

REPUBLIQUE DE COTE D'IVOIRE



Union-Discipline -Travail

Ministère de l'Enseignement Supérieur et  
de la recherche Scientifique (MESRS)

Université Polytechnique de Bingerville



Une Référence Internationale



Année académique : 2022/2023

## MÉMOIRE DE FIN DE CYCLE

Pour l'obtention de la  
*Licence d'Administration et Sécurité des Systèmes et des Réseaux  
Informatiques (ASSRI)*

# ETUDE ET MISE EN PLACE D'UNE DOUBLE AUTHENTIFICATION SUR LES COMPTES VPN

Présenté par :

**DIAKITE ABDOUL JUNIOR**

*En Stage du 15 Juin 2023. Au 16 Septembre 2023.*

Encadrant Académique :

**M. KOFFI ELISEE**

*Enseignant Chercheur*

Maître de Stage :

**M. IRRA BLONDE.G**

**Chef de service RSI Port Autonome d'Abidjan**

**JURY**

<b>PRESIDENT</b>		
<b>RAPPORTEUR</b>		
<b>MEMBRE</b>		

---

## DEDICACE

A ma mère

BAKAYOKO KADIDIATA

## REMERCIEMENTS :

Nos remerciements vont à l'endroit de :

Ma Grande Mère Dosso Mawa pour ses prières de bonheur ;

Mon Papa Bamba Lacina pour tout son soutien durant mon parcours académique

Mon Tuteur Dosso Abou et Ma Tutrice Ouattara Sita, ainsi que toute la famille Dosso qui m'ont accepté chez eux, et ont pris soin de moi durant mon parcours académique

Mon Oncle Bakayoko Hassan pour la bataille qu'il a menée pour me trouver un stage adéquat pour ma formation professionnelle

Mon Grand frère Bakayoko Kader qui m'a toujours aidé financièrement.

Mon Maître de Stage Irra Blonde Gervais qui m'a dit : « l'avantage que tu as aujourd'hui peut être un handicap demain » une phrase que j'ai reçue et qui a été pour moi une source d'inspiration ;

M. KOFFI Elisée, Mon encadrant académique, pour avoir accepté de me superviser, me former;

M. Soumahoro Kê, Directeur Général de l'Université Polytechnique de Bingerville ; L'ensemble du corps professoral de l'UPB, pour nous avoir formé et purement aidé tout au long de notre parcours ;

L'ensemble du personnel de l'Université Polytechnique de Bingerville, pour nous avoir accepté et formé tout au long de ces trois années d'étude universitaires ;

Les membres du jury qui ont accepté d'évaluer notre travail ;

L'ensemble du personnel du Port Autonome d'Abidjan (PAA), pour m'avoir accepté et permis de me former et de réaliser mon stage de fin de cycle dans leur local.

## AVANT-PROPOS :


Ce mémoire est le résultat d'un stage de recherche de 3 mois au sein de la Direction des Systèmes de l'Information Numérique du Port Autonome d'Abidjan afin de valider mon diplôme de licence informatique en administration et Sécurité des systèmes et des réseaux informatiques (ASSRI) effectués à l'UNIVERSITÉ POLYTECHNIQUE DE BINGERVILLE (UPB), université de sciences et technologies comportant six (6) filières principales : ASSRI, MIAGE (Méthode Informatique Appliquée à la Gestion d'Entreprise), SEA (Statistiques et Économie Appliquée), 3EA (Electronique Energie Electrique Automatique), SEG (Sciences et Economie de Gestions), SJAP (Sciences Juridique Administrative et Politique). Le mémoire est présenté conformément aux connaissances acquises au cours de notre formation universitaire et enrichit les expériences acquises au sein de la Direction des Systèmes de l'Information et du Numérique du Port Autonome d'Abidjan. Il a été construit autour d'un environnement d'apprentissage dans l'environnement de gestion des systèmes, des réseaux et sécurité. Le processus de rédaction du présent mémoire s'est amorcé en juin 2023. Ce projet s'articule autour du thème : « « ETUDE ET MISE EN PLACE D'UNE DOUBLE AUTHENTIFICATION SUR LES COMPTES VPN CAS DU PORT AUTONOME D'ABIDJAN » »

Les recherches et les interventions de mon maître de stage ont été très utiles dans la compréhension et le développement de mon thème.

## SOMMAIRE :

DEDICACE-----	I
REMERCIEMENTS -----	II
AVANT PROPOS -----	III
LISTE DES SIGLES ET ABREVIATIONS -----	V
LISTE DES FIGURES ET TABLEAUX-----	VI
INTRODUCTION -----	1
PREMIÈRE PARTIE : GÉNÉRALITÉS -----	2
CHAPITRE I : PRESENTATION GÉNÉRAL DE LA STRUCTURE D’ACCUEIL -----	3
CHAPITRE II : ASPECT THÉORIQUE DU PROJET -----	10
CHAPITRE III : ANALYSE DE L’EXISTANT -----	13
DEUXIÈME PARTIE : ÉTUDE CONCEPTUELLE -----	17
CHAPITRE I : SÉCURITÉ -----	18
CHAPITRE II : ÉQUIPEMENTS DE SECURITE -----	22
TROISIÈME PARTIE : IMPLEMENTATIONS ET RESULTATS -----	25
CHAPITRE I : IMPLÉMENTATION -----	26
CHAPITRE II : RÉSULTATS ET DISCUSSIONS -----	40
I. RÉSULTATS -----	40
II. DISCUSSIONS -----	49
III. ÉVALUATION FINANCIÈRE DU PROJET -----	49
CONCLUSION GÉNÉRALE -----	50

## LISTE DES SIGLES, ABREVIATIONS ET ACCRONYMES:



AD: Active Directory

DMVPN: Dynamic Multipoint Virtual Private Network

DNS : Domaine Name Server

DSIN : Direction des Systèmes de l'Information Numérique

LDAP: Lightweight Directory Access Protocol

MFA: Multifactor Authentication

MPLS VPN: Multiprotocol Label Switching Virtual Private Network

PAA : Port Autonome d'Abidjan

RADIUS: Remote Authentication Dial-In User Service

RSI : Réseau et Sécurité informatique

UPB : Université Polytechnique de Bingerville

VPN : Virtual Private Network

VPN IPSEC: Virtual Private Network Internet Protocol Security

VPN SSL/TLS: Virtual Private Network Secure Sockets Layer/Transport Layer Security

## LISTE DES FIGURES ET DES TABLEAUX :

FIGURE 1 : DIRECTION GENEALE DU PORT AUTONOME D'ABIDJAN-	-3-
FIGURE 2 : ORGANIGRAMME DU PORT AUTONOME D'ABIDJAN-----	-7-
FIGURE 3 : ORGANIGRAMME DE LA DIRECTION DES SYSTEMES D'INFOMATION NUMERIQUE-----	-9-
FIGURE 4 : ARCHITECTURE EXISTANTE-----	-14 -
FIGURE 5 : NOUVELLE ARCHITECTURE-----	-15-
FIGURE 6 : APERÇU SUR LES FABRIQUANTS DES PARE-FEU-----	-23-
FIGURE 7 : CONNEXION À FORTIGATE-----	-26-
FIGURE 8 : TABLEAU DE BORD FORTIGATE-----	-27-
FIGURE 9 : CREATION DE VPN -----	-28-
FIGURE 10 : RÉSEAUX DE DESTINATION-----	-28-
FIGURE 11 : CREATION DES POOLS IP SOURCES-----	-29-
FIGURE 12 : PARAMÈTRE VPN-----	-29-
FIGURE 13 : PARAMÈTRE VPN-----	-30-
FIGURE 14 : CREATION DES GROUPES-----	-30-
FIGURE 15 : AJOUT DES GROUPES-----	-31-
FIGURE 16 : UTILISATEURS VPN-----	-31-
FIGURE 17 : RÈGLES DE PARE-FEU-----	-32-
FIGURE 18 : RÈGLES DE PARE-FEU-----	-33-
FIGURE 19 : CREATION DE GROUPE-----	-34-
FIGURE 20 : CREATION D'UTILISATEUR-----	-35-
FIGURE 21 : CREATION D'UTILISATEUR-----	-36-
FIGURE 22 : CREATION D'UTILISATEUR-----	-37-

FIGURE 23 : CREATION D'UTILISATEUR-----	38-
FIGURE 24 : INTEGRATION FORTIGATE-----	38-
FIGURE 25 : INTEGRATION FORTIAUTHENTICATOR-----	39-
FIGURE 26 : TELECHARGEMENT FORTICLIENT-----	40-
FIGURE 27 : CREATION DE VPN SUR FORTICLIENT-----	41-
FIGURE 28 : CREATION DE VPN SUR FORTICLIENT-----	-
42- FIGURE 29 : TEST CONNECTIVITE-----	-
-43-	
FIGURE 30 : TEST DE CONNECTIVITE-----	44-
FIGURE 31 : PREMIÈRE PHASE D'AUTHENTIFICATION-----	45-
FIGURE 32 : DEUXIÈME PHASE D'AUTHENTIFICATION -----	46-
FIGURE 33 : MAIL DE CONFIRMATION-----	47-
FIGURE 34 : ACCÈS AU RÉSEAU DE L'ENTREPRISE-----	-
48-	
TABLEAU 1 : ÉQUIPEMENTS INFORMATIQUES DU PORT AUTONOME D'ABIDJAN (EXISTANT)-----	13-
TABLEAU 2 : PRIX DES EQUIPMENT'S-----	49-



## INTRODUCTION

Dans un monde de plus en plus connecté, la sécurité des données est devenue une préoccupation majeure pour les organisations, en particulier celles qui gèrent des informations sensibles et confidentielles. Le Port autonome d'Abidjan (PAA), en tant qu'entité stratégique et vitale pour le commerce international en Côte d'Ivoire, ne fait pas exception à cette préoccupation croissante.

Dans le contexte actuel, où les cyberattaques sont de plus en plus sophistiquées et fréquentes, il est impératif pour le Port autonome d'Abidjan (PAA) de renforcer ses mesures de sécurité afin de protéger ses infrastructures et les données de ses utilisateurs. C'est pourquoi « **« L'ETUDE ET LA MISE EN PLACE D'UNE DOUBLE AUTHENTICATION SUR LES COMPTES VPN (VIRTUAL PRIVATE NETWORK) » »** » se présente comme une solution efficace pour renforcer la sécurité de l'accès aux ressources internes.

La double authentification est essentielle pour renforcer la sécurité des comptes VPN du Port Autonome d'Abidjan (PAA) et apporte des avantages significatifs. Pour améliorer l'authentification existante, il est nécessaire de mettre en place une double authentification robuste sur les comptes VPN du PAA.

Afin de répondre à toutes ces interrogations, notre travail s'articulera autour de trois grandes parties comme suit :

- En premier lieu, nous parlerons de notre structure d'accueil.
- Notre étude conceptuelle sera en deuxième étape.
- Enfin, une dernière partie pour l'implémentation de nos résultats et le coût de notre projet associé à la démarche.

## **PARTIE I : GÉNÉRALITÉS**

## CHAPITRE I : PRESENTATION GÉNÉRAL DE LA STRUCTURE D'ACCUEIL

### I. PRÉSENTATION DU PORT AUTONOME D'ABIDJAN (PAA)



Figure 1 : Direction Générale du Port Autonome d'Abidjan

#### I.1 Historique

Située sur le golfe de Guinée, la Côte d'Ivoire possède une façade maritime de 500 kilomètres de long sur l'océan Atlantique ce qui a permis aux navigateurs Portugais, Hollandais, Français d'effectuer avec les autochtones des échanges commerciaux. Le littoral ivoirien étant devenu un centre échanges commerciaux importants, En 1897 est envisagée la construction de wharfs qui offraient plus de sécurité car sa

côte sableuse et rectiligne est soumise à la barre, phénomène de déferlement de la houle se formant à une distance de 80 à 100 mètres et qui, se brisant sur le rivage, rend les côtes particulièrement difficiles d'accès. Pendant très longtemps, tout le trafic maritime de la Côte d'Ivoire s'effectue ainsi via des rades foraines, c'est-à-dire des lieux d'ancrage mal fermés, ouverts aux vents de la mer, située aux débouchés en mer des lagunes : Assinie, Grand-Bassam, Grand-Lahou, Makey, Lagune Tiagba avec la rivière Go, Sassandra, San-Pédro. Le premier wharf est construit à Grand-Bassam en 1897, puis un autre à Grand-Bassam plus long et plus large en raison de l'augmentation du trafic, qui est mis en service en 1923. Ensuite, un troisième wharf est construit à Port-Bouët en 1931. Enfin, en 1951 est mis en service un wharf à Sassandra.

L'emplacement du Wharf de Port-Bouët a été choisi intentionnellement pour inciter toutes les installations commerciales à s'établir à Abidjan qui devait être une capitale. Ainsi, dans le but de faciliter les opérations de chargement et de déchargement sans risque, plusieurs projets de localisation du port de la Côte d'Ivoire ont été suggérés. Finalement en 1898, la mission Française conduite par le capitaine HOUDAILLE et comprenant les capitaines THOMAS et CROSSON-DUPLESSIS a proposé Abidjan à la fois comme port et tête de ligne du chemin de fer qui sera baptisé « Abidjan/Niger ». Une fois le site déterminé, il restait à percer le cordon littoral pour mettre la mer en communication avec le vaste réseau lagunaire, afin de permettre aux navires d'accéder à ces eaux calmes de la lagune Ebrié. Mais les premières tentatives entreprises en 1906 et 1907 se soldèrent par des échecs. Il s'avérait indispensable d'étudier de manière beaucoup plus approfondie le problème de cet échec.

## **I.2 Généralités**

Aujourd'hui, Grand Port Africain de commerce et de pêche, le Port Autonome d'Abidjan (P.A.A) est une société d'Etat avec un capital de Cent Millions (100.000.000.000) F/CFA). Outil moderne de développement au service de l'économie ivoirienne et instrument de coopération régionale, le PAA assure plus

de 90% des échanges extérieurs de la Côte d'Ivoire et une partie substantielle du commerce extérieur des pays de l'hinterland (Burkina Faso, Mali et Niger).

Le PAA a pu jouer et continue de jouer ce rôle dans l'économie ivoirienne et dans la sous-région grâce à une politique d'investissements rigoureusement planifiés, qui lui a permis de disposer d'infrastructures et de superstructures adaptées aux différents trafics, ce qui en fait aujourd'hui l'un des ports les mieux équipés et les plus performants d'Afrique Subsaharienne.

Pour les cinq (05) prochaines années, ce sont plusieurs centaines de milliards de FCFA qui seront investis pour la réalisation d'infrastructures de soutien qui serviront à l'amélioration du port actuel.

### **I.3 Missions et Objectifs**

Le port autonome d'Abidjan a une mission de service public qui consiste en :

- L'exploitation et l'entretien des installations portuaires,
- La gestion du patrimoine immobilier et domanial,
- La réalisation des travaux de construction, d'extension, d'amélioration, de renouvellement et de dragage,
- La coordination des activités de tous les services publics et privés concernant l'exploitation du port,
- La gestion administrative et comptable de l'ensemble des éléments formant le domaine public portuaire et matériel ferroviaire,
- Le suivi de la gestion de l'exploitation concédées,
- La réalisation de toutes opération d'exploitation rattachées aux activités portuaires notamment le remorquage, l'aconage, l'entreposage, la manutention avec possibilité de les concéder à des sociétés appelées à exercer ces opérations y compris celle de transit, d'avitaillement et de consignation devant préalablement recevoir un agrément des services compétents,

- L'accomplissement de toutes opérations industrielles, commerciales, mobilières, immobiliers et financières se rattachant à son objet ou de nature à favoriser le développement de ses activités.

### **Objectifs**

Les grands objectifs du Port Autonome d'Abidjan sont :

#### **Par rapport à l'économie nationale :**

- Poursuivre de manière résolue la politique d'aménagement du PAA visant à accroître sa capacité d'accueil au niveau des infrastructures (accès, quais, aires de stockage) afin de lui permettre de faire face à l'acoissement rapide du trafic induit par la politique et les objectifs de croissance économique du gouvernement,
- Accueillir à l'horizon des cinq prochaines années, un trafic de 20 Million de tonnes, et se préparer à recevoir à moyen terme des porte-conteneurs de 2.000 à 3.000 TEU,
- Adapter l'exploitation au nouvel environnement commercial et technologique afin de créer des conditions visant à faire du PAA un véritable centre de service, ce qui le classerait dans la catégorie des ports de la 3<sup>ème</sup> génération ;
- Créer les conditions d'une concurrence saine entre les opérateurs portuaires

#### **Par rapport à l'environnement international**

- Maintenir et consolider le PAA dans la position de leader incontesté dans la sous-région pour le trafic en transit
- Renforcer le rôle et la position d'Abidjan en tant que principal port de transbordement de la sous-région

#### I.4 Organigramme du Port Autonome d'Abidjan

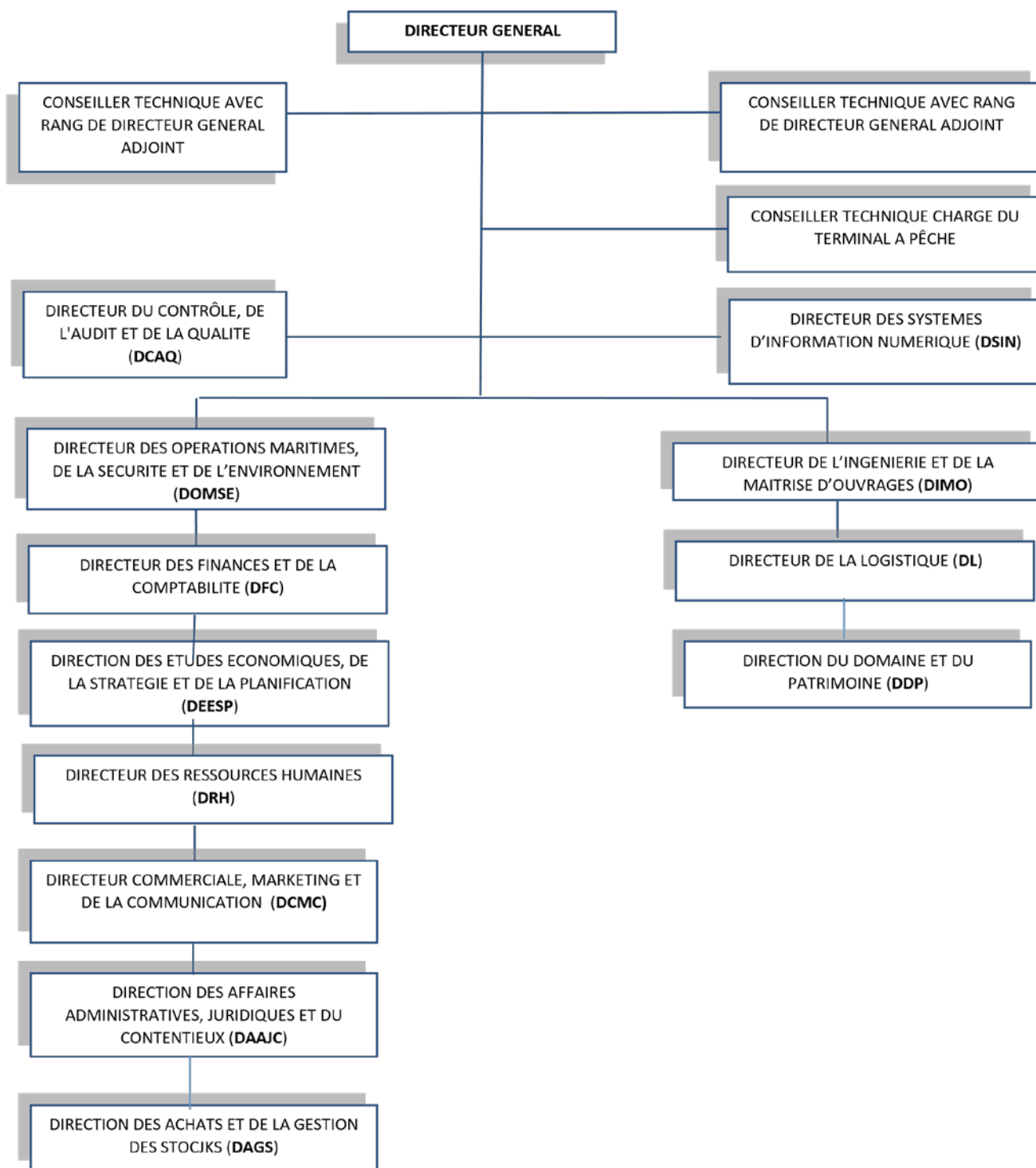


Figure 2 : Organigramme du Port Autonome d'Abidjan



## **II. PRÉSENTATION DE LA DIRECTION DES SYSTÈMES D'INFORMATION NUMÉRIQUE (DSIN)**

### **II.1 Missions et Attributions de la Direction des Systèmes d'Information Numérique (DSIN)**

En sa qualité d'outil d'aide à la décision, des missions et attributions sont assignées à la direction des Systèmes de l'Information Numérique.

Il s'agit d'entre autres de :

#### **Missions**

- Permettre aux Directions métiers de l'Entreprise de mettre en œuvre la stratégie définie par la Direction Générale,
- Contribuer à la compétitivité de l'entreprise en qualité de support à la stratégie d'entreprise
- Déterminer l'orientation technologique de l'information et de la communication
- Contribuer à faire baisser ou maîtriser les coûts d'exploitation ;
- Contribuer à la productivité ou à la valeur ajoutée de l'Entreprise ;
- Contribuer au développement de l'activité portuaire ou/et à offrir de nouveaux services à nos opérateurs économiques et maritimes.

#### **Attributions**

- Assurer la sécurité et le contrôle des systèmes d'information
- Assurer le développement et le management des systèmes d'information
- Assurer les services et les infrastructures du réseau informatique, l'Intranet, de l'Extranet et de l'Internet de l'entreprise
- Bâtir une stratégie informatique et en assurer l'application
- Assurer la qualité des services à travers les outils informatiques



## II.2 Organigramme de la Direction des Systèmes d'Information Numérique (DSIN)

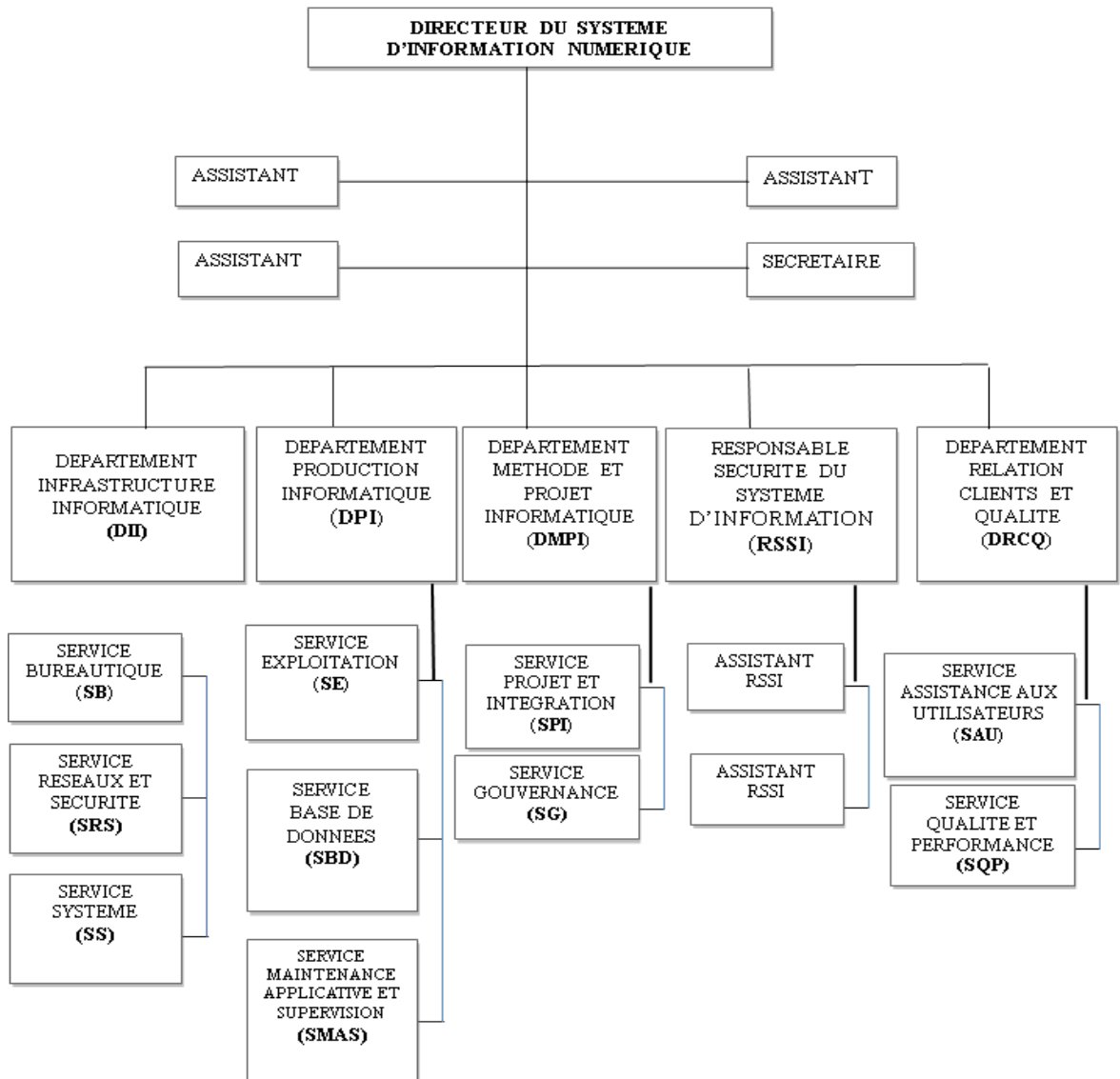


Figure 3 : Organigramme de La Direction des Systèmes d'Information Numérique

## CHAPITRE II : ASPECT THÉORIQUE DU PROJET

Dans ce deuxième chapitre de notre première partie, il est question pour nous d'orienter notre projet dans un contexte. Cela nous permettra de mieux comprendre la situation de l'entreprise afin de dégager la problématique, fixer notre objectif et choisir une démarche afin d'actualiser notre projet.

### I. CONTEXTE

Le Port Autonome d'Abidjan, en Côte d'Ivoire, est conscient de l'importance de sécuriser l'accès à ses comptes VPN (Virtual Private Network), qui sont utilisés par les employés pour accéder à distance aux systèmes et aux données sensibles. Actuellement, le port utilise une méthode d'authentification unique basée sur un nom d'utilisateur et un mot de passe. Cependant, compte tenu de l'évolution constante des menaces et de la nécessité de renforcer la sécurité, le Port Autonome d'Abidjan envisage une étude approfondie et la mise en place d'une double authentification pour améliorer le niveau de protection de ses comptes VPN (Virtual PrivateNetwork).

L'objectif principal de cette initiative est d'ajouter une couche supplémentaire de sécurité en exigeant que les utilisateurs fournissent non seulement un nom d'utilisateur et un mot de passe, mais également une deuxième forme d'identification lors de la connexion à distance aux comptes VPN. Cette mesure vise à réduire les risques d'attaques par hameçonnage, de vols d'identifiants et d'accès non autorisés aux systèmes du Port autonome d'Abidjan

### II. PROBLEMATIQUE

Il est essentiel de garantir la sécurité des comptes VPN (Virtual Private Network) utilisés au sein du Port Autonome d'Abidjan. Actuellement, une méthode d'authentification unique basée sur un nom d'utilisateur et un mot de passe est utilisé pour accéder à ces comptes. Cependant, cette approche présente

Des limitations en termes de sécurité, ce qui expose le port à des risques potentiels tels que la compromission des identifiants et les accès non autorisés. Afin de

renforcer la sécurité et de prévenir de telles situations, il est nécessaire d'envisager l'implémentation d'une double authentification sur les comptes VPN. Ainsi, la problématique centrale de cette étude est la suivante : Comment améliorer l'authentification existante en mettant en place une double authentification robuste sur les comptes VPN du Port Autonome d'Abidjan ?

### **III. OBJECTIFS ET DÉMARCHE**

#### **III.1 Objectifs**

Le but de ce projet est de renforcer la sécurité des comptes VPN (Virtual Private Network) et de prévoir les difficultés auxquelles le Port autonome d'Abidjan pourrait faire face à long terme. Cela permettra la mise en œuvre d'actions et de paramètres techniques, de sorte que son infrastructure IT soit toujours capable de répondre à de multiples demandes simultanément.

Les objectifs propres à ce projet sont les suivants :

- Renforcer la sécurité : l'objectif principale est d'améliorer la sécurité des comptes VPN (Virtual Private Network) en ajoutant une couche supplémentaire d'authentification. La double authentification réduira les risques de compromission des identifiants et les accès non autorisés assurant ainsi une meilleure protection des systèmes et des données sensibles du Port autonome d'Abidjan
- Prévenir les attaques par hameçonnage : La mise en place d'une double authentification contribuera à prévenir les attaques de phishing et les tentatives de vol d'identifiants. En exigeant une seconde forme d'identification, telle qu'un token ou un code à usage unique, les utilisateurs seront mieux protégés contre les techniques d'ingénierie sociale utilisées dans les attaques d'hameçonnage.
- Améliorer la conformité aux normes de sécurité : En mettant en place une double authentification, le Port Autonome d'Abidjan pourra renforcer sa conformité aux normes et réglementations de sécurité en vigueur. Cela peut

inclure des exigences spécifiques telles que celles imposées par les organismes de réglementation ou les partenaires commerciaux.

- Accroître la confiance des utilisateurs : En adoptant des mesures de sécurité supplémentaires, telles que la double authentification, le port démontre son engagement envers la protection des informations et la confidentialité des données. Cela renforce la confiance des utilisateurs dans les systèmes du port et leur assure que leurs informations personnelles et professionnelles sont sécurisées.
- Assurer la continuité des opérations : En renforçant la sécurité des comptes VPN, le Port Autonome d'Abidjan s'assure de la continuité des opérations en minimisant les interruptions potentielles causées par des accès non autorisés ou des activités malveillantes. La double authentification contribue à maintenir l'intégrité des systèmes et la disponibilité des ressources nécessaires aux opérations du port.

### **III.2 Démarche**

Pour mener à bien notre projet et pour répondre efficacement aux besoins de l'entreprise nous avons tenu un échange avec le responsable projet, l'administrateur réseau et sécurité afin d'obtenir la vision recherchée. Il est ressorti de ces échanges que le Port autonome d'Abidjan veut parvenir à une meilleure sécurité pour les comptes VPN de ses utilisateurs afin de garantir le bon état de leurs ressources.

## **IV. Cahier de Charge**

L'objectif du projet est de proposer une solution plus sécurisée avec des équipements adéquate qui pourront permettre aisément une communication sécurisée entre les utilisateurs et les ressources de l'entreprise grâce à des comptes VPN. Les couts et les besoins nécessaires pour la mise en place réseau de la solution et le serveur convenant.

## CHAPITRE III : ANALYSE DE L'EXISTANT

Dans la présente section, nous analyserons et vérifierons les processus et solutions informatiques existants en proposant une innovation.

### I. RECEUIL D'INFORMATIONS

#### I.1 Equipements

Dans le cadre de notre recherche sur l'existant de notre projet au Port Autonome d'Abidjan nous avons eu à échanger avec le chef de département de la RSI (Réseau et Sécurité Informatique) et à visiter la salle serveur pour voir les équipements qui y sont avec le chef de service de la RSI (Réseau et Sécurité Informatique). Et nous avons constatés que le Port Autonome d'Abidjan dispose de nombreux équipements et tous sont de haute gamme tel des switches de distributeurs Huawei et Cisco, Nutanix pour les appliances d'infrastructure hyper convergée, des serveurs Web Apache et NGINX, un serveur de messagerie Microsoft exchange server, des équipements de distribution de donnée internet MTN et ORANGE, Zabbix pour la supervision, des routeurs Mikrotik pour le wifi, et des pare-feu FortiGate de Fortinet pour le contrôle des trafics entrant et sortant avec d'autres services intégrés, un serveur Wallix qui permet de contrôler et gérer les mots de passe et les identifiants.

#### I.2 Inventaires des Périphériques Existants

Equipements	Rôle
FortiGate 601e	Sécurise le réseau Contrôle le trafic réseau
Wallix	Sécurise les comptes à un haut niveau de privilège élevé
Serveurs	Centralise les ressources

Tableau 1 : Équipements informatiques du Port Autonome d'Abidjan (existant)

## II. ANALYSES ET CRITIQUES

### II.1 Constat général

D'après notre étude et collecte d'informations nous comprenons que le réseau du Port Autonome d'Abidjan (PAA) est un générateur de données pour ses employés qui se connectent aux ressources de l'entreprise. Le Port Autonome d'Abidjan dispose (PAA) de plusieurs locaux techniques pour ses équipements de gestion réseau, il utilise un pare-feu FortiGate pour gérer les trafics internes et externes et aussi grâce à ce pare-feu les employés peuvent se connecter à distant aux ressources de l'entreprise grâce à un compte VPN crée par les administrateurs à parti de ce pare-feu.

### II.2 Analyses et Critiques de l'Existant

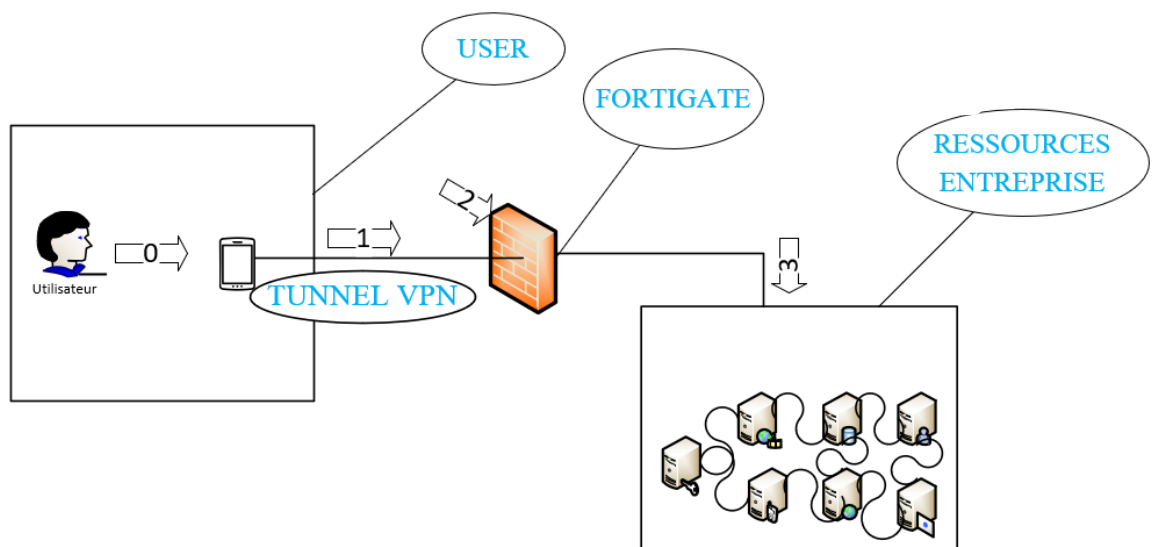


Figure 4 : Architecture Existante

D'après nos observations, le Port Autonome d'Abidjan (PAA) utilise un pare-feu pour gérer les trafics entrants et sortants, mais cela ne se limite par qu'à ça le pare-feu à d'autre fonctionnalité que de gérer les trafics tel que la création des comptes VPN le routage et aussi d'autre services.

A partir de leurs smartphones ou laptop d'où est installé un FortiClient Les utilisateurs du Port Autonome d'Abidjan (PAA) utilisent une connexion VPN et cette connexion VPN passe par le pare-feu pour accéder aux ressources de

l'entreprise, pour rappel un VPN est une connexion sécurisée dans un réseau non sécurisée.

Lorsque l'utilisateur essaie d'accéder aux ressources de l'entreprise à partir de son smartphone ou laptop il le fait à partir d'une connexion VPN et cette connexion VPN est redirigée vers le pare-feu, il puisse aussi dans la base de donnée Wallix afin de voir quel type d'utilisateur veut accéder aux ressources, par la suite le pare-feu fera une vérification afin que l'utilisateur ait accès aux ressources de l'entreprise, si le nom de l'utilisateur ainsi que le mot de passe sont corrects alors le pare-feu autorise l'accès aux ressources de l'entreprise.

Cependant, avec cette unique authentification le Port Autonome d'Abidjan ne peut pas garantir une bonne sécurité optimale pour leurs ressources stockées sur les serveurs, elle peut être confrontée à des risques potentiels tels que la compromission des identifiants et les accès non autorisés, les attaques par hameçonnage et les tentatives de vol d'identifiant.

### III. ÉBAUCHE DE LA SOLUTION

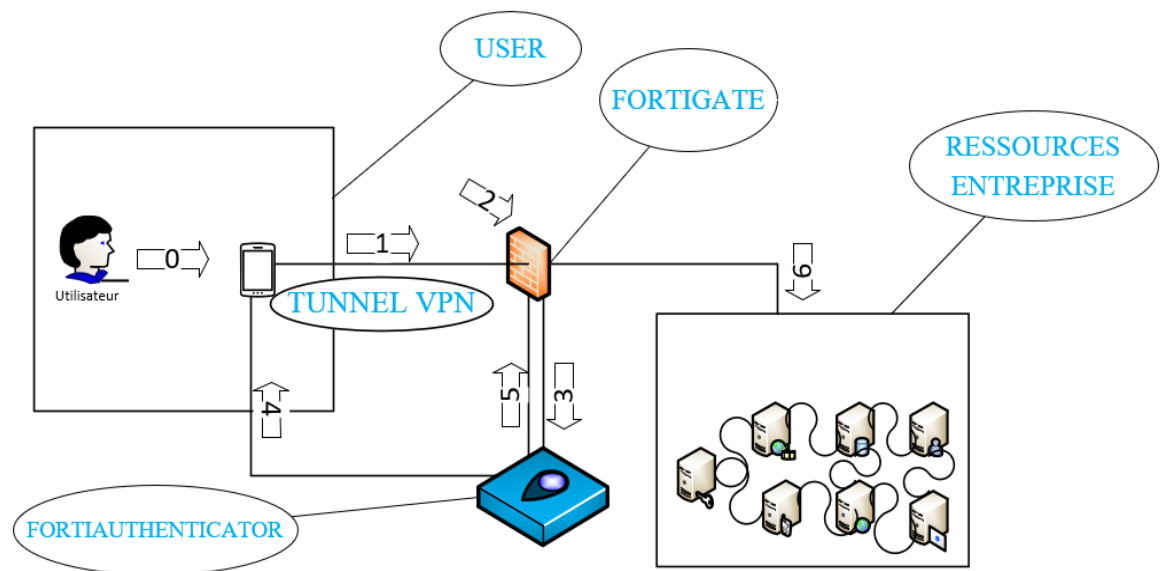


Figure 5 : Nouvelle Architecture

Au cours du reste de nos travaux, il serait sage de mettre en œuvre une solution qui réponde à nos analyses et critiques. En d'autres termes mettre

en place un système de sécurité ayant un taux de protection optimale qui permettra au Port Autonome d'Abidjan (PAA) de garantir une connexion sécurisée entre les utilisateurs et les ressources de l'entreprise.

Cette solution devra prendre en compte la gestion des utilisateurs et des groupes afin de les départager à travers le pare-feu FortiGate qui fait déjà partir des équipements existants, un FortiAuthenticator qui va servir à faire la double authentification sur les comptes VPN des utilisateurs du Port Autonome d'Abidjan à partir d'un mail.

Avec le pare-feu FortiGate l'entreprise pourra bénéficier d'un environnement sécurisé, permettant ainsi une communication entre les utilisateurs et les ressources en interne à travers des connexion VPN. Aussi, réduire le risque commercial avec plusieurs mesures de sécurité intégrées. IL pourra faire évoluer l'entreprise et son infrastructure pour atteindre une grande échelle de disponibilité en matière de services.

En somme, il a été question de présenter l'entreprise ainsi que ses besoins. Dans la suite de notre étude, nous parlerons des aspects que nous allons utiliser pour garantir une meilleure approche pour la sécurité sur les comptes VPN au Port autonome d'Abidjan.



## **PARTIE II : ÉTUDE CONCEPTUELLE**

## CHAPITRE I : SÉCURITÉ

### I. GÉNÉRALITÉ SUR LES AUTHENTIFICATIONS

#### I.1 Définition de l'Authentification

L'authentification est le processus permettant de vérifier l'identité d'un utilisateur ou d'un système informatique pour accéder à des ressources, des données ou des fonctionnalités spécifiques. Elle constitue un élément fondamental de la sécurité des systèmes et est largement utilisée dans de nombreux domaines, tels que les systèmes d'exploitation, les applications en ligne, les services bancaires, les réseaux sociaux, etc.

L'authentification se base sur certains principes (ce que l'on connaît, ce que l'on possède, ce que l'on est.)

#### I.2 Les Facteurs d'Authentification

Il existe 3 (trois) facteurs d'authentifications dans le processus d'autorisation d'accès à des ressources bloquées et sécurisées à savoir :

- **Facteur mémoriel** : une information que l'utilisateur a mémorisée et que lui seul connaît (un mot de passe, un nom)
- **Facteur matériel** : une information que l'utilisateur possède et enregistrée dans un support (une clé USB, badge d'identification).
- **Facteur corporel** : une information qui caractérise l'utilisateur avec une empreinte qui lui est propre (reconnaissance faciale, empreinte digitale)

#### I.3 Authentification à Unique Facteur

L'authentification à unique facteur, également connue sous le nom d'authentification à un seul facteur (Single-Factor Authentication en anglais), est une méthode d'authentification qui repose sur un seul facteur pour vérifier l'identité d'un utilisateur lors de la connexion à un système ou une application.

Quelques exemples d'authentification à facteur unique

- Authentification par mot de passe : L'utilisateur fournit un nom d'utilisateur et un mot de passe pour accéder à un compte ou une application.
- Authentification par identifiant biométrique : L'utilisateur fournit une empreinte digitale, une reconnaissance faciale, une reconnaissance de l'iris ou toute autre caractéristique biométrique unique pour s'authentifier.

L'authentification unique facteur présente des limites en termes de sécurité. Si un attaquant parvient à obtenir le mot de passe de l'utilisateur, il peut accéder au compte ou au système sans autres obstacles. Les mots de passe peuvent être faibles, partagés entre plusieurs comptes, ou facilement devinés, ce qui augmente les risques de compromission.

#### **I.4 Authentification à Multi-Facteurs (MFA)**

L'authentification à multi-facteurs (MFA) est une méthode de sécurité qui renforce le processus d'identification en exigeant que les utilisateurs fournissent au moins deux formes d'authentification différentes lors de leur connexion à un système ou une application.

Quelques exemples d'authentification à multi-facteurs

- Authentification par mot de passe et code à usage unique : L'utilisateur doit fournir un mot de passe ainsi qu'un code à usage unique envoyé sur son smartphone via une application ou un SMS.
- Authentification par badge d'identification et empreinte digitale : L'utilisateur doit fournir à la fois son badge d'identification et permettre le scan d'empreinte digitale pour vérifier son identité.

L'authentification à multi-facteurs offre un niveau de sécurité supérieur par rapport à l'authentification basée sur un seul facteur, car même si un facteur est compromis, l'accès au système ou à l'application reste protégé par les autres facteurs d'authentification. Cela réduit considérablement les risques de vol d'identifiants, de piratage de compte et de violations de données.

## II. GÉNÉRALITÉS SUR LES VPN

### II.1 Définition des VPN

Les VPN (Virtual Private Networks) sont des solutions de réseau privé virtuel qui permettent à des utilisateurs ou à des réseaux distants de se connecter de manière sécurisée à un réseau privé via Internet ou un autre réseau public.

### II.2 PRINCIPES DES VPN

Le principe des VPN (Virtual Private Networks) est de permettre une connexion sécurisée et chiffrée entre un utilisateur ou un réseau distant et un réseau privé. Un VPN crée un tunnel virtuel privé à travers un réseau public, tel qu'Internet, en encapsulant les données dans des paquets chiffrés, assurant ainsi la confidentialité et l'intégrité des informations échangées.

Il existe deux grandes familles de VPN (Virtual Private Network) qui offrent différentes fonctionnalités et utilisations.

Nous avons la famille des VPN d'accès à distance (Remote Access VPN) et la famille des VPN Site-to-Site (ou VPN Inter Site)

- ❖ VPN d'accès à distance (Remote Access VPN) : Cette famille de VPN permet aux utilisateurs individuels de se connecter à un réseau privé à distance, généralement depuis leur domicile ou lorsqu'ils sont en déplacement. Il offre un accès sécurisé aux ressources du réseau interne de l'entreprise.

Quelques types de VPN d'accès à distance (Remote Access VPN)

- VPN basé sur le client : Dans ce type de VPN, un logiciel client VPN est installé sur l'appareil de l'utilisateur, tel qu'un ordinateur portable, un smartphone ou une tablette. Le logiciel établit une connexion sécurisée avec le réseau privé via Internet, permettant à l'utilisateur d'accéder aux ressources internes.
- VPN SSL/TLS (Secure Sockets Layer/Transport Layer Security) : Utilise les protocoles SSL/TLS pour établir une connexion sécurisée entre le client

et le serveur VPN. Les VPN SSL/TLS sont souvent utilisés pour fournir un accès à distance sécurisé aux applications Web via un navigateur.

- VPN IPsec (IP Security) : L'IPsec est un protocole de sécurité largement utilisé pour établir des connexions VPN sécurisées. Il offre un ensemble de protocoles et d'algorithmes de chiffrement pour garantir la confidentialité, l'intégrité et l'authenticité des données.
- ❖ VPN Site-to-Site (ou VPN Inter Site) : Cette famille de VPN est utilisée pour connecter de manière sécurisée des réseaux locaux distincts situés dans des emplacements géographiquement différents. Il crée un tunnel sécurisé entre les réseaux, permettant aux données de circuler de manière confidentielle entre les sites. Les VPN de site à site sont couramment utilisés par les entreprises ayant des succursales, des bureaux régionaux ou des sites distants, leur permettant de partager des ressources, des données et de maintenir une connectivité réseau sécurisée.

Quelques types de VPN Site-to-Site (ou VPN Inter Site)

- MPLS VPN :(Multi Protocol Label Switching) est une technologie de réseau qui permet de créer des VPN site à site en utilisant des étiquettes (labels) pour acheminer efficacement les paquets de données. Les réseaux MPLS VPN sont souvent utilisés par les entreprises pour établir des connexions sécurisées et fiables entre leurs sites distants.
- DMVPN (Dynamic Multipoint VPN) : Le DMVPN est une technologie qui permet d'établir des VPN site à site de manière dynamique. Il offre une connectivité transparente entre les sites distants sans nécessiter de configuration statique préalable.
- VPN basé sur le cloud : Les VPN basés sur le cloud utilisent des services cloud pour établir des connexions sécurisées entre les réseaux des sites distants. Ils offrent une solution pratique et évolutive pour connecter des sites géographiquement dispersés, sans nécessiter d'infrastructures matérielles dédiées.

## CHAPITRE II : ÉQUIPEMENTS DE SECURITE

### I. PARE-FEU

#### I.1 Définition

Un firewall (ou pare-feu) est un matériel ou un logiciel utilisé pour protéger un réseau local des intrusions extérieures. Il agit comme une barrière de protection et de sécurité empêchant la fuite de certaines informations en dehors du réseau informatique. Il permet de gérer, de contrôler, d'analyser, et de sécuriser le réseau de l'entreprise.

#### I.2 Quelques Pare-Feu

La figure ci-dessous nous présente un classement sur les fabricant détenant les meilleurs pare-feu réseau au monde.

Nous avons les Leaders Fortinet, Palo Alto Networks, Check Point Software Technologies qui dominent actuellement le marché.

Ensuite viennent Challengers tel que Cisco, Alibaba Cloud et Juniper qui se situent juste après les Leaders.

Par la suite nous avons les Niche Players Microsoft, Amazon Web Service et SonicWall qui font moins parler d'eux sur le marché.

Enfin viennent en dernière position les Visionnaires Barracuda Hillstone Networks et Sangfor Technologies eux ils sont très peu connus sur le marché par rapport aux Niche Players qui sont un peu plus connus



Source: Gartner (December 2022)

Figure 6 : Aperçu sur les Fabricants de Pare-Feu

## II. SERVEUR D'AUTHENTIFICATION

### II.1 Définition

Un serveur d'authentification, également connu sous le nom de serveur d'authentification centralisée, est un système informatique qui gère et vérifie les informations d'identification des utilisateurs lorsqu'ils tentent de se connecter à un réseau, à une application ou à des ressources spécifiques. Le serveur d'authentification joue un rôle clé dans le processus d'authentification en vérifiant l'identité des utilisateurs et en autorisant leur accès aux systèmes appropriés.

## II.2 Quelques Serveurs d'Authentification

- LDAP (Lightweight Directory Access Protocol) : LDAP permet de rechercher, de modifier ou d'authentifier d'importants volumes de données, d'informations et d'éléments dans des services d'annuaires distribués.
- AD : (Active Directory) est un service de gestion des identités et des accès développée par Microsoft. Il est largement utilisé dans les environnements Windows pour la gestion centralisée des utilisateurs, des groupes, des ordinateurs et des ressources réseau
- RADIUS : (Remote Authentication Dial-In User Service) est un serveur d'authentification largement utilisé pour l'authentification, l'autorisation et la gestion des comptes d'utilisateurs à distance. Il est principalement utilisé pour les connexions réseau telles que les connexions VPN, les connexions d'accès à distance et les connexions d'accès Internet.
- FORTIAUTHENTICATOR : est une solution d'authentification développée par Fortinet, un fournisseur de solutions de cybersécurité renommé. FortiAuthenticator est conçu pour renforcer la sécurité des accès aux réseaux et aux applications en ajoutant une couche supplémentaire de vérification de l'identité des utilisateurs.



## **PARTIE III : IMPLEMENTATIONS ET RESULTATS**

## CHAPITRE I : IMPLEMENTATIONS

Cette section constituera à présenter les étapes de configurations de notre pare-feu FortiGate et de notre serveur d'authentification fortiAuthenticator pour la création des comptes VPN et la mise en place de la double authentification sur les comptes.

### I. CONFIGURATION DU FORTIGATE

FortiGate est le pare-feu réseau le plus déployé au monde, offrant des performances de sécurité et une veille sur les menaces inégalées misant sur l'IA, ainsi qu'une visibilité complète et une convergence de la sécurité et du réseau.

Par défaut pour accéder à l'interface de FortiGate on utilise l'adresse 192.168.1.99 ou 192.168.1.100 sur le port management, mais pour plus de sécurité nous avons édité un nouveau port avec une autre adresse et nous avons désactivé le port management.

La capture ci-dessous nous montre un aperçu sur l'interface de connexion du FortiGate, par défaut pour se connecter au FortiGate on entre comme username (Admin) et sans un mot de passe mais pour plus de sécurité nous avons créés un compte administrateur.

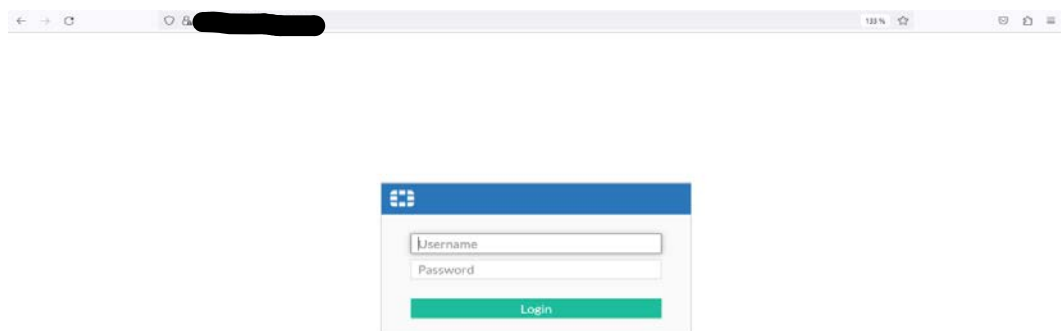


Figure 7 : Connexion a Fortigate

La capture ci-dessous nous montre un ensemble de vue et de services sur le tableau de bord de notre pare-feu FortiGate de Fortinet.

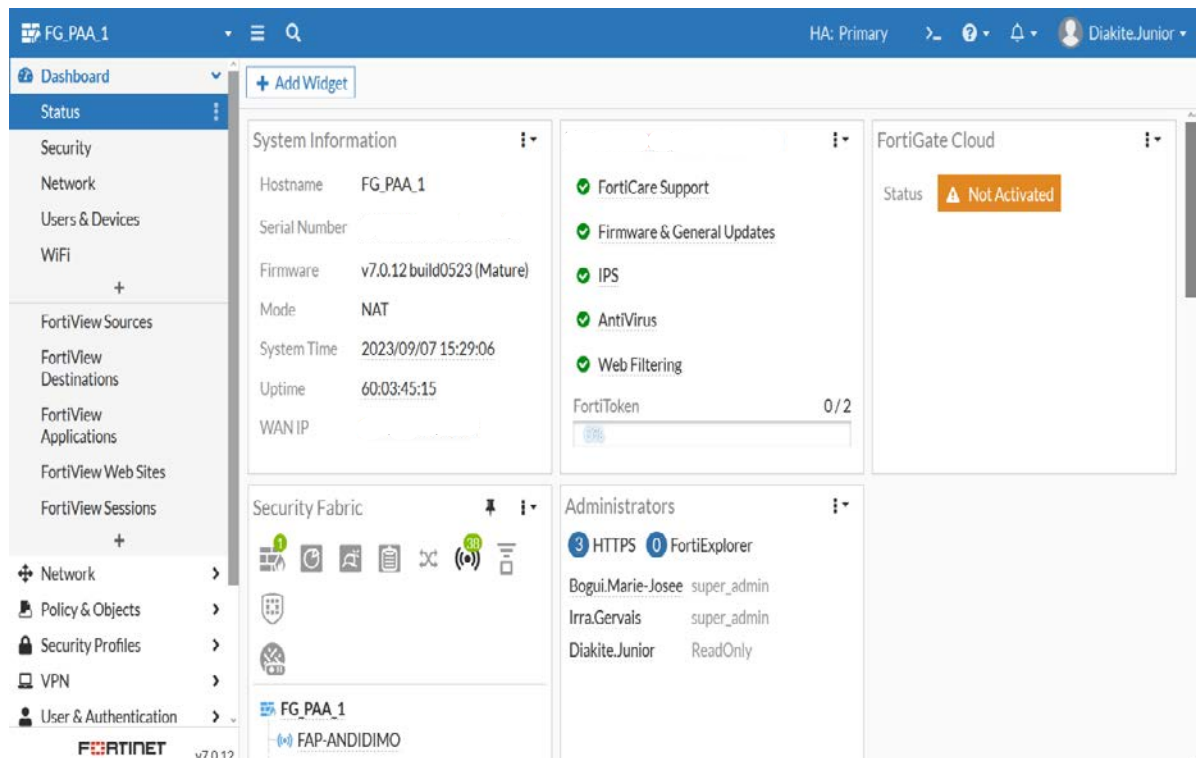


Figure 8 : Tableau de Bord Fortigate

Par la suite nous allons mettre en place notre VPN sur le FortiGate afin de permettre aux utilisateurs distants de se connecter au réseau de l'entreprise en toute sécurité, pour le fait nous allons nous rendre dans la partie VPN, ensuite on clique sur SSL-VPN Portal pour la création de notre VPN.

Nous avons nommé notre VPN comme suit tunnel-access et nous avons limité une seule connexion à la fois pour les utilisateurs afin d'établir une sécurité optimale.

On active le mode tunnel, le split tunneling ou tunnel fractionné est une fonction VPN qui va diviser le trafic internet en deux parties une partie via un tunnel de réseau privé crypté, et l'autre via un tunnel séparé sur le réseau ouvert.

Généralement, le tunnel fractionné vous permet de choisir les applications à sécuriser et celles qui peuvent se connecter normalement sans passer par un serveur VPN.

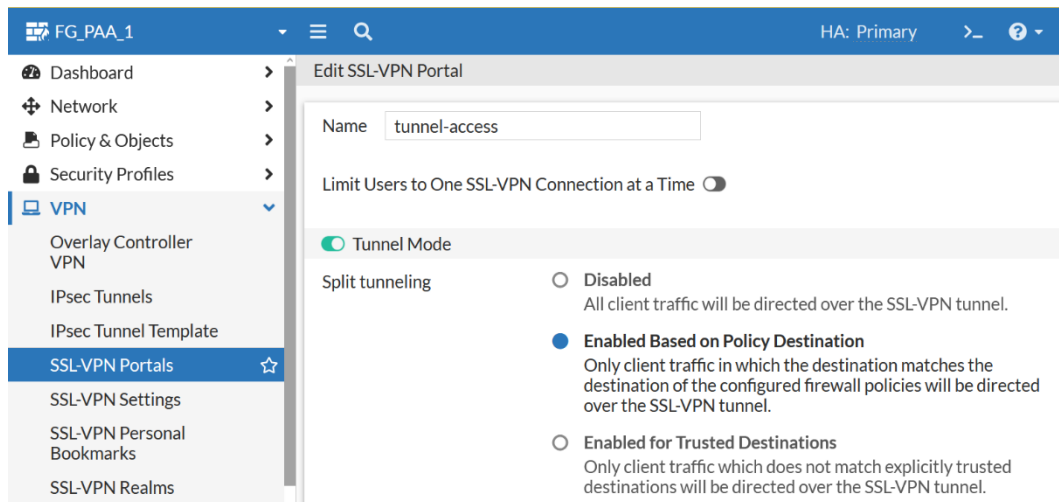


Figure 9 : Création de VPN

La capture ci-dessous nous montre tous les réseaux de destinations que les utilisateurs peuvent atteindre en toute sécurité grâce au VPN que nous mettons en place.

Source IP pools est un mécanisme qui permet de définir une adresse IP unique ou une plage d'adresses IP à utiliser comme adresse source pour la durée de la session. Ces adresses assignées sont utilisées à la place de l'adresse IP assignée à l'interface de FortiGate

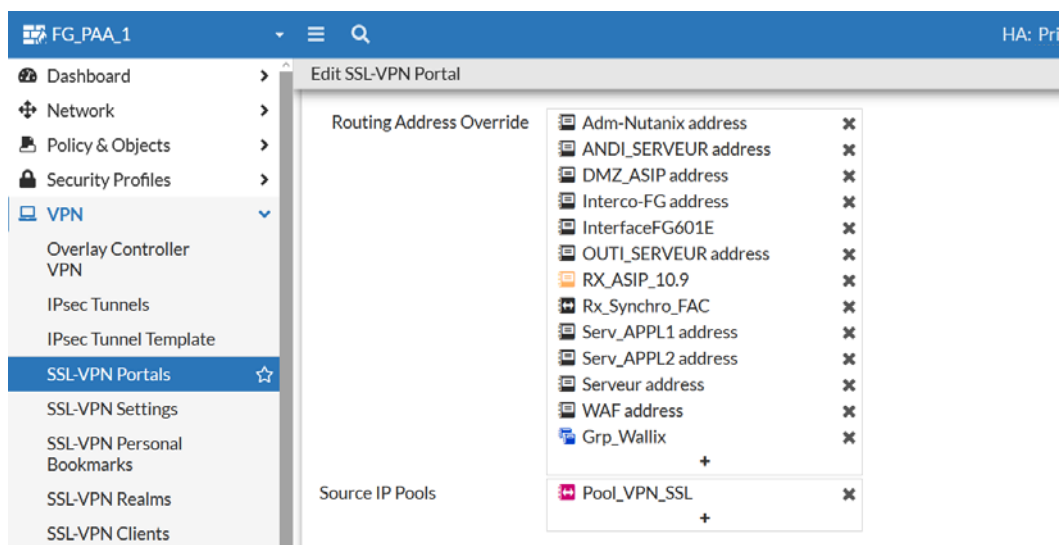


Figure 10 : Réseaux de Destination

La capture ci-dessous nous montre comment nous avons édité notre IP source pools

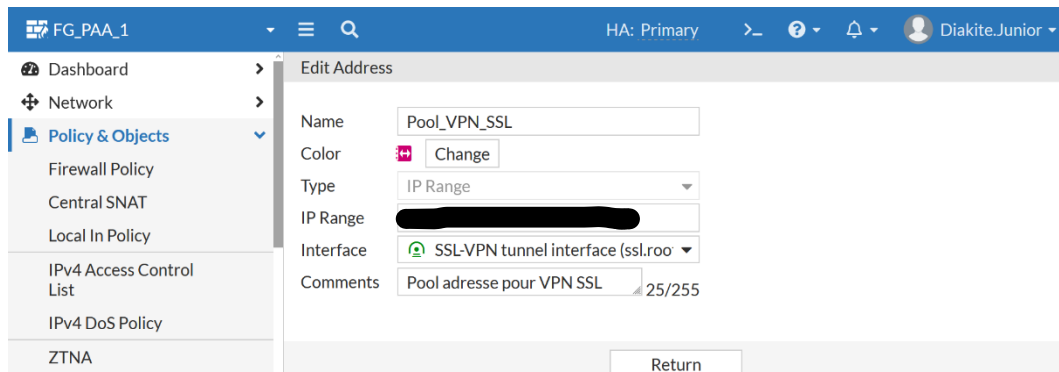


Figure 11 : Création Des Pools IP Sources

Après avoir créé notre VPN, nous allons maintenant configurer quelques paramètres pour cela nous allons nous rendre dans la rubrique SSL-VPN Settings.

Une fois dans les paramètres, nous allons activer d'abord SSL-VPN ensuite ajouter les interfaces d'écoutes ainsi que le port d'écoute que nous avons modifié pour plus de sécurité et aussi ajouter un certificat déjà créer.

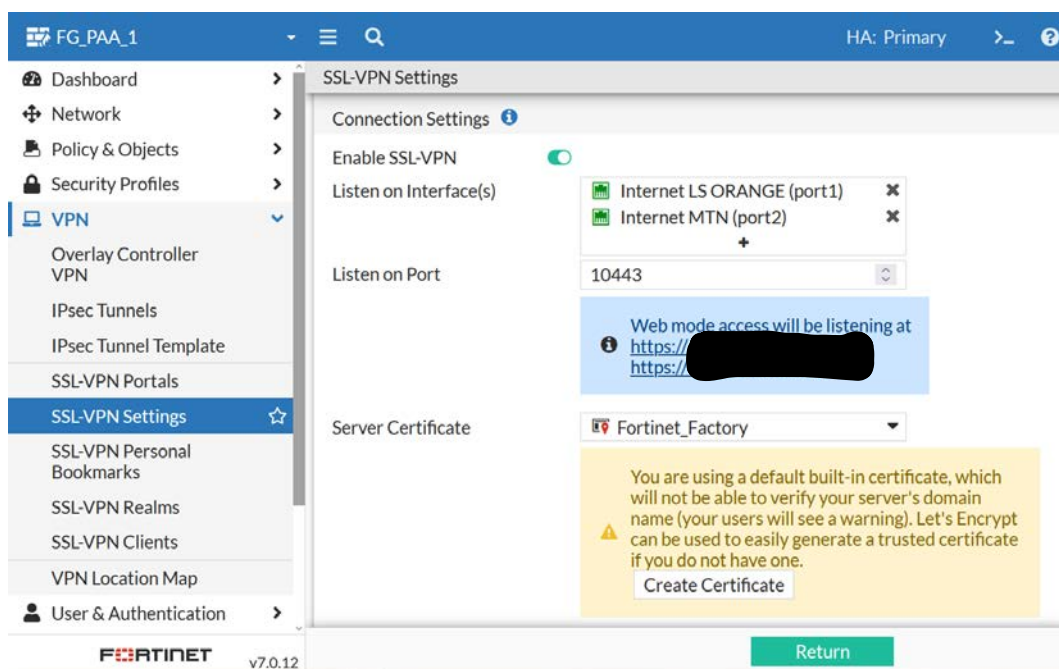


Figure 12 : Paramètre VPN

Nous avons autorisé l'accès à n'importe quelle machine, nous avons aussi défini un temps lorsqu'il n'y a pas d'activité au-delà de 300 secondes l'utilisateur sera déconnecté automatiquement et aussi nous avons spécifié la plage d'adresse que les machines client devront utiliser pour établir leur connexion ainsi que les serveurs DNS pour la résolution des noms.

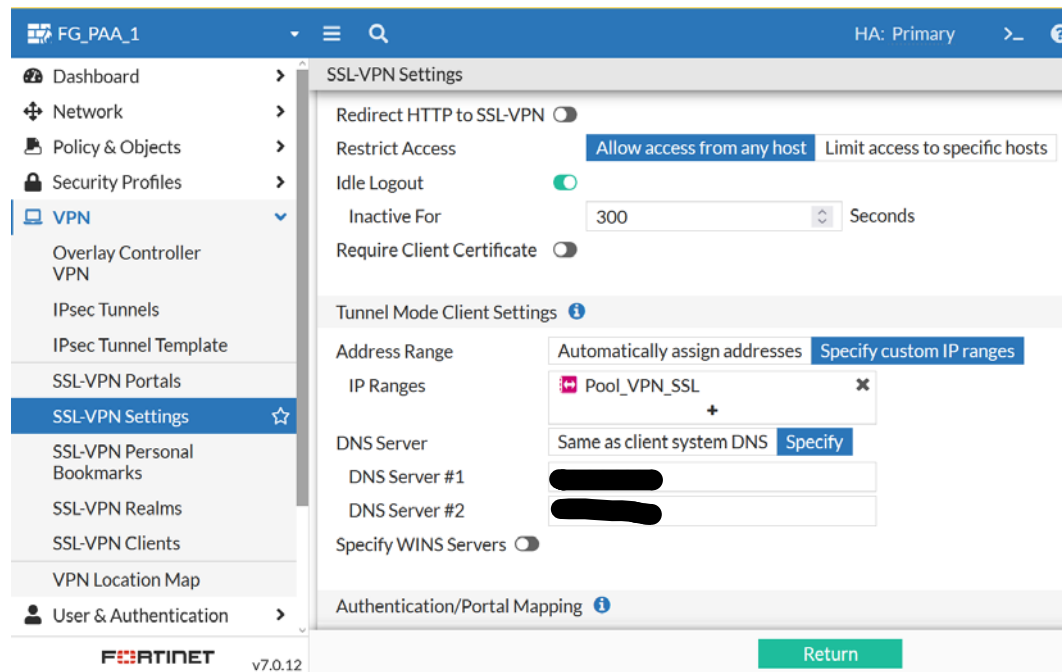


Figure 13 : Paramètre VPN

Après avoir fini de paramétrer notre VPN nous allons créer deux groupes afin d'ajouter les différents utilisateurs dans les groupes, nous avons créé deux catégories de groupe une catégorie pour les utilisateurs distants et une autre catégorie pour les utilisateurs locaux.



Figure 14 : Création de Groupe

Une fois les groupes créés nous allons revenir dans les paramètres de notre vpn pour y ajouter les groupes afin que les utilisateurs soient intégrés dans les groupes correspondants

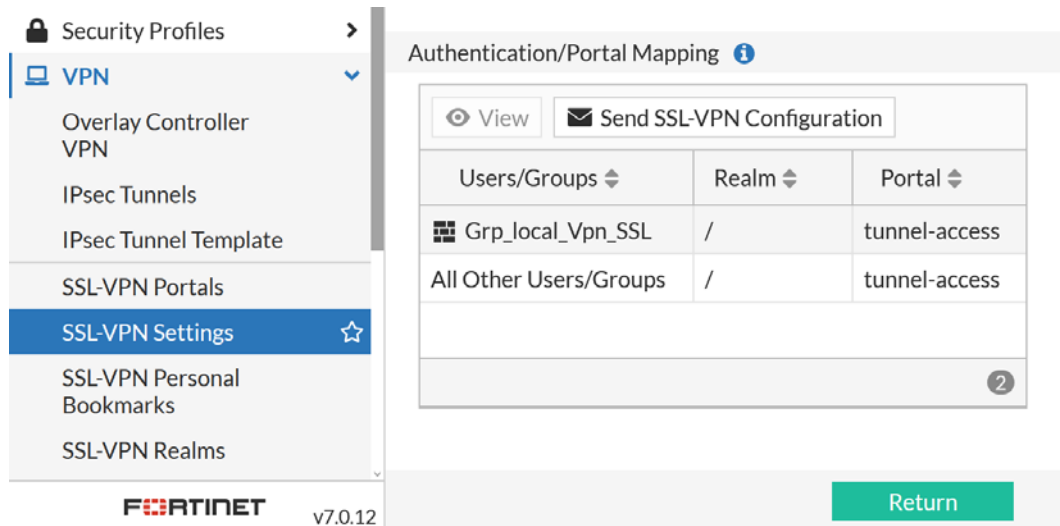


Figure 15 : Ajout des Groupes

La capture ci-dessous montre un ensemble d'utilisateurs qui utilise les connexions VPN afin de se connecter au réseau de l'entreprise en toute sécurité.

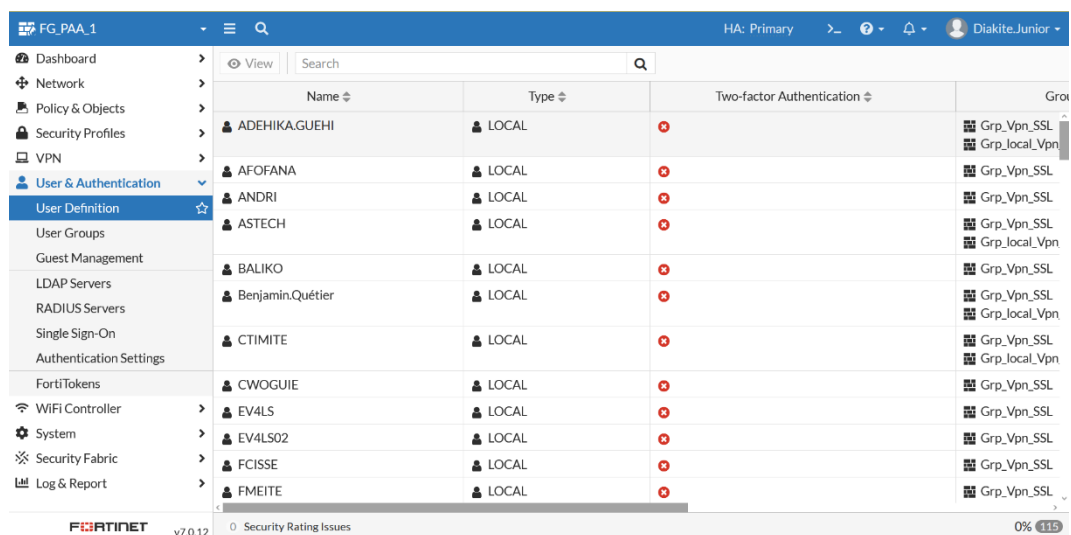


Figure 16 : Utilisateurs VPN

Après avoir paramétrer notre VPN nous allons définir quelques règles de communication de notre VPN aux ressources de l'entreprise.

Pour le fait nous allons nous rendre dans Policy and Objects puis dans firewall Policy et par la suite nous créons les règles de communications maintenant.

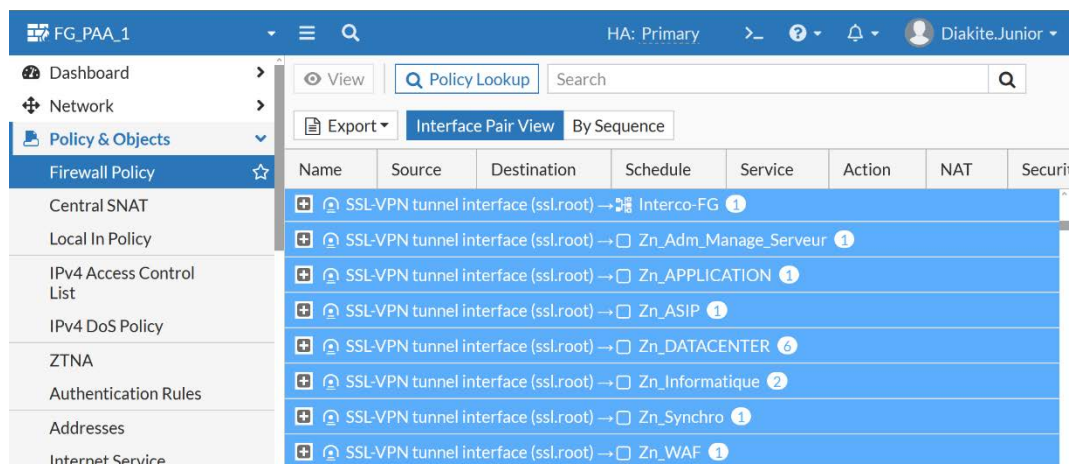


Figure 17 : Règles de Pare-Feu

La capture ci-dessous nous présente un exemple de règle que nous avons établi entre la connexion VPN et les applications internes de l'entreprise



Figure 18 : Règles de Pare-Feu

Après avoir terminé la création de notre VPN ainsi que de ses paramétrages à partir de notre pare-feu FortiGate nous allons maintenant implémenter une double authentification sur les comptes VPN pour les utilisateurs afin de garantir une meilleure sécurité.

## II. CONFIGURATION DU FORTIAUTHENTICATOR

FortiAuthenticator est un produit développé par Fortinet, une société connue pour fournir des solutions de cybersécurité. FortiAuthenticator est une plateforme de gestion des identités et des accès (IAM) qui offre une gamme de fonctionnalités



pour améliorer la sécurité et rationaliser les processus d'authentification au sein d'une organisation.

Par défaut pour accéder à l'interface de FortiAuthenticator on utilise l'adresse 192.168.1.99 ou 192.168.1.100 sur le port management, mais pour plus de sécurité nous avons édité un nouveau port avec une autre adresse et nous avons désactivé le port management, par défaut pour se connecter au FortiAuthenticator

On entre comme username (Admin) et sans un mot de passe mais pour plus de sécurité nous avons créés un compte administrateur.

Après avoir fini de paramétrer notre Fortiauthenticator nous allons créés deux groupes afin d'ajouter les différents utilisateurs dans les groupes, nous avons créés deux catégories de groupe une catégorie pour les utilisateurs distant et une autre catégorie pour les utilisateurs locaux, les groupes que nous allons maintenant créés doivent être identiques à ceux créés auparavant dans le FortiGate avec les mêmes attributs et valeurs.

Pour la création des groupes nous allons nous rendre dans la rubrique User Management puis l'option User Groups et ont remplis les différents champs.

Nous allons configurer la partie RADUIS Attributes cela va nous permettre de mieux faire l'intégration entre FortiGate et Fortiauthenticator pour la l'échange d'information entre les deux équipements.

Pour notre test nous allons utiliser le groupe VPN local

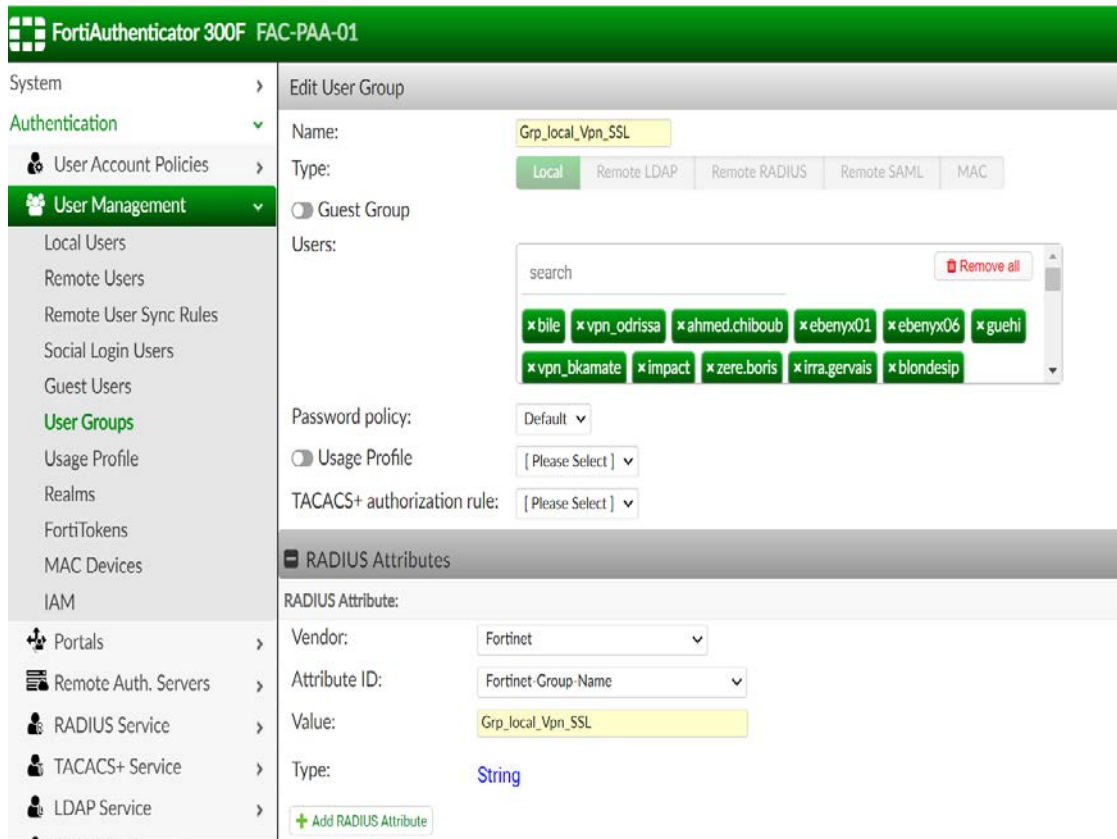


Figure 19 : Création de Groupe

Une fois les groupes créés nous allons revenir dans User Management et se rendre dans Local Users pour créer un utilisateur local pour notre test afin de se rassurer que la double authentification puisse faire effet.

FortiAuthenticator 300F FAC-PAA-01

System > Create New Local User

Authentication >

User Account Policies >

User Management >

Local Users

Remote Users

Remote User Sync Rules

Social Login Users

Guest Users

User Groups

Usage Profile

Realms

FortiTokens

MAC Devices

IAM

Portals >

Remote Auth. Servers >

RADIUS Service >

TACACS+ Service >

LDAP Service >

Username:

Password creation:

Password:

Password confirmation:

☒ Allow RADIUS authentication

☐ Force password change on next logon

Role

Role:

Account Expiration

☐ Enable account expiration

IAM

Account:

Figure 20 : Création d'Utilisateur

Pour notre test nous avons enregistré l'utilisation comme suit

Username : diakite.junior avec pour mot de passe :Abdoul209@

Nous avons activé Raduis authentication pour qu'il puisse interagit avec notre FortiGate de telle sorte qu'il puisse vérifier si l'utilisateur fait déjà partie des utilisateurs existants et garanti aussi que l'utilisateur à l'autorisation d'accéder aux ressources sécurisées du réseau.

FortiAuthenticator 300F FAC-PAA-01

System > Create New Local User

Authentication >

User Account Policies >

User Management >

Local Users

Remote Users

Remote User Sync Rules

Social Login Users

Guest Users

User Groups

Usage Profile

Realms

FortiTokens

MAC Devices

IAM

Portals >

Remote Auth. Servers >

RADIUS Service >

TACACS+ Service >

LDAP Service >

OAuth Service >

Username: diakite.junior

Password creation: Specify a password

Password: .....

Password confirmation: .....

☒ Allow RADIUS authentication

☐ Force password change on next login

Role

Role: Administrator Sponsor **User**

Account Expiration

☐ Enable account expiration

IAM

Account: [ Please Select ]

OK Cancel

Figure 21 : Création d'Utilisateur

Après avoir créé notre utilisateur nous allons activer la double authentification sur la connexion VPN de notre utilisateur par un mail, pour le fait nous allons activer one-time password (OTP) authentication.

Dans user information nous allons entrer comme information le nom et l'un des prénoms de l'utilisateur ainsi que son mail qui fera office de réception de la deuxième authentification

FortiAuthenticator 300F FAC-PAA-01

System > Authentication > User Account Policies > User Management > Local Users

Username: diakite.junior

☐ Disabled

☒ Password authentication [Change Password](#)

☒ One-Time Password (OTP) authentication

Deliver token code by: [FortiToken](#) [Email](#) [SMS](#) [Dual \(Email & SMS\)](#) [Test Token](#)

☐ FIDO authentication

☒ Allow RADIUS authentication

☐ Enable account expiration

☐ Force password change on next logon

☒ Sync in HA Load Balancing mode

User Role

Role: [Administrator](#) [Sponsor](#) [User](#)

☐ Allow LDAP browsing

User Information

First name:  Last name:

Email:  Phone number:

Mobile number:  SMS gateway: [Use default](#) [Test SMS](#)

Street address:

City:  State/Province:

Country:

Language: [Use default](#)

FortiToken Logo: [Please Select](#)

Figure 22 : Création d'Utilisateur

La capture ci-dessous nous montre bien notre utilisateur VPN est bien créé avec les paramètres qu'il faut.

FortiAuthenticator 300F FAC-PAA-01

System > Authentication > User Account Policies > Edit Local User

The local user "diakite.junior" was added successfully. You may edit it again below.

Username: diakite.junior

Figure 23 : Création d'Utilisateur

### III. INTEGRATION DE FORTIGATE ET FORTIAUTHENTICATOR

Après avoir créé notre utilisateur VPN ainsi que ses paramètres nous allons maintenant faire une intégration entre notre pare-feu FortiGate et notre serveur d'authentification FortiAuthenticator, cette intégration va permettre une communication entre les deux équipements grâce à Radius Authentication.

Pour le fait nous allons nous rendre dans User & Authentication sur notre FortiGate ensuite dans RADIUS Servers.

Le name représente le nom de notre FortiAuthenticator, le IP/NAME son adresse IP ainsi que Secret son mot de passe, nous allons faire pareil sur notre FortiAuthenticator pour assurer une meilleure communication entre les deux équipements.

The screenshot shows the 'Edit RADIUS Server' configuration window in the FortiGate GUI. The left sidebar is expanded to 'User & Authentication' > 'RADIUS Servers'. The main panel shows the configuration for a RADIUS server named 'Srv\_FAC\_RADIUS'. The 'Authentication method' is set to 'Default'. The 'NAS IP' field is empty. The 'Include in every user group' checkbox is unchecked. The 'Primary Server' section shows the 'IP/Name' field filled with a redacted value, the 'Secret' field filled with dots, and the 'Connection status' as 'Successful'. There are buttons for 'Test Connectivity' and 'Test User Credentials'. The 'Secondary Server' section is currently empty with 'IP/Name' and 'Secret' fields and corresponding test buttons. At the bottom right are 'OK' and 'Cancel' buttons.

Figure 24 : Intégration Fortigate

Nous allons nous rendre dans Authentication sur notre FortiAuthenticator ensuite dans RADIUS Service puis dans client.

Le name représente le nom de notre FortiGate, le IP/Hostname son adresse IP ainsi que Secret son mot de passe, après cette intégration nous sommes sûre que les deux équipements pourront communiquer sans interruption.

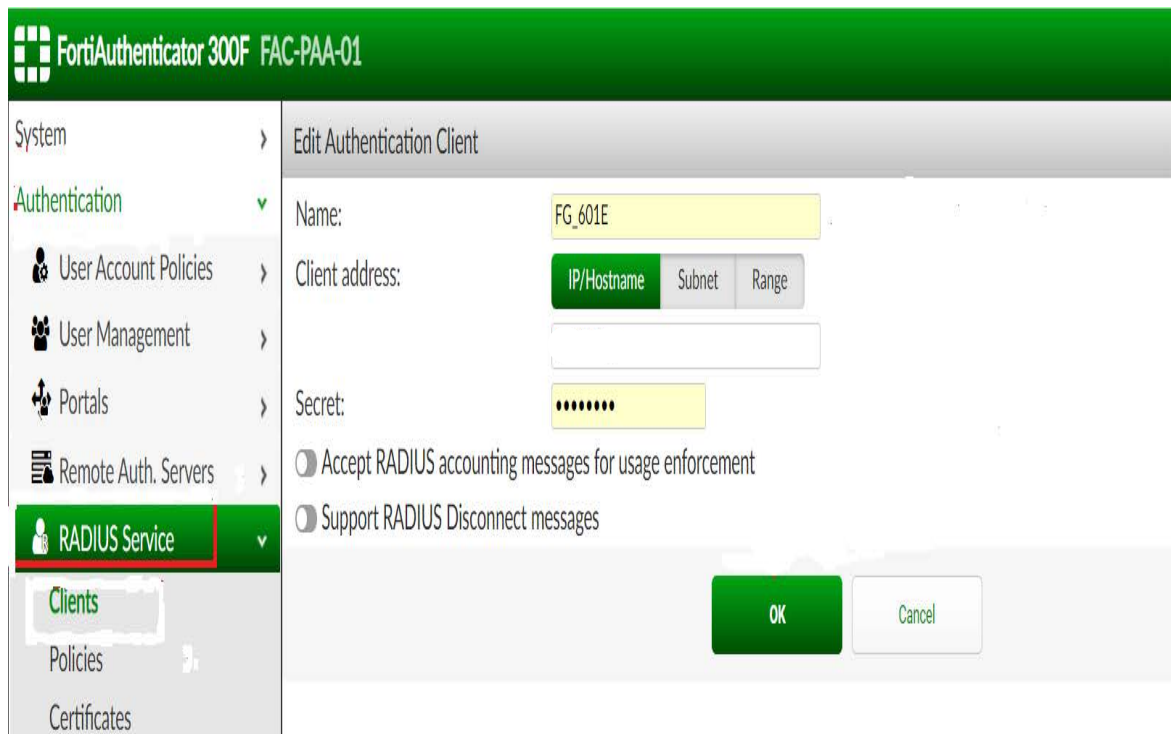


Figure 25 : Intégration Fortiauthenticator

## CHAPITRE II : RESULTATS ET DISCUSSIONS

Dans ce dernier chapitre de notre troisième partie, il est question pour nous de tester notre solution afin de se rassurer qu'elle fonctionne réellement, pour ce fait nous allons installer un FortiClient sur notre smartphone ou sur notre laptop et nous essaierons de nous connecter aux ressources de l'entreprise pour se rassurer également que notre solution est bien en place.

### I. RÉSULTATS

Nous allons dans Play Store pour pouvoir télécharger notre FortiClient (pour notre laptop nous pouvons le télécharger directement sur un navigateur).



Figure 26 : Téléchargement Forticlient



Après avoir téléchargé notre FortiClient nous allons l'installer et le configurer



Figure 27 : Création de VPN Sur FortiClient

Une fois notre application installée nous allons configurer une connexion VPN à travers les paramètres de nos différents équipements.

Nous avons donné le nom MTN à la connexion que nous voulons établir, ainsi que le même numéro de port entré dans les paramètres de notre VPN SSL configuré dans notre FortiGate et aussi l'utilisateur créé lors de la configuration du

Fortiauthenticator, dans la partie serveur nous allons entrer l'adresse du serveur que nous voulons atteindre dans le réseau de notre entreprise.

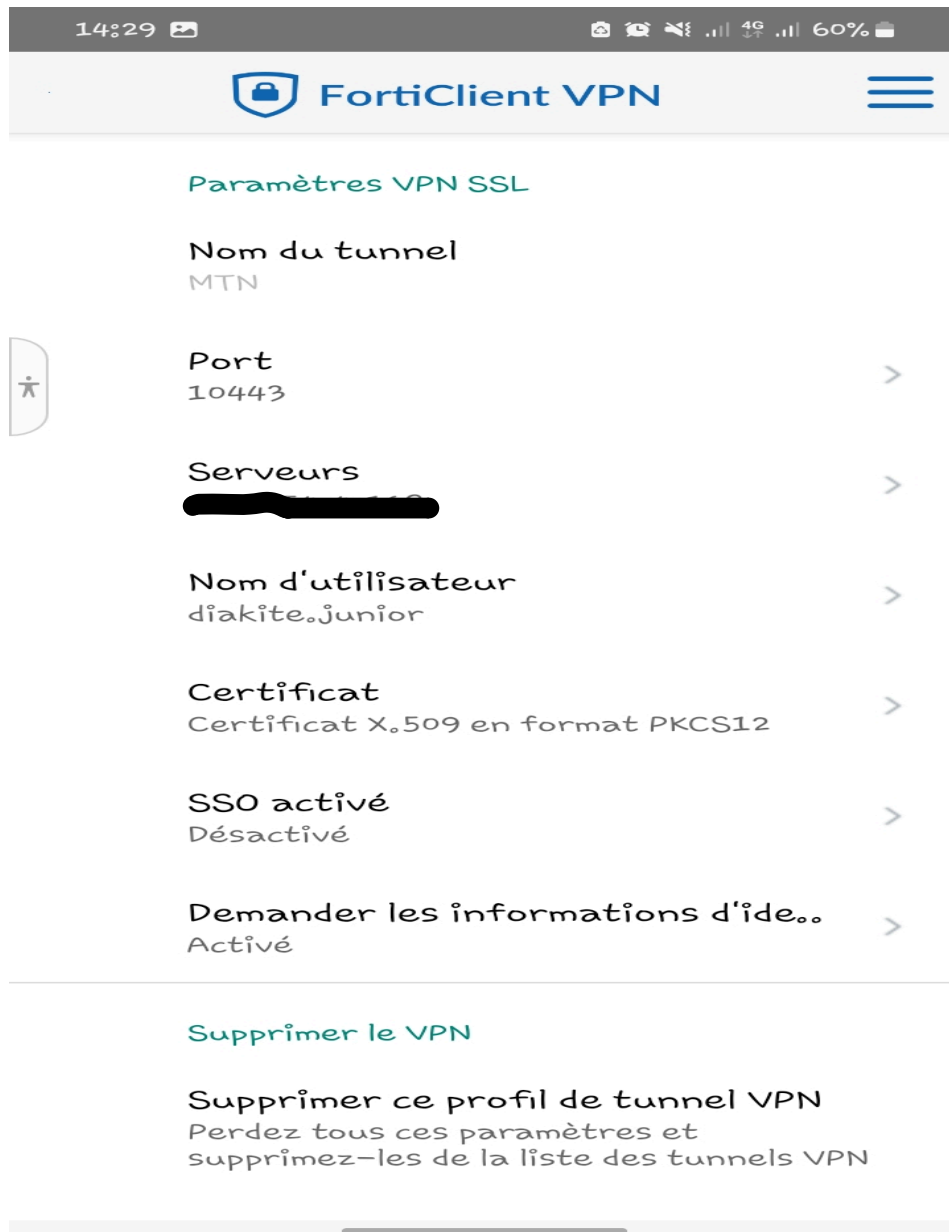


Figure 28 : Création de VPN sur FortiClient

Notre connexion VPN est bien créée comme nous le montre la capture ci-dessous



Figure 29 : Test Connectivité

Nous allons maintenant essayer de nous connecter au réseau de l'entreprise en appuyant sur tunnels VPN pour nom MTN, ensuite on clique sur connecter.

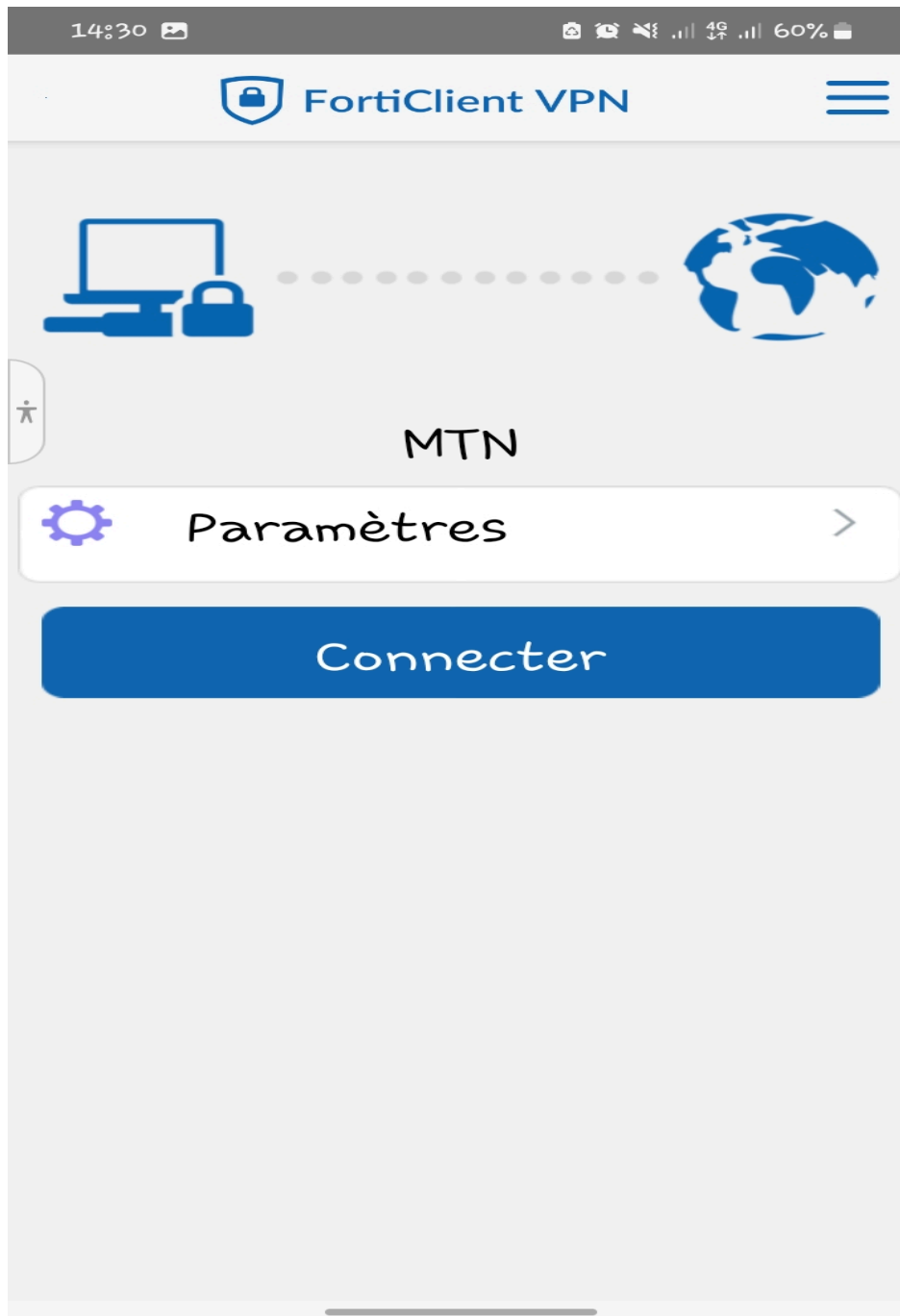


Figure 30 : Test de Connectivite

Lorsque nous essayons de nous connecter au réseau de l'entreprise, il nous ait demandés de renseigner un mot de passe et celui-ci fait office de la première authentification.

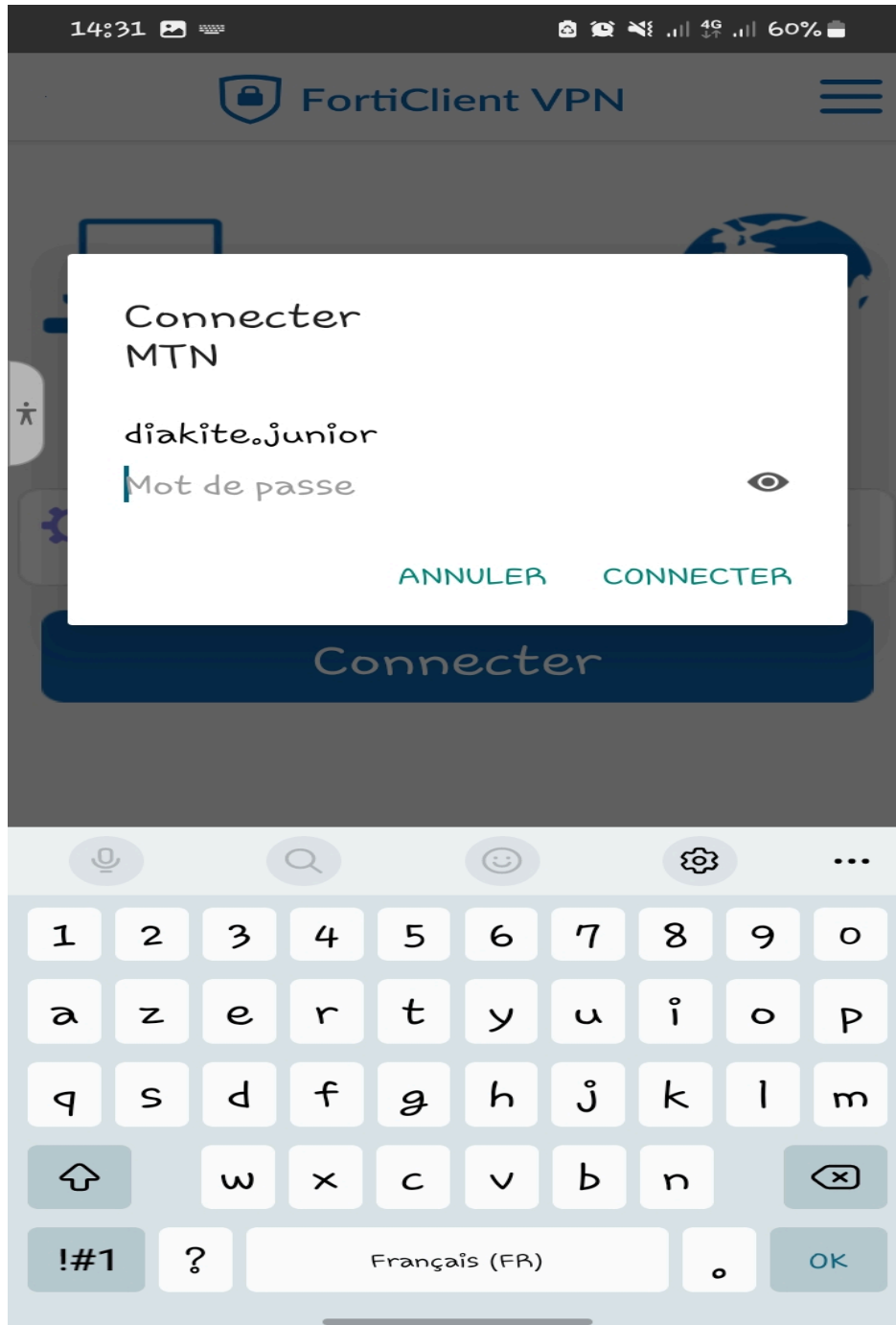


Figure 31 : Première Phase d'Authentification

Après avoir entré le mot de passe il nous ait demander un second mode d'authentification, le mode d'authentification demandé est celui que nous avons configurés sur notre FortiAuthenticator pour rappel nous avons mis le mail de l'utilisateur pour la réception du code de confirmation donc nous allons vérifier la boîte mail de l'utilisateur pour pouvoir validé la deuxième étape d'authentification et avoir accès aux ressources de l'entreprise.

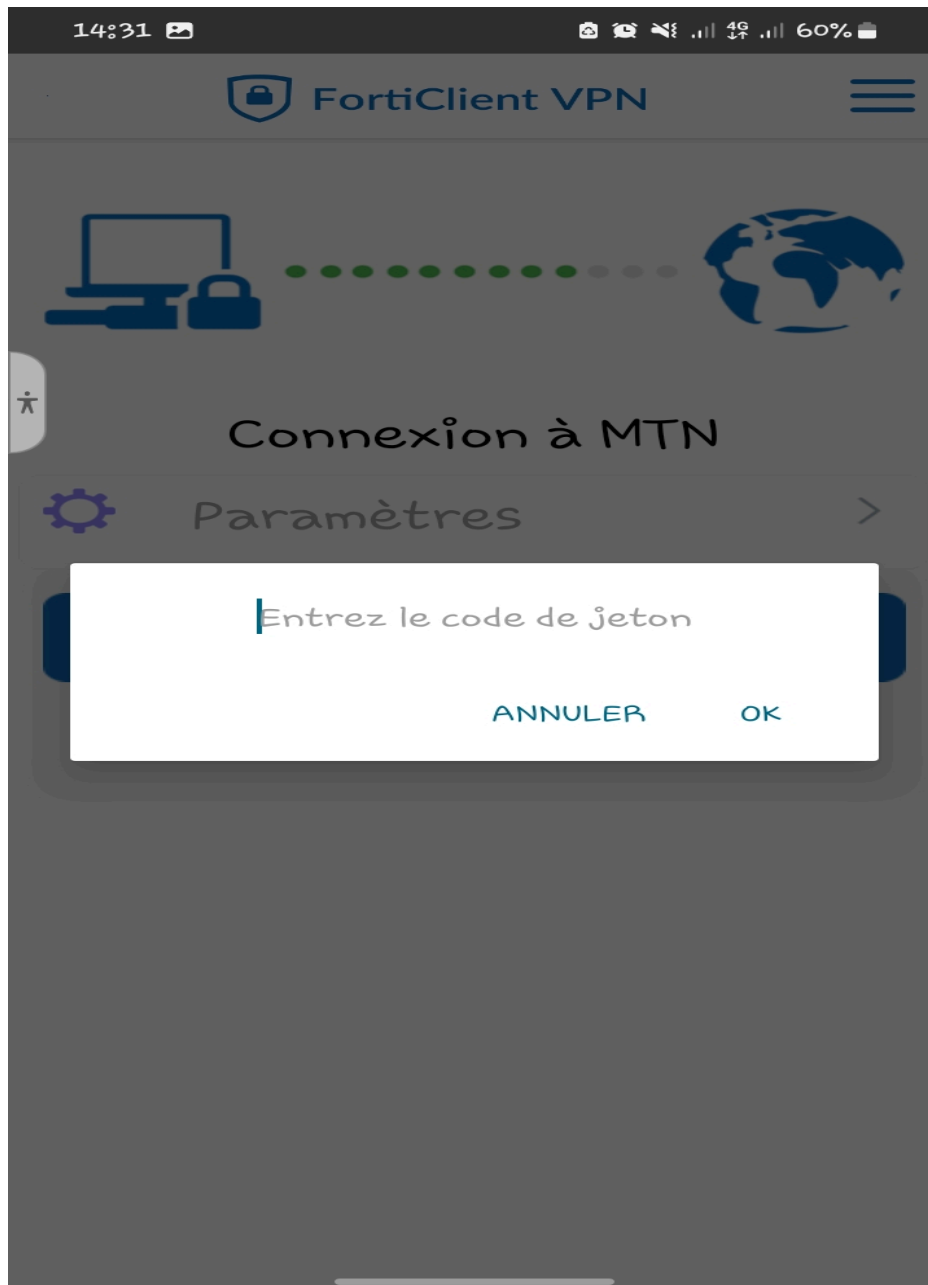


Figure 32 : Deuxième Phase d'Authentification

Effectivement nous avons reçu un code de confirmation à partir du mail de notre utilisateur que nous allons renseigner pour passer la deuxième authentification et avoir accès par la suite aux ressources de l'entreprise

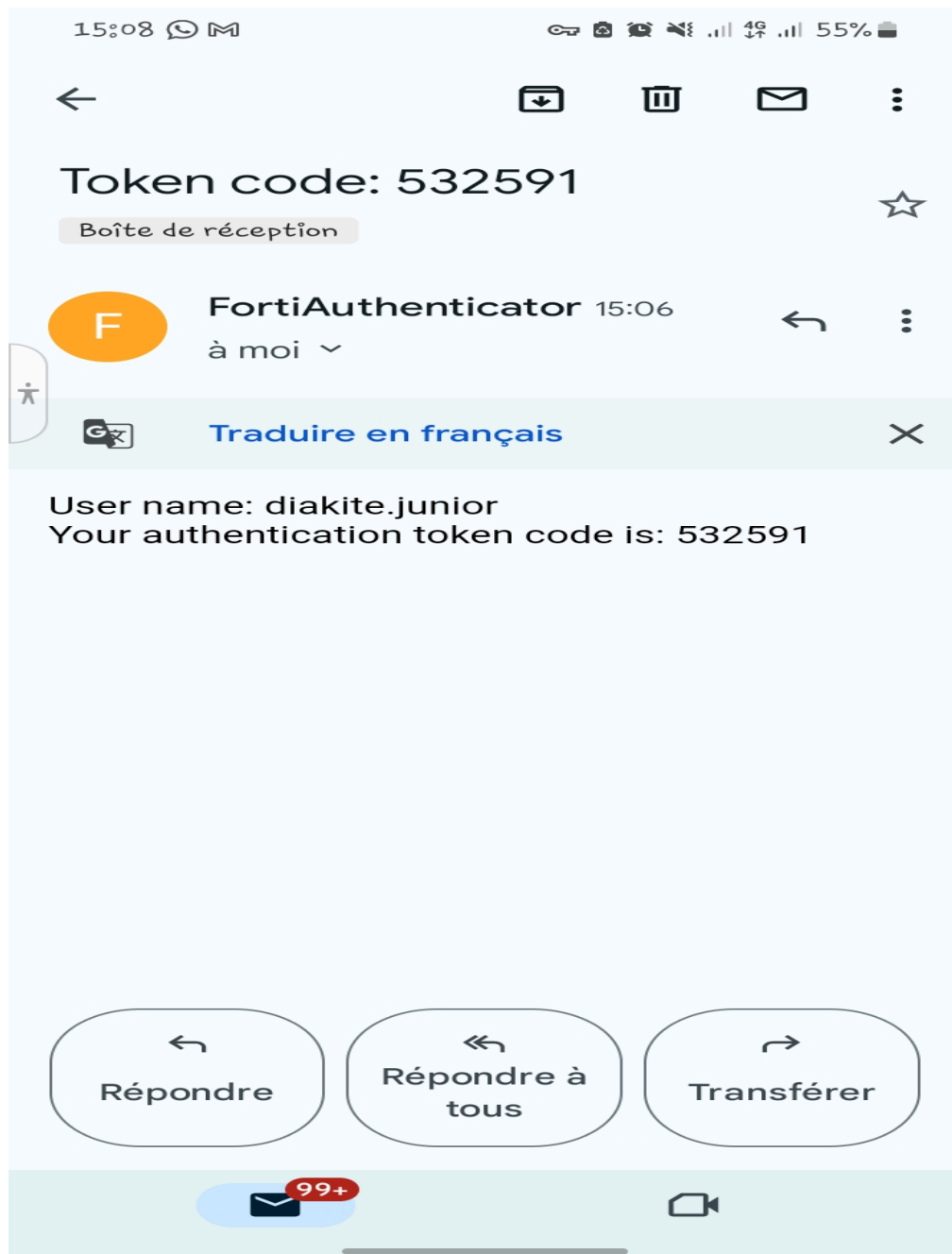


Figure 33 : Mail de Confirmation

La capture ci-dessous nous montre que nous sommes bien connectés sur le réseau l'entreprise et cela signifie que notre solution a été bien mis en place

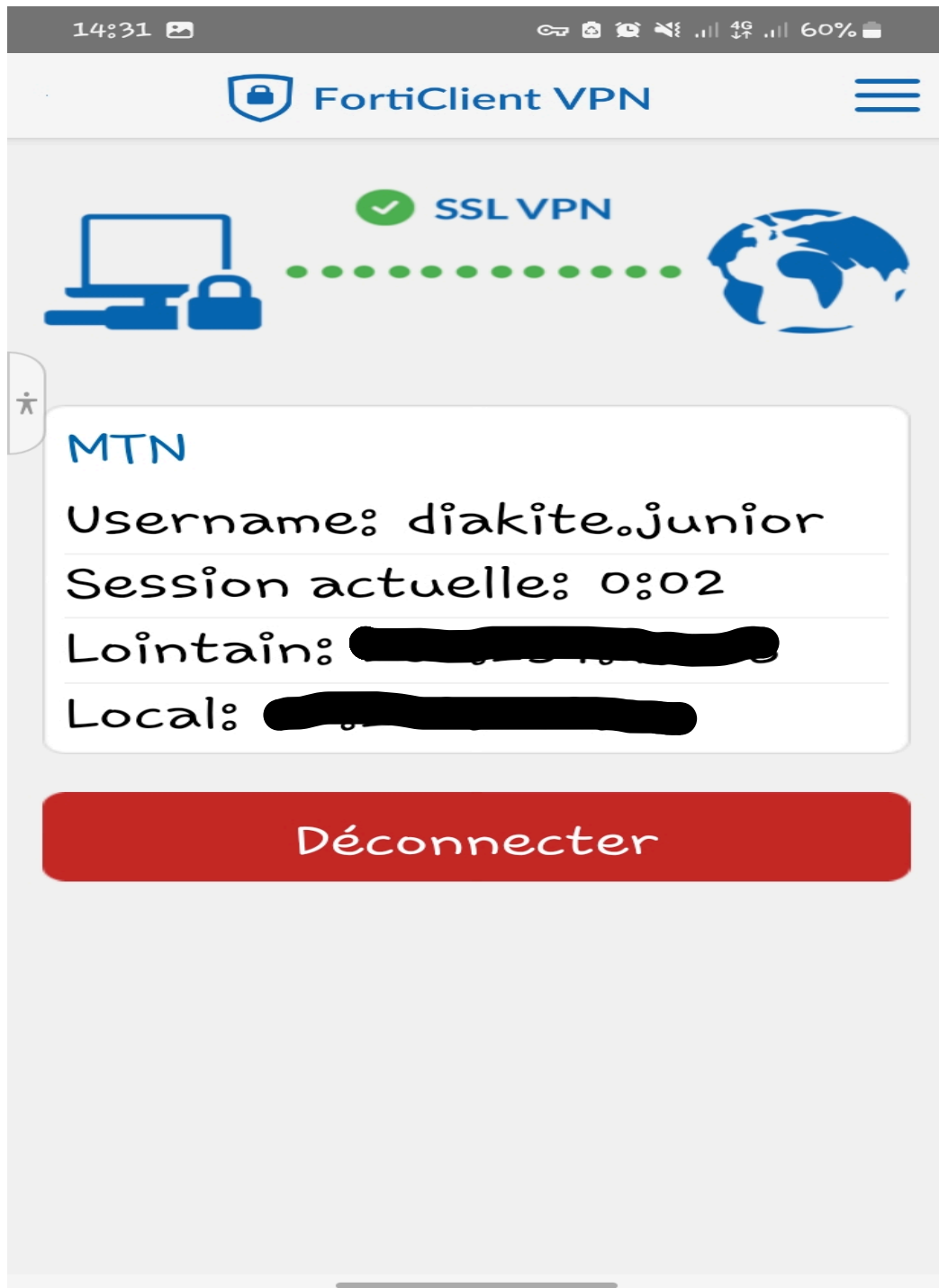


Figure 34 : Accès au Réseau de l'Entreprise



## II. DISCUSSION

Comme énoncé au début de notre étude, nous visions à améliorer l'unique authentification sur les comptes VPN (Virtual Private Network) des utilisateurs du Port Autonome d'Abidjan (PAA) en mettant en place une autre couche d'authentification qui fera office de la deuxième authentification.

Notre solution proposée aidera le Port Autonome d'Abidjan (PAA) à réduire les risques d'attaques par hameçonnage, de vols d'identifiants et d'accès non autorisés aux systèmes de l'entreprise, elle permettra aussi aux utilisateurs du Port Autonome d'Abidjan (PAA) d'être opérationnels tout en étant rassurer que les risques d'attaques soient minimisés.

En effet, notre solution ne s'étend que sur le Port Autonome d'Abidjan (PAA). L'impact pourrait être tout autre sur les Ports africains ainsi que les grandes entreprises. Le travail que nous avons accompli pourrait être complété et poursuivi sous différents aspects. En guise de perspective, il sera intéressant de joindre des entreprises en sous-traitance dans le domaine des transports, assurance, banque, commerce et pour plus de pertinence étendre notre solution à un niveau international.

## III. ÉVALUATION FINANCIÈRE

Équipements	Quantités	Prix Unitaires	Total en Fcfa
FortiGate 601e	1	3210,98 \$	2.001050
FortiAuthenticator 300F	1	2290,34 \$	1.427315
FortiClient VPN	1	Gratuit	Gratuit

Tableau 2 : Prix des Équipement Informatique

## CONCLUSION GENERALE

Ce mémoire a été rédigé dans le cadre du projet de fin d'études réalisé au sein du Port Autonome d'Abidjan (PAA) pour l'obtention de la licence en administration sécurité des systèmes et réseaux informatiques.

Nous sommes appelés dans ce projet à proposer une solution en sécurité afin de garantir une connexion et communication sécurisé entre les utilisateurs et les ressources de l'entreprise et aussi pour éviter au maximum les risques d'attaques que subir les entreprises.

Notre solution a été approuvée par l'entreprise. Les configurations pour la double authentification sur les comptes VPN sont terminées par contre les services déjà configurés sur les équipements auparavant non étés impactés et sont toujours en activités. Dans un jugement personnel, lors de ce stage de trois (3) mois, nous avons pu mettre en pratique nos connaissances théoriques acquises durant notre formation à académique malgré les difficultés du monde professionnel.

Suite à notre intégration rapide dans l'équipe des Stagiaires administrateurs réseaux et sécurité, nous avons eu l'occasion de réaliser plusieurs missions en Administration Réseau Sécurité.

Ce stage a été très bénéfique pour nous car il nous a permis de nous confronter au monde de l'entreprise.

## WEBOGRAPHIE

<https://www.presse-citron.net/vpn/definition/> visité le 14/07/23 9h23min

<https://chat.openai.com/c/7f41dcb9-bf0e-4469-a557-9e515274b441> visité le 14/07/23 9h57min

<https://docs.fortinet.com/> visité le 17/07/23 10h51min

<https://www.syloe.com/glossaire/authentication/> visité le 18/07/23 9h13min

<https://www.sailpoint.com/fr/identity-library/authentication-methods-used-for-network-security/> visité le 18/07/23 11h22min

<https://www.gartner.com/reviews/market/network-firewalls> visité le 18/07/23 14h31min

<https://www.syloe.com/glossaire/firewall-pare-feu/> visité le 19/07/23 10h 27min

<https://www.fortinet.com/fr/solutions/gartner-network-firewalls> visité le 19/07/23 15h11min

<https://www.ionos.fr/digitalguide/serveur/know-how/ldap/> visité le 19/07/23 16h32min

## TABLE DES MATIÈRES

<b>DEDICACE .....</b>	<b>Erreur ! Signet non défini.</b>
<b>REMERCIEMENTS .....</b>	<b>Erreur ! Signet non défini.</b>
<b>AVANT-PROPOS .....</b>	<b>Erreur ! Signet non défini.</b>
<b>SOMMAIRE.....</b>	<b>Erreur ! Signet non défini.</b>
<b>LISTE DES SIGLES, ABREVIATIONS ET ACCRONYMES .....</b>	<b>Erreur ! Signet non défini.</b>
<b>LISTE DES FIGURES ET DES TABLEAUX .....</b>	<b>Erreur ! Signet non défini.</b>
<b>INTRODUCTION.....</b>	<b>1- 1 -</b>
<b>PREMIÈRE PARTIE : GÉNÉRALITÉS .....</b>	<b>-2-</b>
<b>CHAPITRE I : PRESENTATION GÉNÉRAL DE LA STRUCTURE</b>	
<b>D'ACCUEIL.....</b>	<b>-3-</b>
<b>I. PRÉSENTATION DU PORT AUTONOME D'ABIDJAN (PAA).....</b>	<b>-3-</b>
<b>I.1 HISTORIQUE.....</b>	<b>-3-</b>
<b>I.2 GENERALITE .....</b>	<b>-4-</b>
<b>I.3 MISSIONS ET OBJECTIFS.....</b>	<b>-5-</b>
<b>I.4 ORGANIGRAMME DU PORT AUTONOME D'ABIDJAN.....</b>	<b>-7-</b>
<b>II. PRÉSENTATION DE LA DIRECTION DES SYSTÈMES</b>	
<b>D'INFORMATION NUMÉRIQUE (DSIN).....</b>	<b>-8-</b>
<b>II.1 MISSIONS ET ATTRIBUTIONS DE LA DIRECTION DES SYSTEMES</b>	
<b>D'IINFORMATION NUMERIQUE (DSIN).....</b>	<b>-8-</b>
<b>II.2 ORGANIGRAMME DE LA DIRECTION DES SYSTEMES</b>	
<b>D'IINFORMATION NUMERIQUE (DSIN).....</b>	<b>-9-</b>
<b>CHAPITRE II : ASPECT THÉORIQUE DU PROJET .....</b>	<b>-10-</b>
<b>I. CONTEXTE .....</b>	<b>-10-</b>

<b>II. PROBLEMATIQUE</b>	-10-
<b>III. OBJECTIFS ET DÉMARCHE</b>	-10-
III.1 OBJECTIFS	-11-
III.2 DÉMARCHE	-12-
<b>IV. CAHIER DE CHARGE</b>	-12-
 <b>CHAPITRE III : ANALYSE DE L'EXISTANT</b>	 -13-
<b>I. RECUEIL D'INFORMATIONS</b>	-13-
I.1 EQUIPEMENTS	-13-
I.2 INVENTAIRES DES PÉRIPHÉRIQUES EXISTANTS	-13-
<b>II. ANALYSES ET CRITIQUES</b>	-14-
II.1 CONSTAT GENERAL	-14-
II.2 ANALYSES ET CRITIQUES DE L'EXISTANT	-14-
<b>III. ÉBAUCHE DE LA SOLUTION</b>	-15-
 <b>DEUXIÈME PARTIE : ÉTUDE CONCEPTUELLE</b>	 -17-
<b>CHAPITRE I : SÉCURITÉ</b>	-18-
<b>I. GÉNÉRALITÉ SUR LES AUTHENTIFICATIONS</b>	-18-
I.1 DEFINITION DE L'AUTHEMIFICATION	-18-
I.2 LES FACTEURS D'AUTHEMIFICATION	-18-
I.3 AUTHENTIFICATION A UNIQUE FACTEUR	-18-
I.4 AUTHENTIFICATION A MULTI-FACTEURS (MFA)	-19-
<b>II. GÉNÉRALITÉ SUR LES VPN</b>	-20-
II.1 DEFINITION DES VPN	-20-
II.2 PRINCIPES DES VPN	-20-
 <b>CHAPITRE II : ÉQUIPEMENTS DE SECURITE</b>	 -22-
<b>I. PARE-FEU</b>	-22-
I.1 DÉFINITION	-22-
I.2 QUELQUES PARE-FEU	-22-
<b>II. SERVEUR D'AUTHEMIFICATION</b>	-23-

II.1 DÉFINITION-----	-23-
II.2 QUELQUES SERVEURS D'AUTHENTIFICATION -----	-24-
 <b>TROISIÈME PARTIE : IMPLEMENTATIONS ET RESULTATS-----</b>	<b>- 25-</b>
 CHAPITRE I : IMPLÉMENTATION-----	-26-
<b>I. CONFIGURATION DU FORTIGATE-----</b>	<b>-26-</b>
<b>II. CONFIGURATION DU FORTIAUTHENTICATOR-----</b>	<b>-32-</b>
<b>III.INTEGRATION DE FORTIGATE ET FORTIAUTHENTICATOR-</b>	<b>-37-</b>
 CHAPITRE II : RÉSULTATS ET DISCUSSIONS -----	-40-
<b>I. RÉSULTATS-----</b>	<b>-40-</b>
<b>II. DISCUSSIONS -----</b>	<b>-49-</b>
<b>III. ÉVALUATION FINANCIÈRE DU PROJET-----</b>	<b>-</b>
49-	
 <b>CONCLUSION GÉNÉRALE-----</b>	<b>-50-</b>
 <b>WEBOGRAPHIES-----</b>	<b>-VIII-</b>
 <b>TABLE DES MATIÈRES-----</b>	<b>-IX-</b>
 <b>RÉSUMÉ-----</b>	<b>-XI-</b>

## **RÉSUMÉ**

En conclusion, cette étude a mis en lumière l'importance cruciale de renforcer la sécurité des comptes VPN (Virtual Private Network), particulièrement dans le contexte du Port Autonome d'Abidjan (PAA). Le déploiement d'une double authentification se présente comme une solution efficace pour minimiser les risques de compromission des accès aux réseaux sensibles de l'organisation.

Cependant, il est essentiel de noter que la sécurité informatique est un processus continu. Les menaces évoluent constamment, et il est impératif d'adopter une approche proactive en surveillant les tendances et en mettant à jour les mécanismes de sécurité en conséquence.

En somme, l'instauration d'une double authentification sur les comptes VPN du Port Autonome d'Abidjan a démontré son efficacité dans la préservation de l'intégrité des systèmes d'information. Cela constitue un pas significatif vers une sécurité informatique robuste et une protection accrue des ressources critiques de l'organisation.

## **ABSTRACT**

In conclusion, this study has highlighted the crucial importance of strengthening VPN (Virtual Private Network) account security, particularly in the context of the Port Autonome d'Abidjan (PAA). The deployment of dual authentication is an effective solution for minimizing the risk of compromising access to the organization's sensitive networks.

However, it is essential to note that IT security is an ongoing process. Threats are constantly evolving, and it is imperative to adopt a proactive approach by monitoring trends and updating security mechanisms accordingly.

In short, the introduction of double authentication on VPN accounts at the Port Autonome d'Abidjan has proved its effectiveness in preserving the integrity of

information systems. This represents a significant step towards robust IT security and enhanced protection of the organization's critical resources.