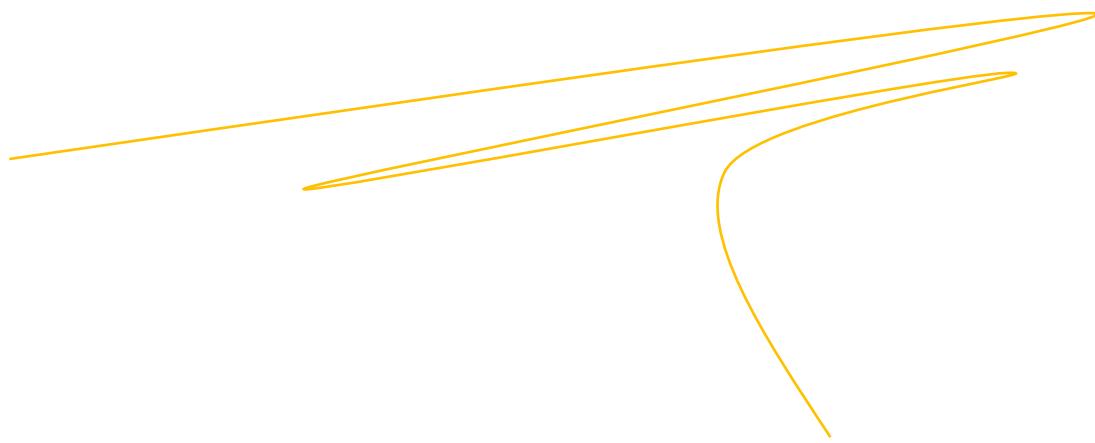




À TOUTE MA FAMILLE 



## REMERCIEMENTS

Leurs apports en entreprise, leurs connaissances, leurs disponibilités, et leurs soutiens physiques et moraux ont été d'une aide capitale et cruciale car ils ont participé à l'augmentation de nos connaissances et nous ont permis de joindre l'écrit à la pratique. C'est donc pour cela que, nos remerciements vont à l'endroit de :

- **Dieu Tout Puissant** sans qui, rien de tout ceci ne serait possible pour moi ;
- Monsieur **ARMAND CLAUDE ABANDA**, Représentant résident de l'IAI Cameroun ;
- Monsieur **WAMBO JEREMIE** pour sa disponibilité et ces précieux conseils durant notre stage académique ;
- Monsieur **CHATCHUIN DJOKO DASSY**, encadreur académique et enseignant à l'IAI-Cameroun Centre de Yaoundé pour son assistance, son expertise durant cette période.
- Le staff du département Informatique de **AFECameroun** pour leur encouragement et leur soutien quotidien tout au long de notre séjour ;
- Toute ma famille en particulier Mes parents ; Madame **SYLVIA EBUDE** et Monsieur **MPACKO ETOUKE** pour le soutien morale et financier inconditionnel qu'ils ne cessent de m'accorder chaque jour.
- Tout le **Corps Enseignant de l'IAI-Cameroun**, centre de Yaoundé en leur qualité de guide pédagogique ainsi que **tous nos camarades** pour leurs regards attentionnés les uns envers les autres.
- Tous ceux qui nous ont soutenu de près ou de loin d'une quelconque manière que ce soit.

## SOMMAIRE

DEDICACE .....	1
REMERCIEMENTS.....	2
SOMMAIRE.....	3
LISTE DES FIGURES .....	5
LISTES DE TABLEAUX.....	10
RESUMÉ .....	11
ABSTRAT .....	12
INTRODUCTION .....	13
PREMIERE PARTIE : DOSSIER D'INSERTION .....	14
INTRODUCTION .....	15
I- ACCUEIL AU SEIN D'AFEC CAMEROUN .....	16
II- PRESENTATION DE LA STRUCTURE.....	16
CONCLUSION.....	23
DEUXIEME PARTIE : PHASE TECHNIQUE .....	24
CHAPITRE 1 :ANALYSE DU PROJET .....	26
CHAPITRE 2:CAHIER DE CHARGES .....	31
I. CONTEXTE DU PROJET.....	32
II. OBJECTIFS DU PROJET .....	32
III. EXPRESSION DES BESOINS DE L'UTILISATEUR .....	33
VI. ESTIMATION DU COÛT DU PROJET.....	34
V. PLANNIFICATION PROJET .....	37
VI. LES CONTRAINTES DU PROJET.....	39
VII. LES LIVRABLES .....	39
CHAPITRE 3: ETAT DE L'ART.....	40
I. INTRODUCTION SUR LA SECURITE RESEAU.....	41

---

II. GENERALITE SUR LA DOUBLE AUTHENTIFICATION.....	54
III. PROTOCOLE RADIUS .....	69
IV. SURVEILLANCES ET GESTIONS DU RESEAU.....	72
INTRODUCTION .....	72
CONCLUSION.....	76
V. NORMES ET REGLEMENTATIONS .....	77
INTRODUCTION .....	77
CONCLUSION.....	78
CHAPITRE 4: IMPLEMENTATION DE LA SOLUTION.....	80
I. CHOIX DE LA SOLUTION NIVEAU AUTHENTIFICATION .....	81
II. ARCHITECTURE UTILISE POUR LA DEMONSTRATION.....	82
III. CONFIGURATION DE LA DOUBLE AUTHENTIFICATION SUR LE SERVEUR WINDOWS.....	83
IV. CONFIGURATION DE LA DOUBLE AUTHENTIFICATION SUR UN ROUTEUR.....	92
V. CONFIGURATION DE LA SUPERVISION PRTG SUR LE SERVEUR WINDOWS.....	117
VI. TEST DE FONCTIONNALITÉS.....	119
CONCLUSION GENERAL .....	128
ANNEXES.....	A
BIBLIOGRAPHIE .....	B
WEBOGRAPHIE .....	C
GLOSSAIRE.....	D
TABLE DE MATIERES .....	E



## LISTE DES FIGURES

Figure 1: Organigramme d'AFEC CAMEROUN.....	20
Figure 2: plan de localisation AFEC (Source : Entreprise).....	20
Figure 3: Topologie actuel de afec.....	28
Figure 4: Diagramme de Gantt.....	38
Figure 5: Attaque directe. (Source : google image).....	44
Figure 6: Attaque par rebond (source : google image).....	44
Figure 7: Attaque indirecte par réponse (source : google image).....	45
Figure 8: Attaque par adresse IP (source : google image).....	45
Figure 9: Attaque par adresse MAC (source : google image).....	46
Figure 10: ARP Spoofing (source: google image).....	46
Figure 12: Utilité d'un parefeu(source : googleimage).....	49
Figure 13: Système VPN (source : google image).....	50
Figure 14: Exemple d'un réseau VLAN (source : google image).....	50
Figure 15: Zone DMZ (source : google image).....	51
Figure 16: Proxy (source : google image).....	51
Figure 17: Schéma d'une requête http.....	54
Figure 18: Fonctionnement de la 2FA (source : google image).....	55
Figure 19: Facteur de la 2FA (source : google image).....	56
Figure 20: Protocole Kerberos.....	64
Figure 21: Protocole LDAP.....	65

---

Figure 22: Protocole OAuth2 .....	66
Figure 23: Protocole SAML.....	67
Figure 24: Protocole RADIUS.....	68
Figure 25: Architecture AFECameroun.....	82
Figure 26: Architecture utilisé pour la demonstration.....	82
Figure 27: Choix de la langue du système.....	83
Figure 28: Choix du système à installer.....	84
Figure 29: Contrat de licence .....	84
Figure 30: Installation de windows server.....	85
Figure 31: Parametres de personnalisation.....	85
Figure 32: Deverouillage de la session.....	86
Figure 33: Ajout d'une nouvelle zone.....	87
Figure 34: Choix du type de zone.....	87
Figure 35: Specifier la zone.....	88
Figure 36: Mise à Niveau.....	89
Figure 37: Fin de l'installation.....	89
Figure 38: Ajout d'un nouveau pointeur.....	90
Figure 39: Ajout du pointeur.....	91
Figure 40: Verification de la foret et du nom de domaine.....	91
Figure 41: Ajout d'un role et fonctionnalité.....	92
Figure 42: Activation de la fonctionnalité ADDS.....	93
Figure 43: Confirmations des sélections d'installations.....	94
Figure 44: Installation de l'ADDS.....	94
Figure 45: Achevement de l'installation de l'ADDS –Tableau de bord.....	95

---

Figure 46: Insertion du nom de domaine.....	96
Figure 47: Insertion du mot de passe .....	97
Figure 48: Indication du nom de domaine NetBIOS .....	97
Figure 49: Indication du chemin d'accès.....	98
Figure 50: Résultat de la vérification des options.....	99
Figure 51: Installation du service ADDS.....	99
Figure 52: Interface de Connexion.....	100
Figure 53: Lancement TOTPRadius.....	101
Figure 55: Lancement TOTPRadius.....	102
Figure 56: Nom de notre serveur TOTPRadius.....	102
Figure 57: Adresse IP de notre seveur TOTPRadius.....	103
Figure 58: Masque de sous reseau.....	103
Figure 59: Gateway de TOTPRadius .....	104
Figure 60: Premier DNS de TOTPradius.....	105
Figure 61: Deuxieme DNS de TOTPradius.....	105
Figure 62: Interface de connexion TOTPradius.....	107
Figure 63: Page de TOTPradius.....	108
Figure 64: Setting de TOTPradius.....	108
Figure 65 :Parametre de radius dans TOTPradius.....	109
Figure 66: IP du serveur radius.....	110
Figure 67: Configuration de LDAP.....	110
Figure 68: Enregistrement des utilisateurs de TOTPRadius.....	111
Figure 69: Interface d'enregistrement des user.....	111
Figure 70: Code QR de l'user Administrateur.....	112

Figure 71: Enregistrement d'administrateur.....	112
Figure 72: Creation des User.....	113
Figure 75: IP des interfaces du routeur.....	114
Figure 74 :: Configuration de l'authentification sur le routeur.....	115
Figure 75: Choix de la langue lors de l'installation de PRTG.....	117
Figure 76: Lire le contrat et appuyer sur je comprends et j'accepte .....	117
Figure 77: Cliquez sur suivant.....	118
Figure 78: Patienter l'installation.....	118
Figure 79: Page d'accueil PRTG.....	119
Figure 80: Cliquer sur ajouter un groupe.....	120
Figure 81: Cliquer sur Infrastructure reseau et puis sur ok.....	120
Figure 82: Entrer Nom du groupe.....	121
Figure 83: Cliquer sur Equipement.....	121
Figure 84: Cliquer sur Votre Groupe .....	122
Figure 85: Entrer le nom de l'equipement et son adresse IP.....	122
Figure 86: Choisir le logo de l'equipement et cochez la decouverte automatique.....	123
Figure 87: Cliquer sur Equipement et cliquer sur ajouter un capteur.....	123
Figure 88: Choisissez le type de capteur que vous souhaitez superviser.....	124
Figure 89: Choix du capteurs des Ping.....	124
Figure 90: Configurer les parametre selon vous et cliquez sur Créer.....	125
Figure 91: Capture de mes equipements et leur Capteur.....	125
Figure 92: Test d'authentification sur le routeur via PuTTY.....	126
Figure 93: Interface du routeur via PuTTY.....	126
Figure 94: Log du serveur TOTPRadius.....	127

Figure 95: Configuration du routeur.....127

## LISTES DE TABLEAUX

Tableau 1 : Fiche Signalétique AFEC .....	21
Tableau 2 : Ressources Matérielles.....	22
Tableau 3: Ressources Logicielles.....	22
Tableau 4 : Critique de l'existence.....	29
Tableau 5 .Ressources Humaines.....	35
Tableau 6: Ressources logicielles (Source : fait sur Word 2019) .....	35
Tableau 7: Ressources matérielles (Source : fait sur Word 2016).....	36
Tableau 8: Cout total du projet .....	37
Tableau 9 : tableau d'ordonnancement.....	38

## RESUMÉ

Au terme de notre formation de trois ans à *L'institut Africain D'informatique*, Centre de Yaoundé, il nous est demandé pour l'obtention de notre **Diplôme D'Ingénieur de Travaux** de réaliser un stage académique. En effet ce stage a pour but de familiariser les étudiants que nous sommes non seulement au monde professionnel, mais aussi de nous permettre de mettre en pratique l'ensemble des connaissances apprises à l'école dans cet univers. C'est dans cette optique que nous avons eu l'opportunité d'effectuer un stage académique dans l'entreprise AFEC Cameroun (***Audit Formation Evaluation Conseil***). A cet effet, durant notre séjour à AFEC, qui s'est effectué sur une période de deux mois allant du 4 aout au 31 septembre 2024, nous avons eu à mettre en œuvre nos compétences en matière de systèmes et réseaux. C'est ainsi que nous avons eu à mettre en place **UN SYSTÈME DE SECURITE (DOUBLE AUTHENTIFICATION AVEC RADIUS) RESEAU AVEC SUPERVISION PRTG** pour l'entreprise AFEC Cameroun en respectant les exigences du systèmes et réseaux qui met un accent particulier sur la sécurité. Durant notre séjour à la AFEC CAMEROUN, nous avons acquis plusieurs notions qui ont forgées notre expérience non seulement sur un point de vue professionnel, mais aussi sur un point de vue moral au sens où nous avons appris comment collaborer en entreprise.

**Mots ou expressions clés :** Supervision, Authentification, Réseaux, Radius,

## ABSTRACT

At the end of our three-year training at the African Institute of Computer Science, Yaoundé Center, in order to obtain our Bachelor of Engineering in abbreviated B.Eng. we are required to carry out an academic internship. Indeed, this internship aims to familiarize the students with the professional world, and also to allow us to put into practice all the knowledge learned at school in this universe. It is with this in mind that we had the opportunity to do an academic internship at the Company; AFEC Cameroun (AUDIT TRAINING EVALUATION CONSULTING). To this end, during our journey at AFEC Cameroun, which took place over a two-month period from August 4 to September 31, 2024, we had to implement our skills in Systems and Networks engineering in general and Networking engineering in particular. This is how we had to come up with **IMPLEMENTATION OF TWO-FACTOR AUTHENTICATION SECURITY SYSTEM WITH RADIUS SERVER? AND NETWORK MONITORING USING PRTG** for the company **AFEC Cameroun**, respecting the requirements of Systems and Networks engineering that puts a particular emphasis on security. During our time at AFEC Cameroun, we acquired several notions that forged our experience not only from a professional point of view, but also from a moral point of view, and we learned how to collaborate in business.

**Keywords or phrases:** Two-factor authentication, Network monitoring

## INTRODUCTION

L'institut Africain d'Informatique est une école inter-état créée en 1972 par décision des chefs d'états en vue de former des élèves ingénieurs dans l'Afrique en informatique. C'est le cas de l'Institut Africain d'Informatique représentation du Cameroun qui, dans le but de réunir toutes les pièces pour un profil « quasi parfait » dans un monde où l'évolution technologique est au cœur de l'actualité dans tous les domaines, exige aux étudiants de deuxième année que nous sommes d'effectuer un stage académique d'une durée de quatre mois afin de parfaire notre formation. Stage durant lequel l'étudiant aura l'occasion une fois de plus de s'en querir des rouages du monde professionnel, de profiler sa formation et pourquoi pas de trouver par la même occasion un emploi. Puisque les Technologies de l'Information et de la Communication sont aujourd'hui un domaine incontournable. Les aptitudes, les capacités et les connaissances dans ce domaine sont de plus en plus sollicitées dans les entreprises.

C'est dans le but d'atteindre ces objectifs que nous avons été accueillis à AFEC Cameroun où nous avons pu constater après une étude des différents besoins de l'entreprise que le réseau de l'entreprise rencontrait quelques difficultés qui affectaient leur productivité au niveau de la gestion de ce département. Ainsi, il est donc judicieux de se demander **Comment sécuriser et superviser le réseau d'AFEC ?** dès lors le besoin de renforcer la sécurité du réseau s'est mis en exergue, C'est la raison pour laquelle nous avons pensé à **MISE EN PLACE D'UN SYSTÈME DE SECURITE (DOUBLE AUTHENTIFICATION AVEC RADIUS) RESEAU AVEC LA SUPERVISION PRTG** pour cette entreprise.

En clair, il est question pour le système de protéger plus efficacement le réseau de tout AFEC Cameroun. Ainsi, la toile de fond de notre analyse s'est divisée en deux parties regroupant chacune plusieurs chapitres. La première partie se rapporte au dossier d'insertion qui décrit l'environnement de travail dans lequel nous avons évolué, la deuxième partie porte sur le dossier technique dans lequel est présenté l'existant, l'étude de notre solution, la mise en place de la solution et enfin les résultats obtenus. Nous finirons ce rapport par une conclusion générale récapitulative des différentes phases de notre travail, signalant les côtés bénéfiques du projet et énonçant les perspectives du travail élaboré.

**PREMIERE PARTIE :**  
**DOSSIER D'INSERTION**

**Préambule :**

Nous commencerons d'abord par présenter l'entreprise hôte dans laquelle nous avons mené notre quotidien pendant deux mois, puis nous présenterons le déroulement de notre stage. Puisque toute activité débute toujours par une prise de contact de l'environnement dans lequel on est appelé à travailler.

**Aperçu :**

---

**INTRODUCTION**

**I. ACCUEIL AU SEIN D'AFEC CAMEROUN**

**II. PRÉSENTATION DE LA STRUCTURE**

**CONCLUSION**

---

## INTRODUCTION

Il existe une seule marche entre le milieu professionnel et l'environnement académique habituel, ce qui est très important pour les étudiants qui sont sur le point de faire la transition vers ce monde passionnant d'opportunités. Cependant, ils sont souvent entravés par un manque de compétences et d'expérience professionnelles. Ils nécessitent donc un environnement professionnel capable de combler ces lacunes. C'est dans cette optique que nous avons été reçus à AFEC Cameroun. Le rapport d'insertion peut être défini comme un document présentant de manière brève le processus d'intégration d'un stagiaire au sein d'une structure. Pour se faire nous devons nous familiariser avec notre entourage en entreprise en mettant en exergue les missions et les réalisations de la structure, et après le thème qui nous aura été attribué au cours de ce stage ; développé dans la prochaine partie. Cette période d'insertion d'une durée de (02) semaines sera détaillée dans la suite de notre document.

## I- ACCUEIL AU SEIN D'AFEC CAMEROUN

La date du **lundi 01 juillet 2023** à 8h00 précise a marqué le début de notre stage académique au sein d'**AFEC CAMEROUN**. Dès notre arrivé, nous avons été accueillis chaleureusement par **M. WAMBO Jérémie** consultant à AFEC, qui nous a conduits à l'atelier d'activités ou nous travaillerons durant toute la période de stage, la salle « **Training room** ». Après une phase de présentation des différents stagiaires, il nous a édifié sur les fonctions principales d'**AFEC CAMEROUN** et les différentes règles qui régissent la structure telle que l'esprit d'équipe, la discipline, le respect, la serviabilité, la discrétion et la ponctualité. Par la suite, nous avons pris connaissance des différents travaux pratiques que nous allons réaliser pendant notre stage, il a été également mis à notre disposition des thèmes de stage au choix. Et en fin de journée il nous a été créé des comptes étudiants sur la plateforme Cisco nous permettant ainsi d'avoir accès aux formations sur lesquelles on travaillera et qui pourront nous aider dans nos différents thèmes de stage.

## II- PRESENTATION DE LA STRUCTURE

Le cabinet professionnel "**Audit Formation Evaluation Conseil**" en abrégé AFEC Cameroun est une entreprise moderne et ambitieuse créée en 1994. Comme pôle de réflexions, d'échange d'idées et d'informations, il offre un cadre de rencontre entre acteurs économiques, décideurs et formateurs, en vue d'analyser les mutations en cours et en construire une vision prospective sur les configurations des organisations de demain. À travers de multiples missions auprès d'importantes entreprises de la place et de diverses administrations, AFEC Cameroun a forgé et affiné sa notoriété, en apportant à chacune selon ses spécificités, une réponse parfaitement adéquate. Elle déploie à ce jour une équipe aguerrie dans divers domaines tels que :

### GESTION DES RESSOURCES HUMAINES

**AFEC CAMEROUN EST DOTÉ D'OUTILS PERMETTANT DE DÉNICHER DES CANDIDATS QUI POSSÈDENT UN SAVOIR-FAIRE CONCURRENTIEL, AINSI QU'UN SAVOIR-ÊTRE ET DES VALEURS COHÉRENTES AVEC LA MISSION DE L'ENTREPRISE. DEUX ENJEUX CRUCIAUX À LA GESTION DES RESSOURCES HUMAINES CONSISTENT À EMBAUCHER UNE MAIN- D'ŒUVRE COMPÉTENTE ET À AFFECTER LES EMPLOYÉS À DES POSTES OU ILS SERONT EFFICACES ET SATISFAITS POUR LES OBJECTIFS SUIVANTS:**

- Maximiser l'utilisation des Ressources Humaines et assurer leur développement continu
- S'assurer d'avoir la capacité de production nécessaire pour soutenir les objectifs organisationnels
- Coordonnée les activités des ressources humaines avec les objectifs organisationnels
- Inciter les personnes compétentes à poser leurs candidatures pour un poste donné
- Augmenter le bassin de connaissances et d'habiletés par l'ajout de nouvelles ressources
- Définir les attentes et les orientations de l'entreprise et donner l'information à tous les employés
- Préciser les règles de fonctionnement de l'entreprise et favoriser l'engagement des employés
- Faciliter et favoriser l'intégration sociale et professionnelle de l'employé dans son nouveau milieu de travail ...etc.

### L'archivistique

C'est un outil de mise en œuvre des principes et techniques régissant la création, l'évaluation, l'accroissement, le classement, la description, l'indexation, la diffusion et la préservation des archives. Par ce service, AFEC Cameroun permet à votre entreprise :

- D'assurer la continuité de sa gestion ;
- De satisfaire les exigences de son environnement réglementaire ;
- D'assumer ses responsabilités à l'égard de ses employés, de ses clients et, éventuellement, de ses actionnaires ;
- De constituer son patrimoine archivistique susceptible d'être partagé avec l'ensemble de la société.

## ➤ La documentation

Outil de mise en œuvre de l'ensemble des techniques permettant le traitement permanent et systématique de documents ou de données, incluant la collecte, le signalement, l'analyse, le stockage, la recherche, la diffusion de ceux-ci, pour l'information des usagers.

## ➤ L'accompagnement Psychologique

Dans ce service, AFEC-Cameroun offre des ateliers PSY (pour l'amélioration de la santé mentale). Comme ateliers nous pouvons avoir :

- Séance de "ConnaissanceDeSoi" à caractère thérapeutique animé par une psychologue
- De la psychologie pour les "PasDuToutFou".

## ➤ La formation professionnelle des adultes

Au cabinet de prestations intellectuelles, la formation est un ensemble d'activités d'apprentissage planifiées. Elle vise l'acquisition du savoir propres à faciliter l'adaptation des individus et des groupes à leur environnement socio-professionnel. Elle contribue à la réalisation des objectifs d'efficacités de l'organisation. Les différents domaines de formations sont :

- Comptabilité / Gestion
- Informatique / Bureautique
- Administration de base de données
- Administration de data Warehouse
- Formation certifiant Oracle
- Formation découverte Linux
- Formation certifiant Linux
- Assistance de Direction
- Gestion des Ressources Humaines/Management
- Techniques Commerciales
- Techniques administratives
- Législation de travail et Contentieux
- Documentation, Gestion d'archives

- Internet (Navigation et création des pages Web).

#### L'ADMINISTRATION DES EXAMENS DE CERTIFICATION

AFEC Cameroun est un centre agréé auprès de divers vendeurs pour des tests de certifications et de reconnaissance de compétences. Elle est l'adresse fiable pour passer aux dates et heures voulues tout examen de certification la certification, entendue comme indicateur de qualification sociale. Nous citons ici ceux que vous trouverez dans nos services en ce jour :

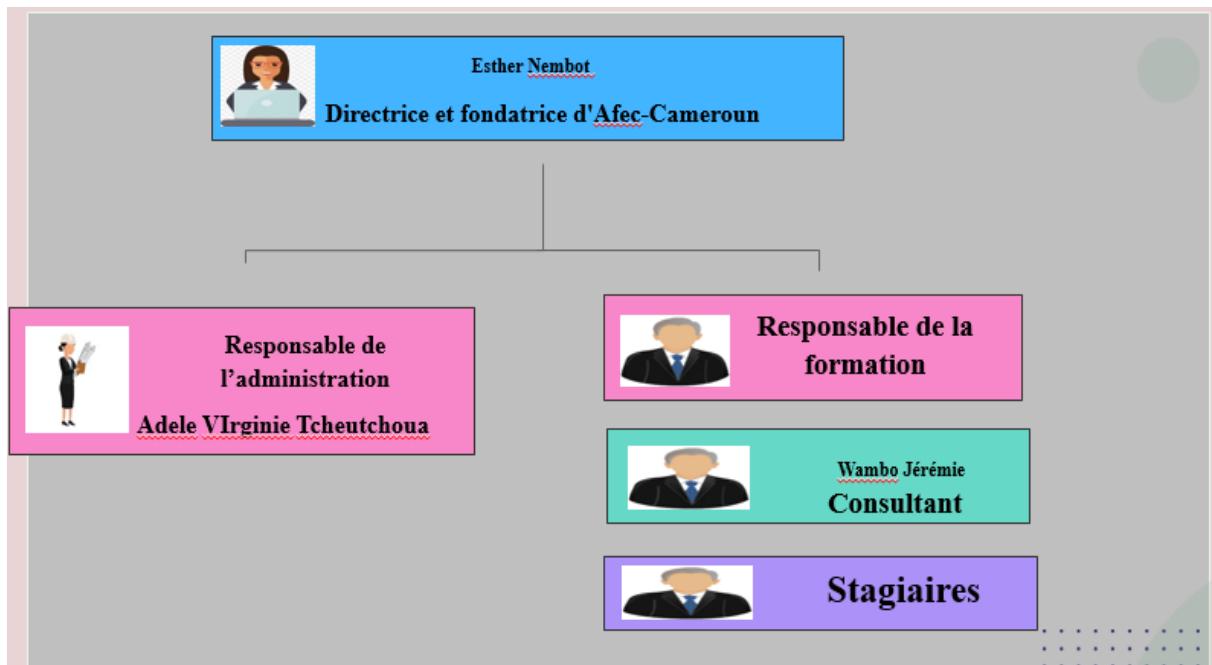
- Pearson VUE
- KRYTERION
- ACT

### **1. LES PARTENAIRES D'AFEC CAMEROUN**

Comme partenaires nous avons :

- La fondation FAIRMED
- Gendarmerie nationale
- EIFORCES
- Crédit du Sahel
- Ministère de l'enseignement supérieur
- L'IAI-Cameroun
- CAMTRAV
- HD Conception
- SINNOTECH
- Les Brasseries du Cameroun

## ORGANIGRAMME



**Figure 1: Organigramme d'AFEC CAMEROUN**

## 2. PLAN DE LOCALISATION

L'entreprise est localisée à Yaoundé plus précisément en face de la pharmacie intendance allant vers camairco.

La localisation exacte de l'entreprise est facilitée par le plan suivant :



**Figure 2: plan de localisation AFEC (Source : Entreprise)**

### **3. FICHE SIGNALÉTIQUE DE LA STRUCTURE**

<i>Nom de la structure</i>	<i>Audit</i> <i>Formation</i> <i>Evaluation</i> <i>Conseil</i>
<i>Logo de la structure</i>	 <b>AFEC Cameroun</b>
	<i>Source : </i> <a href="https://afecameroun.com/">https://afecameroun.com/</a>
<i>Sigle de la structure</i>	<b>AFEC</b>
<i>Date de création</i>	<b>1994</b>
<i>Statut juridique</i>	<b>SARL</b>
<i>Directrice générale</i>	<b>Mme NEMBOT Esther</b>
<i>Siege Social</i>	<b>Yaoundé, Carrefour intendance</b>
<i>Téléphones</i>	<b>+237 242 114 195 / +237 699 904 179</b>
<i>Adresse E-mail</i>	<b>info@afecameroun.com</b>
<i>Site Web</i>	<b>www.afecameroun.com</b>

**Tableau 1 : Fiche Signalétique AFEC**

#### **4. RESSOURCES MATERIELLES ET LOGICIELLES**

AFEC dispose de plusieurs équipements indispensables pour que le rendu des services qu'ils offrent soit optimal.

EQUIPEMENT	MARQUE	QUANTITE
<b>Ordinateur de bureau</b>	<b>DELL</b>	<b>06</b>
<b>Ordinateur portable</b>	<b>DELL</b>	<b>05</b>
<b>Switch</b>	<b>TP-LINK</b>	<b>01</b>
<b>Routeur</b>	<b>Huawei</b>	<b>02</b>
<b>Point d'accès</b>	<b>TP-LINK</b>	<b>01</b>
<b>Imprimante</b>	<b>HP</b>	<b>01</b>
<b>Kit Arduino</b>	/	<b>02</b>

**Tableau 2 : Ressources Matérielles**

TYPES DE LOGICIELS	LOGICIELS
<b>Les Systèmes d'exploitation</b>	<b>Windows</b>
	<b>Debian</b>
<b>Les Technologies</b>	<b>Python</b>
	<b>JavaScript</b>
	<b>C</b>
<b>Les outils de simulation</b>	<b>Cisco Packet Tracer</b>
	<b>GNS 3</b>
	<b>EVE</b>
<b>Les éditeurs de texte</b>	<b>Arduino</b>

**Tableau 3: Ressources Logicielles**

## **CONCLUSION**

Arrivée au terme de cette phase d'insertion, nous avons eu un rapide aperçu du fonctionnement d'AFEC Cameroun. Nous nous sommes familiarisés au monde professionnel et avons pris part aux tâches qui nous ont été confiées. La bonne collaboration ainsi que la disponibilité de nos encadreurs techniques nous ont permis de nous imprégner des réalités et des besoins réels auxquels fait face la société en elle-même. Ainsi nous avons porté un intérêt accru au domaine de la sécurité précisément de la « **MISE EN PLACE D'UN SYSTÈME DE SECURITE (DOUBLE AUTHENTIFICATION AVEC RADIUS) RESEAU AVEC SUPERVISION PRTG** ». Afin de mieux cerner le problème et de faire des propositions de solution, il est donc primordial pour nous d'élaborer un cahier de charges.

## DEUXIEME PARTIE : PHASE TECHNIQUE

### Préambule :

Dans cette deuxième partie de notre rapport, nous ressortirons quelques spécificités du sujet choisi pour notre stage, nous procéderons par la suite à l'examen méthodique et détaillé de la future solution à mettre en place pour obtenir un résultat, et enfin nous ferons des tests pour se rassurer que tout a été bien fait en présentant les résultats obtenus.

### Aperçu :

---

#### INTRODUCTION

**CHAPITRE I : ANALYSE DU PROJET**

**CHAPITRE II : CAHIER DE CHARGES**

**CHAPITRE III : ETAT DE L'ART**

**CHAPITRE IV : PRESENTATION DES OUTILS CHOISIS**

**CHAPITRE V : IMPLEMENTATION ET REALISATION**

**CHAPITRE VI : TESTS ET FONCTIONNALITES**

#### CONCLUSION

---

## **INTRODUCTION**

La phase d'insertion nous ayant permis d'effectuer le recueil d'information relatives à la structure et aux conditions d'accueil qui nous ont été réservées ; cette deuxième partie nous permet de présenter les attentes communes du maître d'œuvre et du maître d'ouvrage en ce qui concerne la réalisation du projet qui nous a été confié pendant la phase d'insertion. C'est la phase technique et pratique de l'analyse informatique. Cette partie de notre rapport mettra en exergue une phase d'analyse, le cahier de charge, l'état de l'art, l'implémentation de la solution et un test accompagné des résultats en vue d'énoncer des différentes perspectives.

## CHAPITRE 1 : ANALYSE DU PROJET

### Préambule :

Ce modèle d'analyse de projet présente des informations concentrées sur le projet et dessine le contour de ses grandes étapes

### Aperçu :

---

I : PRESENTATION DU PROJET

II : ETUDE DE L'EXISTANT

III : CRITIQUE DE L'EXIXTANT

IV : PROBLEMATIQUE

---

## I. PRESENTATION DU PROJET

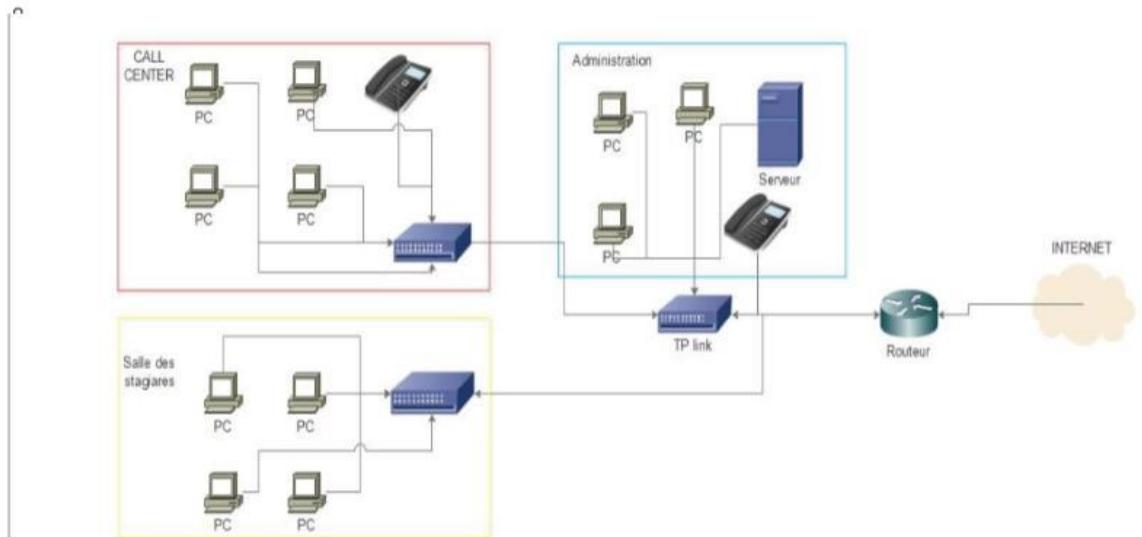
A notre arrivée à AFEC, pour accéder à un routeur il y'avait pas d'authentification à partir de PUTTY c'est-à-dire que pour accéder à un routeur il ne fallait pas insérer son login et son mot de passe via l'application PUTTY ce qui n'était pas sécurisé pour une grande entreprise comme AFEC. Cette façon d'accéder à un routeur était moins sécurisé par conséquent facile pour un man in middle de le pirater ce qui n'étant pas professionnelle pour une entreprise d'une telle envergure. Notre projet s'appuie ainsi sur la « **MISE EN PLACE D'UN SYSTÈME DE SECURITE (DOUBLE AUTHENTIFICATION AVEC RADIUS) RESEAU AVEC SUPERVISION PRTG : cas d'AFEC CAMEROUN** » consistant à implémenter un système pour le renforcement de la sécurité.

## II. ETUDE DE L'EXISTANT

Pour une meilleure compréhension de l'environnement de sécurité informatique, il est essentiel de maîtriser le fonctionnement des dispositifs d'authentification existants, puis de définir les paramètres d'optimisation qui pourraient contribuer à leur amélioration. Dans notre cas, nous nous concentrerons sur la mise en place d'un système de sécurité basé sur l'authentification à double facteur (2FA) avec RADIUS. Après avoir observé les systèmes d'authentification en place dans notre infrastructure, nous avons constaté qu'ils reposent souvent sur des méthodes d'authentification uniques, ce qui expose le réseau à des risques accrus. Cela signifie que les mécanismes de contrôle d'accès sont limités et ne changent pas en fonction des menaces potentielles. Il est également important de noter que certains accès critiques ne disposent pas de mesures de sécurité renforcées, ce qui constitue une vulnérabilité importante. Pour proposer une nouvelle approche en matière de sécurité des accès, nous avons choisi d'examiner un cas concret au sein de notre réseau : l'accès aux ressources sensibles de l'entreprise. Ce cas servira de modèle pour simuler l'implémentation du système d'authentification à double facteur et l'intégration avec PRTG pour la supervision continue.

## **1. ARCHITECTURE DE AFECameroun**

Cette architecture nous permettra de mieux cerner les contours de notre thème :



**Figure 3: Topologie actuel de afec**

## **2. DESCRIPTION DE L'ARCHITECTURE**

Cette architecture comprend :

- 11 PC
- 3 switch
- 1 routeur
- 1 serveur
- 2 téléphone fixe
- Nuage Internet

### III. CRITIQUE DE L'EXISTANT

Après une étude de l'existant, nous avons pu relever quelques manquements.

<i>CRITIQUES</i>	<i>CONSEQUENCES</i>	<i>SOLUTIONS</i>
<b>Utilisation d'un seul mot de passe pour l'accès aux systèmes.</b>	Risque élevé de compromission des comptes en raison de la réutilisation des mots de passe.	Implémentation d'un système de double authentification via RADIUS pour renforcer la sécurité des accès.
<b>Manque de surveillance des activités réseau et des accès utilisateurs.</b>	Difficulté à détecter des tentatives d'intrusion ou des comportements suspects en temps réel.	Mise en place de PRTG pour une supervision continue et des alertes en cas d'anomalies détectées.
<b>Faible sensibilisation des utilisateurs aux bonnes pratiques de sécurité.</b>	Risque accru d'erreurs humaines pouvant compromettre la sécurité (phishing, choix de mots de passe faibles).	Organisation de sessions de formation et de sensibilisation sur la sécurité informatique et l'utilisation de la double authentification.
<b>Difficultés d'intégration des nouveaux outils de sécurité dans l'infrastructure existante.</b>	Risque de dysfonctionnements ou de résistance à l'adoption des nouvelles solutions.	Élaboration d'un plan d'intégration détaillé avec des phases de test et de déploiement progressif.

*Tableau 4 : Critique de l'existence*

### IV. PROBLÉMATIQUE

Les solutions technologiques de sécurité des réseaux sont des outils que les organisations peuvent intégrer dans leurs processus de protection des données pour améliorer de manière rentable la sécurité des accès et la gestion des utilisateurs. Le déploiement de ces solutions, ou la mise à niveau des infrastructures existantes, peut générer d'importants gains

en matière de sécurité et de réduction des coûts liés aux incidents. Ainsi, nous nous posons la question suivante : COMMENT METTRE EN PLACE UN SYSTÈME DE SECURITE (DOUBLE AUTHENTIFICATION AVEC RADIUS) RESEAU AVEC SUPERVISION PRTG ?

## CHAPITRE 2: CAHIER DE CHARGES

### Préambule :

Le cahier de charges a pour but de décrire le fonctionnement du système existant afin d'en dégager les insuffisances et le cas échéant, de proposer d'éventuelles solutions susceptibles d'y remédier et de satisfaire les utilisateurs du dit système.

### Aperçu :

---

**I : CONTEXTE DU PROJET**

**II : OBJECTIFS DU PROJET**

**III : EXPRESSION DES BESOINS DE L'UTILISATEUR**

**IV : ESTIMATION DU COÛT**

**V : PLANIFICATION DU PROJET**

**VI : LES CONTRAINTES DU PROJET**

**VII : LES LIVRABLES**

---

## I. CONTEXTE DU PROJET

La sécurité des réseaux est un enjeu crucial pour les organisations modernes, particulièrement avec l'augmentation des cyber menaces. Les utilisateurs se connectent quotidiennement à des systèmes sensibles pour diverses activités, que ce soit pour le travail, les transactions financières, ou d'autres services en ligne. Selon les rapports de sécurité, les vulnérabilités des systèmes d'authentification sont à l'origine de problèmes tels que le vol de données, les accès non autorisés et les pertes financières. L'augmentation du nombre d'utilisateurs et de dispositifs connectés aggrave la situation, rendant nécessaire une protection renforcée des accès. Les systèmes d'authentification traditionnels, reposant sur des mots de passe uniques, montrent leurs limites face aux nouvelles menaces. De simples mises à jour des protocoles de sécurité peuvent considérablement améliorer la protection des données, ce qui est essentiel pour le développement durable des infrastructures numériques. Il est également impératif d'intégrer des solutions de supervision pour surveiller l'activité des utilisateurs et détecter les comportements suspects en temps réel. Par conséquent, il est nécessaire de simuler et d'optimiser les mécanismes d'authentification. Ces systèmes doivent utiliser diverses technologies pour surveiller, évaluer et gérer les accès afin d'améliorer l'efficacité et la sécurité.

## II. OBJECTIFS DU PROJET

### 1- Objectif global

L'objectif général du projet est de mettre en place un système d'authentification à double facteur (2FA) utilisant le protocole RADIUS pour gérer dynamiquement les accès aux ressources sensibles en fonction des comportements d'accès des utilisateurs.

### 2- Objectifs spécifiques

Pour atteindre cet objectif général, plusieurs objectifs spécifiques doivent être réalisés :

- **Déetecter les tentatives d'accès non autorisées** : grâce à des systèmes de surveillance et d'analyse des logs qui surveillent en permanence les tentatives d'accès aux ressources.
- **Ajuster dynamiquement les niveaux d'accès** : la détection des comportements suspects permettra un contrôle adaptatif, entraînant des ajustements automatiques des permissions d'accès en fonction du risque identifié.
- **Mettre en place un réseau sécurisé pour le centre de contrôle** : assurer une communication fiable entre le serveur RADIUS et les dispositifs clients.
- **Développer un système de comptage et de journalisation** : spécifiant la durée et la nature des accès pour améliorer la traçabilité.

### III. EXPRESSION DES BESOINS DE L'UTILISATEUR

L'efficience d'un projet s'évalue en fonction de la satisfaction des besoins des utilisateurs. L'expression des besoins est un point important dans le cycle de vie d'un dispositif qui permet de déterminer les nouvelles fonctionnalités à apporter à un système pour améliorer son rendement.

#### 1 LES BESOINS FONCTIONNELS

Pour identifier les besoins exprimés par les utilisateurs, nous avons mené une étude sur le fonctionnement des systèmes existants. Grâce aux informations recueillies, nous avons élaboré une stratégie visant à résoudre les problèmes identifiés tout en améliorant la gestion des accès. Il s'agit notamment de :

- **Déetecter les comportements suspects lors des connexions** (sécurité renforcée).
- **Installer un système de surveillance pour l'accès aux ressources** (sécurité publique).

- **Mettre en place une plateforme d'administration et de suivi des accès** (contrôle distant).
- **Authentifier l'administrateur du centre de contrôle** pour garantir la sécurité administrative.
- **Développer un système visuel pour le suivi et la durée des sessions d'accès.**

## 2 LES BESOINS NON FONCTIONNELS

Ces besoins caractérisent le système en termes de performance, matériel ou conception :

- **Respect de la vie privée** : Les dispositifs doivent recueillir des informations pertinentes sans compromettre l'intimité des utilisateurs.
- **Disponibilité** : La sûreté et la fiabilité du système sont essentielles pour garantir un fonctionnement continu.
- **Rapidité du traitement** : Il est impératif que la durée d'exécution des processus soit minimale, surtout dans les situations critiques.
- **Portabilité** : Le système doit être adaptable à divers environnements technologiques tout en maintenant son efficacité.

## VI. ESTIMATION DU COÛT DU PROJET

Il s'agit de l'évaluation de la somme des coûts des ressources humaines, matérielles, et logicielles nous ayant permis de réaliser notre projet. Il faut noter que ces estimations sont faites en prenant en compte l'implémentation de quatre feux.

### 1) LES RESSOURCES HUMAINES

Les détails estimatifs du coût du projet sont ventilés dans le tableau ci-après:

<i>NOMS ET PRENOMS</i>	<i>FONCTIONS</i>	<i>ROLES</i>
<b><i>M. WAMBO Jérémie</i></b>	<i>Consultant à AFEC</i>	<b><i>Encadrant Professionnel</i></b>
<b><i>M. CHATCHUIN DJOKO DASSY</i></b>	<i>Enseignant à l'IAI Cameroun</i>	<b><i>Encadrant Académique</i></b>
<b><i>Mpacko Darren</i></b>	<i>Stagiaire à AFEC</i>	<b><i>Main d'œuvre</i></b>
<b><i>AFECameroun</i></b>	<i>Maitre d'ouvrage</i>	<b><i>Entreprise d'accueil</i></b>

***Tableau 5 :Ressources Humaines***

## **2) Ressources logicielles**

Les ressources logicielles devant être exploitée sont répertoriées dans le tableau ci-après.

Ressources logiciels	Version	Prix unitaires (CFA)
Totpraduis	0.3	3677FCFA
Windows server	2022	655 000 FCFA
Windows 11	2024	130 000 FCFA
Microsoft Office	2016	97 000 FCFA
Microsoft Edge	128.0.2739.63	Gratuit
GNS3	2.2.48.1	Gratuit

***Tableau 6: Ressources logicielles (Source : fait sur Word 2019)***

## **3) Ressources matérielles**

Les ressources matérielles identifiés pour le projet sont répertoriées dans ce tableau

OUTILS	QUANTITÉS	PRIX UNITAIRE (CFA)	PRIX TOTAL (CFA)

<b>CONNECTEUR RJ45</b>	10	100	1.000
<b>SWICTH TP LINK (48)</b>	3	225.945	677.835
<b>ROUTEUR Link Sys wrt160NI- EW</b>	1	85000	85.000
<b>CABLES ETHERNET</b>	2	30.000	60.000
<b>Ordinateur Portables HP PROBOOK (HDD :500Go, RAM :4Go, CORE i5)</b>	3	250.000	750.000
<b>MODEM MTN (Forfait trimestriel)</b>	1	30.000	30.000
<b>MODEM Orange (Forfait trimestriel)</b>	1	30.000	30.000
<b>Totaux</b>	1.603.835		

***Tableau 7: Ressources matérielles (Source : fait sur Word 2016)***

#### **4) COÛT TOTAL DU PROJET**

RESSOURCES	MONTANT
<i>Humaines</i>	<b>21.600.000 Fcfa</b>
<i>Matérielles</i>	<b>1.603.835 Fcfa</b>
<i>Logicielles</i>	<b>324.300 Fcfa</b>
<i>Imprévus (10%)</i>	<b>2.984.000 Fcfa</b>
<b>TOTAL</b>	<b>32.229.800 Fcfa</b>

**Tableau 8: cout total du projet**

#### **V. PLANNIFICATION PROJET**

La planification d'un projet est une étape incontournable et essentielle pour l'avancement et la réussite de ce dernier. Le but étant d'établir le calendrier du projet, il s'agira de :

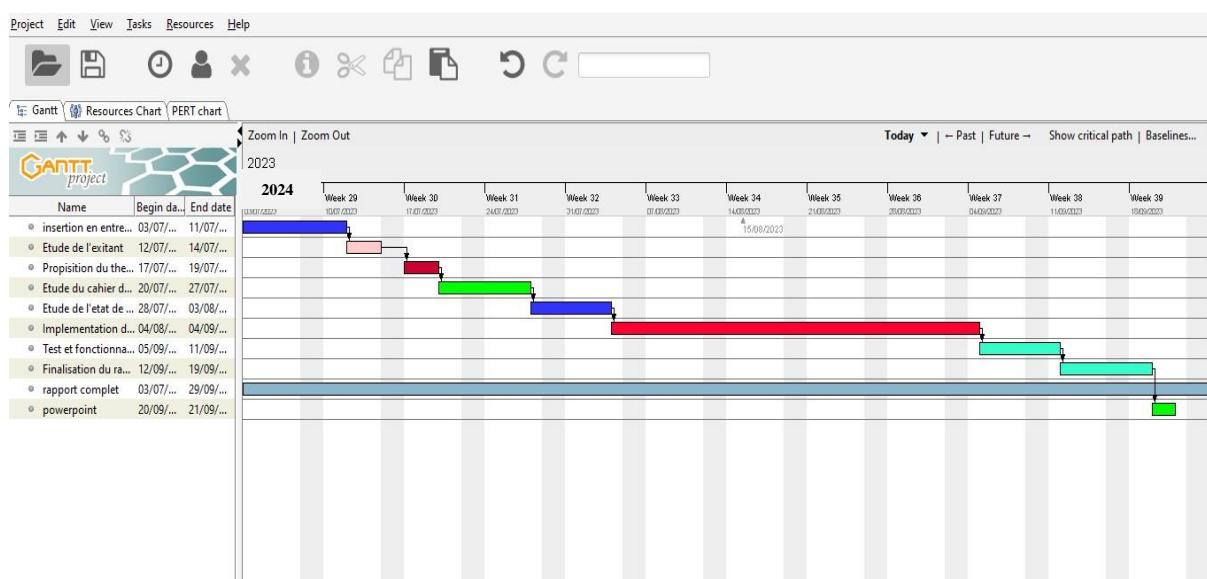
- Identifier les tâches à réaliser et de les hiérarchiser
- Définir leurs durées et leurs échéances (ordonnancement des tâches) ;
- Attribuer à ces tâches les ressources nécessaires (définition du planning) ;
- Identifier les risques.

La phase de planification vise donc à définir comment le projet sera exécuté, surveillé, contrôlé puis clôturé.

PHASE	OBJECTIF	RESULTAT	DUREE (semaine)

<b>INSERTION</b>	<b>Prise de contact et d'informations sur l'entreprise d'accueil</b>	Dossier d'insertion	01
<b>ANALYSE PROJET</b>	<b>Présentation du thème</b> <b>Etude de l'existant</b> <b>Problématique</b>	Chapitre 1	01
<b>CAHIER DE CHARGES</b>	<b>Spécification des besoins utilisateurs</b>	Chapitre 2	01
<b>ETAT DE L'ART</b>	<b>Identification des connaissances</b>	Chapitre 3	01
<b>IMPLEMENTATION DE LA SOLUTION</b>	<b>Configuration</b>	Chapitre 4	05
<b>TESTS DE FONCTIONNALITÉS</b>	<b>Tester la solution</b>	Chapitre 5	01

**Tableau 9 : tableau d'ordonancement**



**Figure 4: Diagramme de Gantt**

## VI. LES CONTRAINTES DU PROJET

### 1) LES CONTRAINTES DE COUT

La réalisation de notre projet nécessitera des dépenses en ressources humaines, Matérielles et logicielles pour un total de **32.229.800 Fcfa.**

### 2) LES CONTRAINTES DE DELAI

Notre projet devra être réalisé sur une durée de 02 mois, à savoir du 04 Aout 2024 au 31 Septembre 2024.

### 3) LES CONTRAINTES DE QUALITE

Le système résultant de la réalisation de notre projet devra suivre les contraintes de qualité suivante :

- Il devra être robuste, c'est-à-dire devra fonctionner avec le moins d'erreurs possible...
- Il devra être évolutif, c'est-à-dire capable de s'adapter aux différentes architectures d'intersections.
- Il devra être ergonomique, c'est-à-dire établir un bon contraste entre les besoins fonctionnels et non fonctionnels de l'utilisateur, tout en gardant un équilibre entre les performances.

## VII. LES LIVRABLES

À la fin de ce projet, nous devons fournir :

- Un document concernant le projet comportant : un dossier d'insertion et un dossier technique ;
- Un DVD comportant : Le rapport de stage, le power point de notre travail et le code source du microcontrôleur et l'application.

L'élaboration d'un cahier de charges est une étape importante dans la conception d'une solution informatique. Ce document nous a permis de mieux cadrer notre projet et de connaître de manière exacte la route à suivre et les tâches à effectuer dans les délais prescrits.

## CHAPITRE 3 : ETAT DE L'ART

### Préambule :

Cette partie consiste à rechercher toutes les informations concernant l'authentification et la supervision et en faire une synthèse.

### Aperçu :

---

**I : INTRODUCTION SUR LA SECURITE RESEAU**

**II : GENERALITE SUR LA DOUBLE AUTHENTIFICATION**

**III : PROTOCOLES RADIUS**

**IV : SURVEILLANCES ET GESTIONS DU RESEAU**

**V : NORMES ET REGLEMENTATIONS**

---

## I. INTRODUCTION SUR LA SECURITE RESEAU

### A. DEFINITION ET OBJECTIFS

#### 1. Définition de la sécurité informatique

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques. Elle est intrinsèquement liée à la sécurité de l'information et des systèmes d'information.

#### 2. Les objectifs de la sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs :

- **La disponibilité** : Le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
- **L'intégrité** : Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.
- **Les confidentialités** : Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.
- **L'authentification** : L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.
- **La non-réputation** : Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

### B. La politique de sécurité

La politique de sécurité exprime la stratégie de l'entreprise en matière de sécurité de l'information. Toutefois, il n'existe pas de règles déclinables à tous, chaque entreprise présente des particularités et utilise une politique de sécurité selon l'architecture de son réseau. La sécurité définit les règles à suivre pour l'accès au réseau informatique et pour gérer les flux de données entrants et sortants. La mise en place d'une politique de sécurité adéquate est essentielle à la bonne sécurisation des réseaux et des systèmes d'information.

Une politique de sécurité doit comprendre au moins les éléments suivants :

- Les fondements de la sécurité de l'information propre à l'organisme intégrant les obligations légales et les missions propres à l'organisme précisera notamment les principes régissant la protection des données à caractère personnel.
- Les exigences de sécurité à respecter en termes de confidentialité, intégrité, disponibilité, imputabilité, authenticité, fiabilité et non répudiation des informations.
- Les différents éléments de sensibilisation aux arguments et au contenu même de cette politique définie par l'organisme.
- La description des différents rôles, responsabilités et règles organisationnelles cadrant la mise en application de la politique.
- La démarche de gestion des risques adoptée par l'organisme afin de détecter les risques, de les apprécier selon des critères définis et de déterminer les modalités pour les traiter en les réduisant à un niveau acceptable.
- La description du cadre organisationnel des processus de gestion des incidents de sécurité.
- Les modalités générales de gestion de la sécurité de l'information, notamment en matière de protection et de prévision.
- Les modalités retenues par l'organisme afin d'intégrer la politique de sécurité dans les processus de développement, de maintenance et de changement.

## 1. Les objectifs d'une politique de sécurité

La définition d'une politique de sécurité est une démarche de toute l'entreprise visant à protéger son personnel et ses biens d'éventuels incidents de sécurité dommageable pour son activité. La définition d'une politique sécurité réseau fait intégralement partie de la démarche sécuritaire de l'entreprise. Elle s'étend à de nombreux domaines dont les suivants :

- Audit des éléments physiques et logiques constituant le système d'information de l'entreprise.
- Formation du personnel utilisant les moyens informatiques du système d'information.
- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace

## C. Les classifications d'attaques

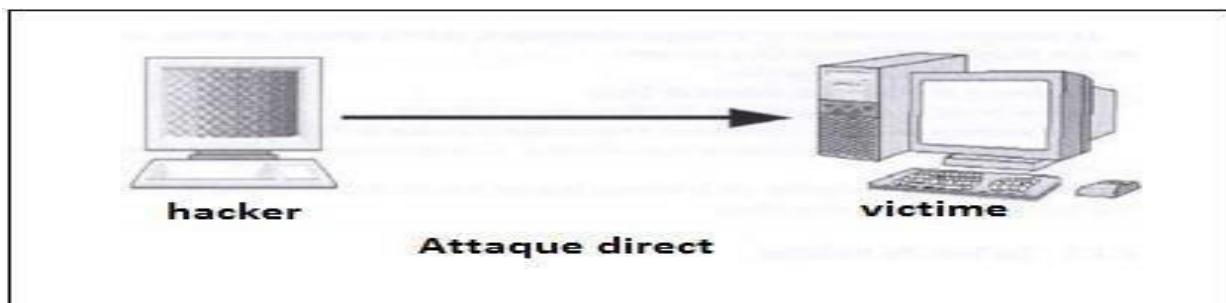
Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Celle-ci est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel, etc.) ou bien même de l'utilisateur à des fins non autorisées par l'exploitant des systèmes.

Sur le réseau Internet, des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire.

### 1. Types d'attaques

#### a) Les attaques directes

C'est la plus simple des attaques à réaliser : L'hacker attaque directement sa victime à partir de son ordinateur par des scripts d'attaques faiblement paramétrable.



**Figure 5: Attaque directe. (Source : google image)**

**b) Les attaques indirectes par rebond**

Dans ce cas, une machine cible est attaquée par l'intermédiaire d'une autre machine.



**Figure 6: Attaque par rebond (source : google image)**

**c) Les attaques indirectes par réponse**

Cette attaque est une dérivée de la précédente. La réponse à la première attaque représente une attaque plus virulente pour la machine cible.

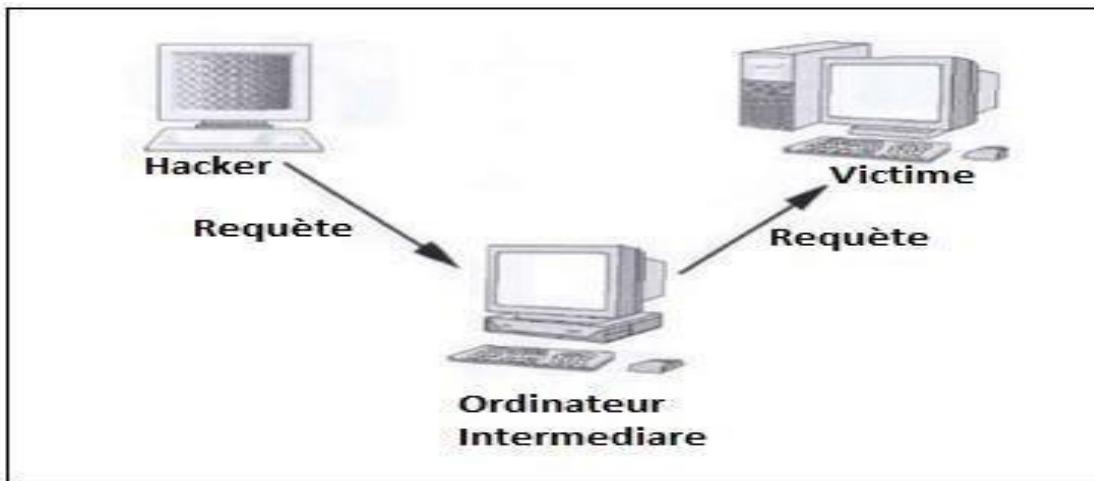


Figure 7: Attaque indirecte par réponse (source : google image)

## 2. Attaques sur les réseaux

### a) Attaque par usurpation d'adresse IP (IP spoofing)

Cette attaque consiste à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.

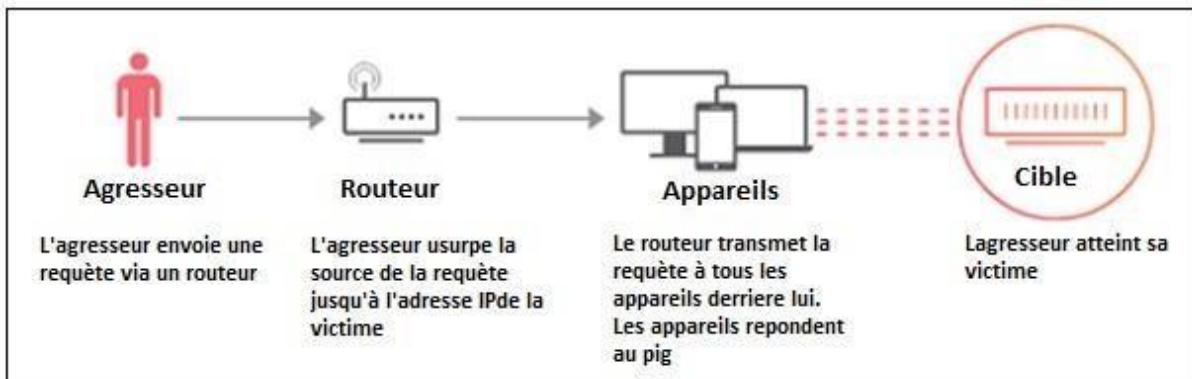
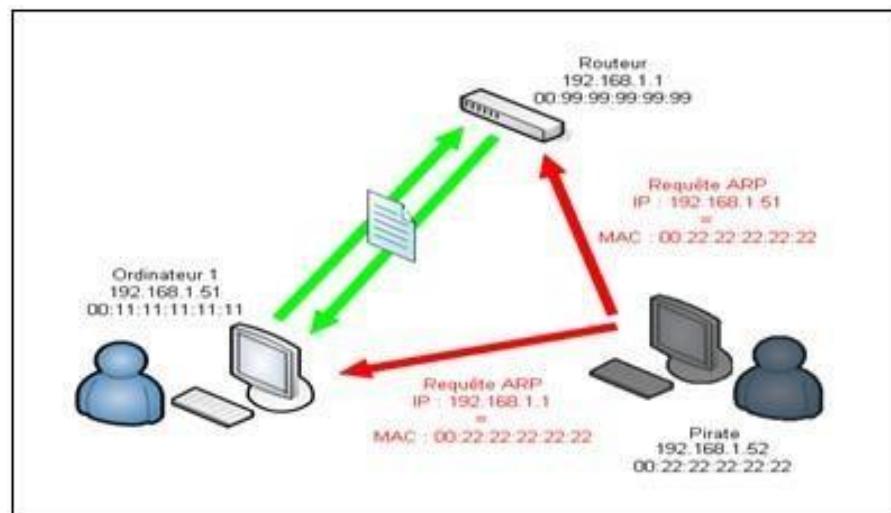


Figure 8: Attaque par adresse IP (source : google image)

### b) Attaque par usurpation d'adresse MAC (MAC spoofing)

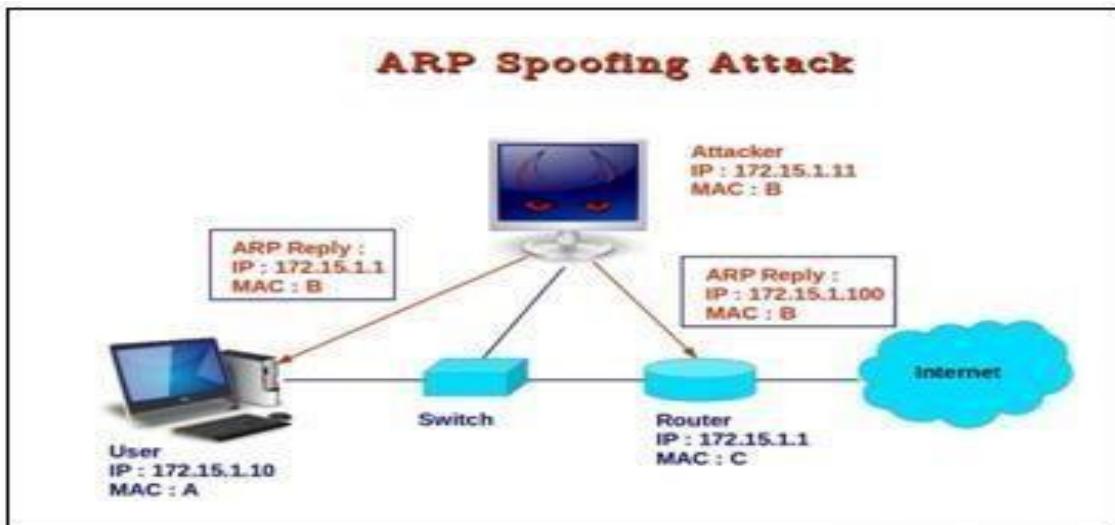
Elle consiste à se faire passer pour une machine autorisée. Il suffit à l'intrus d'utiliser l'identité (adresse MAC) d'une machine autorisée à utiliser un service donné.



**Figure 9: Attaque par adresse MAC (source : google image)**

### c) ARP spoofing

Cette attaque permet de rediriger le trafic d'une machine vers une autre. Grâce à cette redirection une personne mal intentionnée peut se faire passer pour une autre.



**Figure 10: ARP Spoofing (source: google image)**

#### **d) Attaque de mot de passe**

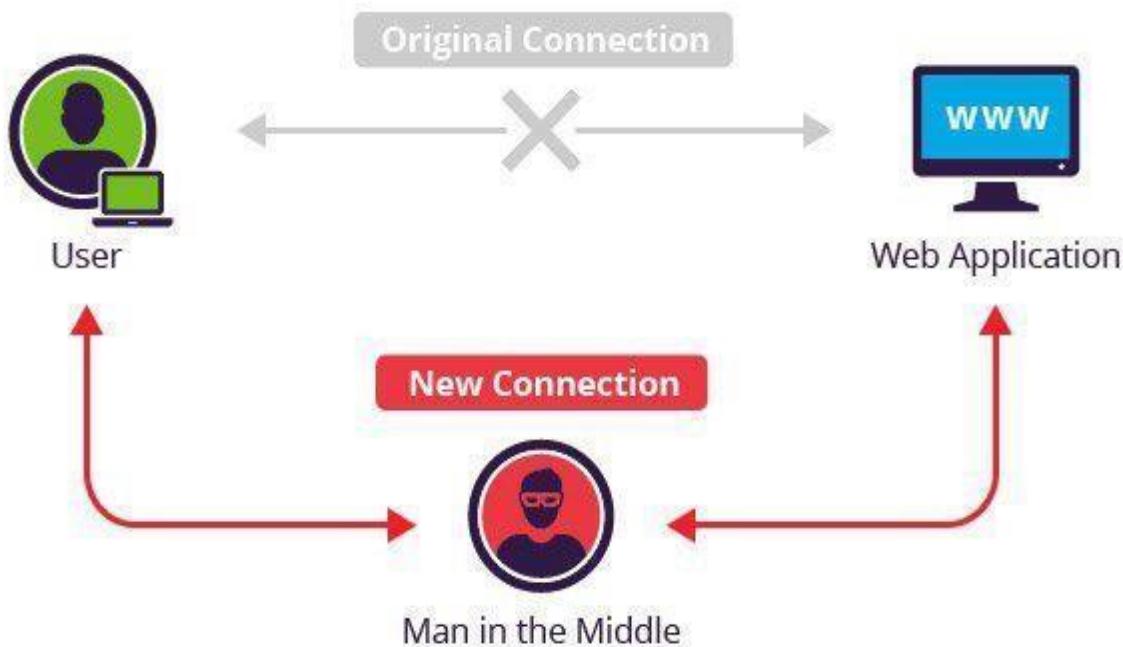
Il est très simple d'obtenir un programme permettant de retrouver le mot de passe utiliser pour l'accès à un service en utilisant des logiciels spéciaux comme les Keyloggers. Il permet de fait l'enregistrement de frappes qui espionne électroniquement l'utilisateur d'un ordinateur.

#### **e) Les portes dérobées (backdoor)**

La porte dérobée est généralement introduite par un développeur de logiciels. Celui-ci crée un chemin non-surveillé pour accéder à l'ordinateur de la victime. Une fois qu'une porte dérobée est installée avec le logiciel développé, l'attaquant a la possibilité de surveiller ce que fait l'utilisateur et de copier ou détruire les données ou bien la possibilité de prendre le contrôle d'un ordinateur (réseau).

#### **f) Attaque Man In The Middle (MITM)**

Cette attaque est une redirection complète du flux échangé entre deux machines. Chacun des interlocuteurs croit dialoguer directement avec l'autre, mais en réalité il s'adresse à une 3ème machine qui joue le rôle d'un intercepteur de ces données.



### **Figure 11:: Attaque Men in The Middle (source: google image)**

## **3. Attaques logiciel**

**Le cheval de Troie :** C'est un programme informatique malveillant parfois destructeur. Il est souvent porté par un logiciel sous licence et protégé, modifié par des hackers pour en faire cadeau à la communauté numérique, et aussi c'est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Son rôle est de faire entrer ce parasite sur l'ordinateur et de l'y installer à l'insu de l'utilisateur.

**Le virus :** C'est un programme malveillant conçu pour se propager à d'autres ordinateurs (Équipements) en s'insérant dans des logiciels légitimes.

**Les vers informatiques :** Un ver, contrairement à un virus informatique, n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

**Un spyware :** Logiciel espion qui s'installe sur un ordinateur, dans le but de collecter et transférer des informations sans que l'utilisateur en ait connaissance.

**Le déni de service (attaque DOS) :** Le principe de cette attaque consiste à envoyer des paquets IP ou de données de taille ou de constitution inhabituelle afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher d'assurer les services voulu.

## **D. Les types de menaces**

Les menaces sont classées en deux catégories :

### **1. Les menaces passives**

Elles consistent essentiellement à copier ou à écouter l'information contenue dans un système. Ces attaques nuisent à la confidentialité des données. Dans ce cas, celui qui prélève une copie ne cherche pas à altérer cette information ou le système. Ce type de menace est difficile à détecter.

## **2. Les menaces actives :**

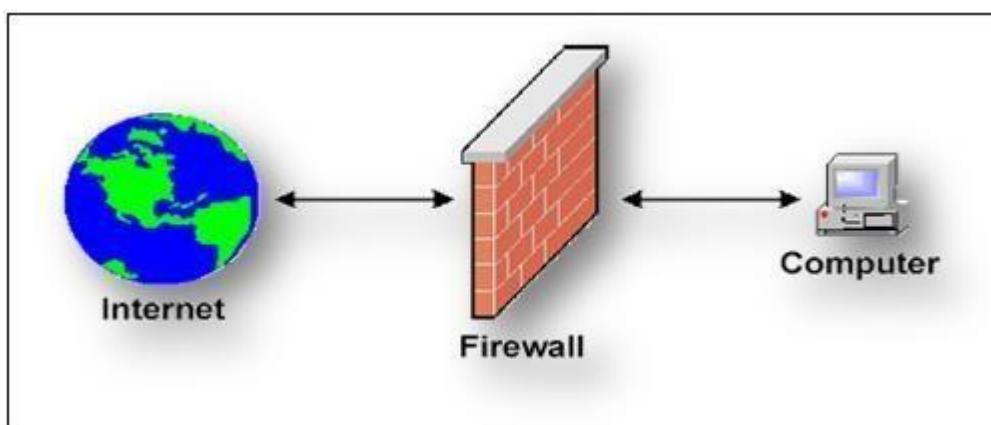
Elles nuisent à l'intégrité des données. Dans ce cas, l'intégrité ou l'existence même du système est menacé.

Les menaces dues aux accidents représentent 26% des menaces. Elles sont le fait d'incendies, de pannes d'équipements ou du réseau, défaut de qualité. 17% des menaces sont dues aux erreurs d'utilisation. 57% sont dues à la malveillance dont 80% sont d'origines interne. Elles concernent les actes tels que : Vol d'équipement, intrusions, écoute du réseau, attaque logique (virus, modification, ...).

## **E. Les outils utilisés pour sécuriser un réseau**

### **1. Le pare-feu (firewall) :**

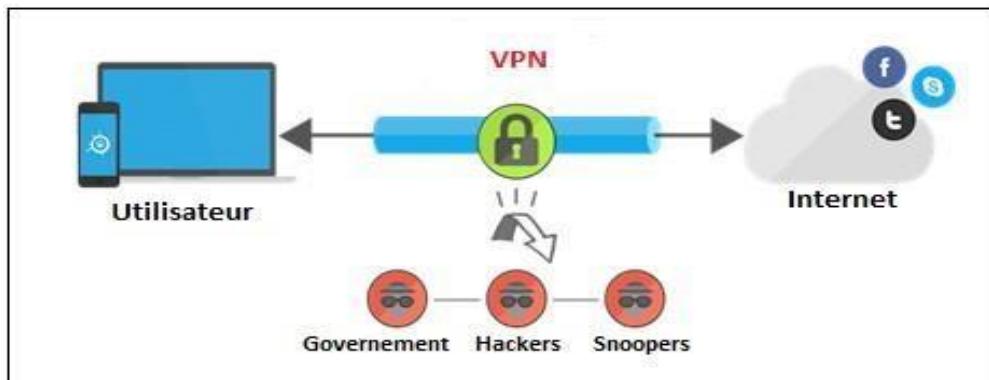
Dispositif qui protège un système informatique connecté à Internet des tentatives d'intrusion qui pourraient en provenir.



**Figure 12: Utilité d'un parefeu(source : googleimage)\***

### **2. Le VPN (Virtual Private Network):**

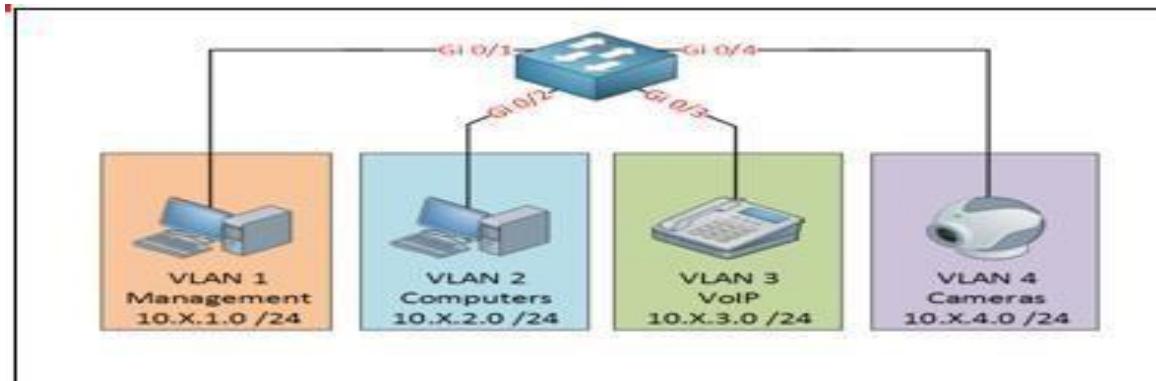
C'est un système permettant de créer un lien direct entre ordinateurs distants.  
C'est un tunnel Sécurisé à l'intérieur d'un réseau (Internet). Cependant, l'information VPN, dispose des informations permettant d'identifier l'utilisateur.



**Figure 13: Système VPN (source : google image)**

### **3. VLAN :**

Un réseau local virtuel, qui est un réseau logique indépendant sert à segmenter le réseau en sous réseaux logiques.

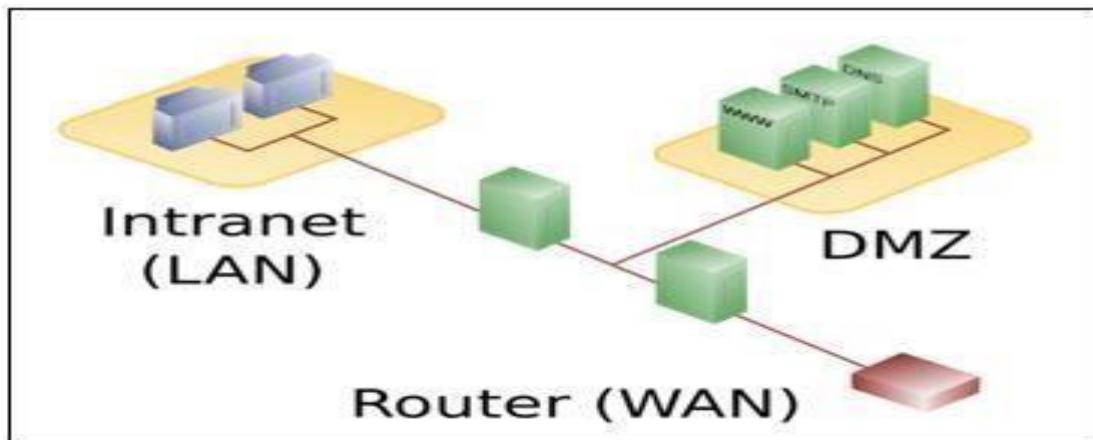


**Figure 14: Exemple d'un réseau VLAN (source : google image)**

### **4. Zone démilitarisée (DMZ) :**

Zone démilitarisée C'est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet. Le pare-feu bloquera donc les accès au réseau local pour garantir

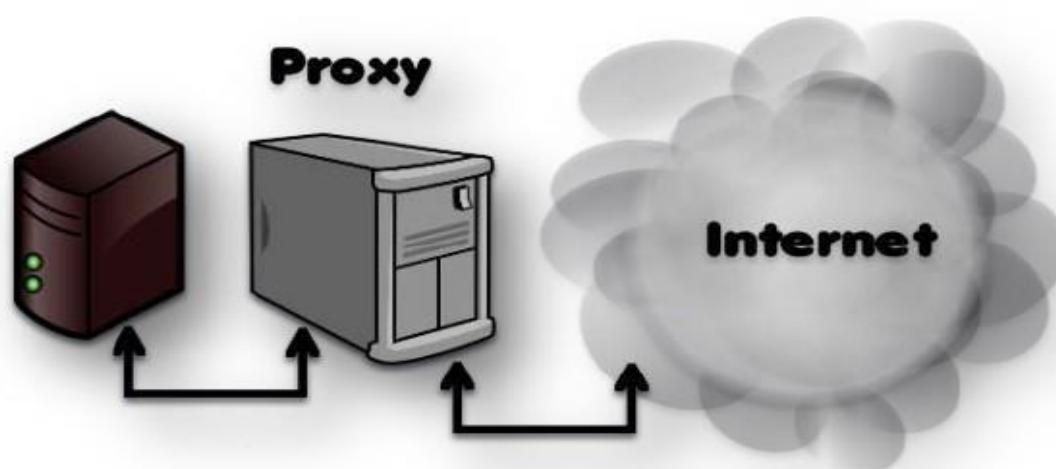
sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ. En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local.



**Figure 15: Zone DMZ (source : google image)**

## **5. Le proxy :**

C'est un composant logiciel qui joue le rôle d'intermédiaire en se plaçant entre hôtes. Dans le cas des réseaux un proxy sert à une machine intermédiaire pour accéder à un autre réseau généralement internet.



**Figure 16: Proxy (source : google image)**

## **6. Les anti-virus :**

Les anti-virus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatiques ne sont qu'une catégorie). Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiants ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

## **F. Les protocoles de sécurité**

### **1. Protocole SSL**

Le SSL est le protocole de sécurité le plus répandu qui crée un canal sécurisé entre un client et un serveur communiquant sur internet ou un réseau interne. Dans notre société centrée sur un internet vulnérable. Le SSL est généralement utilisé lorsqu'un navigateur doit se connecter de manière sécurisée à un serveur web [2]. En pratique, le SSL devrait être utilisé dans les cas suivants :

- Pour sécuriser les transactions bancaires en ligne.
- Pour sécuriser les connexions et tout échange d'information confidentielle.
- Pour sécuriser les applications et les messageries web.
- Pour sécuriser les flux de production et les applications de virtualisation tels que les plates-formes sur le Cloud.

### **2. Protocole SSH**

Le protocole SSH a été mis au point en 1995, il s'agit d'un protocole permettant à un client (un utilisateur ou même une machine) d'ouvrir une

session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisé.

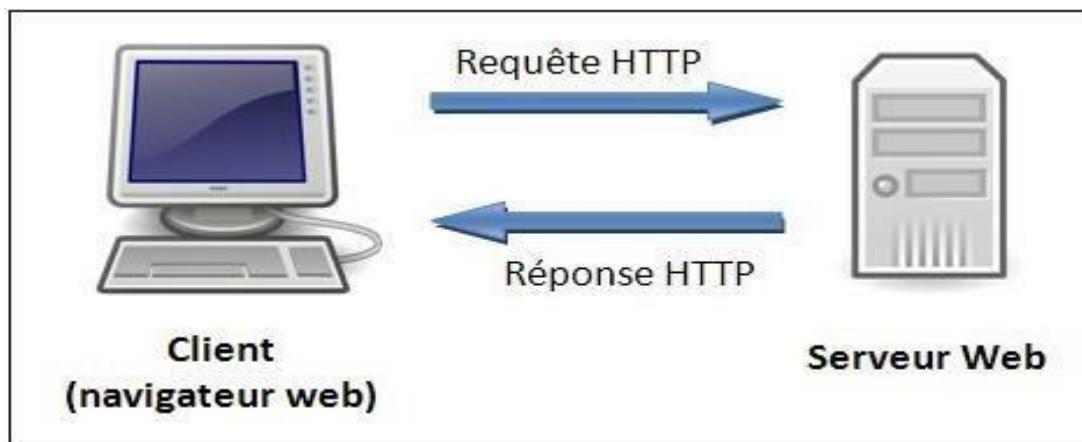
- Les données circulantes entre le client et le serveur sont chiffrés, ce qui garantit leur confidentialité. Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.
- Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur.

SSH est un protocole, c'est-à-dire une méthode standard permettant à des machines d'établir une communication sécurisée. A ce titre, il existe de nombreuses implémentations de clients et de serveurs SSH. Certains sont payants, d'autres sont gratuits ou open source. Son fonctionnement est décrit comme suit :

- Dans un premier temps le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé (couche de transport sécurisée).
- Dans un second temps le client s'authentifie au près du serveur pour obtenir une session.

### **3. Protocole HTTP**

Le protocole HTTP est un protocole de transfert, il définit la communication entre un client et un serveur sur le (WWW). Ce protocole fonctionne sur le principe « requête-réponse ». En prenant un exemple commun, de communication entre un navigateur web et un serveur web, la communication se déroule de la manière décrite sur le schéma suivant :



**Figure 17: Schéma d'une requête http**

#### **4. Protocole HTTPS**

HTTPS est un procédé de sécurisation des transactions http reposant sur une amélioration du protocole http mise au point en 1994 par l'EIT. Il permet de fournir une sécurisation des échanges lors de la transaction de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de toute autre information personnelle.

## **II. GENERALITE SUR LA DOUBLE AUTHENTIFICATION**

### **A. Définition et principe de la Double Authentification (2FA)**

La double authentification (2FA) renforce la sécurité des accès à vos comptes en ajoutant un facteur supplémentaire d'authentification. Contrairement à une méthode d'authentification unique qui se limite à un nom d'utilisateur et à un mot de passe, la 2FA exige que l'utilisateur fournit au moins deux éléments de vérification pour prouver son identité avant d'accéder à des ressources sensibles, telles qu'une application, une messagerie ou un compte en ligne.

En d'autres termes, la double authentification ne se contente pas de vérifier un seul facteur ; elle demande un ou plusieurs éléments additionnels pour garantir que l'utilisateur est bien celui

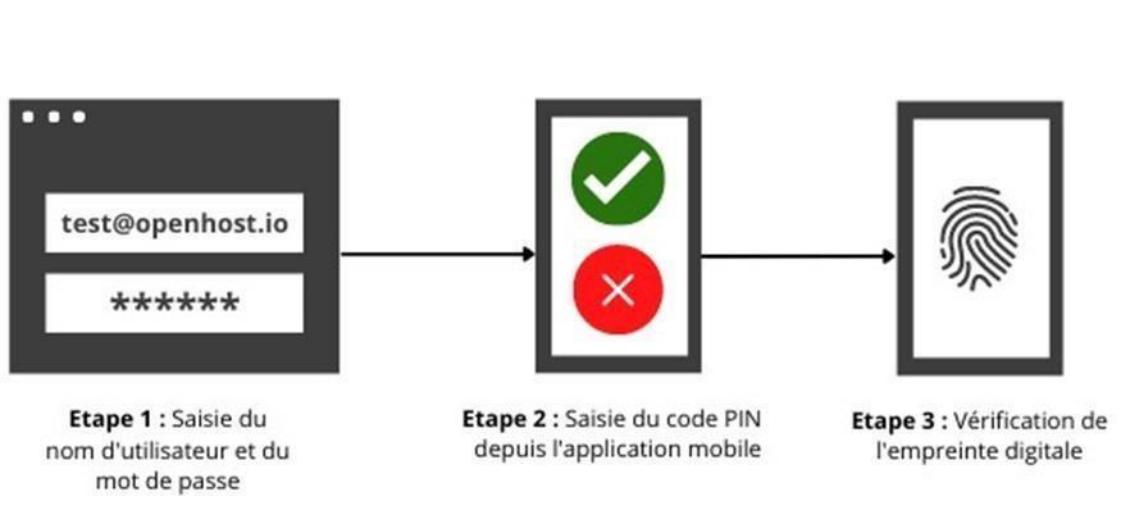
qu'il prétend être. Cela réduit considérablement les risques de succès des cyberattaques, telles que le phishing ou le vol d'identifiants.

L'intégration de la double authentification est devenue essentielle pour établir une politique stricte de gestion des identités et des accès (IAM). C'est pourquoi on observe une augmentation significative du nombre d'entreprises qui offrent des solutions de double authentification dans leurs services.

### B. Fonctionnement de la Double Authentification

La double authentification met en œuvre un facteur d'authentification supplémentaire lié à votre compte. Par exemple, à « ce que vous savez » (comme un mot de passe) peut s'ajouter « ce que vous possédez », tel qu'un code reçu par SMS, un jeton USB, ou une application générant des codes. Le processus de double authentification s'active généralement dans les paramètres de sécurité de votre compte. Une fois activée, votre identité est vérifiée deux fois avant que vous ne puissiez accéder au compte :

- Lorsque vous saisissez votre identifiant et votre mot de passe.
- En utilisant un code d'authentification qui vous est envoyé par SMS, par e-mail, ou généré via une application d'authentification. Ce code est confidentiel et n'est valable que pour une courte durée, généralement quelques minutes.



**Figure 18: Fonctionnement de la 2FA (source : google image)**

## C. Les Facteurs d'authentifications

Le processus de double Authentification nécessite la combinaison de plusieurs informations provenant d'au moins l'une des catégories suivantes : un facteur de connaissance, un facteur de possession et un facteur d'héritage.



**Figure 19: Facteur de la 2FA (source : google image)**

**Un facteur de connaissance** (ce que l'on connaît) comme un mot de passe, une expression, un code PIN... La connaissance est le facteur d'identification le plus couramment utilisé dans les méthodes d'authentification et comprend des combinaisons de nom d'utilisateur et de mot de passe. Les questions de sécurité qui nécessitent également « quelque chose que l'utilisateur sait » sont également regroupées avec ce facteur. Il convient de noter qu'une combinaison nom d'utilisateur / mot de passe compte comme un seul facteur. Il en va de même pour une série donnée de questions de sécurité. La combinaison d'un nom d'utilisateur et d'un mot de passe avec une question de sécurité est toujours considérée comme une authentification à facteur unique, car ils appartiennent tous les deux à cette catégorie.

**Un facteur de possession** (ce que l'on possède) comme un smartphone, un ordinateur, un badge... Traditionnellement, des objets tels que des cartes d'accès ou des jetons matériels étaient détenus par les utilisateurs. Les mots de passe uniques envoyés par SMS ou par e-mail aux téléphones mobiles des utilisateurs ont été de plus en plus classés dans ce facteur. L'utilisation d'appareils mobiles permet de lutter contre le risque de perdre des éléments physiques comme les cartes à puce ou les générateurs de code type RSA. Dans certains systèmes, l'appareil de l'utilisateur lui-même agit comme un facteur dans cette catégorie, ayant été déclaré comme un « appareil de confiance ».

**Un facteur d'héritage** (ce que l'on est) comme une empreinte digitale, la reconnaissance vocale ou faciale... Ce facteur d'authentification inclut toutes les données biométriques qui

pourraient servir de justificatifs d'identité. Les exemples incluent les empreintes digitales, l'ADN, la reconnaissance faciale et les analyses de la rétine. Ce type d'authentification est devenu de plus en plus populaire avec les appareils mobiles dotés de scanners d'empreintes digitales et de reconnaissance faciale intégrés.

Il existe d'autres facteurs d'authentification basés sur **le comportement ou la localisation**. Par exemple, si un utilisateur se connecte depuis un emplacement géographique autre que son bureau, il sera éventuellement invité à répondre à une question de sécurité. On parle d'authentification adaptative.

## D. LES SERVICES D'AUTHENTIFICATION

Les termes associés aux services d'authentification sont : **Identification, Authentification et Autorisation**. Le travail de ces services est avant tout l'authentification.

- **L'identification** permet de vérifier l'identité d'une personne via un login par exemple.
- **L'authentification** permet de s'assurer qu'une personne est bien celle qu'elle prétend être par login et mot de passe.
- **L'autorisation** permet à partir de l'identification et l'authentification de définir des droits à une personne.

Après la phase d'authentification des utilisateurs, le système pourra autoriser ces utilisateurs sur le service auquel ils tentent d'accéder par le contrôle de leurs droits d'accès. Le service d'autorisation est chargé d'évaluer les droits effectifs sur la base des informations fournies par le service d'authentification :

- ☒ **Authentication Windows pour EXCHANGE**
- ☒ **Authentification accès distant (Radius)**
- ☒ **Authentification Web Apache/IIS**
- ☒ **Authentification SGBD Oracle/MySQL**
- ☒ **Authentification messagerie (Webmail)**

On peut distinguer deux types d'authentification : **l'authentification d'un tiers et l'authentification de la source des données**. L'authentification d'un tiers consiste à prouver son identité. L'authentification de la source des données sert à prouver que les données reçues viennent de l'émetteur déclaré.

## D. LES METHODES D'AUTHENTIFICATION

Comme méthode d'authentification nous avons :

### 1. Le combo identifiant / mot de passe

Il s'agit d'une des méthodes les plus utilisées, avec laquelle les utilisateurs sont les plus familiers. Lorsque vous arrivez sur la page, il vous est demandé de saisir votre nom d'utilisateur et votre mot de passe.

Vos informations d'identification sont envoyées au serveur d'identification et comparées aux informations qu'il détient dans sa base. Lorsqu'une correspondance est trouvée, vous pouvez accéder à votre compte.

Les mots de passe sont souvent utilisés pour sécuriser des comptes personnels comme les profils de réseaux sociaux, les sites de banques en ligne et de commerce électronique, ainsi que d'autres ressources en ligne. Cependant, l'utilisation de mots de passe n'est pas une option aussi sûre qu'elle en a l'air. Et les dégâts peuvent être catastrophiques si un pirate parvient à accéder à l'un de ces comptes ou à la base contenant toutes les informations d'identification. De plus, les utilisateurs ont souvent des difficultés à se souvenir de plusieurs mots de passe (personnels et professionnels) et la plupart choisissent la facilité en utilisant un mot de passe unique pour tous les accès. Et pour couronner le tout, c'est souvent un mot de passe simple, que l'on peut trouver en faisant quelques recherches sur la personne (e.g. nom du lycée + année d'obtention du diplôme : Bonaparte1991 ; ou nom de sa petite fille avec l'année de sa naissance : Julie2006, etc.).

Cette méthode est la plus utilisée et de fait, la plus facile à casser.

### 2. L'authentification biométrique

L'authentification biométrique repose sur les caractéristiques biologiques uniques d'un utilisateur afin de vérifier son identité. Cela fait de la biométrie l'une des méthodes d'authentification les plus sûres à l'heure actuelle. En outre, elle entraîne moins de frictions pendant le processus d'authentification que les méthodes mentionnées précédemment, ce qui rend l'expérience de l'utilisateur plus agréable. Les identifiants les plus courants sont la numérisation des empreintes digitales, la reconnaissance faciale et l'identification par la voix. Cependant, pour pouvoir utiliser ce genre de méthodes, il faut investir dans des lecteurs d'empreintes ou dans des technologies de reconnaissance vocale / faciale. Cette méthode est l'une des plus efficaces mais elle a un coût. De plus, selon le facteur choisi, il peut y avoir plus ou moins d'erreurs provoquant tout aussi bien des faux positifs que de faux négatifs. Enfin, il reste la question de vie privée car il s'agit de stocker des informations très personnelles et sensibles sur l'utilisateur. **La sécurité qui doit être mise en place pour protéger ces informations doit être drastique.**

### **3. QR Code / Push Notifications / SMS OTP**

Ce genre de méthode d'authentification est souvent liée à une double authentification permettant d'ajouter une étape supplémentaire de sécurité, soit pour demander un accès à une ressource sensible (MFA, ou *Multi Factor Authentication* pour accéder au site de votre banque), soit pour valider une transaction (QR Code affiché sur un site web après un achat qui doit être scanné via l'application de votre banque).

Dans certains cas, il sert à authentifier directement l'utilisateur sur une application. Par exemple, Uber Eats envoyant un code d'authentification par SMS (le numéro de téléphone étant l'ID) ou alors Slack envoyant un mail avec un lien que lequel cliquer pour s'authentifier.

### **4. Interaction comportementale.**

L'authentification comportementale vérifie l'identité d'un utilisateur sur la base de schémas uniques enregistrés pendant l'interaction avec des appareils.

Exemple :

- **Sur téléphone** : un schéma enregistrant le pattern de mouvement, les angles "sélectionnés", la vitesse exécutée, etc.
- **Sur ordinateur** : Windows Hello proposait de charger une image et de sélectionner un nombre de point précis sur l'image que seul l'utilisateur connaît.  
Ces facteurs d'identification sont semblables à la méthode "combo identifiant / mot de passe" car ils se trouvent dans la catégorie "ce que je sais" mais au lieu d'utiliser des lettres et des chiffres, on utilise des "dessins".

## **E. LES MOYENS D'AUTHENTIFICATION**

### **1. Le mot de passe**

Le mot de passe est la méthode la plus utilisée lors d'un choix d'authentification Web. L'explication en est très simple, il comporte beaucoup d'avantages pour les développeurs des systèmes ainsi que les utilisateurs. Tout d'abord, son coût est très faible, tant au niveau développement qu'au niveau serveur. Ensuite, son utilisation est intuitive. L'utilisateur n'a besoin d'aucune formation pour pouvoir remplir un formulaire lui demandant ses identifiants. Troisièmement, son déploiement est simple et permet de mettre en place un système d'authentification très rapidement. De plus, il n'est aucunement lié à une technologie, un langage de programmation ou encore une plateforme. Nous pouvons noter que du côté serveur, le couple identifiant / mot de passe est souvent stocké dans un annuaire et/ou une base de

données. Ceci peut donc entraîner des coûts supplémentaires mais cela reste faible. Le mot de passe présente un inconvénient majeur : la sécurité.

Il est sujet à un ensemble de type d'attaques. Voici les plus connues : Les attaques de type brute force, Les attaques sur base d'un dictionnaire, Les attaques de types phishing, eavesdropping, malwares ou spywares.

## 2. One-time password

Les OTPs font partie des méthodes d'authentification fortes. Ils sont généralement utilisés en tant que second facteur d'authentification par le biais de devices externes comme les tokens hardwares, les smartphones, listes papiers, etc... Les sites Web tels que ceux des banques 4 sont friands de cette méthode et l'utilisent couramment. Comme le dit leur nom anglais, les OTPs sont des mots de passe temporaires. Leur durée de vie est généralement de 30 ou 60 secondes. Un flux OTP implique deux acteurs : le client avec son device et le serveur. Lors de cet échange, le but sera de prouver que le client connaît le secret sans pour autant que le faire transiter sur le réseau. Pour arriver à cela, deux phases sont nécessaires :

- La première est la génération des codes OTP's. Durant cette phase, le système va créer la séquence de codes. Elle se compose de deux étapes :

Dans la première étape, ou étape d'initialisation, l'utilisateur fournit une entrée ou secret partagé sous forme d'une pass-phrase au système. Celleci est concaténée avec un speed Le résultat de ceci est alors passé dans la fonction de hachage et ensuite réduit à une expression de X bits. Pour l'exemple, nous prendrons une chaîne de 64 bits mais le nombre de bits peut être différent (32,128,256, ...).

La deuxième est l'étape de calcul. Durant celle-ci, le système va utiliser le résultat créé en première étape comme entrée afin de calculer une séquence d'OTPs. Pour ce faire, la fonction de hachage va être appliquée un certain nombre de fois, produisant N OTPs. Le premier OTP correspondra alors à N fois l'application de la fonction. Le second OTP N-1 fois et ainsi de suite.

- La seconde phase est l'authentification proprement dite. Certaines conditions sont obligatoires pour qu'elle se réalise correctement :

Le device utilisé par le client et le serveur doivent utiliser le même algorithme de hachage, sans quoi il sera impossible pour le client et le serveur de se comprendre correctement. Pour utiliser une métaphore, nous pourrions dire qu'ils doivent parler la même langue.

Le client et le serveur doivent se mettre d'accord sur une séquence commune pour faire la vérification du code entré. Ils doivent être synchronisés. Ceci est réalisé via un challenge envoyé par le serveur à l'utilisateur. Ce dernier est constitué d'une séquence de nombre et de la seed.

Il permet au générateur de code OTP de récupérer les paramètres nécessaires pour calculer le bon code OTP à partir du secret partagé.

### **3. Biométrie**

La biométrie est un système permettant de reconnaître et d'authentifier un individu sur base de ces attributs physiques. Il existe plusieurs moyens de reconnaissance mais les plus courantes sont le visage, l'empreinte digitale, la géométrie de la main, l'iris, « keystroke », la signature et la voix. Néanmoins, les quatre principaux utilisés sont l'empreinte digitale, le scan de l'iris, la reconnaissance faciale du visage et enfin la reconnaissance vocale. La biométrie est très peu répandue lors de l'authentification Web depuis un ordinateur. Cependant, elle est tout à fait adaptée aux environnements sur smartphone et tablette. Nous distinguons deux étapes lors de l'utilisation d'un système biométrique. Afin de pouvoir authentifier un utilisateur, il faut donc s'assurer que l'attribut physique servant de référence soit lié à son compte dans le système. Cela se fait lors de l'étape d'enregistrement. Lors de celle-ci, l'utilisateur devra utiliser une première fois le système afin de créer sa correspondance et l'enregistrer dans une base de données ou encore sous un device hardware qu'il pourra présenter lors de l'authentification. Cette phase est critique puisqu'un mauvais enregistrement empêcherait toute authentification future auprès du système.

### **4. Certificat**

L'authentification par certificat est une méthode d'authentification forte dont la sécurité est basée sur la cryptographie asymétrique. Ceci implique donc la mise en place d'une PKI côté serveur.

Dans un flux d'authentification par certificat, nous distinguons deux acteurs : le client et le serveur. Pour réaliser une authentification correctement, le serveur va avoir besoin d'informations présentes dans le certificat. Voici les informations que ce dernier comporte :

- Une clé publique.
- Des informations supplémentaires concernant l'entité représentée (nom, prénom, adresse, etc....).
- La signature des autorités le certifiant de confiance.
- La clé publique est associée à une entité, humain ou machine.

Il existe trois niveaux de certificats. En fonction du niveau utilisé, le contrôle de l'identité est renforcé.

- Le premier niveau va permettre de contrôler l'adresse email du demandeur.
- Le second niveau effectuera un contrôle à distance, en vérifiant typiquement les papiers d'identité, via une photocopie reçue par exemple".
- Le dernier niveau demandera une présence physique lors de la vérification.

## 5. Authentification graphique

L'authentification graphique est une méthode d'authentification qui utilise des mots de passe graphiques afin de laisser accéder les utilisateurs aux zones privées des applications. Ce système est basé sur la reconnaissance d'images. Il implique deux acteurs : le client avec son navigateur et le serveur. Son principe est de prouver au serveur que nous connaissons le secret, sans pour autant le divulguer. Dans un flux complet, nous distinguons deux phases : **l'enregistrement et l'authentification**.

Durant la phase d'enregistrement, l'utilisateur va choisir un pattern d'images ou choisir des points dans une image. Ce choix représentera l'équivalent de la connaissance du secret.

Dans la suivante, il devra s'authentifier avec le pattern créé précédemment.

En fonction du type d'authentification, l'utilisateur devra rejouer celui-ci.

## **6. Token Hardware**

Le principe de ces tokens se base sur un device externe qui est utilisé comme premier ou second facteur d'authentification. Par exemple, le PC-Banking utilise un lecteur de carte dans lequel l'utilisateur entre un code donné par la banque et son code PIN de la carte pour ensuite recevoir un autre code à entrer sur le site. Tout ceci est basé sur des codes OTP. Certains autres systèmes vont envoyer un code OTP via d'autres canaux, comme le SMS ou l'email. Certains types de VPN utilisent des codes OTP afin de renforcer l'authentification et donc l'accès au réseau privé de l'entreprise. La société Yubico propose quant à elle, une clé USB, la Yubikey. Il existe d'autres systèmes similaires, comme RSA SecurID ou encore IronKey.

## **7. Authentification multi-facteurs**

L'authentification multi-facteurs permet de combiner plusieurs méthodes d'authentifications différentes. Généralement, elle se compose d'un mot de passe en premier facteur et d'un code OTP ou d'un certificat en second facteur. Cependant les facteurs d'authentification ne sont pas figés. Nous pourrions avoir un premier facteur qui est un certificat et un second qui est un facteur biométrique. Ce système est fortement répandu sur les sites Web nécessitant une sécurité renforcée. Nous parlons typiquement de deux facteurs d'authentification, mais il pourrait y en avoir plus. Il est possible de chainer les facteurs avec différentes méthodes.

## **8. Google Authenticator**

Google Authenticator est un système d'authentification développé par Google. L'authentification est basée sur des codes QR, c'est à dire des codes-barres à scanner avec un smartphone. Lors de l'initialisation, un code QR sera présenté afin d'être scanné. Il permettra de générer une clé partagée entre le serveur et le smartphone. Lors de l'authentification, un nouveau code QR temporaire sera présenté, il sera une combinaison entre la date de l'horloge et la clé enregistrée lors de l'initialisation. Sachant que le serveur et le smartphone sont normalement réglés à la même heure, vu qu'ils sont synchronisés via internet, ils pourront exécuter le même algorithme, permettant de vérifier que les résultats sont semblables des deux côtés.

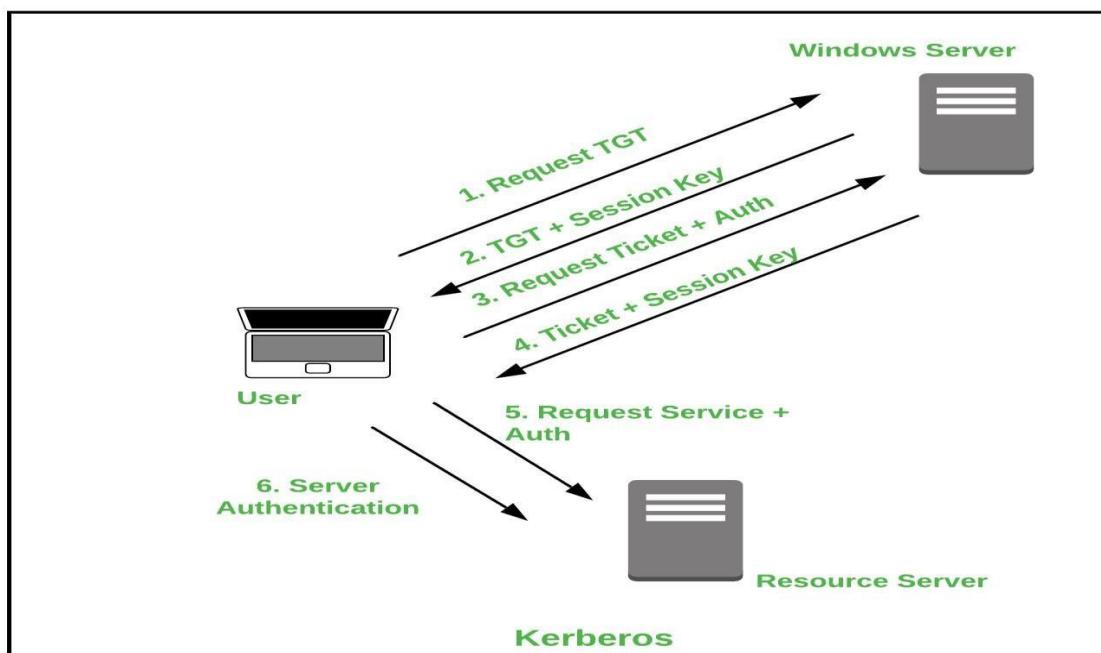
L'avantage principal d'un point de vue sécurité est que ce système permet une authentification forte, à deux facteurs. Il permet de renforcer la sécurité des comptes Gmail, Dropbox ou encore des accès SSH sur une machine Unix.

## **F. TYPES DE PROTOCOLES D'AUTHENTIFICATION**

L'authentification de l'utilisateur est la première priorité lors de la réponse à la demande faite par l'utilisateur à l'application logicielle. Plusieurs mécanismes sont nécessaires pour authentifier l'accès tout en fournissant l'accès aux données. Dans ce blog, nous explorerons les protocoles d'authentification les plus courants et tenterons d'explorer leurs avantages et leurs inconvénients.

### **1. Kerberos :**

Kerberos est un protocole qui facilite l'authentification du réseau. Ceci est utilisé pour valider les clients/serveurs sur un réseau utilisant une clé cryptographique. Il est conçu pour exécuter une authentification forte tout en rendant compte aux applications. L'implémentation globale du protocole Kerberos est ouvertement disponible par le MIT et est utilisée dans de nombreux produits fabriqués en série.



**Figure 20: Protocole Kerberos**

### Quelques avantages de Kerberos :

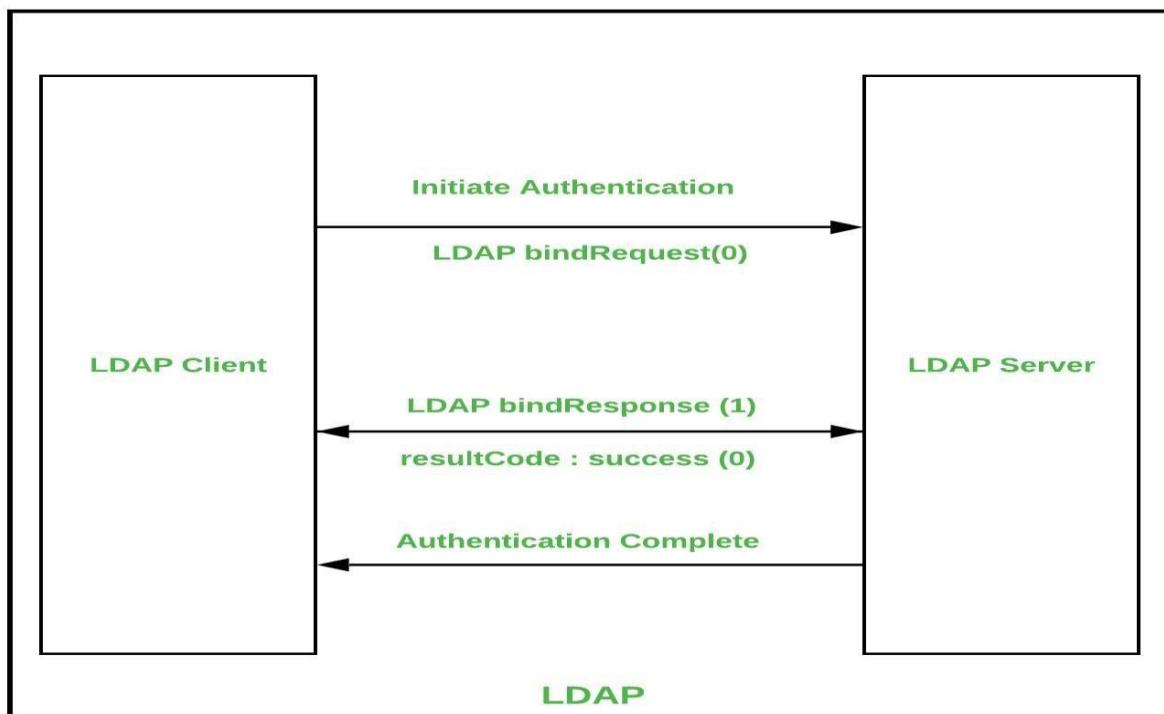
- Il prend en charge divers systèmes d'exploitation.
- La clé d'authentification est partagée de manière beaucoup plus efficace que le partage public.

### Quelques inconvénients de Kerberos :

- Il est utilisé uniquement pour authentifier les clients et les services qu'ils utilisent.
- Il montre la vulnérabilité aux mots de passe logiciels ou faibles.

## 2. Protocole d'accès à l'annuaire léger (LDAP)

LDAP fait référence au protocole léger d'accès à l'annuaire. Il s'agit d'un protocole utilisé pour déterminer les individus, les organisations et les autres appareils d'un réseau, qu'ils soient sur Internet public ou d'entreprise. Il est pratiqué en tant que répertoires en tant que service et constitue le fondement de Microsoft pour créer un répertoire d'activités.



**Figure 21: Protocole LDAP**

### Quelques avantages de LDAP :

- C'est un protocole automatisé qui facilite la modernisation.
- Il prend en charge les technologies existantes et autorise plusieurs répertoires.

### Quelques inconvénients de LDAP :

- Il nécessite l'expérience du déploiement.
- Les serveurs d'annuaire doivent être conformes à LDAP pour le déploiement.

### 3. OAuth2 :

OAuth, comme son nom l'indique, est un cadre d'autorisation qui favorise l'octroi d'un accès limité à l'utilisateur sur son compte via un service HTTP. Lorsqu'un utilisateur demande l'accès aux ressources, un appel d'API est effectué et une fois le jeton d'authentification transmis.

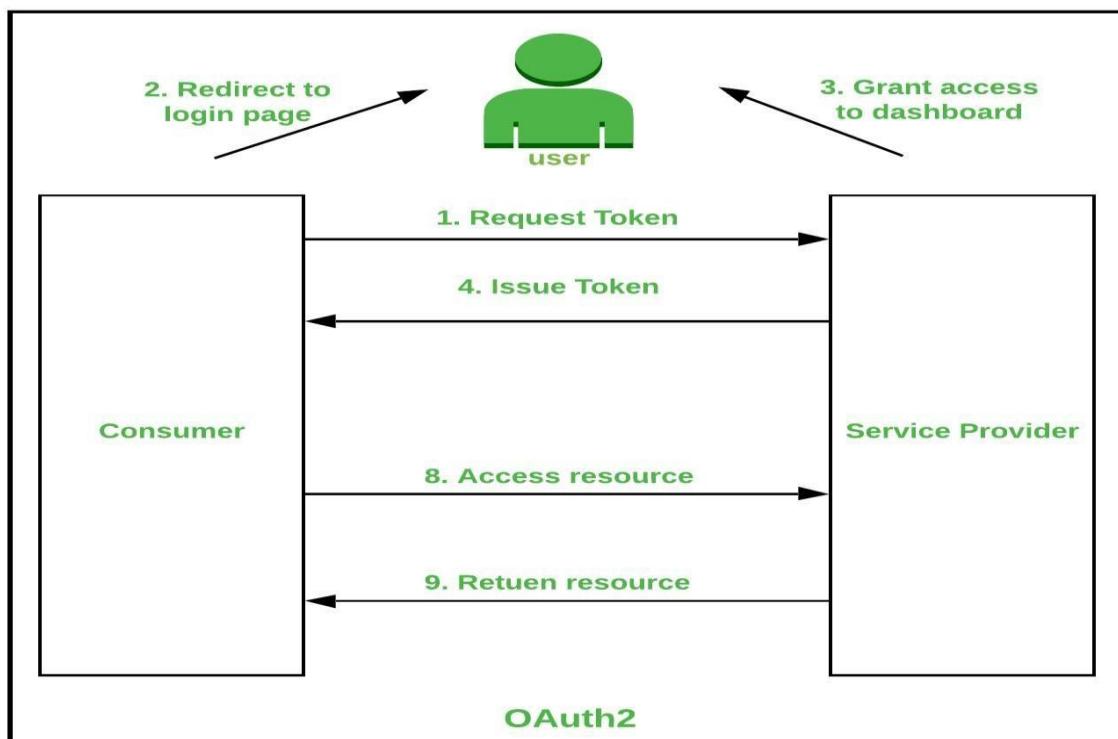


Figure 22: Protocole OAuth2

### Quelques avantages d'OAuth2 :

- C'est un protocole simple et facile à mettre en œuvre.

- Il fournit une autorisation de code côté serveur.

#### Quelques inconvénients d'OAuth2 :

- Il est vulnérable pour gérer différents ensembles de code.
- Il montre des effets graves sur les sites connectés à un autre système affecté.

#### 4. SAML

SAML signifie Security Assertion Markup Language qui est basé sur le format de données d'authentification basé sur XML qui fournit l'autorisation entre un fournisseur d'identité et un fournisseur de services. Il sert de produit du comité technique des services de sécurité OASIS.

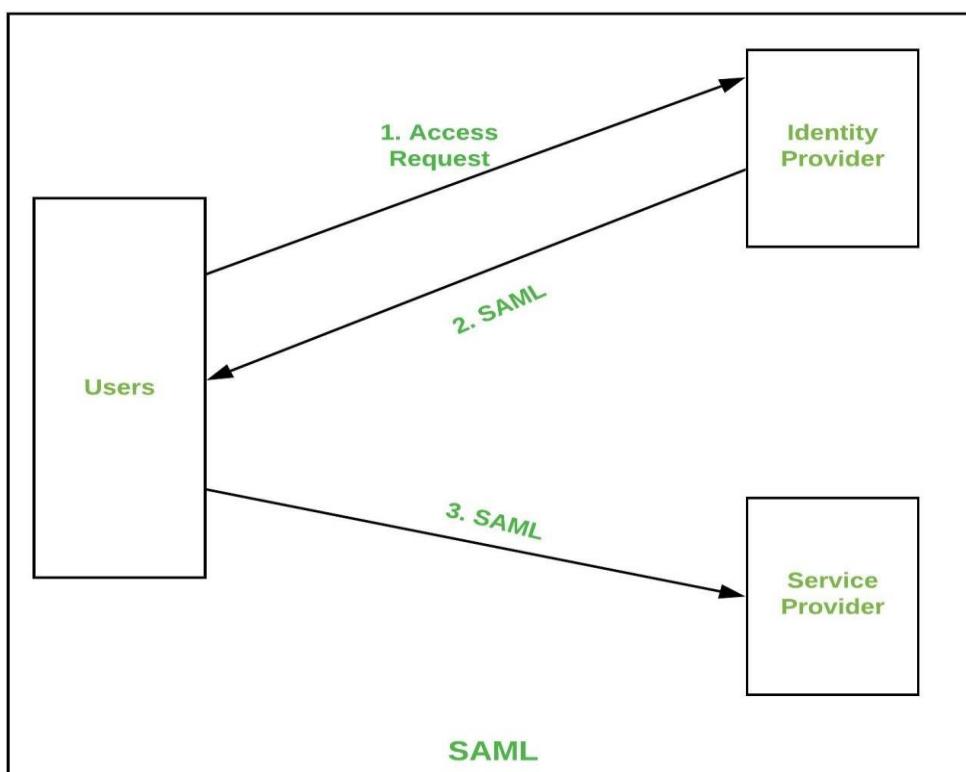


Figure 23: Protocole SAML

#### Quelques avantages de SAML :

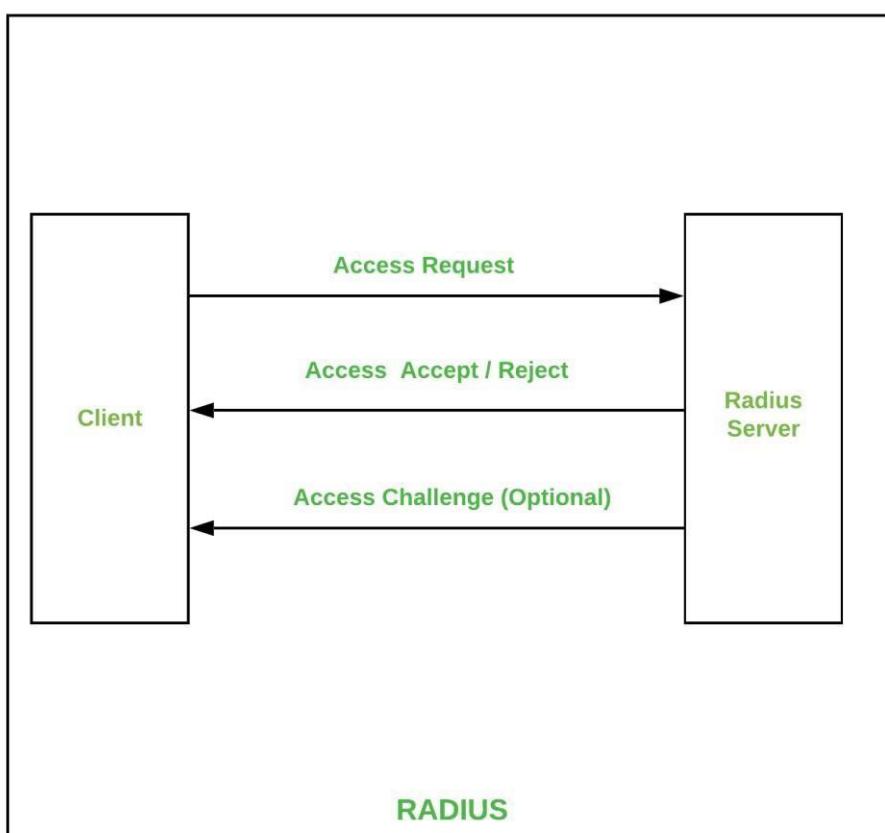
- Cela a réduit les coûts administratifs pour les utilisateurs finaux.
- Il fournit une connexion unique pour l'authentification entre les fournisseurs de services.

### Quelques inconvénients de SAML :

- Il dépend du fournisseur d'identité.
- Toutes les données sont gérées dans un seul format XML.

## 5. RADIUS

RADIUS signifie Remote Authentication Dial-In User Service. Il s'agit d'un protocole réseau qui fournit une authentification, une comptabilité et une autorisation centralisées suffisantes pour les utilisateurs qui utilisent des services réseau. Le fonctionnement du protocole se produit lorsque l'utilisateur demande l'accès aux ressources du réseau, où le serveur RADIUS crypte les informations d'identification saisies par l'utilisateur. Après cela, les informations d'identification de l'utilisateur sont mappées via la base de données locale et fournissent un accès.



**Figure 24: Protocole RADIUS**

### Quelques avantages de RADIUS :

- C'est un excellent mécanisme pour fournir un accès multiple aux administrateurs.
- Il fournit une identité unique à chaque utilisateur d'une session.

### Quelques inconvénients de RADIUS :

- La mise en œuvre initiale de ce mécanisme est difficile sur le matériel.
- Il a une variété de modèles qui peuvent nécessiter une équipe spéciale, ce qui coûte cher. Différencier les protocoles ne rendra pas justice aux protocoles car cela dépend de l'utilisation de l'application et de l'usage auquel elle est destinée.

## III. PROTOCOLE RADIUS

### Introduction

RADIUS (Remote Authentication Dial-In User Service) est un protocole de sécurité largement utilisé pour l'authentification, l'autorisation et la comptabilité (AAA) dans les réseaux informatiques. Développé dans les années 1990, RADIUS est devenu une norme dans l'industrie pour gérer l'accès aux réseaux, particulièrement pour les entreprises, les fournisseurs de services Internet (FSI) et les environnements à distance. Son architecture et ses mécanismes de fonctionnement en font un outil très efficace pour sécuriser les connexions utilisateurs.

### A. Fonctionnalités Principales

#### 1. Authentification

L'authentification est le processus par lequel RADIUS vérifie l'identité d'un utilisateur ou d'un dispositif avant de lui accorder l'accès à un réseau. Lorsqu'un utilisateur tente de se connecter, il fournit un nom d'utilisateur et un mot de passe au client RADIUS (par exemple, un point d'accès ou un routeur). Ce dernier envoie une requête d'authentification au serveur RADIUS.

RADIUS prend en charge plusieurs méthodes d'authentification, y compris :

- Envoie les informations d'identification en clair, ce qui n'est pas recommandé pour les environnements non sécurisés.

Utilise un défi de hachage pour sécuriser les informations d'identification.

- Un cadre qui permet l'utilisation de plusieurs méthodes d'authentification, y compris la biométrie, les certificats numériques, et plus encore.

## **2. Autorisation**

Après l'authentification, RADIUS détermine les droits d'accès de l'utilisateur.

Le serveur RADIUS renvoie des attributs qui définissent ce que l'utilisateur peut faire, tels que les ressources auxquelles il peut accéder et les limitations sur l'utilisation. Grâce à des attributs spécifiques, les administrateurs peuvent contrôler l'accès à des services, des applications et des fonctionnalités réseau.

## **3. Comptabilité**

La comptabilité permet de suivre et d'enregistrer l'utilisation des ressources réseau par les utilisateurs. RADIUS enregistre des informations sur les connexions, y compris l'heure de début et de fin de la session, la durée, et les ressources utilisées. Ces données peuvent être utilisées pour des audits de sécurité, des analyses de performance, et pour répondre à des exigences réglementaires.

# **B. Architecture du Protocole**

## **1. Composants de RADIUS**

RADIUS repose sur une architecture client-serveur, composée de plusieurs éléments clés :

- L'appareil qui nécessite l'authentification (ex. : routeur, point d'accès sans fil, serveur VPN).
- L'entité qui gère les demandes d'authentification et d'autorisation. Il peut être déployé sur un serveur dédié ou intégré à d'autres systèmes de gestion.
- Contient les informations d'identification des utilisateurs. Cela peut être une base de données locale ou une source externe telle que LDAP ou Active Directory.

## **2. Flux de Communication**

Le flux de communication RADIUS est structuré et repose sur des étapes spécifiques :

- L'utilisateur saisit ses informations d'identification sur le client RADIUS.
- Le client envoie une requête d'authentification au serveur RADIUS.
- Le serveur RADIUS vérifie les informations d'identification dans sa base de données.

- Le serveur renvoie une réponse d'acceptation ou de rejet, accompagnée des attributs d'autorisation si l'authentification est réussie.

### C. Avantages de RADIUS

- RADIUS permet une gestion centralisée des utilisateurs, simplifiant l'administration et la mise en œuvre des politiques de sécurité.
- Utilise des mécanismes de cryptage pour protéger les informations d'identification pendant la transmission.
- Les mots de passe ne sont pas envoyés en clair, réduisant ainsi le risque d'interception.
- RADIUS est conçu pour gérer de grandes quantités d'utilisateurs, ce qui le rend idéal pour les environnements d'entreprise ou les FSI.
- RADIUS peut être intégré avec d'autres systèmes de gestion d'identité, tels que les systèmes de gestion des accès (IAM) et d'autres services d'annuaire.

### D. Applications du Protocole RADIUS

- Utilisé dans les entreprises pour gérer l'accès aux réseaux locaux (LAN) et aux réseaux privés virtuels (VPN), permettant une sécurité accrue pour les connexions distantes.
- RADIUS est couramment utilisé pour authentifier les abonnés et gérer les sessions de connexion, en particulier dans les services d'accès à distance.
- Permet l'authentification des utilisateurs qui se connectent à distance via des connexions dial-up, sans fil ou à travers des réseaux publics.

### E. Sécurité et Meilleures Pratiques

- Il est conseillé d'utiliser des méthodes d'authentification sécurisées comme EAP-TLS, qui repose sur des certificats numériques.
- Les administrateurs doivent s'assurer que les mots de passe sont complexes et régulièrement mis à jour.
- Mettre en place des mécanismes de surveillance pour détecter les tentatives d'accès non autorisées et effectuer des audits réguliers des logs de RADIUS.

## Conclusion

Le protocole RADIUS est un élément essentiel de la sécurité des réseaux modernes. En offrant des fonctionnalités d'authentification, d'autorisation et de comptabilité robustes, il permet aux organisations de mieux contrôler l'accès à leurs ressources tout en maintenant un

haut niveau de sécurité. Grâce à sa flexibilité, son évolutivité et sa capacité à s'intégrer à d'autres systèmes, RADIUS reste un choix privilégié pour les entreprises cherchant à renforcer leur architecture de sécurité numérique.

## IV. SURVEILLANCES ET GESTIONS DU RESEAU

### Introduction

La surveillance et la gestion du réseau sont des éléments cruciaux pour garantir la sécurité, la performance, et la disponibilité des infrastructures informatiques. Avec l'augmentation des menaces cybernétiques, la complexité croissante des environnements réseau, et le besoin d'une disponibilité constante des services, les organisations doivent adopter des solutions avancées pour surveiller, analyser et gérer leurs réseaux de manière proactive.

#### A. Objectifs de la Surveillance du Réseau

Les principaux objectifs de la surveillance du réseau incluent :

##### 1. Détection des Anomalies

La détection des anomalies est essentielle pour identifier les comportements atypiques qui pourraient signaler une cyberattaque ou un incident de sécurité. Cela inclut des connexions non autorisées, des transferts de données suspects, ou des variations inattendues dans le trafic réseau.

##### 2. Suivi des Performances

Le suivi des performances du réseau permet de garantir que les ressources fonctionnent de manière optimale. Cela comprend la surveillance de la latence, de la bande passante, et des temps de réponse des applications, afin d'identifier les goulets d'étranglement et d'optimiser l'expérience utilisateur.

##### 3. Conformité Réglementaire

La conformité avec les normes de sécurité et les réglementations en vigueur (comme le RGPD) est primordiale. La surveillance du réseau aide les organisations à s'assurer qu'elles respectent ces exigences, notamment en matière de protection des données et de gestion des accès.

##### 4. Gestion des Ressources

L'optimisation de l'utilisation des ressources réseau est essentielle pour garantir une performance maximale. Cela inclut la gestion de la capacité, le contrôle des coûts, et l'allocation efficace des ressources.

## **B. Outils de Surveillance du Réseau**

Plusieurs outils et solutions sont disponibles pour la surveillance du réseau, chacun offrant des fonctionnalités spécifiques :

### **1. Systèmes de Gestion de Réseau (NMS)**

Ces systèmes permettent de surveiller et de gérer les performances des équipements réseau.

Fonctionnalités :

- Cartographie Réseau : Visualisation de l'architecture du réseau, facilitant l'identification des points critiques.
- Surveillance de l'État des Dispositifs : Suivi en temps réel de la santé des équipements, tels que les routeurs, switchs, et serveurs.
- Alertes en Cas de Défaillance : Notifications automatiques envoyées aux adminis

### **2. Outils de Surveillance de la Sécurité (SIEM)**

Les systèmes SIEM collectent et analysent les données de sécurité provenant de diverses sources.

Fonctionnalités :

- Les systèmes SIEM collectent et analysent les données de sécurité provenant de diverses sources.
- Surveillance des événements de sécurité et des journaux pour détecter des comportements suspects.
- Utilisation d'algorithmes d'apprentissage automatique pour identifier les menaces potentielles.
- Génération de rapports pour soutenir les audits de sécurité et les vérifications réglementaires.

### **3. Outils de Surveillance de la Performance du Réseau (NPM)**

Ces outils se concentrent sur l'analyse des performances du réseau et des applications.

Fonctionnalités :

- Analyse des temps de réponse et des capacités de transmission pour anticiper les problèmes de performance.
- Évaluation de la performance des applications critiques pour l'entreprise.

- Surveillance des applications qui consomment excessivement la bande passante ou d'autres ressources.

## C. PRTG Network Monitor

### 1. Présentation de PRTG

PRTG Network Monitor est un outil de surveillance réseau développé par Paessler AG. Conçu pour surveiller l'ensemble des infrastructures informatiques, PRTG offre une solution complète et intégrée pour la gestion des performances et des ressources. PRTG est utilisé par des entreprises de toutes tailles pour surveiller les réseaux locaux (LAN), les réseaux étendus (WAN), et les services cloud. Il est particulièrement apprécié pour sa flexibilité et sa facilité d'utilisation.

### 2. Fonctionnalités Clés

- PRTG permet de surveiller l'état et la performance des dispositifs réseau, des serveurs, des applications, et des services en temps réel.
- Il offre des systèmes d'alerte configurables qui informent les administrateurs en cas de problèmes de performance ou de défaillances, permettant une réponse rapide.
- Les utilisateurs peuvent créer des tableaux de bord personnalisés pour visualiser les données pertinentes et les indicateurs de performance clés (KPI).
- PRTG prend en charge plusieurs protocoles de surveillance, y compris SNMP, WMI, HTTP, et bien d'autres, permettant une flexibilité dans la surveillance des différents équipements.
- L'outil génère des rapports détaillés sur les performances du réseau, facilitant l'analyse des tendances et la prise de décisions éclairées.

### 3. Avantages de PRTG

- PRTG dispose d'une interface conviviale qui facilite la configuration et l'utilisation de l'outil, même pour les utilisateurs non techniques.
- PRTG peut s'adapter aux environnements de toutes tailles, depuis de petites entreprises jusqu'à de grandes entreprises avec des infrastructures complexes.
- Permet une gestion centralisée de l'ensemble des composants réseau, simplifiant l'administration et augmentant l'efficacité.

- Paessler offre une version d'essai gratuite qui permet aux utilisateurs d'évaluer les fonctionnalités avant de s'engager.

#### **4. Cas d'Utilisation de PRTG**

- Suivi de l'état et de la performance des routeurs, switchs et autres appareils.
- Vérification de la disponibilité et de la performance des serveurs d'applications et des bases de données.
- Analyse des performances des applications critiques pour l'entreprise, garantissant une expérience utilisateur optimale.
- Suivi des performances et de la disponibilité des services cloud utilisés par l'entreprise.

### **D. Méthodes de Gestion du Réseau**

#### **1. Gestion des Configurations**

Maintenir une documentation précise des configurations réseau et des politiques de sécurité est essentiel pour la gestion efficace du réseau.

- Utiliser des outils pour documenter et suivre les changements dans les configurations des équipements.
- Utilisation d'outils d'automatisation pour standardiser et simplifier le processus de mise à jour des configurations.

#### **2. Gestion des Incidents**

La gestion des incidents implique un processus structuré pour répondre aux incidents de sécurité ou de défaillance du réseau.

- Déterminer la nature et la gravité de l'incident pour prioriser la réponse.
- Mobiliser les équipes nécessaires pour résoudre l'incident rapidement.
- Après la résolution, effectuer une analyse pour comprendre les causes et éviter la récurrence.

#### **3. Gestion des Changements**

La gestion des changements assure que tous les changements apportés au réseau sont planifiés, testés et documentés.

- Établir un processus formel pour valider les changements importants avant leur mise en œuvre.
- Informer toutes les parties concernées avant d'apporter des modifications au réseau.

## E. Surveillance en Temps Réel

La surveillance en temps réel est cruciale pour détecter et réagir rapidement aux problèmes:

- Configuration d'alertes pour prévenir les administrateurs en cas d'anomalies, permettant une réponse rapide aux incidents.
- Utilisation de tableaux de bord pour visualiser en temps réel l'état du réseau et des performances, facilitant la prise de décision.
- Suivi des tendances historiques pour anticiper les problèmes futurs, permettant une planification proactive des ressources.

## F. Intégration avec la Sécurité

La surveillance et la gestion du réseau doivent être intégrées aux efforts de sécurité :

- Les équipes réseau et de sécurité doivent travailler ensemble pour identifier les menaces et les vulnérabilités.
- Élaboration de politiques de sécurité qui prennent en compte les spécificités du réseau et des services utilisés.
- Sensibilisation et formation des équipes sur les meilleures pratiques de sécurité et de gestion du réseau.

## Conclusion

La surveillance et la gestion du réseau sont des éléments essentiels pour garantir la sécurité, la performance et la disponibilité des systèmes informatiques. L'utilisation d'outils tels que PRTG facilite cette tâche en offrant des capacités de surveillance avancées, des alertes en temps réel et des analyses approfondies. En mettant en œuvre des outils de surveillance efficaces et en adoptant des pratiques de gestion robustes, les organisations peuvent mieux répondre aux défis croissants liés à la sécurité des réseaux et assurer la continuité de leurs opérations. L'avenir de la gestion réseau repose sur l'intégration de solutions intelligentes, d'analyses prédictives et d'une approche proactive de la sécurité, garantissant ainsi une infrastructure résiliente et sécurisée.

## V. NORMES ET REGLEMENTATIONS

### Introduction

Dans le cadre de la mise en place d'un système de sécurité basé sur l'authentification à double facteur (2FA) avec RADIUS, il est essentiel de se conformer à diverses normes et réglementations. Celles-ci visent à protéger les données sensibles et à garantir la sécurité des systèmes d'information. La conformité à ces normes est non seulement une obligation légale, mais elle contribue également à renforcer la confiance des utilisateurs et à minimiser les risques de cyberattaques.

#### 1. Règlement Général sur la Protection des Données (RGPD)

**Description :** Le RGPD est une réglementation européenne qui vise à renforcer la protection des données personnelles. Il impose des obligations aux entreprises concernant le traitement et la sécurité des données.

**Exigences:** Les organisations doivent mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données personnelles, notamment en intégrant des systèmes d'authentification robustes comme le 2FA.

#### 2. Norme ISO/IEC 27001

**Description:** Cette norme internationale définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un système de management de la sécurité de l'information (SMSI).

**Importance:** Adopter cette norme permet aux organisations de gérer efficacement leurs informations sensibles, d'assurer la continuité des activités et de se conformer aux exigences légales.

#### 3. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

**Rôle :** L'ANSSI émet des recommandations et des bonnes pratiques en matière de sécurité des systèmes d'information en France.

**Impact:** Les entreprises doivent suivre les directives de l'ANSSI pour garantir que leurs systèmes sont sécurisés contre les menaces émergentes.

#### **4. Commission Nationale de l'Informatique et des Libertés (CNIL)**

**Fonction:** La CNIL est l'autorité française chargée de veiller au respect des lois sur la protection des données personnelles.

**Sanctions:** Elle peut imposer des amendes aux entreprises qui ne respectent pas les réglementations, soulignant l'importance d'une conformité rigoureuse.

#### **5. Norme ISO/IEC 27701**

**Extension:** Cette norme complète les normes ISO 27001 et ISO 27002 en intégrant la gestion de la vie privée.

**Objectif:** Aider les organisations à établir un système de management pour protéger les données personnelles, ce qui est crucial lors de l'implémentation du 2FA.

#### **6. Bonnes Pratiques en Matière de Sécurité**

**Sécurisation du Réseau:** Limiter les accès non nécessaires et utiliser des protocoles sécurisés comme WPA3 pour le Wi-Fi.

**Utilisation de VPN:** Imposer un accès VPN pour les connexions distantes avec une authentification robuste.

**Cloisonnement du Réseau:** Séparer le réseau interne du réseau accessible depuis Internet pour réduire l'impact potentiel d'une compromission.

#### **7. Conformité Sectorielle**

Certaines industries peuvent avoir leurs propres réglementations spécifiques, comme HIPAA pour le secteur de la santé ou PCI DSS pour le secteur financier. Il est crucial que les organisations soient conscientes des exigences spécifiques à leur domaine d'activité.

### **Conclusion**

La conformité aux normes et réglementations est essentielle pour garantir la sécurité des systèmes d'information lors de l'implémentation d'un système d'authentification à double facteur avec RADIUS. En suivant ces directives, les organisations peuvent non seulement

protéger leurs données sensibles, mais aussi renforcer leur posture de sécurité face aux cyber menaces croissantes.

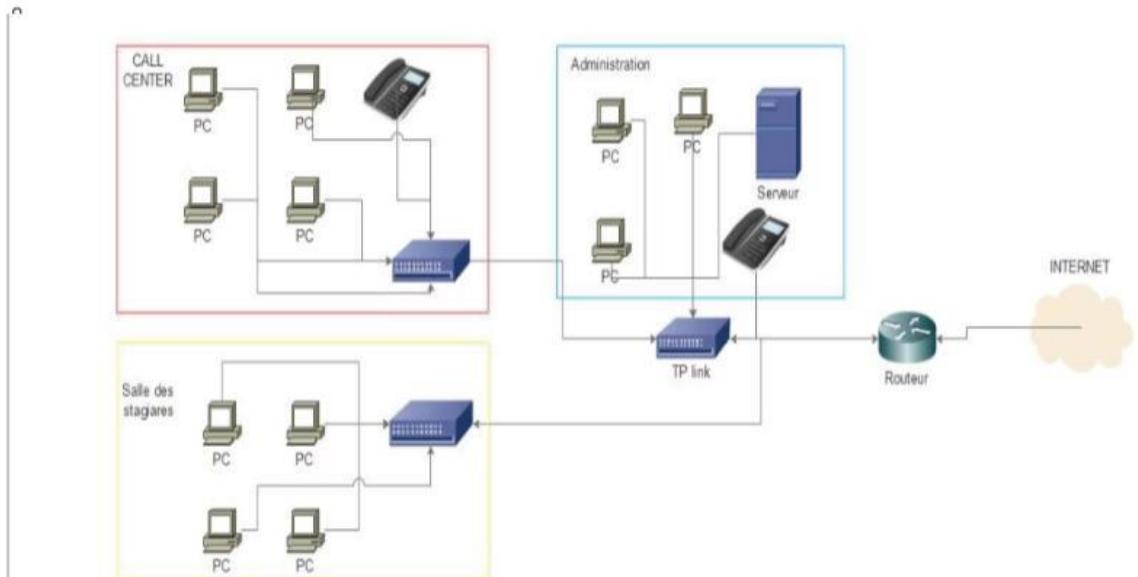
**CHAPITRE 4 :**  
**IMPLEMENTATION DE LA SOLUTION**

## I. Choix de la solution niveau authentification

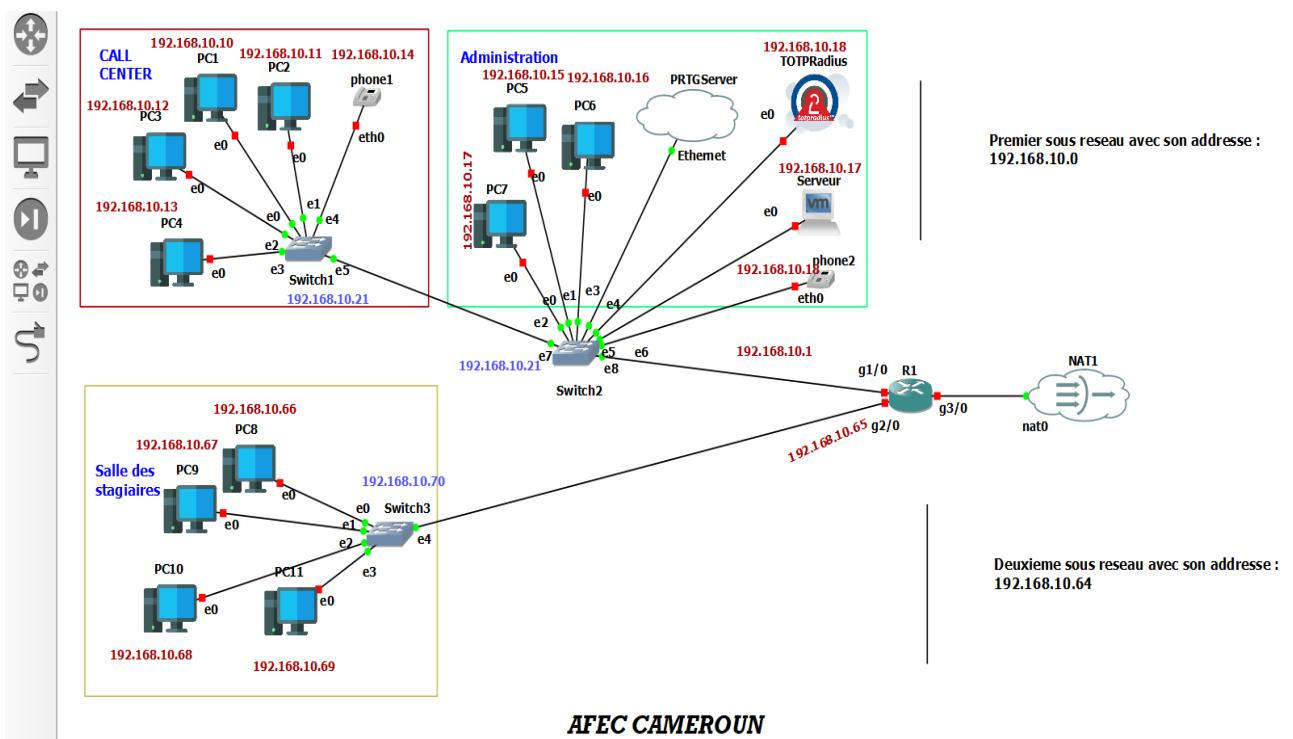
Pour implémenter notre double authentification sur un routeur, nous avons utilisé un **Token2 TOTPRadius** basée sur un logiciel qui s'exécute sur deux hyperviseurs : VMWare ESXi et Microsoft Hyper-V. **Token2 TOTPRadius** fournit le RADIUS RFC-2865 pour l'authentification basée sur TOTP RFC6238. Avec TOTPRadius, vous pouvez intégrer une grande variété de produits et de systèmes tiers avec une authentification multifacteur. Un certain nombre de produits et services d'entreprise tels que les VPN, Citrix XenApp/XenDesktop, VMWare View et bien d'autres prennent en charge les serveurs RADIUS pour valider le deuxième facteur d'authentification des utilisateurs. De plus, l'Appliance TOTPRadius fournit une API RESTful pour l'authentification et l'inscription à deux facteurs (y compris l'inscription en libre-service si possible). Cela permet de mettre en œuvre une authentification à deux facteurs entièrement sécurisée et conviviale prenant en charge les protocoles RADIUS et LDAP ainsi que l'API HTTP avec une seule Appliance. TOTPRadius prend en charge l'authentification OTP uniquement basée sur l'algorithme RFC6238 (TOTP : Time-Based One-Time Password Algorithm), l'authentification combinée mot de passe local + OTP ainsi que l'authentification combinée LDAP+OTP. Il fournit un panneau d'administration Web et un service d'API HTTPS REST conçu pour permettre l'auto-inscription des utilisateurs.

Pour implémenter notre double authentification sur notre server, nous avons utilisé **google Authenticator**.

## II. ARCHITECTURE UTILISE POUR LA DEMONSTRATION



**Figure 25: Architecture AFECameroun**



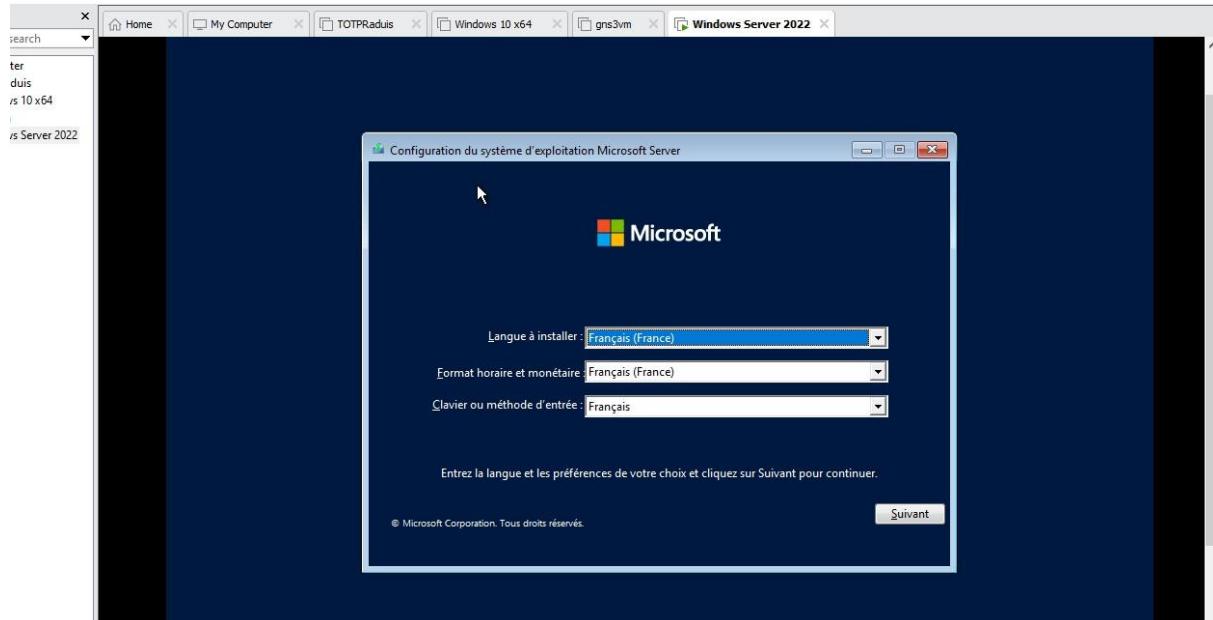
**Figure 26: Architecture utilisé pour la démonstration**

Pour la configuration de la double authentification sur le routeur nous avons besoin :

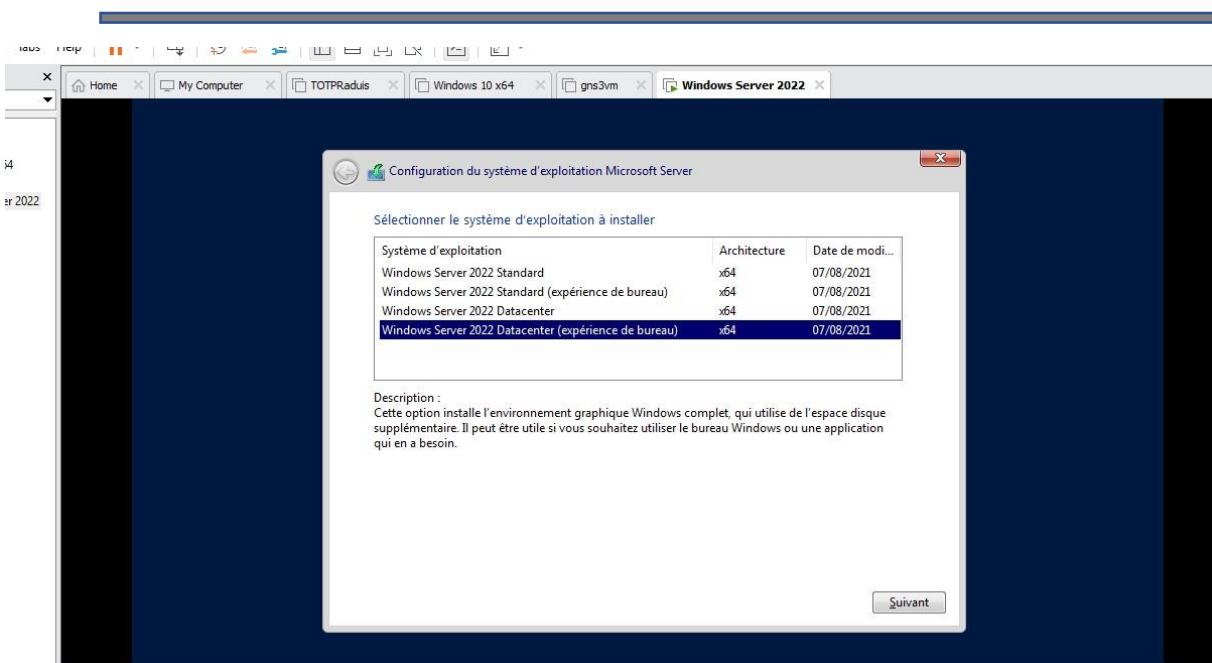
- Une machine (**windows\_serveur2022**) qui nous sert d'annuaire Ldap. Nous allons configurer notre annuaire Ldap sur Windows server2022 avec active directory déployer. C'est sur cette annuaire Ldap que nous allons configurer le premier facteur de connexion au routeur (**R1**) ;
- Une machine (**TOTPRadius**), ici est configurer le totpradius nous permettant de configurer la double authentification sur le routeur (**R1**) ;
- Les applications mobiles compatibles TOTP (google Authenticator) installer sur un téléphone;
- Un Routeur (**R1**), routeur sur quel on implémente la double authentification.

### III. CONFIGURATION DE LA DOUBLE AUTHENTIFICATION SUR LE SERVEUR WINDOWS

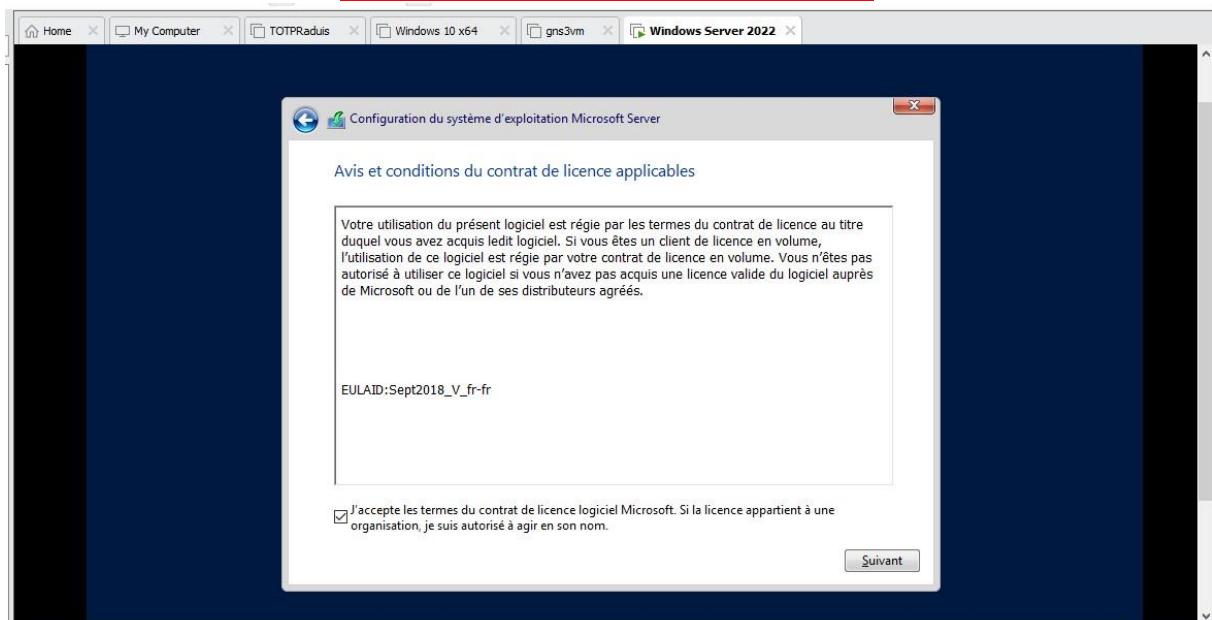
Pour configurer la double authentification sur le serveur, nous avons d'abord



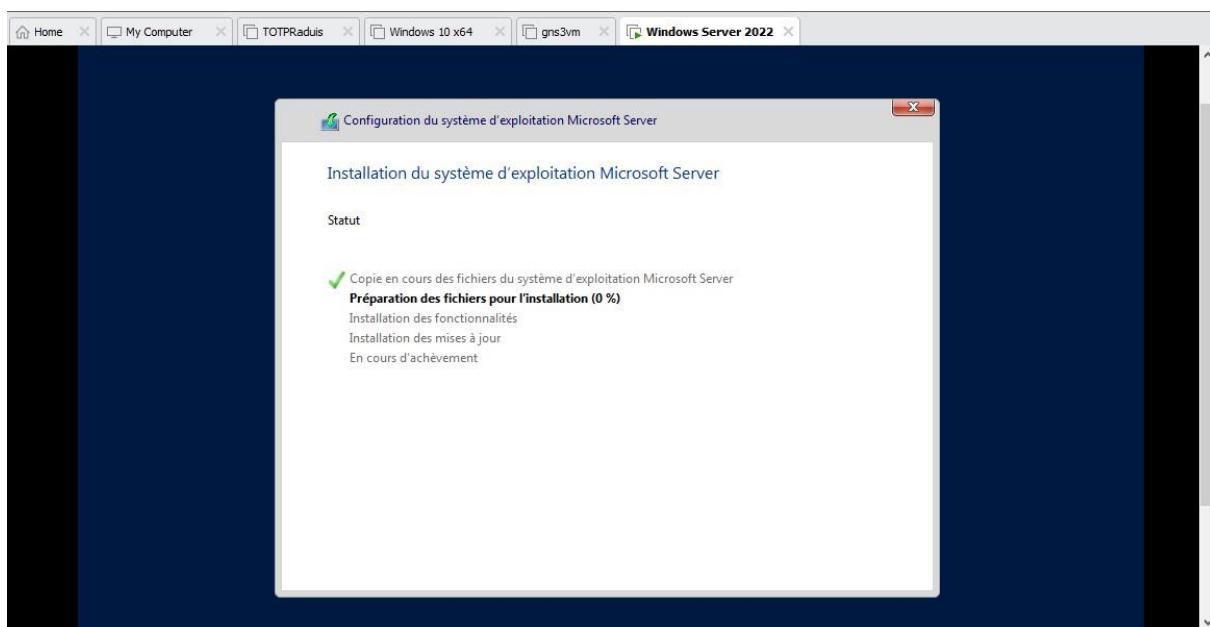
**Figure 27: Choix de la langue du système**



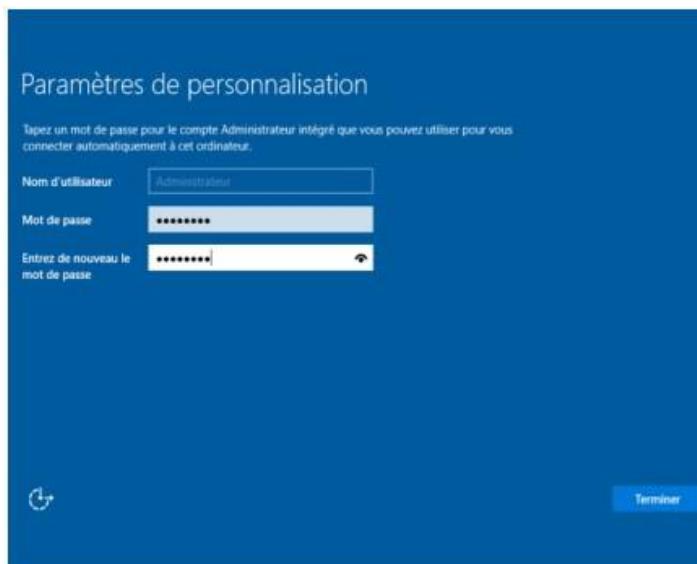
**Figure 28: Choix du système à installer**



**Figure 29: Contrat de licence**

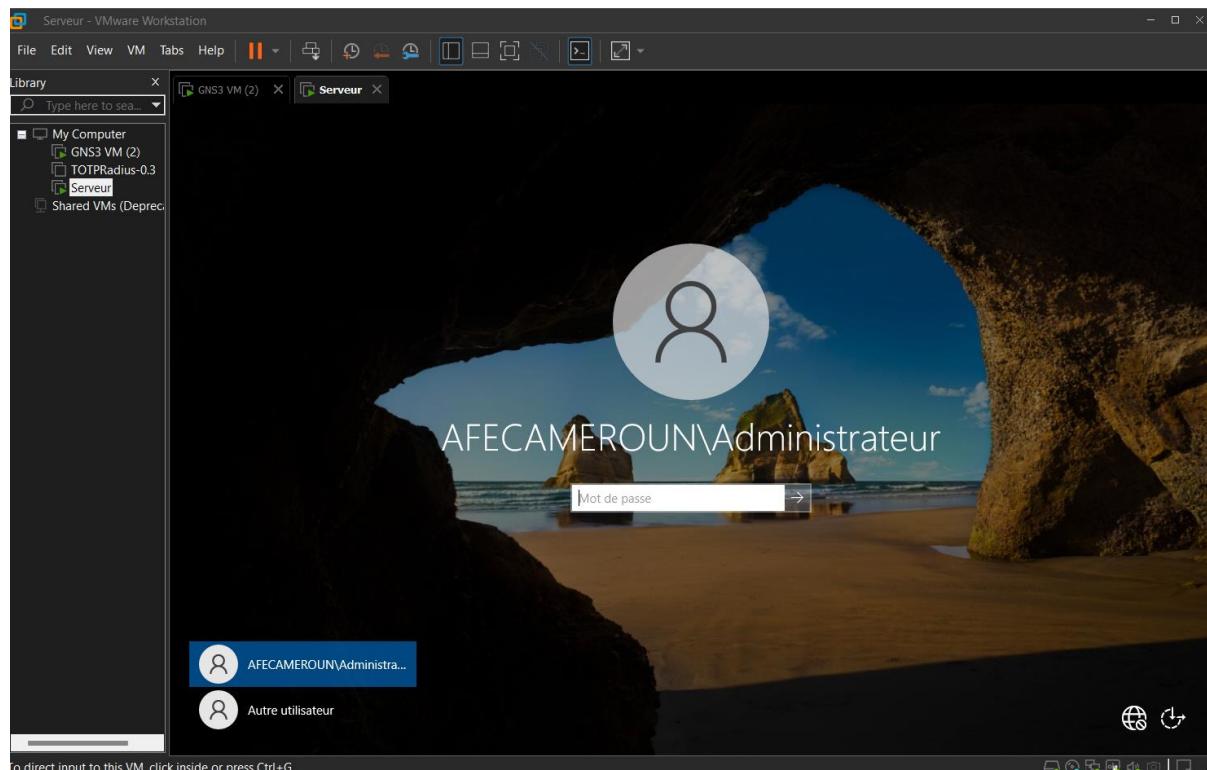


**Figure 30: Installation de windows server**

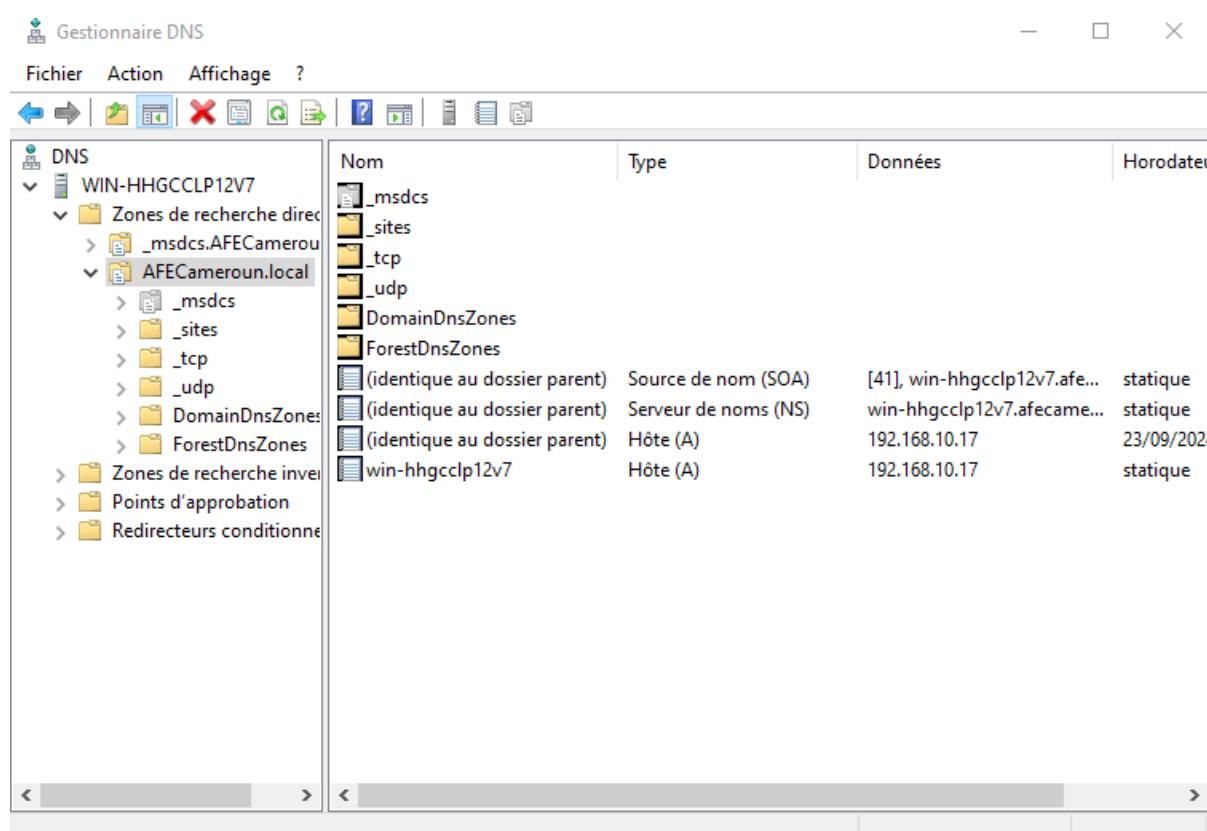


**Figure 31: Parametres de personnalisation**

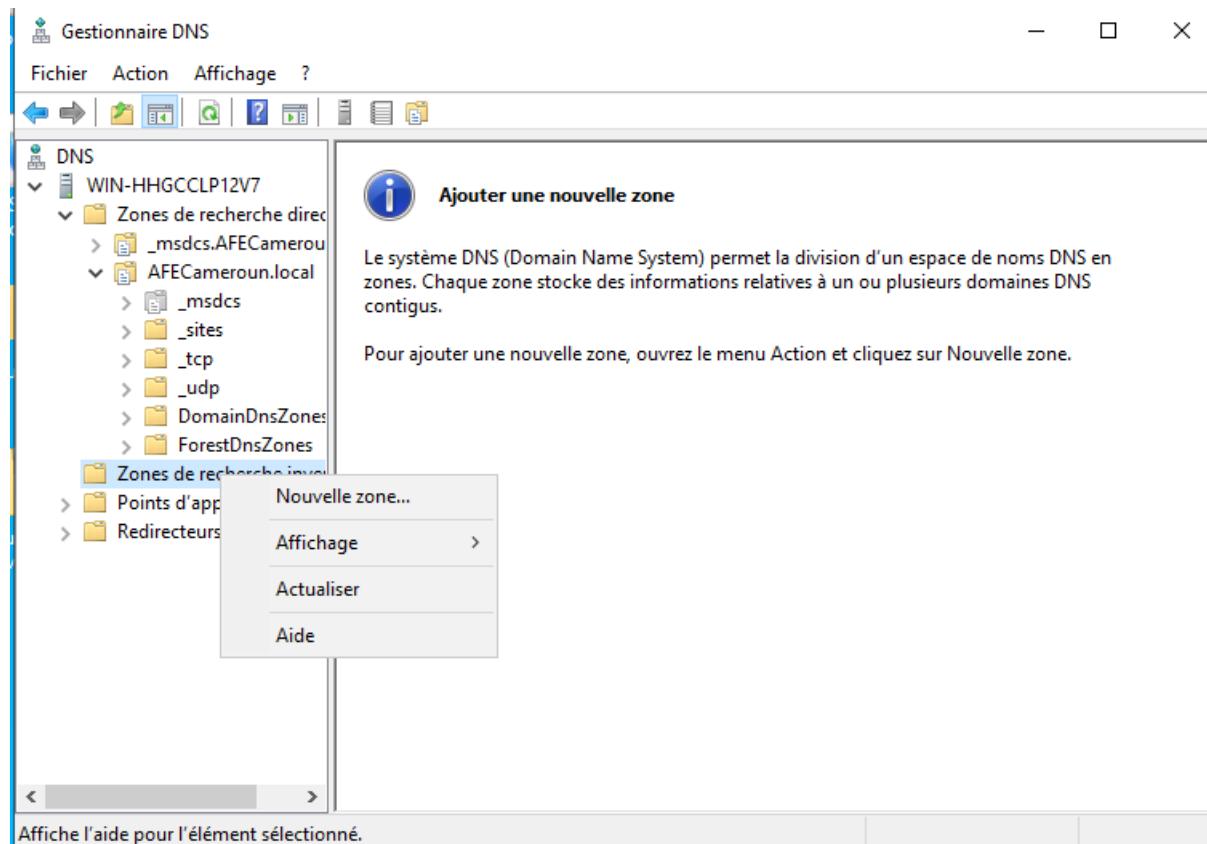
Pour procéder au déverrouillage de votre session, appuyer sur « Ctrl+Alt+Suppr »



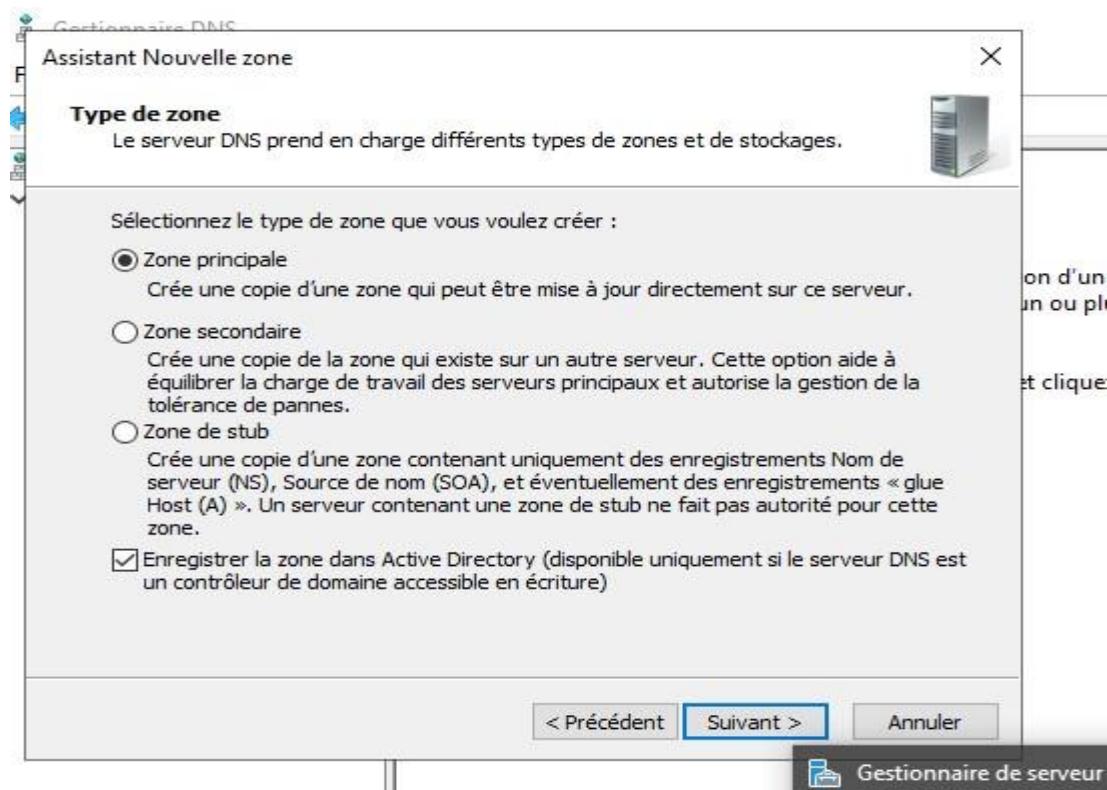
**Figure 32: Déverouillage de la session**  
**Configuration du DNS**



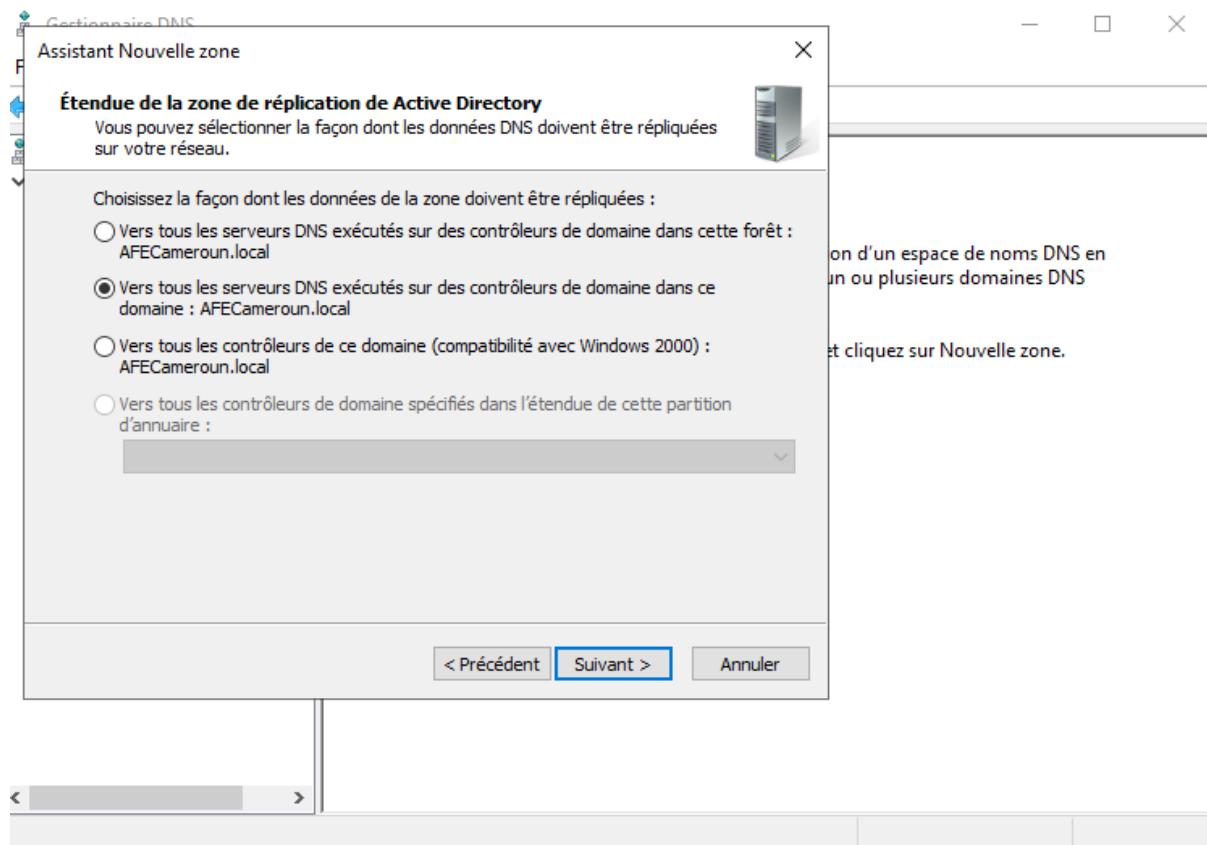
**Figure 32: Interface DNS**



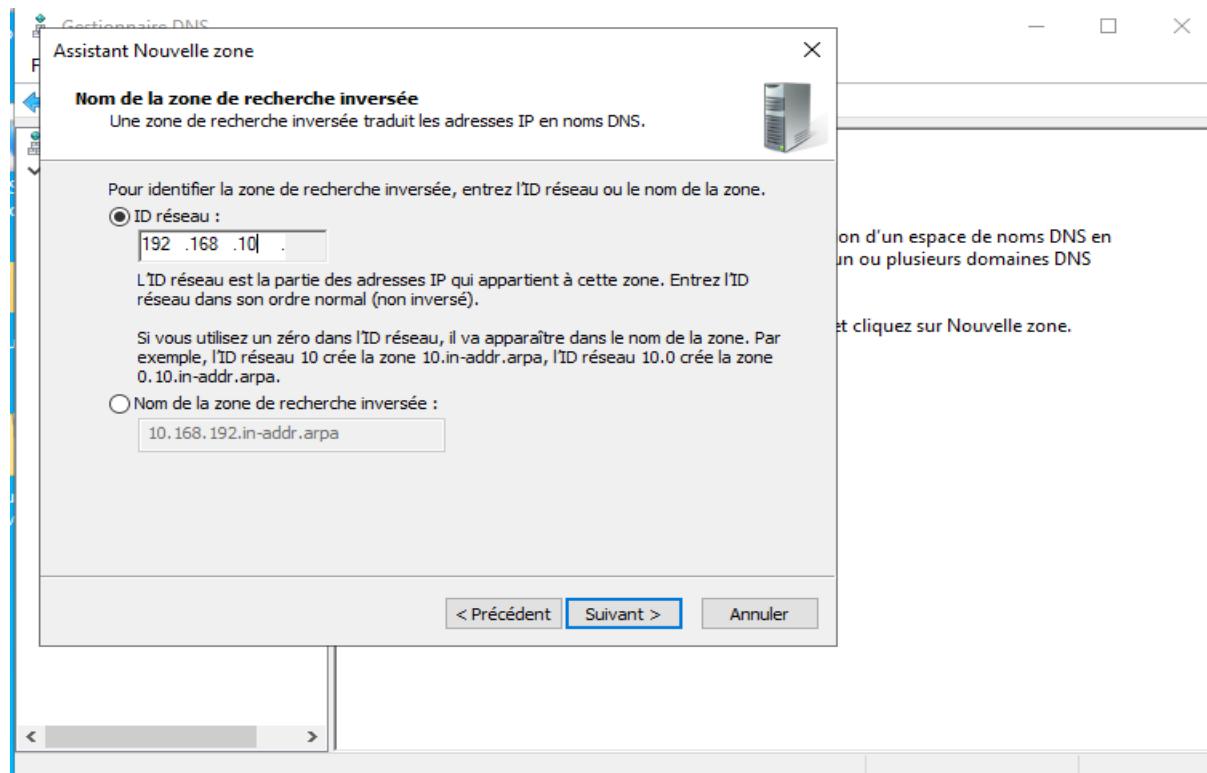
**Figure 32: Ajout d'une nouvelle zone**



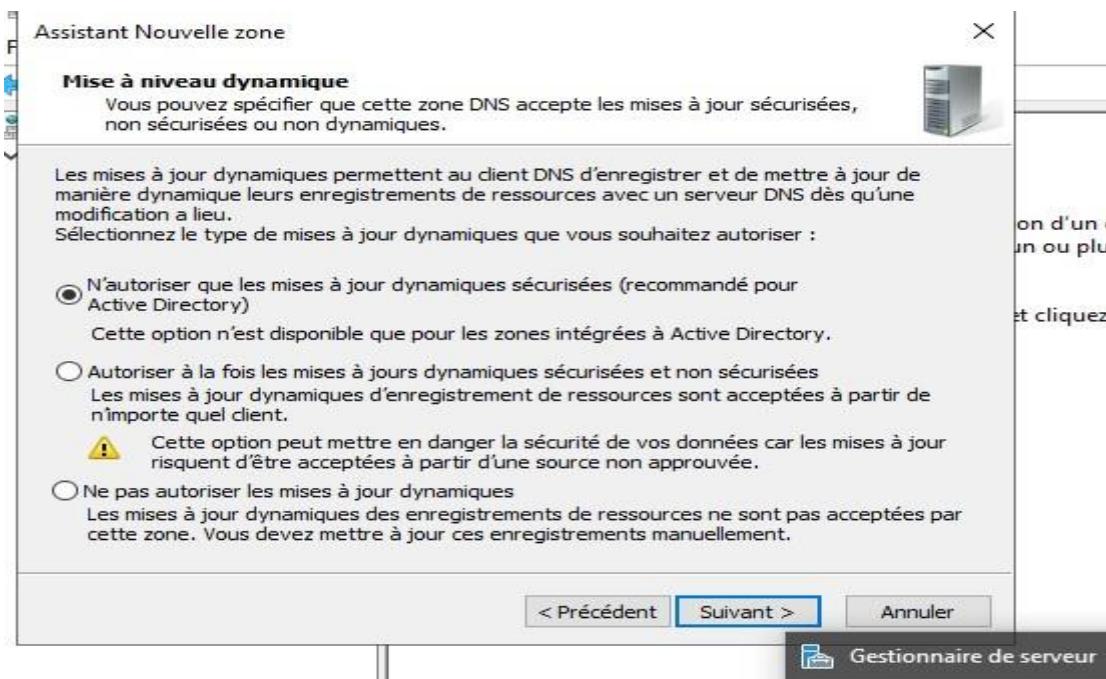
**Figure 32: Choix du type de zone**



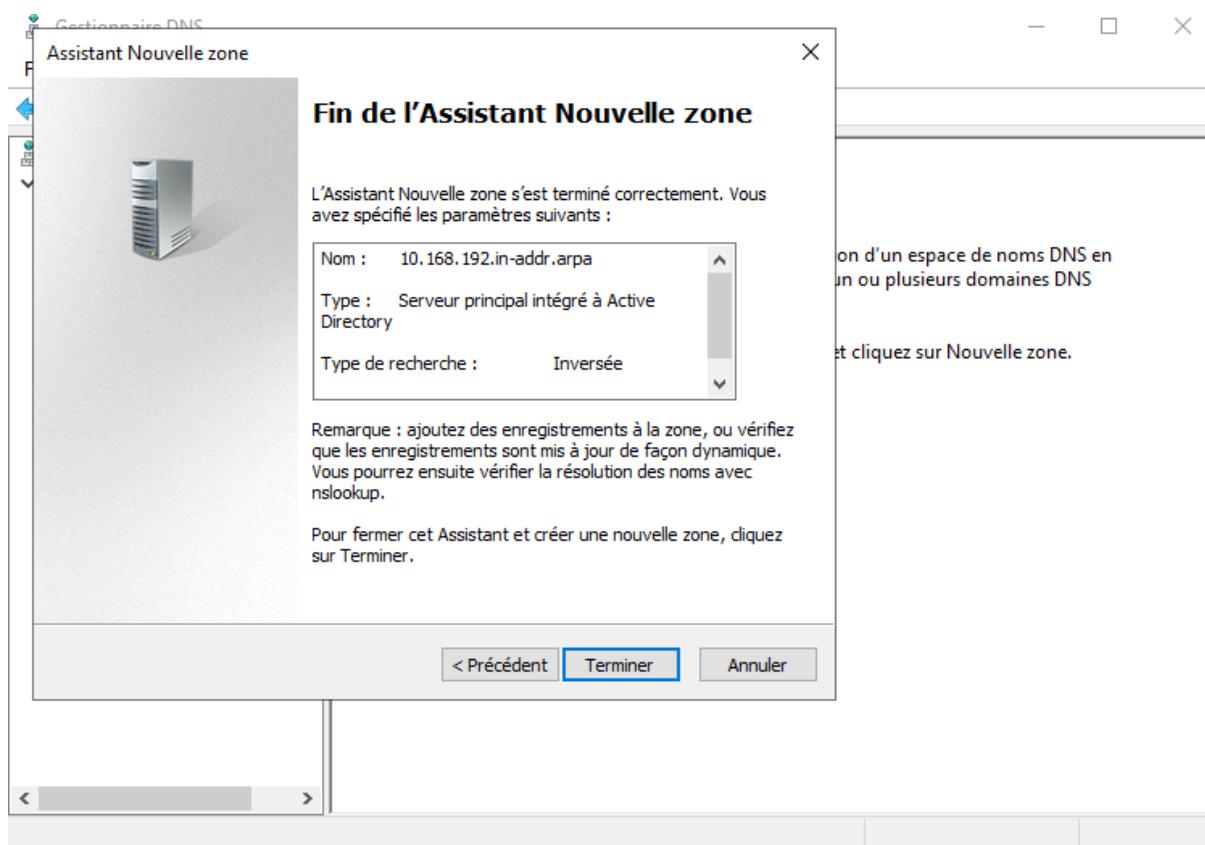
**Figure 33: Spécifier la zone**



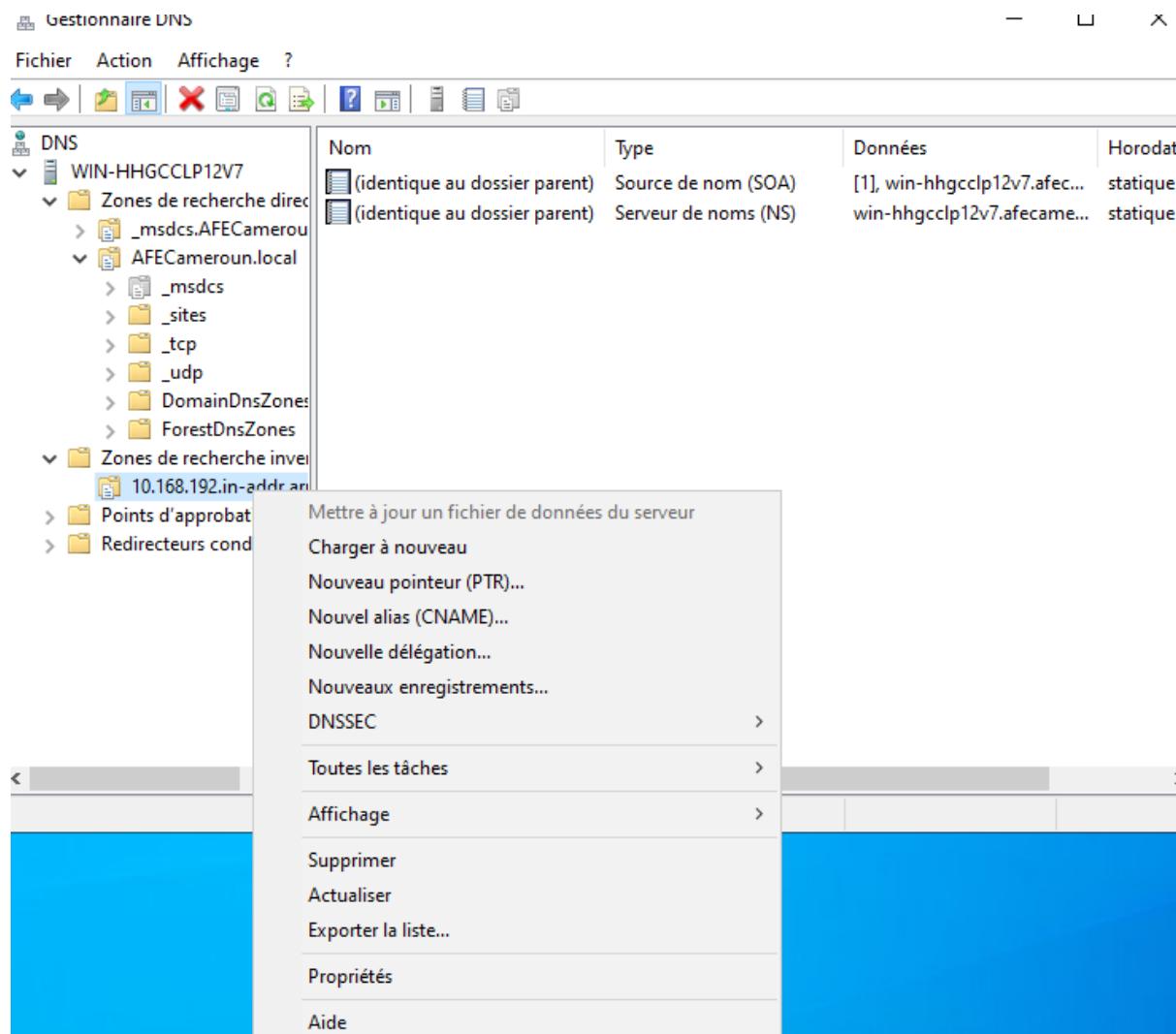
**Figure 34: ajout adresse IP externe**



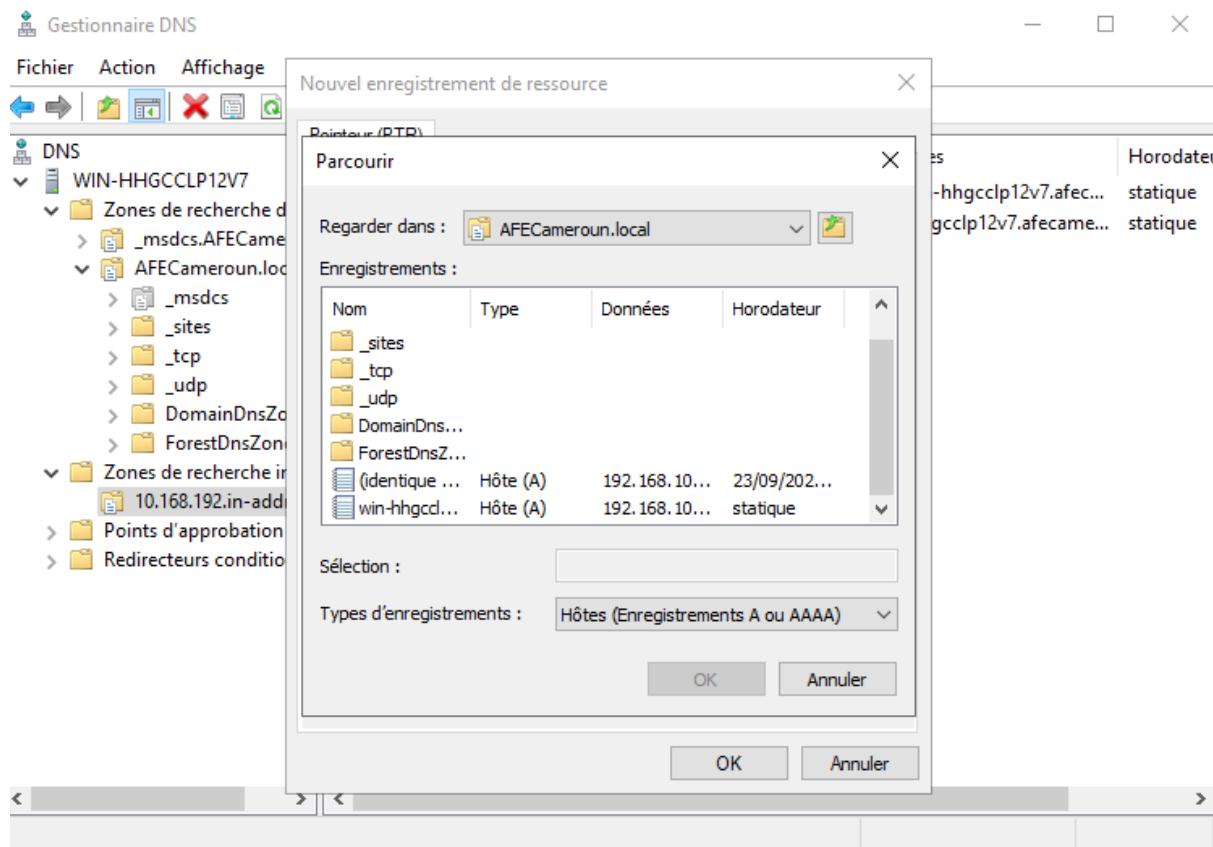
**Figure 35: Mise à Niveau**



**Figure 36: Fin de l'installation**



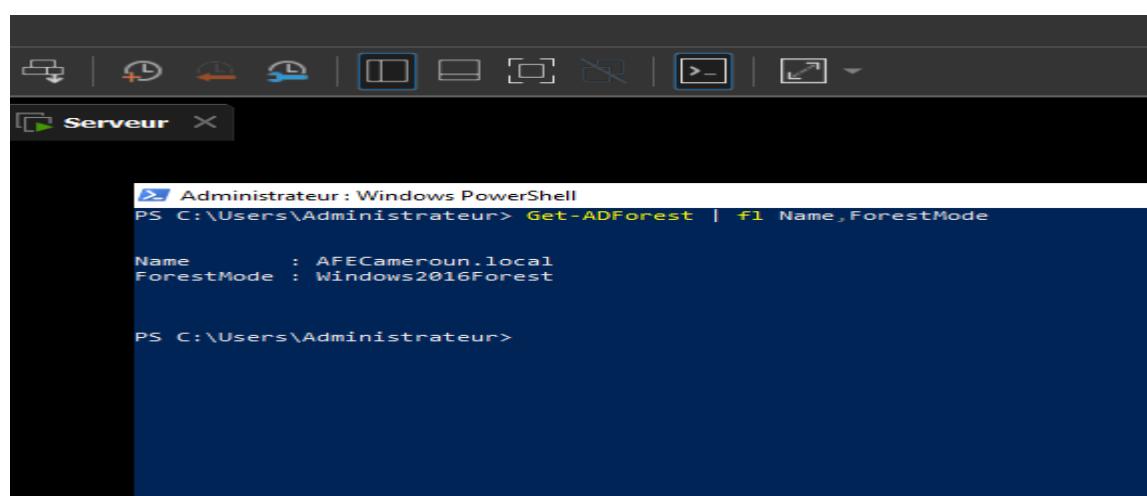
**Figure 37: Ajout d'un nouveau pointeur**



**Figure 38: Ajout du pointeur**

Pour la vérification de notre pointeur et taper :

```
# Get-ADForest | fl Name,ForestMode
```



**Figure 39: Vérification de la foret et du nom de domaine**

Ensuite installer google authenticator et l'ouvrir sur la terminale

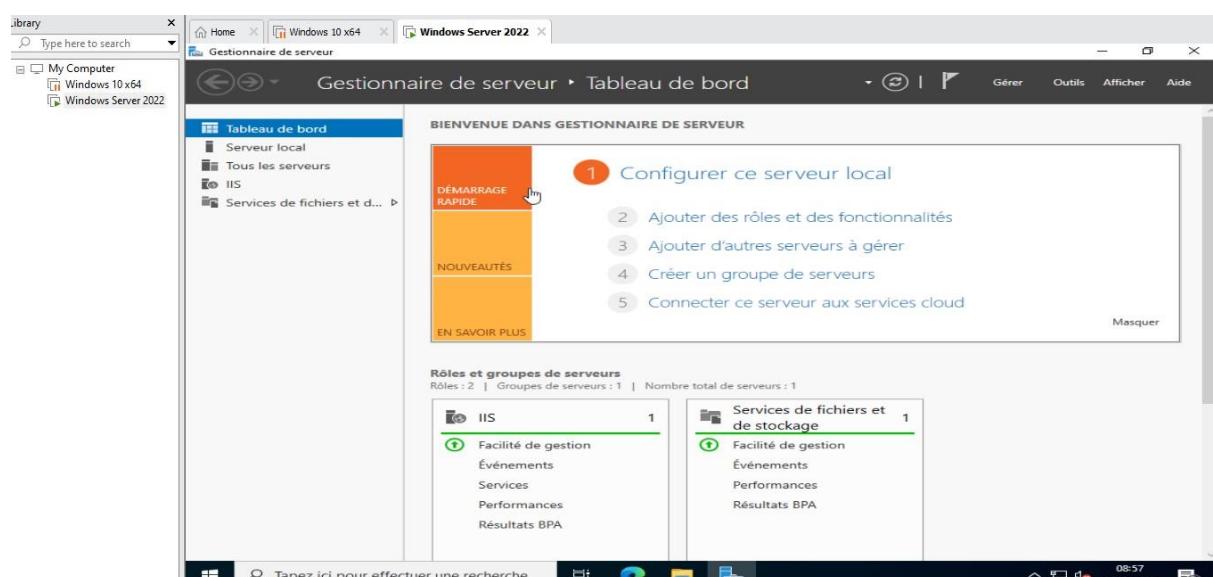
## IV. CONFIGURATION DE LA DOUBLE AUTHENTIFICATION SUR UN ROUTEUR

### 1. Installation de l'annuaire Ldap

Pour installer l'annuaire Ldap, nous installons Windows server 2022 ensuite nous configurons ADDS. Comme son nom l'indique, ADDS permet la mise en place des services de domaine Active Directory, autrement dit la mise en œuvre d'un domaine et d'un annuaire Active Directory.

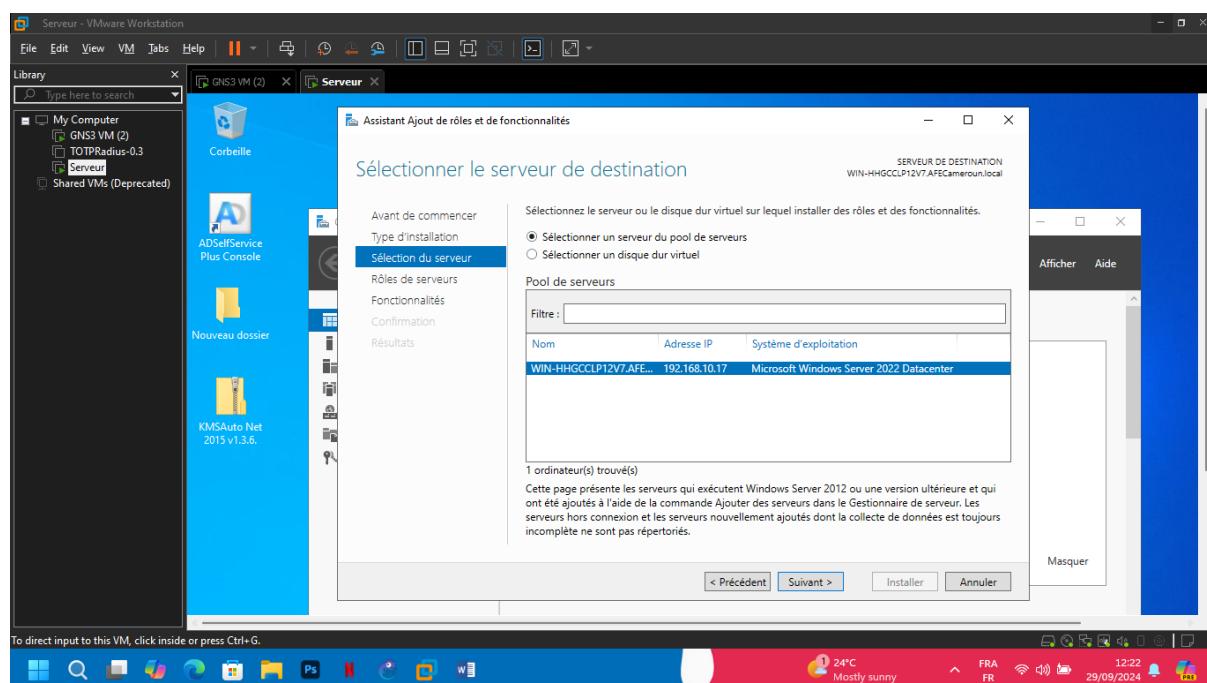
Pour configurer l'ADDS, suivre les étapes suivantes :

- Sur le tableau de bord, Gestionnaire des serveurs, Configurer ce serveur local, cliquer sur ajouter rôles et fonctionnalités



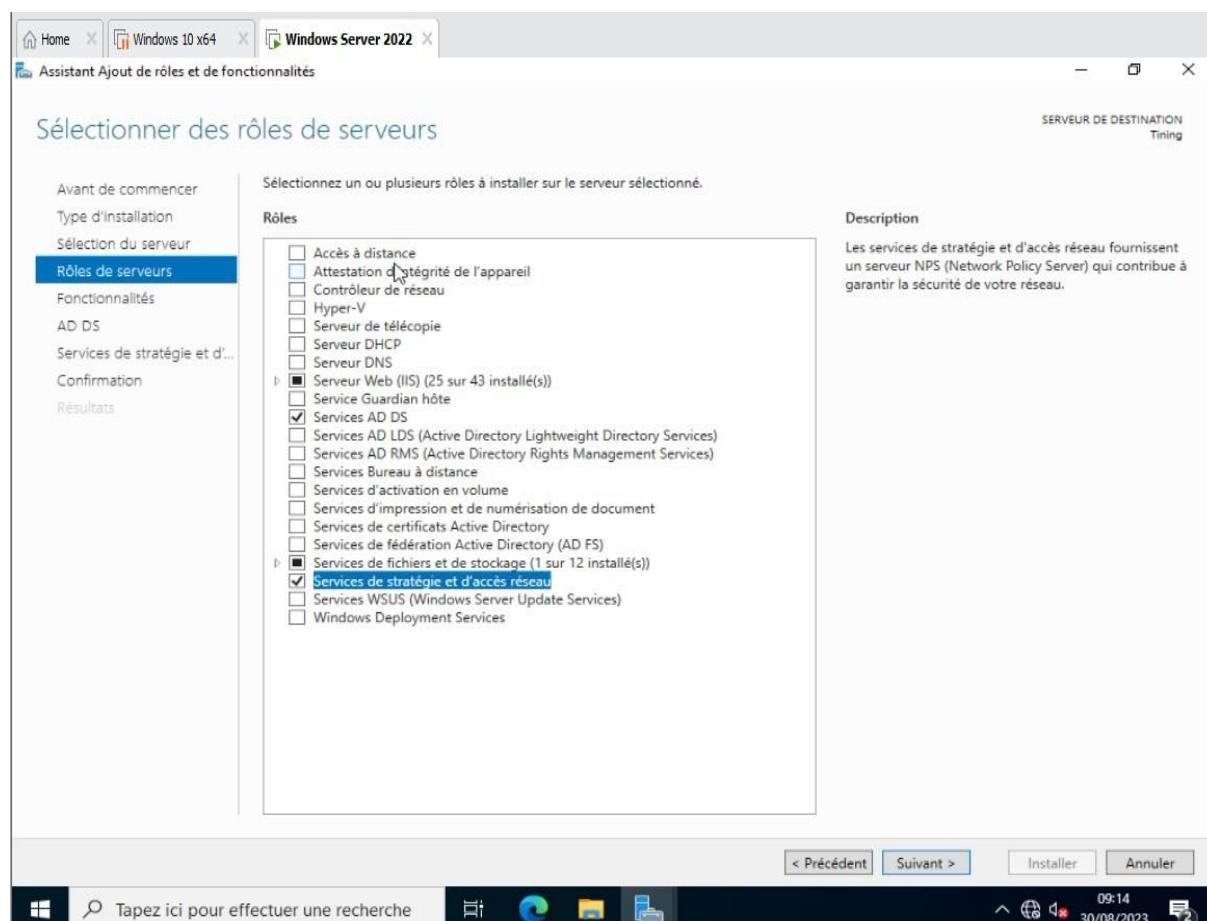
**Figure 40: Ajout d'un role et fonctionnalité**

- Sur l'interface qui s'affiche, cocher Service AD DS pour activer les fonctionnalités qui lui sont liées et cocher sur la fenêtre qui s'affiche ***Inclure les outils de gestion*** puis valider en cliquant sur ***ajouter des fonctionnalités***.

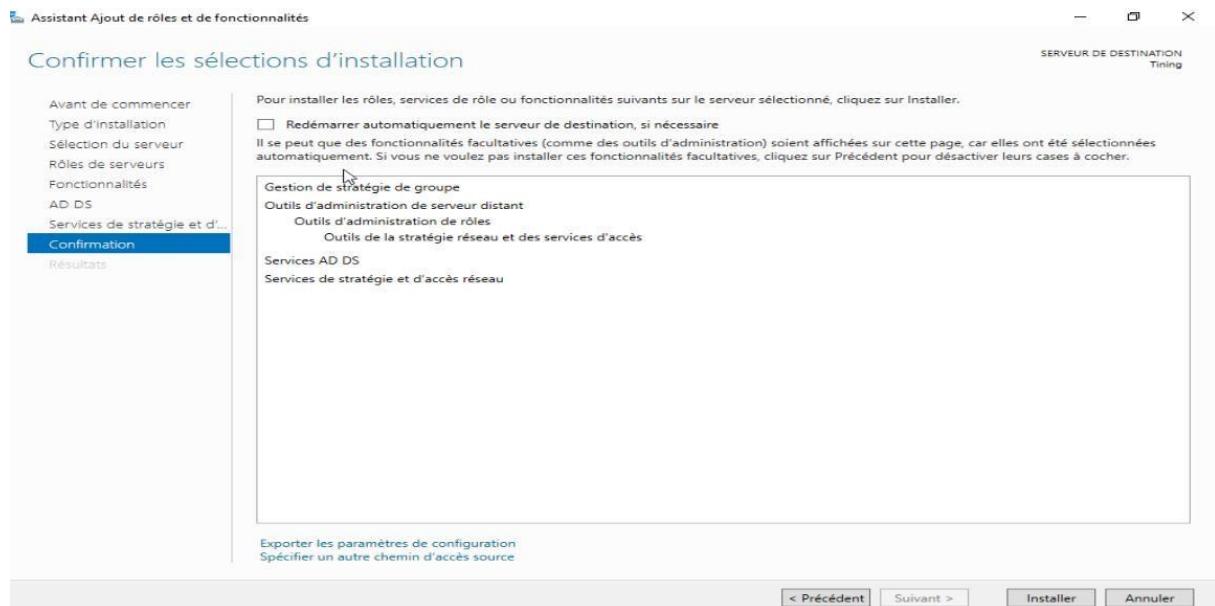


**Figure 41: Activation de la fonctionnalité ADDS**

Cliquer sur suivant pour poursuivre

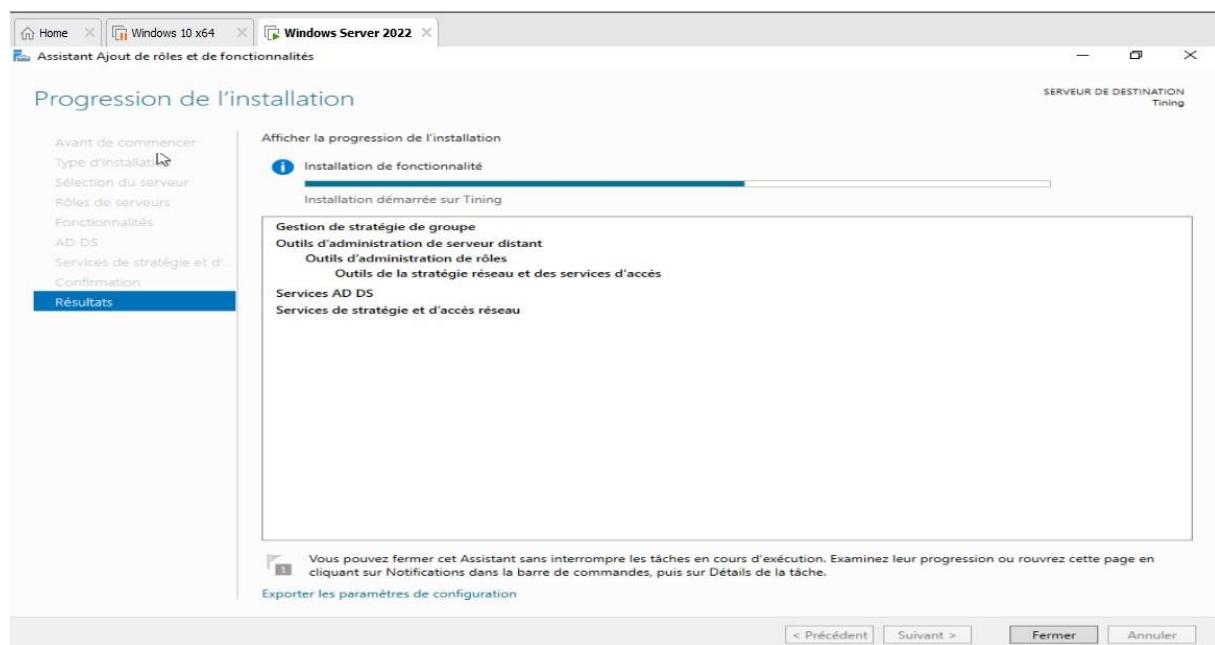


**Figure 42: Validation de l'ajout de la fonctionnalité**



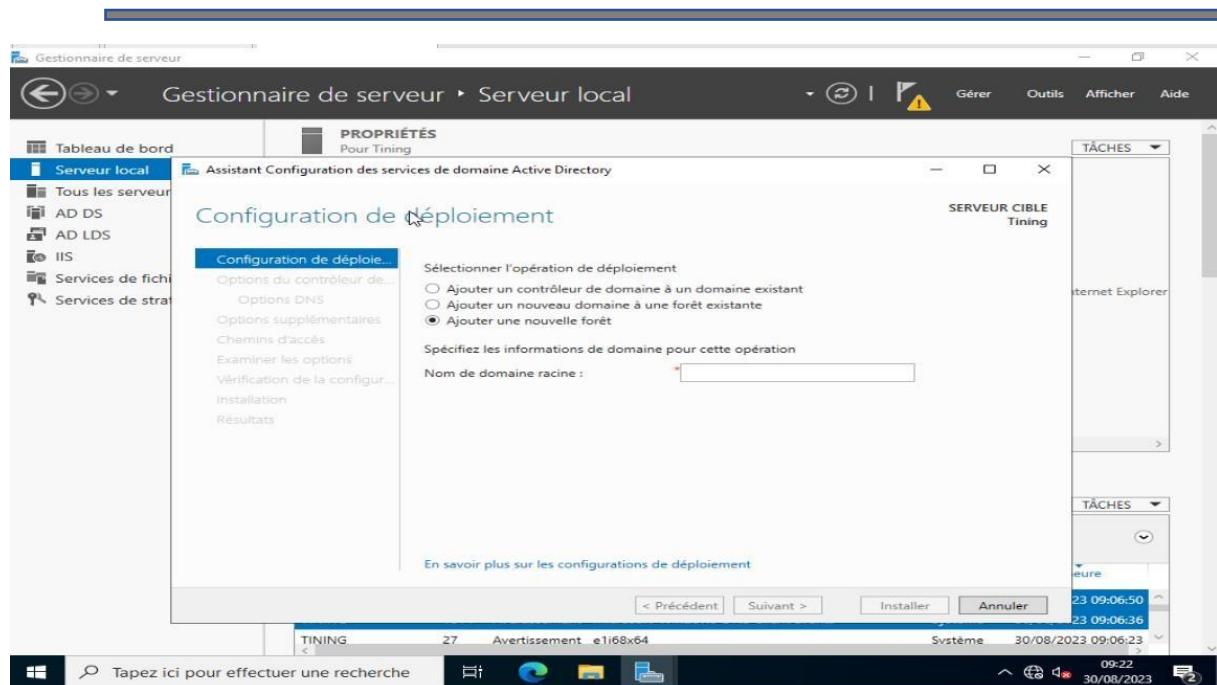
**Figure 43: Confirmations des sélections d'installations**

- Après avoir cliqué sur installer attendre que l'installation démarre et se termine tel qu'affiché sur la capture suivante



**Figure 44: Installation de l'ADDS**

A ce niveau, s'effectue un retour sur le tableau de bord

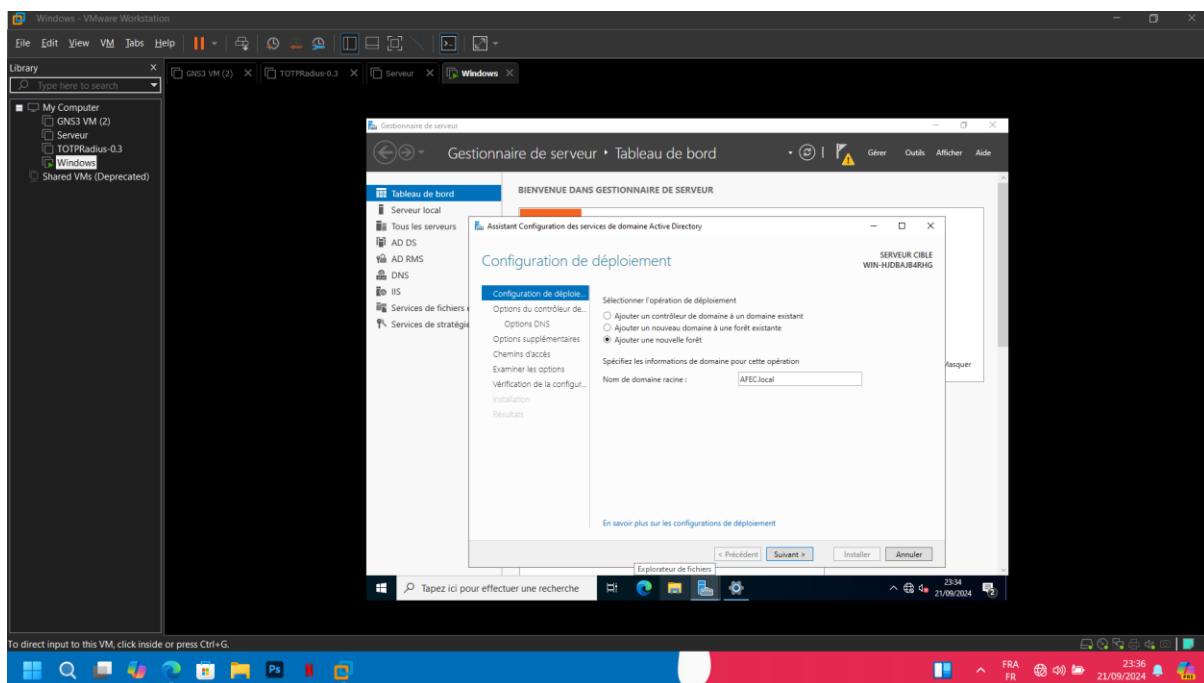


**Figure 45: Achevement de l'installation de l'ADDS –Tableau de bord**

Configuration et déploiement du service de domaine Active Directory. Nous poursuivons avec la configuration du point de déploiement sur l'interface qui s'affiche

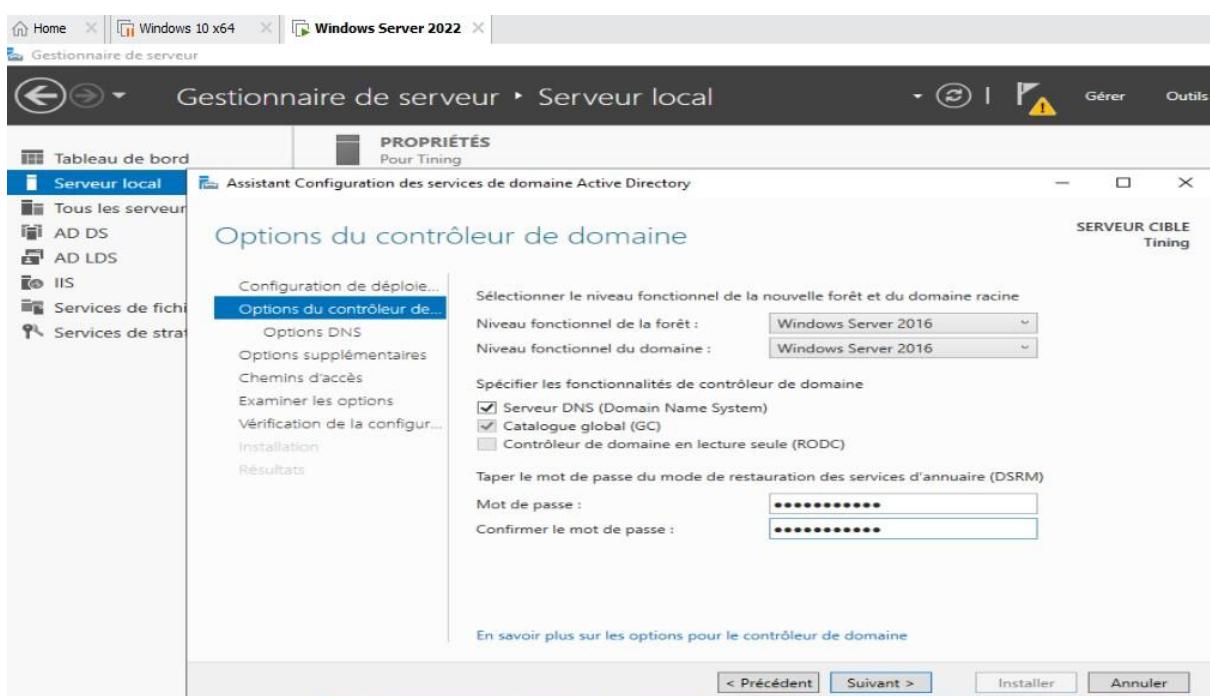
*Figure 47 : Configuration du point de déploiement*

Pour se faire nous devons ajouter une nouvelle forêt en cochant sur **Ajouter une nouvelle forêt**, entrant le nom de domaine racine, dans notre cas le nom de domaine est : **AFECameroun.local**



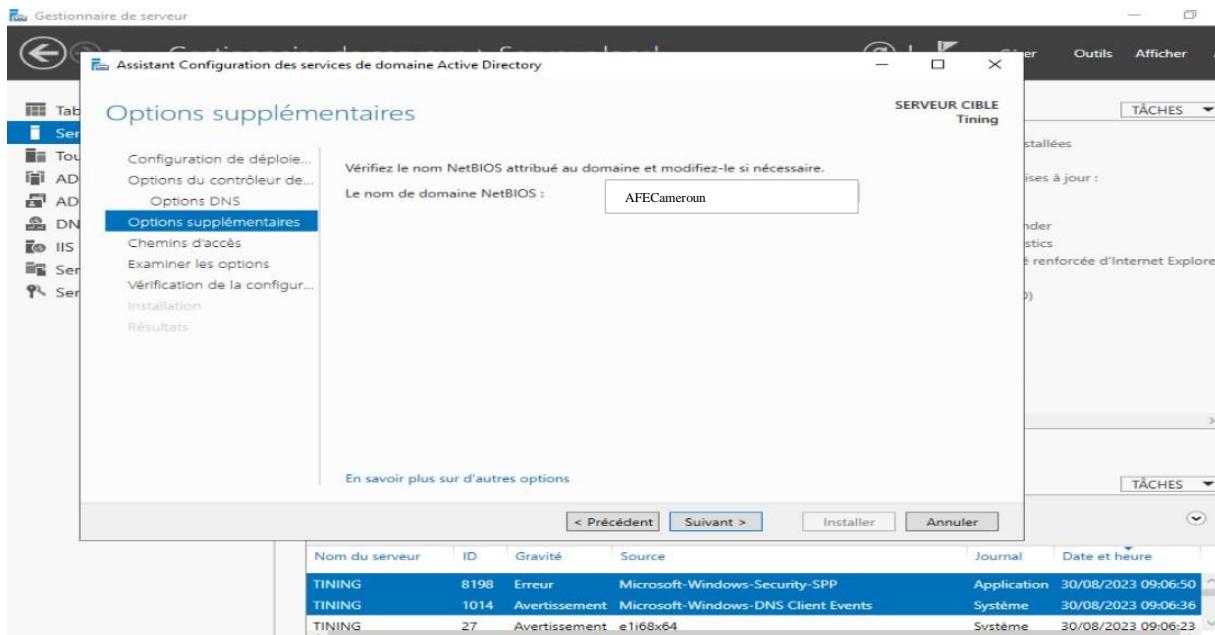
**Figure 46: Insertion du nom de domaine**

Ici il est question d'insérer un mot de passe tout en le confirmant à la fin, les autres options, cases à cocher ne doivent pas être changées.



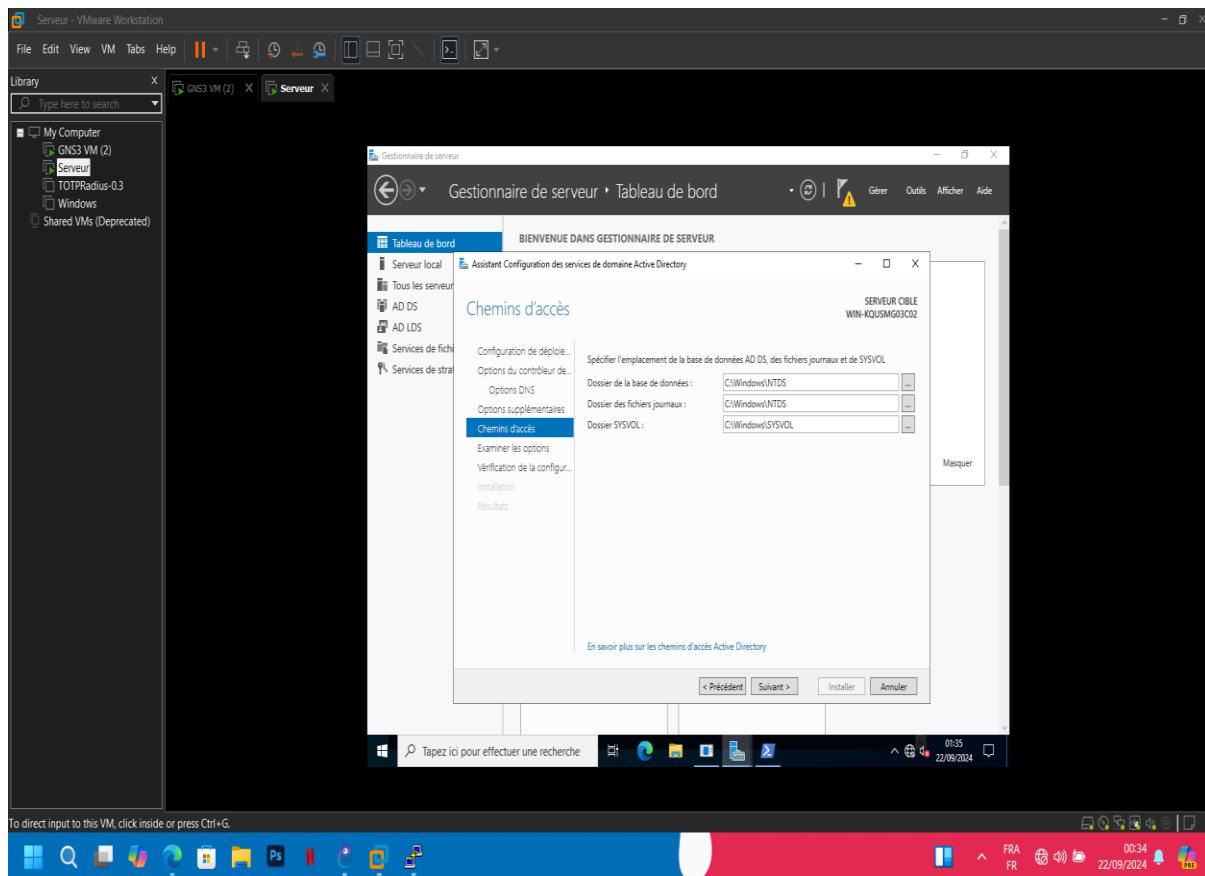
### Figure 47: Insertion du mot de passe

Nous poursuivons avec l'insertion du nom de domaine NetBIOS qui dans notre cas est LABOGENIE



### Figure 48: Indication du nom de domaine NetBIOS

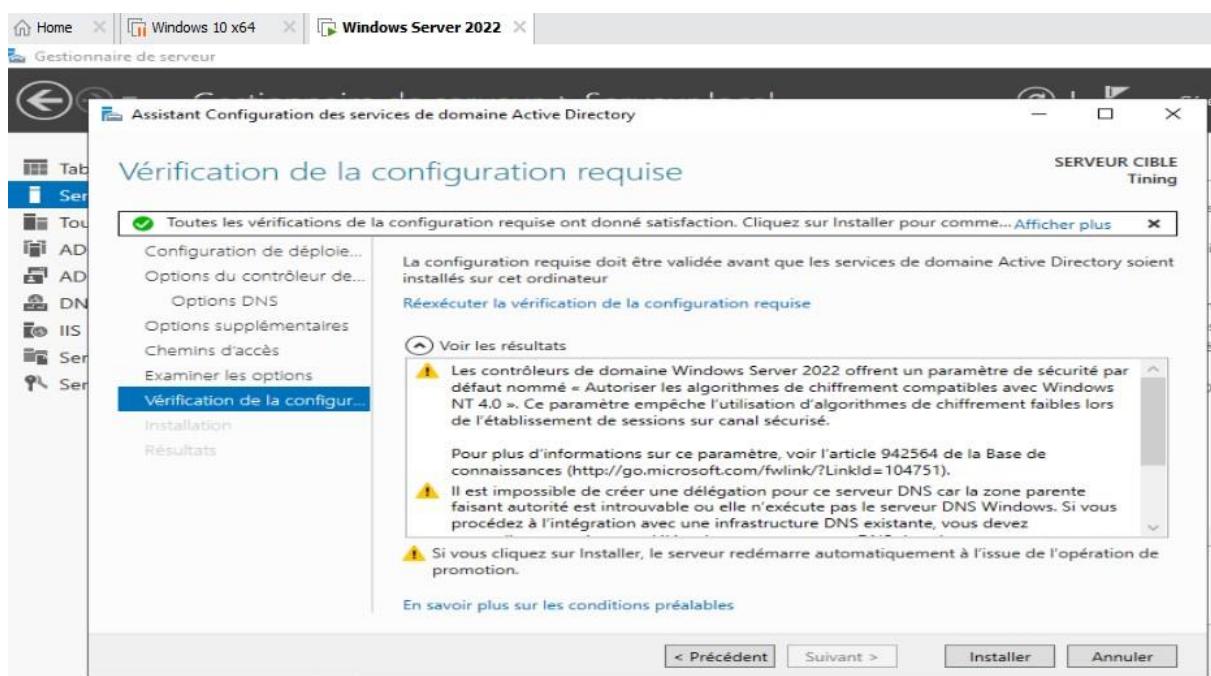
L'indication du chemin d'accès est l'étape qui succède, laisser tous les champs par défaut



**Figure 49: Indication du chemin d'accès**

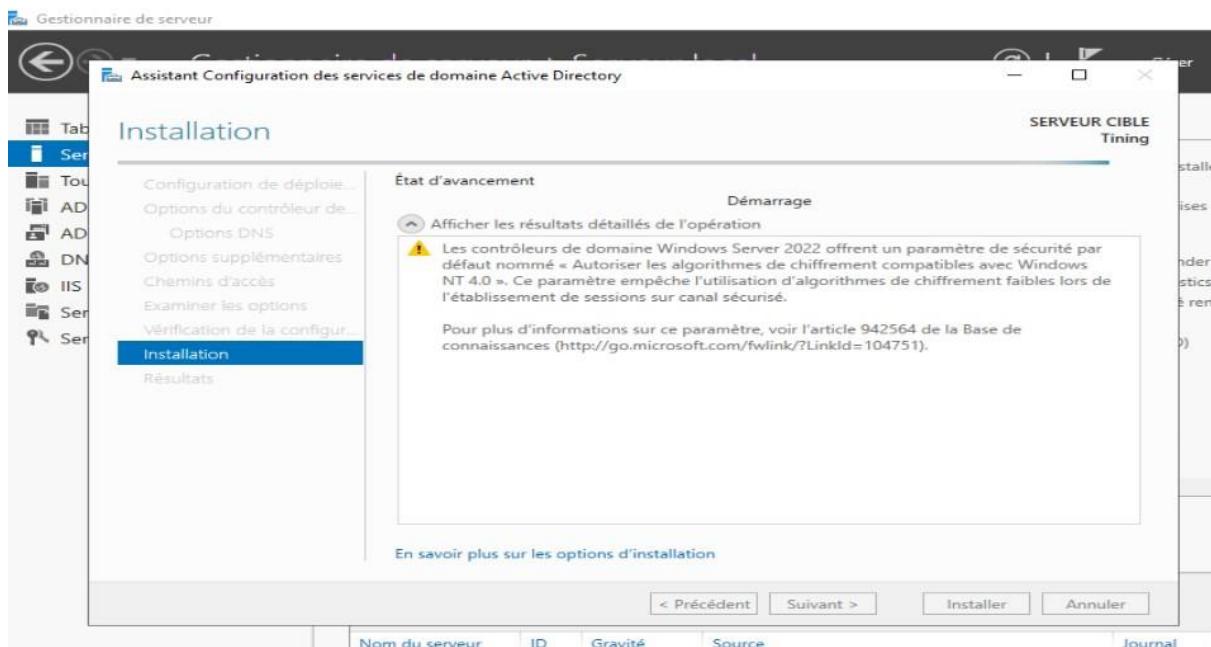
Après avoir indiqué le chemin d'accès, l'étape suivante consistera en la vérification des options, Vérifiez le et cliquer sur suivant.

A la fin de la vérification nous avons un résultat positif, nous pouvons en ce moment cliquer sur le bouton **Installer**



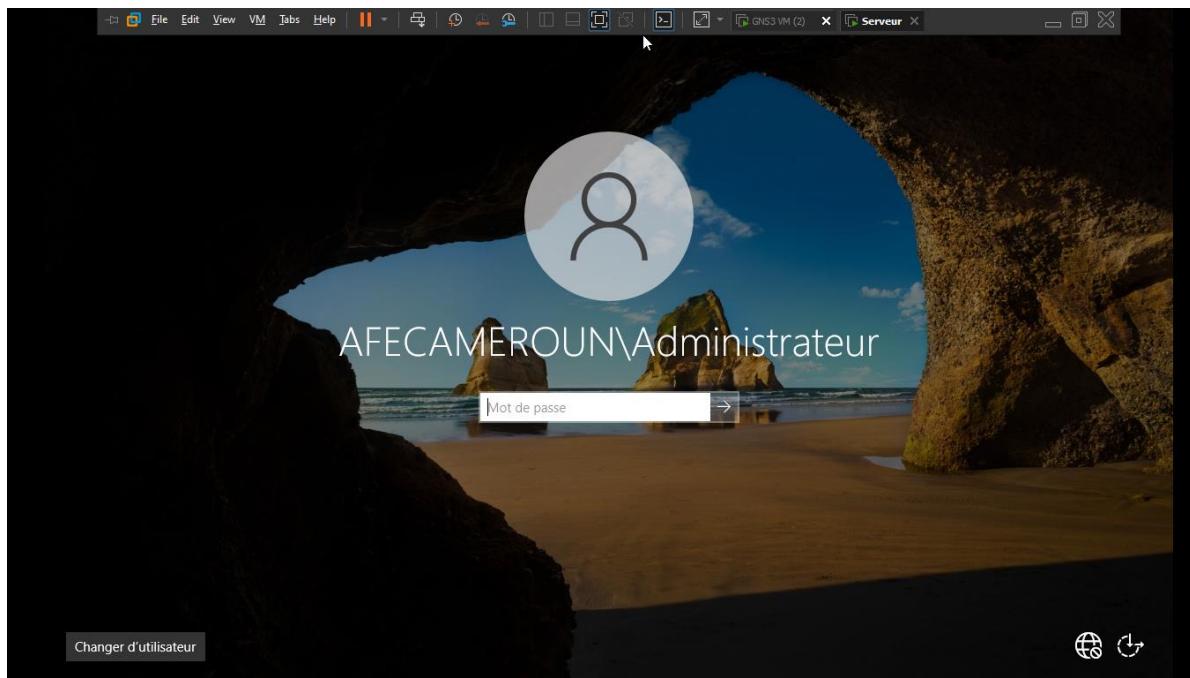
**Figure 50: Résultat de la vérification des options**

Démarrage du processus d'installation, jusqu'au redémarrage du système



**Figure 51: Installation du service ADDS**

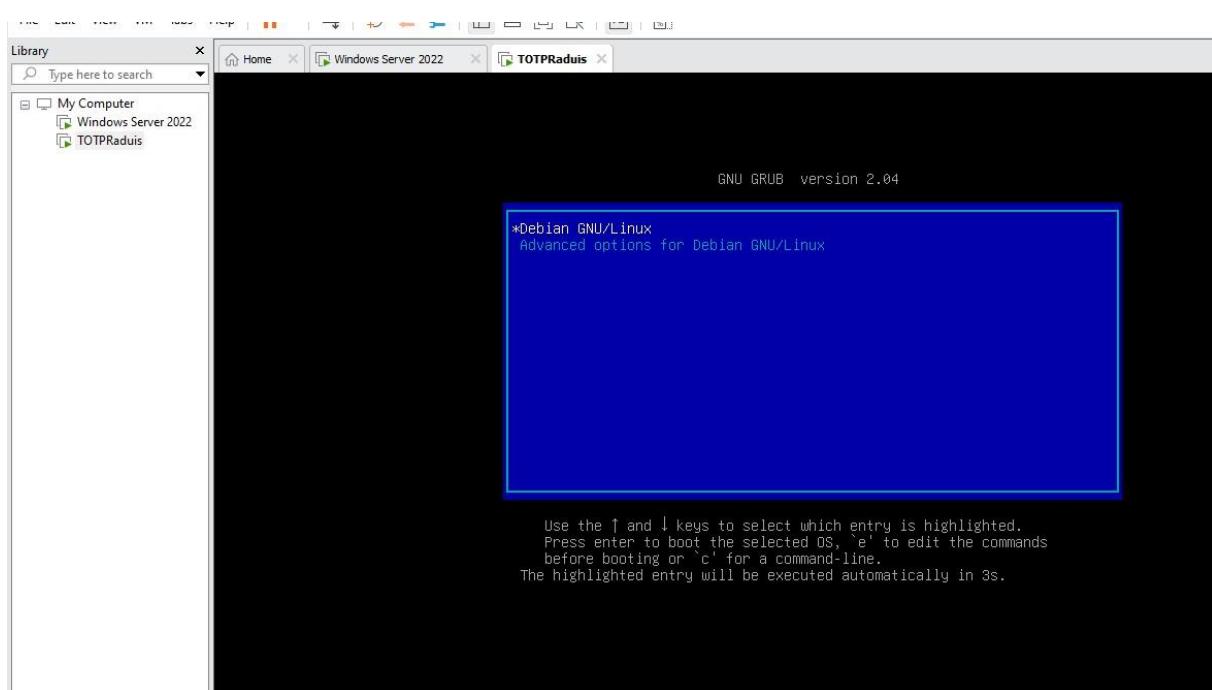
Le système à la fin redémarre en prenant en compte les configurations, on peut apercevoir le compte **AFECAMEROUN\ADMINISTEUR** et un compte pour les autres utilisateurs



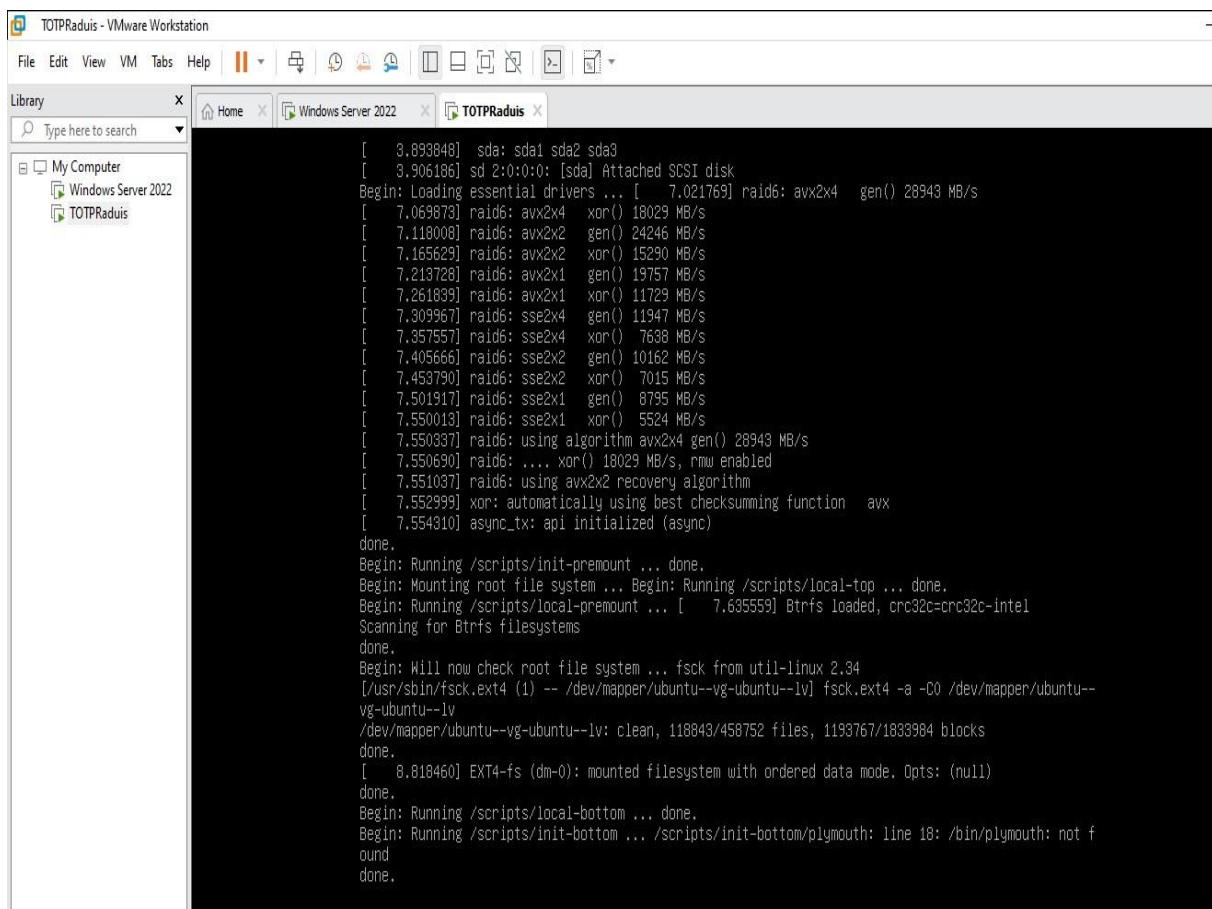
**Figure 52: Interface de Connexion**

## 2. Installation et configuration de l'appliance TOTPRadius

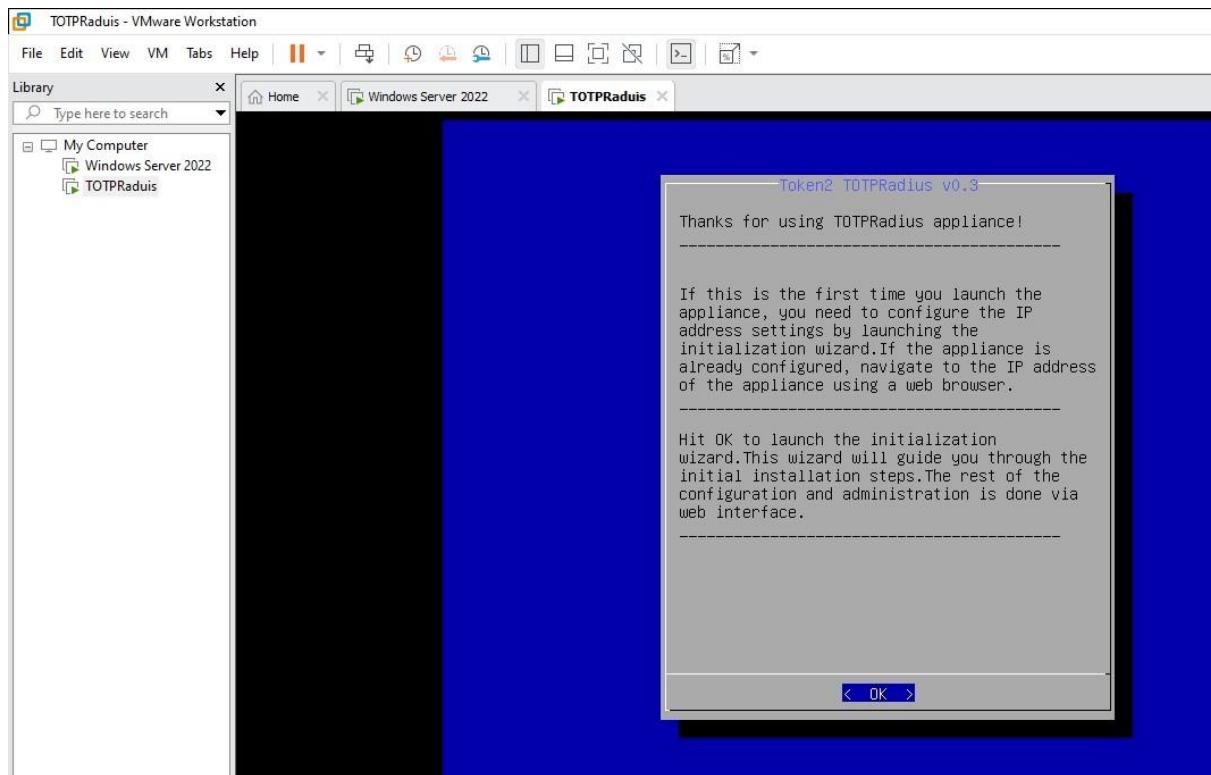
TOTPRadius est déployé au format OVF standard. Suivez les procédures d'importation OVF habituelles pour installer l'appliance. La configuration de TOTPRadius est son nom (**TOTPRadius**), son IP (**192.168.10.18**), son subnet mask (**255.255.255.192**), son Gateway (**192.168.10.1**) et son DNS (**8.8.8.8**) en suivant les étapes suivantes :



**Figure 53: Lancement TOTPRadius**

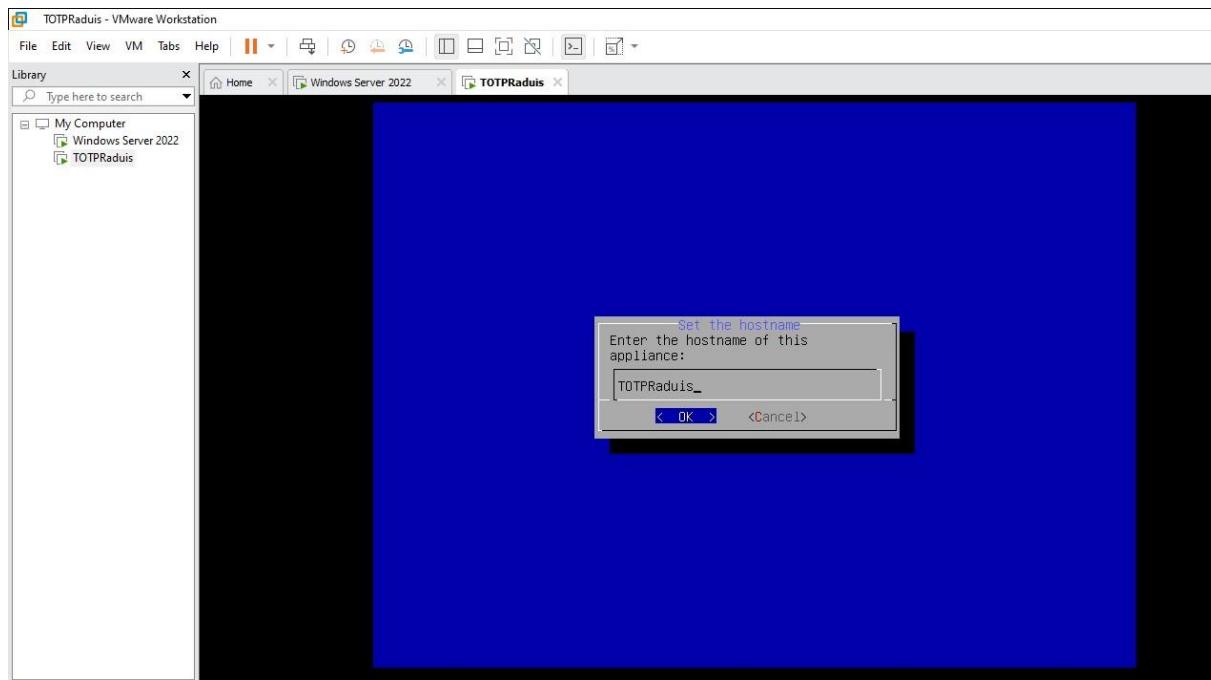


**Figure 54: Chargement de la configuration de TOTPRadius**

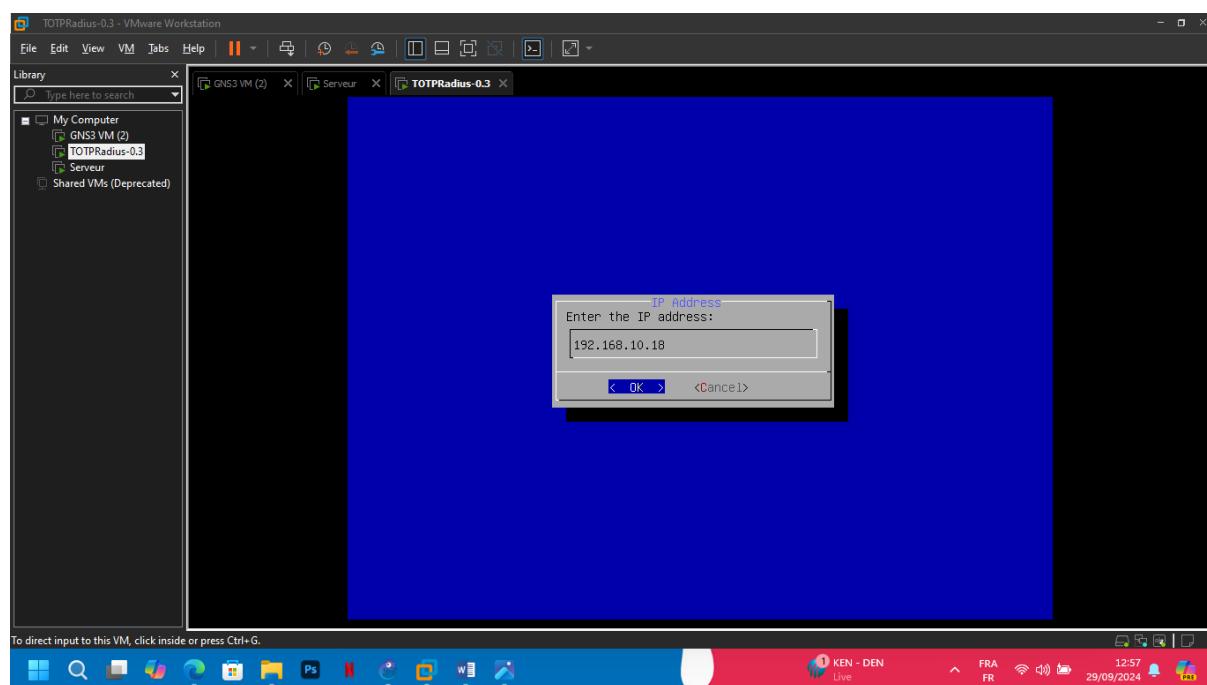


**Figure 55: Lancement TOTPRadius**

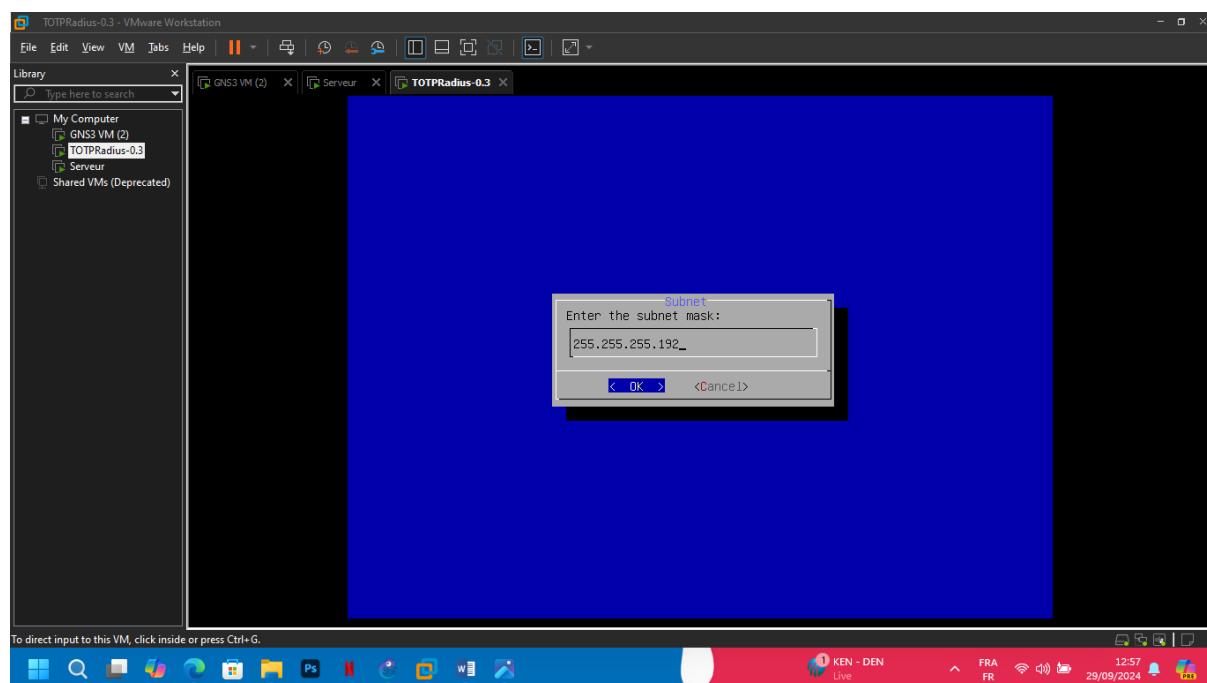
Ensuite



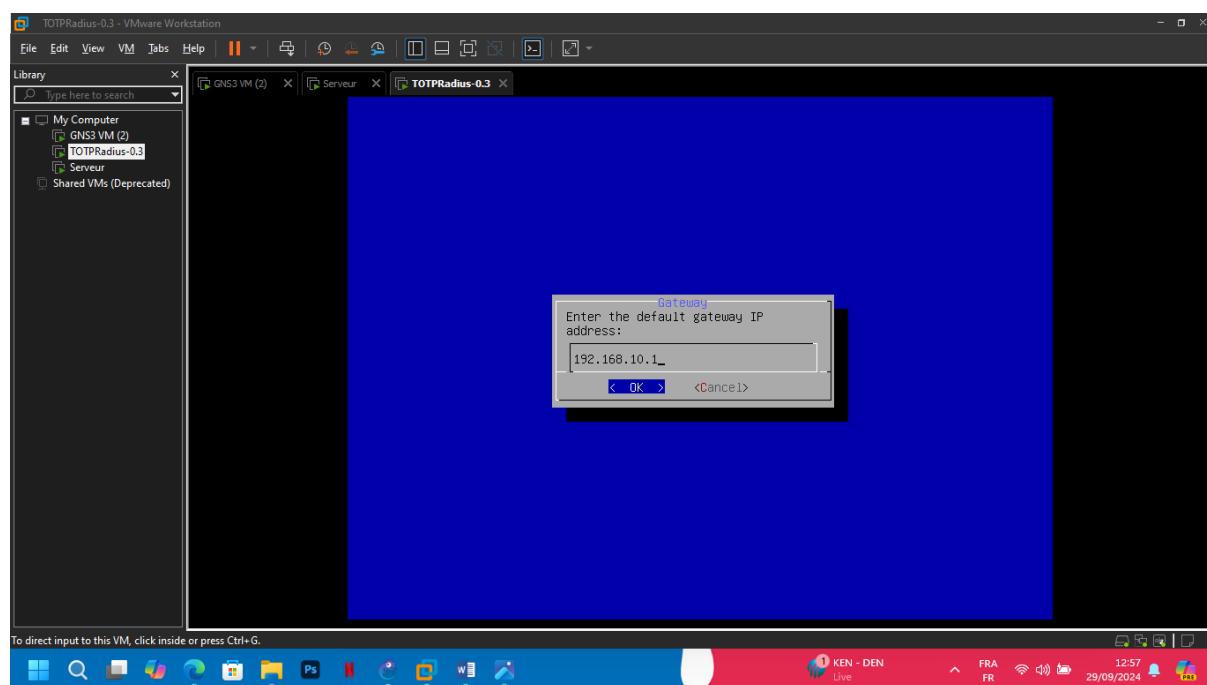
**Figure 56: Nom de notre serveur TOTPRadius**



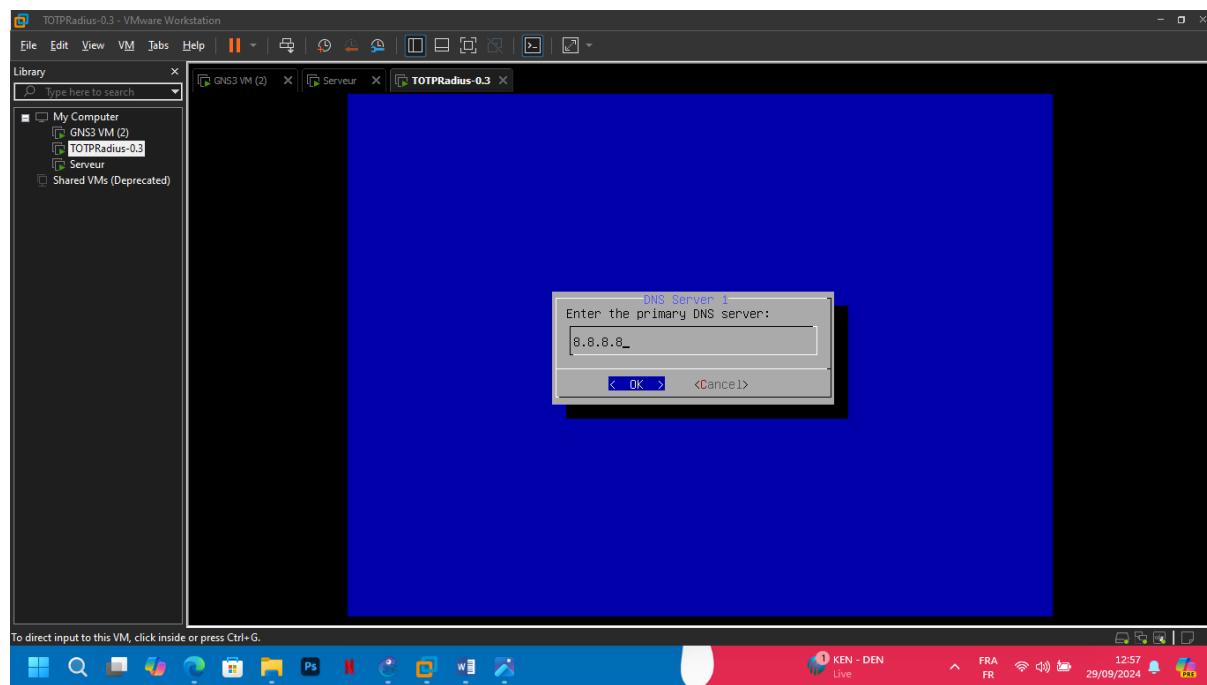
**Figure 57: Adresse IP de notre serveur TOTPRadius**



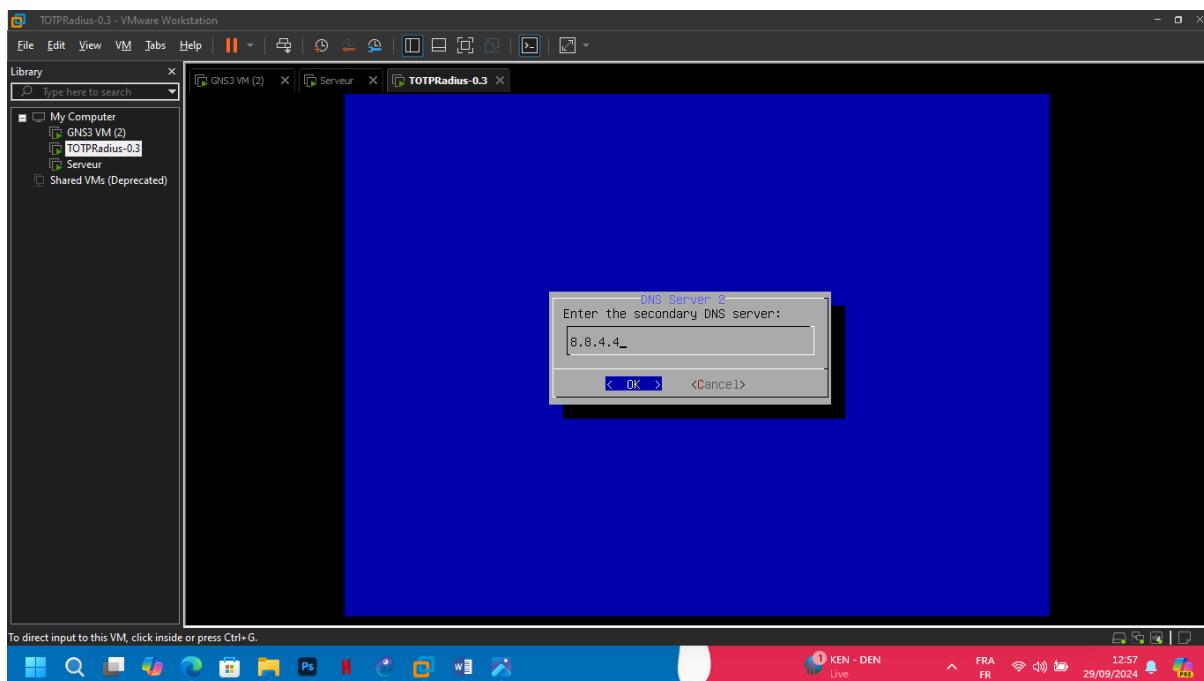
**Figure 58: Masque de sous reseau**



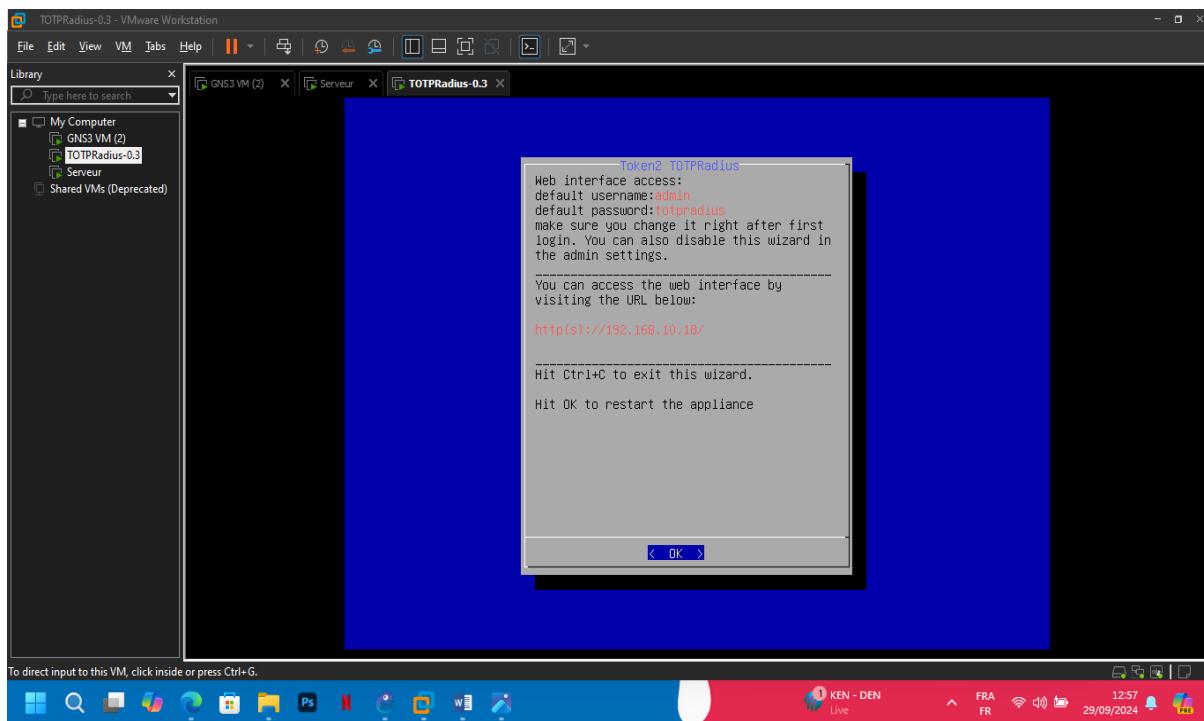
**Figure 59: Gateway de TOTPRadius**



**Figure 60: Premier DNS de TOTPradius**

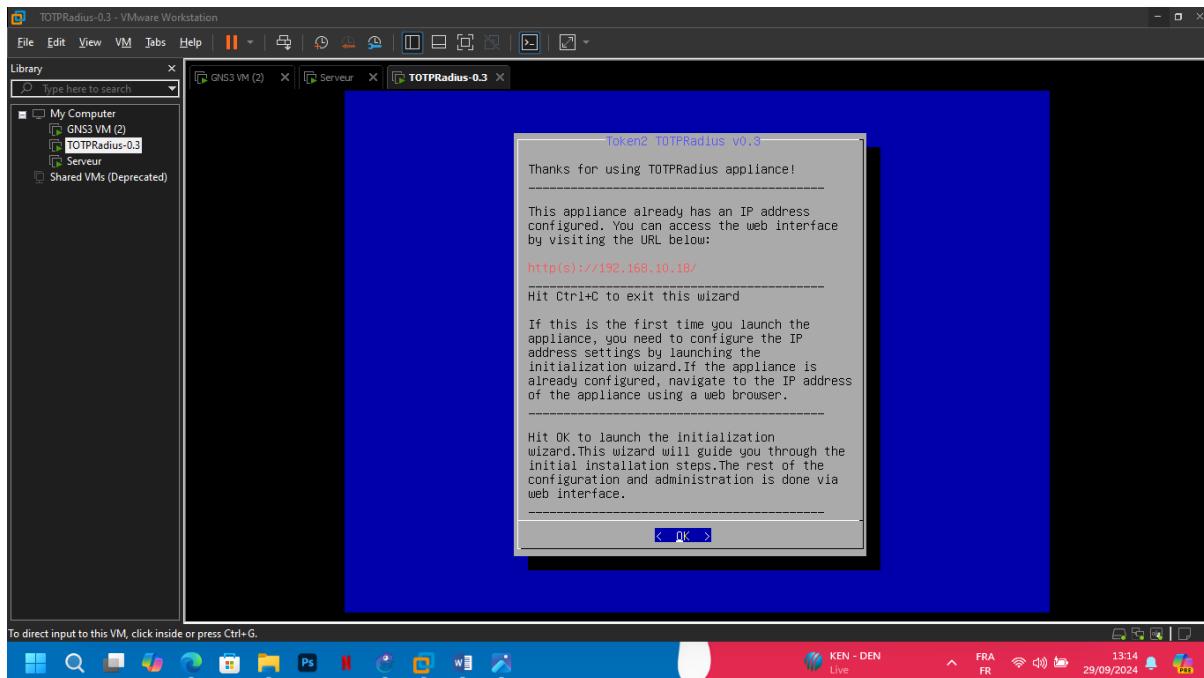


**Figure 61: Deuxieme DNS de TOTPradius**



**Figure 62: Fin de la configuration de TOTPradius**

Une fois terminer cliquer sur OK pour que les configurations soient enregistrées.

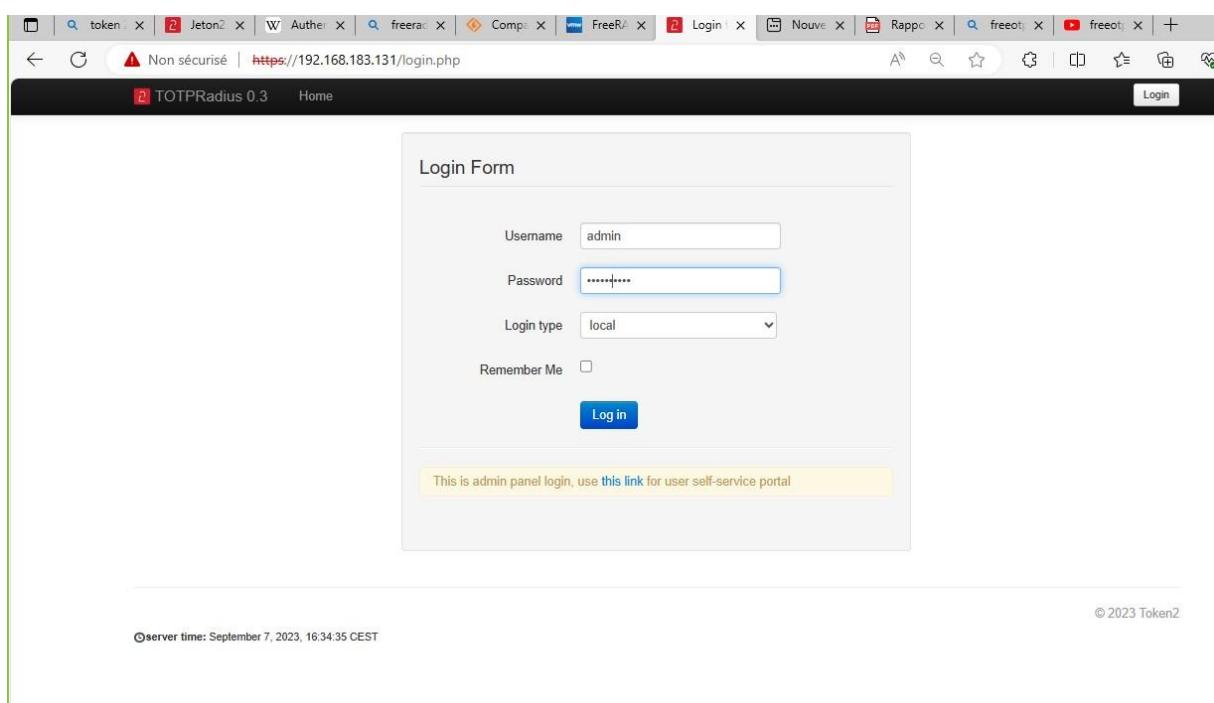


**Figure 63: Interface de TOTPradius**

### **3. Configuration du second facteur d'authentification**

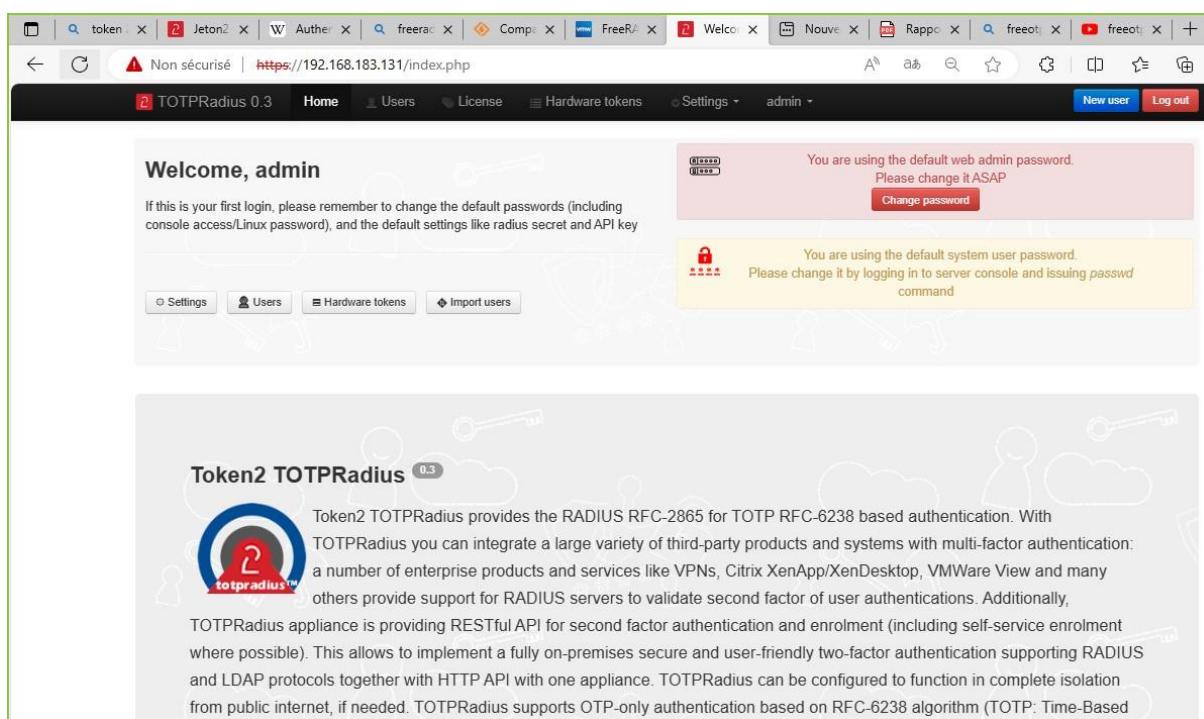
Une fois l'Appliance TOTP Radius installée et initialisée, configurez les paramètres suivants sur la page Paramètres généraux :

Se connecter sur la page web de l'Appliance <http://192.168.10.18> en entrant le **user Name** et le **Password**



**Figure 64: Interface de connexion TOTPradius**

Une connecté, nous avons la possibilité de changer le mot de passe de la page web et de la console.



**Welcome, admin**

If this is your first login, please remember to change the default passwords (including console access/Linux password), and the default settings like radius secret and API key

You are using the default web admin password.  
Please change it ASAP  
[Change password](#)

You are using the default system user password.  
Please change it by logging in to server console and issuing `passwd` command

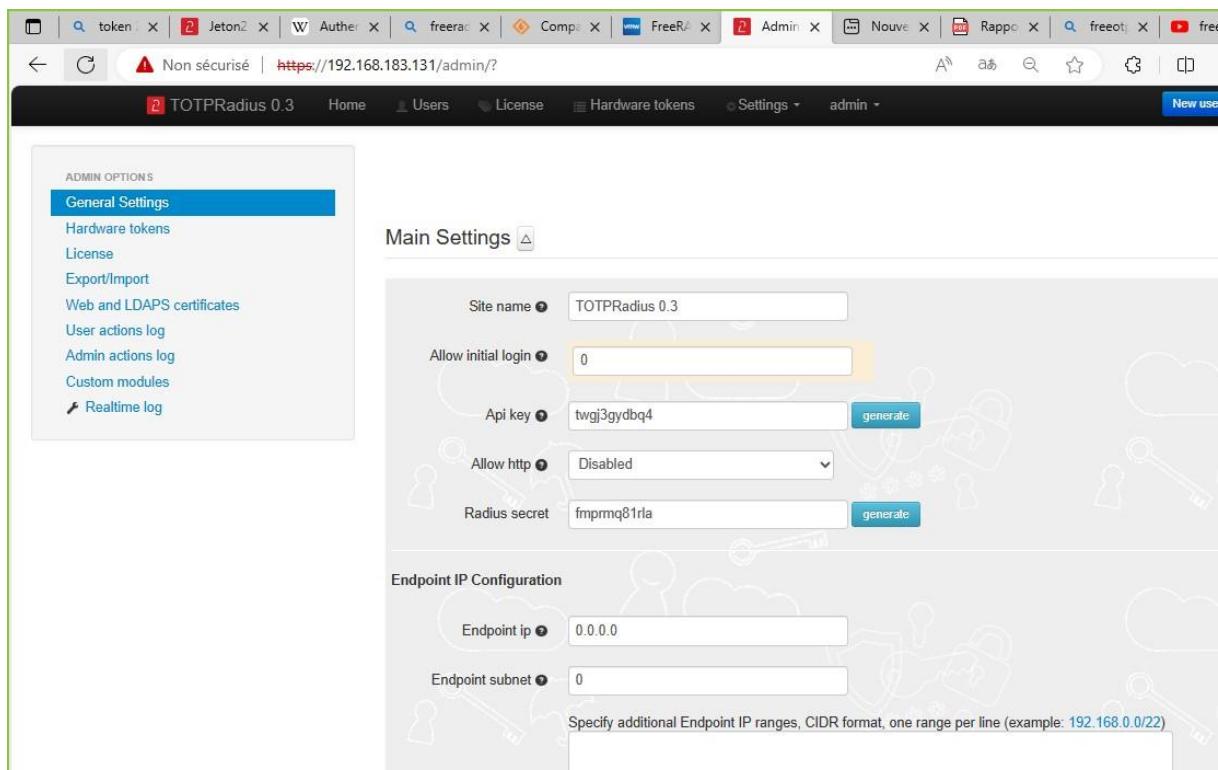
Settings | Users | Hardware tokens | Import users

**Token2 TOTPRadius 0.3**

Token2 TOTPRadius provides the RADIUS RFC-2865 for TOTP RFC-6238 based authentication. With TOTPRadius you can integrate a large variety of third-party products and systems with multi-factor authentication: a number of enterprise products and services like VPNs, Citrix XenApp/XenDesktop, VMWare View and many others provide support for RADIUS servers to validate second factor of user authentications. Additionally, TOTPRadius appliance is providing RESTful API for second factor authentication and enrolment (including self-service enrolment where possible). This allows to implement a fully on-premises secure and user-friendly two-factor authentication supporting RADIUS and LDAP protocols together with HTTP API with one appliance. TOTPRadius can be configured to function in complete isolation from public internet, if needed. TOTPRadius supports OTP-only authentication based on RFC-6238 algorithm (TOTP: Time-Based

**Figure 65: Page de TOTPradius**

Ensuite cliquer sur ‘Setting’ pour configurer la double authentification.



**ADMIN OPTIONS**

**General Settings**

- Hardware tokens
- License
- Export/Import
- Web and LDAPS certificates
- User actions log
- Admin actions log
- Custom modules
- Realtime log

**Main Settings**

Site name: TOTPRadius 0.3

Allow initial login: 0

Api key: twgj3gydbq4 [generate](#)

Allow http: Disabled

Radius secret: fmpmq81rla [generate](#)

**Endpoint IP Configuration**

Endpoint ip: 0.0.0.0

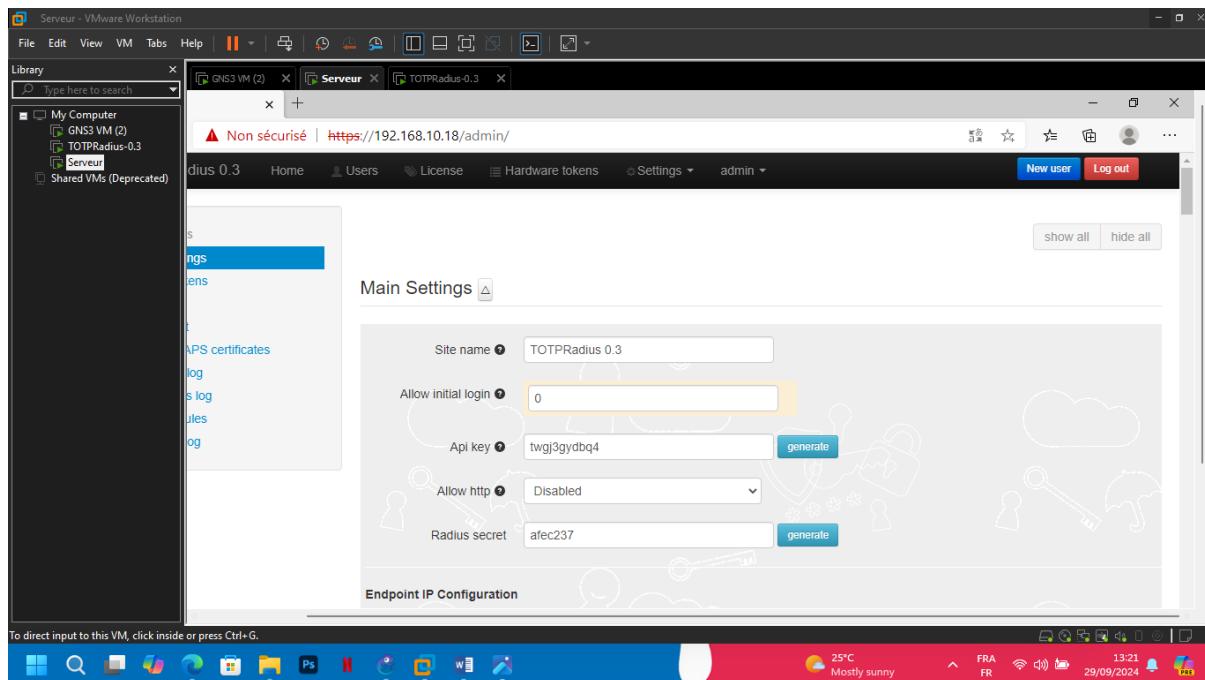
Endpoint subnet: 0

Specify additional Endpoint IP ranges, CIDR format, one range per line (example: 192.168.0.0/22)

**Figure 66: Setting de TOTPradius**

Et remplir les champs suivants :

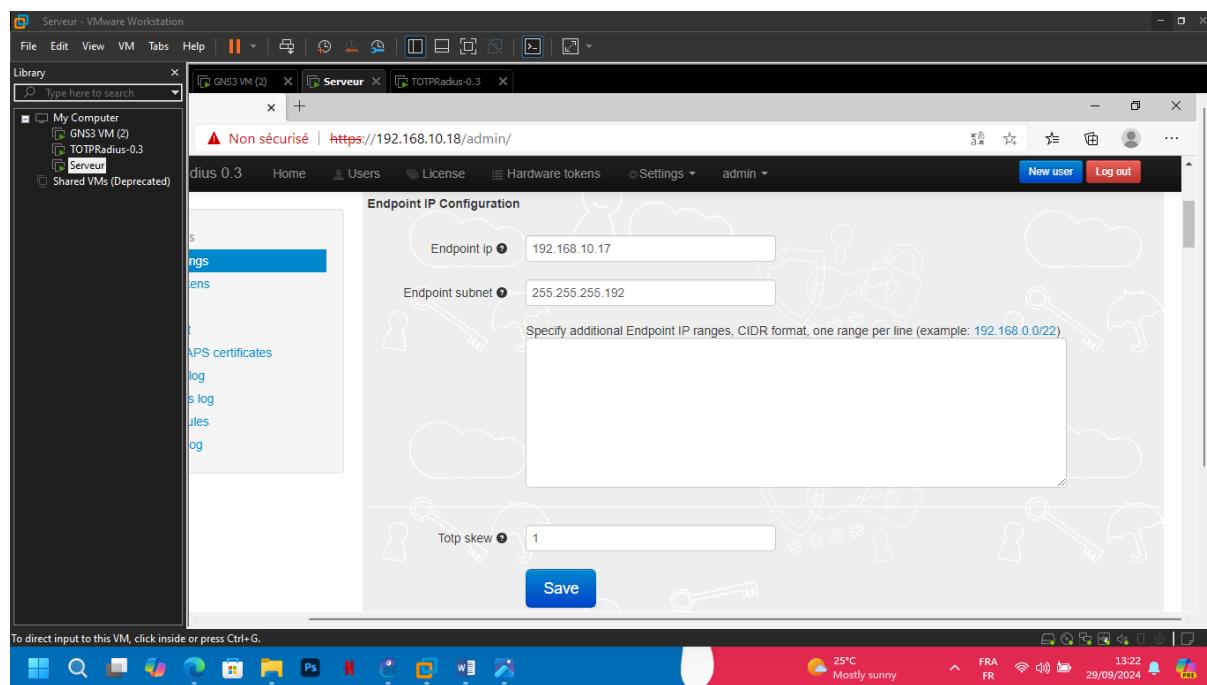
Définir ou générer un nouveau secret Radius et Définissez la valeur Allow initial login' sur zéro



**Figure 67 :Parametre de radius dans TOTPradius**

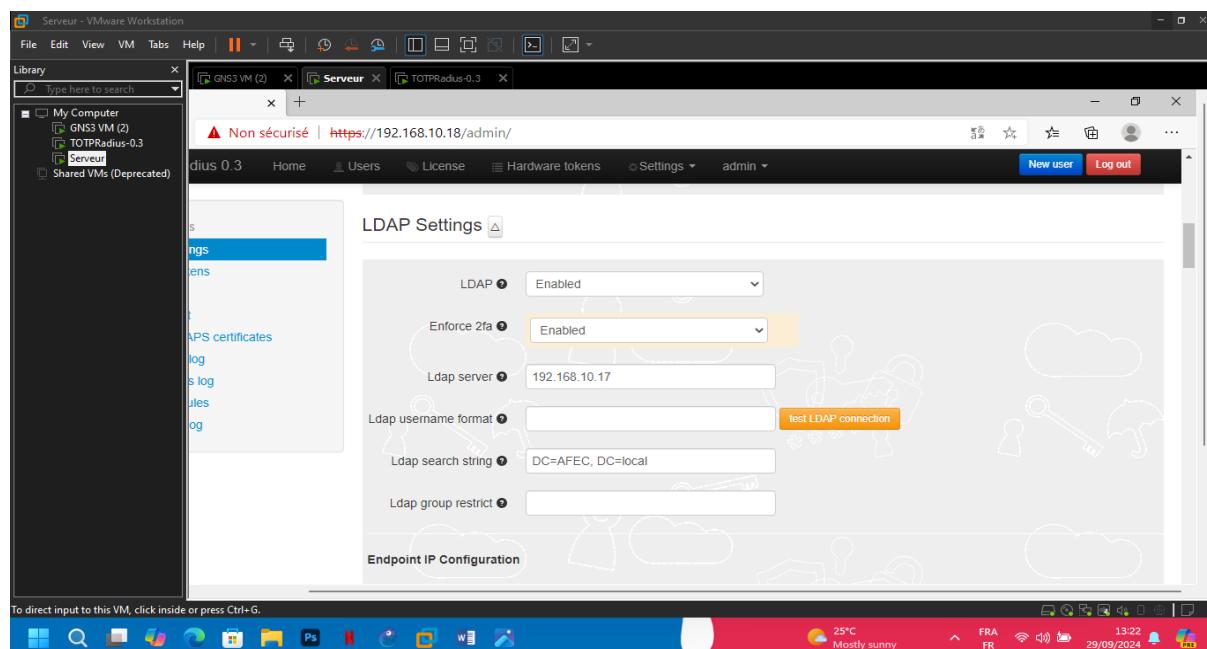
Dans les champs **Endpoint IP** and **subnet** spécifiez les paramètres du routeur ;

**NB : TOTP skew** permet de se connecter avec un OTP "expiré". L'objectif principal est de permettre les connexions à l'aide de smartphones présentant des problèmes de synchronisation de l'heure. Le régler sur '**1**' permet 3 valeurs (valeur OTP actuelle, précédente et suivante). Le mettre à '**0**' n'autorise que l'OTP actuel.



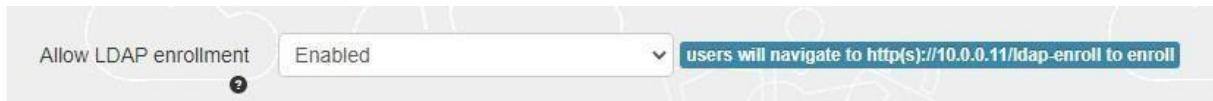
**Figure 68: IP du serveur radius**

Définir LDAP comme activé et spécifiez l'IP/FQDN du serveur LDAP  
(192.168.10.17) et le Ldap search String



**Figure 69: Configuration de LDAP**

Si vous décidez d'autoriser l'auto-inscription, assurez-vous que le paramètre "Autoriser l'inscription LDAP" est activé. Dans la même section, vous pouvez également autoriser la réinscription et modifier le texte d'introduction de la page Web d'inscription LDAP.

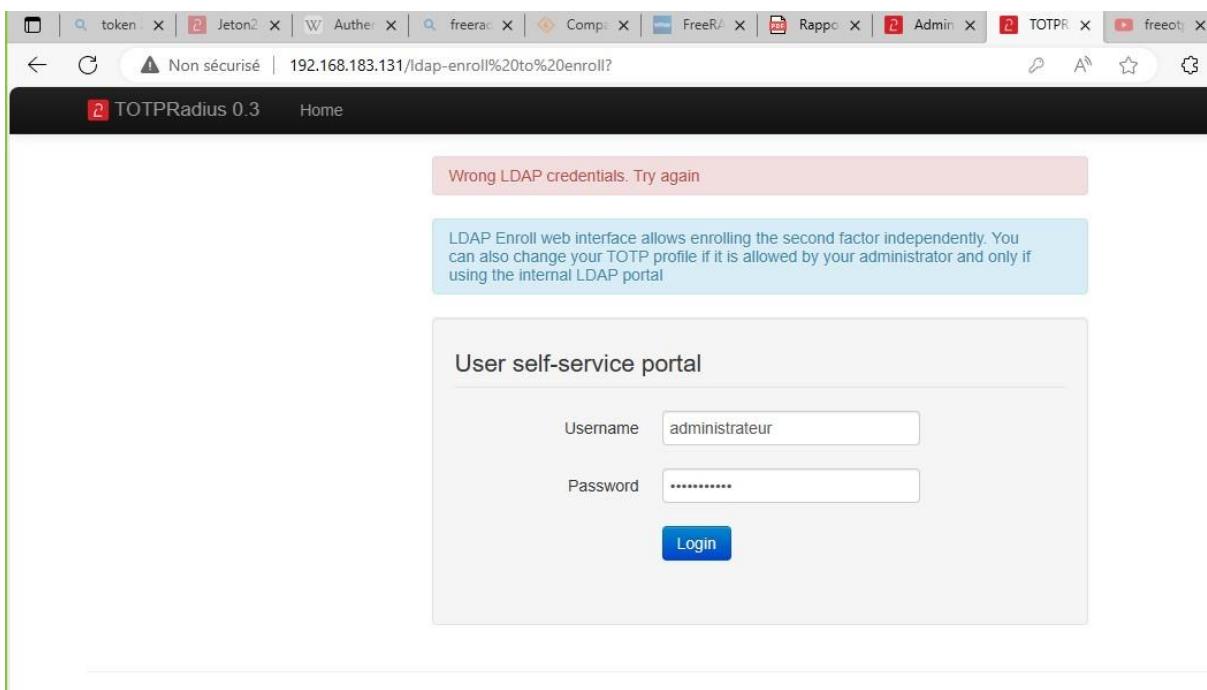


**Figure 70: Enregistrement des utilisateurs de TOTPRadius**

Générer ou définir le deuxième facteur pour l'utilisateur sur l'Appliance TOTPRadius

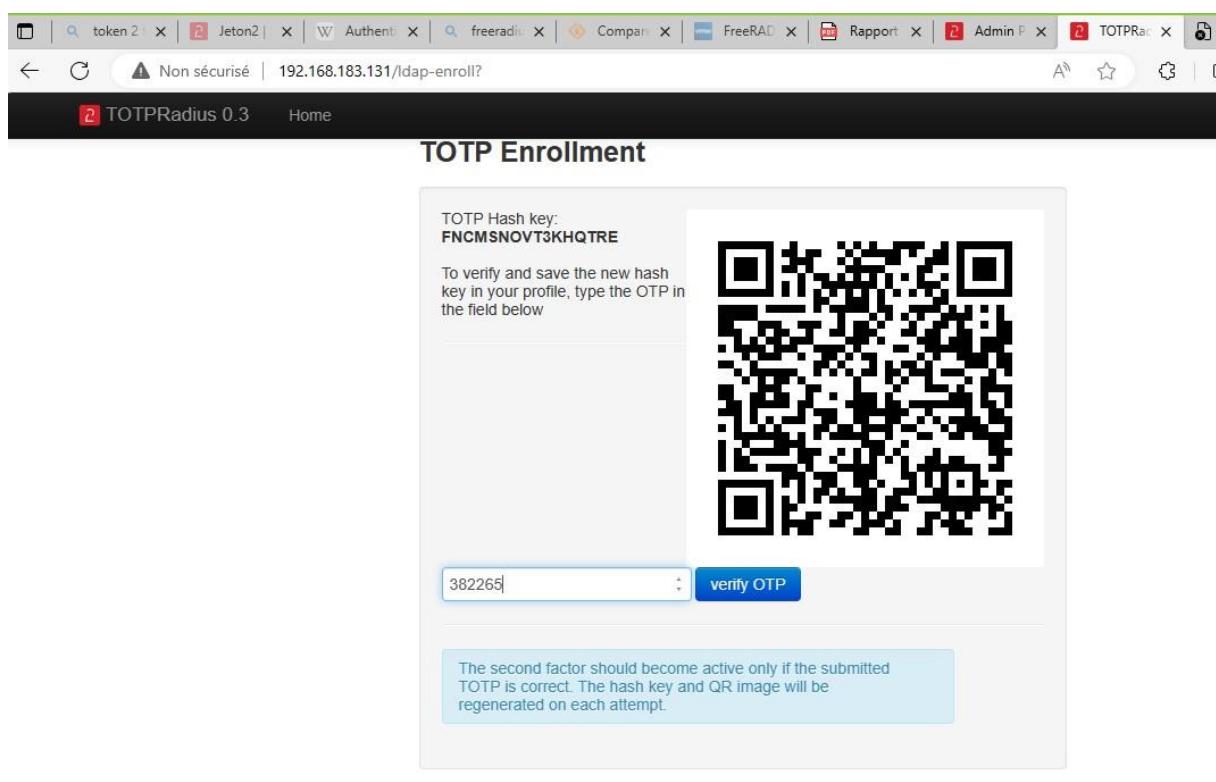
Le deuxième facteur pour l'utilisateur peut être ajouté de deux manières :

- **1<sup>ere</sup> méthode :** Par auto-inscription. Les utilisateurs peuvent inscrire eux-mêmes leurs jetons matériels en utilisant le lien '[http://\(totpradius server\\_ip\)/ldap-enroll](http://(totpradius server_ip)/ldap-enroll)' :

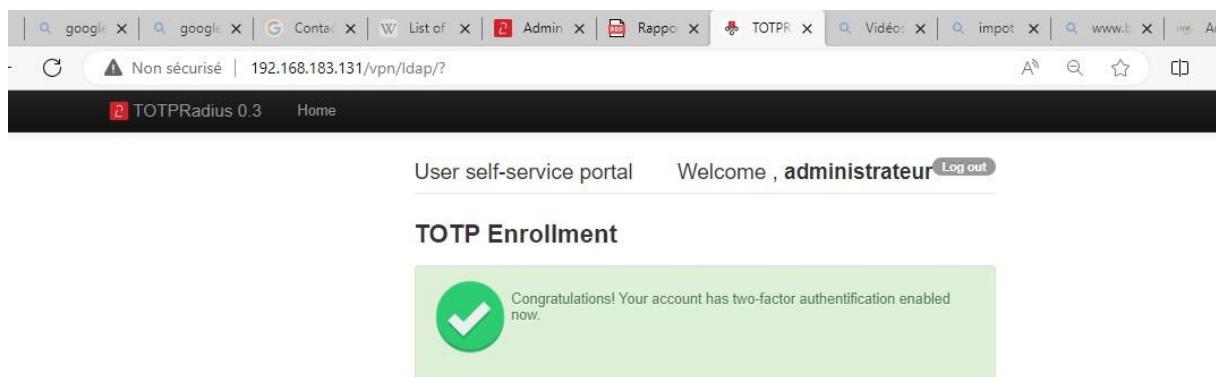


**Figure 71: Interface d'enregistrement des user**

Cliquez sur login et scannez le QR code qui s'affiche avec votre téléphone puis vérifier l'OTP qui s'affiche sur votre téléphone.



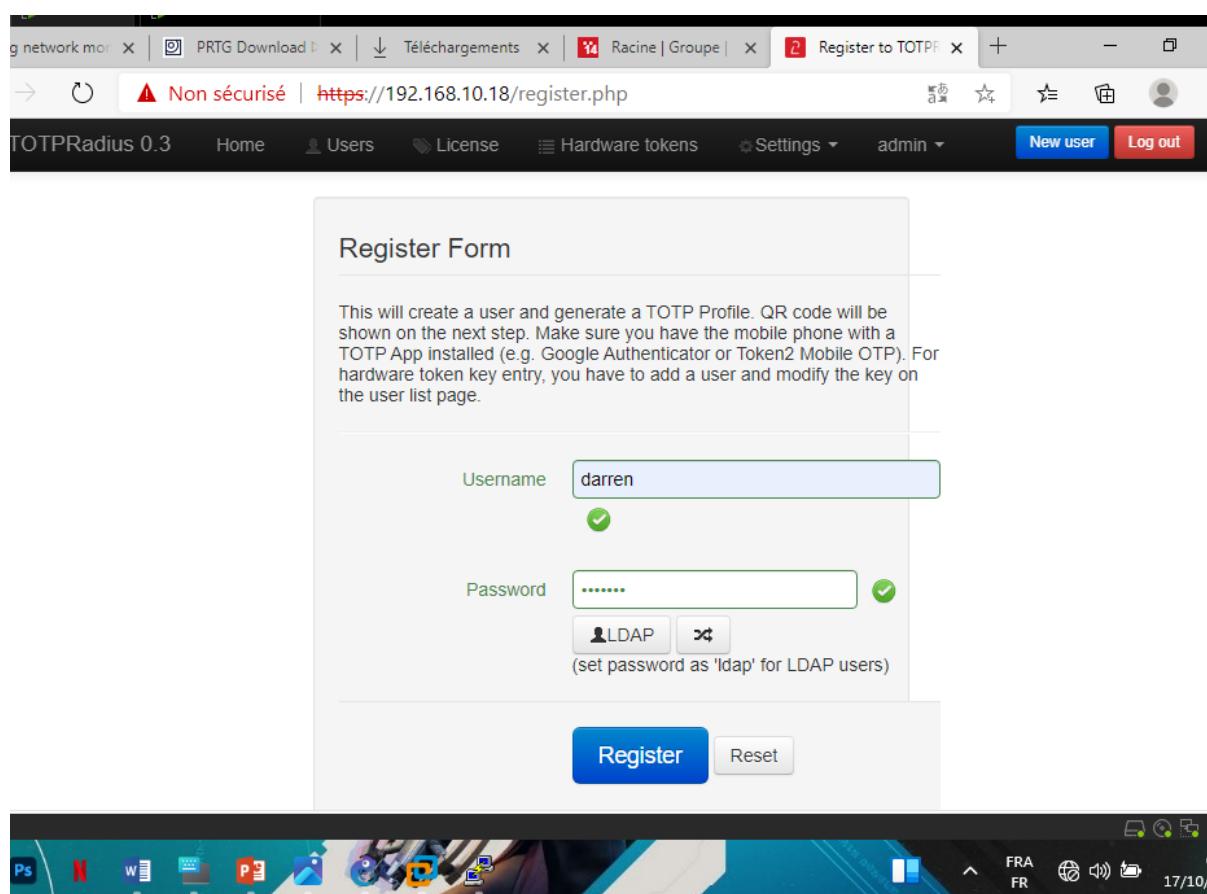
**Figure 72: Code QR de l'user Administrateur**



**Figure 73: Enregistrement d'administrateur**

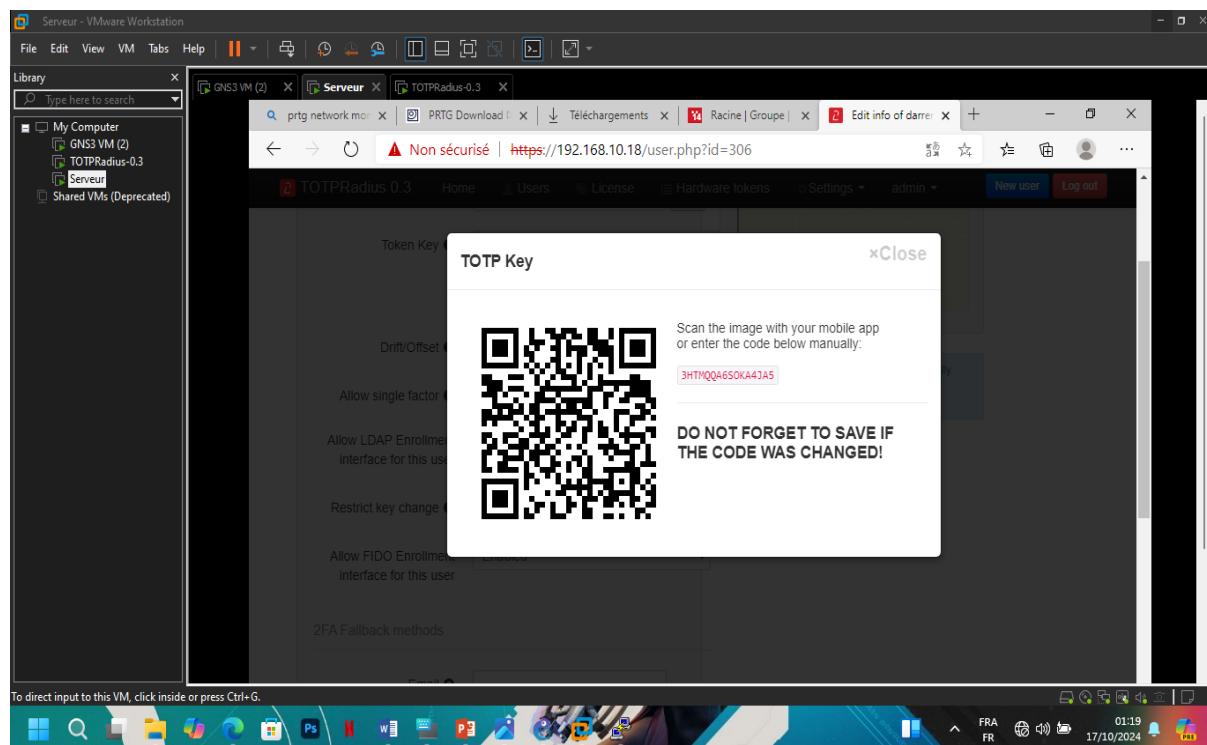
L'auto-inscription est possible à l'aide de n'importe quelle application TOTP (telle que Google Authenticator ou Microsoft Authenticator). Si vous souhaitez utiliser notre matériel programmable, vous pouvez graver le secret sur le jeton matériel en scannant le code QR à l'aide de l'une des applications NFC Burner.

- **2<sup>eme</sup> méthode** : Par l'administrateur de TOTPRadius. Connectez-vous à l'interface d'administration de TOTPRadius et cliquez sur '**New user**' :



**Figure 73: Creation des User**

Scannez le QR code suivant

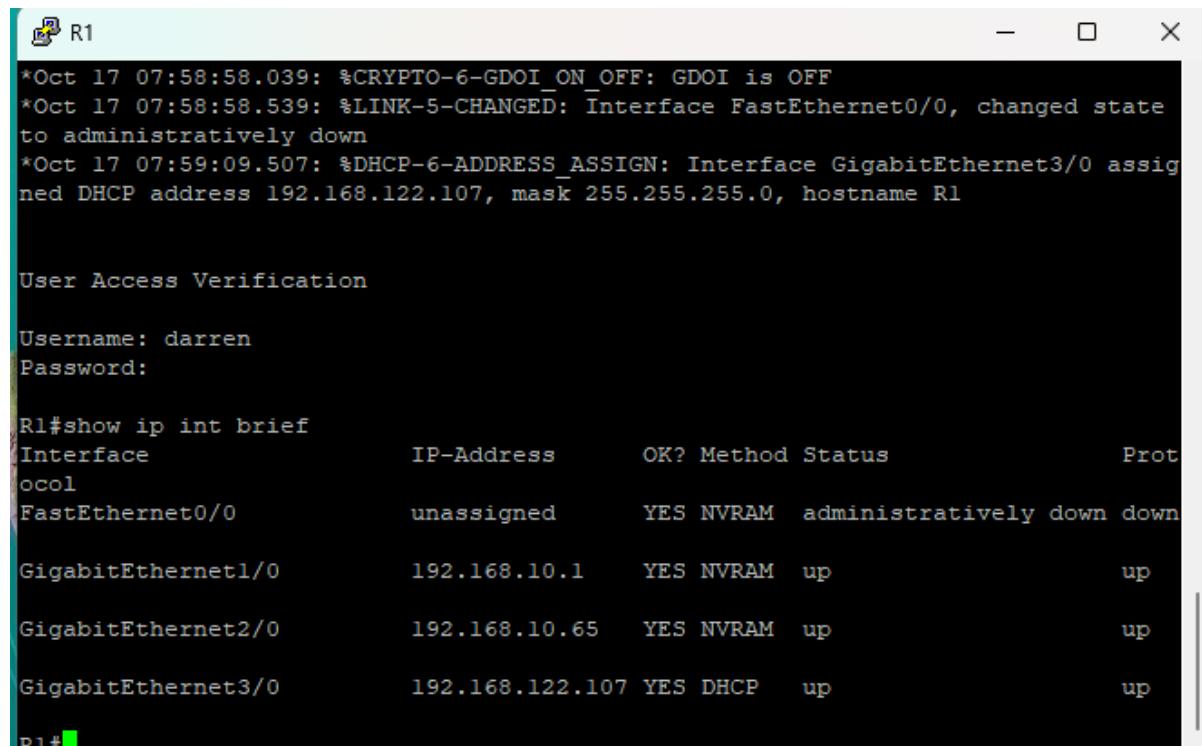


**Figure 73: Code QR de User Darren**

## 4. Routeur

Une fois l'Appliance TOTPRadius configurée, Nous allons configurer le Routeur.

Configurer les adresses des interfaces du routeur



```
R1
*Oct 17 07:58:58.039: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Oct 17 07:58:58.539: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Oct 17 07:59:09.507: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet3/0 assigned DHCP address 192.168.122.107, mask 255.255.255.0, hostname R1

User Access Verification

Username: darren
Password:

R1#show ip int brief
Interface          IP-Address      OK? Method Status      Prot
octl
FastEthernet0/0    unassigned      YES NVRAM  administratively down down
GigabitEthernet1/0  192.168.10.1   YES NVRAM  up          up
GigabitEthernet2/0  192.168.10.65  YES NVRAM  up          up
GigabitEthernet3/0  192.168.122.107 YES DHCP   up          up

R1#
```

**Figure 74: IP des interfaces du routeur**

Pour utiliser TOTPRadius comme serveur Radius. Les commutateurs Cisco ont des fonctionnalités médiocres dans l'interface Web, c'est pourquoi nous utilisons le Shell de commande pour définir les paramètres :

- **aaa new-model** : Cette commande active simplement aaa sur votre routeur et rien de plus.
- **aaa authentication login default group radius** Exec Access utilisant Radius.
- **radius-server host 192.168.10.17 auth-port 1812 key afec123**

```

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#aaa authentication login default group radius
R1(config)#$er host 192.168.10.17 auth-port 1812 acct-port 1813 key afec123
  Warning: The CLI will be deprecated soon
  'radius-server host 192.168.10.17 auth-port 1812 acct-port 1813 key afec123'
  Please move to 'radius server <name>' CLI.
R1(config)#$er host 192.168.10.17 auth-port 1812 acct-port 1813 key afec123
R1(config)#do wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R1(config)#end
R1#
*Oct 17 08:11:27.303: %SYS-5-CONFIG_I: Configured from console by console
R1#

```

**Figure 75: Configuration de l'authentification sur le routeur**

Vous pouvez utiliser la commande **do show running-config** pour vous assurer que les nouveaux paramètres sont ajoutés à la configuration.

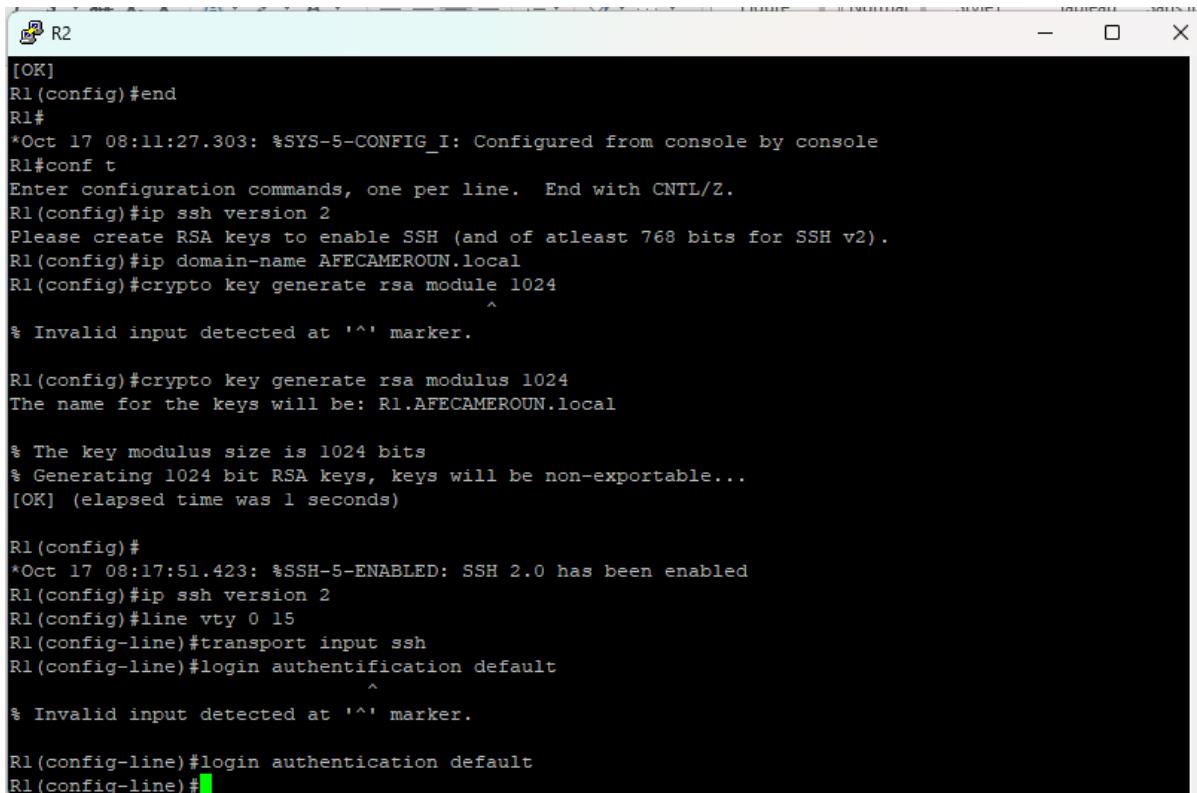
Les paramètres suivants sont nécessaires pour activer ssh. Vous pouvez sauter si vous les avez déjà.

- hostname Router1
- ip domain-name AFECAMEROUN.local (Définir un nom de domaine, qui sera utilisé pour générer la clé de chiffrement)
- crypto key generate rsa modulus 1024 (Cette commande génère une clé de chiffrement)

RSA utilisé par le processus SSH pour générer la clé de session. La variable “modulus 1024” définit la taille de votre clé. A titre d’information, pour une clé asymétrique, 1024 est une taille correcte)

- ip ssh version 2 (active le ssh)
- line vty 0 15 (Pour cela, on définit les lignes virtuelles appelées “vty”. Par défaut, il y a 5 lignes vty actives (de 0 à 4). D'où la commande “line vty 0 4“)
- transport input ssh (définit quel protocole a le droit d'utiliser ces lignes vty)

- login authentication default (permet de préciser où se trouve la base des comptes utilisateur)



```
R2
[OK]
R1(config)#end
R1#
*Oct 17 08:11:27.303: %SYS-5-CONFIG_I: Configured from console by console
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
R1(config)#ip domain-name AFECAMEROUN.local
R1(config)#crypto key generate rsa modulus 1024
^
% Invalid input detected at '^' marker.

R1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R1.AFECAMEROUN.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

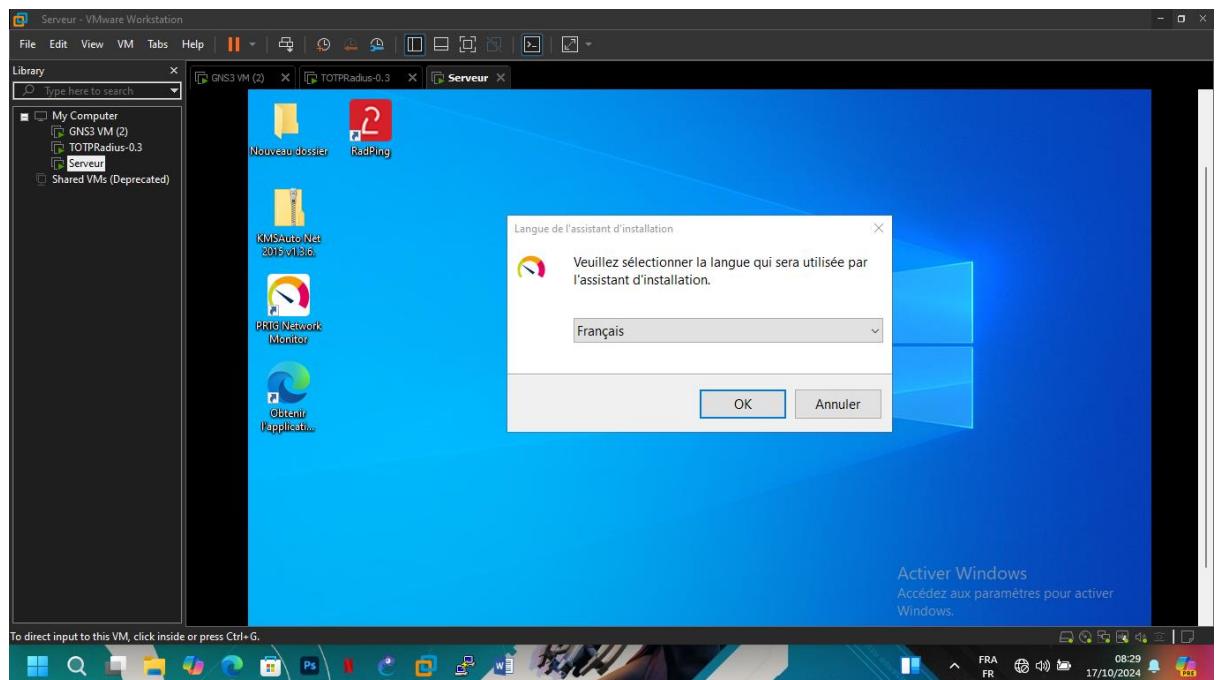
R1(config)#
*Oct 17 08:17:51.423: %SSH-5-ENABLED: SSH 2.0 has been enabled
R1(config)#ip ssh version 2
R1(config)#line vty 0 15
R1(config-line)#transport input ssh
R1(config-line)#login authentication default
^
% Invalid input detected at '^' marker.

R1(config-line)#login authentication default
R1(config-line)#[
```

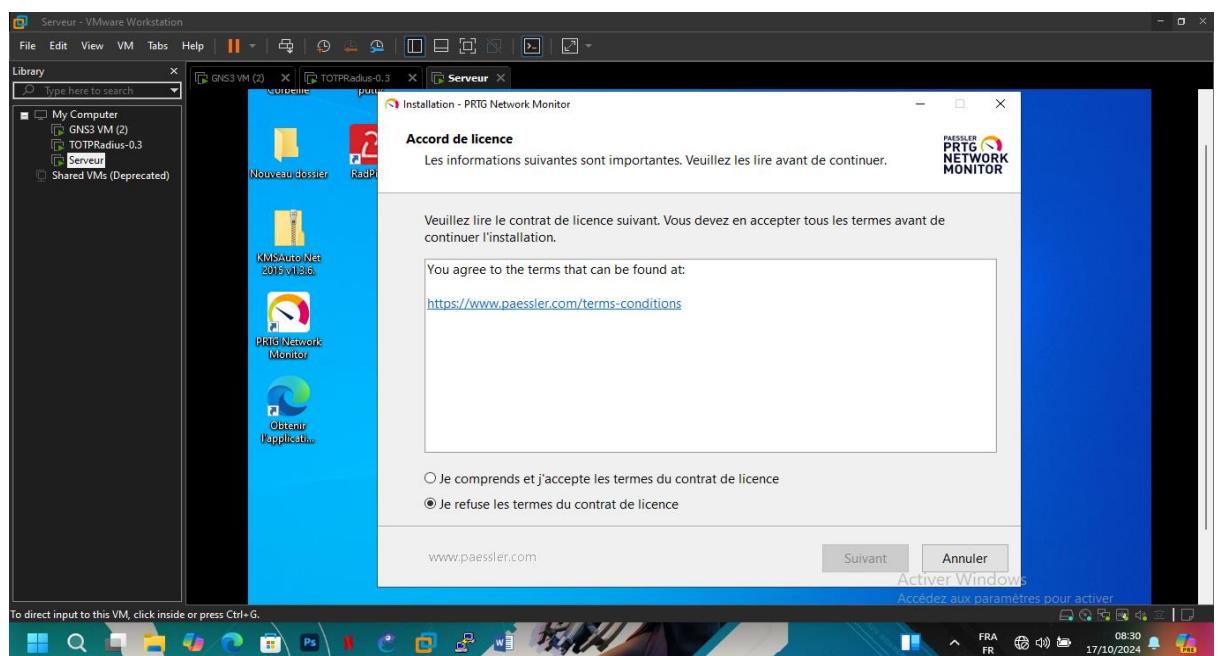
**Figure 76: Configuration ssh**

## V. CONFIGURATION DE LA SUPERVISION PRTG SUR LE SERVEUR WINDOWS

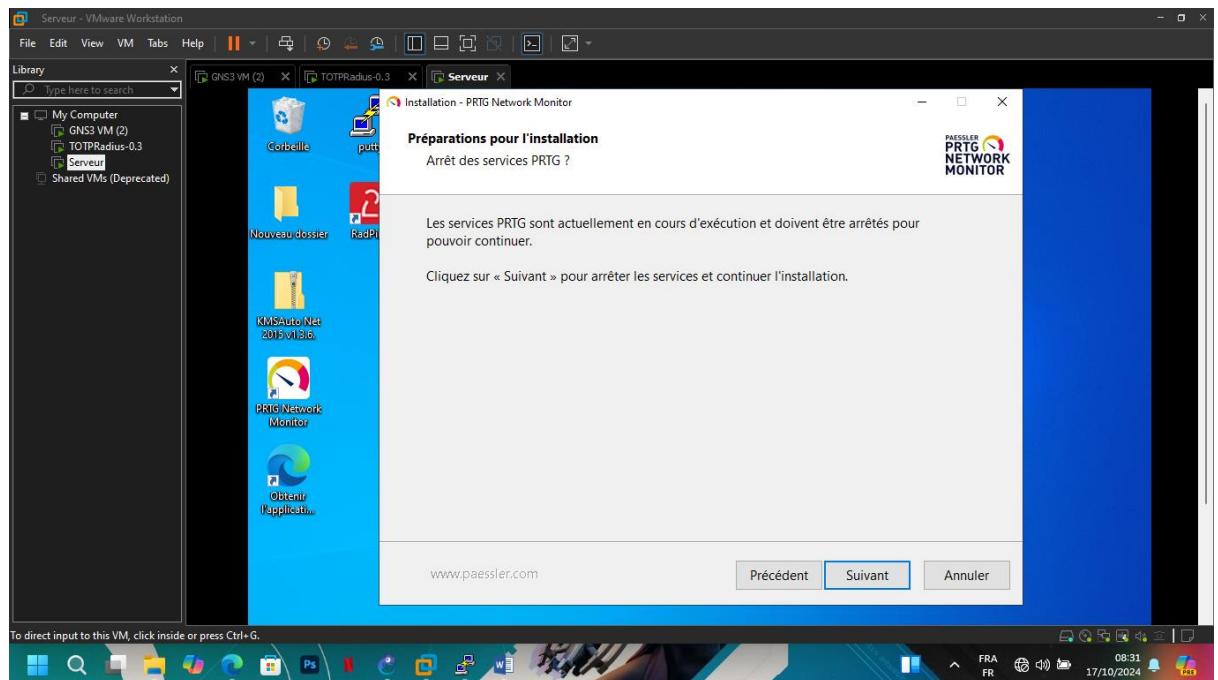
Pour configurer la supervision PRTG, nous devons juste installer PRTG et y Ajouter des équipements



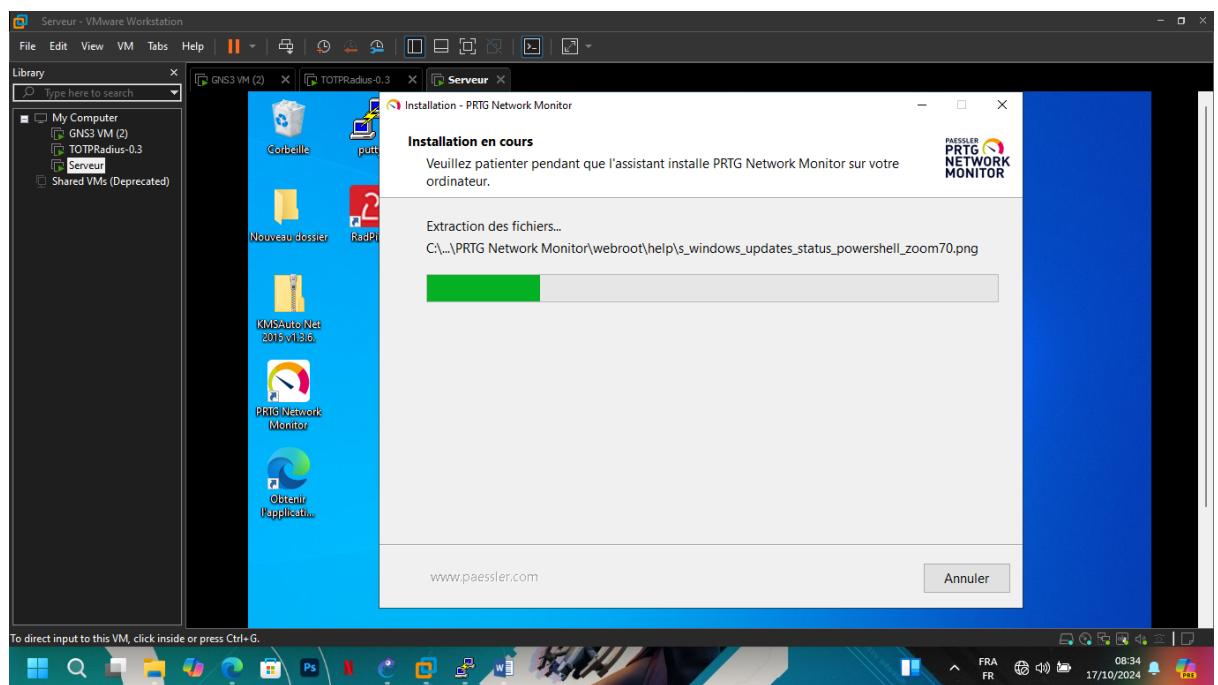
**Figure 77: Choix de la langue lors de l'installation de PRTG**



**Figure 78: Lire le contrat et appuyer sur je comprends et j'accepte**



**Figure 79: Cliquez sur suivant**



**Figure 80: Patienter l'installation**

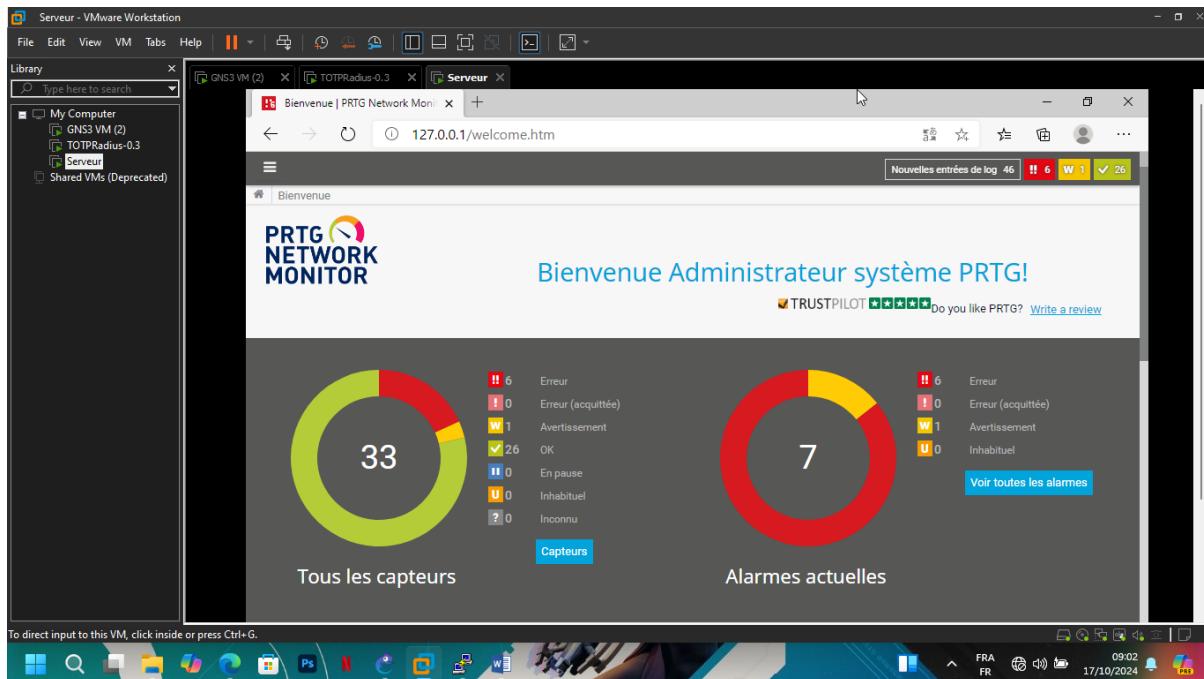
**NB:** Dans d'autre cas on vous demandera d'abord d'insérer votre adresse mail avant de démarrer installation

## VI. Test de Fonctionnalités

### a) Testons les fonctionnalités de notre Supervision PRTG

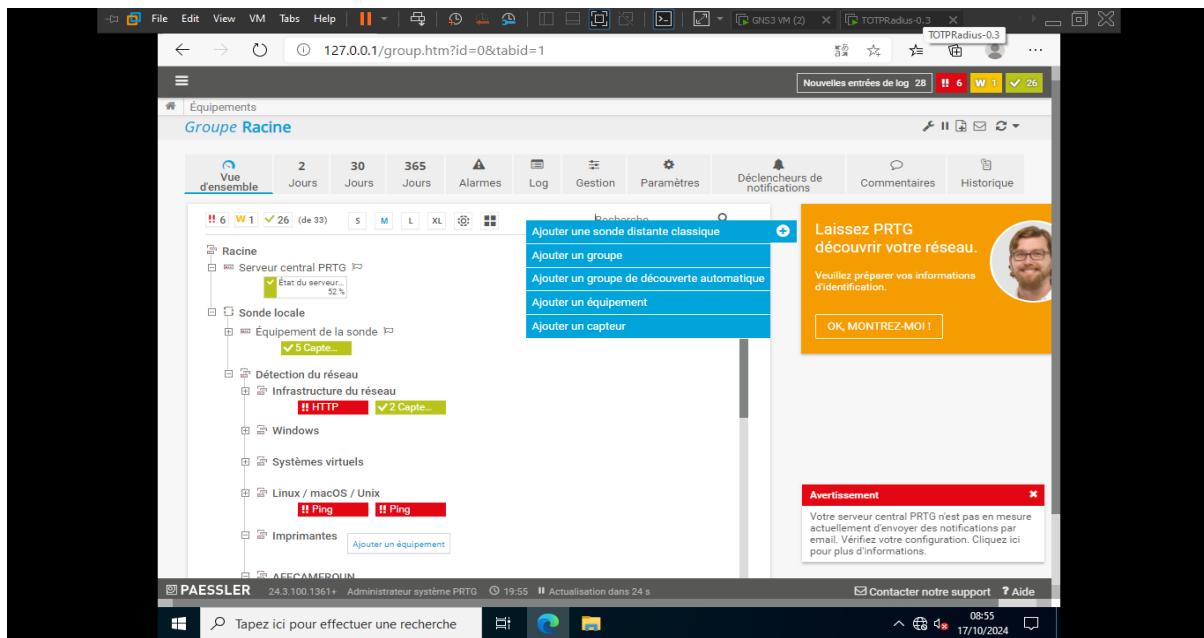
Lorsque vous lancez PRTG et que vous entrez votre nom par défaut **prtgadmin** et votre mot de passe **prtgadmin**. Vous serez dirigé vers la page d'accueil

**Nb:** il est recommandé de modifier le mot de passe

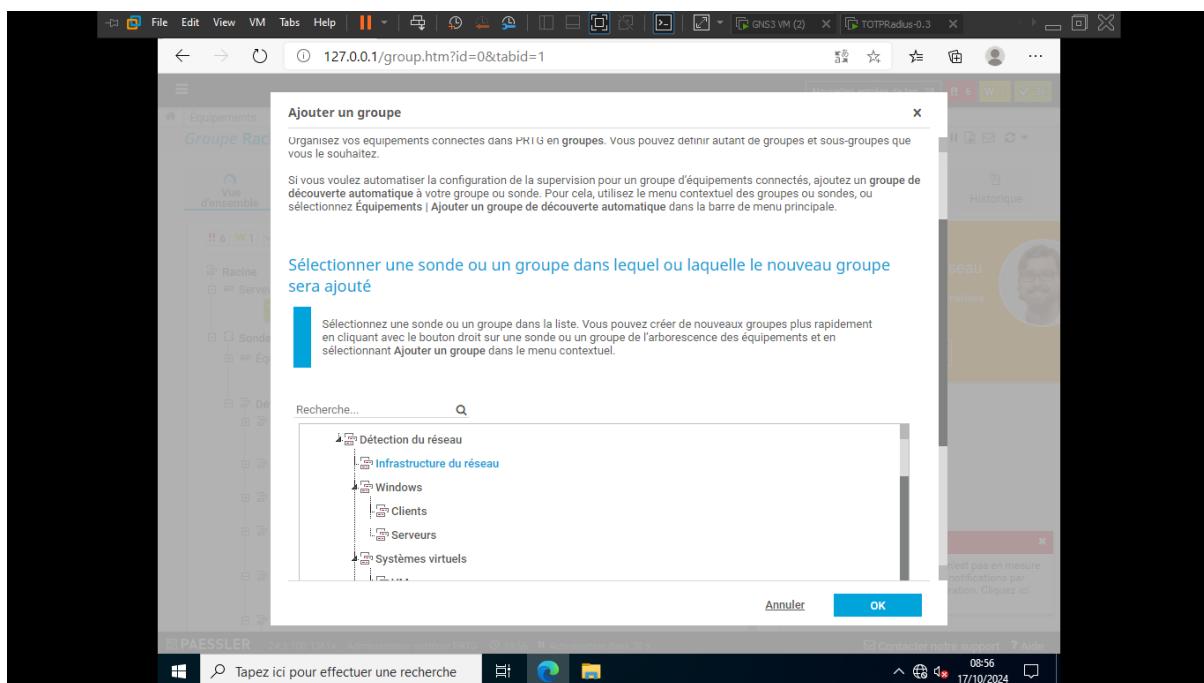


**Figure 81: Page d'accueil PRTG**

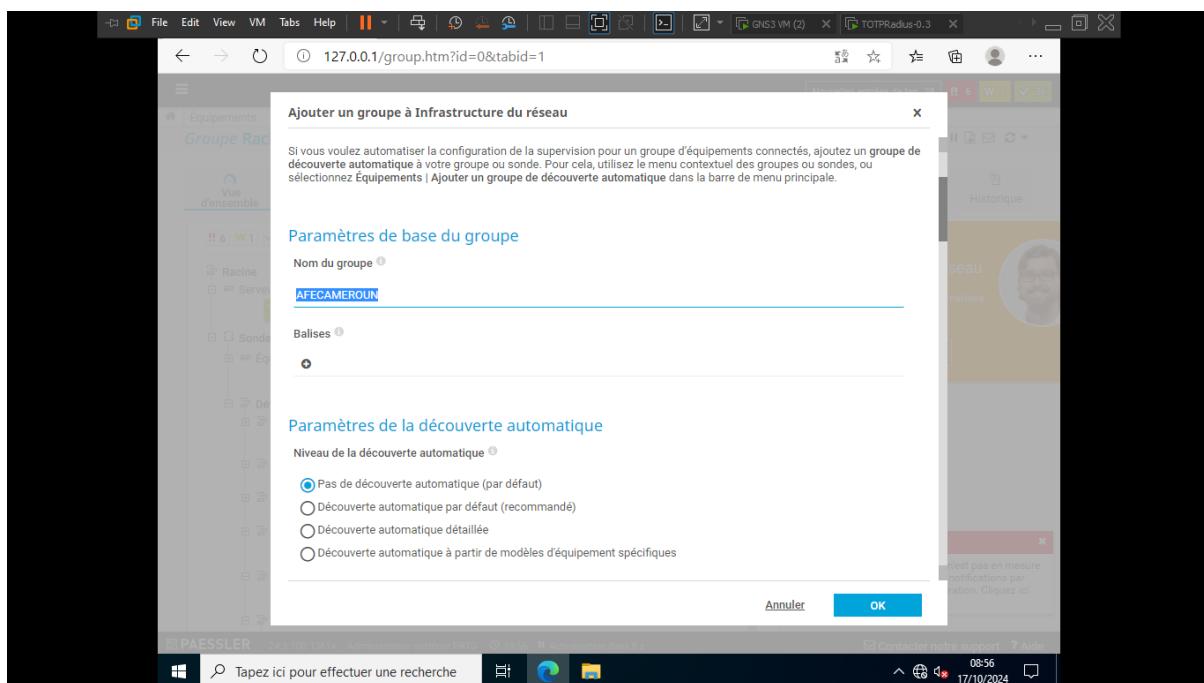
Ensuite allez sur équipement et cliquer sur icone Blue + et choisissez ajouter un groupe



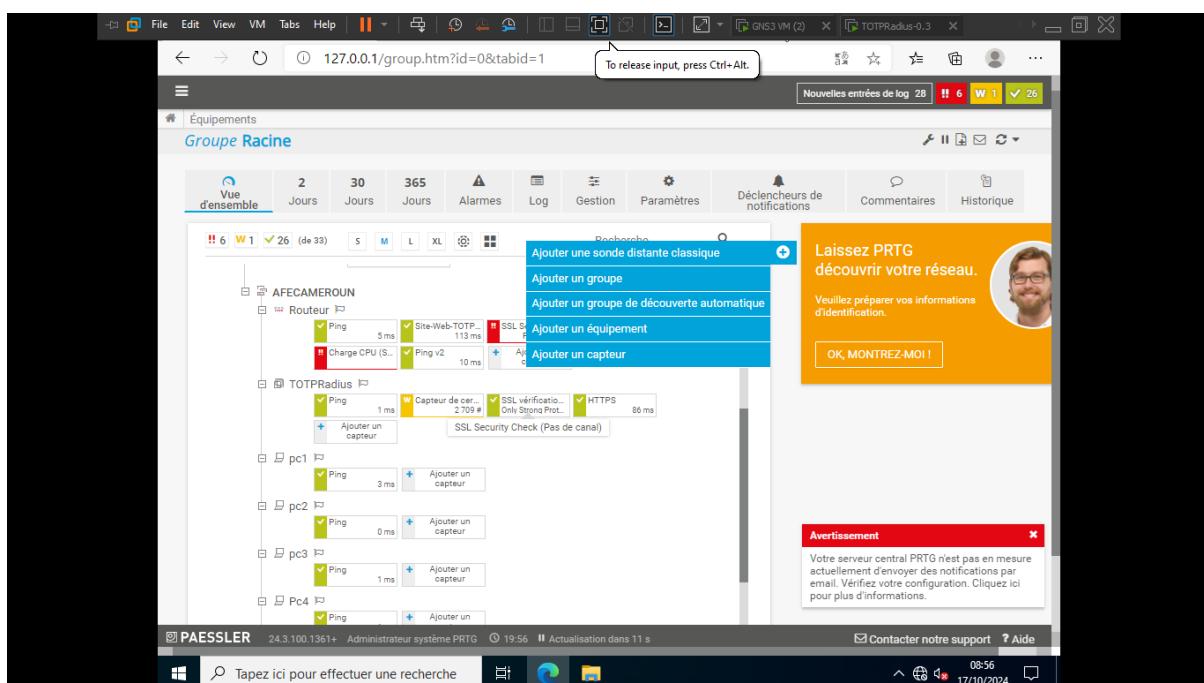
**Figure 82: Cliquer sur ajouter un groupe**



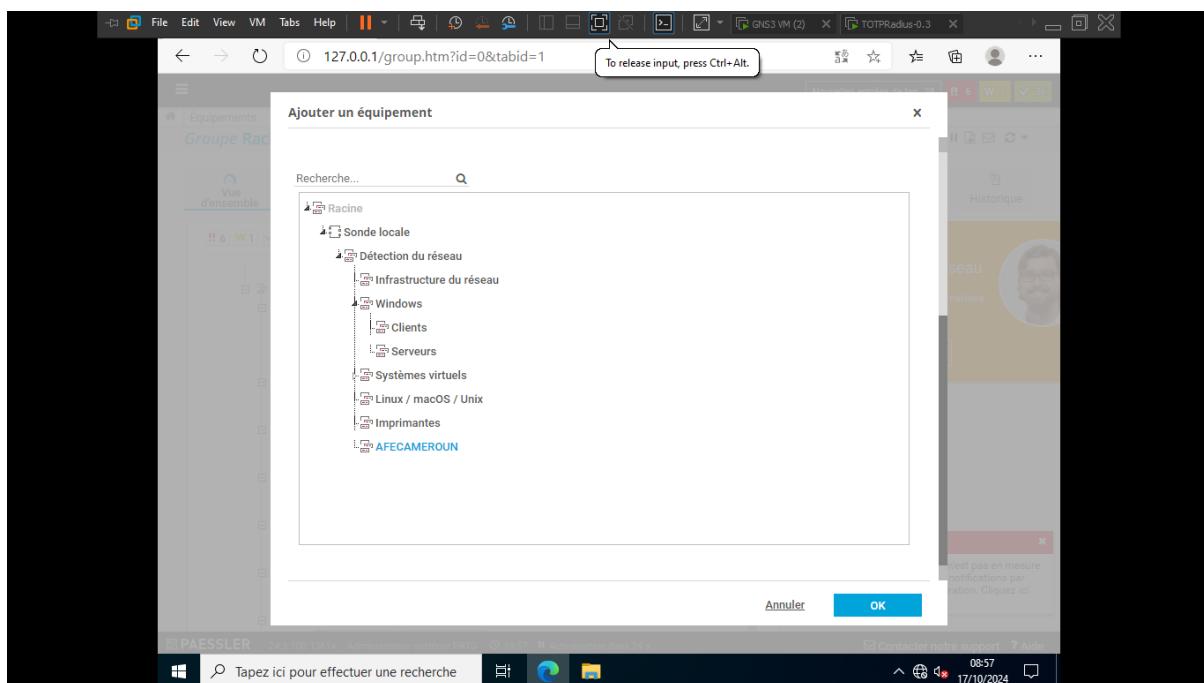
**Figure 83: Cliquer sur Infrastructure reseau et puis sur ok**



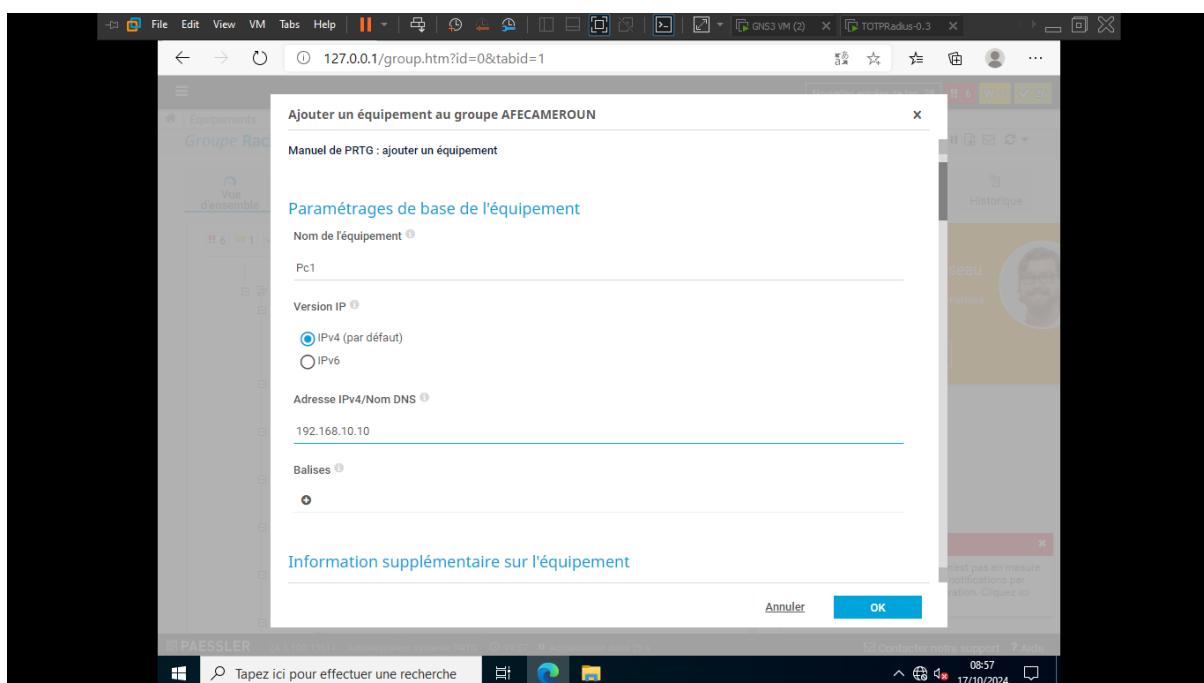
**Figure 84: Entrer Nom du groupe**



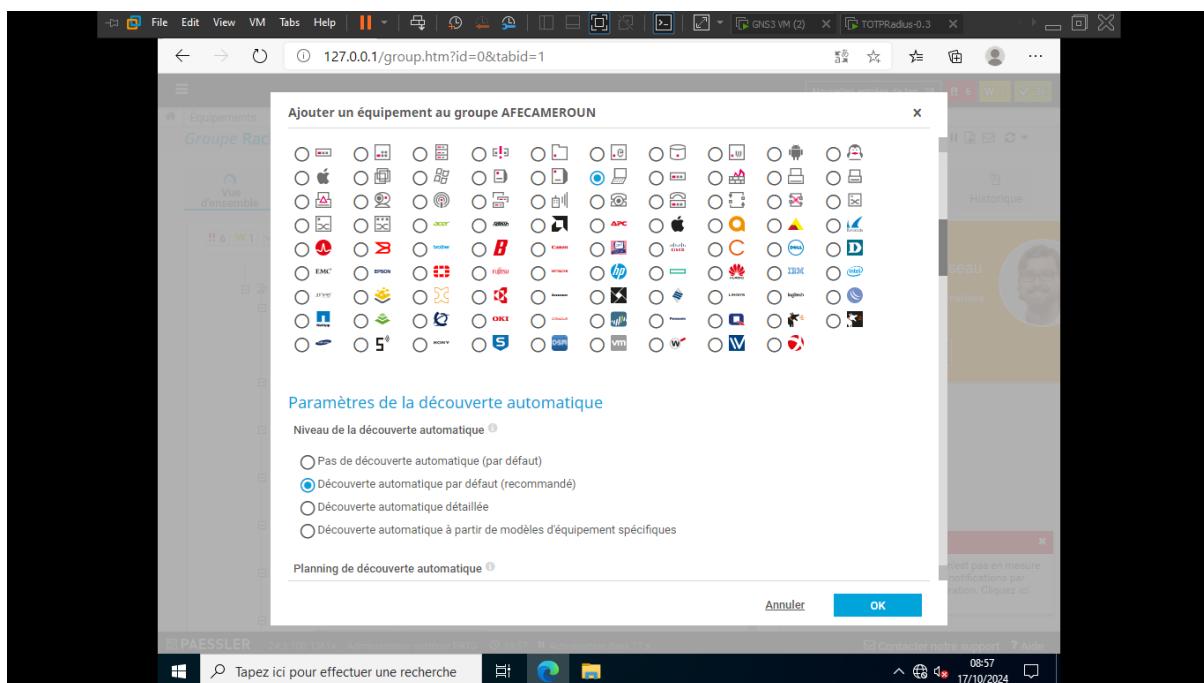
**Figure 85: Cliquer sur Equipement**



**Figure 86: Cliquer sur Votre Groupe**

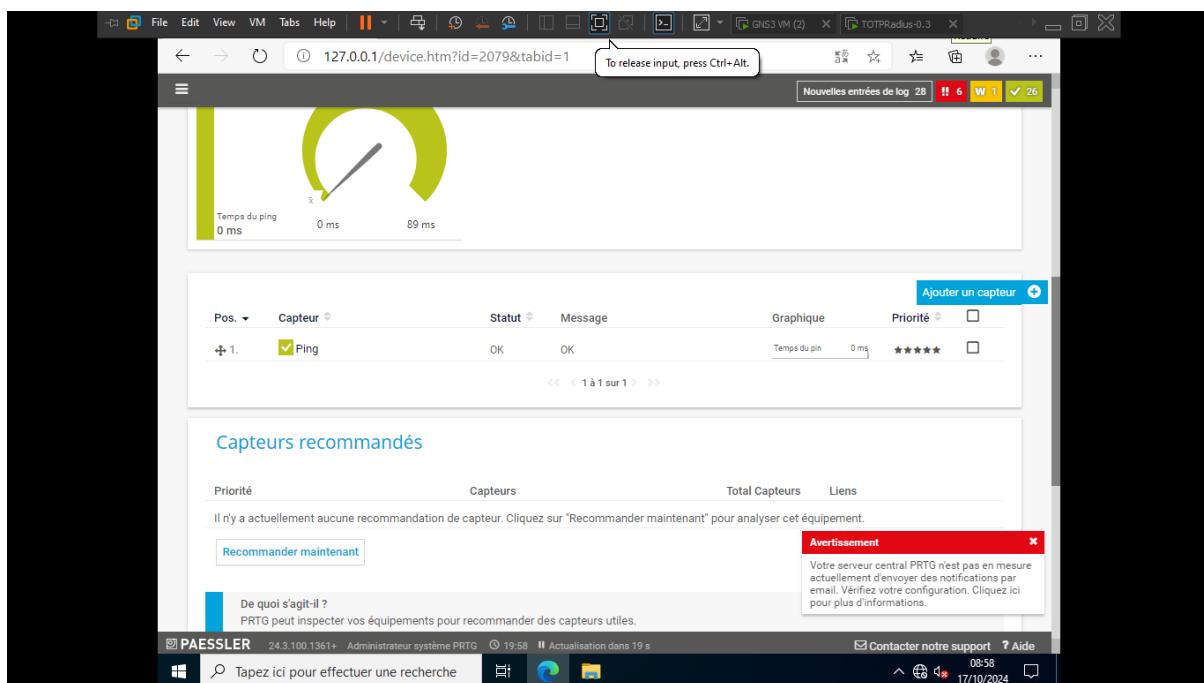


**Figure 87: Entrer le nom de l'équipement et son adresse IP**

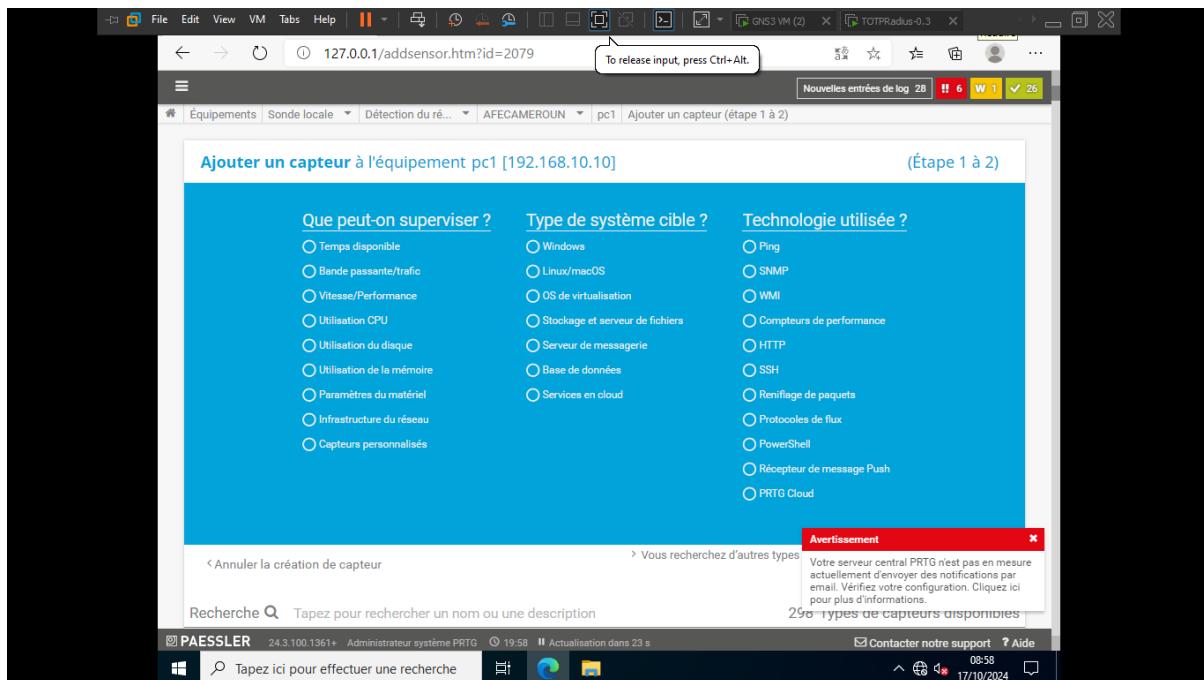


**Figure 88: Choisir le logo de l'équipement et cochez la découverte automatique**

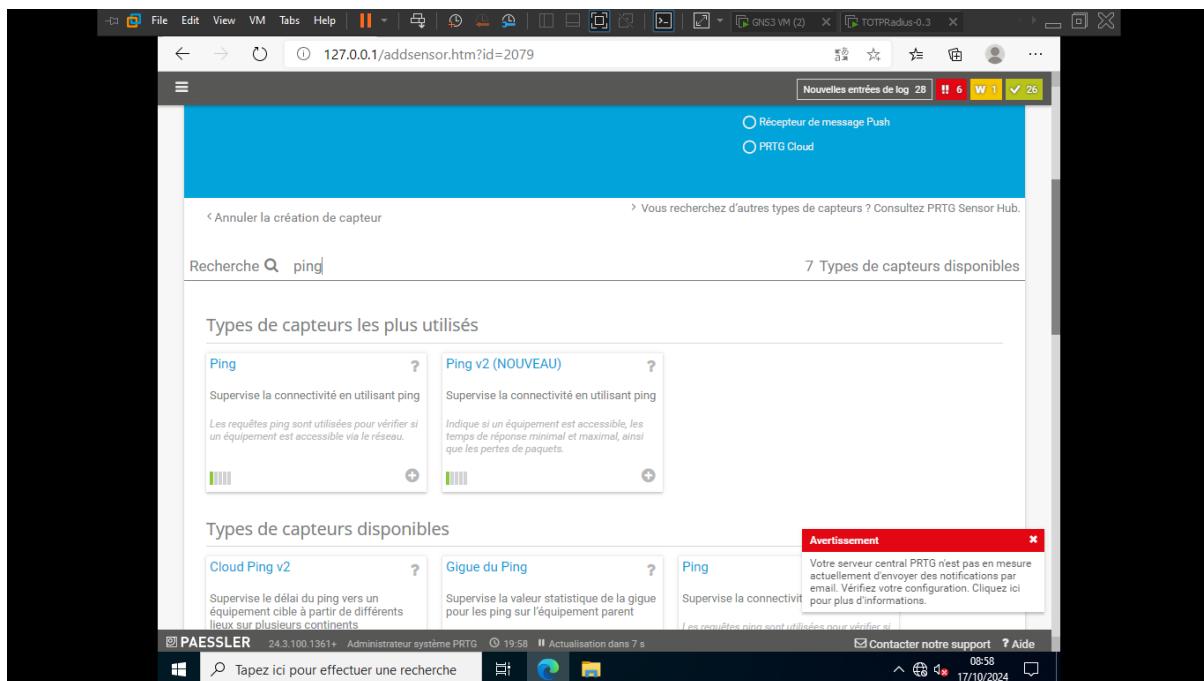
Faites tout le processus sur tous vos équipements



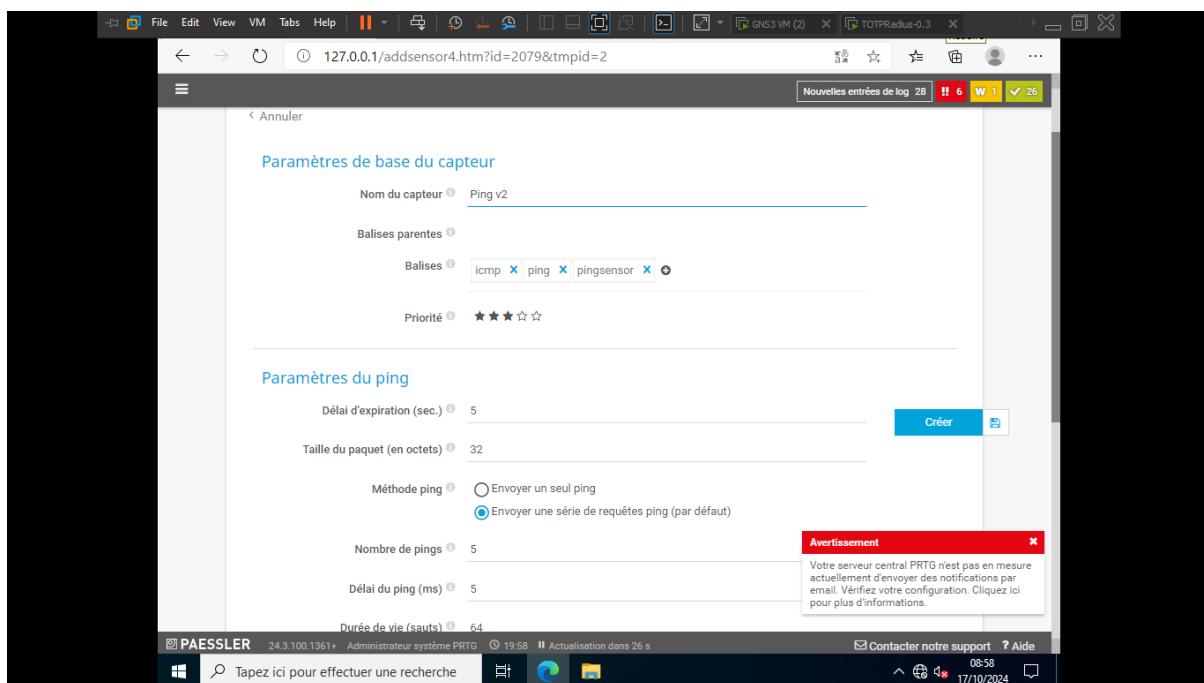
**Figure 89: Cliquer sur Equipement et cliquer sur ajouter un capteur**



**Figure 90: Choisissez le type de capteur que vous souhaitez superviser**

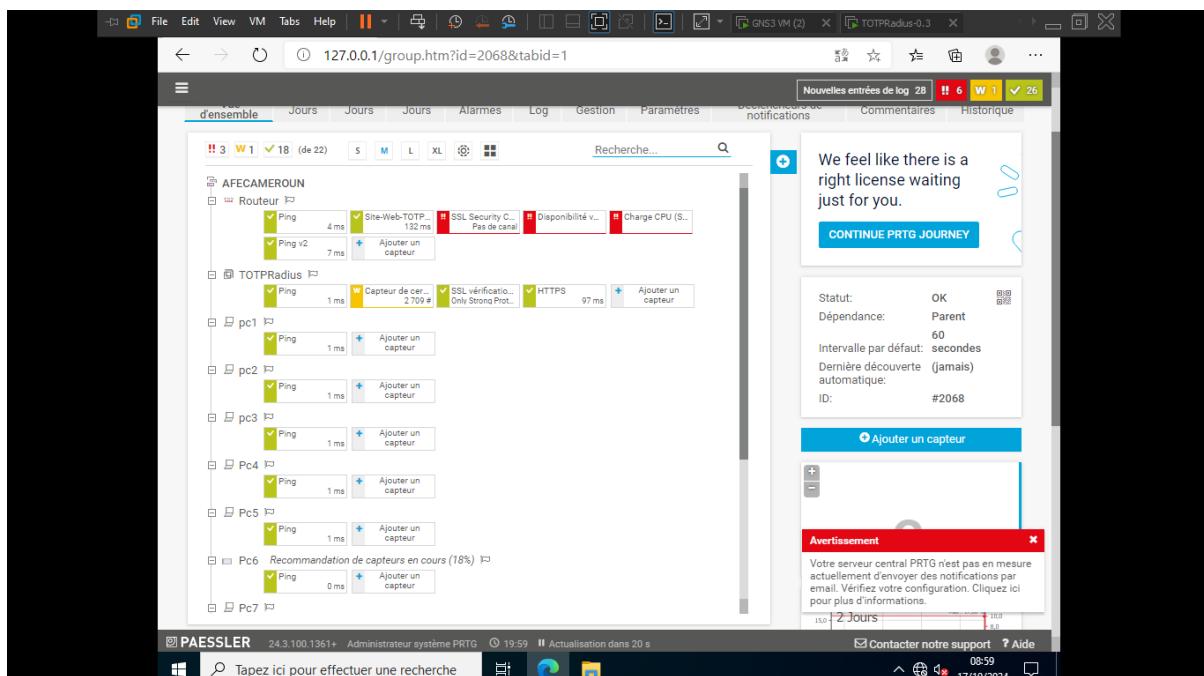


**Figure 91: Choix du capteurs des Ping**



**Figure 92: Configurer les parametre selon vous et cliquez sur Cr閐er**

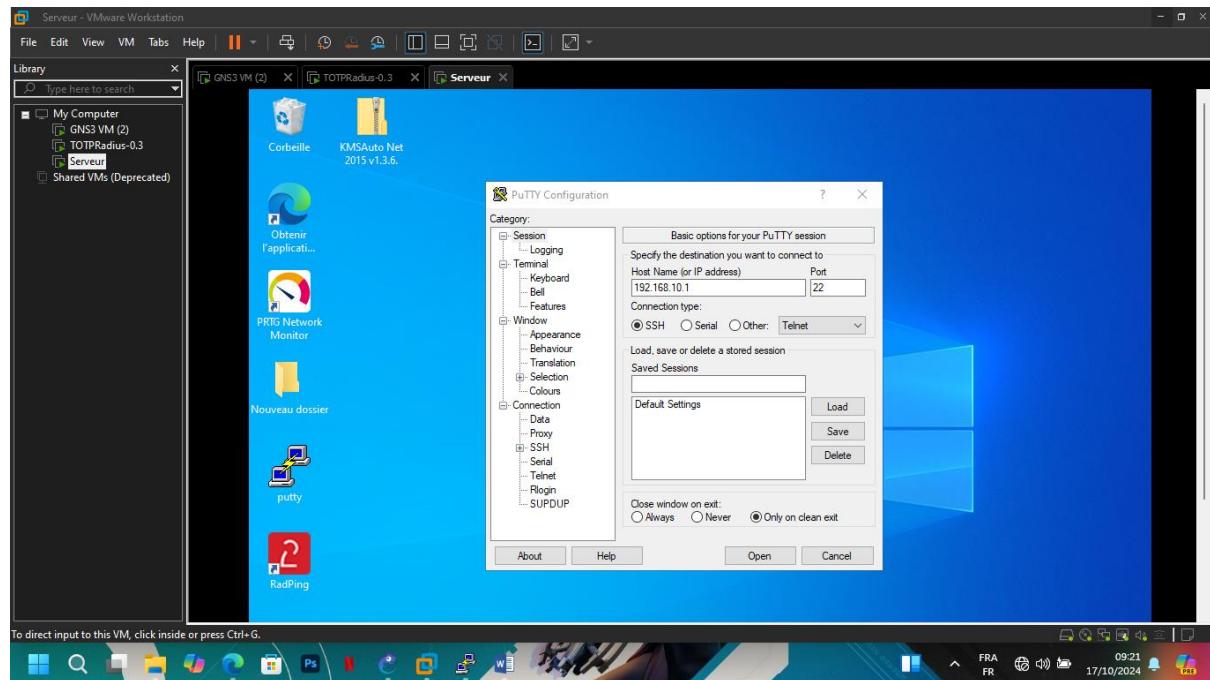
Une fois que vous avez ajouté tout équipement et vos capteurs, votre réseau sera supervisé en temps réel



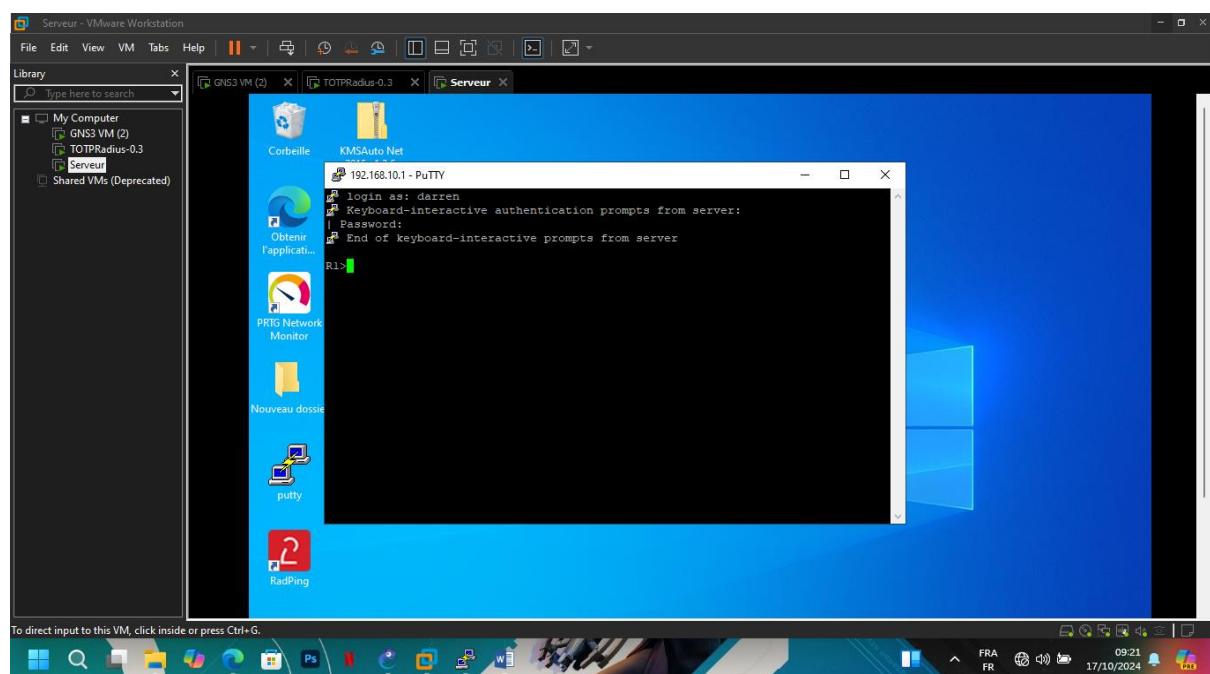
**Figure 93: Capture de mes equipements et leur Capteur**

### a) Testons la double authentification sur le routeur

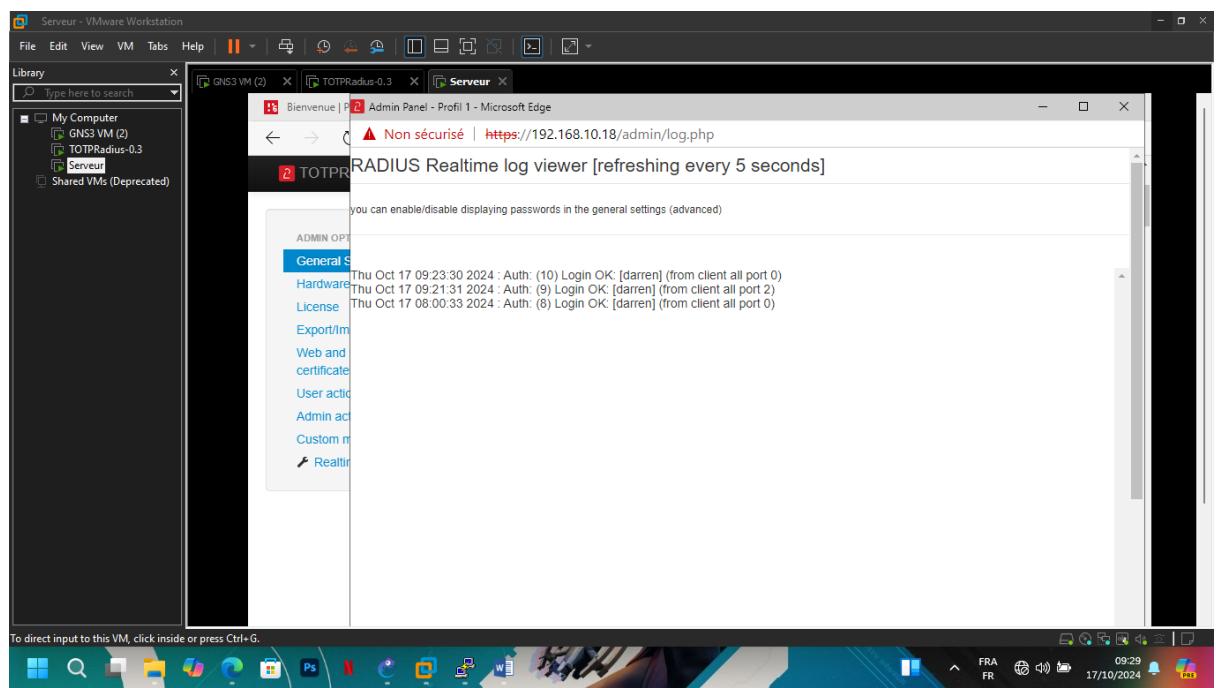
Nous testons l'authentification sur le Routeur en utilisant le mot de passe AD et l'OTP à 6 chiffres généré par le jeton matériel à l'aide de PuTTY ou d'une autre application cliente ssh :



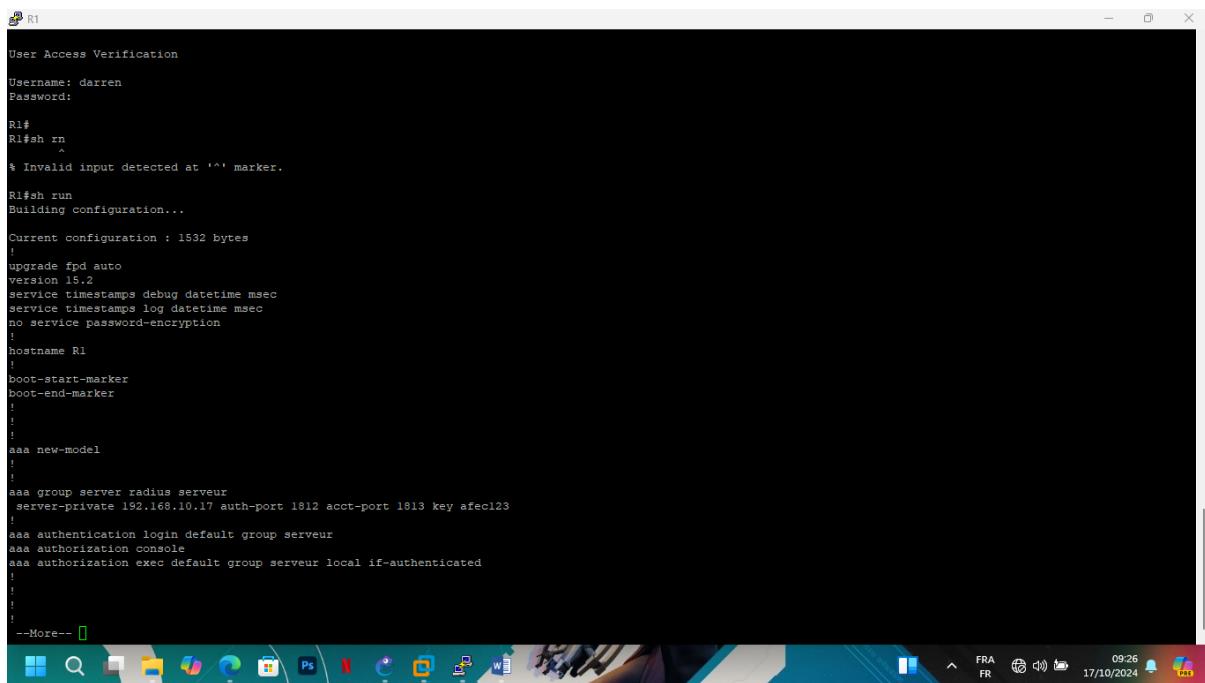
**Figure 94: Test d'authentification sur le routeur via PuTTY**



**Figure 95: Interface du routeur via PuTTY**



**Figure 96: Log du serveur TOTPRadius**



```

User Access Verification
Username: darren
Password:

R1# 
R1#sh rn
^
% Invalid input detected at '^' marker.

R1#sh run
Building configuration...

Current configuration : 1532 bytes
!
upgrade ffd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!

aaa new-model
!
aaa group server radius serveur
    server-private 192.168.10.17 auth-port 1812 acct-port 1813 key afec123
!
aaa authentication login default group serveur
aaa authorization console
aaa authorization exec default group serveur local if-authenticated
!
!
!--More-- 

```

**Figure 97: Configuration du routeur**

## CONCLUSION GENERAL

En conclusion, il nous était question de présenter le thème de Mise en place d'un système de sécurité (Double authentification avec Radius) réseau avec supervision PRTG : cas de AFECAMEROUN. Ce thème nous a permis de mener une étude sur la communication au sein DE AFECAMEROUN, enfin de proposer des améliorations. Ceci permettra à AFECAMEROUN de sécurisé d'avantage leur système, en utilisant une double authentification sur leur équipements réseaux (Routeur) ET DE superviser en temps réel leur réseaux. Il est noté qu'à l'heure actuelle, ce travail n'a été effectuer qu'a quatre-vingt pourcent (80%). Ainsi ce travail nous permis de mettre en place nos différents cours portant sur le réseau informatique et de mieux se familiariser au milieu d'administrateur réseau. La perfection n'étant pas du ressort des humains, toutes remarques et suggestions des potentiels lecteurs seront les bienvenues pour l'amélioration de ce travail

ANNEXES



## BIBLIOGRAPHIE

1. Cours de rédaction scientifique : IAI Cameroun, année académique 2021-2022
2. MFA-Législative-Report : Directeur de l'information de l'État, Département des technologies de l'information, décembre 2015
3. L'authentication : état des lieux et outil de décision, Université de Namur, Faculté d'informatique, Année académique 2015-2016
4. : sécurité, stratégie d'entreprise et panorama du marché
5. *De Guillaume Plouin*
6. : Microsoft évolution ou révolution, Mémoire de recherche, M2IRT 2009  
*Nicolas Grevet*
7. : système d'administration autonome adaptable : application au microsoft,  
*NKOUAYA*,
8. : étude et mise en place d'une solution de messagerie, école national supérieur des postes et des télécommunications, 2021. *Landry Fossouo Noumsi* 10.  
: Cloud-publique-Cloud-et-hybridCloud. *My saas*. Private-
11. : Amazon, Définition et impact pour les SSII, 2012.
12. : « server and Technologies and Strategies of the Ubiquitous Data Center »,  
CRC
13. Press – 2010 *Brian J.S. Chee - Curtis Franklin Jr.*,

## WEBOGRAPHIE

- <https://www.token2.com/site/page/totpradius-mfa-for-ssh-access-to-ciscoswitches>, Ce lien nous a permis d'en savoir plus sur totpradius et de sa configuration
- <https://www.ezeelogin.com/kb/article/how-to-install-google-authenticator-oncentosubuntu-323.html>, Ce lien nous a permis d'implémenter google Authenticator
- <https://reussirsonccna.fr/configuration-du-ssh-sur-ios/>, Ce lien nous a permis de configurer l'acess par ssh sur un routeur
- <https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-accesscontrolleraccess-control-system-tacacs-/10384-security.html>, Ce lien nous a permis de configurer et d'en savoir plus sur l'authentification sur un routeur
- [https://en.wikipedia.org/wiki/Multi-factor\\_authentication](https://en.wikipedia.org/wiki/Multi-factor_authentication), Ce lien nous a permis de savoir ce que sais l'authentification multifacteur.
- [http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing\\_WP.pdf](http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf) strategie de deployment d'un serveur le 27/07/2023 à 13am
- [resultat sur un rapport de stage - Recherche \(bing.com\)](#) éléments constitutifs d'une architecture , le 10/08/2023 à 8 Pm ;
- [www.bing.com/search?q=opennebula](http://www.bing.com/search?q=opennebula): objectif à atteindre dans exchange, 10/08/2023 à 20h30 ;
- [www.bing.com/search?q=cloud/cloud.prive](http://www.bing.com/search?q=cloud/cloud.prive) : recherche sur les différentes modelés de messagerie, le 15/08/2023 à 14h20 ;
- [https://www.bing.com/search?q=opennebula&cvid.securiteducloud](http://www.bing.com/search?q=opennebula&cvid.securiteducloud) : recherche sur l'administration d'un serveur sur postfix, le 20/08/2023 à 22h30
- [https://www.bing.com/search?q=notion/virtualisation/hyper+de+surface&cvid](http://www.bing.com/search?q=notion/virtualisation/hyper+de+surface&cvid) recherche sur la virtualisation, le 20/08/2023 à 23h13  
<http://www.vmware.com/fr/Cloud-Computing/> recherché sur les services cloud le 24/08/2023 à 12h55  
<http://www.computerland.fr/Cloud-Computing/office-365-solutionCloudComputingselon-microsoft/> possibilité de création d'un cloud Windows, le 24/08/2024 à 12h55 ;



## GLOSSAIRE

- **AFEC Cameroun** : Audit Formation Évaluation Conseil, une entreprise spécialisée dans la formation et le conseil en informatique.
- **Authentification** : Processus de vérification de l'identité d'un utilisateur ou d'un système.
- **Double Authentification (2FA)** : Méthode de sécurité qui nécessite deux formes d'identification avant d'accorder l'accès à un système.
- **RADIUS (Remote Authentication Dial-In User Service)** : Protocole de réseau qui fournit des services d'authentification, d'autorisation et de comptabilité pour les utilisateurs accédant à un réseau.
- **PRTG (Paessler Router Traffic Grapher)** : Outil de surveillance de réseau qui permet de surveiller l'état et la performance des infrastructures réseau.
- **Supervision** : Processus de surveillance des systèmes et réseaux pour assurer leur bon fonctionnement et détecter les anomalies.
- **Sécurité Réseau** : Ensemble des mesures prises pour protéger les réseaux informatiques contre les intrusions, les attaques et les accès non autorisés.
- **Attaque directe** : Type d'attaque où l'attaquant cible directement un système ou un réseau sans intermédiaire.
- **ARP Spoofing** : Technique utilisée par des attaquants pour rediriger le trafic sur un réseau local en envoyant des messages ARP falsifiés.
- **Proxy** : Serveur intermédiaire qui agit comme un pont entre un utilisateur et Internet, permettant l'anonymat et le filtrage du contenu.
- **LDAP (Lightweight Directory Access Protocol)** : Protocole utilisé pour interroger et modifier des services d'annuaire.
- **OAuth2** : Protocole d'autorisation qui permet à une application tierce d'accéder aux ressources d'un utilisateur sans partager ses identifiants.

## TABLE DE MATIERES

<b>DEDICACE .....</b>	<b>1</b>
<b>REMERCIEMENTS .....</b>	<b>2</b>
<b>SOMMAIRE.....</b>	<b>3</b>
<b>LISTE DES FIGURES .....</b>	<b>5</b>
<b>LISTES DE TABLEAUX.....</b>	<b>10</b>
<b>RESUMÉ .....</b>	<b>11</b>
<b>ABSTRAT .....</b>	<b>12</b>
<b>INTRODUCTION.....</b>	<b>13</b>
<b>PREMIERE PARTIE :</b>	<b>14</b>
<b>DOSSIER D'INSERTION .....</b>	<b>14</b>
<b>INTRODUCTION.....</b>	<b>15</b>
<b>I- ACCUEIL AU SEIN D'AFEC CAMEROUN .....</b>	<b>16</b>
<b>II- PRESENTATION DE LA STRUCTURE .....</b>	<b>16</b>
<i>Figure 1: Organigramme d'AFEC CAMEROUN .....</i>	<i>20</i>
<i>Figure 2: plan de localisation AFEC (Source : Entreprise) .....</i>	<i>20</i>
<b>CONCLUSION.....</b>	<b>23</b>
<b>DEUXIEME PARTIE :</b>	<b>24</b>
<b>PHASE TECHNIQUE.....</b>	<b>24</b>
<b>CHAPITRE 1 :</b>	<b>26</b>
<b>ANALYSE DU PROJET .....</b>	<b>26</b>
1. ARCHITECTURE DE AFECAMEROUN .....	28
<i>Figure 3: Topologie actuel de afec .....</i>	<i>28</i>
2. DESCRIPTION DE L'ARCHITECTURE .....	28
<b>CHAPITRE 2:</b>	<b>31</b>
<b>CAHIER DE CHARGES .....</b>	<b>31</b>
<b>I. CONTEXTE DU PROJET .....</b>	<b>32</b>
<b>II. OBJECTIFS DU PROJET.....</b>	<b>32</b>
<b>III. EXPRESSION DES BESOINS DE L'UTILISATEUR.....</b>	<b>33</b>
1 <i>LES BESOINS FONCTIONNELS .....</i>	<i>33</i>
2 <i>LES BESOINS NON FONCTIONNELS .....</i>	<i>34</i>

<b>VI. ESTIMATION DU COÛT DU PROJET.....</b>	<b>34</b>
1) LES RESSOURCES HUMAINES .....	34
2) RESSOURCES LOGICIELLES .....	35
3) RESSOURCES MATÉRIELLES.....	35
4) COÛT TOTAL DU PROJET .....	37
<b>V. PLANNIFICATION PROJET .....</b>	<b>37</b>
<i>Figure 4: Diagramme de Gantt .....</i>	38
<b>VI. LES CONTRAINTES DU PROJET .....</b>	<b>39</b>
1) LES CONTRAINTES DE COUT.....	39
2) LES CONTRAINTES DE DELAI.....	39
3) LES CONTRAINTES DE QUALITE .....	39
<b>VII. LES LIVRABLES.....</b>	<b>39</b>
<b>CHAPITRE 3 :.....</b>	<b>40</b>
<b>ETAT DE L'ART .....</b>	<b>40</b>
<b>I. INTRODUCTION SUR LA SECURITE RESEAU .....</b>	<b>41</b>
<b>A. DEFINITION ET OBJECTIFS .....</b>	<b>41</b>
1. DÉFINITION DE LA SÉCURITÉ INFORMATIQUE.....	41
2. LES OBJECTIFS DE LA SECURITÉ INFORMATIQUE .....	41
<b>B. LA POLITIQUE DE SÉCURITÉ.....</b>	<b>41</b>
1. LES OBJECTIFS D'UNE POLITIQUE DE SÉCURITÉ.....	42
<b>C. LES CLASSIFICATIONS D'ATTAQUES .....</b>	<b>43</b>
1. TYPES D'ATTAQUES .....	43
a) <i>Les attaques directes .....</i>	43
<i>Figure 5: Attaque directe. (Source : google image) .....</i>	44
b) <i>Les attaques indirectes par rebond.....</i>	44
<i>Figure 6: Attaque par rebond (source : google image).....</i>	44
c) <i>Les attaques indirectes par réponse .....</i>	44
<i>Figure 7: Attaque indirecte par réponse (source : google image).....</i>	45
2. ATTAQUES SUR LES RÉSEAUX.....	45
a) <i>Attaque par usurpation d'adresse IP (IP spoofing) .....</i>	45
<i>Figure 8: Attaque par adresse IP (source : google image) .....</i>	45
b) <i>Attaque par usurpation d'adresse MAC (MAC spoofing) .....</i>	45
<i>Figure 9: Attaque par adresse MAC (source : google image).....</i>	46
c) <i>ARP spoofing .....</i>	46
<i>Figure 10: ARP Spoofing (source: google image).....</i>	46
d) <i>Attaque de mot de passe .....</i>	47
e) <i>Les portes dérobées (backdoor) .....</i>	47
f) <i>Attaque Man In The Middle (MITM).....</i>	47
<i>Figure 11:: Attaque Men in The Middle (source: google image) .....</i>	48
3. ATTAQUES LOGICIEL.....	48
<b>D. LES TYPES DE MENACES.....</b>	<b>48</b>
1. LES MENACES PASSIVES .....	48
2. LES MENACES ACTIVES : .....	49

<b>E. LES OUTILS UTILISÉS POUR SÉCURISER UN RÉSEAU .....</b>	<b>49</b>
1. LE PARE-FEU (FIREWALL) : .....	49
<i>Figure 12: Utilité d'un parefeu(source : googleimage)*.....</i>	49
2. LE VPN (VIRTUAL PRIVATE NETWORK):.....	49
<i>Figure 13: Système VPN (source : google image).....</i>	50
3. VLAN : .....	50
<i>Figure 14: Exemple d'un réseau VLAN (source : google image) .....</i>	50
4. ZONE DÉMILITARISÉE (DMZ) : .....	50
<i>Figure 15: Zone DMZ (source : google image).....</i>	51
5. LE PROXY : .....	51
<i>Figure 16: Proxy (source : google image).....</i>	51
6. LES ANTI-VIRUS : .....	52
<b>F. LES PROTOCOLES DE SÉCURITÉ .....</b>	<b>52</b>
1. PROTOCOLE SSL.....	52
2. PROTOCOLE SSH.....	52
3. PROTOCOLE HTTP .....	53
<i>Figure 17: Schéma d'une requête http.....</i>	54
4. PROTOCOLE HTTPS.....	54
<b>II. GENERALITE SUR LA DOUBLE AUTHENTIFICATION .....</b>	<b>54</b>
A. DÉFINITION ET PRINCIPE DE LA DOUBLE AUTHENTIFICATION (2FA).....	54
B. FONCTIONNEMENT DE LA DOUBLE AUTHENTIFICATION .....	55
<b>FIGURE 18: FONCTIONNEMENT DE LA 2FA (SOURCE : GOOGLE IMAGE) .....</b>	<b>55</b>
C. LES FACTEURS D'AUTHENTIFICATIONS .....	56
<b>FIGURE 19: FACTEUR DE LA 2FA (SOURCE : GOOGLE IMAGE).....</b>	<b>56</b>
D. LES SERVICES D'AUTHENTIFICATION.....	57
D. LES METHODES D'AUTHENTIFICATION .....	58
1. LE COMBO IDENTIFIANT / MOT DE PASSE .....	58
2. L'AUTHENTIFICATION BIOMETRIQUE .....	58
3. QR CODE / PUSH NOTIFICATIONS / SMS OTP .....	59
4. INTERACTION COMPORTEMENTALE.....	59
E. LES MOYENS D'AUTHENTIFICATION .....	59
1. LE MOT DE PASSE.....	59
2. ONE-TIME PASSWORD .....	60
3. BIOMÉTRIE.....	61
4. CERTIFICAT.....	61
5. AUTHENTIFICATION GRAPHIQUE .....	62
6. TOKEN HARDWARE .....	63
7. AUTHENTIFICATION MULTI-FACTERNS .....	63
8. GOOGLE AUTHENTICATOR.....	63
F. TYPES DE PROTOCOLES D'AUTHENTIFICATION.....	64
1. KERBEROS : .....	64
<b>FIGURE 20: PROTOCOLE KERBEROS .....</b>	<b>64</b>
2. PROTOCOLE D'ACCÈS À L'ANNUAIRE LÉGER (LDAP).....	65
<b>FIGURE 21: PROTOCOLE LDAP .....</b>	<b>65</b>
3. OAUTH2 : .....	66

<b>FIGURE 22: PROTOCOLE OAUTH2.....</b>	<b>66</b>
4. SAML.....	67
<b>FIGURE 23: PROTOCOLE SAML .....</b>	<b>67</b>
5. RADIUS.....	68
<b>FIGURE 24: PROTOCOLE RADIUS .....</b>	<b>68</b>
<b>III. PROTOCOLE RADIUS .....</b>	<b>69</b>
INTRODUCTION .....	69
A. FONCTIONNALITÉS PRINCIPALES .....	69
1. AUTHENTIFICATION.....	69
2. AUTORISATION.....	70
3. COMPTABILITÉ .....	70
B. ARCHITECTURE DU PROTOCOLE .....	70
1. COMPOSANTS DE RADIUS.....	70
2. FLUX DE COMMUNICATION.....	70
C. AVANTAGES DE RADIUS .....	71
D. APPLICATIONS DU PROTOCOLE RADIUS .....	71
E. SÉCURITÉ ET MEILLEURES PRATIQUES .....	71
<b>CONCLUSION.....</b>	<b>71</b>
<b>IV. SURVEILLANCES ET GESTIONS DU RESEAU .....</b>	<b>72</b>
<b>INTRODUCTION.....</b>	<b>72</b>
A. OBJECTIFS DE LA SURVEILLANCE DU RÉSEAU.....	72
1. DÉTECTION DES ANOMALIES .....	72
2. SUIVI DES PERFORMANCES .....	72
3. CONFORMITÉ RÉGLEMENTAIRE.....	72
4. GESTION DES RESSOURCES .....	72
B. OUTILS DE SURVEILLANCE DU RÉSEAU .....	73
1. SYSTÈMES DE GESTION DE RÉSEAU (NMS).....	73
2. OUTILS DE SURVEILLANCE DE LA SÉCURITÉ (SIEM).....	73
3. OUTILS DE SURVEILLANCE DE LA PERFORMANCE DU RÉSEAU (NPM) .....	73
C. PRTG NETWORK MONITOR .....	74
1. PRÉSENTATION DE PRTG .....	74
2. FONCTIONNALITÉS CLÉS.....	74
3. AVANTAGES DE PRTG .....	74
4. CAS D'UTILISATION DE PRTG .....	75
D. MÉTHODES DE GESTION DU RÉSEAU .....	75
1. GESTION DES CONFIGURATIONS .....	75
2. GESTION DES INCIDENTS .....	75
3. GESTION DES CHANGEMENTS.....	75
E. SURVEILLANCE EN TEMPS RÉEL.....	76
F. INTÉGRATION AVEC LA SÉCURITÉ.....	76
<b>CONCLUSION.....</b>	<b>76</b>
<b>V. NORMES ET REGLEMENTATIONS .....</b>	<b>77</b>
<b>INTRODUCTION.....</b>	<b>77</b>
1. REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES (RGPD).....	77
2. NORME ISO/IEC 27001.....	77

3. AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION (ANSSI) .....	77
4. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL) .....	78
5. NORME ISO/IEC 27701.....	78
6. BONNES PRATIQUES EN MATIERE DE SECURITE.....	78
7. CONFORMITE SECTORIELLE .....	78
<b>CONCLUSION.....</b>	<b>78</b>
<b>CHAPITRE 4 :</b> .....	<b>80</b>
<b>IMPLEMENTATION DE LA SOLUTION.....</b>	<b>80</b>
I. CHOIX DE LA SOLUTION NIVEAU AUTHENTIFICATION.....	81
II. ARCHITECTURE UTILISE POUR LA DEMONSTRATION.....	82
<b>FIGURE 25: ARCHITECTURE AFECAMEROUN .....</b>	<b>82</b>
<b>FIGURE 26: ARCHITECTURE UTILISÉ POUR LA DEMONSTRATION .....</b>	<b>82</b>
III. CONFIGURATION DE LA DOUBLE AUTHENTIFICATION SUR LE SERVEUR.....	83
WINDOWS.....	83
<b>FIGURE 27: CHOIX DE LA LANGUE DU SYSTEME.....</b>	<b>83</b>
<b>FIGURE 28: CHOIX DU SYSTÈME À INSTALLER.....</b>	<b>84</b>
<b>FIGURE 29: CONTRAT DE LICENCE .....</b>	<b>84</b>
<b>FIGURE 30: INSTALLATION DE WINDOWS SERVER .....</b>	<b>85</b>
<b>FIGURE 31: PARAMETRES DE PERSONNALISATION.....</b>	<b>85</b>
<b>FIGURE 32: DEVEROULLAGE DE LA SESSION .....</b>	<b>86</b>
<i>Figure 32: Ajout d'une nouvelle zone.....</i>	87
<i>Figure 32: Choix du type de zone .....</i>	87
<i>Figure 33: Specifier la zone.....</i>	88
<i>Figure 35: Mise à Niveau .....</i>	89
<i>Figure 36: Fin de l'installation .....</i>	89
<i>Figure 37: Ajout d'un nouveau pointeur .....</i>	90
<i>Figure 38: Ajout du pointeur .....</i>	91
<b>FIGURE 39: VERIFICATION DE LA FORET ET DU NOM DE DOMAINE .....</b>	<b>91</b>
IV. CONFIGURATION DE LA DOUBLE AUTHENTIFICATION SUR UN ROUTEUR .....	92
1. INSTALLATION DE L'ANNUAIRE LDAP .....	92
<b>FIGURE 40: AJOUT D'UN ROLE ET FONCTIONNALITE .....</b>	<b>92</b>
<b>FIGURE 41: ACTIVATION DE LA FONCTIONNALITE ADDS .....</b>	<b>93</b>
<b>FIGURE 43: CONFIRMATIONS DES SELECTIONS D'INSTALLATIONS .....</b>	<b>94</b>
<b>FIGURE 44: INSTALLATION DE L'ADDS .....</b>	<b>94</b>
<b>FIGURE 45: ACHEVEMENT DE L'INSTALLATION DE L'ADDS –TABLEAU DE BORD .....</b>	<b>95</b>
<b>FIGURE 46: INSERTION DU NOM DE DOMAINE .....</b>	<b>96</b>
<b>FIGURE 47: INSERTION DU MOT DE PASSE .....</b>	<b>97</b>
<b>FIGURE 48: INDICATION DU NOM DE DOMAINE NETBIOS.....</b>	<b>97</b>
<b>FIGURE 49: INDICATION DU CHEMIN D'ACCES .....</b>	<b>98</b>

<b>FIGURE 50: RESULTAT DE LA VERIFICATION DES OPTIONS .....</b>	<b>99</b>
<b>FIGURE 51: INSTALLATION DU SERVICE ADDS .....</b>	<b>99</b>
<b>FIGURE 52: INTERFACE DE CONNEXION.....</b>	<b>100</b>
<b>FIGURE 53: LANCEMENT TOTPRADIUS .....</b>	<b>101</b>
<b>FIGURE 55: LANCEMENT TOTPRADIUS .....</b>	<b>102</b>
<b>FIGURE 56: NOM DE NOTRE SERVEUR TOTPRADIUS.....</b>	<b>102</b>
<b>FIGURE 57: ADRESSE IP DE NOTRE SEVEUR TOTPRADIUS.....</b>	<b>103</b>
<b>FIGURE 58: MASQUE DE SOUS RESEAU.....</b>	<b>103</b>
<b>FIGURE 59: GATEWAY DE TOTPRADIUS.....</b>	<b>104</b>
<b>FIGURE 60: PREMIER DNS DE TOTPRADIUS .....</b>	<b>105</b>
<b>FIGURE 61: DEUXIEME DNS DE TOTPRADIUS .....</b>	<b>105</b>
3.    CONFIGURATION DU SECOND FACTEUR D'AUTHENTIFICATION .....	106
<b>FIGURE 64: INTERFACE DE CONNEXION TOTPRADIUS.....</b>	<b>107</b>
<b>FIGURE 65: PAGE DE TOTPRADIUS .....</b>	<b>108</b>
<b>FIGURE 66: SETTING DE TOTPRADIUS.....</b>	<b>108</b>
<b>FIGURE 67 :PARAMETRE DE RADIUS DANS TOTPRADIUS .....</b>	<b>109</b>
<b>FIGURE 68: IP DU SERVEUR RADIUS.....</b>	<b>110</b>
<b>FIGURE 69: CONFIGURATION DE LDAP .....</b>	<b>110</b>
<b>FIGURE 70: ENREGISTREMENT DES UTILISATEURS DE TOTPRADIUS .....</b>	<b>111</b>
<b>FIGURE 71: INTERFACE D'ENREGISTREMENT DES USER.....</b>	<b>111</b>
<b>FIGURE 72: CODE QR DE L'USER ADMINISTRATEUR.....</b>	<b>112</b>
<b>FIGURE 73: ENREGISTREMENT D'ADMINISTRATEUR .....</b>	<b>112</b>
<b>FIGURE 73: CREATION DES USER .....</b>	<b>113</b>
4.    ROUTEUR .....	114
<i>Figure 74: IP des interfaces du routeur.....</i>	114
<i>Figure 75: Configuration de l'authentification sur le routeur.....</i>	115
<b>V. CONFIGURATION DE LA SUPERVISION PRTG SUR LE SERVEUR WINDOWS .....</b>	<b>117</b>
<i>Figure 77: Choix de la langue lors de l'installation de PRTG .....</i>	117
<i>Figure 78: Lire le contrat et appuyer sur je comprends et j'accepte.....</i>	117
<i>Figure 79: Cliquez sur suivant.....</i>	118
<i>Figure 80: Patienter l'installation.....</i>	118
<b>VI. TEST DE FONCTIONNALITÉS.....</b>	<b>119</b>
A)    TESTONS LES FONCTIONNALITÉS DE NOTRE SUPERVISION PRTG .....	119
<i>Figure 81: Page d'accueil PRTG .....</i>	119
<i>Figure 82: Cliquer sur ajouter un groupe .....</i>	120
<i>Figure 83: Cliquer sur Infrastructure reseau et puis sur ok .....</i>	120
<i>Figure 84: Entrer Nom du groupe .....</i>	121
<i>Figure 85: Cliquer sur Equipement .....</i>	121
<i>Figure 86: Cliquer sur Votre Groupe .....</i>	122

---

<i>Figure 87: Entrer le nom de l'équipement et son adresse IP .....</i>	122
<i>Figure 88: Choisir le logo de l'équipement et cochez la découverte automatique.....</i>	123
<i>Figure 89: Cliquer sur Equipment et cliquer sur ajouter un capteur .....</i>	123
<i>Figure 90: Choisissez le type de capteur que vous souhaitez superviser.....</i>	124
<i>Figure 91: Choix du capteurs des Ping .....</i>	124
<i>Figure 92: Configurer les paramètres selon vous et cliquez sur Créer.....</i>	125
<i>Une fois que vous avez ajouté tout équipement et vos capteurs, votre réseau sera supervisé en temps réel .....</i>	125
<i>Figure 93: Capture de mes équipements et leur Capteur .....</i>	125
A) TESTONS LA DOUBLE AUTHENTIFICATION SUR LE ROUTEUR .....	126
<i>Figure 94: Test d'authentification sur le routeur via PuTTY .....</i>	126
<i>Figure 95: Interface du routeur via PuTTY .....</i>	126
<i>Figure 96: Log du serveur TOTPRadius .....</i>	127
<i>Figure 97: Configuration du routeur.....</i>	127
<b>CONCLUSION GENERAL .....</b>	<b>128</b>
<b>ANNEXES .....</b>	<b>129</b>
<b>BIBLIOGRAPHIE .....</b>	<b>130</b>
<b>WEBOGRAPHIE .....</b>	<b>131</b>
<b>GLOSSAIRE .....</b>	<b>132</b>
<b>TABLE DE MATIERES .....</b>	<b>133</b>