جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

République Algérienne Démocratique et populaire
Ministère de l'enseignement Supérieur et de la recherche scientifique
Université Abderrahmane.Mira-Béjaia

Faculté des sciences exactes
Département d'Informatique

Mémoire de fin de cycle
En vue de l'obtention du diplôme de Master en Informatique
Option : Administration et Sécurité des réseaux

Thème

Configuration d'un serveur RADIUS pour l'authentification des utilisateurs via VPN : Cas d'étude BMT

Présenté par :

AMRANI Amina & AMEZRAR Sabrine

Soutenu le : **4 juillet 2024,** devant le jury, composé de :

✓ **Dr** SADI Mustapha	**MCB UAM BEJAIA**	**President**
✓ **Dr** L. KHENOUS	**MCB UAM BEJAIA**	**Encadrant**
✓ **Dr** BENNAI Yani-Athmane	**MCB UAM BEJAIA**	**Examinateur**

2023-2024

Remerciements

Tout d'abord on remercie le bon dieu "Allah", le tout Puissant, et le Miséricordieux, d'avoir toujours été là pour nous, de nous avoir donné les capacités et le courage à surmonter les obstacles qu'on a rencontrés durant ce parcours et achever ce travail, tout en prenant du plaisir et en faisant de belles rencontres. Et pour tout on lui rend grâce.

On adresse nos remerciements également aux personnes qui nous ont aidés dans la réalisation de ce projet

On présente nos sincères remerciements à Mr BOUMERZOUG Moussa qui nous a accueillie au sein de l'entreprise BMT

On aimerait tout particulièrement remercier notre encadrant Mr KHENOUS Lachemi d'avoir toujours été à l'écoute, pour ses conseils, sa disponibilité, son soutien, ses encouragements, sa patience et sa bienveillance. Qu'il trouve ici l'expression de nos profondes gratitudes.

On tient à remercier Mr REGREG Abdellah qui nous a encadré durant la durée de notre stage.

On souhaiterait également présenter nos chaleureux remerciements à nos camarades BEKKA Aimad, BENKHELAT Oussama, et AMZAL Massinissa qui nous ont beaucoup aidé et orienté tout au long de notre mémoire.

Je tiens aussi à remercier tous les membres du jury, pour leurs temps et attention consacré à notre mémoire.

Dédicace

Avant toute chose je dois remercier DIEU pour tous les biens qui m'a procuré ; la santé, la gratitude, la famille, les amis, les ambitions, la joie de vie, et surtout de m'avoir permis de sentir son existence et vouloir apprendre à le connaitre.

Je dédie ce travail à mes très chers parents : je suis la plus chanceuse d'être votre fille, vous avez fait tout pour que je réussisse, et m'épanouir. Je vous aime très forts.

***Ma mère** Hayette ; tu m'as toujours soutenu dans les moments les plus difficiles de ma vie, tu m'as supporté et tu m'as accepté comme je suis. Tes conseils, tes mots doux, et ton sourire radieux, gravés dans mon cœur sont ma source de force pour affronter les difficultés de la vie.*

***Mon père** Omar ; tu es mon héros, et mon exemple. A travers nos conversations et sorties très chaleureuses et enrichissantes tu m'as transmis des valeurs et principes indispensables au fondement de ma vie. Tu as toujours cru en moi, Tu m'as encouragé, tu m'as appris à avoir confiance en moi, à être moi-même.*

*A mes **frères** Samir et Yacine, à ma **sœur** Anissa, avec qui j'ai partagé mon enfance. On a vécu ensemble des moments inoubliables. A mon **beau-frère** Bizak et ma **belle-sœur** Anaïs, à mes **nièces** Nadjet et Nélia.*

A ma binôme AMZRAR Sabrine je tiens à exprimer mes remerciements pour son soutien et son engagement tout au long de notre travail

À toute ma famille : oncles, tantes, cousins et cousines, merci d'être les personnes merveilleuses que vous êtes. Vous avez toujours été là pour moi et je vous en suis profondément reconnaissant.

À mes amies (BBA) qui sont devenues ma famille, je vous remercie du fond du cœur pour les fous rires, les larmes, les bons moments passés ensemble. Merci pour votre amitié et votre amour. Vous êtes des personnes extraordinaires.

Amina

Dédicace

Avant tout, je remercie ***Dieu*** *pour la santé, la force et l'opportunité de réaliser ce mémoire. Sa guidance et Ses bénédictions ont été essentielles.*

Je dédie ce travail à :

Ma chère mère *Fatima, ton amour inconditionnel, tes prières et ton soutien m'ont été une source inépuisable de motivation. Tu es l'étoile qui illumine mon chemin et la force qui me pousse à aller de l'avant. Même lorsque les jours étaient difficiles, tu étais toujours là pour moi, m'encourageant et me donnant la force de persévérer. Je te suis éternellement reconnaissante pour tout ce que tu as fait pour moi.*

Mon père *Saddek, merci pour tes conseils sages et ton soutien constant. Ta patience et ta foi en moi m'ont permis de surmonter bien des obstacles. Tu as toujours su trouver les mots justes pour m'encourager et me donner confiance en moi.*

Mes grands frères *Lamine et Yazid, bien que vous soyez loin de moi, vous avez toujours été présents dans mon cœur. Votre guidance et votre soutien, même à distance, m'ont été d'un grand secours. Chaque message, chaque appel, chaque pensée de votre part m'a rappelé que je ne suis jamais seule. Vous avez été des modèles et des piliers dans ma vie, et je suis profondément reconnaissante pour votre amour et votre soutien constants.*

Ma meilleure amie *Kenza, ton amitié sincère et ta présence constante ont été précieuses tout au long de ce chemin. Tu es plus qu'une amie, tu es comme une sœur pour moi. Merci d'être une amie extraordinaire et de m'avoir soutenue dans les moments les plus difficiles.*

Ma binôme *Amina, ta collaboration, ton dévouement et ton soutien ont été d'une valeur inestimable tout au long de ce projet. Merci d'avoir été une part essentielle de cette réussite.*

Mes amis *qui nous ont apporté leur soutien inestimable tout au long de notre démarche, et qui par leurs encouragements, on a pu surmonter tous les obstacles.*

Toute ma famille *merci pour votre amour et votre soutien qui sont une grande source de bonheur pour moi. Chaque moment passé ensemble, bien que rare, reste précieux et m'est cher.*

Sabrine

Table des matières

Table des figures

Liste des tableaux

La liste des abréviations

AAA	**A**uthentication, **A**uthorization, **A**ccounting
ACL	**A**ccess **C**ontrol **L**ist
AD DS	**A**ctive **D**irectory **D**omain **S**ervices
BMT - SPA	**B**ejaia **M**éditerranéen **T**erminal - **S**ociété **P**ar **A**ctions
CA	**C**ertificat **A**uthority
CDI	**C**ontrat à **D**urée **I**ndéterminée
CDD	**C**ontrat à **D**urée **D**éterminée
CPE	**C**onseil de **P**articipation de l'**É**tat
CPU	**C**entral **P**roccessing **U**nit
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DNS	**D**omain **N**ame **S**ystem
DRHM	**D**irection des **R**essources **H**umaines et **M**oyens
EAP	**E**xtensible Authentication Protocol
EPB	**E**ntreprise **P**ortuaire de **B**ejaia
FTP	**F**ile **T**ransfer **P**rotocol
FreeBSD	**F**ree **B**erkeley **S**oftware **D**istribution
GNS3	**G**raphical **N**etwork **S**imulator-3
HSE	**H**ealth, **S**afety, and **E**nvironment
HTTP	**H**yperText **T**ransfer **P**rotocol
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
IETF	**I**nternet **E**ngineering **T**ask **F**orce
IP	**I**nternet **P**rotocol
IPsec	**I**nternet **P**rotocol **S**ecurity
ISO	**I**nternational **O**rganization for **S**tandardization
KDC	**K**ey **D**istribution **C**enter
LAN	**L**ocal **A**rea **N**etwork
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol
LLC	**L**ogical **L**ink **C**ontrol
MAC	**M**edia **A**ccess **C**ontrol
MAN	**M**etropolitan **A**rea **N**etwork
MD5	**M**essage **D**igest **A**lgorithm 5
MITM	**M**an **I**n **T**he **M**iddle
MSCHAPv2	**M**icrosoft **C**hallenge **H**andshake **A**uthentication **P**rotocol version 2

NPS	**N**etwork **P**olicy **S**erver
PAN	**P**ersonal **A**rea **N**etwork
Pfsense	**O**pen source **f**irewall/router software based on **F**reeBSD
RADIUS	**R**emote **A**uthentication **D**ial-In **U**ser **S**ervice
RAM	**R**andom **A**ccess **M**emory
RFC	**R**equest **F**or **C**omments
SSL/TLS	**S**ecure **S**ockets **L**ayer / **T**ransport **L**ayer **S**ecurity
TACACS+	**T**erminal **A**ccess **C**ontroller **A**ccess-**C**ontrol **S**ystem **P**lus
TGT	**T**icket **G**ranting **T**icket
TCP	**T**ransmission **C**ontrol **P**rotocol
TCP/IP	**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol
TLS	**T**ransport **L**ayer **S**ecurity
UDP	**U**ser **D**atagram **P**rotocol
VPN	**V**irtual **P**rivate **N**etwork
WAN	**W**ide **A**rea **N**etwork
X509	**P**ublic **K**ey **I**nfrastructure standa

Introduction Générale

En cette ère numérique, les réseaux informatiques sont devenus omniprésents, reliant individus, entreprises et organisations dans un monde hyperconnecté. Cette connectivité globale, si elle offre des opportunités immenses, s'accompagne également de risques croissants en matière de sécurité. Les réseaux informatiques, devenus des cibles privilégiées pour les cybercriminels, contiennent des données sensibles et des ressources précieuses qui doivent être protégées.

Face à ces menaces, la sécurité des réseaux informatiques devient un impératif incontournable. Il est essentiel de mettre en œuvre des mesures de sécurité solides afin de préserver la confidentialité des données, prévenir les intrusions et garantir la continuité des activités. Parmi ces mesures, l'authentification des utilisateurs joue un rôle crucial.

L'authentification des utilisateurs garantit l'accès exclusif aux ressources réseau aux seuls utilisateurs autorisés. Elle consiste à vérifier l'identité des utilisateurs en s'appuyant sur des facteurs d'authentification tels que des noms d'utilisateur, des mots de passe, des clés physiques ou des données biométriques.

Le protocole RADIUS (Remote Authentication Dial-In User Service) pourrait être une solution pour l'authentification centralisée des utilisateurs dans les réseaux d'entreprise. Il offre une architecture flexible et évolutive, permettant de gérer efficacement les accès d'un grand nombre d'utilisateurs sur des réseaux étendus. Par ailleurs, pour faciliter l'accès des employés depuis l'extérieur au réseau local de l'entreprise, OpenVPN peut être déployé. Il crée des connexions VPN (Virtual Private Network) sécurisées qui protègent les données pendant leur transmission, assurant ainsi une gestion d'accès efficace et une meilleure confidentialité des communications.

Ce mémoire s'inscrit dans le cadre de la mise en place d'un serveur d'authentification RADIUS sous GNS3 (Graphical Network Simulator-3), en prenant le cas spécifique de BMT (Bejaia Méditerranéen Terminal) de. L'objectif est de renforcer la sécurité du réseau de BMT en centralisant l'authentification des utilisateurs via un VPN, en facilitant la gestion des comptes à distance, et en offrant une solution flexible et évolutive pour un accès sécurisé aux ressources du réseau.

Nous avons structuré notre mémoire en quatre chapitres comme suit :

Le premier chapitre Traite des concepts fondamentaux des réseaux informatiques et de la sécurité des réseaux.

Le deuxième chapitre présente l'entreprise BMT de Bejaia en détaillant son historique, sa structure organisationnelle, sa localisation au port de Bejaia et ses activités, en mettant en avant ses certifications ISO (International Organization for Standardization). Il aborde également la problématique spécifique rencontrée par l'entreprise et propose une solution pour y remédier.

Le troisième chapitre aborde la sécurisation des accès aux données sensibles par l'utilisation des méthodes telles que les mots de passe et les certificats numériques. Il compare RADIUS et TACACS+ (Terminal Access Controller Access-Control System Plus) pour la sécurité et la gestion des comptes, explore l'architecture AAA (Authentication, Authorization, Accounting) pour la gestion des identités réseau, et discute les protocoles EAP (Extensible Authentication Protocol) pour sécuriser les réseaux locaux et les VPN. Le chapitre se penche également sur la sécurisation des VPN avec OpenVPN, SSL/TLS, ainsi que l'utilisation du pare-feu pfSense pour une gestion avancée de la sécurité des réseaux.

Le quatrième chapitre Détaille la configuration et la mise en œuvre pratique de la solution RADIUS via un VPN OpenVPN en utilisant GNS3, incluant les différents outils déployés pour l'implémentation de cette solution, les étapes de configuration et les tests de fonctionnement.

Enfin, nous concluons notre travail en présentant une conclusion générale, décrivant les éléments clés qui ont été développés dans ce mémoire, ainsi que quelques perspectives pour ce projet.

Chapitre I : Notions de base sur la sécurité informatique

1. Introduction

La sécurité des réseaux est devenue cruciale dans un monde de plus en plus connecté où Internet est devenu une infrastructure essentielle pour les entreprises et les organisations. Les réseaux informatiques facilitent la communication, la collaboration et le partage d'informations, ce qui facilite le travail d'équipe, mais sont toujours menacées par des attaques qui mettent en péril la sécurité et la confidentialité des données. Dans ce premier chapitre, nous allons mettre en revue quelques notions de base sur les réseaux, que nous jugeons nécessaires de les rappeler très brièvement pour une meilleure compréhension de l'avancement de notre travail.

2. Principes fondamentaux des réseaux

Voici les principes fondamentaux des réseaux qui constituent la base de leur fonctionnement. Ils sont essentiels pour assurer une communication efficace et sécurisée entre les différents dispositifs connectés.

2.1. Définition

Un réseau informatique est un ensemble interconnecté d'au moins deux ordinateurs permettant la transmission et le partage d'informations ou de ressources. En d'autres termes, c'est un système de communication interconnectant divers dispositifs informatiques, facilitant ainsi le partage de ressources communes. Un réseau se caractérise par une dimension physique (les câbles ou autres supports transportant les signaux) et une dimension logique (les programmes gérant les protocoles de communication).[1]

2.2. Les types de réseau

Il existe plusieurs types de réseaux informatiques qui se différencient principalement par leur taille géographique [2]

- **Personal Area Network (PAN)**

Un PAN est un réseau personnel qui relie des appareils électroniques autour d'une personne, généralement dans un rayon de quelques mètres. Il peut utiliser des connexions filaires comme l'USB ou sans fil comme le Bluetooth, le Wifi ou l'infrarouge.

- **Local Area Network (LAN)**

Un LAN est un réseau local qui interconnecte des équipements informatiques sur une zone géographique restreinte comme une maison, une école ou une entreprise. Sa portée est généralement limitée à un bâtiment ou un campus.

- **Métropolitain Area Network (MAN)**

Un MAN est un réseau métropolitain qui couvre une zone géographique plus étendue comme une ville ou une région. Il utilise souvent des fibres optiques et permet des débits de données élevés sur de plus longues distances que les LAN.

- **Wide Area Network (WAN)**

Un WAN est un réseau étendu qui interconnecte plusieurs réseaux locaux sur de grandes distances géographiques, voire à l'échelle mondiale. L'exemple le plus connu est Internet, qui est un WAN public. Mais il existe aussi des WAN privés reliant les sites d'une même organisation.

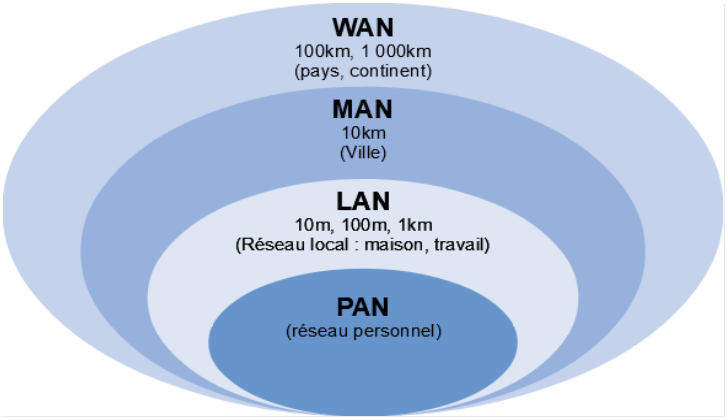

Figure 1.1 types de réseau [3]

Les différentes tailles des réseaux informatiques sont classées, allant du réseau personnel (PAN) au réseau mondial (WAN), en passant par les réseaux locaux (LAN) et métropolitains (MAN). Leur architecture et leurs technologies diffèrent selon leur étendue géographique et leurs exigences particulières.

3. Sécurité des réseaux informatique

La sécurité des réseaux informatiques est devenue essentielle dans notre monde numérique en évolution constante. Les réseaux facilitent la transmission des données dans tous les domaines, mais ils sont également exposés à une multitude de menaces, des attaques sophistiquées aux erreurs humaines. Ainsi, assurer la sécurité des réseaux est primordial pour protéger les données, maintenir la confiance des utilisateurs et garantir la continuité des activités.

3.1. Définition

La sécurité informatique est devenue une préoccupation majeure tant pour les entreprises que pour les particuliers, en raison de l'importance croissante de la transmission d'informations sensibles et du désir de garantir leur confidentialité. Les cyberattaques et les violations de données sont devenues monnaie courante, mettant en lumière la complexité croissante de la sécurité face à l'évolution constante des capacités des hackers. De plus, la montée en puissance du Cloud comptine rend la localisation des données plus floue, tandis que la demande d'un accès omniprésent aux données souligne l'importance de rester constamment vigilant en matière de protection des données pour les gouvernements, les entreprises et les particuliers. [4]

3.2. L'objectif de la sécurité [5]

Les objectifs de la sécurité des réseaux sont les suivants

- **Disponibilité :** la disponibilité implique de garantir l'accessibilité d'un système ou d'une donnée dans un délai déterminé. Il s'agit d'une propriété qui permet aux personnes autorisées d'accéder aux biens (données ou systèmes) au moment souhaité.

- **Confidentialité :** la confidentialité vise à garantir que seules les personnes autorisées peuvent accéder à une donnée. Il s'agit de s'assurer que ce qui est secret reste confidentiel. En d'autres termes, c'est l'éviter de lire des données sans autorisation.

- **Intégrité :** l'intégrité implique que les informations doivent correspondre aux attentes et ne doivent pas être modifiées de manière accidentelle, illicite ou malveillante. En d'autres termes, les éléments pris en compte doivent être précis et complets.

- **Non répudiation :** la propriété de non-répudiation garantit que les parties impliquées dans une transaction ne peuvent pas nier avoir participé à cette transaction Elle assure que l'authenticité et l'intégrité des données sont maintenues, empêchant ainsi toute négation de l'envoi ou de la réception d'un message.

3.3. Types de sécurité [6]

Les types de sécurité des réseaux informatiques comprennent à la fois des mesures de sécurité physique et logique pour protéger les systèmes d'information.

3.3.1. La sécurité physique

La sécurité physique englobe l'ensemble des éléments liés à l'environnement dans lequel les Ressources sont implantées. Elle peut englober

• La sécurité physique des salles de serveurs, des périphériques réseau, etc.

• La lutte contre les accidents et les feux.

• Les systèmes de l'alimentation ininterrompue.

• La Surveillance vidéo, etc.

3.3.2. La sécurité logique

La sécurité logique désigne la mise en place d'un système de contrôle d'accès, par logiciel, afin de garantir la sécurité des ressources. Elle peut englober

• La mise en place d'une stratégie de sécurité solide pour les mots de passe.

• Le développement d'un modèle d'accès basé sur l'authentification, l'autorisation et la traçabilité, ainsi que la configuration adéquate des pares-feux de réseau.

• L'installation des IPS (systèmes de prévention d'intrusion).

• L'utilisation des VPN (réseau privé virtuel), etc.

3.4. Terminologie de la sécurité informatique

Terminologie de la sécurité est essentiel pour comprendre les enjeux et les stratégies de protection des réseaux.

- **Vulnérabilité :** fait référence à une vulnérabilité ou une faille présente dans un système informatique, une application ou un protocole de communication, qui peut être exploitée par des attaquants afin de compromettre la sécurité du système ou d'accéder à des informations confidentielles. Ces vulnérabilités peuvent être de nature matérielle ou logicielle. Aucun système, aussi avancé soit-il, n'est entièrement sécurisé contre les cyberattaques.[7]

- **Menace :** représente une éventuelle cause d'un incident de sécurité susceptible de causer des dommages à un système informatique ou aux données qu'il contient. Les menaces peuvent être causés par diverses sources, telles que les attaques externes, les erreurs humaines, les problèmes matériels ou les catastrophes naturelles.[7]
- **Attaque** : est une action malveillante qui cherche à compromettre la sécurité d'un élément (système informatique, réseau, application, etc.) en exploitant une faille. Il n'est donc possible d'attaquer (et de réussir) que si le bien est touché par une vulnérabilité.[7]

3.5. Mécanismes de sécurité

Parmi les mécanismes de sécurité employés afin de préserver les réseaux informatiques des attaques externes et internes, on peut citer :

- **Pare-feu** : est un dispositif qui permet d'isoler des zones réseau entre elles et de ne permettre le passage que de certains flux.[7]

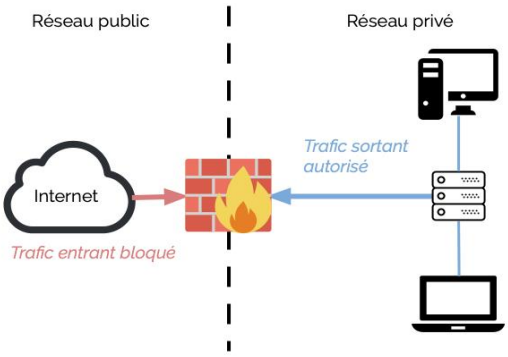

Figure 1. 2 Le pare-feu

- **VPN** : offre la possibilité de créer un tunnel sécurisé entre deux réseaux distants, offrant ainsi aux utilisateurs un accès sécurisé au réseau à distance. Les VPN font appel à des protocoles de cryptage afin de garantir la sécurité des échanges entre les réseaux.[7]

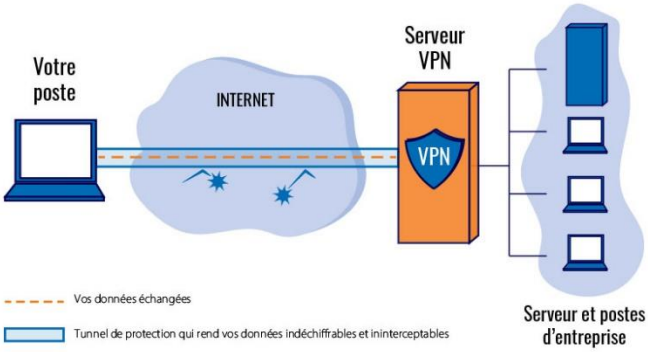

Figure 1.3 Fonctionnement d'un VPN [9]

- **Antivirus et antimalware** : sont utilisés pour repérer et éliminer les logiciels malveillants et les virus déjà détectés par la communauté de sécurité.[7]

3.6. La Cryptographie

La cryptographie consiste à rendre des informations secrètes (illisibles) pour qu'elles puissent être accessibles à un seul destinataire authentifié. Elle repose principalement sur l'arithmétique : il s'agit de convertir les lettres qui constituent le message en une succession de chiffres, puis à effectuer des calculs sur ces chiffres pour :

- Les altérer de manière à les rendre incompréhensible.
- Faire en sorte que le destinataire saura les décrypter.

Coder un message pour le rendre secret s'appelle le cryptage. La méthode opposée est connue sous le nom de décryptage et elle requiert une clé de décryptage.[10]

Il existe deux types de cryptage : le cryptage symétrique et le cryptage asymétrique.

3.6.1. Cryptage symétrique

Cryptage symétrique, également connue sous le nom de cryptage à clé secrète ou chiffrement conventionnel, utilise une même clé pour crypter et décrypter le message. Cette technique repose sur la distribution des clés dans un réseau étendu car elle Nécessite le partage d'une seule clé avec chaque correspondant.[10]

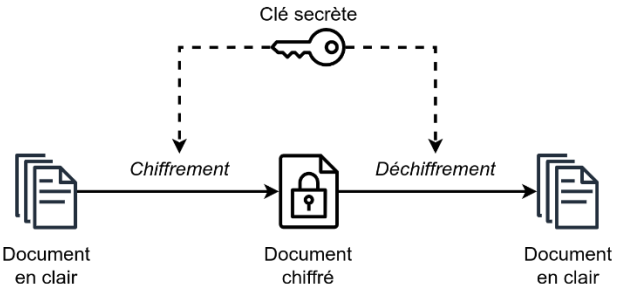

Figure 1.4 Cryptage symétrique [11]

3.6.2. Cryptage asymétrique

Deux clés distinctes sont utilisées par ce système de cryptage pour chaque utilisateur, l'une des clés est privée et connue uniquement par son propriétaire, tandis que l'autre est publique et accessible à tous.

L'algorithme de cryptage relie les clés publiques et privées de manière mathématique, de sorte qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante, car ces deux clés sont créées simultanément. Ainsi, une clé est employée pour le cryptage et l'autre pour le décryptage.

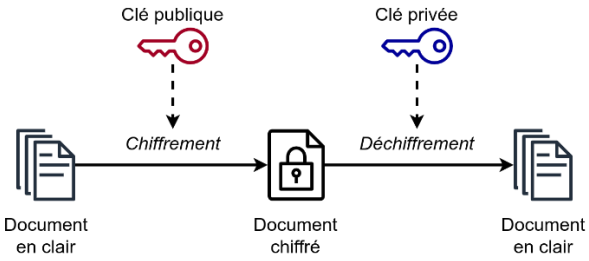

Figure 1.5: Cryptage asymétrique [12]

4. Conclusion

Les types de sécurité des réseaux informatiques en clôture de ce chapitre dédié à la sécurité des réseaux informatiques, il apparaît clairement que la protection de ces infrastructures est un impératif indiscutable dans notre ère numérique. À travers une approche proactive, une surveillance constante et une collaboration étroite entre les acteurs concernés, nous pouvons construire des réseaux informatiques résilients face aux défis actuels et futurs de la cybersécurité. Dans le prochain chapitre, nous aborderons en détails l'organisme d'accueil ou nous avons effectué notre stage, en présentant son organisation et ses missions. Cette section permettra de mieux comprendre le contexte dans lequel notre projet s'inscrit.

Chapitre II : Présentation de l'organisme d'accueil

1. Introduction

BMT - SPA est une jointe venture entre l'Entreprise Portuaire de Bejaia (EPB) et Porte System & Equipment. L'EPB est l'autorité portuaire qui gère le port de Bejaia. PORTEK System and Equipment, une filiale du Groupe PORTEK, qui est un opérateur de Terminaux à conteneurs présent dans plusieurs ports dans le monde et également spécialisé dans les équipements portuaires.

Dans cette section nous allons présenter l'organisme d'accueil, l'historique de cette entreprise, les missions, les activités et différentes structures dans cette entreprise.

2. Historique, présentation et situation géographique de BMT Spa

2.1. L'historique

Dans son plan de développement 2004-2006, l'entreprise portuaire de Bejaia (EPB) avait inscrit à l'ordre du jour le besoin d'établir un partenariat pour la conception, le financement, l'exploitation et l'entretien d'un terminal a conteneurs au port de Bejaia.

Dès lors l'EPB s'est lancées dans la tâche d'identifier les partenaires potentiels et a arrêté son choix sur le groupe PORTEK qui est spécialisé dans le domaine de la gestion des terminaux à conteneurs. Le projet a été présenté au conseil de participation de l'état (CPE) en février 2004, le CPE a donné son accord au projet en mai 2004.

Sur accord du gouvernement Bejaia Méditerranéen Terminal Spa « BMT Spa » a vu le jour avec la jointe venture de l'entreprise portuaire de Bejaia (EPB) a 51% et PORTEK une société Singapourienne a 49%, PORTEK est un opérateur de terminaux spécialisé dans les équipements portuaire il est présent dans plusieurs ports dans le monde.

En 2011 PORTECK System and Equipment, a été racheté par le groupe Japonais MITSUI.

2.2. Présentation de BMT Spa

BMT Spa est une société par action, c'est une entreprise prestataire de service spécialisées dans le fonctionnement, l'exploitation, et la gestion du terminal a conteneur pour atteindre son objectif, elle s'est dotée d'un personnel compétant particulièrement former dans l'opération de gestion des terminaux à conteneurs. Elle dispose d'équipements d'exploitation des plus perfectionnées pour les opérations de manutention et d'acconage afin d'offrir des prestations de services de qualité, d'efficacité et de fiabilité en des temps records et a des couts compétitifs. BMT Spa offre ses prestations sur la base 24H /7j.

Le niveau de la technologie mis en place et la qualité des infrastructures et équipements performant (portiques de quai, portiques gerbeurs) font aujourd'hui du port de Bejaia et de BMT Spa, le premier terminal moderne d'Algérie avec une plate-forme portuaire très performante.

- Raison sociale, statut juridique et capital social de BMT SPA

BMT est érigée sous forme de SPA (société par actions), son capital social s'élève à 500000000 da répartis à raison de 51% pour l'EPB et 49% pour PORTEK (Mitsui).

Figure 2. 1 les actionnaires de BMT Spa

1.1. Situation géographique

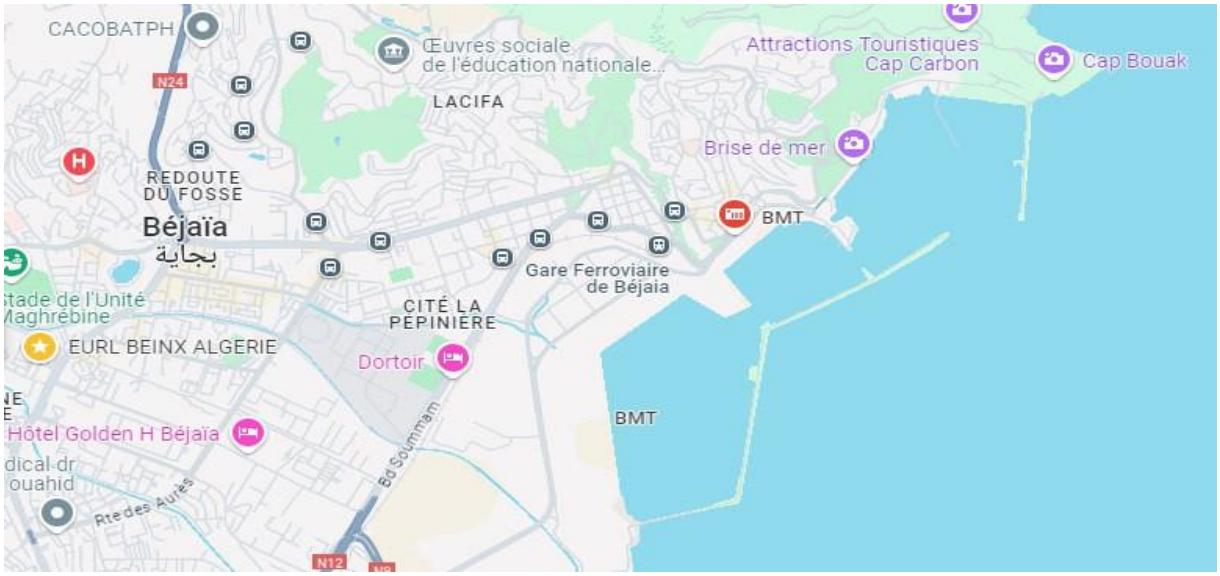

Figure 2.2 Situation géographique BMT Spa

Bejaia méditerranéen terminal SPA est localisée au nouveau quai, dans le bassin sud du port de BEJAIA, ce dernier dessert un hinterland important et très vaste par des infrastructures routières reliant l'ensemble des villes du pays, des voix ferroviaires et d'un aéroport International. Se situant au centre de l'Algérie, sa position géographique est privilégiée, car elle bénéfice d'une baie des plus détritée en méditerranée, afin de servir la région centre ainsi que les hauts plateaux.

BMT SPA se trouve à proximité de la gare ferroviaire, à quelques minutes de l'aéroport de Bejaia, reliée au réseau routier national qui facilite le transport de marchandises conteneurisées de toute nature vers l'arrière-pays et vers d'autres destinations telles que la banlieue d'Alger.

2. Missions, Valeurs et Objectifs de BMT spa

2.1. Missions de BMT Spa

Faire du terminal à conteneurs de BMT un terminal aux normes internationales pouvant rivaliser avec les terminaux les mieux gérés du monde assurant une productivité et une profitabilité garantissent son succès et sa pérennité.

2.2. Les valeurs de BMT Spa

BMT veille au développement et à la gestion de son terminal à conteneurs où l'intégrité, la productivité, l'innovation, la courtoisie, et la sécurité sont de rigueur. BMT est constamment soucieuse des intérêts de ses clients avec lesquels elle partage le souci de performance et de coût. Elle met à la disposition de ses clients des ressources humaines et des moyens nécessaires pour optimiser sa productivité et atteindre des niveaux de performance concurrentielle.

- **INTEGRITE :** Intégrité, en esprit et en forme, est notre règle de conduite et d'engagement. Nous œuvrerons, en toute circonstance et à tout moment, avec le respect absolu de l'intégrité et de L'honnêteté dans notre environnement de travail. Mentir, voler, décevoir, soudoyer, accepter des faveurs, ou faire du favoritisme vont à l'encontre de l'intégrité. L'intégrité est notre Guide et Centre de Gravité.
- **INNOVATION :** Montrer de la curiosité et stimuler les nouvelles idées et la créativité. Rechercher de nouvelles opportunités d'affaires. Avoir le courage de remettre en cause les vérités établies et oser explorer de nouveaux champs et horizons. Comprendre et gérer les risques.
- **PERFORMANCE :** Toujours rechercher les solutions les plus appropriées et partager son expérience. Développer l'expertise de manière continue et ciblée. Faire preuve de compétence commerciale et d'orientation clientèle. Rechercher la simplification. La clarté et éviter les activités qui n'ajoutent pas de valeur. Promouvoir la diversit
- **TENACITE :** Fixer des objectifs ambitieux et respecter ses engagements. Prendre des décisions et s'assurer de leur réalisation. Travailler en équipe, éliminer les barrières et s'imposer des exigences constructives mutuelles. Montrer de la persévérance jusqu'a l'aboutissement et se concentrer sur les points importants.
- **SECURITE :** Contribuer à la protection de la santé, à l'amélioration de la sécurité et des conditions de travail dans notre entreprise. Veiller à l'application des règles relatives à la protection des employés, des clients, et des visiteurs. Protéger et agrémenter l'environnement de travail et respecter la protection de l'environnement et les directives HSE. Assurer la sécurité des biens de nos clients.
- **COURTOISIE :** Le client est la raison d'être de notre simple existence. Lui montrer qu'il est le centre de notre souci et l'objet de notre entreprise. Montrer du respect a l'égard des services, de l'autorité, de la hiérarchie et des règlements établis. Respecter l'éthique du

professionnalisme et de la décence sociale. Respect en tout temps ses collègues.

2.3. Les objectifs de BMT Spa

- Faire du terminal à conteneur de BMT une infrastructure moderne à même de répondre aux exigences les plus sévères en matière de qualité dans le traitement du conteneur.
- La mise à disposition d'une nouvelle technologie dans le traitement du conteneur pour :

- Un gain de productivité.
- Une réduction du cout d'escale.
- Une fiabilité de l'information.
- Un meilleur service des clients.

- Sauvegarder la marchandise des clients.
- Faire face à la concurrence national et international.
- Gagner des parts importantes de marché.

3. Activités et performances de BMT Spa

3.1. Activités de BMT Spa

L'activité principale de BMT Spa est la gestion et l'exploitation du Terminal à conteneurs. Sa mission principale est de traiter dans les meilleures conditions de délais, de coûts et de sécurité, l'ensemble des opérations qui ont rapport avec le conteneur. Pour ce faire, elle s'est dotée d'équipements performants et de systèmes informatiques pour le support de la logistique du conteneur afin d'offrir des services de qualité, efficaces et fiables pour assurer une satisfaction totale des clients.

Bejaia méditerranéen terminal reçoit annuellement un grand nombre de navires pour lesquels elle assure les opérations de planification, de manutention et d'acconage avec un suivi et une traçabilité des opérations.

3.2. Les opérations du terminal

- **Opérations planification**

- Planification des escales
-Planification déchargement /chargement
- Planification du parc à conteneurs
- Planification des ressources : équipes et moyens matériels

- **Opérations de manutention**

- La réception des navires porte-conteneurs
- Le déchargement des conteneurs du navire
- La préparation des conteneurs pour chargement au navire
- Le chargement des conteneurs du navire

- **Opération d'acconage**

- Transfert des conteneurs vers les zones d'entreposage
- Transfert des conteneurs frigorifiques vers la zone « REEFERS »
- Mise à disposition des conteneurs pour visite des services de contrôle aux frontières
- Mise à disposition des conteneurs vides pour empotage
- Suivi des livraisons et des dépotages
- Suivi des restitutions et des mises à quai pour embarquement
- Gestion des conteneurs dans les zones de stockages
-Sécurité absolue sur le terminal

4. Les Différentes structures de BMT

4.1. Direction Générale

A sa tête le Directeur Général qui gère la société BMT Spa, à le pouvoir de décision, administre l'entreprise, assigne des directives au directeur Général Adjoint qui fait la liaison et coordonne entre les différentes directions de BMT.

4.2. Direction des Ressources Humaines et Moyens

La Direction des Ressources Humaines et Moyens est assuré par le DRHM. La DRHM est placée sous l'autorité directe de Directeur Général. Sa mission est de mettre en œuvres des systèmes de gestion intégrée à la stratégie de BMT pour atteindre ses objectifs et qui traduisent une adéquation entre les impératifs économiques et les attentes du personnel.

4.3. Direction des Finances et Comptabilité

La mission de la Direction des Finances et Comptabilité est :

- Veiller à l'adéquation de la politique financière de l'entreprise avec les objectifs globaux ;
- Coordonner et suivre les relations avec les institutions financières ;
- Assurer les relations avec les banques, et les administrations fiscales et parafiscales ;

- Assurer le recouvrement des créances de toute nature ;

- Etablir et suivre les budgets et les plans de financement ;

- Elaborer les plans de financement en assurant l'actualisation et l'exécution ;

- Déterminer, rechercher et négocier les financements les plus appropriés en relation avec les établissements concernés ;
- Veiller à l'application des règles comptables et à la tenue correcte des livres au sein de la société ;
- Elaborer le bilan et autres états financiers et comptables ;

- Etablir et analyser le bilan de fin d'année.

4.4. Direction Marketing

La Direction Marketing est restructurée récemment après la jonction des trois départements (Commercial + Marketing). Sa mission est de :

- Élaboration une politique commerciale et tarifaire.

- Élaboration le plan marketing.

- Coordonner et veiller à la bonne exécution des actions marketing.

- Assumer le rôle de représentation de l'entreprise en Algérie et à l'étranger.

- Participer à l'élaboration du Business Plan.

- Assurer la veille technologique en matière de la communication et de l'information.

- Elaboration des plans d'action de l'entreprise en termes d'efficacité de facturation de recouvrement et d'amélioration de la relation client.

4.5. Direction des Opérations

La mission de la Direction des Opérations est de :

- Assurer la planification des escales, de parc à conteneurs et la planification des ressources, équipes et équipements.
- Prendre en charge les opérations de manutentions, comme la réception des navires porte-conteneurs et leurs chargements et déchargement.
- Suivre les opérations de l'acconage tel que : le suivi des livraisons, dépotages, restitutions du

vide et le traitement des conteneurs frigorifiques.

4.6. Direction Technique

La mission de la Direction Technique est d'assure une maintenance préventive et curative des engins du parc à conteneurs.

Situation des Effectifs au 31/12/2023									
Relation de travail	**Cadre**			**Maitrise**			**Exécution**		
	M	**F**	**T**	**M**	**F**	**T**	**M**	**F**	**T**
Contrat à Durée Indéterminée "CDI"	34	6	**40**	106	14	**120**	458	14	**472**
Contrat à Durée Déterminée "CDD"	6	0	**6**	0	0	**0**	25	0	**25**
Totaux	**40**	**6**	**46**	**106**	**14**	**120**	**483**	**14**	**497**
Contrat à Durée Indéterminée "CDI"	**632**						**95,32**		
Contrat à Durée Déterminée "CDD"	**31**						**4,68**		
Totaux	**663**						**100**		

Tableau 2.1 Situation des effectifs BMT Spa

5. Les certificats de qualité

➢ **ISO 9001 versions 2015**

- La date de certification initiale est le 24 Janvier 2020
- La date de la mise à jour est le 15 Janvier 2023
- La date d'émission du certificat est le 12 mai 2023
- La date d'expiration c'est le 23 Janvier 2026
- L'organisme certificateur : Intertek

Figure 2.3 ISO 9001

- **ISO 14001 versions 2015**

- La date de certification initiale est le 24 Janvier 2020
- La date de la mise à jour est le 15 Janvier 2023
- La date d'émission du certificat est le 12 Mai 2023
- La date d'expiration c'est le 23 Janvier 2026
- L'organisme certificateur : Intertek
- L'organisme accompagnateur : Consultant CETIC

Figure 2.4 ISO 14001

- **ISO 45001 versions 2018 :**

- La date de certification initiale est le 24 Janvier 2020
- La date de la mise à jour est le 15 Janvier 2023
- La date d'émission du certificat est le 15 Janvier 2023
- La date d'expiration c'est le 23 Janvier 2026
- L'organisme certificateur : Intertek
- L'organisme accompagnateur : Consultant CETIC

Figure 2.5 ISO 45001

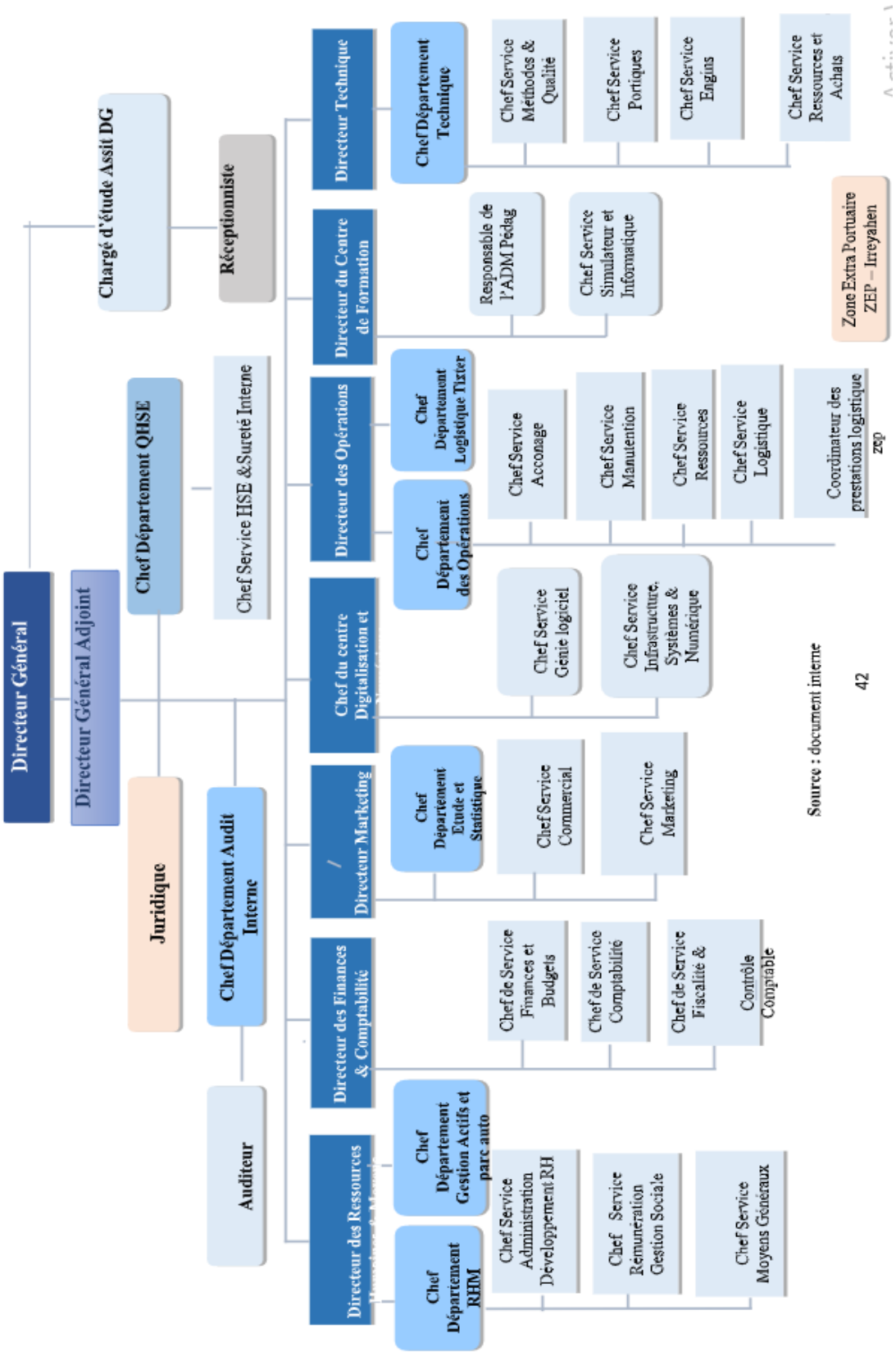

Figure 2.6 Organigramme générale de BMT

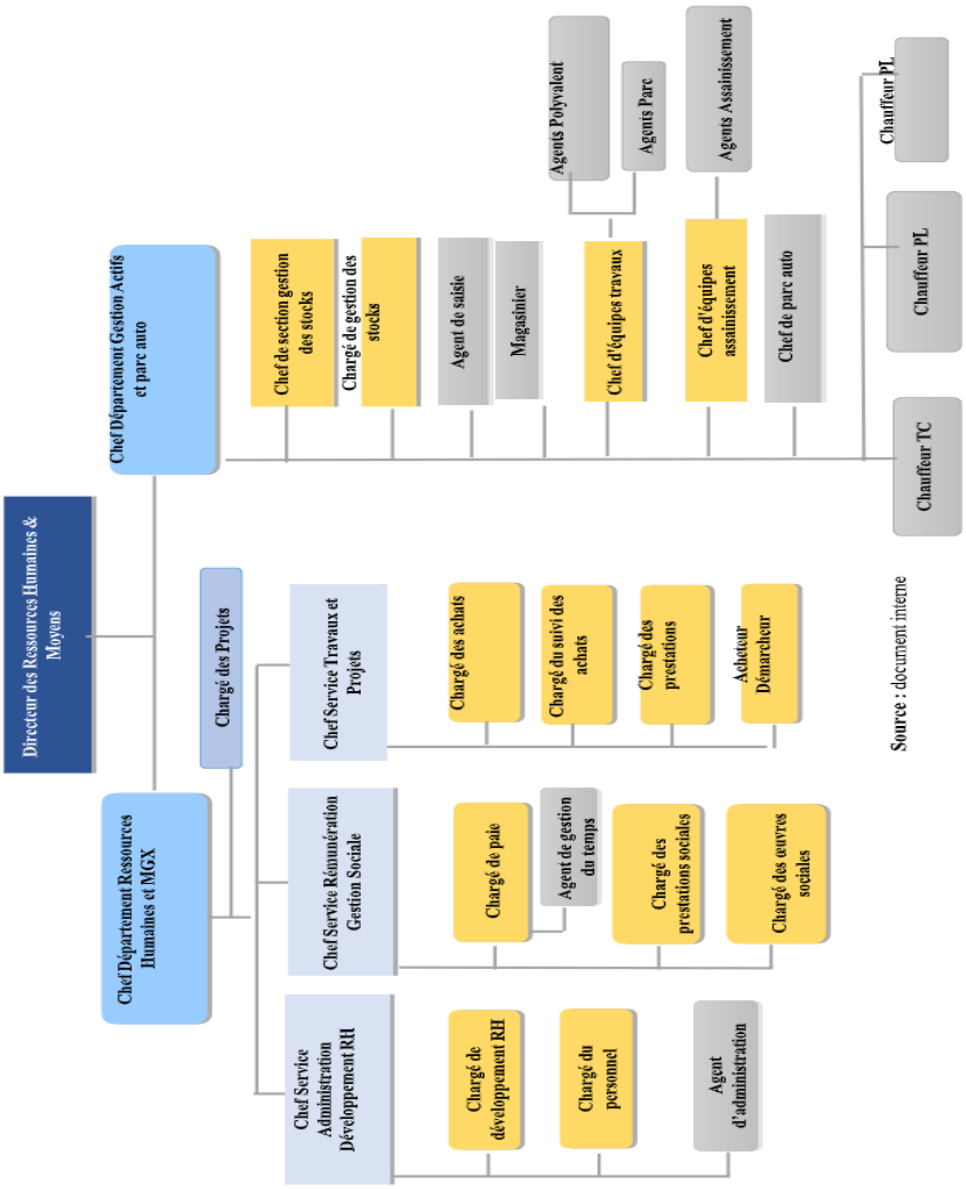

Figure 2.7 organigramme du département RHM

6. Problématique

La problématique de ce mémoire porte sur la sécurisation des accès distants au réseau interne de l'entreprise port BMT à travers l'utilisation d'un VPN. Dans le contexte actuel, où le télétravail et les déplacements professionnels sont de plus en plus courants, il est essential pour les entreprises de garantir que leurs employés puissent accéder aux ressources internes de manière sécurisée, où qu'ils se trouvent. Cela soulève la question de l'authentification des utilisateurs distants, un aspect fondamental pour prévenir les accès non autorisés et protéger les données sensibles de l'entreprise.

Les solutions d'authentification sont multiples et varient en complexité et en niveau de sécurité offert. Parmi les méthodes disponibles, on trouve les authentifications basées sur des certificats, des identifiants et mots de passe, ou des jetons. De même, il existe diverses technologies de VPN, chacune avec ses propres avantages et inconvénients en termes de sécurité, de performance et de facilité de déploiement, telles que IPsec, SSL, et OpenVPN.

Cependant, l'implémentation d'une solution VPN sécurisée nécessite une gestion stricte de l'authentification des utilisateurs. Cette problématique est particulièrement complexe pour les entreprises comme port BMT, qui doivent assurer que leurs employés, accédant au réseau depuis l'extérieur, puissent le faire sans compromettre la sécurité globale du système informatique.

L'objectif de ce mémoire est donc de réfléchir aux différentes méthodes et technologies permettant de mettre en place une infrastructure d'authentification robuste pour les connexions VPN, tout en répondant aux besoins spécifiques de sécurité et de praticité de l'entreprise port BMT. Cette réflexion inclura une analyse des différentes options disponibles, les défis associés à chaque solution, et les critères de choix pour déterminer l'approche la plus adaptée pour cette entreprise.

En somme, ce mémoire vise à répondre à la question suivante : comment peut-on mettre en place un système d'authentification efficace et sécurisé pour les connexions VPN des employés de l'entreprise port BMT, afin de garantir un accès distant sécurisé au réseau interne ?

7. Solution

Face à la diversité des méthodes d'authentification disponibles, ainsi que des technologies VPN, le choix d'une solution adaptée présente une importance capitale. Chaque méthode et technologie présente des avantages spécifiques en termes de sécurité, de performance et de déploiement, influençant directement la résilience du système face aux menaces actuelles en matière de cybersécurité.

Dans ce contexte, la mise en place d'une infrastructure combinant RADIUS pour l'authentification et OpenVPN pour le VPN se positionne comme une solution robuste pour l'entreprise port BMT. Le protocole RADIUS permet une gestion centralisée des identités et des droits d'accès des utilisateurs, intégrant efficacement avec l'infrastructure existante telle qu'Active Directory pour une gestion optimisée. De son côté, OpenVPN offre une connexion VPN sécurisée grâce à des certificats SSL/TLS, assurant un tunnel chiffré entre les utilisateurs distants et le réseau interne.

L'objectif de ce mémoire est donc d'explorer en profondeur les modalités de mise en œuvre de cette solution intégrée, en évaluant les défis techniques et opérationnels rencontrés par l'entreprise port BMT. Cette analyse approfondie permettra de déterminer les critères de choix pertinents pour une implémentation réussie, en tenant compte des exigences spécifiques de sécurité et de praticité propres à l'entreprise.

8. Conclusion

Ce chapitre a présenté BMT Spa, une joint-venture entre l'Entreprise Portuaire de Bejaia et PORTEK System and Equipment, spécialisée dans la gestion des terminaux à conteneurs, en abordant son historique, sa situation géographique, ses missions, valeurs, objectifs et structures organisationnelles. La problématique principale porte sur la sécurisation des accès distants, soulignant l'importance d'une authentification pour protéger les données internes de l'entreprise dans un contexte de télétravail croissant

Chapitre III : Etude des éléments d'authentification

1. Introduction

Dans le cadre complexe de la sécurité des réseaux d'entreprise, établir une infrastructure robuste est importante pour contrôler l'accès aux données sensibles et prévenir les intrusions, tout comme la protection d'un réseau familial contre les menaces internes est essentielle. Les organisations doivent se prémunir contre les risques qui pourraient compromettre la confidentialité et l'intégrité des données.

Ce chapitre propose des solutions en explorant les méthodes et protocoles d'authentification, notamment le protocole RADIUS et le protocole AAA, ainsi que l'utilisation de SSL/TLS, EAP utilisés dans notre étude.et autres outils pour sécuriser efficacement les accès réseau.

2. L'authentification

Il s'agit de vérifier des données concernant une personne ou un processus informatique. L'authentification permet de prouver une identité déclarée. Au sein d'un serveur, un processus de contrôle confirme l'identité et une fois authentifiée, autorise l'accès aux données, applications, bases de données, fichiers ou sites Internet.[13]

2.1. Les méthodes d'authentification

Pour sécuriser l'accès aux systèmes et aux données, plusieurs méthodes d'authentification sont disponibles, Voici quelques-unes de ces méthodes :

2.1.1. Mot de mot passe

La méthode la plus simple et la plus classique pour garantir que seules les personnes autorisées peuvent accéder à une partie du réseau est de sécuriser certaines zones du réseau avec un mot de passe. Beaucoup d'utilisateurs optent pour des mots de passe simples à mémoriser, tels que des dates d'anniversaire, des numéros de téléphone ou des noms d'animaux de

compagnie. D'autres négligent de changer régulièrement leurs mots de passe et ne se préoccupent pas de leur confidentialité.[13]

2.1.2. Les certificats numériques

Un certificat numérique est un fichier permettant de certifier l'identité du propriétaire d'une clé publique, similaire à une carte d'identité.

Une autorité de certification génère un certificat dans une infrastructure à clés publiques, ce qui lui permet de créer des certificats numériques contenant la clé publique en question. Le format reconnu actuellement est le format X509 version 3 et il contient les informations suivantes [14]

- Sa version qui est la 3 actuellement.
- Le nom de l'entité de certification ayant émis le certificat.
- Le nom et le prénom de la personne.
- Son entreprise et Son service.
- Le numéro de série et le type de certificat.
- Les dates de validité du certificat.
- La clé publique qui va être transmise.
- L'adresse e-mail de la personne propriétaire.
- La signature électronique.

La signature électronique est produite par l'autorité de certification en utilisant les informations personnelles, comme le nom, le prénom, l'adresse e-mail, le pays du demandeur, etc. à l'aide de sa propre clé privée.

2.1.3. Les jetons

Les jetons sont une méthode d'authentification qui permet de vérifier l'identité d'un utilisateur en échange d'un jeton d'accès unique. Pendant toute la durée de vie du jeton, les utilisateurs ont alors la possibilité d'accéder au site Web, à l'application ou à la ressource sans avoir à saisir à nouveau leurs informations d'identification. Il est constitué de trois composants clés : [15]

- **L'en-tête :** définit le type de jeton utilisé, ainsi que l'algorithme de signature impliqué.

- **La charge :** utile est chargée de définir l'émetteur du jeton et les détails d'expiration du jeton. Il fournit également des informations sur l'utilisateur ainsi que d'autres métadonnées.
- **La signature** : vérifie l'authenticité d'un message et qu'un message n'a pas changé pendant le transit.

2.2. Les protocoles d'authentifications

L'authentification repose souvent sur des protocoles spécifiques qui garantissent la confidentialité et l'intégrité des échanges d'informations lors de l'identification. Ci-dessous, nous présenterons quelques-uns de ces protocoles**.**

2.2.1. Le protocole RADIUS

RADIUS est un protocole mis au point par Livingston Enterprise qui est devenu une norme de fait décrite par les RFC2865 et 2866. Il repose sur une architecture client/serveur et vise à offrir des services d'authentification, d'autorisation et de gestion des comptes pour l'accès à distance au réseau.[16]

2.2.2. Le protocole TACACS+

Il s'agit d'un serveur d'authentification qui permet de centraliser les autorisations d'accès au sein d'un réseau. CISCO Système a créé ce Protocole qui a pris la place de TCACAS et XTACACS. TACACS+ offre la possibilité de vérifier l'identité des utilisateurs distants et, grâce au modèle AAA, autorise et surveille également leurs actions au sein du réseau local.[13]

2.2.3. Le protocole Kerberos

Kerberos est un protocole d'authentification réseau utilise un mécanisme de clés secrètes (chiffrement symétrique) et des tickets plutôt que des mots de passes en clair, afin d'éviter toute interception frauduleuse des mots de passe des utilisateurs. [17]

2.3. Comparaison des protocoles

Critère	**Radius**	**TACACS+**	**Kerberos**
Fonction principale	Authentification, Autorisation et comptabilité (AAA)	Authentification, Autorisation et comptabilité (AAA)	Authentification, Autorisation
Architecture	Client-serveur	Client-serveur	Clé de chiffrement symétrique distribuée (KDC)
Chiffrement	Utilise UDP, le chiffrement n'est pas obligatoire	Chiffrement Complet de bout En bout (TCP)	Utilise le chiffrement symétrique (Tickets)
Transport	UDP	TCP	UDP ou TCP
Ports utilisés	1812 (authentification)/ 1813 (comptabilité)	49	88 (KDC)
Composantes principales	Serveur RADIUS , client RADIUS (NAS)	Serveur TACACS+, client TACACS+	KDC (Key Distribution Center),Ticket Granting Ticket (TGT)
Interopérabilité	Largement utilisé pour les VPN et les réseaux sans fil	Utilisé principalement dans les réseaux Cisco	Utilisé dans les environnements Microsoft et les systèmes basés sur Unix

Tableau 3.1 Comparaison des protocoles

3. Protocole RADIUS

RADIUS est utilisé pour faire de l'AAA avec des utilisateurs qui se connectent à Internet via des modems téléphoniques. Il transmet des informations au serveur d'accès NAS (Network Access Server) qui permet de les authentifier (login/password). En cas d'authentification correcte, le serveur autorise l'accès de l'utilisateur au réseau, sinon la connexion est rejetée.

RADIUS a été conçu pour supporter un nombre ilimité d'équipements et d'utilisateurs. De nos jours, les opérateurs doivent être en mesure de fournir des services et d'authentifier des milliers d'utilisateurs qui utilisent des technologies variées. Ils doivent également avoir la capacité de fournir des services à des utilisateurs provenant de différents opérateurs, de préférence de manière sécurisée.[18]

3.1. Architecture Radius [19]

Trois éléments principaux composent l'architecture RADIUS

- **Le client RADIUS :** en règle générale, il s'agit d'un dispositif réseau tel qu'un routeur, un point d'accès Wi-Fi ou un serveur d'accès distant (NAS - Network Access Server). Les demandes d'authentification des utilisateurs sont transmises par le client RADIUS au serveur RADIUS.
- **Le serveur RADIUS :** c'est le serveur central qui est responsable de la gestion des services d'authentification, d'autorisation et de comptabilité. Il possède une base de données qui stocke les informations d'identification des utilisateurs, telles que les noms d'utilisateur et les mots de passe, etc...
- **Les utilisateurs :** sont les entités qui sollicitent l'accès au réseau et dont l'authentification est prise en charge par le serveur RADIUS.

3.2. Fonctionnement de Radius

Radius repose sur un système client/serveur qui gère les accès d'utilisateurs distants à un réseau en utilisant le protocole UDP et les ports 1812 et 1813. Le protocole Radius est principalement basé sur un serveur (le serveur Radius), connecté à une base d'identification (base de données, Active Directory, annuaire LDAP, etc.) et un client Radius, appelé NAS, qui joue le rôle d'intermédiaire entre l'utilisateur final et le serveur. Les échanges entre le client Radius et le serveur Radius sont sécurisés et authentifiés grâce à un secret partagé.[16]

La figure 3.1 illustre le mécanisme d'authentification sur le serveur Radius

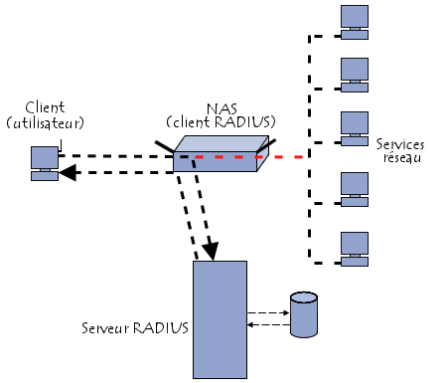

Figure 3.1 Mécanisme d'authentification sur radius [20]

- **Scénario de fonctionnement [21]**

- **Demande d'Accès :** un utilisateur envoie une requête au NAS pour autoriser une connexion à distance.
- **Transmission de la Demande :** le NAS achemine la demande au serveur RADIUS.
- **Consultation de la Base de Données** : le serveur RADIUS consulte sa base de données d'identification pour déterminer le type de scénario d'identification demandé pour l'utilisateur.
- **Réponse du Serveur :** le serveur RADIUS retourne l'une des quatre réponses suivantes :

ACCEPT : l'identification a réussi.

REJECT : l'identification a échoué.

CHALLENGE : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un "défi" (en anglais "challenge").

CHANGE PASSWORD : e serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

- **Phase d'Autisation :** suite à cette phase d'authentification, le serveur RADIUS retourne les autorisations de l'utilisateur.

3.3. Format du paquet Radius [22]

Radius utilise quatre types de paquets pour assurer les transactions d'authentification.Tous les paquets ont le format général indiqué par la figure suivante:

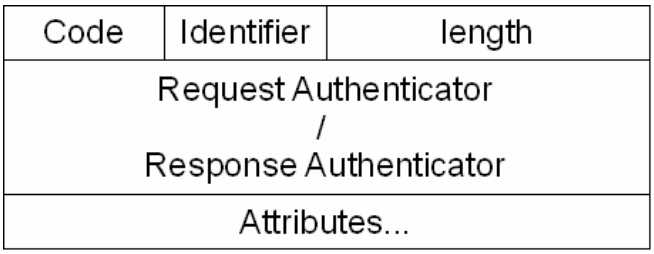

Figure 3.2 En-tête d'un paquet Radius [22]

- **Code :** définit le type de trame (acceptation, rejet, challenges, requête).
- **Identifier :** associe les réponses reçues aux requêtes envoyées.
- **Length :** champ longueur.
- **Authentificator :** champ d'authentification comprenant les éléments nécessaire.
- **Attribuées :** Ensemble de couples (attribut, valeur).

3.4. Avantages de Radius [23]

Radius présente de nombreux atouts pour les administrateurs réseau, les principaux sont

- **Sécurité améliorée :** offre des services d'authentification et d'autorisation solide, garantissant ainsi que seuls les utilisateurs autorisés peuvent accéder aux ressources du réseau. Ceci assure la protection contre tout accès non autorisé et diminue le risque de violation des données.
- **Gestion centralisée :** permet une gestion centralisée des comptes utilisateurs, ce qui facilite la gestion de l'accès aux ressources réseau. Ceci offre une économie de temps et diminue le risque d'erreurs.
- **Évolutivité :** Radius est hautement évolutif, ce qui signifie qu'il peut être utilisé pour gérer l'accès à des réseaux de toute taille. Cela en fait une option parfaite pour les entreprises de toutes tailles.

- **Compatibilité** : Radius est une norme très répandue qui peut être utilisée avec une variété d'équipements réseau, tels que des serveurs, des routeurs et des points d'accès sans fil.

4. Protocole AAA

Le protocole AAA est essentiel dans les infrastructures réseau pour gérer l'authentification, l'autorisation et la comptabilité des utilisateurs et des dispositifs connectés. Voici sa définition ainsi que son architecture détaillée.

4.1. Définition

AAA a été introduit dans les années 1990 à la suite de l'effort de normalisation issue de la collaboration entre l'IEEE et l'IETF à travers leur groupe de travail AAA. Cette équipe a créé des applications AAA, qui sont un système de mécanismes, de protocoles et d'architectures visant à gérer les identités.[24]

4.2. L'architecture AAA

AAA fournit des services de contrôle d'accès à travers de multiples technologies de réseaux et de plateformes. Ces services se décomposent en trois points distincts :

- **Authentication :** processus visant à assurer que l'utilisateur qui cherche à accéder au réseau possède un compte valide. On compare le mot de passe de l'utilisateur aux entrées d'une base de données centrale.[18]
- **Authorization :** offre à l'exploitant du réseau la possibilité de déterminer les services réseau dont les utilisateurs finaux peuvent bénificier . .Un utilisateur peut par exemple demander une bande passante spécifique, et le serveur AAA décidera si cette demande est autorisée ou non.[18]
- **Accounting :** le serveur AAA peut collecter des informations sur l'utilisation des ressources, ceci permet à un opérateur de facturer un Utilisateur en fonction de sa consommation. Les clients utilisent des routeurs ou des serveurs d'accès au réseau pour être hébergés.[18]

5. Le protocole EAP

Le protocole EAP joue un rôle central dans l'authentification sécurisée des utilisateurs et des dispositifs réseaux.

5.1. Définition

Le protocole EAP est un protocole de communication réseau conçu pour permettre l'utilisation de diverses méthodes d'authentification pour les technologies d'accès réseau

sécurisées. Il est conçu pour être extensible, permettant ainsi d'ajouter de nouvelles méthodes d'authentification sans modifier le protocole de base. Son objectif est de protéger la sécurité des réseaux locaux sans fil (802.1X) et câblés, de l'accès à distance, ainsi que des réseaux privés virtuels (VPN). **[25]**

5.2. Méthodes d'authentifications

Les méthodes d'authentification EAP incluent :

Méthode EAP	**Description de l'authentification**
EAP-MD5	Authentification avec un mot de passe.
EAP-TLS	Authentification avec un certificat électronique.
EAP-PEAP	Authentification avec nimporte quelle méthode d'authentification EAP, au sein d'un tunnel TLS.
EAP-MSCHAP v2	Authentification avec un mot de passe.

Tableau 3.2 Méthodes d'authentification

Pour notre cas, nous avons utilisé deux méthodes d'authentification spécifiques : MSCHAPv2 pour l'authentification par mot de passe et TLS pour l'authentification via certificat électronique. Leurs définitions sont présentées ci-dessous.

- **EAP-TLS :** (Extensible Authentication Protocol - Transport Layer Security) est un standard ouvert de l'IETF (Internet Engineering Task Force) qui permet une authentification sécurisée entre un client et un serveur. En utilisant le protocole TLS, il crée un tunnel assurant ainsi l'authentification mutuelle entre les deux parties, ce qui signifie que chaque partie peut vérifier l'identité de l'autre.

EAP-TLS offre un cryptage robuste, ce qui renforce la sécurité des communications. Il est également couramment employé dans des environnements nécessitant une sécurité élevée, tels que les réseaux sans fil d'entreprise et les VPN.**[26]**

- **EAP-MSCHAPv2** : est une méthode d'authentification utilisée dans le contexte du protocole EAP Elle est basée sur le protocole CHAP (Challenge Handshake Authentication Protocol) et utilise une version améliorée de MSCHAP (Microsoft Challenge-Handshake Authentication Protocol) pour l'authentification des utilisateurs.

L'authentification est réalisée par un challenge envoyé par le serveur, qui est déchiffré par le client avec une clef secrète. Si le client arrive à déchiffrer le challenge, cela prouve son identité. Concernant le cryptage, Les informations circulent dans un canal sécurisé, ce qui rend l'authentification plus robuste**.[25]**

Ces méthodes permettent à un client VPN de s'authentifier de manière sécurisée pour accéder à notre réseau.

6. VPN

Un VPN, ou réseau privé virtuel, établit une connexion privée entre des appareils à travers Internet. Les VPN permettent de transmettre des données de façon sécurisée et anonyme sur des réseaux publics. Ils fonctionnent en masquant les adresses IP des utilisateurs et en cryptant les données de manière qu'elles soient illisibles pour toute personne non autorisée à les recevoir.[27]

6.1. Fonctionnement

Lorsqu'un VPN est activé, une connexion au serveur VPN s'établit. Dès lors, toutes les données qui entrent et sortent d'un appareil passent par un tunnel chiffré grâce à un processus d'encapsulation. Ce chiffrement sécurise la connexion en rendant le trafic illisible, à l'exception de ceux qui ont la clé de chiffrement.[27]

6.2. Les différentes architectures des VPN

- **Poste à poste** : C'est le cas d'utilisation le plus simple. L'objectif est d'établir une connexion entre deux serveurs. Le cas d'utilisation peut être le besoin de synchronisation de base de données entre deux serveurs d'une entreprise, chacun ayant un accès internet. Il n'est pas nécessaire d'avoir un accès réseau complet dans ce type de situation.[28]

Figure 3.3 VPN poste à poste [29]

- **Poste à site** : un utilisateur à distance n'a qu'à installer un client VPN sur son PC pour accéder au site de l'entreprise via sa connexion Internet. Ce type d'utilisation est favorisé par le développement de l'ADSL.Cependant, Il est important de ne pas autoriser l'accès à Internet depuis le poste « localement ». En raison de la sécurité, il sera nécessaire de naviguer à travers le réseau de l'entreprise.

  Ce point est essential et s'inscrit dans une réflexion plus large sur la sécurité des sites connectés via VPN. Lorsque les niveaux de la sécurité sont différents, lorsque les deux sites sont reliés, le niveau de sécurité le plus bas est appliqué aux deux. Si une faille de sécurité est présente sur un site (ou sur un poste normale), elle peut être exploitée.[28]

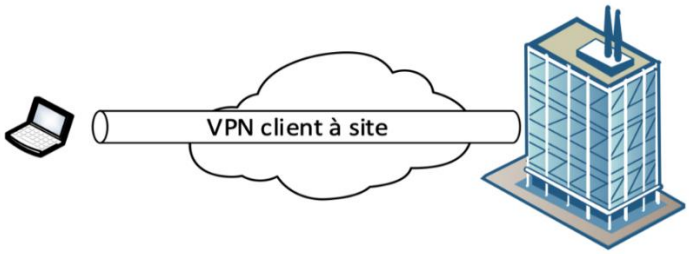

Figure 3.4 VPN poste à site [29]

- **Site à site :** elle correspond à un type d'infrastructure de réseau étendu, où l'interconnexion entre les VPN remplace et améliore les réseaux privés déjà en place. Elle est employée afin de connecter un site à des filiales de manière sécurisée et économique.[28]

  Électrique et Informatique, Département Électronique). Dirigé par Leila Lehdir. Tizi Ouzou, Algérie.

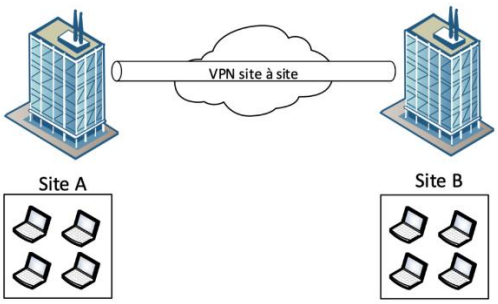

Figure 3.5 VPN site à site[29]

6.3. Le protocole OpenVPN

OpenVPN est un protocole cryptographique qui accorde une grande importance à la sécurité. C'est un logiciel open source, cela permet aux utilisateurs de vérifier eux-mêmes qu'il n'y a rien dans les protocoles qui pourrait compromettre leur sécurité. Les utilisateurs avertis peuvent même y apporter des modifications. De plus, OpenVPN est un protocole extrêmement compatible qui propose de multiples options de configuration.[30]

6.4. Le protocole SSL

Le protocole SSL était le protocole cryptographique le plus couramment employé afin de garantir la sécurité des communications sur Internet Il a été largement remplacé par TLS, mais le terme "SSL" est souvent utilisé de manière interchangeable pour faire référence à SSL/TLS. SSL permet de créer une connexion chiffrée entre un client (comme un navigateur web) et un serveur (comme un site web), assurant ainsi la confidentialité, l'intégrité et l'authenticité des données échangées. [31]

7. Firewall Pfsense

Avant de définir spécifiquement le pare-feu pfSense il est important de clarifier ce qu'est un pare-feu.

7.1. Définition d'un firewall

Un firewall (ou pare-feu) est un dispositif de sécurité réseau, matériel ou logiciel, qui surveille et contrôle le trafic entrant et sortant d'un réseau informatique selon un ensemble de

règles de sécurité prédéfinies, il agit comme une barrière de protection en filtrant les paquets de données échangés entre les deux réseaux. Il analyse le trafic au niveau des ports, qui sont les points d'entrée où les informations sont échangées avec des appareils externes. Le firewall autorise, bloque ou rejette les connexions en fonction des règles configurées.[32]

Un firewall ne suffit pas à lui seul pour assurer la sécurité d'un réseau. Il doit être accompagné d'une politique de sécurité globale et d'une veille constante pour être efficace face aux menaces évolutives.

7.2. Définition Pfsense

Pfsense est une plateforme open source de pare-feu et de routeur qui repose sur FreeBSD. Elle propose une variété de caractéristiques de sécurité et de gestion réseau, comme le filtrage des paquets, la gestion des VPN, le portail captif et la surveillance du trafic. Grâce à son interface web intuitive, sa souplesse et sa possibilité de personnalisation, Pfsense est fréquemment employé pour assurer la sécurité des réseaux d'entreprise et domestiques.[33]

Pfsense est une solution polyvalente et évolutive, adaptée à des contextes divers, permettant une gestion efficace et sécurisée des infrastructures réseau. Ses capacités avancées en matière de sécurité et de gestion du trafic en font un choix privilégié pour les administrateurs réseau cherchant à optimiser et sécuriser leur environnement informatique.

7.3. Fonctionnalités d'un Pfsense

Pfsense offre la possibilité de concevoir un pare-feu et un routeur sécurisé. Voici les principales fonctionnalités de Pfsense [33]

- **Pare feu**
  - Contrôle des échanges sur le réseau
  - Filtrage des IP sources et des destinations
  - Support de NAT, IPv6, DHCP, VPN

- **Routeur**
  - Support de routage et de NAT
  - Mise en place des connexions entre les divers réseaux.
  - Mise en place de fonctionnalités de routage et de NAT afin de relier plusieurs réseaux informatiques différents.

- **VPN**
  - Support de VPN
  - Gestion des connexions VPN
  - Mise en place de fonctionnalités de VPN afin de garantir la sécurité des échanges sur le réseau.

- **Portail Captif**
  - Support de portail captif.
  - Gestion des utilisateurs.
  - Mise en place de fonctionnalités de portail captif afin de gérer les accès au réseau.

- **Gestion des Certificats**
  - Gestion des certificats SSL/TLS.
  - Gestion des certificats pour assurer la sécurité des échanges sur le réseau.

- **Gestion des utilisateurs**
  - Gestion des utilisateurs.
  - Contrôle des accès aux ressources réseau.
  - Mise en place de modules de gestion des utilisateurs afin de garantir la sécurité de l'accès au réseau.

Pfsense est un outil puissant et convivial qui offre une grande variété de fonctionnalités pour sécuriser et gérer les réseaux informatiques.

8. Conclusion

La sécurisation des réseaux d'entreprise requiert une infrastructure solide avec des protocoles d'authentification comme RADIUS et d'autres technologies. Ce chapitre a exploré ces concepts théoriques essentiels. Le prochain chapitre se concentrera sur l'implémentation pratique d'un serveur d'authentification RADIUS avec un VPN, permettant ainsi de mettre à l'épreuve nos connaissances dans un environnement opérationnel et d'améliorer la sécurité de notre réseau. Cette mise en pratique se déroulera sous GNS3, offrant ainsi une simulation réaliste pour tester et optimiser notre solution de sécurité réseau.

Chapitre IV : mise en œuvre et réalisation

1. Introduction

Dans ce chapitre, nous passons de la théorie à la pratique en mettant en place un serveur d'authentification RADIUS dans un environnement simulé à l'aide de GNS3. Après avoir exploré les concepts fondamentaux de l'authentification réseau et du protocole RADIUS dans les chapitres précédents, nous abordons maintenant la phase cruciale de l'implémentation concrète. En utilisant GNS3, nous détaillons les étapes de configuration en intégrant des composants clés tels que pfSense, Windows Server 2016 et d'autres périphériques réseau. Après avoir présenté la topologie simulée, nous décrivons chaque étape de configuration avec des captures d'écran pour une meilleure compréhension. Enfin, des tests d'authentification sont effectués pour évaluer l'efficacité du serveur RADIUS.

2. Méthodologies de réalisation

Pour notre projet, nous avons adopté une méthodologie en quatre étapes principales : d'abord, l'installation des machines physiques, suivie de l'installation des machines virtuelles, puis la configuration des systèmes, et enfin la réalisation des tests. Voici la figure 4.1 qui présente notre méthodologie.

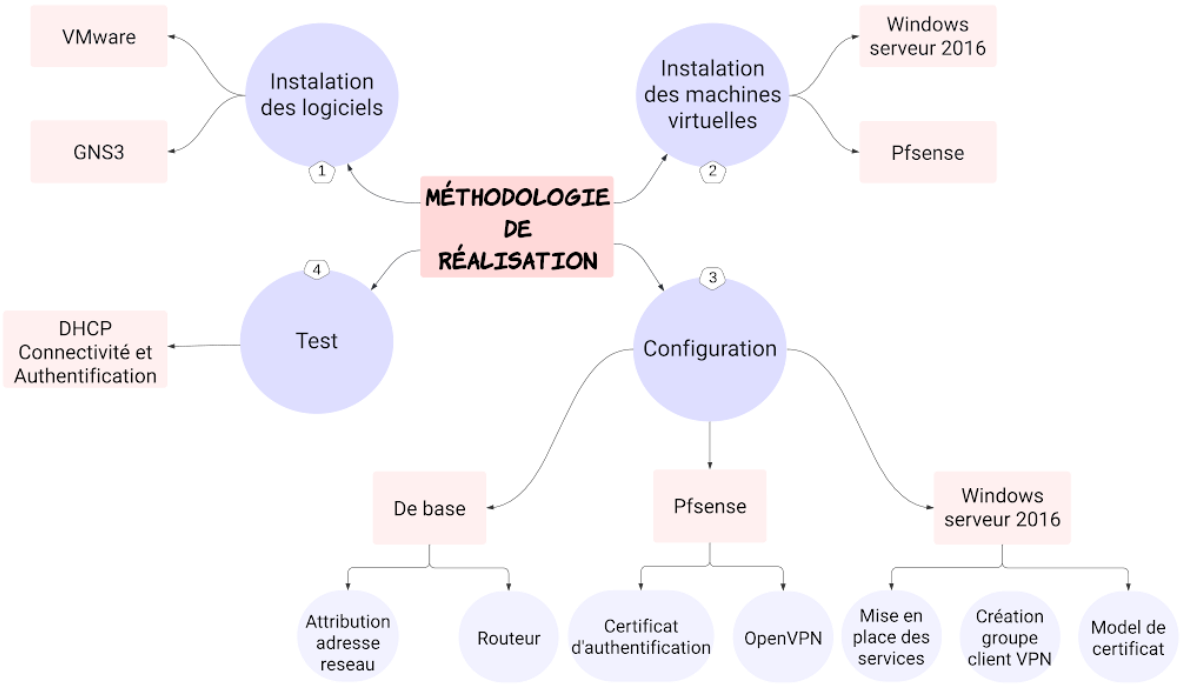

Figure 4.1 Méthodologie et réalisation

2.1. Présentation et installation des outils utilisés

Avant d'entrer dans la configuration détaillée, nous commencerons par présenter les outils utilisés et décrire comment nous avons installés pour préparer notre environnement de travail

2.1.1. GNS3

Le simulateur de réseau graphique GNS3 offre la possibilité de créer, configurer, tester et résoudre des problèmes complexes dans des réseaux virtuels. Les ingénieurs réseau, les étudiants en informatique et les professionnels de l'informatique l'utilisent principalement pour concevoir des environnements de laboratoire réalistes et tester des configurations de réseau sans avoir besoin de matériel physique. Voici le lien officiel pour l'installation « gns3.com », la figure 4.2 montre le logo de GNS3.

Figure 4.2 Logo GNS3 [34]

2.1.2. VMware

VMware est à la fois une entreprise et un ensemble de technologies qui offrent la possibilité de virtualiser des ressources informatiques. Les produits qu'il propose simplifient la gestion des infrastructures informatiques en proposant des solutions performantes, adaptables et sécurisées pour la création et la gestion de machines virtuelles. Ces technologies jouent un rôle crucial pour les entreprises qui désirent maximiser leurs ressources et mettre en place des stratégies de cloud computing. Voici le lien officiel pour l'installation « docs.vmware.com », la figure 4.3 montre le logo de VMware

Figure 4.3 Logo VMware [35]

Après avoir installé les deux logiciels précédents, suivez ces étapes pour faire la liaison entre GNS3 et VM

- Il faut aller dans **Édition > Préférences > GNS3 VM**.
- Puis cocher l'option **Activer le GNS3 VM** et configurez les paramètres VMware.
- Enfin Démarrer la GNS3 VM.

2.2. Installation des images ISO

Nous avons téléchargé les images ISO de pfSense, Windows Server 2016, routeur, switch et d'autres logiciels nécessaires depuis leurs sites officiels, en veillant à choisir des versions compatibles avec GNS3. Ensuite, nous avons importé ces images dans GNS3 en accédant à l'onglet "Préférences" puis à la section "Images IOS", où nous avons cliqué sur "Ajouter" pour sélectionner et importer les images téléchargées.

Après l'importation, nous avons configuré les périphériques virtuels en sélectionnant les images ISO correspondantes et en ajustant les paramètres spécifiques comme la quantité de RAM, le nombre de cœurs CPU et les interfaces réseau. Enfin, nous avons correctement connecté les interfaces réseau des périphériques dans notre topologie GNS3, les reliant aux commutateurs, routeurs, et autres périphériques.

2.2.1. Installation Windows Server 2016

Windows Server 2016 est un système d'exploitation serveur développé par Microsoft il est conçu pour les entreprises qui recherchent des solutions de serveur robustes, sécurisées et hautement flexibles pour soutenir leurs applications et infrastructures modernes. Voici quelques étapes de l’installation de Windows server dans la figure 4.4.

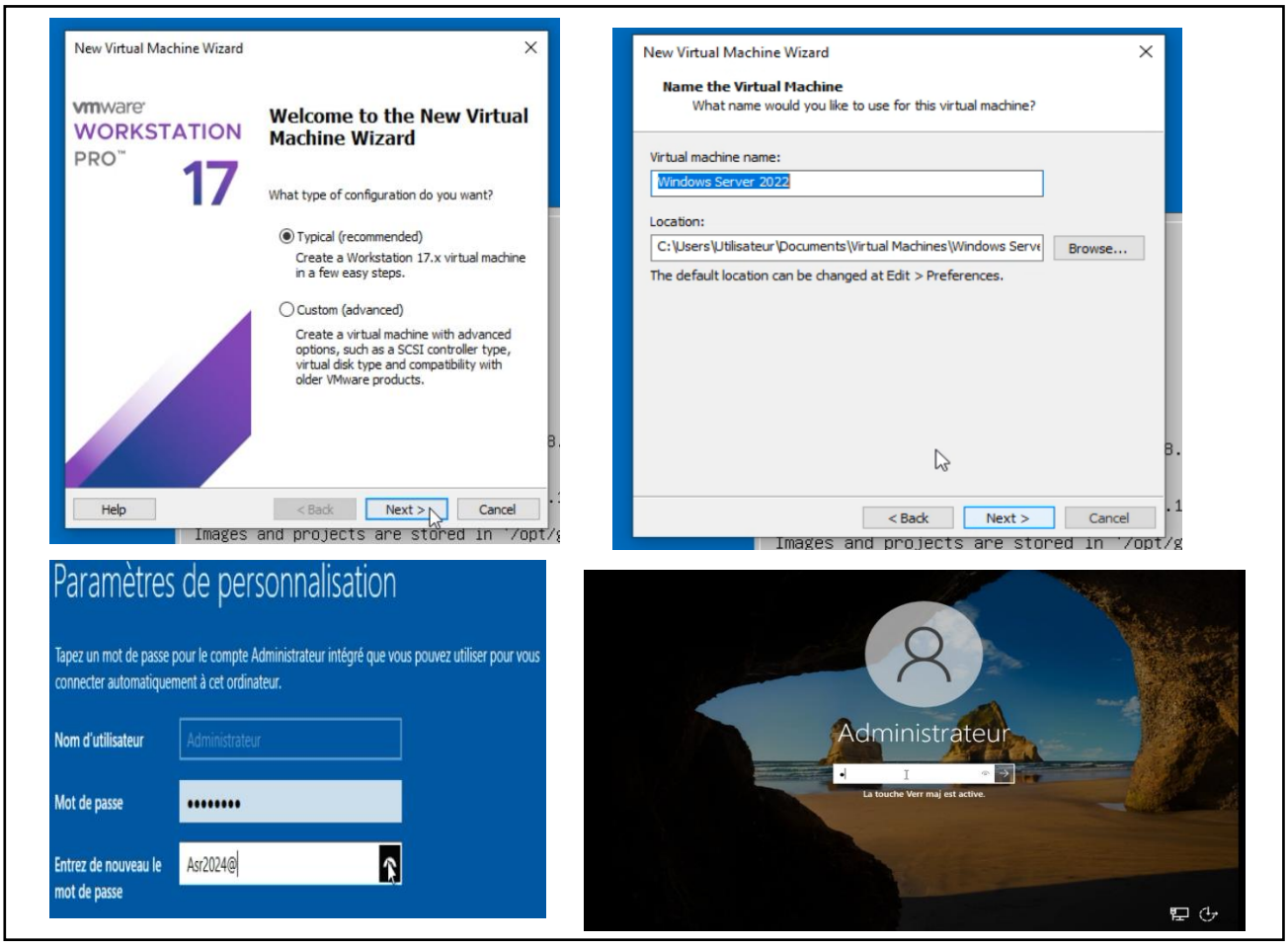

Figure 4.4 Installation Windows Server

2.2.2. Topologie mise en œuvre

Dans la figure 4.5, nous présentons notre topologie réseau. Elle comprend un réseau externe WAN, qui contient un routeur, un client VPN et un NAT, ainsi qu'un réseau LAN, qui inclut un pare-feu, plusieurs ordinateurs et un serveur Windows qui permet d'authentifier notre client VPN.

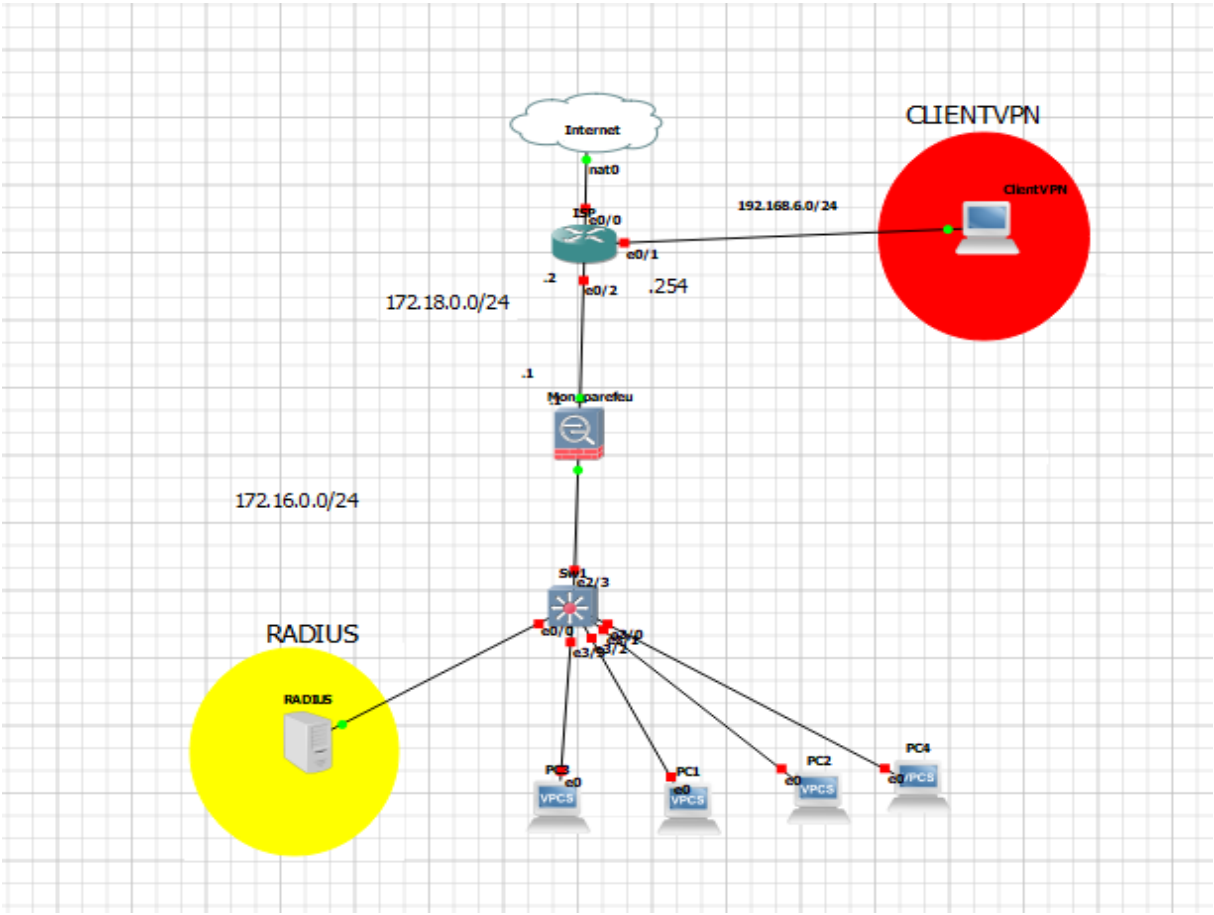

Figure 4.5 Topologie réseau

2.3. Configurations

Nous abordons maintenant la partie importante qui est la configuration, ou nous détaillons toutes les étapes et paramètres configurés

2.3.1. Configurations de base

- **Les adresse IP du réseaux LAN et WAN**

On a attribué des adresses IP réseau de manière statique dans VMware en cliquant sur « Edit » puis dans la fenêtre « Virtuel Network Editor » on tape les adresses suivantes, LAN « 172.16.0.0 », WAN « 172.18.0.0 », comme le montre la figure 4.6 ci-dessous.

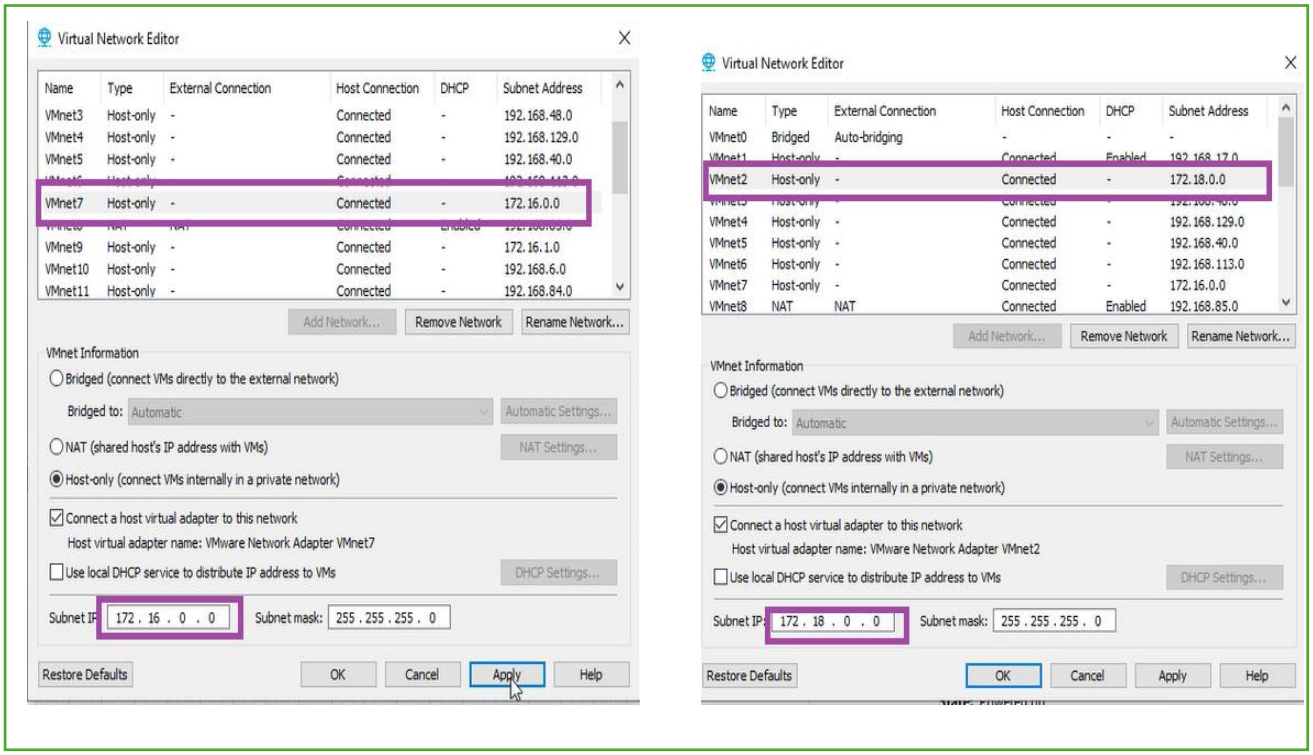

Figure 4. 6 Adresse LAN & WAN

➢ Routeur

Tout d'abord, nous avons configuré notre routeur pour attribuer une adresse IP à l'interface Ethernet 0/0 via DHCP.

```
ISP#show  ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.122.190 YES DHCP   up                    up
Ethernet0/1                unassigned      YES NVRAM  administratively down down
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
Ethernet1/0                unassigned      YES NVRAM  administratively down down
Ethernet1/1                unassigned      YES NVRAM  administratively down down
```

Figure 4. 7 Adresse Ethernet 0/0

Nous avons testé la connectivité Internet depuis le routeur, comme le montre la figure 4.8.

```
ISP#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/50/56 ms
ISP#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 45/47/52 ms
```

Figure 4. 8 Accès Internet depuis routeur

Nous avons attribué une adresse IP pour l'interface Ethernet 0/1 d'une manière statique.

```
ISP(config-if)#ip address 192.168.6.254 255.255.255.0
ISP(config-if)#end
ISP#
ISP#
ISP#wr
```

Figure 4.9 Adresse Ethernet 0/1

La commande « Ip nat inside » permet de traduire les adresses IP internes (privées) en adresses IP externes (publiques)

```
ISP(config)#interface  range ethernet 0/1-2
ISP(config-if-range)#ip nat insi
ISP(config-if-range)#ip nat inside
ISP(config-if-range)#exit
```

Figure 4.10 Ip nat inside

Cette commande montrée dans la figure 4.11 permet à toutes les adresses IP de la plage 192.168.6.0 à 192.168.6.255 et 172.18.0.0 à 172.18.0.255 de passer par la liste de contrôle d'accès (ACL) standard nommée "NAT" spécifie que seuls les 8 derniers bits de l'adresse IP peuvent varier.

```
ISP(config)#ip access-list st
ISP(config)#ip access-list standard NAT
ISP(config-std-nacl)#per
ISP(config-std-nacl)#permit 192.168.6.0 0.0.0.255
ISP(config-std-nacl)#per
ISP(config-std-nacl)#permit 172.18.0.0 0.0.0.255
ISP(config-std-nacl)#exit
```

Figure 4.11 ip access-list

2.3.2. Configuration PfSense

Nous avons configuré les adresses des interfaces LAN et WAN dans pfSense en suivant les étapes montrer dans la figure 4.12 ci-dessous :

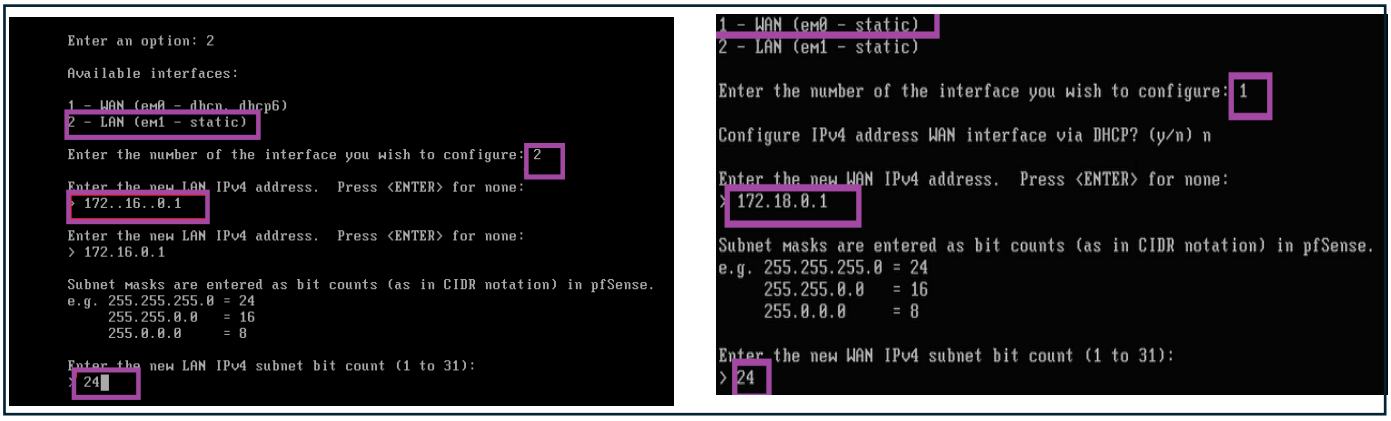

Figure 4.12 adresses interface LAN WAN

Nous avons défini la plage d'adresses pour le réseau LAN afin d'attribuer des adresses aux PC en utilisant DHCP.

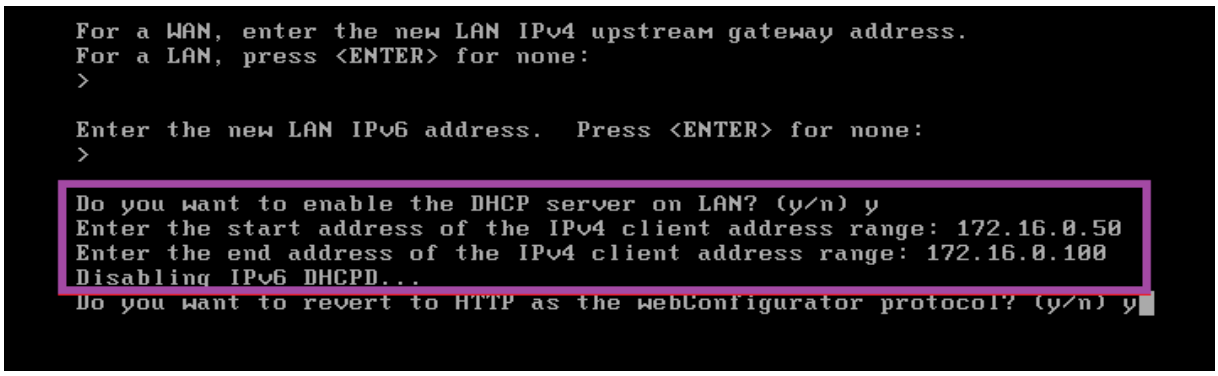

Figure 4. 13 plage d'adressage

Pour accéder à l'interface de gestion de pfSense, nous utilisons un navigateur web. Dans la barre d'adresse du navigateur, nous saisissons l'adresse IP spécifique de l'interface pfSense, qui est 172.16.0.1, pour configurer et gérer diverses fonctionnalités. Le nom d'utilisateur par défaut est "admin" et le mot de passe est "pfSense". Pour des raisons de sécurité, nous avons modifié le mot de passe, qui est désormais "admin123".

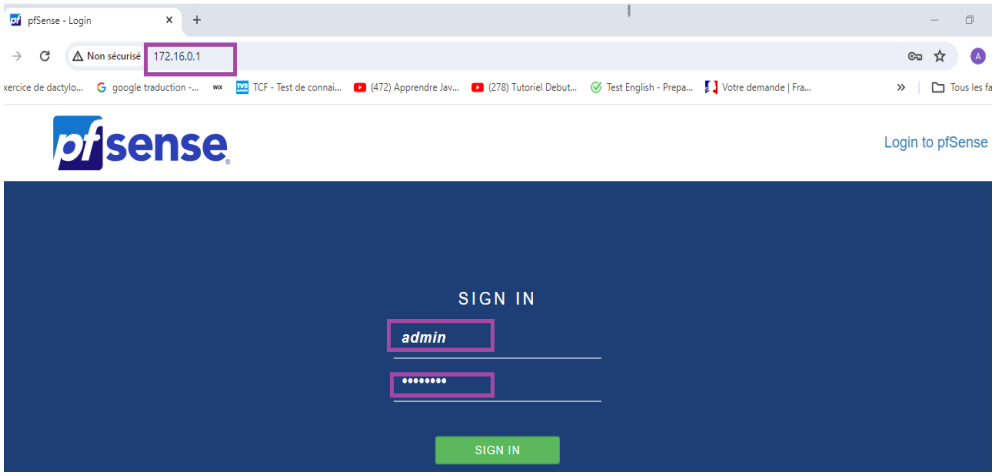

Figure 4.14 Interface d'authentification pfSense

Après avoir saisi le nom d'utilisateur et le mot de passe, la fenêtre principale s'affiche, comme le montre la figure 4.15 ci-dessous.

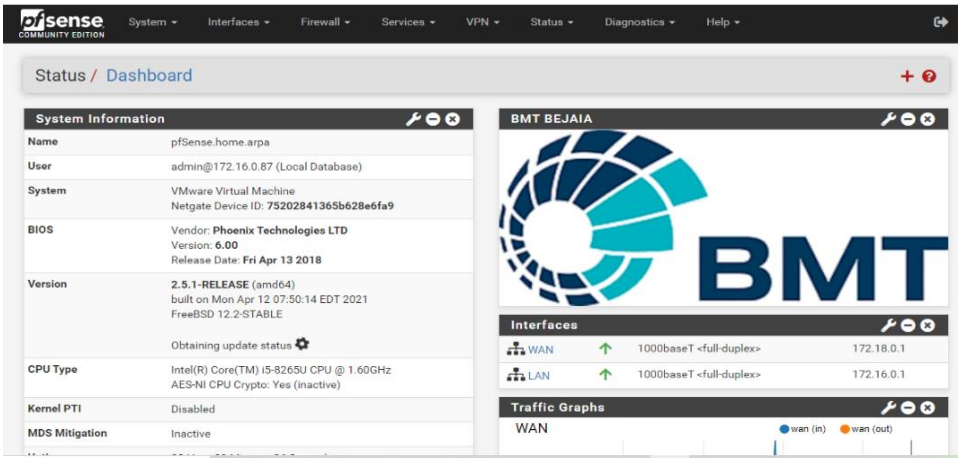

Figure 4.15 interface principale de pfSense

➢ **Ajout des règles**

Les règles de pare-feu configurées pour l'interface LAN, incluant des règles par défaut pour permettre le trafic depuis le réseau LAN vers n'importe quelle destination, ainsi qu'une règle spéciale pour prévenir le verrouillage administratif.

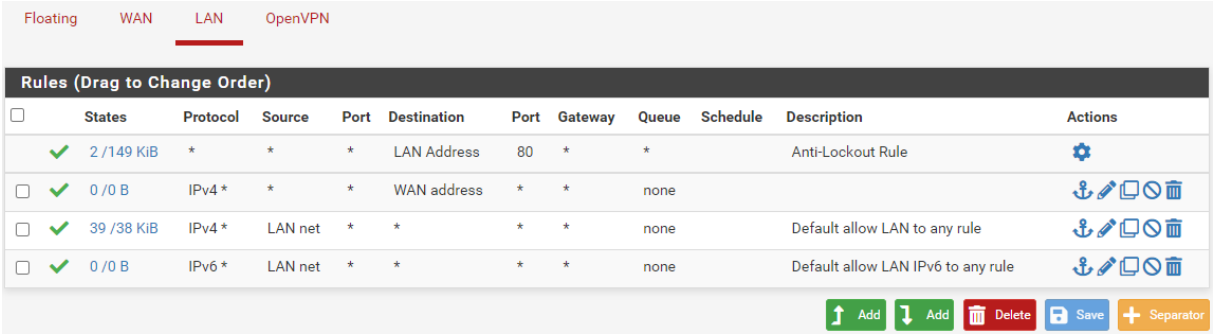

Figure 4.16 les règles de LAN

Une règle de pare-feu configurée pour autoriser le trafic OpenVPN (UDP sur le port 1194) sur l'interface WAN, ce qui est nécessaire pour que les clients OpenVPN puissent se connecter au serveur OpenVPN situé derrière ce pare-feu.

Figure 4.17 La règle de WAN

Cette règle autorise tout le trafic entrant sur l'interface OpenVPN à accéder au réseau LAN interne.

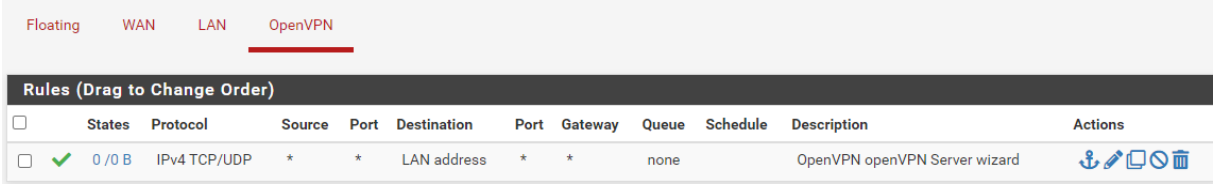

Figure 4.18 La règle OpenVPN

➢ **Ajout d'un serveur radius VPN**

Cette interface permet de gérer les serveurs d'authentification utilisés par le système pour valider les identités des utilisateurs. Ici, un serveur RADIUS avec l'adresse IP 172.16.0.2 est configuré, et la base de données locale de pfSense est également utilisée pour l'authentification.

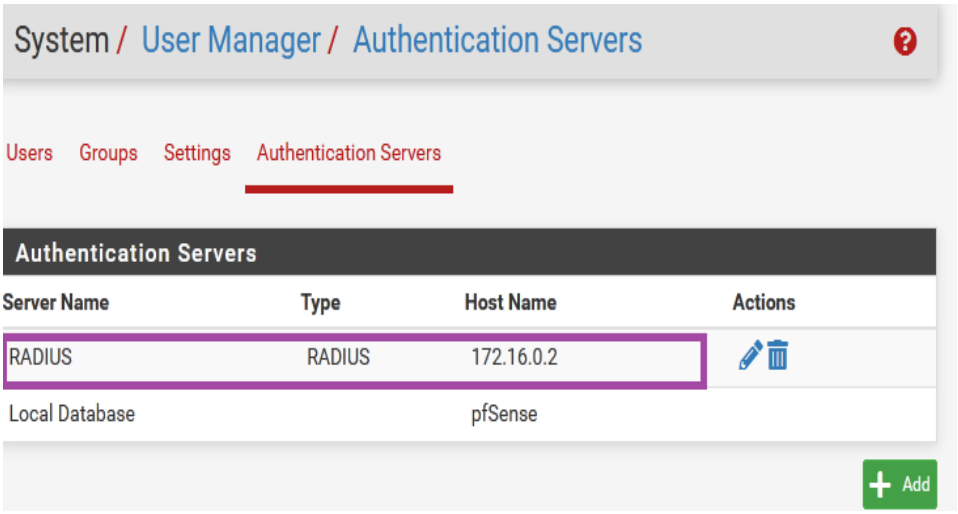

Figure 4.19 Serveur radius VPN

➢ **Création de certificat d'autorité**

Les certificats d'autorité de certification (CA Certificates) sont essentiels pour sécuriser les communications sur Internet. Ils permettent l'authentification des identités, le chiffrement des données et assurent l'intégrité des informations transmises.

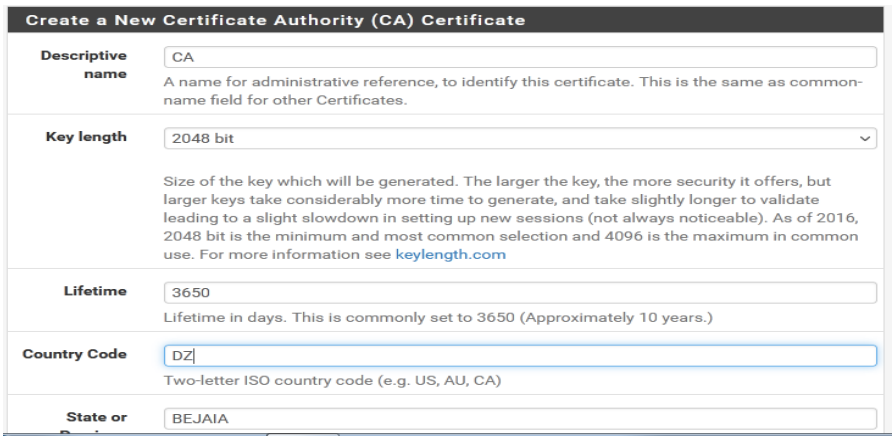

Figure 4.20 certificat d'autorité

➢ **Création d'un serveur OpenVPN**

La création du serveur OpenVPN permet d'établir des connexions sécurisées à travers le réseau WAN, offrant un accès sécurisé aux ressources du réseau pour les utilisateurs distants.

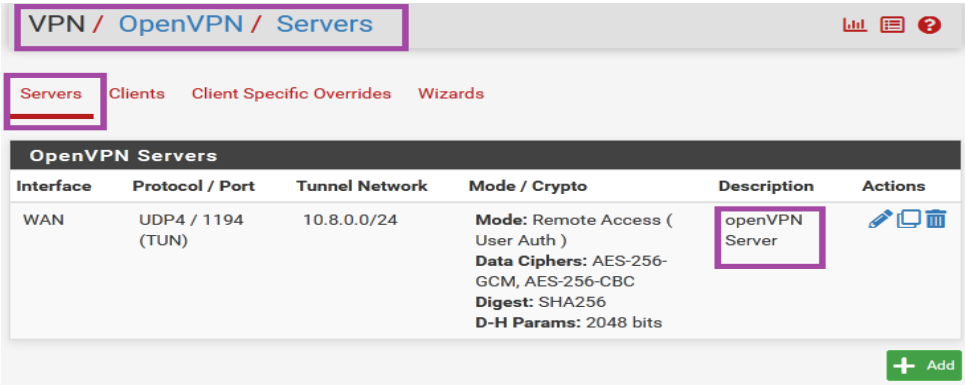

Figure 4.21 Serveur OpneVPN

2.3.3. Configuration Windows server

Nous passons maintenant à la configuration du Windows server 2016 afin de mettre en place et d'optimiser ses fonctionnalités et services clés.

➢ **Installation du rôle Active Directory**

Une fois connectés, nous avons ouvert le "Gestionnaire de serveur". C'est l'outil principal utilisé pour gérer les rôles et les fonctionnalités sur un serveur Windows. Ensuite Nous avons cliqué sur "Ajouter des rôles et des fonctionnalités". Cette option a lancé l'assistant qui nous a guidés tout au long du processus d'installation du rôle AD DS.

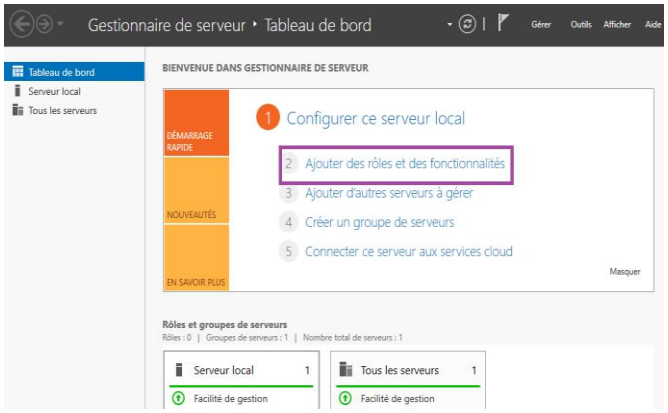

Figure 4.22 ajout des rôles

Nous avons installé plusieurs rôles essentiels sur notre serveur, notamment le serveur DNS, le serveur Active Directory Domain Services (AD DS) et le serveur DHCP. Ces rôles jouent

chacun un rôle crucial dans la gestion et la sécurité de notre réseau. Le serveur DNS assure la résolution des noms de domaine en adresses IP. Le serveur AD DS centralise la gestion des utilisateurs, des groupes et des ordinateurs. Le serveur DHCP, quant à lui, automatise l'attribution des adresses IP aux appareils du réseau, En installant ces rôles, nous avons renforcé l'infrastructure de notre réseau, assurant une meilleure performance et une gestion plus efficace des ressources.

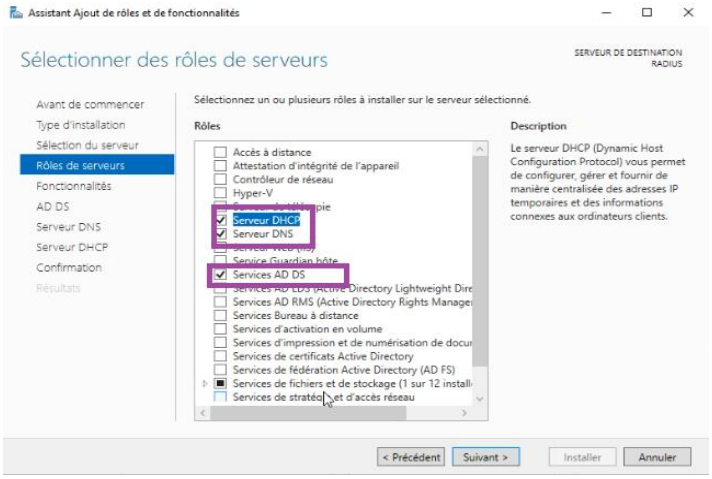

Figure 4.23 les rôles installés

- **Server NPS**

Le serveur NPS, configuré comme serveur RADIUS, joue plusieurs rôles clés dans la gestion des connexions réseau. Il authentifie les utilisateurs cherchant à se connecter au réseau en vérifiant leur identité selon les paramètres administratifs. Il gère également l'autorisation des connexions en définissant les niveaux d'accès appropriés pour chaque utilisateur ou groupe selon les politiques établies. Pour accéder aux informations d'identification et aux utilisateurs stockés dans Active Directory, le serveur NPS doit être enregistré dans Active Directory, établissant ainsi une connexion sécurisée pour l'accès aux informations d'identification.

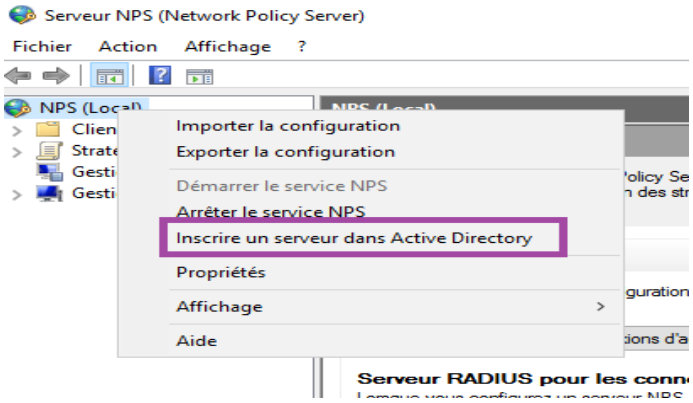

Figure 4.24 inscrire NPS dans AD

- **Création de domaine des groupes et des utilisateurs**

Pour créer un groupe, un clic droit sur notre domaine "BMT.local", "new" puis "group"

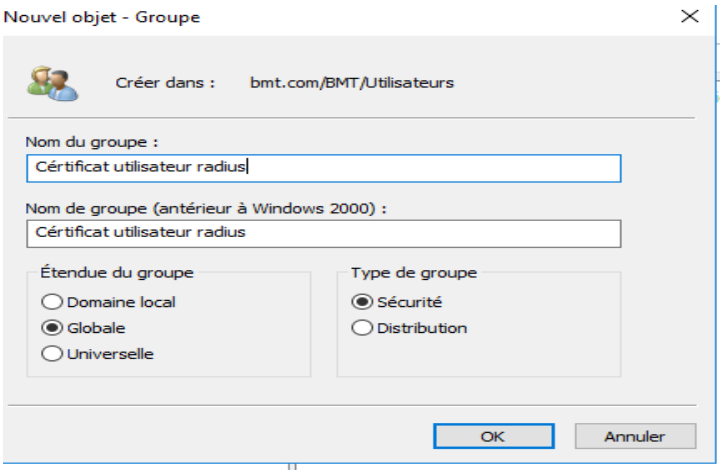

Figure 4.25 Nouveau groupe

Pour créer un utilisateur, nous appuyons sur le clic droit sur le domaine "BMT.local" puis "New user"

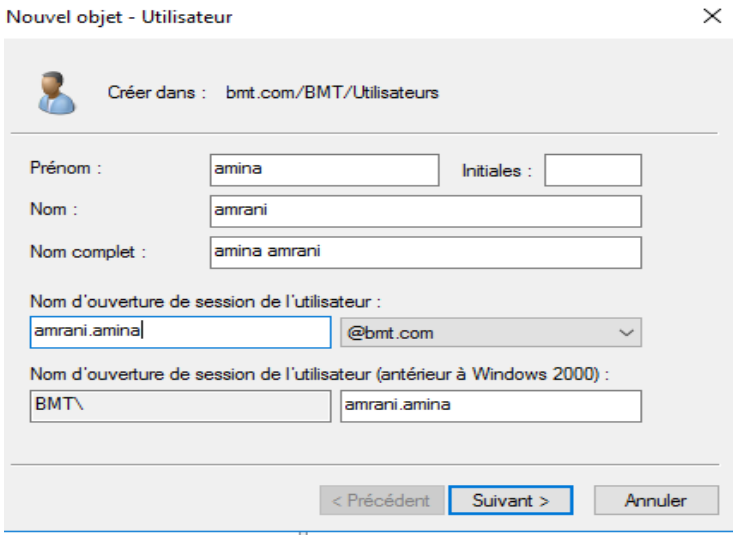

Figure 4.26 création d'un utilisateur

Après avoir cliqué sur "Suivant ", on doit introduire le mot de passe « Asr2024@ », et cocher les deux cases " l'utilisateur ne peut pas changer le mot de passe " et " le mot de passe n'expire jamais

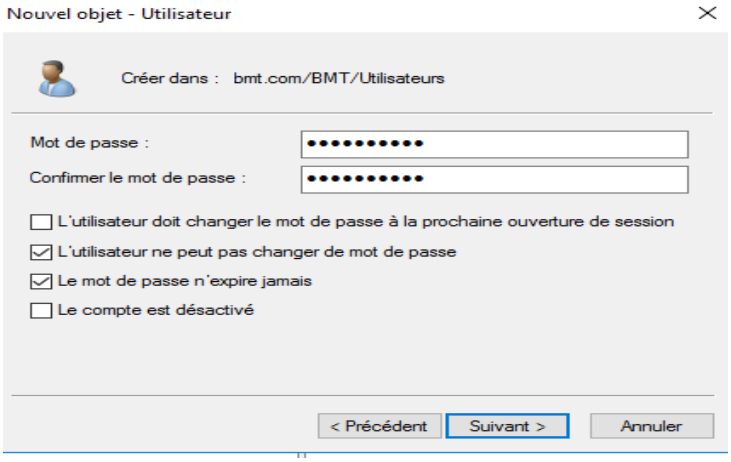

Figure 4.27 insérer le mot de passe de l'utilisateur

2.3.4. Tableau d'adressage

Dans le tableau 4.1 ci-dessous, nous donnons les adresses utilisées dans notre topologie.

Catégorie	Interface	Adresse/Subnet Mask
Réseau LAN	-	172.16.0.0/24
Réseau WAN	-	172.18.0.0/24
Interface	e0/0	192.168.122.190/24
Interface	e0/1	192.168.6.254/24
Interface	e0/2	172.18.0.2/24
ClientVPN	-	192.168.6.1/24
Serveur RADIUS	-	172.16.0.2/24
PfSense	-	172.16.0.1/24

Tableau 4.1 Les adresses utilisée

2.4. LES TESTS

Nous commençons maintenant la phase de tests pour évaluer la performance et la fiabilité de notre configuration.

2.4.1. Test DHCP

Nous avons attribué des adresses IP aux PC en utilisant DHCP, comme le montrent la figure 4.28 ci-dessous.

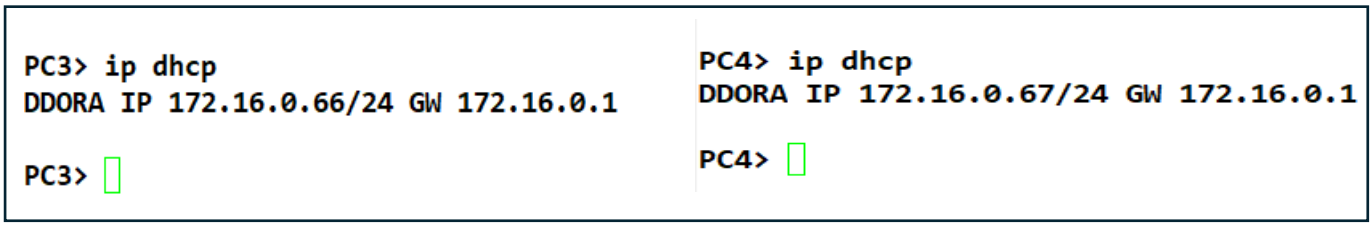

Figure 4. 28 TEST adresses PC avec DHCP

2.4.2. Test de connectivité

Nous vérifions la connexion du pfSense à Internet en effectuant un test de ping vers l'adresse IP 8.8.8.8. Comme le montre la figure 4.29, le test a réussi.

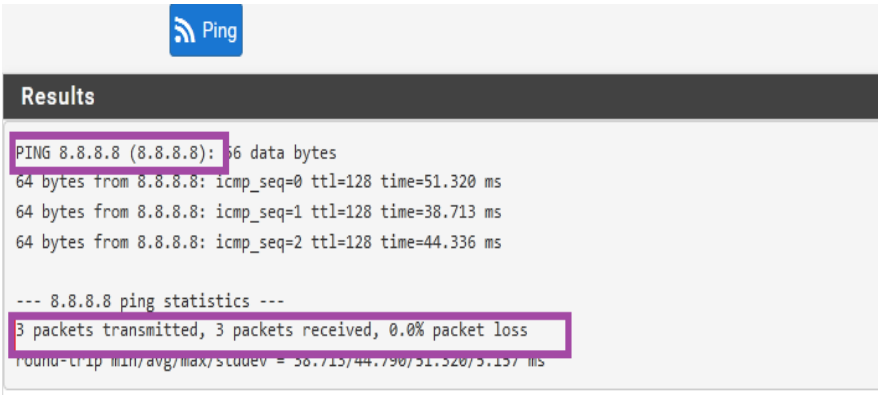

Figure 4.29 TEST accès Internet depuis pfSense

La figure 4.30 ci-dessous montre que nous avons effectué un ping de pfSense vers Windows Server et que cela fonctionne.

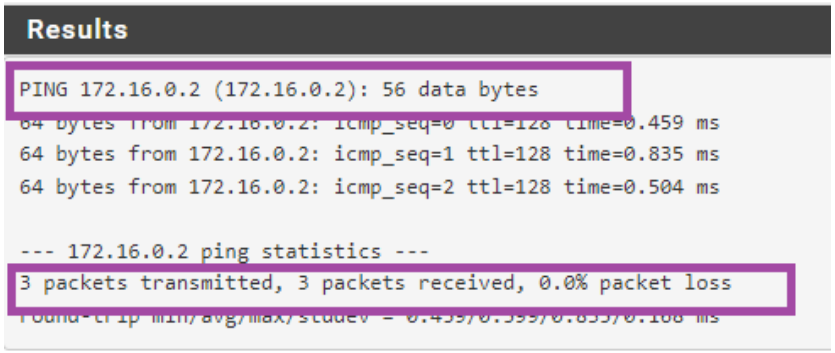

Figure 4.30 TEST de connectivité entre pfSense et Radius

Nous testons la connectivité entre le client VPN et le serveur Windows. La connectivité fonctionne correctement, comme l'illustre la figure 4.31.

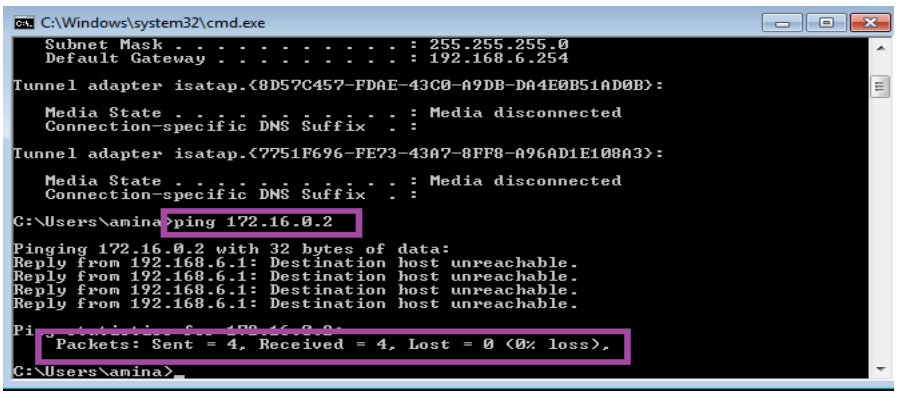

Figure 4.31 TEST de connectivité entre ClientVPN et radius

2.4.3. Test d'authentification

Pour vérifier l'authentification des utilisateurs avec accès à distance, nous avons installé l'application OpenVPN. La fenêtre affichée ci-dessous permet de saisir le nom d'utilisateur et le mot de passe pour se connecter.

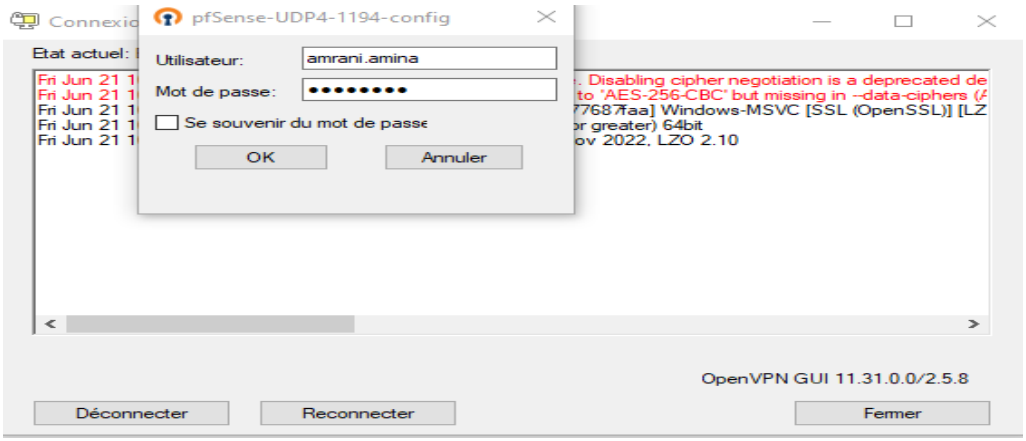

Figure 4.32 Fenêtre pour se connecter

La figure 4.33 indique que l'authentification de l'utilisateur "amrani.amina" a réussi, et cette vérification a été effectuée sur Windows Server 2016

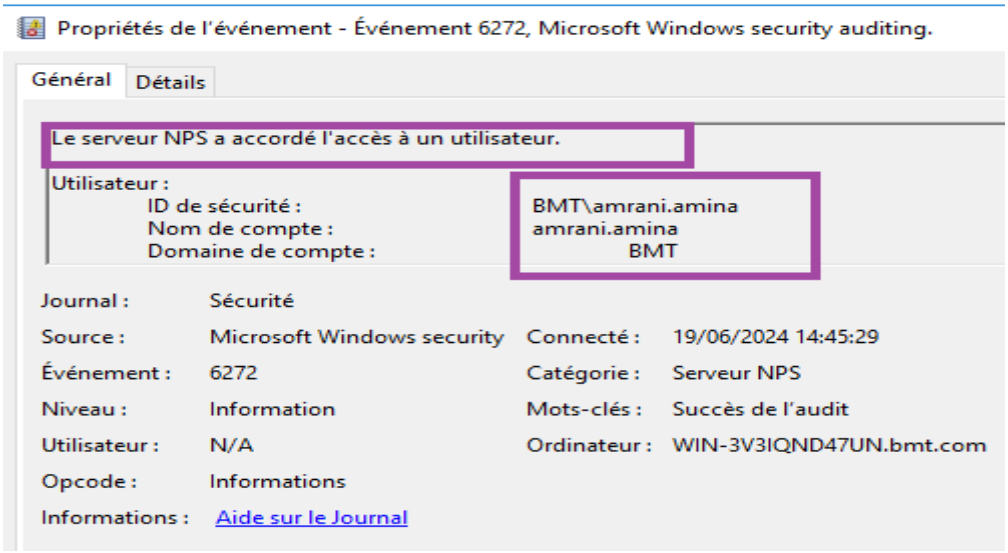

Figure 4.33 TEST NPS a accordé l'accès

La figure 4.34 indique que le serveur NPS a refusé l'accès à un utilisateur, ce qui signifie que l'authentification a échoué.

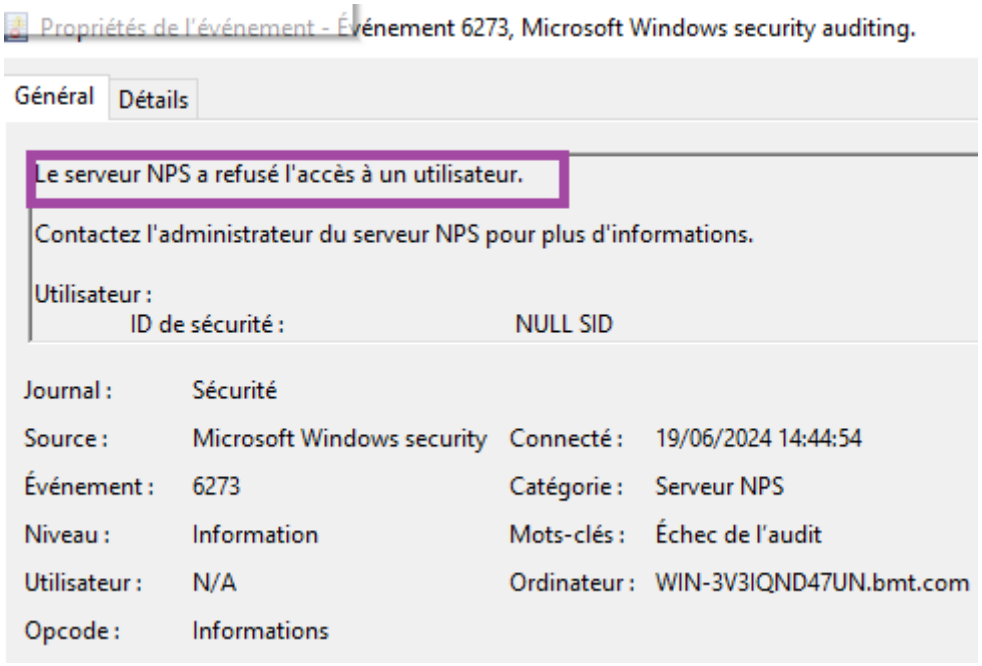

Figure 4.34 TEST NPS a refusé l'accès

La figure 4.35 montre que l'authentification de l'utilisateur "amrani.amina" a réussi, et cette vérification a été effectuée dans pfSense.

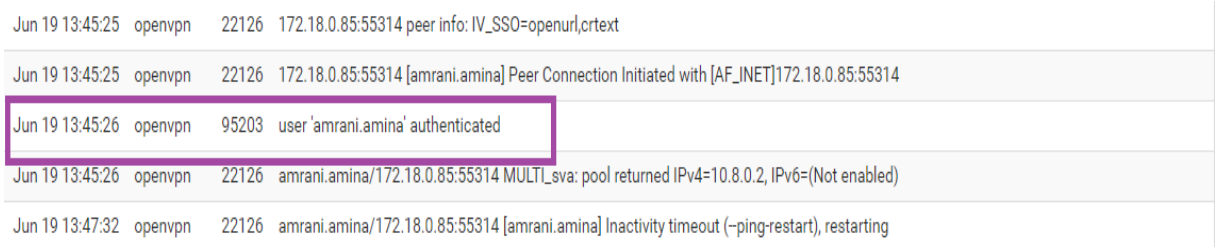

Figure 4.35 TEST authentification réussi dans pfSense

La figure 4.36 montre que l'authentification de l'utilisateur "amrani.amina" a échoué car un mot de passe incorrect a été saisi.

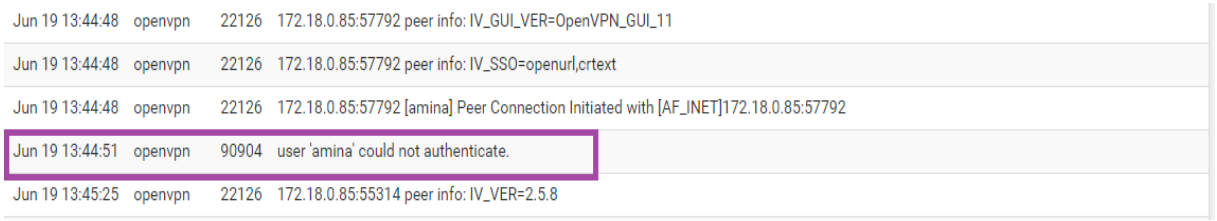

Figure 4.36 TEST d'authentification a échoué dans pfSense

Wireshark est un analyseur de paquets réseau qui permet de capturer et d'interpréter les données circulant sur un réseau informatique. Il est utilisé par les administrateurs réseau, les ingénieurs en sécurité, les développeurs et les étudiants pour diagnostiquer et résoudre des problèmes réseau, analyser les performances, comprendre les protocoles réseau et renforcer la sécurité.

La figure 4.37 ci-dessous montre deux cycles distincts d'authentification RADIUS :

- Le premier cycle, avec l'identifiant id=7, montre une tentative d'authentification réussie où le client est accepté.
- Le second cycle, avec l'identifiant id=188, montre une tentative d'authentification échouée où le client est rejeté.

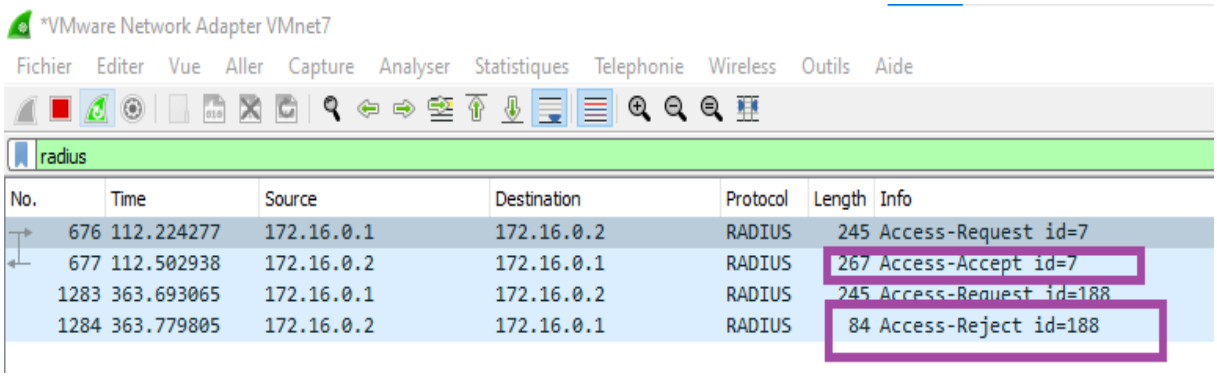

Figure 4.37 TEST dans wireshark

3. CONCLUSION

Ce chapitre a permis de démontrer l'importance de sécuriser les accès distants aux réseaux d'entreprise. En intégrant le protocole RADIUS, nous avons pu centraliser la gestion des authentifications et renforcer la sécurité des connexions VPN. Cette solution offre non seulement une meilleure protection contre les accès non autorisés, mais aussi une gestion simplifiée des utilisateurs et des politiques d'accès. Le succès de cette mise en œuvre valide l'efficacité du protocole RADIUS dans un environnement VPN, et ouvre la voie à des améliorations future

Conclusion Générale

Face à la croissance des attaques, de nouvelles méthodes de sécurité ont émergé, mettant en avant l'importance capitale de la gestion des accès.

Pour répondre à la problématique posée dans l'introduction générale, nous avons présenté dans ce mémoire l'avantage d'utiliser le protocole RADIUS pour sécuriser les réseaux. RADIUS se concentre sur l'authentification des utilisateurs et leur autorisation à accéder aux services réseau. En fournissant une infrastructure centralisée, il assure une gestion sécurisée des accès par divers moyens**.** RADIUS facilite la gestion des sessions utilisateur et la collecte de données sur l'utilisation des ressources réseau, essentielle pour la surveillance et la conformité aux politiques de sécurité. Sa flexibilité et sa compatibilité avec une variété de périphériques en font un choix indispensable pour sécuriser et administrer efficacement les accès réseau.

L'implémentation réussie d'un serveur d'authentification RADIUS via un VPN a été réalisée dans un environnement virtuel utilisant GNS3 et VMware, dans le cadre de notre stage à l'entreprise BMT de Bejaïa. Cette solution a été mise en œuvre pour sécuriser l'accès réseau, simulant ainsi des conditions réelles malgré l'utilisation de technologies de virtualisation comme GNS3 et VMware.

Notre implémentation a débuté par la configuration du pare-feu pfSense afin de sécuriser le réseau. Ensuite, nous avons mis en place le serveur Windows Server 2016 pour héberger le serveur d'authentification RADIUS, garantissant ainsi une identification sécurisée des utilisateurs. Le routeur a été configuré pour gérer efficacement le trafic entre les différentes zones du réseau. Enfin, nous avons intégré un client VPN OpenVPN pour offrir un accès sécurisé aux ressources du réseau à distance, La suite de ce travail consiste à essayer de tester ces mécanismes, étudiés théoriquement et implémentés pratiquement.

Bibliographie

[1] Mohamed, G., & Amine, R O U K H. (2018/2019). *La mise en place et la gestion d'un réseau informatique*, mémoire de master. Mostaganem : FSEI.

[2] IONOS. (2019, 6 septembre). Les types de réseaux informatiques à connaître. Ionos.

[3] Turgot Limoges. (n.d.). Les différents types de réseaux. https://turgotlimoges.scenari-community.org/STI2D/2_TSTI2D/1_MEI/COURS_MEI/TD_IMPRIMANTE_web/co/Types_de_reseaux.htm.

[4] https://www.cisco.com/go/offices. Consulté le 22 avril 2024

[5] Kaba, M. (2021, 12 mars). *Disponibilité, Intégrité et Confidentialité*. Ciberobs. https://ciberobs.com/2021/03/12/disponibilite-integrite-et-confidentialite/

[6] Bennacer, Y., & Mokrani, Y. (2021). *Les outils d'administration et sécurité des réseaux informatiques : Cas d'étude Sonatrach* (Mémoire de master , Université de Béjaïa). Université de Béjaïa.

[7] Université de Batna 2. (n.d.). *Sécurité des réseaux - Partie 1*. Université de Batna 2. https://cs.univ-batna2.dz/sites/default/files/web/files/securite_des_reseaux_partie_1.pdf

[8] Syloé. (2024). Firewall ou pare-feu - Glossaire Syloé. https://www.syloe.com/glossaire/firewall-pare-feu/

[9] https://www.alliance-informatique.fr/revue-blog/qu-est-ce-qu-un-vpn-et-comment-ca-fonctionne/. Consulté le 28 avril 2024.

[10] ZIANI, R., BOUAZIZ, S., FAREZ, N., & MAMOU, A. (2013). *Sécuriser un réseau Wifi en implémentant le protocole d'authentification 802.1x sur le serveur RADIUS. Mémoire de master, Université A. MIRA de Bejaia.*

[11] https://fr.wikipedia.org/wiki/Cryptographie_sym%C3%A9trique. Consulté le 5 mai 2024.

[12] https://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique. Consulté le 5 mai 2024.

[13] Nardjes, D., & Nabila, D. (2015). *Mise en place d'un système de sécurité basé sur le serveur d'authentification TACACS+, Thèse* de doctorat, Université Mouloud Mammeri.

[14] Archimbaud, J. L. (2000). Certificats (électroniques): Pourquoi? Comment? .

[15] https://www.entrust.com/fr/resources/learn/what-is-token-based-authentication. Consulté le 10 mai 2024

[16] Borderes, S. (2006). *Authentification réseau avec Radius*. Collection Blanche.

[17] Messous, M. (2015). *Mise en place d'un système de sécurité basé sur l'authentification dans un réseau IP*, mémoire de master, Université Mouloud Mammeri de Tizi-Ouzou.

[18] Ziani, R., Bouaziz, S., & Farez, N. (2013). *Sécuriser un réseau Wifi en implémentant le protocole d'authentification 802.1x sur le serveur RADIUS*, mémoire de Master, Université Mouloud Mammeri de Tizi-Ouzou.

[19] Duvallet, C. (2007-2008). *Architectures et Protocoles des Réseaux Chapître 8- Le protocole RADIUS*. Université du Havre, UFR des Sciences et Techniques.

[20] https://web.maths.unsw.edu.au/~lafaye/CCM/authentification/radius.htm. Consulté le 13 mai 2024.

[21] Duvallet, C. (s.d.). *Le protocole RADIUS Remote Authentication Dial-In User Service*. CNAMSMB214-215. Université du Havre, UFR des Sciences et Techniques.

[22] https://igm.univ-mlv.fr/~dr/XPOSE2007/jgauth02_RADIUS/protocol.html. Consulté le 10 juin 2024

[23] https://www.rcdevs.com/fr/glossary-radius/. Consulté le 19 juin 2024

[24] Mansouri, S., & Madi, M. (2023). *Mise en place d'une politique AAA, cas d'étude : BMT*, mémoire de Master en Informatique, Université Abderrahmane Mira de Béjaïa.

[25]https://learn.microsoft.com/fr-fr/windows-server/networking/technologies/extensible-authentication-protocol/network-access?tabs=eap-tls%2Cserveruserprompt-eap-tls%2Ceap-sim. Consulté le 20 juin 2024

[26] Spasojevic, A. (2024). Qu'est-ce que le protocole d'authentification extensible (EAP) ? *PhoenixNAP Glossaire*. Consulté à partir de https://phoenixnap.fr/glossaire/protocole-d%27authentification-extensible-eap

[27] https://www.01net.com/vpn/definition/. Consulté le 20 juin 2024

[28] Rahmani, T., & Sadaoui, F. (2017). *Étude et mise en place d'un réseau VPN* (Mémoire de Master, Université Mouloud Mammeri de Tizi Ouzou, Faculté du Génie Électrique et Informatique, Département Électronique). Dirigé par Leila Lehdir. Tizi Ouzou, Algérie.

[29] Synetis. (2021, janvier 12). Développement du télétravail : démocratisation des VPN. Synetis. https://www.synetis.com/developpement-du-teletravail-democratisation-des-vpn/

[30] Nemchick, E. (2023, 22 septembre). VPN Protocols Explained and Compared. Avast Academy. https://www.avast.com/fr-fr/academy/vpn-protocols-explained-and-compared

[31] https://www.globalsign.com/fr/centre-d-information-sur-le-ss. Consulté le 22 juin 2024

[32] https://www.syloe.com/glossaire/firewall-pare-feu/. Consulté le 22 juin 2024

[33] Titusss. (2020, 18 février). PFSense Installation / configuration / fonctionnalité et packages. Portail informatique et sécurité du web

[34] Krahenbuhl, V. (2018, novembre 21). GNS3. All IT Network. https://all-it-network.com/gns3/

[35] Electronic Team, Inc. (2023). Tutoriel étendu sur le port série VMware. Serial over Ethernet. https://www.serial-over-ethernet.com/fr/serial-port-virtual-machine/vmware-serial-port/

Résumé

Le projet de sécurisation du réseau de l'entreprise BMT face au télétravail croissant vise à protéger les données sensibles et les ressources internes. Pour cela, un serveur d'authentification RADIUS a été mis en place via OpenVPN, utilisant GNS3 et VMware pour simuler l'infrastructure réseau. La configuration a inclus un pare-feu pfsense et un serveur Windows Server 2016 pour l'authentification centralisée via Active Directory et le service NPS. Cette solution améliore la sécurité du réseau en combinant RADIUS avec VPN, garantissant une protection contre les accès non autorisés et une gestion sécurisée des connexions utilisateur. Le projet a également permis d'acquérir des compétences en gestion de réseau, sécurité informatique et virtualisation.

Mots clés : BMT, WINDOWS SERVER 2016, RADIUS, VPN, GNS3, VMWARE, NPS et Active dictory.

Abstract

The project to secure the network of BMT in response to the increasing trend of remote work aims to protect sensitive data and internal resources. To achieve this, a RADIUS authentication server was implemented via OpenVPN, using GNS3 and VMware to simulate the network infrastructure. The configuration included a pfsense firewall and a Windows Server 2016 for centralized authentication via Active Directory and the NPS service. This solution enhances network security by combining RADIUS with VPN, ensuring protection against unauthorized access and secure management of user connections. The project also allowed for the acquisition of skills in network management, IT security, and virtualization.

Keywords: BMT, WINDOWS SERVER 2016, RADIUS, VPN, GNS3, VMWARE, NPS et Active dictory.