management at DCAT.
- **Result**: The solution is operational, enabling technicians and clients to manage tickets online efficiently and securely.
- **Impact**: Significant improvement in technical intervention management, optimizing response times and client satisfaction.

2. Participation in Internal Projects

- **Description**: Collaboration on various internal projects at DCAT, including stock, financial, and administrative management.
- **Result**: Successful deployment of these systems, improving internal organization and tracking within the company.
- **Impact**: Contribution to operational efficiency and streamlining of internal processes.

3. Participation in External Projects on Sites

- **Description**: Involvement in technical missions at DCAT's clients' sites, such as networking workstations in a radio studio.
- **Result**: Successful completion of client projects, meeting their specific needs and enhancing their technical infrastructure.
- **Impact**: Demonstration of the team's ability to satisfy clients and provide reliable technical solutions.

4. Participation in Audiovisual Training (MAirList)

- **Description**: Attended training on using the MAirList software suite for computerized radio program management.
- **Result**: Acquisition of knowledge on MAirList, enabling efficient management of radio programs and broadcasts.
- **Impact**: Contribution to DCAT's audiovisual projects, adding value to the company's services.

II. ACQUIRED SKILLS

1. Technical Skills

- Project management
- Network administration
- Deployment of web solutions
- Technical support
- Basics of containerization
- Basic accounting

2. Personal Skills

- Communication
- Teamwork
- Time management
- Adaptability

III. SUGGESTIONS TO THE COMPANY

1. Enhance Investments

Increase investments in hosting and remote access for other web applications under development.

2. Involve Staff More

Raise awareness among staff about security best practices and the technologies being used.

3. Improve Availability and Security

Invest in robust infrastructure and advanced technologies to enhance service availability and security.

4. Become a Leading Local Host

Focus on optimizing performance, security, and reliability of solutions to become a leading local host.

CONCLUSION

We have successfully addressed the initial challenge of enabling secure remote access to DCAT's technical intervention ticket management application. Our goal was to meet connectivity and security needs while ensuring optimal use of the HELPDESK DCAT web application.

By following a rigorous methodology, we began with a detailed needs analysis, selecting suitable technologies such as Nginx Proxy Manager for the reverse proxy. Configuring security rules, implementing SSL/TLS certificates, and optimizing port forwarding were crucial for the security and efficiency of the remote access system. We also trained and supported users to facilitate the adoption of the new solution.

The project has been a success, achieving all set objectives. The application is now accessible remotely over the internet, secured, and usable by employees and clients. We overcame challenges through a proactive approach and continuous adaptation to technical hurdles. For the future, we recommend enhancing investments and staff involvement in hosting and remote access for DCAT's web applications, paving the way for ongoing improvements and better efficiency of IT systems.

BIBLIOGRAPHY

Theses and Reports

- ***DIALLO Azise Oumar, TALL Hamadoun***, (2019). "Study and Implementation of a Secure IT Network at the Day Hospital of the Sanou Souro University Hospital Center in Bobo-Dioulasso". Final thesis, Bobo-Dioulasso, UPB: School of Computer Science, 2009-2010, 75 pages;

- ***OUEDRAOGO Souleymane***, "Implementation of an Automatic Audio Backup Solution for a Radio Station: Case of AL HIKMAH Radio". Final thesis, Yamoussoukro, INP-HB: ESI, 2018-2019, 64 pages;

- ***Ezan TAHI***, "Design of APIs for a School Management Application". Final thesis, Yamoussoukro, INP-HB: ESI, 2021-2022, 64 pages;

- ***KOMBO Madou Hope Othniel***, "Design and Implementation of a Payment Management Application: Case of Saint-Joseph Church". Final thesis, Yamoussoukro, INP-HB: ESI, 2022-2023, 127 pages;

WEBOGRAPHY

- https://www.youtube.com/watch?v=QxH9DNWY4yo | importer conteneur sur mon Synology | accessed on 24/05/2024 at 17:14
- https://www.youtube.com/watch?v=QxH9DNWY4yo | Docker avec Synology: Container Manager | accessed on 24/05/2024 at 15:34
- https://www.docker.com | Documentation Docker | accessed on 24/05/2024 at 10:32
- https://www.proxmox.com/en | Documentation Proxmox | accessed on 19/05/2024 at 11:13
- https://www.youtube.com/watch?v=Bw4akxSfnCM | Proxmox à moindre coût: J'installe un serveur Puissant pour 40 EUR | accessed on 19/05/2024 at 10:42
- https://www.youtube.com/watch?v=okm29mVf0nM | Formation Docker - Les bases en moins de 20 minutes | accessed on 18/05/2024 at 17:22
- https://www.youtube.com/watch?v=4LyyLURi544 | Installer Nginx Proxy Manager - Exposer vos services | accessed on 10/05/2024 at 14:57
- https://www.youtube.com/results?search_query=nginx+proxy+manager | Nginx proxy manager | accessed on 10/05/2024 at 14:12
- https://www.youtube.com/watch?v=IDD2K7qmYhw&list=PPSV | Les Tutos - Proxmox No 1 : Installation, configuration, création stockage et VM - (CE*) | accessed on 09/05/2024 at 22:12
- https://nginxproxymanager.com | Documentation Nginx Proxy Manager | accessed on 08/05/2024 at 16:43

TABLE OF CONTENTS