

REPUBLIQUE TOGOLAISE

-----  
Travail-Liberté-Patrie

MINISTRE DE LA PLANIFICATION, DU  
DEVELOPPEMENT ET DE LA  
COOPERATION



Institut Africain d'Informatique-  
Représentation du Togo (IAI-TOGO)

**E-mail :** [iaitogo@iai-togo.tg](mailto:iaitogo@iai-togo.tg)

**Site Web:** [www.iai-togo.tg](http://www.iai-togo.tg)

**Tél :** (+228) 22 20 47 00

07 BP 12456 Lomé 07, TOGO



Bureau de Conseils-Etude et Contrôle  
en Ingénierie

**E-mail :** [Groupe\\_ie@hotmail.com](mailto:Groupe_ie@hotmail.com)

**Tél :** (+228) 98 93 89 18 / 91 54 85 49

**Site web :** [ingenieursetexperts.wixsite.com](http://ingenieursetexperts.wixsite.com)

Maison 15, 128 Rue Cocoteraie Quartier Totsi  
BP 4794 Lomé-TOGO

**PROJET DE FIN DE FORMATION POUR L'OBTENTION DU DIPLOME DE LICENCE  
PROFESSIONNELLE EN INFORMATIQUE  
OPTION :  
ADMINISTRATION DES SYSTEMES ET RESEAUX**

**SECURISATION D'UN SYSTEME DE STOCKAGE NAS : LES  
ENVIRONNEMENTS JAILS (TRUENAS CORE)**

Période : du 28 Juin au 18 Septembre 2021

Rédigé et présenté par :

**AKAKPO Amandine Laura**

Etudiante en troisième année

Année Académique : 2020 - 2021

SUPERVISEUR

**Mme D'ALMEIDA Yvonne**

Enseignante à l'IAI-TOGO

MAITRE DE STAGE :

**M. KOSSI-TITRIKOU Marc-Olivier**  
Responsable Adjoint du département  
informatique

## DEDICACES

Je dédie ce mémoire

**A mes parents AKAKPO Komivi Laurent et FOLLIGAN Kayissan Mireille,**  
qui m'ont toujours soutenu durant mon parcours de trois ans à l'IAI-TOGO et qui  
m'ont fourni de bonnes conditions de travail afin de pouvoir réussir.

**A mon frère Cédric AKAKPO et à ma sœur Carine AKAKPO,**  
pour leur compréhension face à certaines situations. Je leur en suis très  
reconnaissante et je remercie beaucoup mon Dieu de m'avoir donné des parents si  
compréhensifs.

## REMERCIEMENTS

J'adresse mes sincères remerciements à :

- ❖ **M. AGBETI Kodjo**, Directeur Général du CENETI, Représentant Résident de l'IAI-TOGO, pour toutes les dispositions qu'il a prises afin de fournir de bonnes conditions de travail à nous ses étudiants et pour améliorer nos compétences et favoriser notre réussite ;
- ❖ **M. AMEYIKPO Kossi**, Directeur des Affaires Académiques et de la Scolarité à l'IAI-TOGO, pour son accueil, ses conseils, son soutien et son écoute.
- ❖ **M. DAVON Essè**, enseignant à IAI-TOGO pour son soutien et sa compréhension ;
- ❖ Tous les membres du département informatique de l'IE (Ingénieurs et Experts) pour leur accueil et leur convivialité ;
- ❖ **Mme D'ALMEIDA Yvonne** ma superviseure, pour sa disponibilité, son calme et sa compréhension ;
- ❖ **M. KOSSI-TITRIKOU Elom Marc-Olivier**, mon maître de stage pour son accueil, son aide et sa disponibilité malgré ses journées très chargées ;
- ❖ *Le corps professoral et l'administration de l'IAI-TOGO* pour leurs efforts afin de nous dispenser une bonne formation et leur patience.

Je vous en suis très reconnaissante. Et que DIEU vous le rende au centuple !!

## AVANT-PROPOS

L'Institut Africain d'Informatique (IAI) est une institution régionale, ouverte le 29 Janvier 1971 à Fort - Lamy actuelle N'Djamena, capitale de la République du Tchad, par onze (11) pays à savoir le Bénin, le Burkina Faso, le Cameroun, la Côte d'Ivoire, la Centrafrique, la République du Congo, le Gabon, le Niger, le Sénégal, le Tchad et le Togo. Son siège se trouve à Libreville au Gabon. L'IAI forme des ingénieurs informaticiens à Libreville et des ingénieurs des travaux informatiques dans ses représentations.

L'IAI-TOGO, ouvert depuis 2002 prodigue une formation de trois (3) ans en deux parcours : Ingénieurs des Travaux Informatiques et Licence Professionnelle dans trois filières : Génie Logiciel et Système d'informations (GLSI), Administration des Systèmes & Réseaux (ASR) et Multimédia, Technologies Web et Infographie (M-TWI). Il intègre à la fin de cette formation de trois ans, un stage de trois (03) mois en entreprise pour l'obtention du Diplôme d'Ingénieur des Travaux Informatiques ou de la Licence Professionnelle en Informatique.

Ainsi, afin d'obtenir notre diplôme de Licence Professionnelle en Informatique nous avons bénéficié d'un stage d'une durée de trois (03) mois au sein du groupe INGENIEURS & EXPERTS.

# SOMMAIRE

	Pages
DEDICACES .....	i
REMERCIEMENTS .....	ii
AVANT-PROPOS .....	iii
SOMMAIRE .....	iv
RESUME .....	v
GLOSSAIRE .....	vi
LISTE DES FIGURES .....	vii
LISTE DES TABLEAUX .....	ix
LISTE DES PARTICIPANTS AU PROJET .....	x
INTRODUCTION GENERALE .....	1
PARTIE I : PRESENTATIONS .....	2
1.1 PRESENTATION DE L'IAI-TOGO .....	3
1.2 PRESENTATION DU GROUPE INGENIEURS & EXPERTS .....	6
PARTIE II : ETUDE ET REALISATION DU PROJET .....	9
Chapitre 1 : Contexte de travail et approches de solutions .....	10
Chapitre 2 : Généralités et documentations .....	16
Chapitre 3 : Mise en œuvre et perspectives .....	28
PARTIE III : GUIDE D'UTILISATION .....	56
CONCLUSION .....	63
BIBLIOGRAPHIE INDICATIVE .....	64
WEBOGRAPHIE INDICATIVE .....	65
TABLE DES MATIERES .....	67

## RESUME

Dans la perspective d'obtenir notre diplôme de Licence Professionnelle en Informatique, nous avons été amenée à effectuer un stage de trois (03) mois dans la structure de l'IE (Ingénieurs et Experts). Il nous a alors été soumis le thème « **sécurisation d'un système de stockage NAS : les environnements jails (TrueNAS CORE)** ».

La mise en place d'un système de sécurisation permettra la protection des données ainsi que du système. Ainsi malgré les attaques extérieures du système, les données et le système de stockage seront sains et saufs sans aucune modification. Afin de pouvoir réaliser ce projet, nous dégagerons tout d'abord une problématique, proposer des approches de solutions ainsi que la méthodologie à suivre afin de déterminer la meilleure solution, présenter la solution retenue et implémentée et enfin présenter les résultats obtenus. Ainsi, après étude et analyse, nous avons configuré les environnements jails de TrueNAS CORE sur ce système de stockage afin de le sécuriser en interne, mis en place le pare le pare feu Zentyal pour la sécurisation des trafics entrants et sortants et ensuite configurer le vpn OpenVPN pour la sécurisation de l'accès à distance (de l'extérieur vers l'intérieur) au système de stockage.

# GLOSSAIRE

*Tableau 1: Glossaire des abréviations et acronymes*

SIGLE	DEFINITION
<b>A2F</b>	<b>Authentification à 2 Facteurs</b>
<b>BSD</b>	<b>Berkeley Software Distribution</b>
<b>DHCP</b>	<b>Dynamic Host Configuration Protocol</b>
<b>HTTPS</b>	<b>HyperText Transfer Protocol Secure</b>
<b>IP</b>	<b>Internet Protocol</b>
<b>NAS</b>	<b>Network Attached Storage</b>
<b>SSL</b>	<b>Secure Socket Layer</b>
<b>Wi-Fi</b>	<b>Wireless Fidelity</b>
<b>WLAN</b>	<b>Wireless Local Area Network</b>

## LISTE DES FIGURES

	Pages
Figure 1: Organigramme de l'IAI-TOGO .....	5
Figure 2: Plan de localisation de l'IAI-TOGO .....	6
Figure 3: Organigramme d'INGENIEURS & EXPERTS.....	7
Figure 4: Plan de localisation de l'IE .....	8
Figure 5: Illustration de l'architecture simplifiée du réseau d'INGENIEURS & EXPERTS.....	12
Figure 6: Logo de TrueNAS CORE [22].....	17
Figure 7: Illustration d'un pare-feu dans un réseau [21].....	21
Figure 8: Logo de Pfsense [23].....	22
Figure 9: Logo de Zentyal [24] .....	23
Figure 10: Illustration de l'utilisation d'un vpn d'un réseau public distant vers un réseau local [25] .....	25
Figure 11: Logo d'OpenVPN [3].....	26
Figure 12: Logo de VMware Workstation [26].....	30
Figure 13: Démarrage de la machine virtuelle TrueNAS .....	32
Figure 14: Démarrage de la configuration en ligne de commande .....	33
Figure 15: Fin de la configuration .....	33
Figure 16: Interface de TrueNAS en ligne de commande.....	34
Figure 17: Interface web de TrueNAS CORE .....	35
Figure 18: Configuration du réseau de TrueNAS.....	36
Figure 19: Création d'un compte utilisateur .....	37
Figure 20: Création du groupe informatique .....	37
Figure 21: Attribution du groupe informatique à l'utilisateur marc .....	38
Figure 22: Création du pool IE_pool1 .....	39
Figure 23: Création du dataset public.....	40
Figure 24: Définitions des différentes autorisations au dataset public .....	41
Figure 25: Activation du service samba SMB .....	42
Figure 26: Création du partage samba au dataset public .....	42
Figure 27: Création du certificat d'autorité de certification racine .....	43
Figure 28: Création d'un certificat d'authentification OpenVPN .....	44



Figure 29: Configuration du service OpenVPN Server .....	45
Figure 30: Activation du service OpenVPN Server .....	45
Figure 31: Création du certificat de connexion au client OpenVPN .....	46
Figure 32: Choix du certificat client.....	47
Figure 33: Installation de Zentyal.....	48
Figure 34: Interface de Zentyal.....	49
Figure 35: Installation du plugin Nextcloud.....	49
Figure 36: Configuration du plugin Nextcloud.....	50
Figure 37: Fin de l'installation du plugin Nextcloud.....	50
Figure 38: Interface de connexion de Nextcloud .....	51
Figure 39: Connexion au Nextcloud .....	52
Figure 40: Connexion au VPN avec un compte utilisateur.....	53
Figure 41: Illustration d'une connexion établie [3].....	53
Figure 42: Proposition de la nouvelle architecture réseau d'IE.....	55
Figure 43: Interface de connexion de l'administrateur .....	58
Figure 44: Création d'un utilisateur .....	58
Figure 45: Procédure d'administration pour les utilisateurs Nextcloud .....	59
Figure 46: Interface de connexion de l'employé .....	59
Figure 47: Tableau de bord de connexion de l'utilisateur [3] .....	60
Figure 48: Interface de connexion d'OpenVPN.....	60
Figure 49: Interface d'OpenVPN après authentification de l'employé .....	61
Figure 50: Page d'authentification de Nextcloud.....	62
Figure 51: Page d'accueil de Nextcloud .....	62

## LISTE DES TABLEAUX

	Pages
Tableau 1: Glossaire des abréviations et acronymes .....	vi
Tableau 2: Tableau de la liste des participants.....	x
Tableau 3: Tableau de comparaison des outils de sécurisation .....	20
Tableau 4: Tableau comparatif des technologies de pare-feu étudiées .....	24
Tableau 5: Tableau comparatif des technologies VPN .....	27
Tableau 6: Politique de sécurité d'accès aux serveurs à l'IE .....	31
Tableau 7: Tableau des coûts liés à la mise en place de la solution .....	54

## LISTE DES PARTICIPANTS AU PROJET

*Tableau 2: Tableau de la liste des participants*

Nom et Prénom(s)	Fonctions	Rôle
<b>AKAKPO Amandine Laura</b>	Etudiante en troisième année Option Administration des Systèmes et Réseaux à l'IAI-TOGO	Réalisatrice
<b>Mme D'ALMEIDA Yvonne</b>	Enseignante à IAI-TOGO	Superviseure
<b>M. KOSSI-TITRIKOU Elom Marc-Olivier</b>	Responsable adjoint du département informatique du groupe Ingénieurs & Experts	Maître de stage

# INTRODUCTION GENERALE

De nos jours, nombreuses sont les entreprises qui ont fait des outils informatiques l'un des piliers de leur essor. Cependant, cette révolution technologique requiert une sécurité informatique adéquate et performante ainsi que des ressources nécessaires, afin de se protéger contre les cyber-attaques et le piratage des données qui ont accru ces derniers temps.

C'est dans cette logique que INGENIEURS & EXPERTS – le groupe dans lequel nous avons effectué notre stage – s'est doté, pour sa part, d'un système de stockage dénommé TrueNAS ; ledit système requiert, toutefois, l'implémentation de solutions de sécurisation adéquates, puisque toutes les données sont centralisées. C'est donc dans cette optique qu'il nous a été donné de travailler sur le thème : « **Sécurisation d'un système de stockage NAS à partir des environnements jails (TrueNAS)** ».

Dans ce document nous allons tout d'abord présenter l'IAI-Togo et le groupe INGENIEURS & EXPERTS, ensuite faire une étude de l'existant et de la problématique qui débouchera sur une phase de recherche et choix de solution, puis de la mise en œuvre de la solution.

## PARTIE I : PRESENTATIONS

## 1.1 PRESENTATION DE L'IAI-TOGO

### 1.1.1 Historique de l'IAI-TOGO

L'Institut Africain d'Informatique Représentation du TOGO, a vu le jour le 22 Octobre 2002. L'IAI-TOGO est membre du réseau IAI (Institut Africain d'Informatique) créé le 29 janvier 1971 à Fort Lamy (actuel N'Djamena) en République Démocratique du Tchad sous l'initiative des chefs d'Etats de l'ancienne Organisation Commune Africaine, Malgache et Mauritanienne (OCAM). Le siège fut fixé à Libreville au Gabon. L'institut Africain d'Informatique est composé de 11 pays que sont : le Bénin, le Burkina-Faso, le Cameroun, le Congo, la Côte d'Ivoire, le Gabon, le Niger, la République Centrafricaine, le Sénégal, le Tchad et le Togo. Le TOGO est membre du conseil d'administration de l'IAI. Ainsi, depuis le 24 Octobre 2002, le Centre National d'Etudes et de Traitements Informatiques (C.E.N.E.T.I) héberge la représentation de l'IAI au Togo sous l'appellation d'IAI-TOGO. Il forme en trois ans des Ingénieurs des Travaux Informatiques et en Licence Professionnelle Informatique dans les filières suivantes : Génie Logiciel et Système d'Information (GLSI), Administration Systèmes et Réseaux (ASR) et MTWI (MultiMedia Technologie Web et Infographie).

### 1.1.2 Objectifs de l'IAI-TOGO

L'IAI-TOGO a pour objectifs :

- ❖ d'offrir un cadre de formation professionnelle ;
- ❖ d'offrir une formation de qualité aux étudiants ;
- ❖ de produire des Ingénieurs des Travaux Informatiques qualifiés et compétents en Licence Professionnelle Informatique.

### 1.1.3 Formations à l'IAI-TOGO

L'IAI-TOGO forme des Ingénieurs des travaux Informatiques et des diplômés en Licence Professionnelle Informatique sur une durée de trois (3) ans dans trois (3) filières : **Génie Logiciel et Système d'Information (GLSI), Administration Systèmes et Réseaux (ASR) et MTWI (MultiMedia Technologie Web et Infographie)**. Il propose également en parallèle une formation modulaire Cisco. Une certification est proposée à la fin de chaque module. Cette formation est destinée aux techniciens réseaux, revendeurs de produits Cisco et à toute personne désirant approfondir ses connaissances en réseau.

#### 1.1.4 Structure organisationnelle de l'IAI-TOGO

L'Institut Africain d'Informatique, représentation du Togo est doté d'une structure organisationnelle de type hiérarchique et comprend :

- ❖ La Direction Générale, à la tête de laquelle se trouve le Représentant Résident.  
Cette direction est composée de plusieurs cellules et services à savoir :
  - ✓ un secrétariat Central ;
  - ✓ un secrétariat Particulier ;
  - ✓ une cellule de Contrôle interne ;
  - ✓ une cellule Communication et Relations Extérieures ;
- ❖ la Direction des Affaires Académiques et de la Scolarité (DAAS) ;
- ❖ la Direction Administrative et Financière (DAF).

L'organigramme de l'IAI-TOGO est sur la Figure 1:

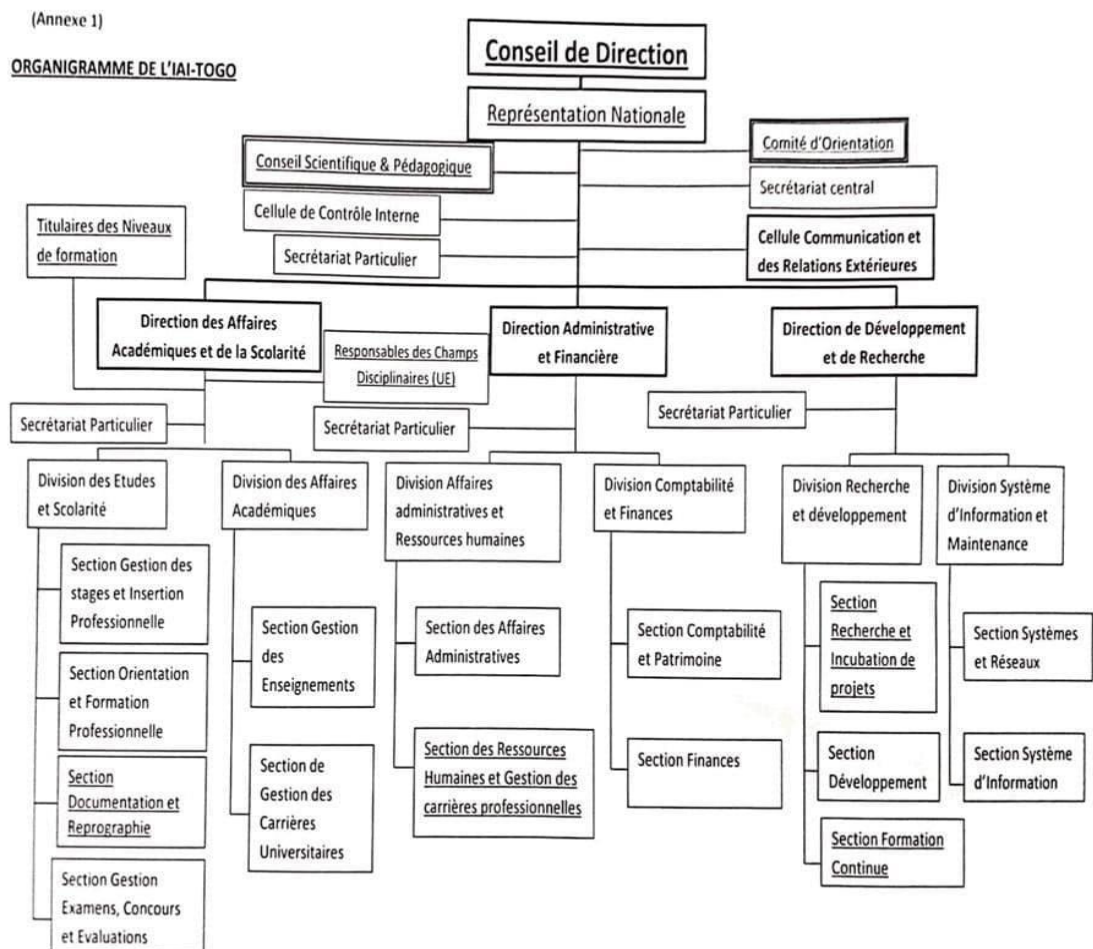


Figure 1: Organigramme de l'IAI-TOGO

### 1.1.5 Plan de localisation de l'IAI-TOGO

IAI-TOGO se situe à Lomé dans le quartier administratif sur la rue de la Kozah derrière l'immeuble de SUNU Assurance dans les locaux du Centre National d'Etudes et de Traitements Informatiques (C.E.N.E.T.I) non loin de la Communauté Electrique du Benin (CEB) comme l'indique le plan de localisation (figure 2) :



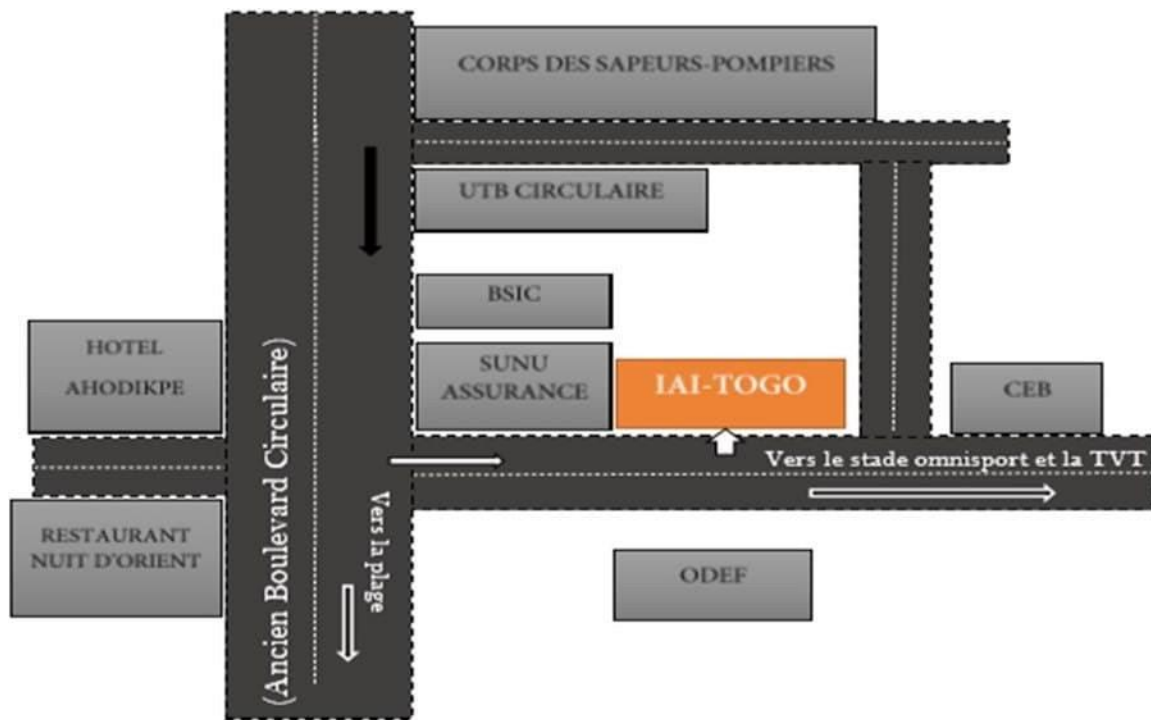


Figure 2: Plan de localisation de l'IAI-TOGO

## 1.2 PRESENTATION DU GROUPE INGENIEURS & EXPERTS

### 1.2.1 Statut

Le groupe INGENIEURS & EXPERTS est une structure regroupant des ingénieurs et des experts de divers domaines ayant pour objectif la recherche de solutions aux divers problèmes relevant de l'ingénierie soumis à leurs interventions.

Il est né de l'association de deux ingénieurs ayant décidé d'unir leurs compétences afin de fournir un service global dans le domaine de l'ingénierie sous toute ses formes. Il est créé le 01 février 2018 et intervient dans un premier temps dans le domaine de l'ingénierie Civil, l'architecture, l'ingénierie électrique et l'ingénierie informatique.

### 1.2.2 Missions

Le groupe propose dès lors des conseils, des propositions et des études techniques. En marge de cela, il prend en charge des besoins d'autres structures en assurant des services comme le suivi et le contrôle de qualité sur des travaux, les laboratoires et montages de dossiers d'appels d'offres, des entretiens d'embauches et spécialisés etc. Le groupe est implémenté à Lomé au TOGO.

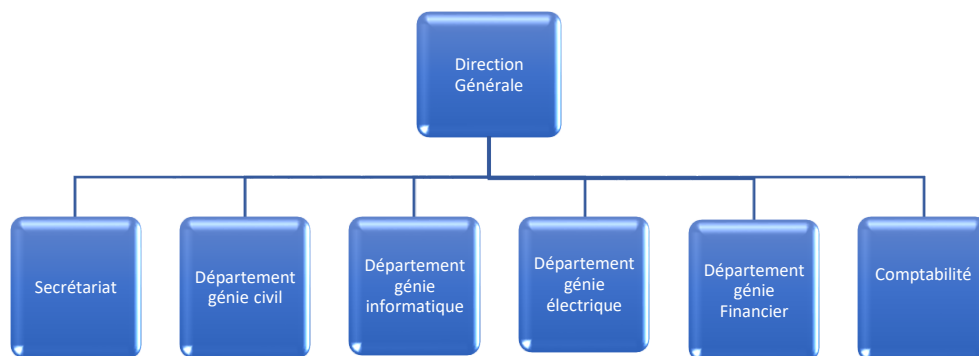
### 1.2.3 Activités

Le groupe INGENIEURS & EXPERTS intervient dans le domaine de l'ingénierie global. Les domaines touchés sont :

- ❖ L'ingénierie informatique ;
- ❖ L'ingénierie électrique ;
- ❖ L'ingénierie civile.

### 1.2.4 Organigramme

L'organigramme du groupe INGENIEURS & EXPERTS se présente comme suit :



*Figure 3: Organigramme d'INGENIEURS & EXPERTS*

### 1.2.5 Service d'accueil du groupe INGENIEURS & EXPERTS

Le lundi 28 juin 2021 à 08 h 00 nous avons débuté notre stage dans les locaux d'INGENIEURS ET EXPERTS. Nous étions au nombre de cinq stagiaires en Systèmes et Réseaux. Dès l'arrivée de notre maître de stage l'informaticien M. KOSSI-TITRIKOU Marc-Olivier, il nous présenta les locaux de notre lieu de stage. Quelques minutes plus tard, il nous communiqua les objectifs et les horaires de travail que nous devrions respecter tout au long de ces trois (03) mois. Dans l'après-midi nous avons discuté des thèmes de stages. Nous avons ensuite discuté des thèmes de stages à travailler. Leur gentillesse et leur accueil nous ont donné envie de donner le maximum de nous-même durant ce stage.

### 1.2.6 Plan de localisation

La figure 4 présente le plan de localisation du groupe INGENIEURS & EXPERTS :

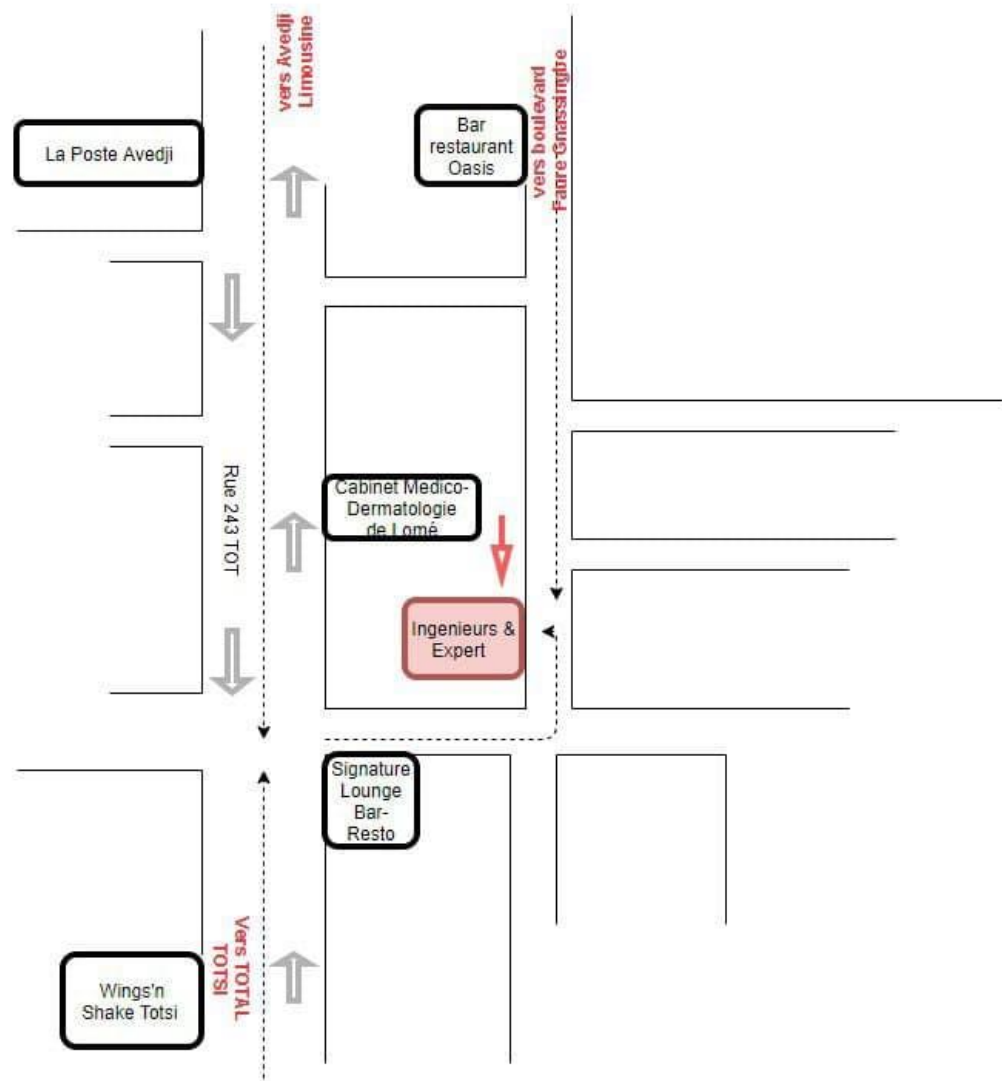


Figure 4: Plan de localisation de l'IE

## PARTIE II : ETUDE ET REALISATION DU PROJET

## **Chapitre 1 : Contexte de travail et approches de solutions**

## **INTRODUCTION**

Dans ce chapitre, nous allons faire l'étude des lieux en faisant une étude de l'existant puis une critique de cet existant afin d'en dégager une problématique et de suivre une méthodologie de recherche qui nous permettra d'opter à une solution plus fiable pour régler le problème trouvé.

### **1.1 Etude de l'existant**

Le groupe INGENIEURS & EXPERTS dispose d'une architecture système et d'une architecture réseau.

#### **1.1.1 Architecture système d'INGENIEURS & EXPERTS**

L'architecture système est un édifice fonctionnel composé d'équipements de transmission, de logiciels et protocoles de communication et d'une d'infrastructure filaire ou radioélectrique permettant la transmission des données entre les différents composants.

Un système d'information correspond à l'ensemble de moyens d'acquisition et de restitution, de traitement et de stockage de données dédié au traitement des informations. Il permet aux différents acteurs de véhiculer et de communiquer grâce à un ensemble de ressources matérielles, logicielles et humaines.

Les machines dont dispose le groupe INGENIEURS & EXPERTS sont essentiellement des ordinateurs portables HP et DELL fonctionnant sous Windows 10 édition professionnelle, famille et entreprise 64 bits et dotées d'un microprocesseur Intel® Core™ i3, i5 et i7. Afin de permettre à son personnel d'avoir accès à l'information, INGENIEURS & EXPERTS utilise des applications professionnelles de visioconférence modernes tels que : Google Meet, Zoom. Le groupe IE possède également un serveur de stockage TrueNAS sur lequel sont centralisées les données de l'entreprise.

#### **1.1.2 Architecture réseau d'INGENIEURS & EXPERTS**

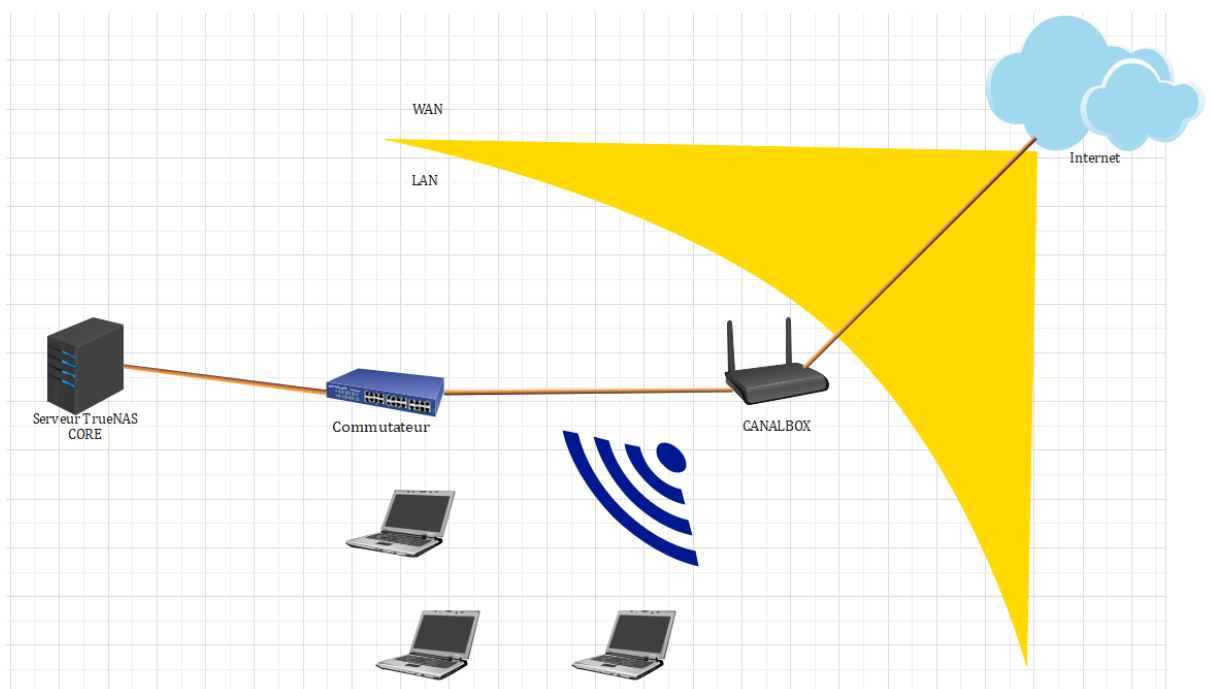
C'est quoi une architecture réseau ? Une architecture réseau concerne la structure de communication ainsi que le mode de fonctionnement des éléments constituant le réseau d'une organisation.

La structure IE ne dispose que d'un réseau WLAN utilisant la technologie wifi norme 802.11g. L'interconnexion de ses équipements se fait selon le mode infrastructure.

Ce mode est un réseau sans fil qui possède un point d'accès centralisé au cœur du réseau. Ainsi, dans le cas de l'IE les équipements communiquent entre eux et sont connectés à internet par le biais d'un modem routeur fibre optique CANALBOX qui est l'équipement central (point d'accès). Cet équipement permet au personnel de l'IE d'être toujours connecté à internet avec un débit de 10Mbit/s.

Les paramètres réseaux sont attribués dynamiquement aux machines via la fonction DHCP activée sur le modem CANALBOX. Les adresses IP sont attribuées suivant la plage d'adresse 192.168.1.51 à 192.168.1.253.

L'architecture réseau de l'IE se présente de manière très simple comme suit :



*Figure 5: Illustration de l'architecture simplifiée du réseau d'INGENIEURS & EXPERTS*

## 1.2 Critique de l'existant

### 1.2.1 Points forts

- ❖ Stockage : les données de l'IE sont sauvegardées sur un système de stockage NAS : TrueNAS CORE ;
- ❖ Accessibilité : l'infrastructure de l'IE offre une facilité d'accès aux données de l'entreprise car celles-ci sont centralisées ;
- ❖ Flexibilité : les ressources allouées peuvent être augmentées au besoin ;

- ❖ Sécurité : l'authentification de ce système est basée sur l'authentification à double facteur (A2F) qui consiste à ce que l'on indique un identifiant et un mot de passe ainsi qu'un code que l'on reçoit sur un autre appareil, généralement un smartphone afin de se connecter au NAS.

### 1.2.2 Points faibles

Cependant, l'utilisation de l'A2F présente un désavantage en ce qui concerne la disponibilité des données à tout moment. De plus, l'A2F n'est pas à l'épreuve des pirates malgré son efficacité. Par exemple, avec une cyberattaque par interception (man-in-the-middle) qui consiste à intercepter les communications entre deux parties ou lorsqu'un pirate nous incite à visiter son site web frauduleux et nous demande nos informations d'authentification A2F. Ainsi, cette sécurité n'est pas fiable et donc ne protège pas réellement l'entreprise pour ce qui en est de leur sécurité sur Internet et s'en découlent les problèmes suivants :

- ❖ les ressources informatiques sont exposées aux cyberattaques ;
- ❖ la politique de confidentialité des données mise en place n'est pas fiable ;
- ❖ l'accès à distance des données n'est pas sécurisé ;
- ❖ de plus, l'utilisateur ne peut pas avoir accès à distance aux données se trouvant sur le serveur NAS.

## 1.3 Problématique

Aujourd'hui, l'outil informatique est présent dans toutes les entreprises. Nous générons tous de plus en plus de données, certaines confidentielles ou stratégiques, d'autres peu importantes et négligeables. Et ces données informatiques figurent au cœur de nombreuses activités professionnelles. Cependant, le véritable défi pour ces entreprises est la sécurité de leurs données. Car le nombre d'attaques grandissant, il est nécessaire pour ces dernières de protéger leurs données et d'améliorer la sécurité de leur système d'information. Or après l'étude de l'architecture de l'IE, nous avons remarqué qu'elle présente certaines lacunes. Le système de stockage présente toujours des vulnérabilités et est empreint aux attaques de pirates car même avec l'utilisation de l'A2F, s'il arrivait par exemple que le smartphone soit mort ou volé, l'accès aux services serait impossible. Et cela occasionnerait :

- ❖ le vol des identifiants de connexion au serveur de stockage;



- ❖ l'impossibilité d'avoir accès aux données ;
- ❖ le réseau informatique de l'entreprise est exposé aux menaces et aux intrusions : l'entreprise devient une proie facile pour les cybers hackers.

Ainsi, découle à la vue de ces situations cette question suivante :

Quelle mise en place pouvons effectuer afin de rendre invulnérable le système de stockage NAS de l'IE et surtout d'avoir accès aux données peu importe l'endroit où l'on se trouve de manière sécurisée ?

C'est à cette question que notre projet répondra à travers la mise en place d'une solution de sécurisation du système de stockage NAS de l'IE.

## 1.4 Intérêt du sujet

### 1.4.1 Objectifs

Comme pour toute étude, des objectifs doivent être atteints pour prétendre avoir rempli la tâche donnée. Dans notre cas, les objectifs attendus sont de :

- ❖ renforcer encore plus la sécurité du NAS ;
- ❖ protéger les données du NAS contre les cyberattaques ;
- ❖ assurer l'intégrité des données ;
- ❖ accéder aux données en temps réel de façon sécurisée ;
- ❖ permettre l'accès à distance et sécurisé aux ressources du système de stockage NAS ;
- ❖ mettre en place un pare-feu pour sécuriser le système de stockage.

### 1.4.2 Résultats attendus

Les résultats espérés après la réalisation de ce projet sont les suivants :

- ❖ Les données du système de stockage NAS doivent être hors d'atteinte lors d'une cyberattaque ;
- ❖ les pirates ne doivent pas être en mesure de modifier les données du groupe IE;
- ❖ l'accès aux données est sécurisée.

## 1.5 Méthodologie de recherches de solutions

Afin de proposer une meilleure solution qui répondra au mieux aux attentes de l'IE, nous ferons :

- ❖ une recherche documentaire basée sur les généralités du serveur TrueNAS CORE ;
- ❖ une recherche documentaire sur les outils de sécurisation du système de TrueNAS CORE et choix de la solution adaptée ;
- ❖ une recherche documentaire sur la mise en place d'un pare-feu et choix de la solution adéquate ;
- ❖ une recherche documentaire sur la sécurisation de l'accès à distance et choix de la solution adaptée ;
- ❖ une synthèse des solutions retenues pour la mise en place de la sécurisation du système.

## **CONCLUSION**

Ce chapitre nous a permis d'avoir une idée sur l'état des lieux de notre structure de stage, de faire ressortir les différents manquements et d'établir une stratégie de recherche afin de trouver une solution adéquate au groupe INGENIEURS & EXPERTS. Nous aborderons à présent un deuxième chapitre « Généralités et documentation » qui parlera des différentes technologies et outils qui pourront permettre de mettre une sécurisation hautement qualifiée au système de stockage TrueNAS CORE du groupe INGENIEURS & EXPERTS.

## Chapitre 2 : Généralités et documentations

## **INTRODUCTION**

Dans ce second chapitre, nous allons tout d'abord faire une étude des différentes solutions existantes possibles permettant de sécuriser de manière plus efficace le serveur NAS, de faire ensuite une synthèse des différentes solutions étudiées et enfin de faire une présentation de la solution retenue.

### **2.1 Généralités sur TrueNAS CORE**

TrueNAS est un système d'exploitation sous licence BSD basé sur FreeBSD qui offre une solution de stockage et de partage de fichiers. Il est une alternative à ceux qui souhaitent implémenter leur propre serveur de stockage sans avoir à recourir à une solution tierce et propriétaire.

#### **2.1.1 Installation de TRUENAS CORE**

TrueNAS peut être installé sur une Compact Flash, une clé USB ou un disque dur dédié. Le système d'exploitation prend peu d'espace disque (compter de l'ordre de 1 Go). L'administration du système s'effectue principalement via une interface web. TrueNAS offre la possibilité d'exploiter le système de fichiers ZFS permettant ainsi une gestion des volumes de grosses capacités.<sup>[1]</sup> Après installation manuelle nécessaire, il s'administre ensuite à distance depuis l'interface web, ce qui rend son utilisation plus facile. La figure suivante montre une illustration du logo de TrueNAS CORE :



*Figure 6: Logo de TrueNAS CORE [22]*

<sup>[1]</sup> : [www.projet-plume.org/fiche/freenas](http://www.projet-plume.org/fiche/freenas)

### 2.1.2 Fonctionnement de TRUENAS CORE

TrueNAS est basé sur ZFS, qui est un système de fichiers open source, un contrôleur RAID (est une carte ou une puce située entre le système d'exploitation et les disques de stockage, généralement des disques durs et qui fournit une redondance des données et / ou améliore les performances du disque dur) et un gestionnaire de volumes au niveau de l'entreprise, garantissant une parfaite intégrité des données. Il a également d'autres fonctionnalités comme la possibilité de créer des partages SMB/CIFS (partage de fichiers Windows), NFS (partage de fichiers Unix), AFP (partage de fichiers Apple) et iSCSI (partage de blocs), la possibilité de se connecter via FTP et S3 (basé sur Minio) et la capacité de capture de données en réplication.<sup>[2]</sup>

## 2.2 Les différents outils de sécurisation du système de stockage en interne

### 2.2.1 Les environnement jails de TRUENAS CORE

Un environnement jail est une fonctionnalité avancée des systèmes BSD (TrueNAS est basé sur FreeBSD) qui permet d'installer des applications sur notre système de stockage en toute sécurité. Il est en fait une partie virtualisée du système de stockage, ainsi pour un processus installé dedans tout est comme s'il était installé directement dans le système sauf que si ce processus devient malveillant il ne pourra pas compromettre le système car il compromettra un système virtuel. <sup>[3]</sup>

Cette solution présente elle aussi des avantages et des inconvénients :

#### *Avantages*

- ❖ Les environnements jails permettent de garder le système en parfait état en cas de piratage ;
- ❖ Les environnements jails permettent de créer une image virtuelle du système ;
- ❖ Ils permettent de conserver l'intégrité des données même après une cyberattaque ;

<sup>[2]</sup> : <https://www.iperiusbackup.net/fr/freenas-comment-installer-et-le-configurer-pour-une-sauvegarde-nas/>

<sup>[3]</sup> : <https://www.amenschool.fr/interet-certificat-ssl/>

- ❖ Les environnements jails assurent la confidentialité des données ;
- ❖ Ne supporte aucun coût.

#### *Inconvénient*

- ❖ Nécessite une connaissance un peu poussée sur le sujet.

### 2.2.2 Certificat SSL (Secure Socket Layer)

Un certificat SSL est un fichier de données qui lie une clé de cryptographie aux informations d'une organisation que l'on installe sur un serveur. Cette solution est généralement installée sur un serveur et active le cadenas et le protocole « https », afin d'assurer une connexion sécurisée entre le serveur web et le navigateur. Il utilise une cryptographie à clé publique qui lui permet de relier ensemble :

- ❖ un nom de domaine, un nom de serveur et un nom d'hôte ;
- ❖ l'identité de l'organisation (nom de l'entreprise) et le lieu.

Dans notre cas, le certificat SSL sera lié à un nom de domaine à qui sera par la suite relié l'adresse IP du NAS. Cependant il présente des avantages et des inconvénients :

#### *Avantages*

- ❖ l'installation d'un certificat SSL sur un serveur assure la confidentialité, l'espionnage ou l'interception des données ;
- ❖ l'installation d'un certificat SSL sur un serveur rend impossible le piratage des informations échangées entre le navigateur et le serveur ;
- ❖ l'installation d'un certificat SSL sur un serveur permet d'authentifier un site et assure au visiteur qu'il s'agit bien du site officiel de l'entreprise recherchée. <sup>[4]</sup>

#### *Inconvénients*

- ❖ Certificat payant à un coût élevé ;
- ❖ Nécessite des frais supplémentaires pour la mise en cache des données ;
- ❖ Difficile à configurer et nécessite parfois des modifications du logiciel en interne.

<sup>[4]</sup> : durindel.fr

### 2.2.3 Synthèse sur les différents outils de sécurisation du système de stockage et choix de la solution

En vue de proposer une solution adéquate au groupe INGENIEURS & EXPERTS, nous avons étudié plusieurs choix possibles pouvant résoudre ce problème. En étudiant ces solutions possibles, nous avons remarqué qu'elles présentent des avantages comme des inconvénients. Ainsi, nous allons procéder à une comparaison afin de choisir la solution la mieux adaptée en fonction des ressources existants et des besoins du groupe IE.

Le tableau 3 présente une comparaison entre les différentes solutions précitées :

Tableau 3: Tableau de comparaison des outils de sécurisation

SOLUTIONS	CERTIFICAT SSL	ENVIRONNEMENTS JAILS
Coût d'acquisition	Payant	Gratuit
Difficulté d'implémentation/Conception de la solution	Elevée	Moyenne
Durée d'implémentation de la solution	Très longue	Courte

Compte tenu des ressources disponibles ainsi que du temps d'implémentation par rapport à la solution à choisir, le choix du groupe INGENIEURS & EXPERTS s'est donc porté sur la solution 2 : **la mise en place des environnements Jails**.

## 2.3 Généralités sur les technologies pare-feux

Un pare-feu informatique est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, de surveiller et de contrôler les applications et les flux de données et de protéger le système informatique connecté à internet des tentatives d'intrusions qui pourraient en provenir. La figure 7 illustre un réseau dans lequel se trouve un pare-feu :

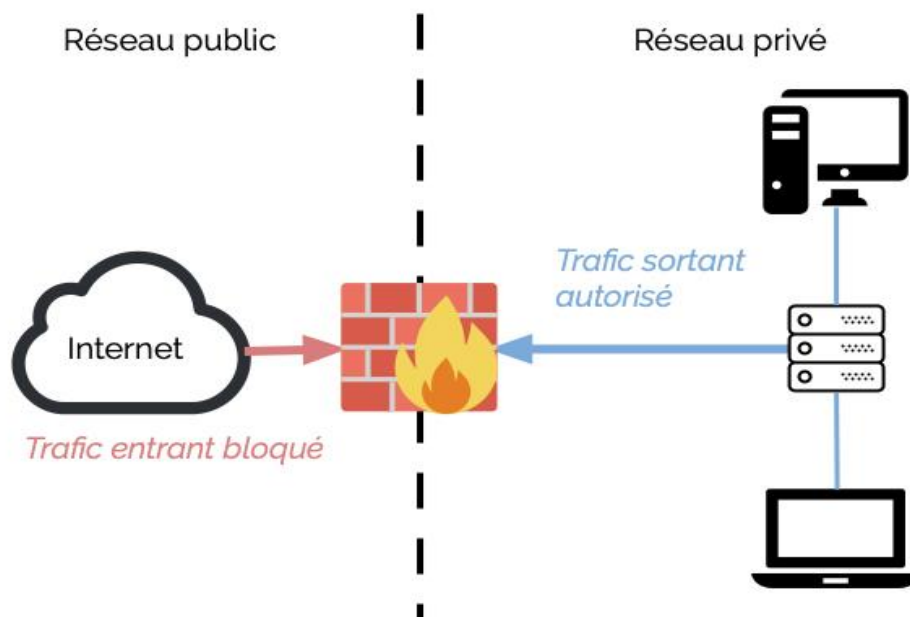


Figure 7: Illustration d'un pare-feu dans un réseau [21]

### 2.3.1 Pfsense

Pfsense est un routeur/pare-feu open-source basé sur le système d'exploitation FreeBSD. Il utilise des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. Après l'installation manuelle nécessaire pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web. Pfsense gère nativement les VLAN. La figure 8 montre l'illustration du logo de Pfsense :





*Figure 8: Logo de PfSense [23]*

PfSense présente des avantages et des inconvénients :

#### *Avantages*

- ❖ il est un logiciel open source et gratuit ;
- ❖ il dispose d'une communauté de développeurs pas d'un éditeur unique ce qui favorise l'évolution constante du logiciel ;
- ❖ le développement communautaire favorise la réactivité lorsqu'il s'agit de corriger un bug ou une faille de sécurité ;
- ❖ il permet le déploiement d'un pare-feu.

#### *Inconvénients*

- ❖ tout le monde peut étudier son fonctionnement et trouver des failles;
- ❖ aucune garantie n'est ajoutée;
- ❖ l'interface peut paraître intuitive et trop fournie ;
- ❖ aucune garantie si vous avez un problème matériel ou logiciel, vous devez vous débrouiller ou alors payer pour du support ;
- ❖ moins stable qu'un pare-feu matériel.

### 2.3.2 Zentyal

Zentyal (antérieurement eBox Platform) est un serveur de réseau unifié open source (ou une plate-forme réseau unifiée) destinée aux petites et moyennes entreprises (PME). Il peut agir comme un pare-feu, un serveur samba, un serveur proxy squidguard, etc... Le tout unifié sous une interface web et peut être installé sur une version desktop ou serveur d'Ubuntu (version TLS recommandée). Afin de profiter de toutes les fonctionnalités offertes, il est nécessaire d'avoir au moins 2 interfaces réseau. La figure suivante montre une illustration du logo de Zentyal.



*Figure 9: Logo de Zentyal [24]*

Zentyal présente des avantages et des inconvénients :

#### *Avantages*

- ❖ Avec un seul CD nous avons tout ce dont nous avons besoin et ce qui manque selon le besoin ;
- ❖ il permet la gestion de l'infrastructure réseau, de la passerelle, du serveur de communication ;
- ❖ il dispose d'une large documentation ;
- ❖ il dispose du support d'une grande communauté ;
- ❖ il simplifie considérablement le travail de l'administrateur, ce qui lui permet de se concentrer sur des tâches plus spécifiques ;
- ❖ il est une solution mature et stable dans tous les sens et en développement continu.

#### *Inconvénient*

- ❖ la version plus sophistiquée que peut utiliser les grandes entreprise est payante.

### 2.3.3 Synthèse sur les technologies Pare-feu

Le tableau ci-après fait une comparaison des technologies pare-feu citées plus haut :

*Tableau 4: Tableau comparatif des technologies de pare-feu étudiées*

SOLUTIONS	PFSENSE	Zentyal
Coût d'acquisition	Gratuit	Gratuit
Difficulté d'implémentation/Conception de la solution	Elevée	Moyenne
Durée d'implémentation de la solution	Elevée	Courte
Stabilité	Moyenne	Elevée

En fonction des ressources disponibles dans le groupe IE et de sa politique de sécurité de l'IE, le pare-feu Zentyal est celui qui a été retenu.

## 2.4 Sécurisation de l'accès à distance : Les technologies VPN

Un réseau privé virtuel (VPN) est un service qui permet d'accéder au Web de manière sécurisée et privée en acheminant la connexion via un serveur et qui cache toutes actions en ligne. Un VPN d'accéder à un réseau local en toute sécurité lorsque l'on utilise sur un réseau de télécommunication public. Il permet donc d'avoir accès au réseau interne (réseau d'entreprise par exemple) depuis l'extérieur. Pour cela, il crée un tunnel privé sur internet ouvert. Alors, peu importe les paquets envoyés dans ce canal de communication privé, ceux-ci sont encapsulés et cryptés de manière à ne pas pouvoir être déchiffrés même s'ils sont interceptés. Un VPN dispose généralement aussi d'une passerelle permettant d'accéder à l'extérieur, ce qui permet de changer l'adresse IP source apparente de ses connexions.

La figure 10 montre une illustration de l'utilisation d'un VPN d'un réseau public vers un réseau local distant :

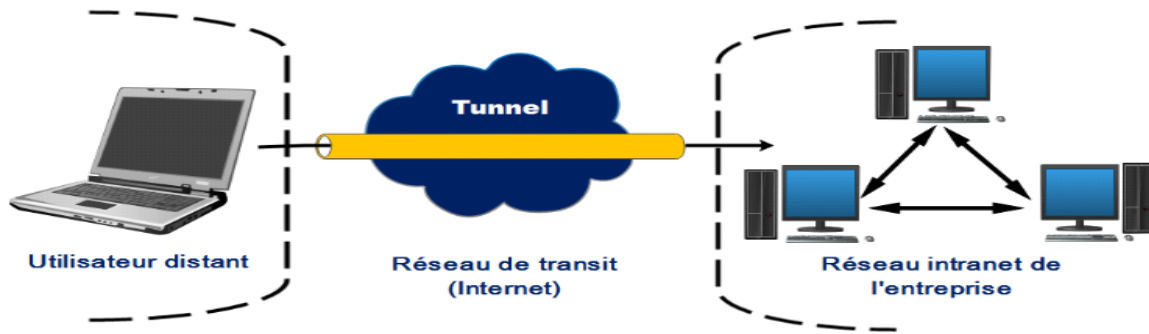


Figure 10: Illustration de l'utilisation d'un vpn d'un réseau public distant vers un réseau local [25]

Il existe aujourd'hui plusieurs technologies VPN tels que IKEv2, OpenVPN...

#### 2.4.1 IPVanish

WireGuard est une application et un protocole réseau permettant de mettre en place un tunnel VPN chiffré. Ce logiciel est un logiciel libre sous licence GPLv2 et est disponible sur toutes les plateformes. WireGuard est écrit dans les langages « C » et « Go » et fonctionne sous Windows, macOS, BSD, iOS et Android. WireGuard permet de créer un tunnel crypté. Sur le principe, WireGuard est un protocole VPN pair-à-pair décentralisé car plutôt que de recourir impérativement à un serveur, WireGuard permet d'ouvrir directement un tunnel entre deux machines. Les flux de données passent par ce tunnel et sont ainsi protégés de tout accès par des personnes non autorisées. La connexion est établie de façon similaire à Secure Shell(SSH) : avec ce protocole, les utilisateurs (appelés « pairs ») génèrent une clé publique et se l'échangent. Cette clé permet aux pairs de s'authentifier mutuellement et de chiffrer les paquets de données pour l'autre interlocuteur. En dehors d'un cryptage fort, WireGuard offre également des optimisations pour les systèmes mobiles et les appareils de l'« Internet des objets (IdO) ».

##### *Avantages*

- ❖ Le protocole supporte par l'itinérance, c'est-à-dire le passage automatique du Wi-Fi au réseau mobile et vice versa. Donc si la connexion devait malgré tout s'interrompre, WireGuard permet généralement de rétablir la connexion plus rapidement que les protocoles concurrents ;
- ❖ La faible complexité du logiciel implique une plus grande performance vis-à-vis de la sécurité ;
- ❖ Il établit les connexions de façon similaire au protocole SSH.

### *Inconvénients*

- ❖ L'application présente des bugs ;
- ❖ Aucune version stable permettant le contrôle des failles et vulnérabilités communes n'existe ;
- ❖ Les plates-formes autres que Linux ne sont pas prises en charge.

### 2.4.2 OpenVPN

**OpenVPN** est un logiciel libre permettant de créer un VPN. Il utilise le protocole TCP/UDP pour assurer le transport des paquets sur le réseau, ce qui lui confère une très grande fiabilité. Il est très robuste et très utilisé. Il a deux modes d'authentification :

- ❖ clé statique : ce mode utilise une clé statique pré-partagée ;
- ❖ TLS : ce mode utilise des certificats SSL/TLS pour l'authentification et l'échange de clés.

En mode clé statique, une clé pré-partagée est générée et partagée entre les deux pairs OpenVPN avant le démarrage du tunnel. Cette clé statique contient 4 clés indépendantes : l'envoi HMAC (**HMAC** est un protocole utilisé pour les messages d'authentification), la réception HMAC, le chiffrement et le déchiffrement. Par défaut en mode clé statique, les deux hôtes utiliseront la même clé HMAC et la même clé de chiffrement/déchiffrement.

En mode SSL/TLS, une session SSL est établie avec une authentification bidirectionnelle (c'est-à-dire que chaque côté de la connexion doit présenter son propre certificat). Si l'authentification SSL/TLS réussit, le chiffrement/déchiffrement et le matériel source de la clé HMAC sont alors générés de manière aléatoire et échangés via la connexion SSL/TLS. La figure suivante présente le logo d'OpenVPN :



*Figure 11: Logo d'OpenVPN [3]*

Les avantages et inconvénients d'OpenVPN sont :

#### Avantages

- ❖ ne requiert aucun matériel spécifique ;
- ❖ bon débit des liaisons ;
- ❖ tunnel très sécurisé ;
- ❖ multiplateforme;
- ❖ stable et fiable ;
- ❖ libre et gratuit.

#### Inconvénients

- ❖ problème de compatibilité avec d'autres protocoles VPN ;

### 2.4.3 Synthèse et choix de la technologie VPN adaptée

Le tableau ci-après fait une comparaison des technologies VPN citées plus hauts :

*Tableau 5: Tableau comparatif des technologies VPN*

SOLUTIONS	WireGuard	OpenVPN
Chiffrement	AES-256	AES-256
Sécurité	Faible	Très élevée
Rapidité	Très rapide	Rapide

## 2.5 Choix des solutions adaptées

Après analyse des solutions examinées ci-haut et en fonction de la politique de sécurité du groupe INGENIEURS & EXPERTS, les environnements jails de TrueNAS, le pare-feu Zentyal et le protocole OpenVPN sont celles qui sont retenues pour la sécurisation du système de stockage TrueNAS.

## **Chapitre 3 : Mise en œuvre et perspectives**

Dans ce chapitre, nous allons implémenter les différents composants qui nous permettront de déployer la solution retenue. Nous allons configurer les outils et technologies retenues, de fiabiliser le système en assurant sa sécurité. Nous ferons ensuite les tests de fonctionnement. Cette solution n'étant pas gratuite, nous terminerons ce chapitre par une évaluation financière de celle-ci.

### 3.1 Les éléments de réalisation

Pour pouvoir mettre en place les environnements jails il nous a fallu :

- ❖ virtualiser l'environnement de travail avec VMware Workstation ;
- ❖ mettre en place un pare-feu avec Zentyal ;
- ❖ installer le système de stockage TrueNAS CORE ;
- ❖ mettre en place la sécurité à double facteurs d'authentification sur TrueNAS ;
- ❖ ajouter les utilisateurs sur TrueNAS ;
- ❖ configurer les groupes, les Datasets et les partages Samba sur TrueNAS ;
- ❖ configurer un environnement jail sur TrueNAS (Nextcloud) ;
- ❖ déployer le serveur VPN OpenVPN sur TrueNAS .

#### 3.1.1 VMware Workstation

VMware Workstation Pro est un hyperviseur de type 2. C'est aussi la version station de travail du logiciel. Elle permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte. La version Linux présente l'avantage de pouvoir sauvegarder les fichiers de la machine virtuelle pendant son fonctionnement.

La figure 12 présente le logo de VMware Workstation :





*Figure 12: Logo de VMware Workstation [26]*

### 3.1.2 OpenVPN

OpenVPN est un logiciel libre permettant de créer un VPN. Il utilise le protocole UDP pour assurer le transport des paquets sur le réseau, ce qui lui confère une très grande fiabilité. OpenVPN Access Server est une version de OpenVPN qui prend en charge une interface graphique de gestion et permet l'authentification via des comptes locaux, LDAP, SAML ...

## 3.2 Mise en œuvre

### 3.2.1 Politique de sécurité

Une politique de sécurité est une stratégie visant à maximiser la sécurité d'une entreprise.

#### 3.2.1.1 Conditions générales d'accès aux serveurs

Dans cette partie, nous allons procéder à l'inventaire des différentes entités autorisés à l'accès aux différents serveurs ainsi que des différentes actions autorisées sur ceux-ci.

Le tableau 6 présente les conditions générales d'accès aux serveurs :

Tableau 6: Politique de sécurité d'accès aux serveurs à l'IE

SERVEURS	ENTITES AUTORISEES	DESCRIPTION
Tous les serveurs	L'administrateur	L'administrateur a pleine autorité sur les serveurs
SERVEUR VPN	SERVEUR TRUENAS, SERVEUR ZENTYAL	
SERVEUR TRUENAS CORE	SERVEUR NEXTCLOUD, SERVEUR VPN, SERVEUR ZENTYAL	
SERVEUR NEXTCLOUD	Le personnel autorisé	Le personnel autorisé peut avoir accès aux fichiers du Nextcloud

### 3.2.1.2 Accès à distance aux ressources du système de stockage TrueNAS

L'accès à distance des ressources du système de stockage TrueNAS sera conditionné par l'utilisation de VPN. Pour la connexion aux serveurs, seul le groupe d'administrateurs seront autorisés. Pour ce faire, une fois les serveurs intégrés au contrôleur de domaine, nous allons fixer les adresses IP que recevront les administrateurs lors de leur authentification sur le VPN.

### 3.2.1.3 Sécurité des données

Pour assurer une sécurité élevée aux données du système de stockage TrueNAS nous allons configurer un environnement jail. Cette configuration consistera à configurer le plugin Nextcloud en tant qu'une prison sur TrueNAS CORE. Pour mettre en place ce système nous avons utilisé VMware Workstation.

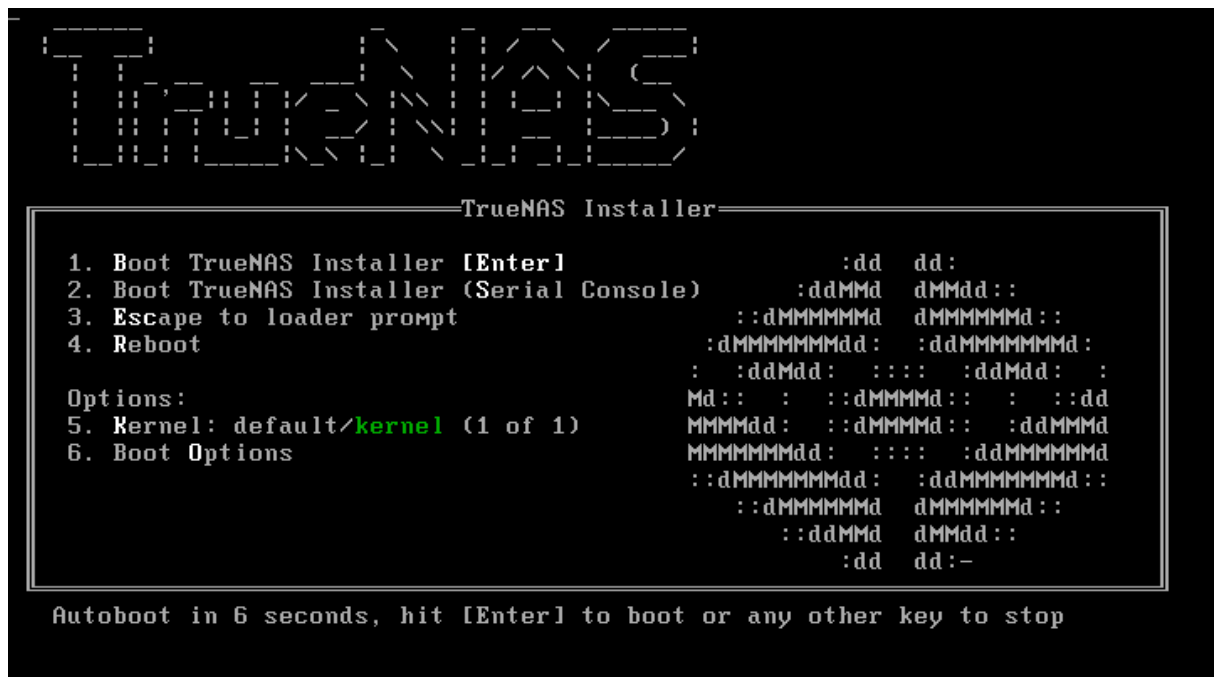
## 3.2.2 Mise en place de l'infrastructure réseau

### 3.2.2.1 Mise en place du serveur TrueNAS CORE

Pour installer le serveur TrueNAS CORE, nous l'avons déployé sur une machine virtuelle virtualisée sur VMware Workstation. Pour commencer, nous devons insérer l'image disque iso de TrueNAS dans la nouvelle machine virtuelle créée sur VMware Workstation. Ensuite, nous allons démarrer la machine virtuelle TrueNAS CORE afin de procéder à sa configuration. Sa configuration se déroule en deux étapes : en ligne de commande et ensuite sur une interface web.

### a- Installation et configuration de TrueNAS CORE en ligne de commande

La figure suivante montre le démarrage de la configuration en ligne de commande de TrueNAS CORE :



*Figure 13: Démarrage de la machine virtuelle TrueNAS*

Ensuite commence la configuration de la machine virtuelle en ligne de commande. Les figures 14, 15 et 16 montrent certaines étapes de la configuration de la machine virtuelle TrueNAS :

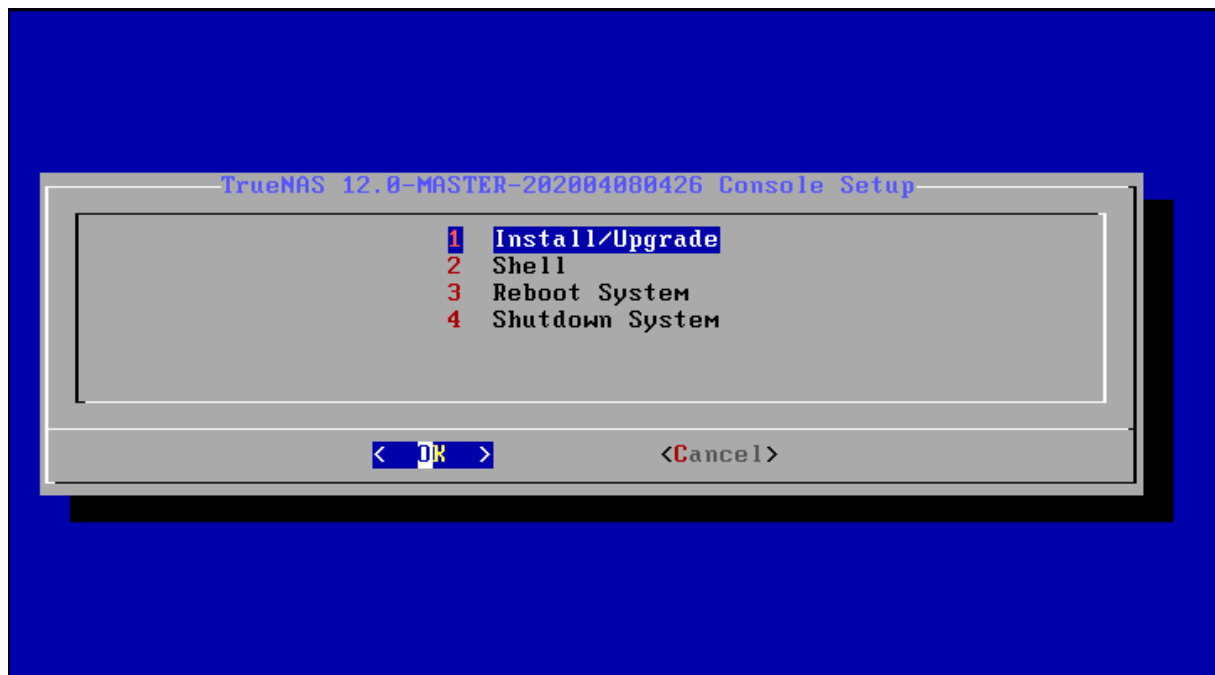


Figure 14: Démarrage de la configuration en ligne de commande

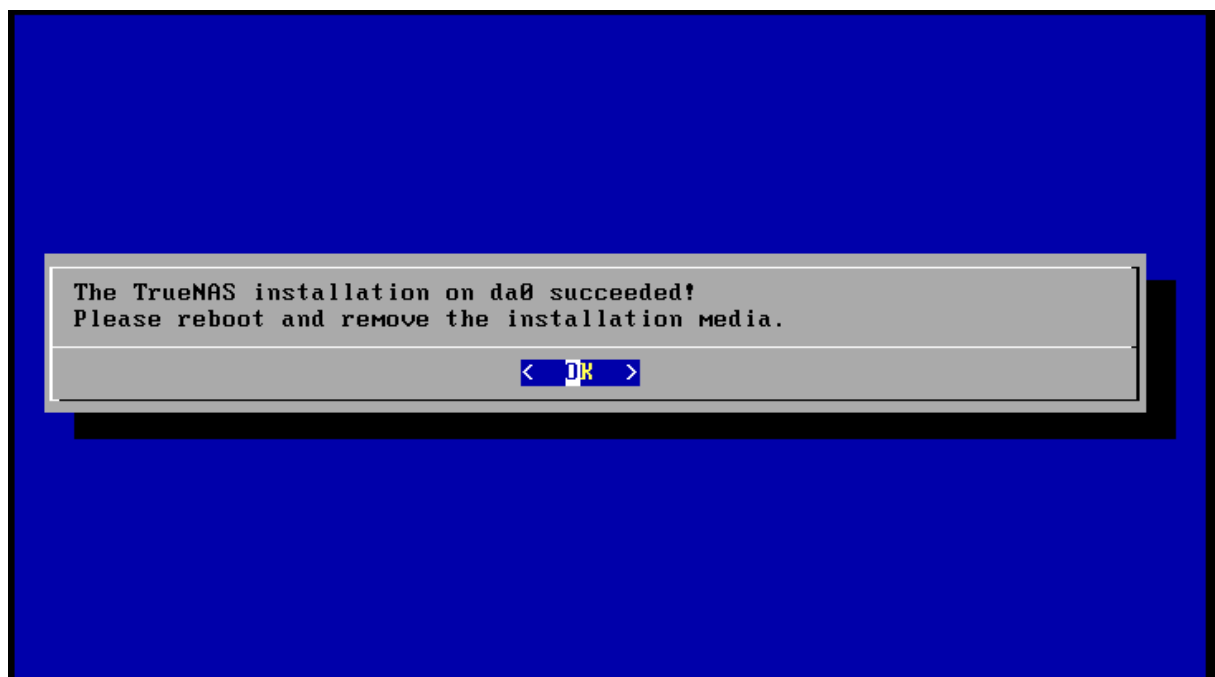


Figure 15: Fin de la configuration

```
FreeBSD/amd64 (truenas.local) (ttyv0)

Console setup
-----

1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web user interface is at:

http://192.168.204.149
https://192.168.204.149

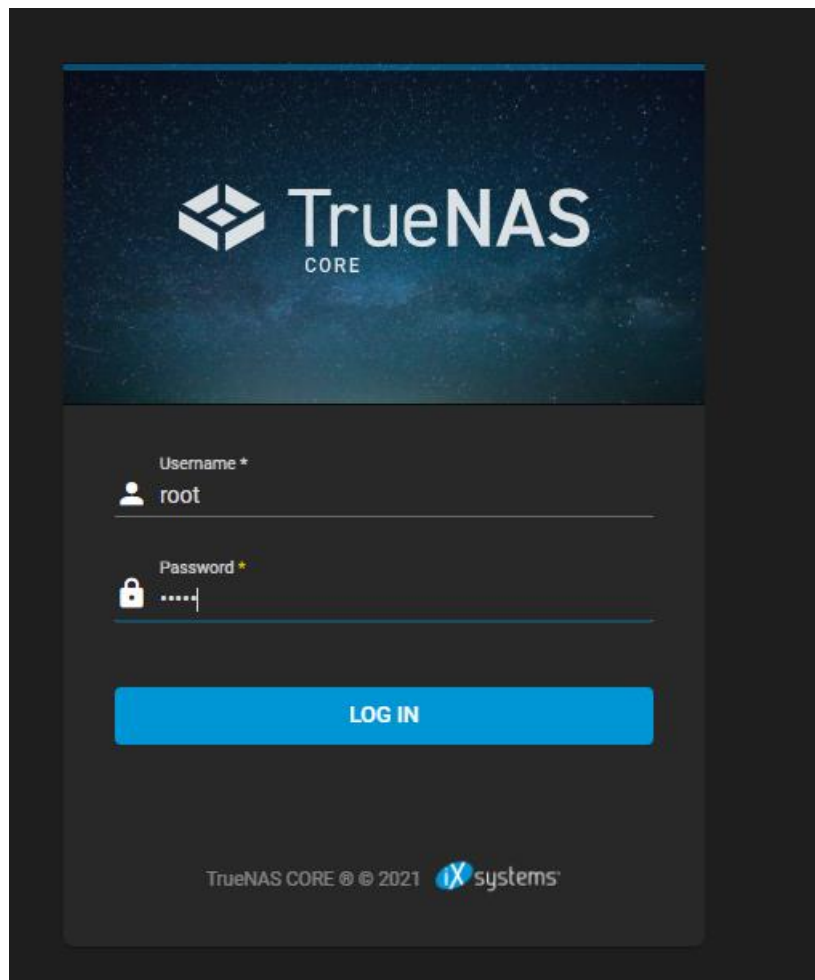
Enter an option from 1-11: █
```

*Figure 16: Interface de TrueNAS en ligne de commande*

#### b- Configuration de TrueNAS CORE sur l'interface web

Ensuite nous allons nous rendre sur l'interface web de connexion de TrueNAS CORE à partir de l'adresse IP 192.168.204.149 où nous allons continuer notre configuration.

La figure 17 présente l'interface de connexion de TrueNAS CORE :



*Figure 17: Interface web de TrueNAS CORE*

Nous allons ensuite procéder à la configuration globale du réseau de TrueNAS comme le montre la figure 18 :

The screenshot shows the TrueNAS network configuration page. It is divided into several sections: 'Hostname and Domain', 'Service Announcement', 'DNS Servers', 'Default Gateway', 'Other Settings', and a 'Host Name Database' section. The 'Hostname and Domain' section has fields for 'Hostname' (truenas) and 'Domain' (local). The 'Service Announcement' section has checkboxes for 'NetBIOS-NS' (unchecked), 'mDNS' (checked), and 'WS-Discovery' (checked). The 'DNS Servers' section has three fields for 'Nameserver 1' (1.1.1.1), 'Nameserver 2' (8.8.8.8), and 'Nameserver 3' (empty). The 'Default Gateway' section has two fields for 'IPv4 Default Gateway' and 'IPv6 Default Gateway' (both empty). The 'Other Settings' section has a checkbox for 'Enable Netwait Feature' (unchecked) and a field for 'HTTP Proxy' (empty). The 'Host Name Database' section has a field for 'Host Name Database' (empty). A blue 'SAVE' button is at the bottom left.

Section	Field	Value
Hostname and Domain	Hostname	truenas
	Domain	local
	Additional Domains	
Service Announcement	NetBIOS-NS	<input type="checkbox"/>
	mDNS	<input checked="" type="checkbox"/>
	WS-Discovery	<input checked="" type="checkbox"/>
DNS Servers	Nameserver 1	1.1.1.1
	Nameserver 2	8.8.8.8
	Nameserver 3	
Default Gateway	IPv4 Default Gateway	
	IPv6 Default Gateway	
Other Settings	HTTP Proxy	
	Enable Netwait Feature	<input type="checkbox"/>
Host Name Database	Host Name Database	

*Figure 18: Configuration du réseau de TrueNAS*

Nous allons ensuite passer à la création des comptes utilisateurs comme l'illustre la figure 19 :

**Identification**

Full Name \*  
KOSSI-TITRIKOU Marc-Olivier

Username \*  
marc

Email

Password

Confirm Password

**User ID and Groups**

User ID  
1000

Primary Group  
marc

Auxiliary Groups  
builtin\_users, Informatique, Public

**Directories and Permissions**

Home Directory  
+ /mnt/IE\_pool1/Users\_Info

▶ /mnt

Home Directory Permissions

	Read	Write	Execute
User	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Authentication**

SSH Public Key

Disable Password  
No

Shell  
sh

☐ Lock User

Figure 19: Création d'un compte utilisateur

Passons à la création de groupes d'utilisateurs comme le présente la figure suivante :

**Group Configuration**

GID  
1003

Name \*  
Informatique

☐ Permit Sudo

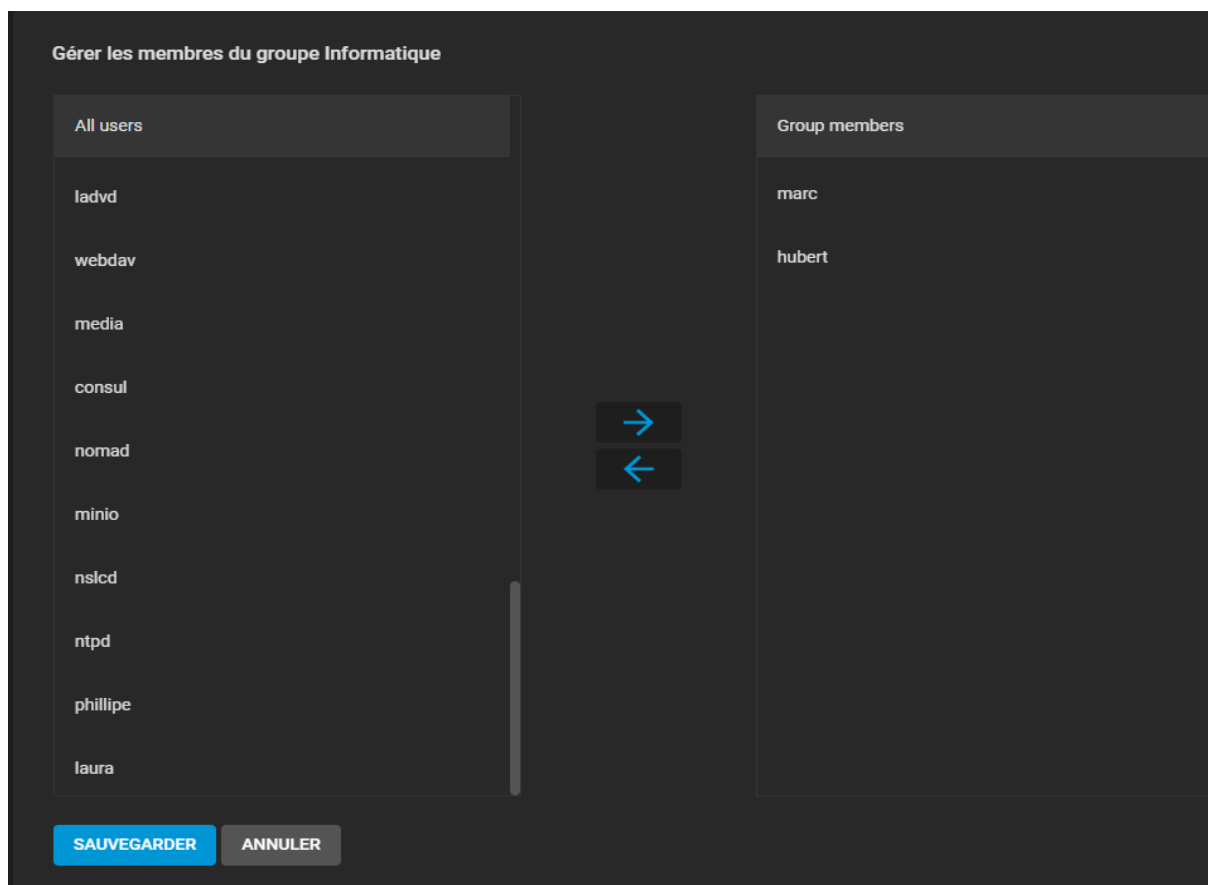
☒ Samba Authentication

SAVE CANCEL

Figure 20: Création du groupe informatique

Attribuons ensuite les utilisateurs aux différents groupes. La figure 21 qui suit l'illustre :





*Figure 21: Attribution du groupe informatique à l'utilisateur marc*

Créons ensuite un espace de stockage sur TrueNAS appelé Pool, des datasets ainsi que les différentes permissions aux différents utilisateurs. Les figures 22, 23 et 24 qui suivent illustrent la création d'un espace de stockage Pool, d'un dataset ainsi que l'affectation des ACL à un dataset :

### Nom et options

Nom

IE\_pool1

commentaires

Synchroniser

Standard

Niveau de compression

LZ4

Activer l'heure

au

### Autres options

Déduplication ZFS

désactivé

Sensibilité à la casse

Sensible

SAUVEGARDER

ANNULER

OPTIONS AVANCÉES

*Figure 22: Création du pool IE\_pool1*

### Nom et options

Nom

IE\_pool1/Public

commentaires

Dataset Public

Synchroniser

Hériter (standard)

Niveau de compression

Hériter (lz4)

Activer l'heure

Hériter (activé)

### Autres options

Déduplication ZFS

désactivé

Sensibilité à la casse

Insensible

SAUVEGARDER

ANNULER

OPTIONS AVANCÉES

*Figure 23: Création du dataset public*

**Informations sur le fichier**

Chemin  
/mnt/IE\_pool1/Public

Utilisateur  
root

☐ Appliquer l'utilisateur

Groupe  
wheel

☐ Appliquer le groupe

**SÉLECTIONNEZ UN PRÉRÉGLAGE ACL**

**Liste de contrôle d'accès**

Qui \*  
everyone@

Type de liste de contrôle d'accès \*  
Permettre

Type d'autorisation \*  
De base

Autorisations \*  
Modifier

Type de drapeaux \*  
De base

Drapeaux \*  
Hériter

**EFFACER**

Qui \*  
propriétaire@

Type de liste de contrôle d'accès \*  
Permettre

Type d'autorisation \*  
De base

Autorisations \*  
Contrôle total

Type de drapeaux \*  
De base

Drapeaux \*  
Hériter

**EFFACER**

*Figure 24: Définitions des différentes autorisations au dataset public*

Passons à l'activation du service samba et à la création des partages samba aux différents datasets du pool IE\_pool1. Les figures 25 et 26 illustrent l'activation du service samba et la création des partages samba à un dataset :

Name	Running	Start Automatically
NFS	<input type="checkbox"/>	<input type="checkbox"/>
OpenVPN Client	<input type="checkbox"/>	<input type="checkbox"/>
OpenVPN Server	<input type="checkbox"/>	<input type="checkbox"/>
Rsync	<input type="checkbox"/>	<input type="checkbox"/>
S.M.A.R.T.	<input type="checkbox"/>	<input type="checkbox"/>
S3	<input type="checkbox"/>	<input type="checkbox"/>
SMB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 25: Activation du service samba SMB

### De base

Chemin \*

?

▼ /mnt

▼ IE\_pool1

- ▶ iocage
- ▶ Publique LCA
- ▶ Utilisateurs\_Architecture LCA
- ▶ Utilisateurs\_Informatique LCA
- ▶ Utilisateurs LCA

Nom

Public

But

Paramètres de partage par défaut ▼ ? La description

☒ Activée ?

**SAUVEGARDER** **ANNULER** **OPTIONS AVANCÉES**

Figure 26: Création du partage samba au dataset public

### 3.2.2.2 Déploiement et installation du serveur VPN sur TrueNAS CORE

#### a- Installation du serveur VPN OpenVPN

Afin de pouvoir se connecter à notre serveur VPN nous avons besoin d'un certificat d'authentification. Alors, au lieu de payer un certificat, TrueNAS CORE nous donne la possibilité de créer notre propre certificat d'autorité de certification racine OpenVPN qui aura pour but de reconnaître notre propre certificat d'authentification que nous utiliserons. Pour créer notre propre autorité de certification racine, allons dans **Menu > Système > CAs > Ajouter**. Nous allons ensuite procéder à sa création. La figure qui suit illustre la création d'un certificat d'autorité de certification racine :

The screenshot shows the 'Add Certificate' form in TrueNAS CORE, specifically for creating a root CA. The form is divided into several sections:

- Identifier and Type:**
  - Name \*: OpenVPN\_ROOT\_CA
  - Type: Internal CA
  - Profiles: Openvpn Root CA
- Certificate Options:**
  - Key Type \*: RSA
  - Key Length \*: 2048
  - Digest Algorithm \*: SHA256
  - Lifetime \*: 825
- Certificate Subject:**
  - Country \*: Togo
  - State \*: Lomé
  - Locality \*: Lomé
  - Organization \*: INGENIEURS & EXPERTS
  - Organizational Unit: Groupe\_ie@hotmail.com
  - Common Name: ie\_domain.com
  - Subject Alternate Names \*: www.ie\_domain.com
- Basic Constraints:**
  - Enabled: ☒
  - Path Length: ?
  - Basic Constraints Config: CA, Critical Extension
- Authority Key Identifier:**
  - Enabled: ☒
  - Authority Key Config: Authority Cert Issuer
- Extended Key Usage:**
  - Enabled: ☒
  - Usages \*: CLIENT AUTH, SERVER AUTH
- Key Usage:**
  - Enabled: ☒
  - Key Usage Config: Key Cert Sign, CRL Sign, Critical Extension

*Figure 27: Création du certificat d'autorité de certification racine*

Nous allons ensuite créer notre propre certificat d'authentification que nous pourrions utiliser pour nous connecter à notre serveur OpenVPN. Pour cela, allons dans **Menu**

> **Système > Certificats > Add**. La figure suivante illustre la création d'un certificat d'authentification :

Identifier and Type		Certificate Options	
Name *	OpenVPN_Server	Signing Certificate Authority *	OpenVPN_ROOT_CA
Type	Internal Certificate	Key Type *	RSA
Profiles	Openvpn Server Certificate	Key Length *	2048
		Digest Algorithm *	SHA256
		Lifetime *	825
Certificate Subject		Authority Key Identifier	
Country *	Togo	State *	Lomé
Locality *	Lomé	Organization *	INGENIEURS & EXPERTS
Organizational Unit		Email *	Groupe_je@hotmail.com
Common Name	ie_domain.com	Subject Alternate Names *	www.ie_domain.com
Basic Constraints		Key Usage	
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled	
Path Length	0	Authority Key Config	Authority Cert Issuer
Basic Constraints Config			
Critical Extension			
Extended Key Usage	<input checked="" type="checkbox"/> Enabled		

*Figure 28: Création d'un certificat d'authentification OpenVPN*

Notre certificat d'authentification ainsi créé, allons dans **Menu > Services > OpenVPN Server > Editer** afin de passer à la configuration du service OpenVPN Server. La figure 29 illustre la configuration du service OpenVPN Server :

*Figure 29: Configuration du service OpenVPN Server*

Nous allons ensuite activer le service OpenVPN Server. La figure suivante illustre l'activation du service OpenVPN:

Name	Running	Start Automatically	Actions
AFP	<input type="checkbox"/>	<input type="checkbox"/>	
Dynamic DNS	<input type="checkbox"/>	<input type="checkbox"/>	
FTP	<input type="checkbox"/>	<input type="checkbox"/>	
iSCSI	<input type="checkbox"/>	<input type="checkbox"/>	
LLDP	<input type="checkbox"/>	<input type="checkbox"/>	
NFS	<input type="checkbox"/>	<input type="checkbox"/>	
OpenVPN Client	<input type="checkbox"/>	<input type="checkbox"/>	
OpenVPN Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

*Figure 30: Activation du service OpenVPN Server*

Afin de pouvoir se connecter au serveur OpenVPN Server et ceci en toute sécurité, nous avons besoin de télécharger une configuration cliente. Cependant, pour télécharger la configuration cliente, nous aurons besoin d'un certificat qui nous permettra de se connecter à notre client OpenVPN. Pour cela, nous allons créer ce certificat. Pour créer ce certificat, allons dans **Menu > Système > Certificats > Add**. La figure 31 illustre la création du certificat du client OpenVPN :



Identifier and Type		Certificate Options	
Name *	OpenVPN_User01	Signing Certificate Authority *	OpenVPN_ROOT_CA
Type	Internal Certificate	Key Type *	RSA
Profiles	Openvpn Client Certificate	Key Length *	2048
		Digest Algorithm *	SHA256
		Lifetime *	825
Certificate Subject			
Country *	Togo	State *	Lomé
Locality *	Lomé	Organization *	INGENIEURS & EXPERTS
Organizational Unit		Email *	Groupe_ie@hotmail.com
Common Name	ie_domain.com	Subject Alternate Names *	www.ie_domain.com
Basic Constraints		Authority Key Identifier	
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled	
Path Length		Authority Key Config	Authority Cert Issuer
Basic Constraints Config			
Critical Extension			
Extended Key Usage		Key Usage	
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled	

*Figure 31: Création du certificat de connexion au client OpenVPN*

Chaque utilisateur doit avoir son propre certificat de connexion au client OpenVPN. A présent, passons au téléchargement de la configuration cliente en allant dans **Menu > Services > OpenVPN Server > Editer > Télécharger la configuration cliente > Sélectionner le certificat client > soumettre**. La figure 32 illustre le téléchargement de la configuration cliente :

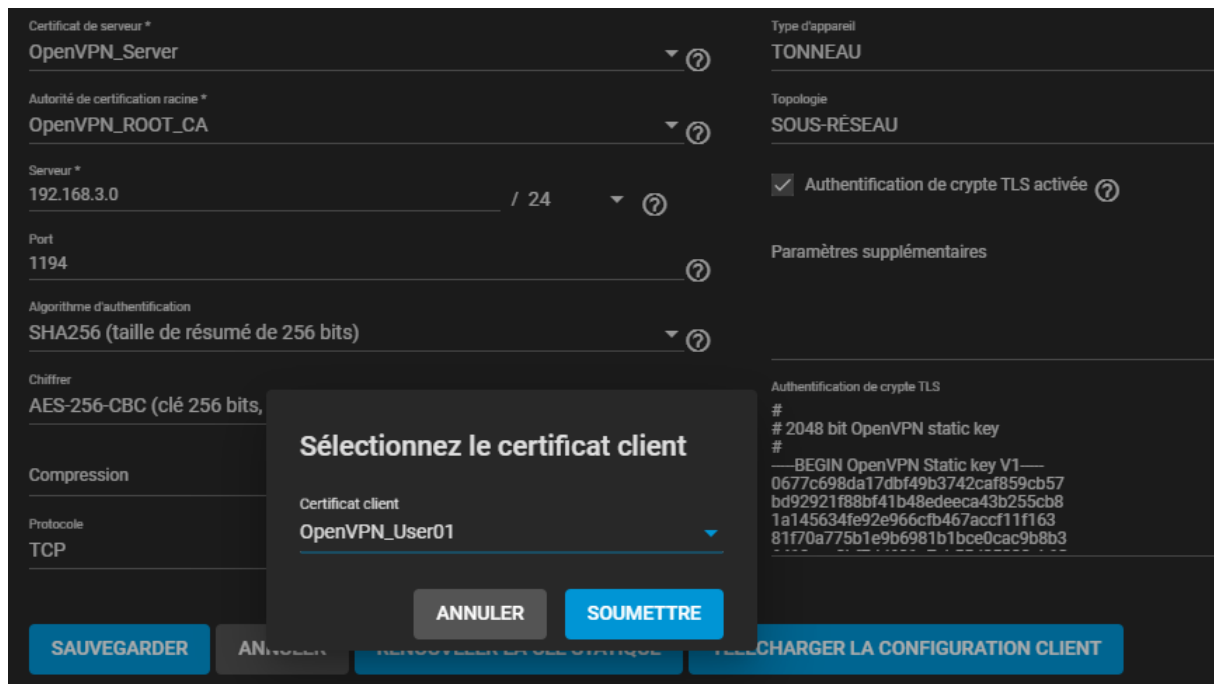


Figure 32: Choix du certificat client

Après téléchargement, on obtient un fichier **openVPNClientConf.ovpn** que l'on copiera sur la machine distante. Et cela permettra au client OpenVPN de se connecter au serveur TrueNAS CORE via le service VPN que nous venons de créer.

Cependant, puisque nous sommes sur un sous-réseau local et que sur internet directement nous ne le sommes pas, nous allons devoir transférer le port que nous utilisons à partir du routeur dans notre sous-réseau local vers ce port avant de pouvoir se connecter à distance au serveur TrueNAS.

#### b- Installation et Configuration du pare-feu Zentyal

Pour installer Zentyal, nous allons créer une machine virtuelle. Pour ce faire, nous allons nous connecter à l'interface de gestion de VMware Workstation. Ensuite nous allons dans **Files > Create a new virtual machine**. Une nouvelle fenêtre s'ouvre. Nous choisissons « **Custom (Advanced)** ». S'ouvre alors une interface de configuration. Cette interface nous permet de choisir l'image disc ISO de Zentyal à installer. Les nouvelles fenêtres qui s'affichent ensuite montrent les étapes de configuration du nom de la machine ainsi que le système d'exploitation à installer et le chemin de location de la machine virtuelle. Après avoir rempli les champs, cliquons sur **suivant**. Les interfaces qui s'affichent ensuite concernent la configuration du nombre de processeur que l'on veut utiliser pour notre machine virtuelle, la taille de la mémoire RAM et celle du disque dur. Ensuite cliquons sur « **suivant** » jusqu'à ce que

nous arrivons sur la dernière interface sur laquelle on doit cliquer sur « **Customize hardware** ». A ce niveau nous allons configurer les cartes réseaux de la machine virtuelle à créer. Cliquons ensuite sur OK et après sur terminer pour finaliser la création de la nouvelle machine virtuelle Zentyal.

Nous allons par la suite lancer la machine virtuelle où il nous sera demandé l'action qu'on veut faire. La figure suivante illustre l'interface d'installation de Zentyal :



*Figure 33: Installation de Zentyal*

Nous allons choisir « Install » et laisser l'installation se poursuivre. La figure 34 montre comment se présente l'interface du serveur Zentyal après installation :



Figure 34: Interface de Zentyal

#### c- Installation et configuration d'un environnement Jail : Nextcloud

Pour configurer un environnement jail dans TrueNAS nous avons besoin d'installer un plugin. Pour notre part, nous avons décidé d'installer comme plugin celui du Nextcloud. Pour l'installer, allons dans **Menu > Plugins > Nextcloud > Installer**. Les figures 35, 36 et 37 qui suivent illustrent son installation et sa configuration :

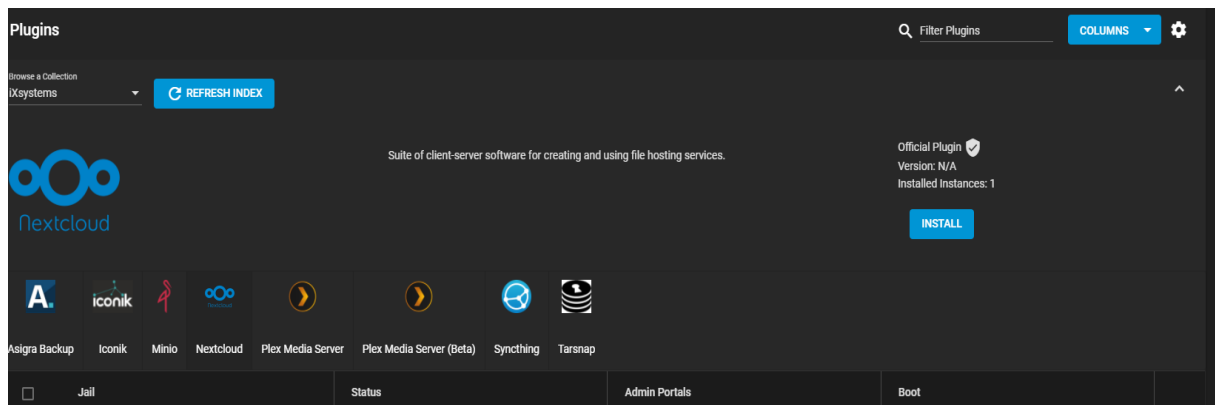


Figure 35: Installation du plugin Nextcloud

Figure 36: Configuration du plugin Nextcloud


<input type="checkbox"/>	Jail	Status	Admin Portals	Boot
<input type="checkbox"/>	 nextcloud	up	http://20.20.20.2:8282	<input checked="" type="checkbox"/>

Figure 37: Fin de l'installation du plugin Nextcloud

A présent nous allons nous connecter au serveur Nextcloud via l'adresse IP **20.20.20.2** via le port **8282**.

La figure 38 illustre l'interface de connexion et l'interface d'accueil de Nextcloud :



Figure 38: Interface de connexion de Nextcloud

A présent, notre instance Nextcloud est enfermée dans un Jail, donc les données ne sont pas directement accessibles depuis nos partages réseau. Pour faciliter le partage de nos données, il va falloir créer des points de montage et ajouter un « Stockage Externe » sur Nextcloud.

#### d- Création d'un point de montage

La première chose à faire est de créer un ou des points de montage dans notre Jail Nextcloud qui pointera vers un Dataset auxquels nous souhaitons accéder via Nextcloud.

### 3.2.3 Nouvelle architecture système d'INGENIEURS & EXPERTS

L'architecture du système est conçue afin de lui fournir une sécurité fiable et avancée. Le système est composé :

- ❖ un serveur de stockage et de sauvegarde NAS : TrueNAS CORE pour les fichiers ;
- ❖ un serveur Nextcloud comme environnement jail ;

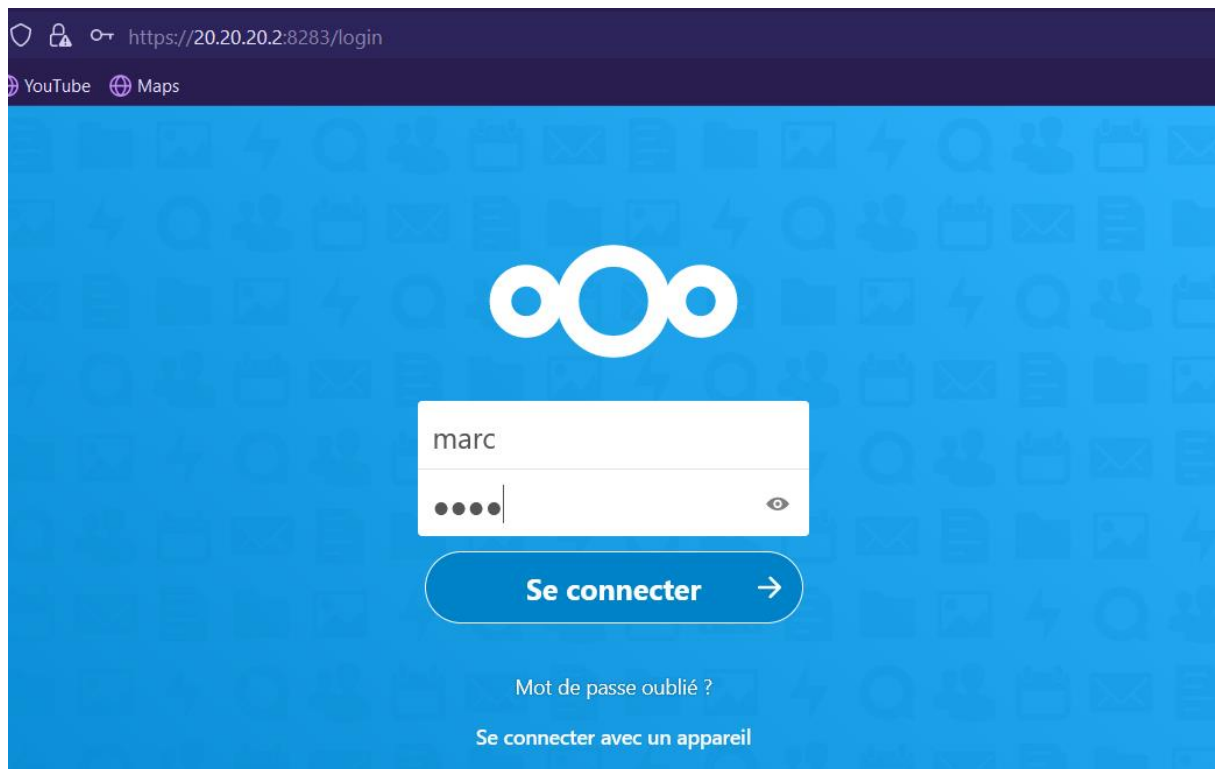
- ❖ un serveur VPN pour l'accès à distance des données ;
- ❖ un serveur Zentyal en tant que pare-feu.

### 3.3 Tests de fonctionnement

Pour effectuer les tests de fonctionnement de notre système, nous allons premièrement nous connecter à l'environnement jail (Nextcloud) avec un compte utilisateur et essayer de nous connecter au VPN et essayer d'accéder à distance aux données.

#### ❖ Connexion au Nextcloud

Pour tester l'accès à Nextcloud, nous allons nous rendre dans un navigateur web et taper dans la barre d'URL l'adresse IP du serveur comme le montre la figure ci-dessous :



*Figure 39: Connexion au Nextcloud*

#### ❖ Connexion au VPN

Pour commencer nous allons lancer le client OpenVPN Connect et essayer de nous connecter comme le montre les figures suivantes :

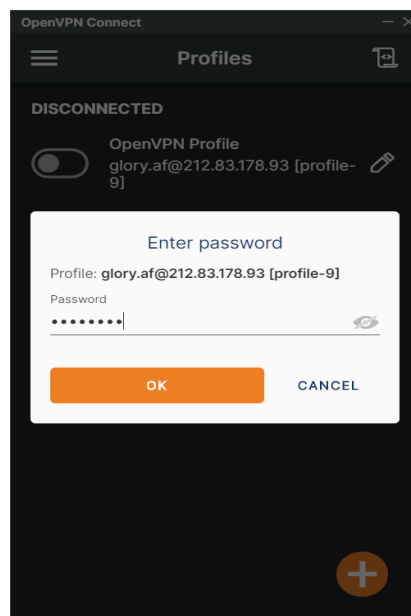


Figure 40: Connexion au VPN avec un compte utilisateur

Nous pouvons donc voir que la connexion au VPN est réussie.

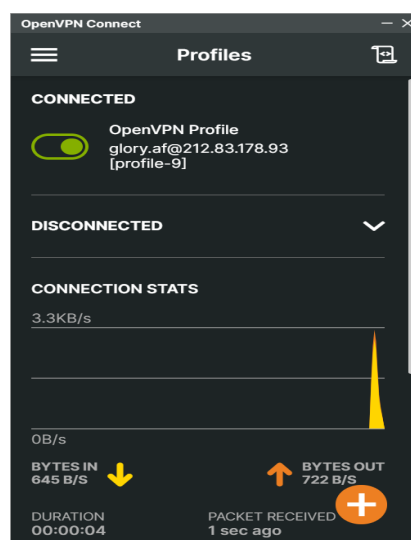


Figure 41: Illustration d'une connexion établie [3]

### 3.4 Evaluation financière

Puisque le groupe INGENIEURS & EXPERTS dispose des ressources nécessaires à la mise en place du projet, l'évaluation financière du projet a été réalisée seulement en fonction des ressources humaines.

- ❖ les ressources humaines : il s'agit des coûts liés à la formation, la maintenance et la conception et le déploiement de la solution;

Le tableau 7 présente l'évaluation financière de la mise en place des solutions retenues :



Tableau 7: Tableau des coûts liés à la mise en place de la solution

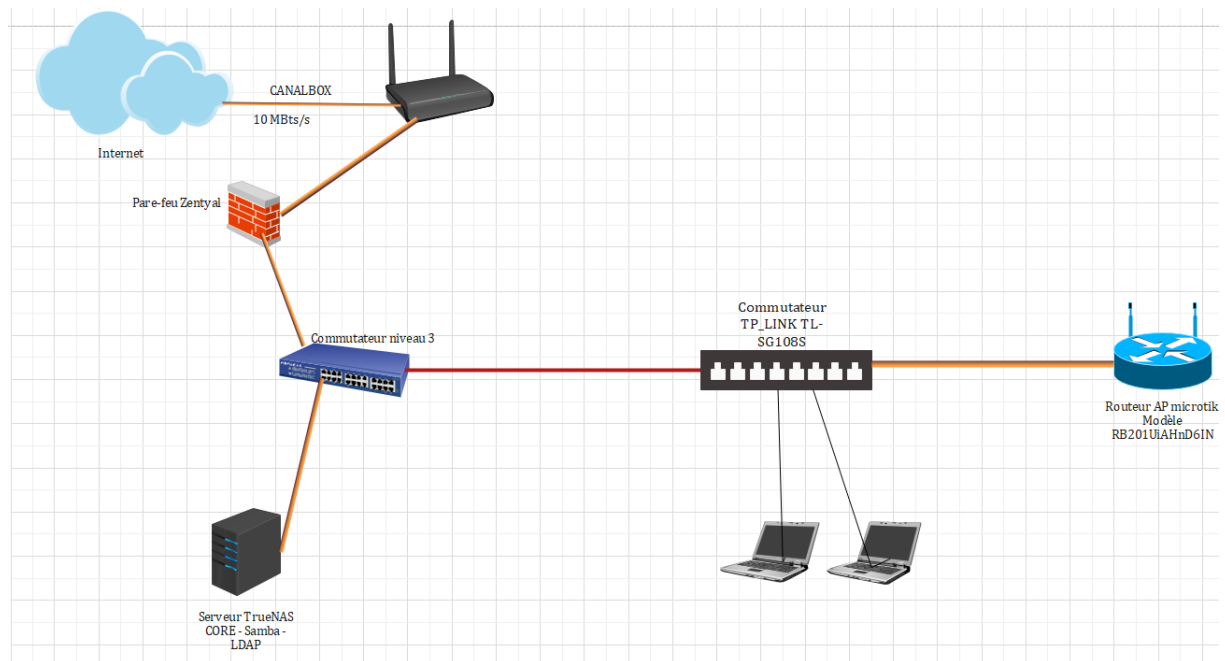
Désignation	Durée (jours)	Coût journalier (F CFA)	Nombre de personnes	Total en F CFA
Conception et déploiement de la solution	14	10 000	1	140 000
Formation	5	30 000 (par personne)	1	150 000
Maintenance	-	200 000 (forfait par an)	1	200 000
<b>TOTAUX</b>	490 000			

### 3.5 Perspective

Ce point a pour optique de proposer une nouvelle architecture réseau encore plus fiable à la structure INGENIEURS & EXPERTS. Nous proposons comme perspective à l'IE, la mise en place d'un contrôleur de domaine avec LDAP qui leur permettra de gérer encore mieux les demandes d'authentification et de contrôler les utilisateurs de leur réseau informatique. Cela améliorera également la gestion du réseau en apportant plus de souplesse dans son administration et apportera davantage de sécurité.

### 3.6 Proposition d'une meilleure architecture réseau pour l'avenir

La figure ci-dessous montre une illustration de cette architecture :



*Figure 42: Proposition de la nouvelle architecture réseau d'IE*

## PARTIE III : GUIDE D'UTILISATION

Dans la partie précédente de ce document, nous avons mis en place un système de sécurisation d'un système de stockage NAS. La présente partie « Guide d'utilisation » servira à guider les utilisateurs du système sur les manipulations requises.

Notre système de stockage aura principalement deux types d'utilisateurs :

- ❖ les administrateurs ;
- ❖ les employés.

## 1. Guide d'utilisation pour les administrateurs

Un administrateur du système de stockage NAS a pour rôle de créer des comptes VPN pour les utilisateurs du système.

### 1.1 Création d'un compte VPN

Pour créer un compte VPN, l'administrateur se connecte à l'interface d'administration d'OpenVPN en tapant dans le navigateur <https://ie.domain.com/admin>. La figure 43 illustre l'interface de connexion d'administration d'OpenVPN :

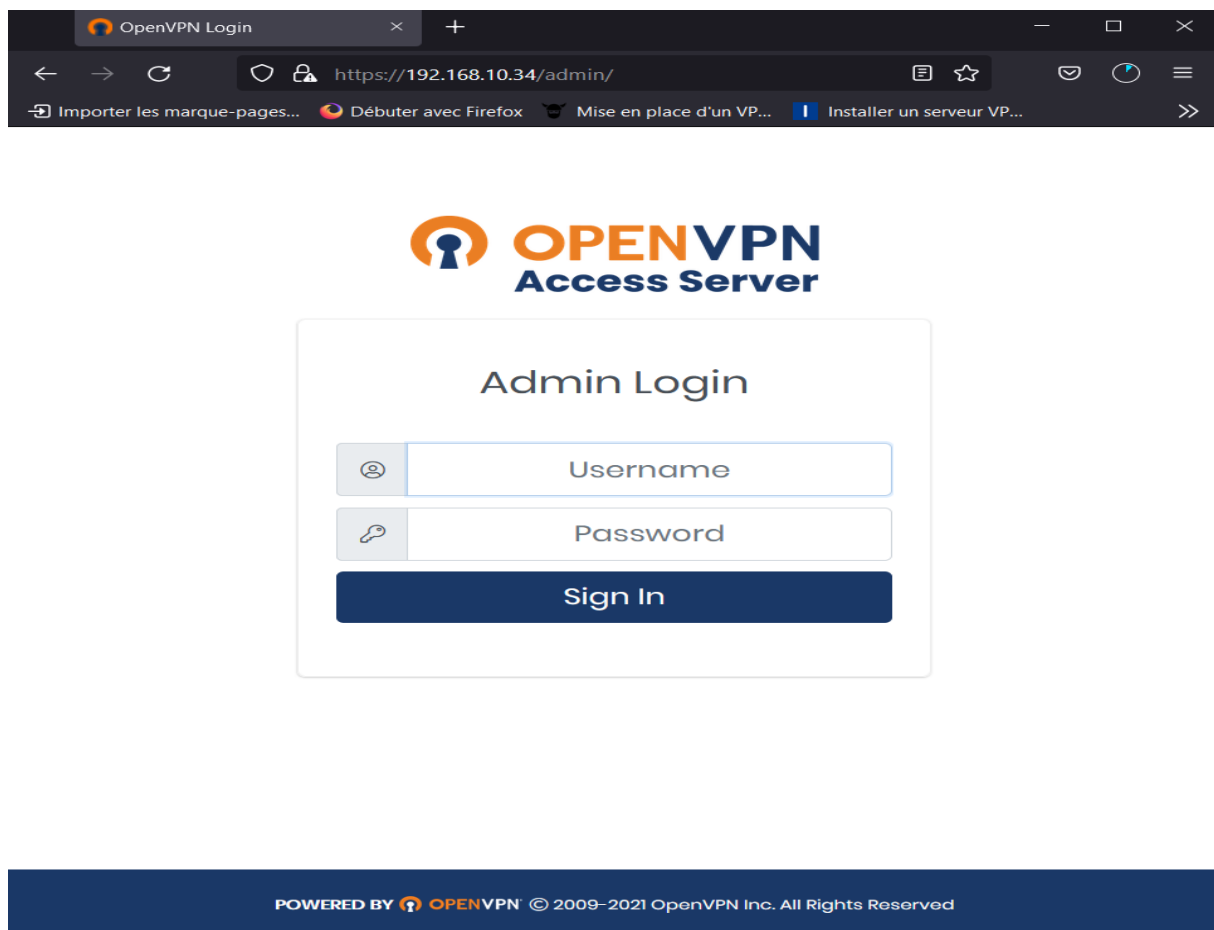


Figure 43: Interface de connexion de l'administrateur

Pour créer un utilisateur, l'administrateur se rend dans le menu « USER MANAGEMENT » > « User Permissions ». La figure suivante illustre la création d'un utilisateur VPN :

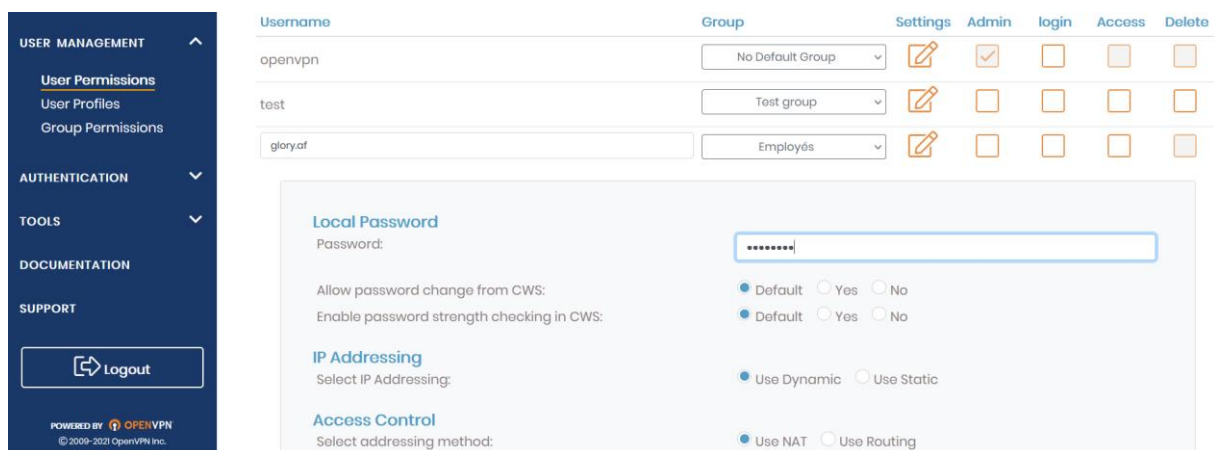


Figure 44: Création d'un utilisateur

Pour désactiver le compte d'un utilisateur, il suffit à l'administrateur de supprimer son compte VPN.

## 1.2 Gestion des utilisateurs sur le Nextcloud

Pour le Nextcloud, l'administrateur peut agir sur les utilisateurs depuis son interface d'administration comme l'indique la figure ci-dessous :

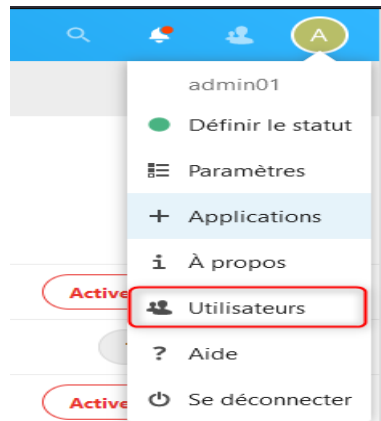


Figure 45: Procédure d'administration pour les utilisateurs Nextcloud

## 2. Guide d'utilisation pour les employés

Pour accéder aux ressources du système de stockage TrueNAS CORE en local, les employés doivent passer par le Nextcloud. Cependant, pour y accéder à distance les employés doivent passer par le VPN.

### 2.1 Connexion au serveur VPN

Pour se connecter au VPN, l'employé doit disposer du client VPN OpenVPN Connect. Pour se faire, l'employé se rend sur le site <https://ie.domain.top> . La figure suivante montre l'interface de connexion de l'employé :



Figure 46: Interface de connexion de l'employé

Il se connecte avec ses identifiants et télécharge le fichier d'installation du client OpenVPN Connect en fonction de sa plateforme comme le montre la figure qui suit :



Figure 47: Tableau de bord de connexion de l'utilisateur [3]

L'employé installe alors l'application OpenVPN Connect et l'ouvre. La figure ci-après montre l'interface d'accueil de OPENVPN Connect :

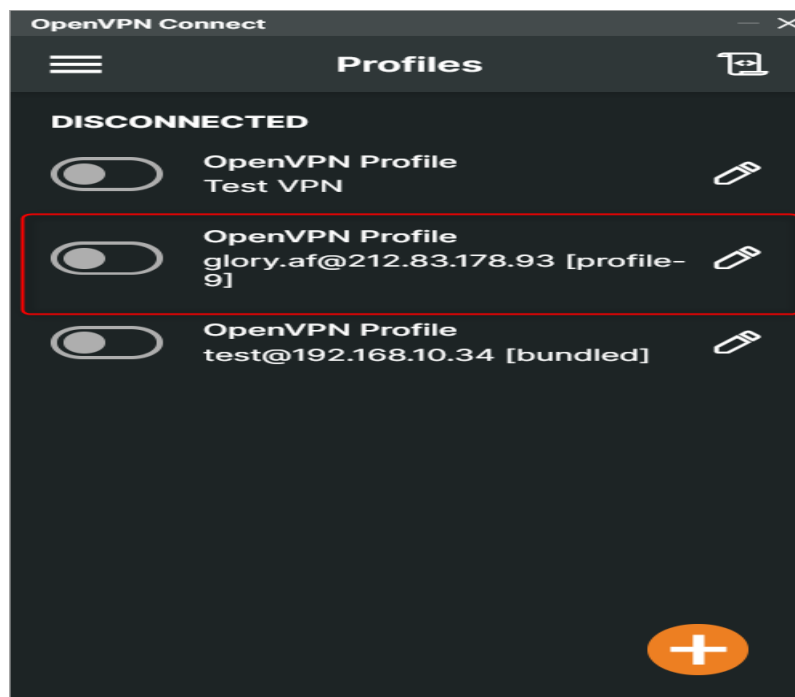


Figure 48: Interface de connexion d'OpenVPN

L'employé s'authentifie et une fois qu'il passe l'authentification, il aura une interface illustrée par la figure suivante :

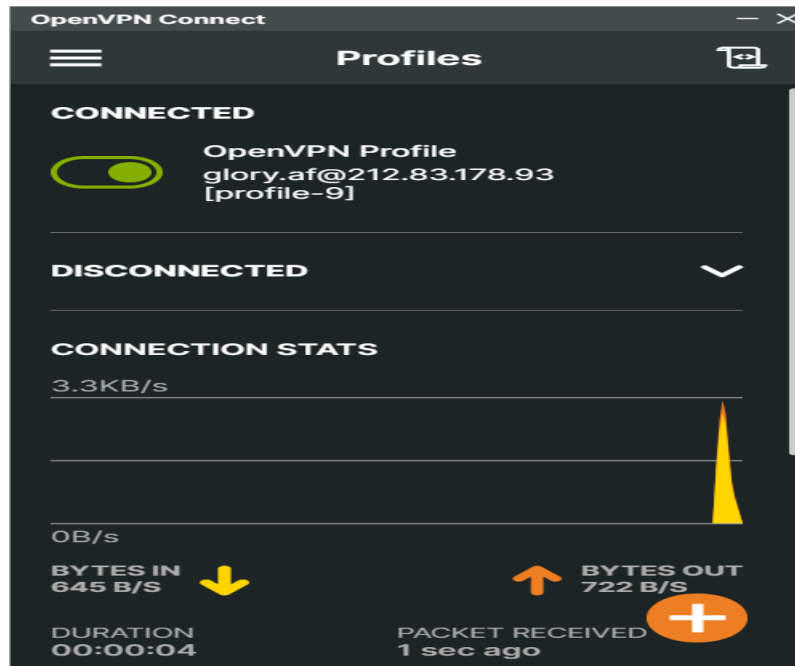


Figure 49: Interface d'OpenVPN après authentification de l'employé

## 2.2 Connexion à la solution de travail collaboratif

Pour se connecter au Nextcloud, l'employé tape dans son navigateur Internet l'URL [https://ie\\_domain.com](https://ie_domain.com). Il sera dirigé sur la page d'authentification de Nextcloud où il s'authentifie comme l'illustre la figure 50 :



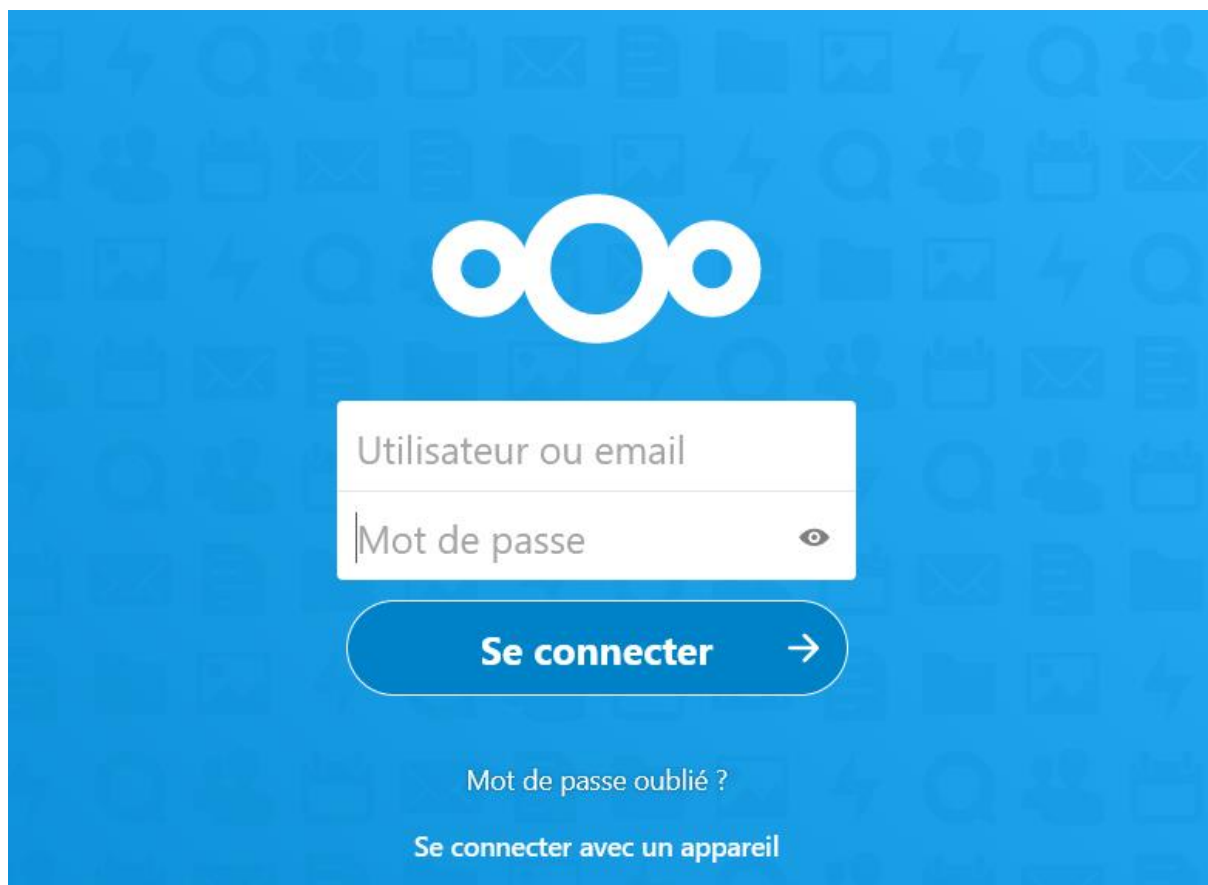


Figure 50: Page d'authentification de Nextcloud

Après s'être authentifié, l'utilisateur accède à la page d'accueil de Nextcloud. Il peut alors manipuler les fichiers sur lesquels il a les droits. La figure 51 qui suit illustre la page d'accueil de Nextcloud :

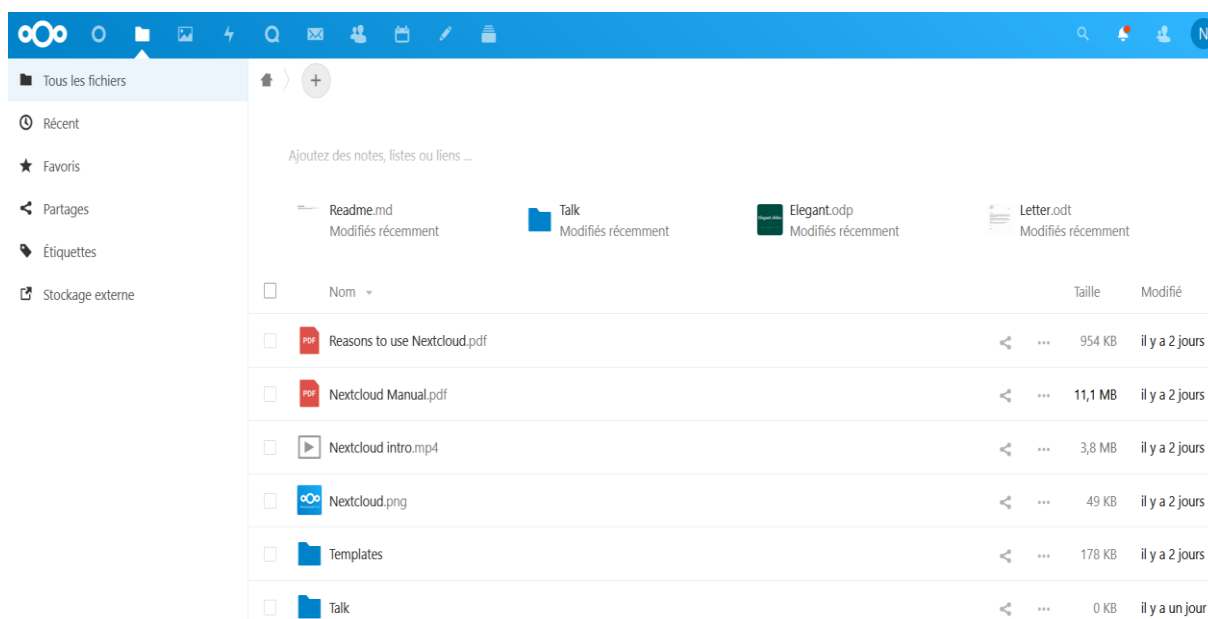


Figure 51: Page d'accueil de Nextcloud

## CONCLUSION

Ce stage de trois (03) mois effectué au sein du groupe INGENIEURS & EXPERTS nous a permis de mettre en pratique toutes nos connaissances acquises tout au long de notre parcours de trois ans de formation à l'IAI-TOGO. Pour mettre en place ce projet nous avons rencontré plusieurs difficultés et en même temps appris beaucoup de choses qui nous serviront durant toute notre carrière. Ce stage a été un moyen pour nous de nous confronter à certaines réalités du travail et de s'y préparer. Ce document composé de trois (02) parties, que sont : la partie présentations, la partie étude et réalisation du projet sont le résultat du travail que nous avons effectué au sein du groupe INGENIEURS & EXPERTS durant notre période de stage. Le résultat de notre projet est la mise en place de méthodes de sécurisation du système de stockage NAS comme un environnement jail et la mise en place d'un VPN pour les accès à distance. Ce stage a été pour nous une occasion d'acquérir de nouvelles connaissances notamment dans le domaine de sécurisation de stockage. Cependant, pour des raisons de performance, ne serait-il pas mieux de mettre en place un contrôleur de domaine afin de mieux gérer les demandes d'authentification et de contrôler les utilisateurs de leur réseau informatique ?

## BIBLIOGRAPHIE INDICATIVE

### ❖ Anciens mémoires consultés

**[1] « MISE EN PLACE D'UN SYSTEME DE GESTION DU RESEAU VIA LE WIFI IMPLIQUANT LA SURVEILLANCE, L'ALLUMAGE ET L'EXTINCTION DE TERMINAUX INFORMATIQUES ET ELECTRONIQUES » : ABLI Hodalo Rebecca (2019-2020) ;**

**[2] « GESTION DES ACCES ET DES RESSOURCES D'UN RESEAU D'UNE ENTREPRISE » : AVOYI Yaovi God's Will (2019-2020) ;**

**[3] « ETUDE ET MISE EN PLACE D'UN CLOUD HYBRIDE DE TYPE IAAS : CAS DE SOFTSOLUX » : AFIVI Daniel (2020-2021) ;**

### ❖ Notes de cours

**[4]** Administration et sécurité des systèmes (semestre 3) 2020-2021 : M. GBOKPA ;

**[5]** Administration et sécurité réseaux (semestre 3) 2020-2021 : M. ALI-MIZOU ;

**[6]** Architectures avancées des réseaux (semestre 4) 2020-2021 : Mme D'ALMEIDA ;

**[7]** Modèles et structuration des réseaux (semestre 4) 2020-2021 : Mme D'ALMEIDA.

## WEBOGRAPHIE INDICATIVE

- [8] « Le stockage en réseau, ou NAS, qu'est-ce que c'est ? » <https://www.redhat.com/fr/topics/data-storage/network-attached-storage> (consulté le 26 juin 2020) ;
- [9] « FreeNAS : Recyclez un vieux PC en NAS (Network Attached Storage) » <https://www.monpc-pro.fr/tuto/freenas-recyclez-un-vieux-pc-en-nas/> (consulté le 1 juillet 2020) ;
- [10] <https://doc.zentyal.org/en/installation.html#installation-on-top-of-ubuntu-20-04-lts-server-or-desktop> (consulté le 2 juillet 2020) ;
- [11] <https://doc.zentyal.org/en/> (consulté le 2 juillet 2020) ;
- [12] « Le RAID c'est quoi ? » <https://www.commentcamarche.net/faq/159-le-raid-c-est-quoi> (consulté le 28 juillet 2020) ;
- [13] « NAS DIY 🛠️ : COMMENT INSTALLER TRUENAS CORE ? » <https://www.youtube.com/watch?v=VquEirV-eOE> (consulté le 17 Août 2020) ;
- [14] « File.truenas/documentation » <https://github.com/truenas/documentation/find/master> (consulté le 17 Août 2020) ;
- [15] « Comment configurer votre serveur FreeNAS pour accéder à vos fichiers de n'importe où » <https://fr.tipsandtricks.com/how-set-up-your-freenas-server-access-your-files-from-anywhere-756859> (consulté le 4 septembre 2020) ;
- [16] « RAID (informatique) » [https://fr.wikipedia.org/wiki/RAID\\_\(informatique\)](https://fr.wikipedia.org/wiki/RAID_(informatique)) (consulté le 5 septembre 2020) ;
- [17] « Tuto : accéder aux données de son NAS » <https://www.justegeek.fr/tuto-acceder-aux-donnees-de-nas/> (consulté le 5 septembre 2020) ;
- [18] « Héberger un site web sur TrueNAS » <https://forums.commentcamarche.net/forum/affich-37171668-heberger-un-site-web-sur-truenas> (consulté le 11 septembre 2020) ;
- [19] « Setup OpenVPN Server on TrueNAS | 4K TUTORIAL » <https://www.youtube.com/watch?v=S8l-liQYVas> (consulté le 19 septembre 2020) ;

[20] « Comment installer Nextcloud sur TrueNAS Core 12 - Tech2Tech | News, Astuces, Tutos, Vidéos autour » <https://www.tech2tech.fr/comment-installer-nextcloud-sur-truenas-core-12/> (consulté le 19 septembre 2020) ;

[21]

[https://www.google.com/search?q=trafic+entrant+et+sortant&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjAILXO38T0AhXE4uAKHWq5CA0Q\\_AUoAXoECAEQAw&biw=1536&bih=762&dpr=1.25#imgrc=sr0Eb\\_Q9iwb16M&imgdii=1epoylty1yjgeM](https://www.google.com/search?q=trafic+entrant+et+sortant&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjAILXO38T0AhXE4uAKHWq5CA0Q_AUoAXoECAEQAw&biw=1536&bih=762&dpr=1.25#imgrc=sr0Eb_Q9iwb16M&imgdii=1epoylty1yjgeM) ;

[22]

[https://www.google.com/search?q=truenas+core+logo&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjWjYmt4MT0AhVOxhoKHRFVDmwQ\\_AUoAXoECAEQAw](https://www.google.com/search?q=truenas+core+logo&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjWjYmt4MT0AhVOxhoKHRFVDmwQ_AUoAXoECAEQAw);

[23]

[https://www.google.com/search?q=pfsense+logo&source=lnms&tbm=isch&sa=X&ved=2ahUKEwji3a-84cT0AhXRfMAKHQ49BRkQ\\_AUoAXoECAEQAw#imgrc=4zNExkVB1Zc2IM](https://www.google.com/search?q=pfsense+logo&source=lnms&tbm=isch&sa=X&ved=2ahUKEwji3a-84cT0AhXRfMAKHQ49BRkQ_AUoAXoECAEQAw#imgrc=4zNExkVB1Zc2IM);

[24]

[https://www.google.com/search?q=zentyal+logo&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjbzJvz4cT0AhWRmFwKHQncAIAQ\\_AUoAXoECAEQAw&biw=1536&bih=762&dpr=1.25#imgrc=KMWbHG-nRSCYXM](https://www.google.com/search?q=zentyal+logo&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjbzJvz4cT0AhWRmFwKHQncAIAQ_AUoAXoECAEQAw&biw=1536&bih=762&dpr=1.25#imgrc=KMWbHG-nRSCYXM);

[25]

<https://www.google.com/search?q=utilisation+de+vpn+tunnel&tbm=isch&ved=2ahUKEwi3guaNhsX0AhXT0oUKHaNaA3oQ2-cCegQIABAA#imgrc=TBgun2PTCh0KSM&imgdii=11AP0VpDK9yoHM>;

[26]

[https://www.google.com/search?q=vware+logo&tbm=isch&ved=2ahUKEwiQn5fNhsX0AhXK0YUKHVInARUQ2-cCegQIABAA&oq=vware+&gs\\_lcp=CgNpbWcQARgAMgQIABATogUIABCABD0ECAAQqz0lCAAQgAQQsQM6CwgAEIAEELEDEIMBOqYIABAFEB46BAgAEBg6BAgAEB5QiwZY2F9g3bABaAFwAHgFgAG4OIgBkJICkgERMi0xLjAuMy4zLjEuMC4yLjSYAQcQAQgQAQ&tnd3Mtd2l6LWltZ7ABAMABAQ&scclient=img&ei=SL0oYZDbIcqJlwTZzoWoAQ#imgrc=rt8wsTbEiu4jRM&imgdii=YVu\\_cxvFuNhU75M](https://www.google.com/search?q=vware+logo&tbm=isch&ved=2ahUKEwiQn5fNhsX0AhXK0YUKHVInARUQ2-cCegQIABAA&oq=vware+&gs_lcp=CgNpbWcQARgAMgQIABATogUIABCABD0ECAAQqz0lCAAQgAQQsQM6CwgAEIAEELEDEIMBOqYIABAFEB46BAgAEBg6BAgAEB5QiwZY2F9g3bABaAFwAHgFgAG4OIgBkJICkgERMi0xLjAuMy4zLjEuMC4yLjSYAQcQAQgQAQ&tnd3Mtd2l6LWltZ7ABAMABAQ&scclient=img&ei=SL0oYZDbIcqJlwTZzoWoAQ#imgrc=rt8wsTbEiu4jRM&imgdii=YVu_cxvFuNhU75M).

## TABLE DES MATIERES

	Pages
DEDICACES .....	i
REMERCIEMENTS .....	ii
AVANT-PROPOS .....	iii
SOMMAIRE .....	iv
RESUME .....	v
GLOSSAIRE .....	vi
LISTE DES FIGURES .....	vii
LISTE DES TABLEAUX .....	ix
LISTE DES PARTICIPANTS AU PROJET .....	x
INTRODUCTION GENERALE .....	1
PARTIE I : PRESENTATIONS .....	2
1.1    PRESENTATION DE L'IAI-TOGO .....	3
1.1.1    Historique de l'IAI-TOGO .....	3
1.1.2    Objectifs de l'IAI-TOGO .....	3
1.1.3    Formations à l'IAI-TOGO .....	3
1.1.4    Structure organisationnelle de l'IAI-TOGO .....	4
1.1.5    Plan de localisation de l'IAI-TOGO .....	5
1.2    PRESENTATION DU GROUPE INGENIEURS & EXPERTS .....	6
1.2.1    Statut .....	6
1.2.2    Missions .....	6
1.2.3    Activités .....	7
1.2.4    Organigramme .....	7
1.2.5    Service d'accueil du groupe INGENIEURS & EXPERTS .....	7
1.2.6    Plan de localisation .....	7
PARTIE II : ETUDE ET REALISATION DU PROJET .....	9

Chapitre 1 : Contexte de travail et approches de solutions .....	10
1.1 Etude de l'existant.....	11
1.1.1 Architecture système d'INGENIEURS & EXPERTS .....	11
1.1.2 Architecture réseau d'INGENIEURS & EXPERTS.....	11
1.2 Critique de l'existant.....	12
1.2.1 Points forts.....	12
1.2.2 Points faibles .....	13
1.3 Problématique.....	13
1.4 Intérêt du sujet .....	14
1.4.1 Objectifs.....	14
1.4.2 Résultats attendus.....	14
1.5 Méthodologie de recherches de solutions.....	14
Chapitre 2 : Généralités et documentations .....	16
2.1 Généralités sur TrueNAS CORE.....	17
2.1.1 Installation de TRUENAS CORE .....	17
2.1.2 Fonctionnement de TRUENAS CORE.....	18
2.2 Les différents outils de sécurisation du système de stockage en interne.....	18
2.2.1 Les environnement jails de TRUENAS CORE.....	18
2.2.2 Certificat SSL (Secure Socket Layer) .....	19
2.2.3 Synthèse sur les différents outils de sécurisation du système de stockage et choix de la solution .....	20
2.3 Généralités sur les technologies pare-feux .....	20
2.3.1 Pfsense.....	21
2.3.2 Zentyal .....	23
2.3.3 Synthèse sur les technologies Pare-feu.....	24
2.4 Sécurisation de l'accès à distance : Les technologies VPN.....	24
2.4.1 IPVanish .....	25
2.4.2 OpenVPN .....	26
2.4.3 Synthèse et choix de la technologie VPN adaptée .....	27
2.5 Choix des solutions adaptées .....	27
Chapitre 3 : Mise en œuvre et perspectives .....	28
3.1 Les éléments de réalisation .....	29
3.1.1 VMware Workstation.....	29
3.1.2 OpenVPN.....	30
3.2 Mise en œuvre .....	30

3.2.1	Politique de sécurité.....	30
3.2.1.1	Conditions générales d'accès aux serveurs .....	30
3.2.1.2	Accès à distance aux ressources du système de stockage TrueNAS .....	31
3.2.1.3	Sécurité des données.....	31
3.2.2	Mise en place de l'infrastructure réseau .....	31
3.2.2.1	Mise en place du serveur TrueNAS CORE.....	31
a-	Installation et configuration de TrueNAS CORE en ligne de commande	32
b-	Configuration de TrueNAS CORE sur l'interface web.....	34
3.2.2.2	Déploiement et installation du serveur VPN sur TrueNAS CORE ...	43
a-	Installation du serveur VPN OpenVPN.....	43
b-	Installation et Configuration du pare-feu Zentyal .....	47
c-	Installation et configuration d'un environnement Jail : Nextcloud .....	49
d-	Création d'un point de montage.....	51
3.2.3	Nouvelle architecture système d'INGENIEURS & EXPERTS.....	51
3.3	Tests de fonctionnement.....	52
3.4	Evaluation financière.....	53
3.5	Perspective .....	54
3.6	Proposition d'une meilleure architecture réseau pour l'avenir .....	54
<b>PARTIE III : GUIDE D'UTILISATION.....</b>		<b>56</b>
1.	<i>Guide d'utilisation pour les administrateurs.....</i>	<i>57</i>
1.1	Création d'un compte VPN .....	57
1.2	Gestion des utilisateurs sur le Nextcloud .....	59
2.	<i>Guide d'utilisation pour les employés.....</i>	<i>59</i>
2.1	Connexion au serveur VPN .....	59
2.2	Connexion à la solution de travail collaboratif .....	61
<b>CONCLUSION .....</b>		<b>63</b>
<b>BIBLIOGRAPHIE INDICATIVE.....</b>		<b>64</b>
<b>WEBOGRAPHIE INDICATIVE .....</b>		<b>65</b>
<b>TABLE DES MATIERES .....</b>		<b>67</b>



