# EPIGRAPHE

« L’objectif d’une DMZ est d’isoler les services accessibles au public du réseau interne, offrant ainsi une couche de sécurité supplémentaire »

**GENE SAFFORD**

# DEDICACES

A mes parents Papa Aimé LUKWAYA et Maman Thérèse NAWA que j’ai connus ce monde et qui ont joué avec plénitude leur rôle des parents responsables.

**ATUEKA ENOCK**

# 

# REMERCIEMENTS

Nous exprimons notre profonde gratitude à l’endroit de

Qu’il nous soit digne de remercier tout le corps professoral et personnel administratif de l’institut Supérieur Pédagogique et Technique de Kinshasa.

Nos remerciements s’adressent à Monsieur le Professeur ANGOMA, d’heureux travail qui, en dépit de ses multiples occupations, ont accepté d’assurer la direction du présent travail.

Nous exprimons également notre reconnaissance au Co-directeur Assistante MAYI qui, nonobstant ses multiples occupations a encadré efficacement cette recherche. Ses observations pertinentes nous ont été d’une grande utilité.

Nous sommes reconnaissants envers nos frères et sœurs : Sarah LUKWAYA, Grâce LUKWAYA, Chiko Jeancy, Sebiano LUKWAYA, Neville ATUEKA, Fabiano LUKWAYA

Qui, de prêt ou de loin nous ont soutenu grâce à leurs conseils et suggestions.

**ATUEKA ENOCK**

# LISTE DES ABREVIATIONS

|  |  |
| --- | --- |
| **ABREVIATIONS** | **DESCRIPTIONS** |
| **BNC** | Bayonnet Neill-Concelman Connector |
| **CSMA/CD** | carrier sense multiple access with collision |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DNS** | Domaine Name Serveur |
| **DMZ** | Demilitarized zone |
| **FTP** | File Transfert Protocol |
| **http** | HyperText Transfert Protocol |
| **IEEE** | Institute of Electrical and Electronic Ingeneer |
| **InterNic** | Internet Network Information Center |
| **IP** | Internet Protocol |
| **ISO** | Interconnexion des Systèmes Ouverts |
| **ISPT** | Institut Supérieur Pédagogique et Technique de Kinshasa |
| **LAN** | Local Area Network |
| **Li-fi** | Light – Fidelity |
| **MAN** | Métropolitain Area Network |
| **OSI** | Open System Interconnexion |
| **PAN** | Personal Area Network |
| **RJ45** | Registered Jack 45 |
| **TCP** | Transmission Control Protocol |
| **UDP** | User Datagram Protocol |
| **USB** | Universal Serial Bus |
| **UTP** | Unshielded Twisted Pair |
| **WAN** | Wide Area Network |
| **WI-FI** | Wireless Fidelity |
| **WWW** | World Wide Web |
| **OSI** | Open System Interconnexion |
| **PAN** | Personal Area Network |
| **RJ45** | Registered Jack 45 |
| **TCP** | Transmission Control Protocol |
| **TDMA** | Time Division Multiplexing Access |

# LISTE DES FIGURES

# LISTE DES TABLEAUX

# INTRODUCTION GENERALE

# 0.1 Présentation du Sujet

Dans un monde de plus en plus connecté, la sécurité des données est

devenue une préoccupation majeure pour les institutions publiques et privées. La Caisse Nationale de Sécurité Sociale (CNSS), en tant qu'organisme chargé de la gestion des droits sociaux, traite une multitude d'informations sensibles relatives aux assurés et à leurs prestations. La protection de ces données est cruciale non seulement pour garantir la confidentialité et l'intégrité des informations, mais également pour maintenir la confiance des utilisateurs.

La conception et l'optimisation d'une infrastructure de réseau local sécurisé, intégrant une zone démilitarisée (DMZ), représentent une réponse stratégique aux défis de la cybersécurité. La DMZ agit comme une barrière protectrice, isolant les systèmes internes des menaces extérieures tout en permettant des échanges sécurisés avec le monde extérieur. Cette approche permet de renforcer la sécurité des utilisateurs en minimisant les risques d'intrusion et de fuite de données.

Ainsi, cette étude vise à explorer les meilleures pratiques pour concevoir une infrastructure réseau robuste et sécurisée pour la CNSS, en tenant compte des spécificités de son environnement de travail et des exigences réglementaires en matière de protection des données. En abordant les enjeux stratégiques, techniques et humains, cette réflexion s'inscrit dans une démarche proactive pour anticiper et répondre aux menaces qui pèsent sur les systèmes d'information de l'organisation.

La conception et l'optimisation d'une infrastructure de réseau local sécurisé, intégrant une zone démilitarisée (DMZ), sont essentielles pour protéger les données sensibles d'organisations comme la Caisse Nationale de Sécurité Sociale (CNSS). Une infrastructure bien conçue permet de créer un environnement sécurisé pour les utilisateurs en isolant les systèmes critiques des menaces potentielles provenant d'Internet. La DMZ sert de zone tampon, permettant des interactions contrôlées avec des services externes tout en garantissant que le réseau interne demeure protégé. Ce processus implique l'analyse des besoins spécifiques, la mise en œuvre de mécanismes de sécurité robustes et une surveillance continue pour s'adapter aux menaces évolutives, assurant ainsi la protection des informations sensibles et la conformité aux réglementations en vigueur.

# 0.2 Choix du sujet

Le choix de la thématique Conception et optimisation d’une infrastructure de réseau local sécurisé intégrant une zone démilitarisée pour renforcer la protection des utilisateurs dans le cas de la CNSS s'inscrit dans un contexte où la sécurité des informations est devenue une priorité stratégique pour toutes les organisations, particulièrement celles qui manipulent des données sensibles.

# 0.3 Problématique

La problématique c’est le problème que présente un sujet de recherche rendu visible par un questionnement. Elle ne demande pas une définition d'un mot, elle implique un travail de reformulation qui peut être sous la forme d'un paradoxe. C'est une question complexe qui demande d'être capable de conjuguer plusieurs informations, parfois divergentes, en les justifiant, tout en restant neutre.[[1]](#footnote-1)

Le Professeur Tazi, définit la problématique comme étant le problème soulevé par le sujet de la recherche ; Elle est opérationnalisée (rendu visible) par la question de la recherche.[[2]](#footnote-2)

Actuellement, l’informatique est au cœur de toutes les entreprises. Le système d’information d’une entreprise est composé de matériels et de logiciels. Elle s’immisce maintenant dans la plupart des objets de la vie courante, que ce soit dans l’objet proprement dit, ou bien dans le processus de conception ou de fabrication de cet objet. La CNSS rencontre plusieurs problème tels que le risque élevé de fuites d'informations sensibles en raison de failles de sécurité ou d'erreurs humaines ; compromettant la confidentialité des assurés, faible niveau de sensibilisation des employés aux enjeux de la cybersécurité, ce qui peut entraîner des comportements à risque et des violations de sécurité ; difficultés de communication et de coordination entre les différents départements, ce qui complique la mise en œuvre de politiques de sécurité cohérentes.

Suite aux difficultés évoquées ci-haute, nous passerons par les jeux des questions afin de trouver des solutions dans les chapitres qui suivent :

* Quelles sont les spécificités des données sensibles gérées par la CNSS et comment doivent-elles être protégées contre les menaces cybernétiques ?
* Quelles technologies et meilleures pratiques doivent être mises en œuvre pour garantir une sécurité robuste tout en minimisant l'impact sur les opérations quotidiennes ?
* Comment établir des mécanismes de surveillance et de réponse aux incidents pour assurer une réactivité optimale face aux menaces émergentes ?

Dans les lignes qui suivent, nous essayerons de réponses aux questions posées.

# 0.4 Hypothèse

Au regard des questions posées à la problématique, nous pouvons dire ceci : qu’il est important que nous ayons les mêmes entendements du concept hypothèse. L’hypothèse est une réponse anticipative ou provisoire que l’on apportera aux questions posé à la problématique. Elles sont généralement formulées au conditionnel.[[3]](#footnote-3)

* Concernant la protection des données sensibles, la CNSS pourrait mettre en place des contrôles d'accès stricts, des cryptages des données au repos et en transit, ainsi que des audits réguliers de sécurité.
* L'adoption de pare-feu de nouvelle génération en Intégration d’une DMZ et VPN pour les accès distants pourraient être conçue pour isoler les serveurs accessibles à l'extérieur (comme les portails de services) des systèmes internes critiques.
* La mise en œuvre du mécanisme de surveillance et de réponse d'une équipe de réponse aux incidents de cybersécurité, renforcrait par des outils de surveillance en temps réel, permet de détecter et de réagir rapidement aux menaces. L'établissement de protocoles clairs pour la gestion des incidents et des rapports réguliers sur l'état de la sécurité contribue également à une meilleure réactivité.

# 0.5 Objectifs

L'objectif principal de la conception et de l'optimisation d'une

Infrastructure de réseau local sécurisé, intégrant une zone démilitarisée (DMZ) pour la Caisse Nationale de Sécurité Sociale (CNSS), est d’Assurer la protection des données sensibles des utilisateurs tout en garantissant un accès sécurisé et efficace aux services, en conformité avec les réglementations en matière de sécurité des données.

# 0.6 Méthode et Technique

Le concept méthode désigne l’ensemble concret d’opérations mises en œuvre pour atteindre un ou plusieurs objectifs.[[4]](#footnote-4)

D’une autre manière, nous définissons la méthode comme un cadre traçant la voie que le chercheur utilise pour parvenir à un résultat scientifique digne. Nous avons basé notre travail sur des méthodes ci-après :

# 0.6.1 Méthode

Nous avons basé notre travail sur des méthodes ci-après :

1. **La Méthode Historique** : Cette méthode nous a permis d’analyser et ensuite, de présenter l’évolution de la CNSS à travers le temps, tout en expliquant les époques, les faits et les évènements passés et leur enchainement pour aboutir à la vérité des faits.
2. **La Méthode structuro-fonctionnelle** : Cette méthode nous a servi de mener les recherches des impératifs fonctionnels et structurels pour maintenir l’équilibre d’un système. C'est-à-dire : connaitre la structure fonctionnelle de la CNSS.

# 0.6.2 Technique

La technique est un outil utilisé dans la collecte d’informations (chiffrées ou non) qui devront plus tard être soumises à l’interprétation et à l’explication grâce aux méthodes. Pour ce travail, nous avons utilisé les techniques ci- après :

1. **Technique d’observation** : elle nous a permis de comprendre le fonctionnement de la CNSS et récolté facilement les données dont nous avons besoins.
2. **Technique documentaire** : cette technique nous a facilité la récolte des données, par la lecture des certains documents ayant trait avec notre sujet de recherche.

# 0.7. Délimitation du sujet

Il est vrai qu'un travail scientifique pour être bien précis, doit être délimité. Ainsi, nous avons pensé circonscrire notre étude dans le temps et dans l'espace.

## 0.7.1 Spatiale

Dans l’espace, nos recherches sont orientées à la Caisse Nationale de Sécurité Sociale (CNSS en sigle)

## 0.7.2 Temporelle

Dans le temps, le présent travail ne concerne que la période allant du Mois de Février 2025 au Mois d’Août 2025.

# 0.8 Subdivision du Travail

Le présent travail est subdivisé en quatre chapitres, hormis l’introduction et la conclusion :

* Le premier chapitre aborde Généralité sur les Réseaux Locaux et Conception de la DMZ
* Le troisième chapitre s’étale de la Description de l’entreprise,
* Le quatrième chapitre sur la mise en œuvre du nouveau système

# CHAPITRE 1 : GENERALITE SUR LES RESEAUX LOCAUX

# 1.0 INTRODUCTION

Dans ce chapitre, nous allons parler de la généralité du réseau informatique où nous allons voir les différents types de réseau ainsi que d’autres choses faisant trait avec le modèle de communication, nous allons aussi parler de la Sécurité avec DMZ.

# 1.1 DEFINITION

Le réseau informatique est un ensemble des moyens matériels et logiciels mis en œuvre pour assurer les communications entre terminaux informatiques[[5]](#footnote-5).

En outre, le réseau informatique est l’ensemble des terminaux reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques (valeurs binaires, c'est-à-dire codées sous forme de signaux pouvant prendre deux valeurs : 0 et 1).[[6]](#footnote-6)

# 1.2 TYPOLOGIE DES RESEAUX

Il existe plusieurs types de réseau informatique selon le découpage géographique dont la subdivision a été rendue possible par rapport à leur taille, débit ou aire géographique, qui se résume en quatre grands types ou catégories :

# 1.2.1 Le Réseau PAN (Personal Area Network)

Le réseau personnel permet l’échange de donnée des appareils modernes comme notamment les Smartphones, tablettes, ordinateurs portables ou les ordinateurs de bureau, ces derniers peuvent être connectés à un réseau adapté. Le réseau personnel sans fil (WPAN pour Wireless personale Area Network) repose sur des technologies comme le Bluetooth, USB sans fil.[[7]](#footnote-7)



Figure 1. 1 Le réseau PAN

# 1.2.2 Réseau LAN (Local Area Network)

Le réseau local est un groupe d’équipement relié en local (privé) dans une limite bien limitée. Un tel réseau peut relier deux ordinateurs d’une maison ou alors plusieurs centaines d’appareils au sein d’une entreprise.

Mais également des réseaux dans des institutions publiques comme les administrations, les écoles ou les universités sont généralement mis en œuvre sous la forme d’un LAN. Une norme commune très répandue pour les réseaux locaux câblés est le protocole Ethernet.[[8]](#footnote-8)

Un LAN est conçu pour permettre un transfert rapide de grandes quantités de données. Selon la structure du réseau et du moyen de transmission utilisé, un débit de données de 10 à 1000 Mbit/s est courant. Les réseaux locaux permettent un échange d’informations confortable entre les différents périphériques qui sont connectés au réseau.



Figure 1. 2 Réseau LAN

# 1.2.3 RESEAU MAN (Métropolitain Area Network)

C'est l'interconnexion des réseaux locaux se trouvant dans une même ville ou dans une même région. Ce réseau peut utiliser des lignes du réseau public (service de télécommunication, radiocommunication, câbles téléphoniques, ...) ou privées pour assurer la liaison entre deux ou plusieurs sites. Il permet à des utilisateurs se trouvant à plusieurs endroits géographiques de partager les ressources par le réseau comme s'ils étaient dans un LAN. Dans ce type de réseau, la distance entre les sites ne dépasse pas 200 Km.[[9]](#footnote-9)



Figure 1. 3 Réseau Man

# 1.2.3 Le Réseau WAN (Wide Area Network)

Un réseau WAN (Wide Area Network), s’étend sur une vaste zone géographique telle qu’un pays, voire un continent. Le réseau WAN se compose de deux types de composants : les lignes de transmission et les équipements de commutation. La plupart des entreprises ne possédant pas de lignes de transmission, elles en louent à un opérateur téléphonique. Les équipements de commutation, ou plus simplement commutateurs, sont des ordinateurs spécialisés qui servent à interconnecter trois lignes de transmission ou plus. Lorsque des données arrivent sur une ligne entrante, l’équipement de commutation doit choisir une ligne sortante vers laquelle les aiguiller. [[10]](#footnote-10)



Figure 1. 4 Réseau WAN

# 1.3. EQUIPEMENTS D’INTERCONNEXION RESEAUX

Un réseau local sert à interconnecter les ordinateurs d'une organisation, toutefois une organisation comporte généralement plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux. Dans ce cas des équipements spécifiques sont nécessaires. Les principaux équipements matériels mis en place dans les réseaux locaux sont :

# 1.3.1 Commutateur (SWITCH)

Le Switch est un dispositif qui établit une relation privilégiée entre deux nœuds du réseau et qui acheminent les paquets vers le récepteur en utilisant des références, également appelées identificateurs ou étiquettes (en anglais labels). Une référence est suite de chiffres accompagnant un bloc (trame, paquet, etc).[[11]](#footnote-11)



Figure 1. 5 Switch

# 1.3.2 Concentrateur (HUB)

Un concentrateur est un élément matériel permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. Le concentrateur est ainsi une entité possédant un certain nombre de ports (il possède autant de ports qu'il peut connecter de machines entre elles, généralement 4, 8, 16 ou 32). Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports. Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé répéteur multiports[[12]](#footnote-12).



Figure 1. 6 Hub

# 1.3.3 Les Routeurs

# Sont les plus puissants, ils sont capables d'interconnecter plusieurs réseaux utilisant différents protocoles entre eux. Ils travaillent au niveau de la couche 3 du modèle OSI, les routeurs disposent d'une table de routage qui leur permet d'aiguiller les trames vers le bon réseau. Ils permettent une structure maillée, indispensables pour la construction de l'internet. Les routeurs peuvent utiliser divers protocoles pour maintenir entre eux leurs tables de routage. Ils sont capables d'exploiter plusieurs routes possibles pour rejoindre la même cible.



Figure 1. 7 Le Routeur

# 1.3.4 Passerelle

Une passerelle est un système matériel et logiciel permettant de passer des informations d'un réseau à un autre. La passerelle peut se présenter sous la forme d'un connecteur physique de réseau et être utilisée comme une interface pour transférer les informations entre les différents réseaux. Elle peut également se présenter sous forme de logiciel conçu pour permettre à deux protocoles différents d'échanger des informations sur le même réseau. Lorsqu'un réseau ne parvient pas à reconnaitre la destination des informations il les transmet au réseau suivant en utilisant une passerelle par défaut.

## 1.3.5 Carte Réseau

Elle se présente sous la forme d'une grosse carte de visite, elle se configure automatiquement et elle est reconnue directement par Windows[[13]](#footnote-13). Chaque carte réseau possède une adresse spécifique, elle sert à identifier la carte réseau lorsque les informations sont envoyées ou reçues au sein du réseau.

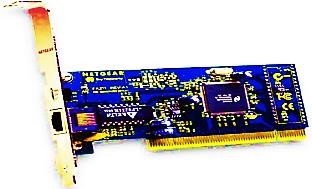


Figure 1. 8 Carte réseau

# 1.3.6 Le Pont

# Sont utilisés pour interconnecter deux réseaux utilisant les mêmes Protocoles. Les ponts travaillent au niveau de la couche 2 (liaison de données) du modèle OSI. Les ponts se basent sur l'adresse MAC et le nom de la station sur le réseau pour savoir si la trame doit traverser le pont ou non. En d'autres termes, les informations ne passeront le pont que si elles doivent aller d'un réseau à l'autre.

# 1.4 TOPOLOGIE DES RESEAUX

# La topologie est une représentation d’un réseau. Cette représentation peut être considérée du point de vue de l’emplacement des matériels (câbles, postes, dispositifs de connectivité,), et l’on parle de « topologie physique », ou du point de vue du parcours de l’information entre les différents matériels, et l’on parle de « topologie logique ». La topologie logique détermine la manière dont les stations se partage le support et dépend de la méthode d’accès au réseau.

## 1.4.1 Topologie Physique

### 1.4.1.1 La topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau. Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté. [[14]](#footnote-14)

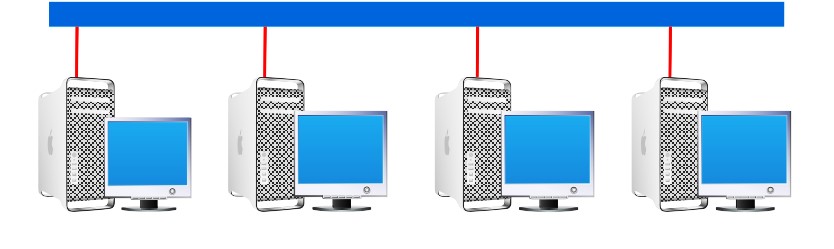


Figure 1. 9 la topologie en bus

# 1.4.1.2 La topologie en étoile

# La topologie en étoile, plus communément appelée topologie en étoile hiérarchique, est la topologie la plus utilisée dans les réseaux locaux. Cette topologie est plus coûteuse que la topologie de bus car elle nécessite davantage de câbles. Cependant, un nœud ou un câble endommagé ne fera pas tomber le réseau entier. Le principal problème avec une configuration en étoile hiérarchique est qu’il est susceptible de connaître un seul point de défaillance. Cependant, si l’ensemble du réseau tombe en panne car un périphérique central a un problème, alors vous savez où est le problème, il vous suffit de regarder le périphérique central.



Figure 1. 10 la topologie en étoile

# 1.4.1.3 La topologie en anneau

La topologie de l'anneau est également l'une des topologies réseaux les plus anciennes à notre disposition, et elle est similaire à la topologie de bus dans le sens où vous avez câble le dorsal unique auquel tous les nœuds ou tous les ordinateurs se connectent.[[15]](#footnote-15)



Figure 1. 11 la topologie en anneau

# 1.4.2 TOPOLOGIE LOGIQUE

Elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token-ring et FDDI.

# 1.4.2.1 Réseau Ethernet

Ethernet est aujourd’hui l’un des réseaux les plus utilisés en local. Il repose sur une topologie physique en étoile.

* **CSMA CA** (Carrier Sense Multiple Access Collision Avoidance) ou Accès multiple avec écoute de la porteuse. Il fonctionne en détectant l’état du support afin d’empêcher ou de récupérer d’une collision. Une collision se produit lorsque deux émetteurs émettent en même temps. Les données sont brouillées et les récepteurs ne seraient pas en mesures de les distinguer les uns des autres. Les informations perdues doivent être renvoyées pour que le destinataire les obtienne.

* **CSMA CD** (Carrier Sense Multiple Access Collision Detection) fonctionne en détectant l’occurrence d’une collision. Une fois qu’une collision est détectée.

**CSMA CD** met immédiatement fin à la transmission afin que l’émetteur n’ait pas à perdre beaucoup de temps à continuer. Les dernières informations peuvent être retransmises. En comparaison, CSMA ne s’occupe pas de la récupération après une collision. Il vérifie si le support est utilisé. S’il est occupé, l’émetteur attend qu’il soit inactif avant de commencer à émettre.

# 1.4.2.2 Réseau FDDI (Fiber Distributed Data Interface)

Cette topologie n’est qu’une évolution de la topologie Token-ring. Le FDDI repose sur la technique du réseau à jeton sécurisée, en double boucle bidirectionnelle, constituée et utilise de fibres optiques.

Le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Pour transmettre les données. C’est une topologie qui offre beaucoup d’avantages du point de vue transmission, bande passante et le débit. Il est constitué de deux anneaux : un anneau primaire et anneau secondaire. L'anneau secondaire sert à rattraper les erreurs de l'anneau primaire ; Ce qui fait que si une station MAU tombe en panne, le réseau continuera de fonctionner.

# 1.5 SUPPORTS DE TRANSMISSION

### 1. Le Câble à Paire Torsadée

Une paire torsadée est une ligne de transmission formée de deux fils conducteurs enroulés en hélice l'un autour de l'autre. Cette configuration a pour but de maintenir précisément la distance entre les fils et de diminuer la diaphonie. Il existe deux types de paires torsadées : La paire torsadée blindée (STP) et la paire torsadée non blindée (UTP).

### 2. Le Câble Coaxial

### Ce câble est parfois appelé câble BNC, est un fil de cuivre relativement rigide noyé dans une housse en plastique isolante, elle-même entourée d'un second conducteur constitué d’une treille métallique jouant le rôle d'écran vis-à-vis des interférences. Ici les données sont aussi envoyées sous forme des impulsions électriques et ils peuvent atteindre 200m sans répéteur.

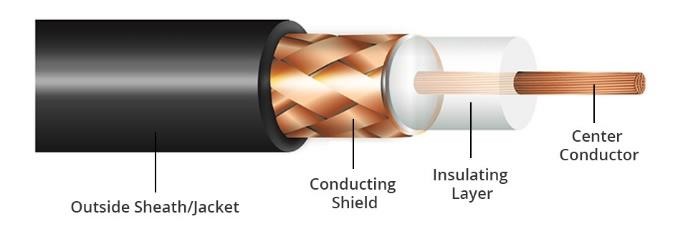


Figure 1. 12 le câble coaxial

### 3. La Fibre Optique

C’est un fil en verre protégé par un enrobage en plastique très fin

qui a la propriété de conduire la lumière. Elle est insensible aux interférences car la lumière n'est pas sensible aux parasites électromagnétiques..[[16]](#footnote-16)



Figure 1. 13 la fibre optique

# 1.5.2 Support de Transmission non Filaire

La transmission sans fil ou non guidés, s’effectue grâce aux ondes électromagnétiques. Ces supports sont utilisés généralement dans la technologie GSM, Bluetooth, WI-FI, Li-Fi, WIMAX, etc.

### 1. Les ondes lumineuses

Elles sont sur le principe suivant, une source de lumière concentrée laser envoie un faisceau unique, porteur de données, à un récepteur optique pouvant être situé à plusieurs certaines de mètres.

### 2. Les ondes radio

Une onde radioélectrique, communément abrégée en onde radio, est une onde électromagnétique dont la fréquence est inférieure à 300 MHz, soit une longueur d'onde dans le vide supérieur à 1 mètre.

### 3. Les ondes infrarouges

L’infrarouge permet de crée des liaisons sans files de quelques mètres avec un débit pouvant monter à quelques mégabits par seconde. Avant l'arrivée des technologies radio comme le Wi-Fi et le Bluetooth, il était malgré tout possible de transférer des données sans fil entre deux appareils, grâce à l'infrarouge.[[17]](#footnote-17)

# 1.6 ARCHITECTURE DES RESEAUX

# 1.6.1. Architecture Post to Post

Dans une architecture Post to Post (où dans sa dénomination anglaise peer to peer), contrairement à une architecture de réseau de type [client/serveur,](https://bastien.smeuh.org/initiation/client.php3) il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau est un peu serveur et un peu client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder via le réseau.[[18]](#footnote-18)

Les réseaux poste à poste ne nécessite pas les mêmes niveaux de

performance et de sécurité que les logiciels réseaux pour serveurs dédiés. La mise en œuvre d'une telle architecture réseau repose sur des solutions standards :

* Placer les ordinateurs sur le bureau des utilisateurs
* Chaque utilisateur est son propre administrateur et planifie lui-même sa sécurité
* Pour les connexions, on utilise un système de câblage simple et apparent

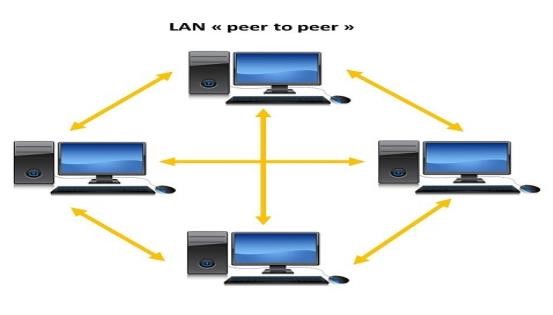


Figure 1. 14 Architecture Post to Post

# 1.6.2. Architecture Client-Serveur

L’environnement client–serveur désigne un mode de transaction (souvent à travers un [réseau)](https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique) entre plusieurs [programmes](https://fr.wikipedia.org/wiki/Programme_(informatique)) ou [processus](https://fr.wikipedia.org/wiki/Processus) : l'un, qualifié de [client,](https://fr.wikipedia.org/wiki/Client_(informatique)) envoie des requêtes ; l'autre, qualifié de [serveur,](https://fr.wikipedia.org/wiki/Serveur_informatique) attend les requêtes des clients et y répond. Le serveur offre ici un service au client.

Les [entrées-sorties](https://fr.wikipedia.org/wiki/Entr%C3%A9es-sorties) et les [connexions réseau,](https://fr.wikipedia.org/wiki/Connexion_r%C3%A9seau) afin de pouvoir répondre de manière efficace à un grand nombre de clients. Les clients sont souvent des ordinateurs personnels ou terminaux individuels (téléphone, tablette), mais pas systématiquement. Un serveur peut répondre aux requêtes de plusieurs clients. Parfois le client et le serveur peuvent être sur la même machine[[19]](#footnote-19).

Il existe une grande variété de serveurs et de clients en fonction des besoins ou services à fournir :

* un [serveur Web](https://fr.wikipedia.org/wiki/Serveur_web) publie des pages Web demandées par des [navigateurs Web](https://fr.wikipedia.org/wiki/Navigateur_web) ;
* un [serveur de messagerie électronique](https://fr.wikipedia.org/wiki/Serveur_de_messagerie_%C3%A9lectronique) transmet les courriels à des [clients de messagerie](https://fr.wikipedia.org/wiki/Client_de_messagerie) ;
* un [serveur de fichiers](https://fr.wikipedia.org/wiki/Serveur_de_fichiers) permet de partager des fichiers sur un réseau aux machines qui le sollicitent ;
* un [serveur de base de données](https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_gestion_de_base_de_donn%C3%A9es) permet aux clients de récupérer des données stockées dans une [base de données,](https://fr.wikipedia.org/wiki/Base_de_donn%C3%A9es) etc.20

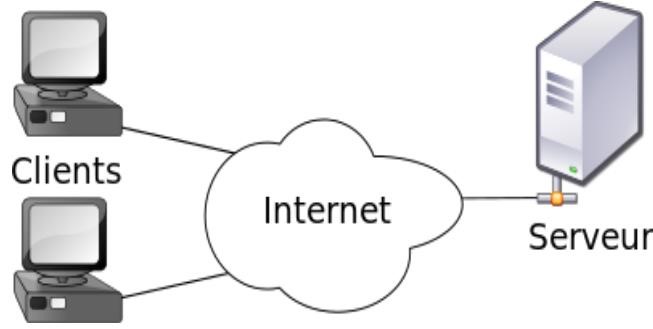


Figure 1. 15 Architecture Client-Serveur

# 1.7 Le modèle de Référence

# 1.7.1 Le modèle de Référence OSI

Le modèle OSI (Open System Interconnect ou Interconnexion de Systèmes Ouverts) a été créée par l’ISO qui a pour but de spécifier l’Architecture de réseau. On peut retenir qu’un modèle OSI sert à mettre en relation tous les terminaux se trouvant dans les mêmes ou différents environnements afin de se changer ou se communiquer entre eux.

Les couches sont reparties de la manière suivante : Les couches 1, 2, 3 et 4 sont dites les couches basses et les couches 5, 6 et 7sont dites les couches hautes. Cette répartition des fonctions réseau est appelée organisation en couches.[[20]](#footnote-20)

|  |  |  |
| --- | --- | --- |
| **N°** | **COUCHE** | **FONCTION** |
| **07** | **APPLICATION** | Assure l’utilisation d’un navigateur Web, quand vous êtes connecté. Ex : Google ; Opera, etc… |
| **06** | **PRESENTATION** | Prend en charge la représentation des données circulant entre les différents systèmes d’un réseau. Permet de rendre les fichiers compatibles dans un format idéal de la machine émettrice et réceptrice. |
| **05** | **SESSION** | Permet à deux machines de créer une connexion permanente. Cette couche oriente le traitement de la communication entre deux machines. Vérifie le type de système de fichier de l’information que vous voulez envoyer. |
| **04** | **TRANSPORT** | Veillent à ce que les paquets soient livrés selon l’ordre dans lequel ils ont été envoyés, sans porté ni duplication des données. |
| **03** | **RESEAU** | Détermine le chemin d’accès physique des données à transmettre, en fonction du réseau, de la priorité du service.   * Le Routeur intervient à ce niveau * Le Switch Manageable   Gère les couches physiques et liaison  Adresse matérielle ou MAC |
| **02** | **LIAISON** | Elle est chargée d’assurer un transfert de trames des données, exemple : une erreur entre deux ordinateurs via la couche physique. C’est à ce niveau qu’intervient l’adresse MAC (Medium Acess Control).  S’occupe de :   * Définir des règles pour l’émission et la réception de données * Accès au média |
| **01** | **PHYSIQUE** | Cette couche permet de transformer un signal binaire en un signal compatible avec le support choisi (cuivre, fibre optique, etc.) S’occupe de :   * La transmission de bits sur un canal de communication ; * Les supports physiques de transmission de données ; * La résolution de possibilités de transmission dans les deux sens (Half et Full duplex) ; |

Tableau 1. 1 couches du Modèle OSI

# 1.7.2 Le modèle de Référence TCP/IP

TCP/IP est une suite de protocoles. Le sigle TCP/IP signifie «

Transmission Control Protocol/Internet Protocol » et se prononce « T-C-P-IP ». TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données[[21]](#footnote-21).

# 1.7.2.1. Couche accès réseau

La couche accès réseau est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau :

* Acheminement des données sur la liaison ;
* Coordination de la transmission de données (synchronisation) ;
* Format des données ;
* Conversion des signaux (analogique/numérique) ;  Contrôle des erreurs à l'arrivée.

#### 1.7.2.2. La couche internet

La couche Internet est la couche "la plus importante" (elles ont

toutes leur importance) car c'est elle qui définit les datagrammes, et qui gère les notions d'adressage IP. Elle permet l'acheminement des datagrammes (paquets de données) vers des machines distantes ainsi que de la gestion de leur fragmentation et de leur assemblage à réception[[22]](#footnote-22).

La couche Internet contient 5 protocoles :

* Le protocole IP
* Le protocole ARP
* Le protocole ICMP
* Le protocole RARP
* Le protocole IGMP Les trois premiers protocoles sont les protocoles les plus importants de cette couche.

# 1.7.2*.*3. La couche transport

Les protocoles des couches précédentes permettaient d'envoyer des informations d'une machine à une autre. La couche transport permet à des applications tournant sur des machines distantes de communiquer. La couche transport contient deux protocoles permettant à deux applications d'échanger des données indépendamment du type de réseau emprunté (c'està-dire indépendamment des couches inférieures...), il s'agit des protocoles suivants :

* TCP, un protocole orienté connexion qui assure le contrôle des erreurs
* UDP, un protocole non orienté connexion dont le contrôle d'erreur est archaïque

# 1.7.2*.*4. La couche application

La couche application est la couche située au sommet des couches de protocoles TCP/IP. Celle-ci contient les applications réseaux permettant de communiquer grâce aux couches inférieures. Les logiciels de cette couche communiquent donc grâce à un des deux protocoles de la couche inférieure (la couche transport) c'est-à-dire TCP ou UDP[[23]](#footnote-23). Les applications de cette couche sont de différents types, mais la plupart sont des services réseau, c'est-àdire des applications fournies à l'utilisateur pour assurer l'interface avec le système d'exploitation. On peut les classer selon les services qu'ils rendent :

* Les services de gestion (transfert) de fichier et d'impression ;
* Les services de connexion au réseau ;
* Les services de connexion à distance ;
* Les utilitaires Internet divers.

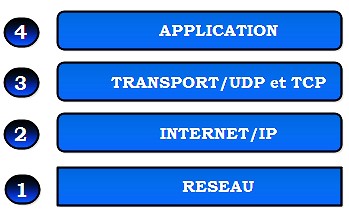


Figure 1. 16 modèle TCP/IP

# 1.8 NOTION DE BASE D’ADRESSAGE IP

Une adresse IP est un numéro unique attribué à un équipement qui veut être connecté en réseau. Si deux équipements reliés directement l’un à l’autre par une liaison de données n’ont pas de problème d’identification du correspondant, il n’en va pas de même pour les abonnés des grands réseaux : chacun d’eux doit posséder une identité unique, afin que les commutateurs acheminent les données au bon destinataire.[[24]](#footnote-24)

# 1.8.1 Adresse Physique

L’adresse physique est l’adresse de l’équipement situé au plus près du support de transmission. Elle identifie l’interface série utilisée pour l’émission et la réception des données. Elle distingue, parmi plusieurs interfaces série disponibles, celle vers laquelle émettre ou depuis laquelle sont reçues des données.[[25]](#footnote-25)

# 1.8.2 Les Adresses IP (Internet Protocol)

L’adressage utilisé dans l’Internet est un adressage logique. Chaque équipement possède un nom symbolique auquel on fait correspondre l’adresse logique appelée adresse IP. Celle-ci se décompose en deux parties : l’identificateur du réseau, où se trouvent l’équipement, et l’identificateur de la machine elle-même (qui a une signification locale à ce réseau). L’ensemble tient sur 32 bits soit 4 octets.[[26]](#footnote-26)

# 1.8.3 Les Classe d’adresses

Notions de sous-réseaux et de masque La hiérarchie à deux niveaux (réseau et machine) de l’adressage IP : s’est rapidement révélée insuffisante à cause de la diversité des architectures des réseaux connectés. Nous avons 5 plages d’IP mais il y a que 3 adresses qui sont désignés pour une utilisation strictement en interne et donc privée notamment :

|  |  |  |
| --- | --- | --- |
| **CLASSE** | **DETAIL** | **PLAGE D’ADRESSE IP PRIVEE** |
| **A** | 1-126 | 10.0.0.0 - 10.255.255.255 |
| **B** | 128-191 | 172.16.0.0 - 172.31.255.255 |
| **C** | 192-223 | 192.168.0.0 -192.168.255.255 |
| **D** | 224-239 | AUCUN |
| **E** | 240-255 | AUCUN |

Tableau 1. 2 Classe d'adresse IP

# 1.8.4 Les Adresses IP Publiques

Les adresses IP publique sont des adresses qui sont utilisées sur des hôtes, qui doivent être accessible au public depuis l’Internet. La stabilité d’Internet dépend du fait que chaque adresse publique soit unique.

# 1.9 LA SECURITE INFORMATIQUE 28

La sécurité des systèmes d’information (SSI) ou plus simplement la sécurité informatique, est l’ensemble des moyens matériels, logiciels, techniques, organisationnels et humains nécessaires à la mise en place des systèmes visant à empêcher l’utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d’information.

#### 1.9.1 Introduction à la sécurité informatique

La mesure représente le type d’action susceptible de nuire dans l’absolu, tandis que la vulnérabilité représente le niveau de l’exposition face à la menace dans un contexte particulier. Enfin la contre-mesure est l’ensemble des actions mises en œuvre en prévention de la menace.

# 1.9.2 Les cause de l’insécurité

On distingue généralement deux types d’insécurités :

* **L’état actif de l’insécurité** ; c’est-à-dire la non connaissance par l’utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple le fait de ne pas désactiver des services réseaux non nécessaires à l’utilisateur).
* **L’état passif de l’insécurité ;** c’est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l’administrateur (ou l’utilisateur) d’un système ne connait pas les dispositifs de sécurité dont il dispose.

# 1.9.3 Objectifs de la sécurité informatique

Le système d’information est généralement défini par l’ensemble des données et des ressources matérielles et logicielles de l’entreprise permettant de les stocker ou de le faire circuler. Le système d’information représente un patrimoine essentiel de l’entreprise, qu’il convient de protéger.

La sécurité informatique, d’une manière générale, consiste à mesurer que les ressources matérielles ou logicielles d’une organisation sont uniquement utilisées dans le cadre prévu. [[27]](#footnote-27)

La sécurité informatique vise généralement quatre principaux objectifs :

**L’intégrité** : c’est-à-dire, garantir que les données sont bien celles que l’on croit être ; vérifier l’intégrité des données consiste à déterminer si les données n’ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

* **La confidentialité** : consiste à mesurer que seules les personnes autorisées aient accès aux ressources échangées ; c’est-à-dire rendre l’information inintelligible à d’autres personnes que les seuls acteurs de la transaction.
* **La disponibilité** : permettre de maintenir le bon fonctionnement du système d’information et garantir l’accès à un service ou à des ressources.
* **L’authentification** : consiste à mesurer que les seuls les personnes autorisées aient accès aux ressources. C’est aussi assurer l’identité d’un utilisateur.

1.9.4 Les attaques et anarques [[28]](#footnote-28)

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Une attaque est l’exploitation d’une faille d’un système informatique (système d’exploitation, logiciel ou bien même de l’utilisateur) à des fins non connues par l’exploitant du système et généralement préjudiciables. Afin de contrer ces attaques il est indispensable de connaitre les principaux types d’attaques afin de mettre en œuvre des dispositions préventives. Les motivations des attaques peuvent être de différentes sortes :

* Obtenir un accès au système ;
* Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
* Glaner des informations personnelles sur un utilisateur ;
* Récupérer des données bancaires ;
* S’informer sur l’organisation (entreprise de l’utilisateur, etc…)

## 1.9.5 Types d’attaque[[29]](#footnote-29)

Les systèmes informatiques mettent en œuvre différentes composantes, allant de l’électricité pour alimenter les machines au logiciel exécuté via le système d’exploitation et utilisant le réseau.

Les attaques peuvent intervenir à chaque maillon de cette chaine, pour peu qu’il existe une vulnérabilité exploitable. Il est ainsi possible de catégoriser les risques de la manière suivante :

* **Accès physique** : il s’agit d’un cas où l’attaquant à accès aux locaux, éventuellement même aux machines :
* Coupure de l’électricité ;
* Extinction manuelle de l’ordinateur ;
* Vandalisme ;
* Ouverture du boitier de l’ordinateur et vol de disque dur.
* **Interception de communication**
* Vol de session ;
* Usurpation d’identité ;
* Détournement ou altération de messages.

* **Denis de service** : il s’agit d’attaques visant à perturber le bon fonctionnement d’un service. On distingue habituellement les types de déni de service suivant :
  + Exploitation de faiblesse des protocoles TCP/IP ;  Exploitation de vulnérabilité des logiciels serveurs.
* **Intrusions** :
  + Balayage de port ;
  + Elévation de privilèges : ce type d’attaque consiste à exploiter une vulnérabilité d’une application en envoyant une requête spécifique, non prévue par son concepteur, ayant pour effet un comportement anormal conduisant parfois à un accès au système avec les droits de l’application. Les attaques par débordement de tampon utilisent ce principe ;
  + Maliciels (virus, vers et chevaux de Troie)

# 1.10 Conclusion

Ce chapitre nous a permis de faire une généralité sur le réseau informatique et les aspects élémentaires des réseaux informatiques, où nous avons décrit les modèles OSI, le TCP/IP.

# CHAPITRE 2. PRESENTATION GENERALE DE LA CAISSE NATIONALE DE SECURITE SOCIALE

# 20. INTRODUCTION

Dans ce chapitre, nous allons nous borner sur la présentation de l’entreprise (organisation) faisant office de notre champ d’investigation à l’instar de la Caisse nationale de Sécurité Sociale de Kinshasa où nous allons analyser le système existant en matière de communication et l’échange entre différents postes pour effectuer une analyse critique afin d’y proposer une solution meilleure pouvant améliorer les conditions de travail de cette firme.

# 

# 2.1. APERÇUS HISTORIQUE DE LA CAISSE NATIONALE DE SECURITE SOCIALE

La caisse nationale de sécurité sociale CNSS jadis institut national de sécurité sociale INSS a été créé le 29 juin 1961, sous la dénomination de la « caisse de suspension » qui existait à l’époque coloniale. Devenu l’INSS par le décret-loi n° 16/009 du 07 juillet 2008, portant disposition générale applicable à l’établissement publics.

1. **Reformes (de l’INSS à la CNSS)**

Par le biais de la promulgation de la loi n° 16/009 du 15 juillet 2016, le régime général de sécurité sociale jadis géré par l’INSS, a connu sa première grande réforme depuis sa création. Entre en vigueur le 15 juillet 2018 la suffixé qui fixe les règles relatives aux régimes général de sécurité sociale, a apporté des innovations importantes en ce qui concerne la gestion du régime général, la couverture sociale, les prestations sociales ainsi que leurs conditions d’octroi. Cependant la pension et le risque professionnel étaient les deux branches principales de la sécurité sociale.

C’est ainsi qu’à 2018 la CNSS subrogea l’INSS en reprenant ses actifs et également ses passifs, créée sous la forme d’une entreprise privée dont l’Etat a une main mise soit créée sous tutelle de l’Etat.

En outre, la CNSS subrogea l’INSS dans les mêmes conditions dont le bénéfice, les engagements, la charge de tous les contrats et les conventions quelconques existant dans ce dernier.

* 1. **Les assujettis**

Voici les différents assujettis de la CNSS

* Les personnels publics de l’Etat, des provinces et des entités territoriales décentralisées ne bénéficiant pas de la rémunération en vertu des dispositions légales ou réglementaires d’un régime particulier de sécurité sociale ;
* Les mandataires de l’Etat dans les entreprises publiques et dans les sociétés économiques mixtes ;
* Les employés locaux des missions diplomatiques accréditées et établies en République Démocratiques du Congo ;
* Les associés actifs des sociétés ;
* Les hauts cadres des sociétés et des entreprises publiques des lors qu’ils ne sont pas liés par un contrat de travail ;
* Les membres des sociétés coopératives ouvrières de production ainsi que les gérants non-salariés des coopératives et leurs proposés ;
* Les assurés volontaires ;
* Les débiteurs exécutant un travail périlleux victime d’un accident survenu à l’occasion du travail ;
* Les assurés volontaires.

# 2.2 MISSION DE LA CAISSE NATIONALE DE SECURITE SOCIALE

La CNSS a pour mission de rendre l’importance de la sécurité sociale compréhensible par tous. Quelles actions de cette mission sont notamment :

* La filiation des employeurs ayant un ou plusieurs travailleurs ;
* L’immatriculation des travailleurs ;
* La perception des cotisations sociales des travailleurs ;
* Le paiement de prestations sociales ;
* Le suivie des dossiers des accidents ;
* Assurer la vulgarisation des employeurs et des travailleurs ;
* Assurer les transactions financières entre les cotisations versées et les prestations attribuées.

# 2.3 CADRE ORGANIQUE ET FONCTIONNEMENT

# 2.3.1. Structure organique

Selon les dispositions du décret N° 009/53 du 3 décembre 2009 fixant le statut d’un établissement public, la CNSS est un établissement public jouissant d’une personnalité juridique et d’une autonome financière, sa fonction technique et financière est placée sous tutelle du ministère de travail et prévoyance sociale.

Les organes statutaires sont :

**2.3.1.1. Le conseil d’administration**

Qui a pour mission de concevoir et orienter la grande stratégie de l’entreprise, il dispose d’un président du conseil d’administration, 2 représentants de l’Etat un représentant des organes professionnel des employeurs et un représentant des organisations des travailleurs.

**2.3.1.2 La direction générale**

Elle dispose d’un directeur général D.G et un directeur général adjoint D.G.A nommés sous l’ordonnance du président de la république qui doivent gérer l’entreprise au quotidiennes.

**2.3.1.3 Le collège de commissaire au compte**

Elle a pour mission de contrôler des transactions financières de la CNSS, il est disposé de deux membres venant de différentes structures professionnelles et également de deux membres venant de l’Etat.

**2.3.1.4 Organisation administrative**

Elle est composée par un secrétariat de des organes statutaires qui est organisée et coordonnée par 3activités dont :

La coordination de centre de gestion : c’est elle qui coordonne toutes les activités de la CNSS

Le secrétariat de la direction générale : elle est constituée d’un cabinet de travail de la direction générale

**2.3.1.5. Les directions de la CNSS**

1. La direction des ressources humaines : elle s’occupe de la gestion administrative et dans les divers rôles entre autres :

* La gestion de carrière
* La gestion du personnel : elle contrôle la ponctualité et la régularité des personnelles
* Le niveau d’étude
* La performance et l’efficacité de chaque travailleur
* Le calcul de paie des travailleurs
* Le contrôle des effectifs sur tous les travailleurs

1. La direction de l’audit interne : elle s’occupe du contrôle des enregistrements comptables et des pièces justificatives ;
2. La direction financière : elle s’occupe des transactions financières dont les paiements et les réceptions soit les cotisations sociales et les prestations sociales ;
3. La direction juridique : elle s’occupe des affaires juridiques entre la CNSS et les tiers mondes, elle s’occupe également des problèmes des contrats ;
4. La direction de recouvrement ; elle se charge de recouvrer les personnes soumises au régime général ou des assurés sociaux ;
5. La direction type et plan : elle se charge de la planification
6. La direction d’étude et organisation ; elle est chargée de structurer et organisée les activités régulières au sein de la CNSS
7. La direction de formation : elle se charge de la formation des travailleurs ou personnels de la CNSS envie de pérenniser leurs connaissances dans la pratique des différents services de l’entreprise ;
8. La direction technique : elle s’occupe de l’activité principale de la CNSS qui est « la perception des cotisations sociales et le paiement des prestations sociales »

**2.3.1.6 Les grandes directions urbaines**

* La direction urbaine de Kinshasa Sud-est (siège à Mont-ngafula) ;
* La direction urbaine de Kinshasa Ouest (siège Kintambo) ;
* La direction urbaine de Kinshasa Nord-est (siège Kinkolo) ;
* La direction urbaine de Kinshasa Centre ouest (siège Bandal) ;
* La direction urbaine de Kinshasa centre (siège Kalamu) ;
* La direction urbaine de Kinshasa Est (siège Ndjili) ;
* La direction urbaine de Kinshasa Sud (siège limete) ;
* La direction urbaine de Kinshasa Nord (siège Gombe).

**2.3.1.7 Les directions provinciales**

* La direction provinciale de LUBUMBASHI
* La direction provinciale de LIKASI
* La direction provinciale de KISANGANI
* La direction provinciale de KOLWEZI
* La direction provinciale de MATADI
* La direction provinciale de BOMA
* La direction provinciale de BUKAVU
* La direction provinciale de GOMA
* La direction provinciale de BANDUNDU
* La direction provinciale de MBUJI-MAYI
* La direction provinciale de KANANGA
* La direction provinciale de MBANZA-NGUNGU
* La direction provinciale de BUNIA
* La direction provinciale de KIKWIT
* La direction provinciale de KALEMI
* La direction provinciale de KASUMBALESA
* La direction provinciale de KINDU

**2.3.1.8 Bureaux de district**

* Bureau de district de KAMINA
* Bureau de district de KASANGI
* Bureau de district de BOENDE
* Bureau de district de BOTEMBO
* Bureau de district de TSHIKAPA
* Bureau de district de LISALA
* Bureau de district de d’HISIRO
* Bureau de district de GBADOLITE
* Bureau de district de d’UVIRA
* Bureau de district de KABINDA
* Bureau de district de LUANDA
* Bureau de district de LODJA
* Bureau de district de GEMENA
* Bureau de district de d’ILEBO

**2.3.1.9 LES ANTENNES**

* Antenne de MASISI
* Antenne de MOANDA
* Antenne de BUMBA
* Antenne de d’ARU
* Antenne de KIPUSHI
* Antenne de WASTIA
* Antenne de KALEMI
* Antenne de FIZI
* Antenne de MWEKA
* Antenne de MWENEDITU
* Antenne d’IDJOFA
* Antenne de BENI

**2.3.1.10 Les Centres De Perceptions**

* Centre de perception de KENYA
* Centre de perception de GOLF
* Centre de perception de KIMBANSEKE
* Centre de perception de BARUMBA
* Centre de perception de LEMBA
* Centre de perception de COMMERCE
* Centre de perception de la REVOLUTION
* Centre de perception de MATETE
* Centre de perception de MAKALA

**2.3.1.11 Niveau d’étude exigé pour accès à la CNSS**

* Rédacteur : diplômé d’Etat
* Chef de section : gradué
* Chef de service : licencié
* Chef de service principal : diplômé d’Etat approfondie
* Chef de division : docteur en thèse

**2.3.1.12 Catégorie et classification des emplois**

**III.3.1.12.1 Emplois des commandements (personnel direction et personnel** **d’encadrement)**

* Directeur
* Sous-directeur
* Chef de service principal
* Chef de division

**2.3.1.12.1 Emplois de collaboration (personnel de maitrise)**

* Chef de service adjoint
* Chef de section
* Chef de section adjoint
* Rédacteur adjoint

**2.3.1.12.2 Emplois d’exécution (personnel qualifié et manœuvre)**

* Commis chef
* Commis principal
* Huissier

# 2.3.2. ORGANIGRAMME HIERARCHIQUE DE LA CNSS

Figure 2. 1 Organigramme hiérarchique de la CNSS

# 2.4. ANALYSE DE L’EXISTANT

Le but final de ce projet est de mettre en place un système de messagerie à l’aide de Windows Serveur Windows intégrant le serveur MailEnable pour la messagerie afin de permettre aux agents de la CNSS de pouvoir se communiquer.

L’analyse de l’existant peut être défini comme étant une compréhension du point de vue structurel et fonctionnel du système (KONKFIE IPEPE, 2021).

Cette analyse consiste à émettre des critiques pertinentes sur le système en place afin de déceler les anomalies qui bloquent son bon fonctionnement et les points positifs contribuant ainsi à son bon fonctionnement.

# 2.4.1. Le Parc d’ordinateurs et imprimantes

Le but de cette présentation est d’avoir un aperçu général des d’ordinateurs et des imprimantes constituant le Parc informatique au sein de la Caisse Nationale de Sécurité Sociale, CNSS en sigle, en voici l’illustration :

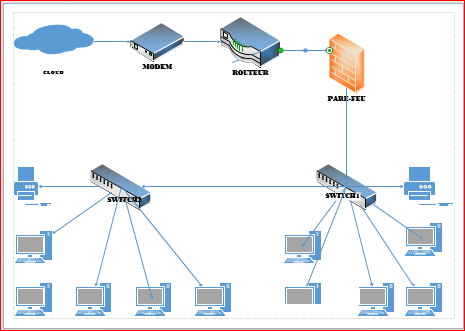


Figure 2. 2 Présentation des matériels de la CNSS

Au Total nous avons : (10) Ordinateurs ; (2) Switchs ; (6) Imprimantes ; (1) Pare-feu ; (1) Routeur ; (1) Modem

# 2.4.2 Analyse des matériels

Le but de l’analyse de l’existant est d’aboutir à l’émission des critiques objectives afin de mettre en place un système de messagerie afin de leurs permettre de commencer à se communiquer en local.

Nous remarquons que les terminaux se trouvant dans cette entreprise ont de faibles capacités.

Nous remarquons que les ordinateurs sont de faibles capacités, certains sont en assez bon états et d’autres sont en mauvaises états.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N°** | **NOM DU**  **MATERIEL** | **Nbre** | **MARQUE** | **ETAT** |
| 01 | Ordinateurs | 10 | * (10) FIXE HP Disque dur :320Go / RAM : 2 Go Processeur :2.20 Ghz SE : Windows 10 64bits | (10) : Bon  (2) : Mauvais |
| 02 | Imprimantes | 06 | * (2) LaserJet 202 /Color * (4) Noir & Blanc 426 DW Vitesse 38ppm Format : A4   Résolution: 1200×1200p | (6) Bon |
| 03 | Routeur | 01 | * D-LINK 4 Ports Ethernet et 1 WAN | (1) Bon |
| 04 | Switch | 01 | * D-LINK 24 Ports FasthEthernet | (1) Bon |
| 05 | Modem | 01 | D-LINK | (1) Bon |

Tableau 2. 1Description du parc informatique de la CNSS

# 2.5 CRITIQUE DE L’EXISTANT

# 2.5.1. POINTS FORTS

La CNSS organise une bonne collaboration entre ses agents.

# 1.5.2. POINT FAIBLE

Les ressources matérielles de la CNSS sont correctes et fonctionnent normalement sans souci majeur. Il est juste impérieux d’y ajouter certains matériels qui seront nécessaire lors de l’amélioration du système existant.

Les logiciels qui sont installés dans des ordinateurs dans la CNSS nécessitent une fréquence (journalière, hebdomadaire ou mensuelle) de mise à jour. L’utilisation des logiciels obsolètes peut parfois être fatale pour l’entreprise. Il faudrait mieux aussi ajouter certains logiciels plus spécifiques pour la bonne gestion du réseau.

# 2.6 CONCLUSION

Ce chapitre était concentré à l’analyse de l’existant, nous avions fait les critiques de l’existant de la Caisse Nationale de Sécurité Sociale. CNSS en sigle.

# **CHAPITRE 3 : DEPLOIEMENT DU NOUVEAU SYSTEME**

# [**3.1**](tel:3.1)**. INTRODUCTION**

Dans ce chapitre nous allons procéder aux différentes configurations pour la réalisation du système de notre réseau Local. Pour atteindre ce but nous passerons en revue quelques notions rudimentaires et techniques indispensables au déploiement du système.

# [3.2](tel:3.2). ÉTUDE TECHNIQUE

Cette étude va permettre de déterminer plusieurs paramètres techniques tels que l’Architecture, l’inventaire de matériels, la qualité de service et autres… ; pour la mise en place en œuvre de notre nouveau système.

Parmi les normes existantes dans le réseau, nous portons le choix sur la norme 802.3, car dans cette norme, le réseau gère une ou plusieurs *bases* (ou *bornes* ou *points d’accès*). Lorsqu’un réseau comprend plusieurs bornes, celles-ci sont raccordées par un réseau Ethernet filaire. Outre l’acheminement des données, nous avons :

* Topologie physique utilisée est en étoile
* Topologie Logique utilisée est Ethernet
* La confidentialité, cela consiste à utiliser une méthode de chiffrement.
* La distribution, c’est l’équivalent du routage dans un réseau classique.

# 3.3 CHOIX DES MATERIELS INFORMATIQUES

|  |  |  |
| --- | --- | --- |
| **Equipements** | **Détail et commentaire** | **Nombre** |
| Onduleur | Onduleur VICTRON Phoenix 48/15 KVA  Le Victron permet de conserver de l’énergie plus longtemps et une meilleure gestion à distance, on configure le remote Ethernet afin de gérer l’équipement via un réseau IP. | 11 |
| Routeur | D-LINK D:\Projet\A\8.pnggère le routage des paquets entre différents réseaux capacité de filtrage et de VPN peut être un plus | 1 |
| Switch | D-LINK Est un switch dédié pour les entreprises, permet la gestion des interfaces | 1 |
| Pare-feu | PFSENSE  contrôle le trafic entre les réseaux interne; externes et la DMZ | 1 |

Tableau 3. 1 Choix des matériels

# 3.4 CHOIX DES LOGICIELS

|  |  |  |
| --- | --- | --- |
| **Anti-Virus** | Eset Solution V7 pour 4 postes y compris le serveur. Le serveur d’Anti-Virus nécessite un serveur de gestion des Licences pour la protection contre les virus | **3** |

Tableau 3. 2 Choix des logiciels

# 3.5 PLAN D'ADRESSAGE IP

|  |  |
| --- | --- |
| **ADRESSE RESEAU** | 192.168.0.0 |
| **MASQUE PAR DEFAUT** | 255.255.255.0 |
| **PARE-FEU PFSENSE** | 192.168.0.1 |
| **ROUTEUR** | 192.168.0.2 |
| **PLAGE D’ADRESSES DHCP** | |
| **ADRESSE DU DEBUT** | 192.168.0.3 |
| **ADRESSE DE LA FIN** | 192.168.0.254 |
| **ADRESSE DE DIFFUSION** | 192.168.0.255 |

Tableau 3. 3 Plan d’adressage

# [3.5](tel:3.2.4). SCHEMA DE CABLAGE DU RESEAU

# 

Figure 3. 1 schéma de câblage du réseau

Figure 3. 2 Schéma de câblage du réseau

# [3.](tel:3.2.5)6. SCHEMA DE PRINCIPE DU RESEAU

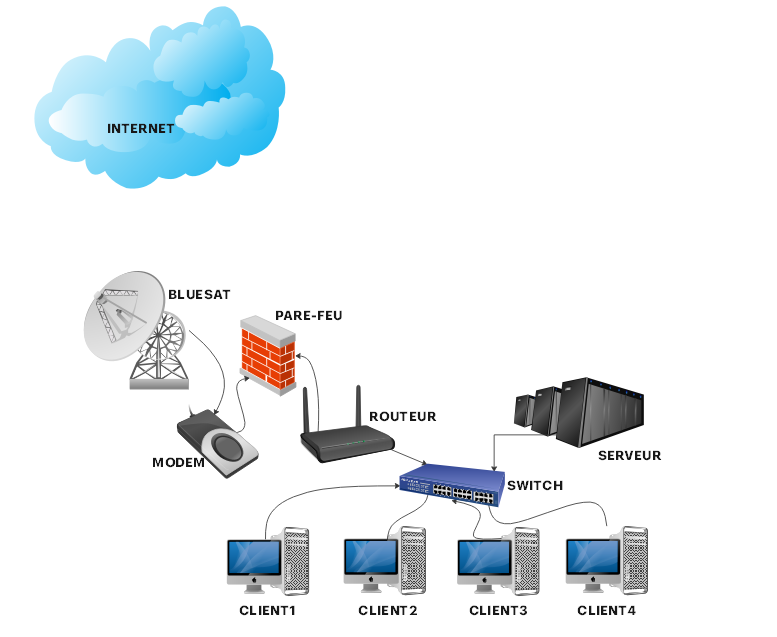
****

Figure 3.3 Schéma de principe du réseau

3.7. INSTALLATION ET CONFIGURATION DES TERMINAUX   
[3.7.1](tel:3.3.1). Installation du Système d'exploitation

L’installation de Windows 10 peut se passer vers la clé USB ou vers le DVD et nous aurons besoins de deux fichiers principaux :

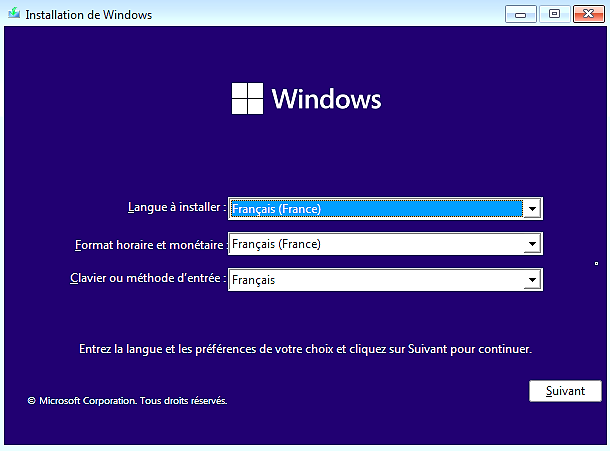


Figure 3. 4 Fenêtre d’accueil d’installation de Windows 11

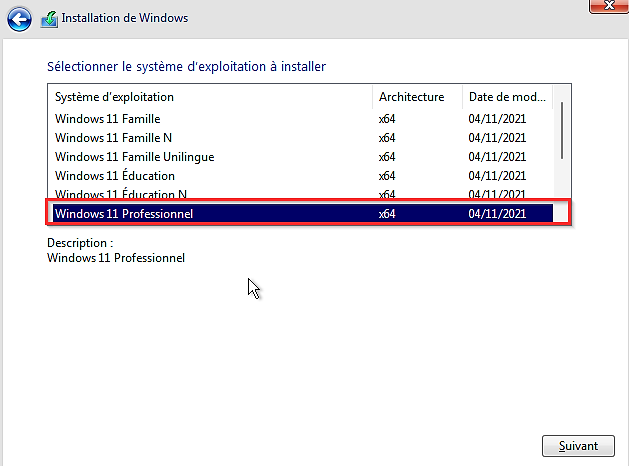
Nous allons choisir le type de système à installer, vu notre cas, nous allons choir le type Professionnel.

Figure 3. 5 Le Choix du Type

Nous allons accepter le terme de contrat et licence

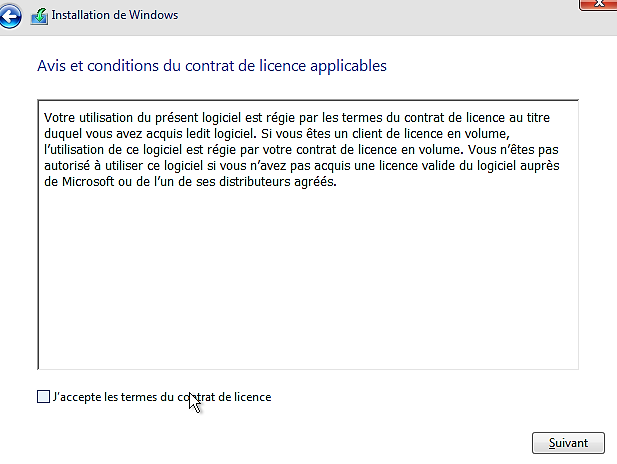


Figure 3. 6 Acceptation du terme de contrat de licence

Deux choix s’offre à nous : la mise à niveau et personnalisé, cliquer sur personnalisé.

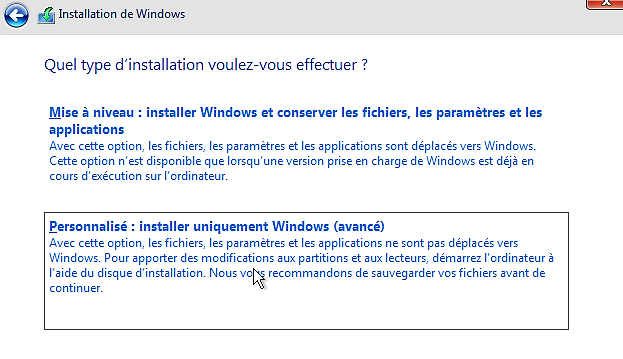


Figure 3. 7 Choix d'installation

A ce niveau, nous allons allouer notre espace de stockage

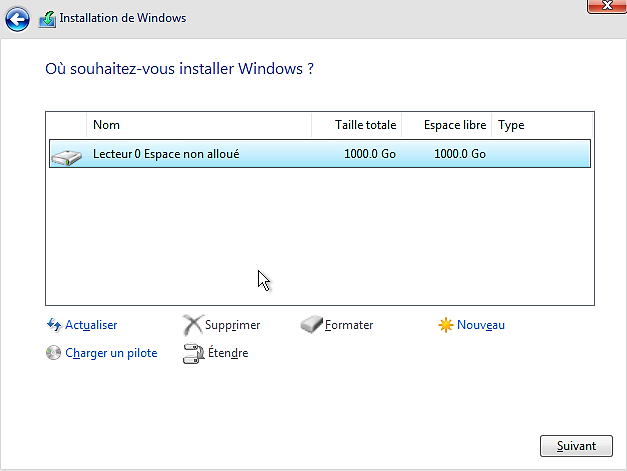


Figure 3. 8 Allocation de l'espace de stockage

Enfin se poursuit l’installation du système d’exploitation :

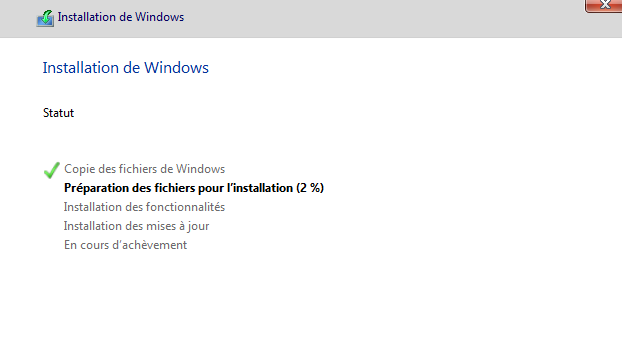


Figure 3. 9 Processus d'installation

# 3.7.2 INSTALLATION ET CONFIGURATION DU PARE-FEU

1. **Installation du routeur pfSense**

Pour choisir le boot pfSense ou laisser démarrer avec l'option par défaut.

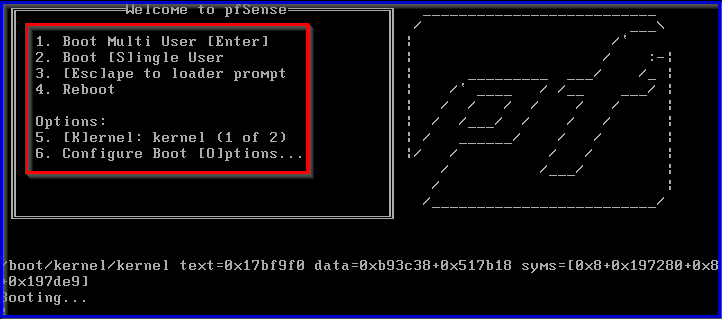


Figure 3. 10 Démarrage de PfSense

Accepter les choix en descendant puis valider ;



Figure 3. 11 Acceptation de l’installation

Opter pour une installation facile puis confirmer à l'écran suivant.

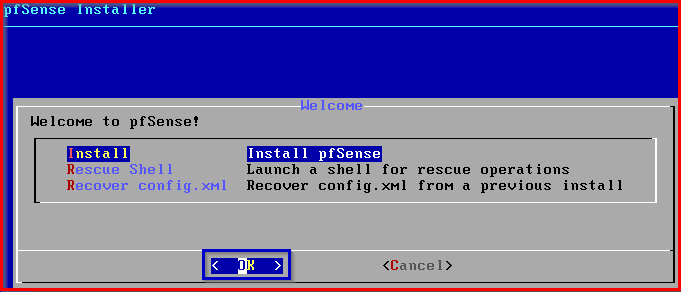


Figure 3. 12 Installation du Pfsense

L’installation du noyau : laisser le choix par défaut puis valider.



Figure 3. 13 Installation du noyau

Choisissons la partition automatique ‘’UFS’’

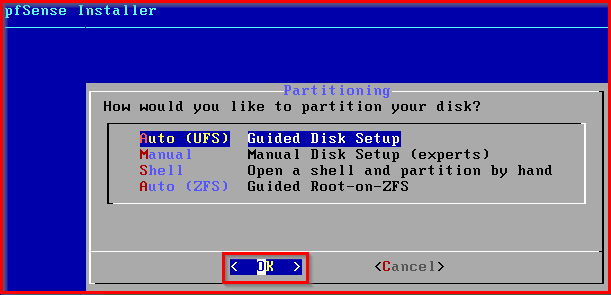


Figure 3. 14 Partitionnement UFS

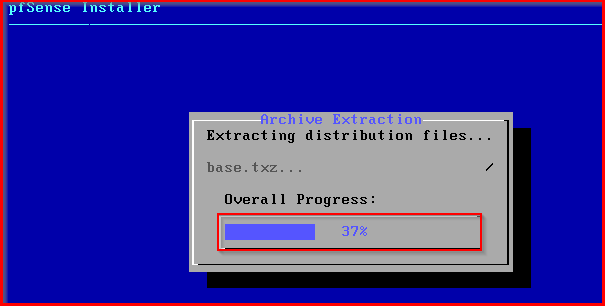
Cliquez sur **ok** pour lancer l’installation de routeur pfSense

Figure 3. 15 Progression d’installation

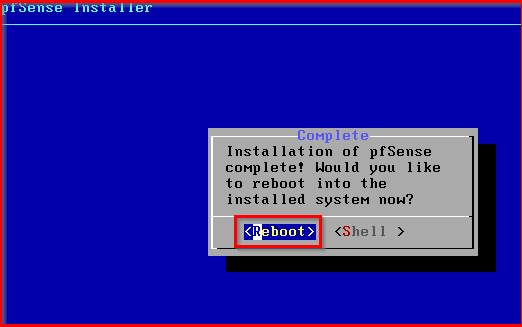
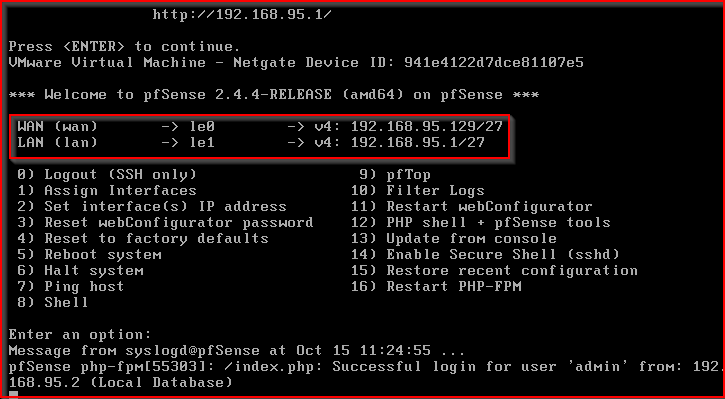
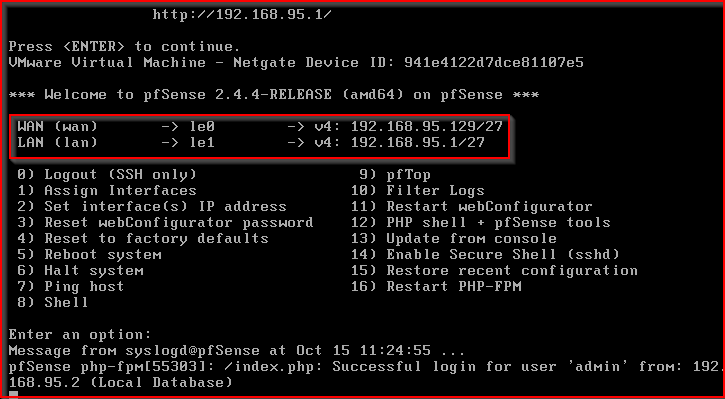
Rebooter lorsqu’on y est invités.

Figure 3. 16 Rebooter

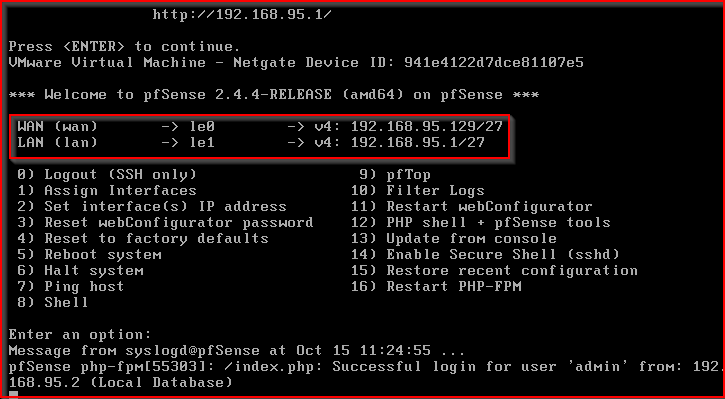
**CONFIGURATION DES INTERFACES RESEAU**

Dans notre cas « le0 » correspond à l’interface WAN par contre le1 correspond au LAN qu’il faudra configurer. Entrer « 2 » pour lancer la configuration IP d'une interface.

Répondre aux questions pour configurer l’interface : adresse IP via DHCP ou adresse IP statique, nombre de bits de sous-réseau etc. La configuration IP d'une interface se termine par une question demandant si nous souhaitons autoriser l'accès en http à l'interface web via cette interface.



**192.168.0.1**



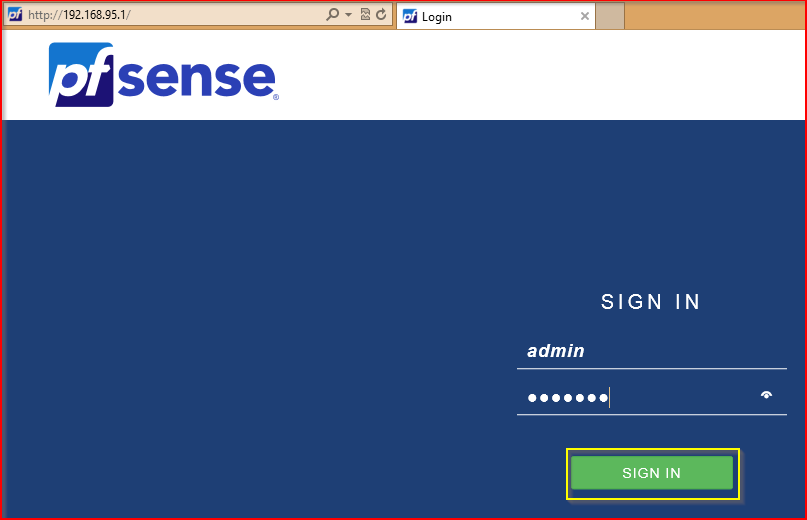
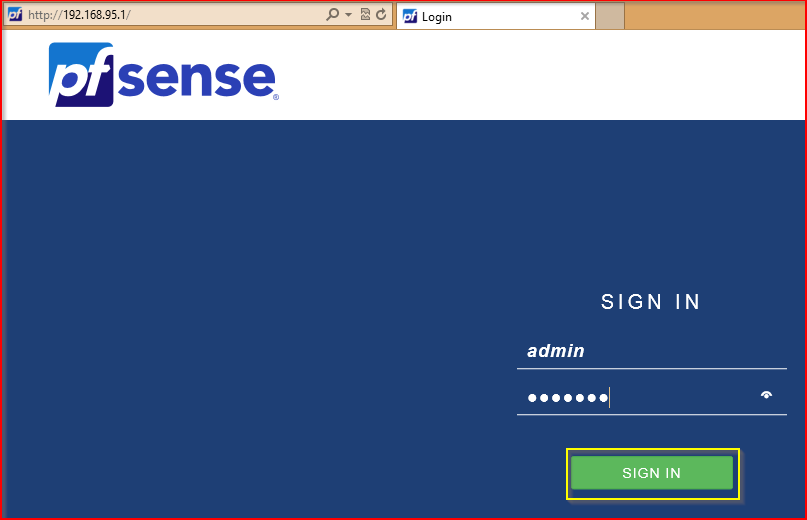
**10.10.10.1/8**

**192.168.0.1/24**

Figure 3. 17 Fin de Configuration des interfaces

Nous allons entrer les informations suivantes :

Figure 3. 18 Authentification du pare-feu



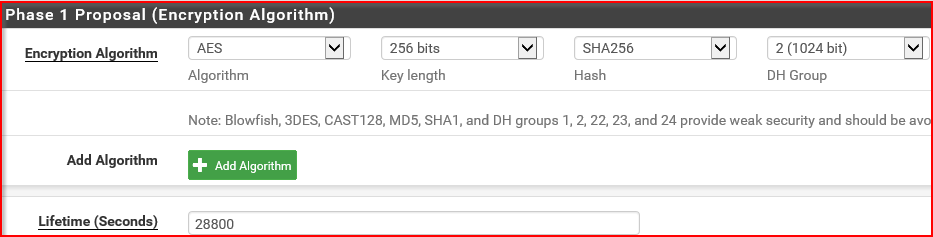


Figure 3. 19 L’algorithme de cryptage

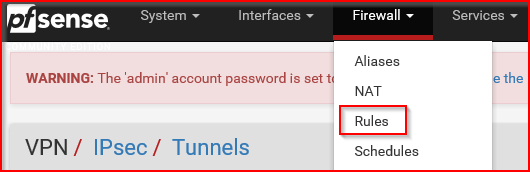
Nous allons cliquer sur Firewall ensuite sur Rules

Figure 3. 20 Lancement de la configuration de pare-feu

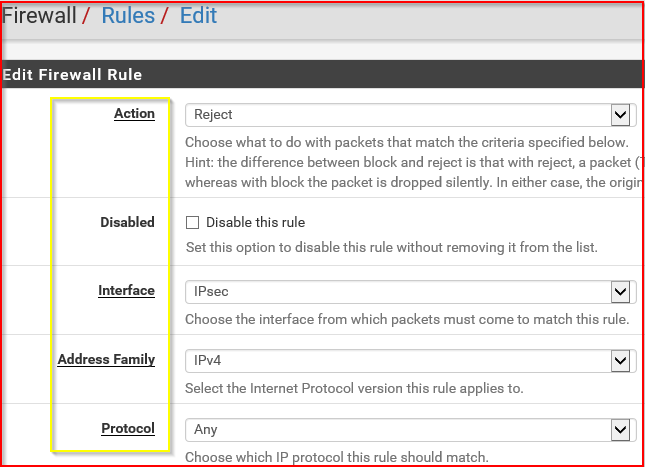
Nous allons activer les actions afin de rejecter les activités.

Figure 3. 21 Action de pare-feu pfSense

A retenir que cette même opération sera faite pour l’interface WAN et voici le résultat dans la figure ci-dessous.

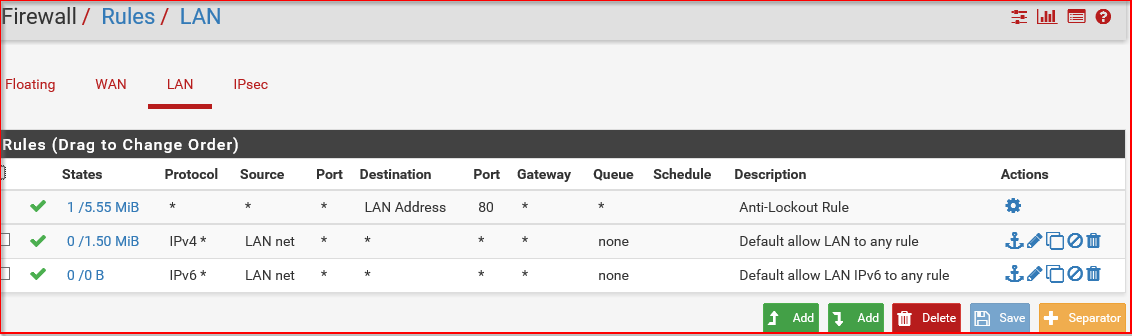


Figure 3. 22 Fin de la configuration de firewall

# 3.7.3 TEST DE CONNECTIVITE

Pour Tester la connectivité, nous irons dans l’invite de commande. Nous allons faire appel à la commande PING suivie de l’adresse IP

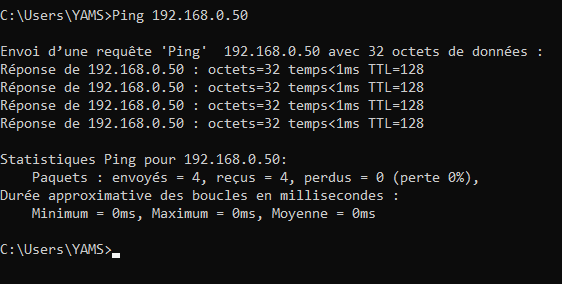
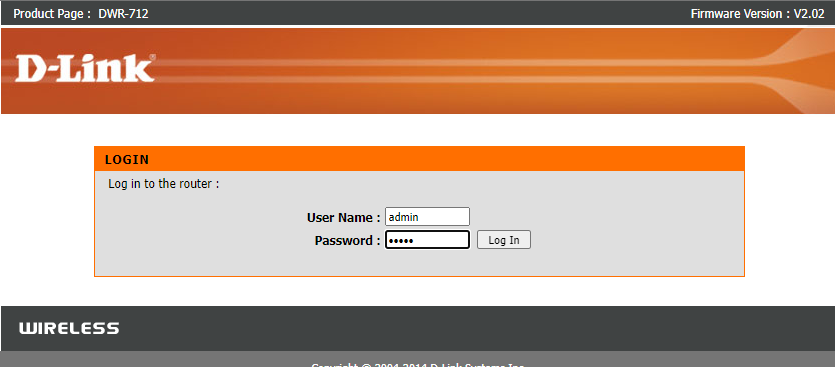
****

Figure 3. 23 Test de connectivité

Figure 3. 24 Test de connectivité

# 3.8 CONFIGURATION DU DMZ VIA LE ROUTEUR D-LINK

Nous allons s’authentifier en tant qu’Administrateur

Dans ce niveau, nous allons cliquer sur ADVANCE pour configurer

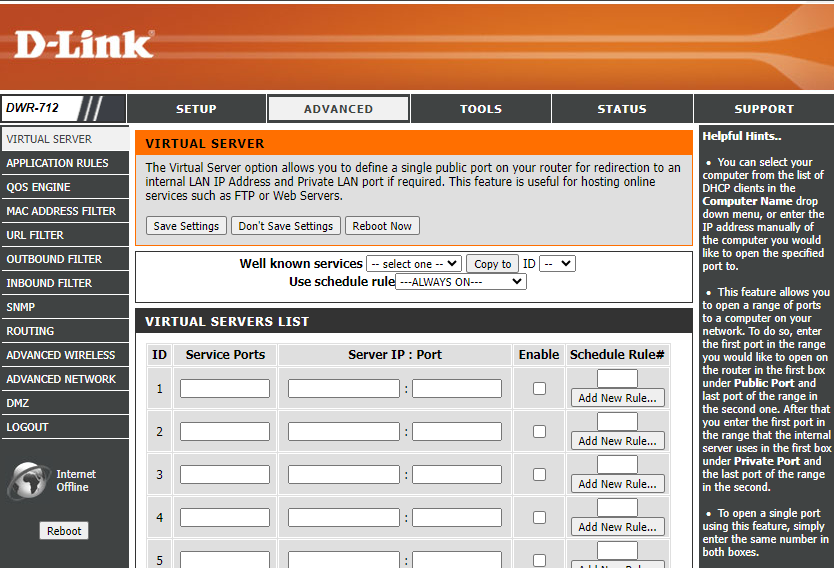


Figure 3. 25 Activation du DMZ

Figure 3. 26 Authentification

Nous allons identifier les plages qui seront dans le DMZ

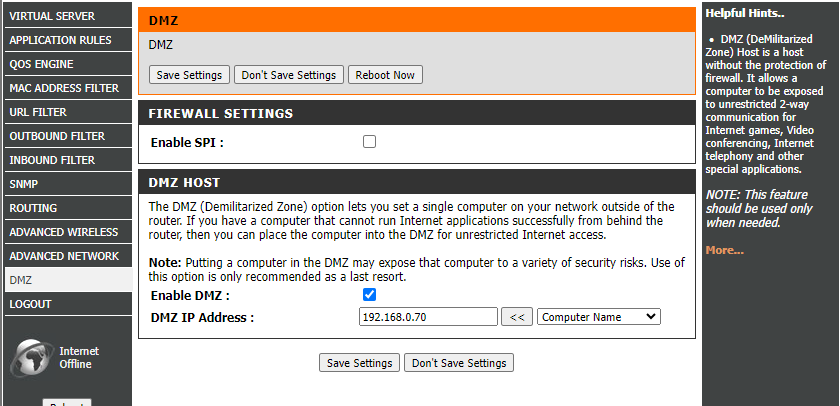


Figure 3. 27 Ajout d'adresse IP dans la ZONE DMZ

Nous allons ajouter une liste d’adresses qui seront dans la Zone DMZ

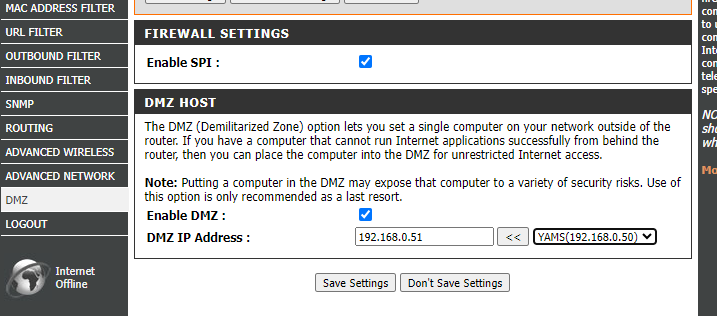


Figure 3. 28 Ajout de Host dans le DMZ

Interdiction des passages dans les sites suivants :

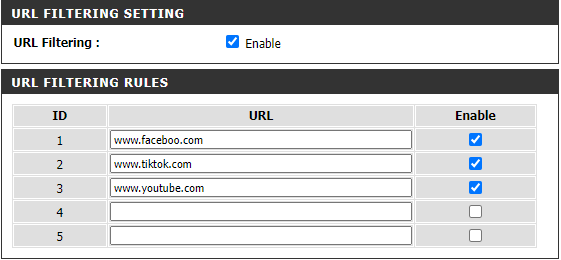


Figure 3. 29 Filtrage des sites

# 3.9. Estimation des coûts du projet

Voici dans le tableau ci-après l’estimation des coûts de notre projet :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N° | Matériels | Quantité | Prix unitaire | Prix total |
| 01 | Ordinateur | 11 | 300$ | 2750$ |
| 02 | Routeur | 1 | 100$ | 100$ |
| 03 | Pare-feu | 1 | 150$ | 150$ |
| 04 | Switch | 1 | 80$ | 80$ |
| 05 | Onduleur | 11 | 40$ | 440$ |
| 06 | Anti-virus | 3 | 30 | 90$ |
| **TOTAL** | | | | **3 610$** |
| Main d’œuvre 30% Achat de matériels | | | | **1083$** |
| Imprévu 10% achat de matériels | | | | **361$** |
| Cout total du projet | | | | **5054$** |

Tableau 3. 4 Tableau synthèse du projet

# 3.9 CONCLUSION

Tout au long de ce chapitre nous avions mise en place une zone démilitarisée au sein de la CNSS, pour parvenir à ce résultat nous avions tout au début considéré les spécifications techniques puis nous avions configuré le point d’accès sans fil pour diffuser le signal sans fil aidant les utilisateurs à se connecter.

# CONCLUSION GENERALE

Nous voici arriver à la fin de notre travail, qui a porté sur CONCEPTION ET OPTIMISATION D’UNE INFRASTRUCTURE DE RESEAU LOCAL SECURISE INTEGRANT UNE ZONE DEMILITARISE POUR RENFORCER LA PROTECTION DES UTILISATEURS CAS DE CNSS» Le problème rencontré sur le terrain de recherche était caractérisé notamment par la manque d’un système informatiser pouvait leurs permettre de se communiquer en local en temps réel et de se protéger contre toutes les attaques.

Pour désengorger ce problème, il nous a fallu mettre sur pied un réseau local qui va mettre tous les équipements en commun en vue de partager les ressources et gérer les informations au sein de ce dernier.

Pour ce faire, par cette réalisation, nous pouvons dire que l’issue de ce travail affirme notre hypothèse.

L’installation de cette solution est le fruit d’un long temps de recherche et de travail. C’est une façon de donner le meilleur de nous-même et de contribuer à la documentation scientifique dans le domaine des réseaux informatiques. Il servira donc, d’un guide pour tous ceux qui emprunteront la même voie que nous, pour le souci d’améliorer, développer ou exploiter les bases que nous avons établies.

Nous reconnaissons qu’étant une œuvre humaine, il n’y manquera pas d’imperfections. Nous sommes ouverts à toutes formes de suggestions ou critiques que ce soit. Et laissons la place à tout autre chercheur d’améliorer si possible ce domaine de recherche.

# BIBLIOGRAPHIE

BINDUNGWA, M., comment élaborer un travail de fin de cycle Contenu et étapes, Ed. Médiaspaul, Kinshasa 2008

MACE, G. et PETRY F., Initiation à la Recherche Scientifique, Ed. Delux, 2008

ATELIN P., Réseau informatique, Ed. ENI paris, 2009, p.4

LORENZ Pascal, *architectures des réseaux et télécommunications*, Ellipse, paris, 2001

* DROMARD D. et SERET D., Architectures des Réseaux, Ed. Pearson, Paris, 2009

PUYOLLE Guy, Réseaux informatiques, Ed. Eyrolles, Paris 2008

LEMAINQUE Fabrice & PILLOU Jean-François, Tout sur les Réseaux et Internet, 3e édition Dunod, Paris 2012

DEVANBLANC O., Installer un petit réseau de PC, Ed. Dunod, Paris, 2003.

MICHAL ZALEWSKI, Menaces sur le réseau: guide pratique des attaques passives et indirectes, Edition eyrolles paris 2008

**NOTE DES COURS**

Alphonse Jacques MVIBUDULU KALUYIT KAKO, Initiation aux modèles, méthodes et pratique de la recherche opérationnelle ; Edition CRSAT, Kinshasa, Juin 2000

FATAKI J., Recherches Opérationnelles, notes de cours, L2 Réseau, ISC-Bdd, 2020-2021

MAKANGU J. architecture et réseau, notes de cours, GTMR, ISC/BDD, 2020-2021, page 29. (Inédite)

Malela G., Cours du Séminaire Informatique, G3 TMR, ISC-Bandundu 2020-2021

MALELA V.  Note de cours de réseau informatique 1, G2 TMR ISC/BDD, 2020.

PEZO NASUKA, Télématique et Réseaux informatique, L1 Réseaux Informatique, ISC – Bandundu, 2016 – 2017

**WEBOGRAHIE**

https://www.commentcamarche.net/contents/539-tcp-ip

* https://www.africmemoire.com/part.10-chapitre-ii-architecture-reseaux-troisieme-partie-714.html

[www.securité\_informatique&pratique\_configuration.fr](http://www.securité_informatique&pratique_configuration.fr)

# TABLE DES MATIERES

[EPIGRAPHE i](#_Toc206925421)

[DEDICACES ii](#_Toc206925422)

[REMERCIEMENTS iii](#_Toc206925423)

[LISTE DES ABREVIATIONS iv](#_Toc206925424)

[LISTE DES FIGURES v](#_Toc206925425)

[LISTE DES TABLEAUX v](#_Toc206925426)

[INTRODUCTION GENERALE 1](#_Toc206925427)

[0.1 Présentation du Sujet 1](#_Toc206925428)

[0.2 Choix du sujet 2](#_Toc206925429)

[0.3 Problématique 2](#_Toc206925430)

[0.4 Hypothèse 3](#_Toc206925431)

[0.5 Objectifs 3](#_Toc206925432)

[0.6 Méthode et Technique 4](#_Toc206925433)

[0.6.1 Méthode 4](#_Toc206925434)

[0.6.2 Technique 4](#_Toc206925435)

[0.7. Délimitation du sujet 4](#_Toc206925436)

[0.7.1 Spatiale 5](#_Toc206925437)

[0.7.2 Temporelle 5](#_Toc206925438)

[0.8 Subdivision du Travail 5](#_Toc206925439)

[CHAPITRE 1 : GENERALITE SUR LES RESEAUX LOCAUX 6](#_Toc206925440)

[1.0 INTRODUCTION 6](#_Toc206925441)

[1.1 DEFINITION 6](#_Toc206925442)

[1.2 TYPOLOGIE DES RESEAUX 6](#_Toc206925443)

[1.2.1 Le Réseau PAN (Personal Area Network) 6](#_Toc206925444)

[1.2.2 Réseau LAN (Local Area Network) 7](#_Toc206925445)

[1.2.3 RESEAU MAN (Métropolitain Area Network) 8](#_Toc206925446)

[1.2.3 Le Réseau WAN (Wide Area Network) 8](#_Toc206925447)

[1.3. EQUIPEMENTS D’INTERCONNEXION RESEAUX 9](#_Toc206925448)

[1.3.1 Commutateur (SWITCH) 9](#_Toc206925449)

[1.3.2 Concentrateur (HUB) 9](#_Toc206925450)

[1.3.3 Les Routeurs 10](#_Toc206925451)

[1.3.4 Passerelle 10](#_Toc206925453)

[1.3.5 Carte Réseau 11](#_Toc206925454)

[1.3.6 Le Pont 11](#_Toc206925455)

[1.4 TOPOLOGIE DES RESEAUX 11](#_Toc206925457)

[1.4.1 Topologie Physique 12](#_Toc206925459)

[1.4.1.1 La topologie en bus 12](#_Toc206925460)

[1.4.1.2 La topologie en étoile 12](#_Toc206925461)

[1.4.1.3 La topologie en anneau 13](#_Toc206925463)

[1.4.2 TOPOLOGIE LOGIQUE 13](#_Toc206925464)

[1.4.2.1 Réseau Ethernet 14](#_Toc206925465)

[1.4.2.2 Réseau FDDI (Fiber Distributed Data Interface) 14](#_Toc206925466)

[1.5 SUPPORTS DE TRANSMISSION 15](#_Toc206925467)

[1. Le Câble à Paire Torsadée 15](#_Toc206925468)

[2. Le Câble Coaxial 15](#_Toc206925469)

[3. La Fibre Optique 15](#_Toc206925471)

[1.5.2 Support de Transmission non Filaire 15](#_Toc206925472)

[1.6 ARCHITECTURE DES RESEAUX 16](#_Toc206925476)

[1.6.1. Architecture Post to Post 16](#_Toc206925477)

[1.6.2. Architecture Client-Serveur 17](#_Toc206925478)

[1.7 Le modèle de Référence 18](#_Toc206925479)

[1.7.1 Le modèle de Référence OSI 18](#_Toc206925480)

[1.7.2 Le modèle de Référence TCP/IP 19](#_Toc206925481)

[1.7.2.1. Couche accès réseau 20](#_Toc206925482)

[1.7.2*.*3. La couche transport 20](#_Toc206925483)

[1.7.2*.*4. La couche application 21](#_Toc206925484)

[1.8 NOTION DE BASE D’ADRESSAGE IP 22](#_Toc206925485)

[1.8.1 Adresse Physique 22](#_Toc206925486)

[1.8.2 Les Adresses IP (Internet Protocol) 22](#_Toc206925487)

[1.8.3 Les Classe d’adresses 22](#_Toc206925488)

[1.8.4 Les Adresses IP Publiques 23](#_Toc206925489)

[1.9 LA SECURITE INFORMATIQUE 28 23](#_Toc206925490)

[1.9.2 Les cause de l’insécurité 23](#_Toc206925491)

[1.9.3 Objectifs de la sécurité informatique 24](#_Toc206925492)

[1.9.4 Les attaques et anarques 24](#_Toc206925493)

[1.9.5 Types d’attaque 25](#_Toc206925494)

[1.10 Conclusion 26](#_Toc206925495)

[CHAPITRE 2. PRESENTATION GENERALE DE LA CAISSE NATIONALE DE SECURITE SOCIALE 27](#_Toc206925496)

[20. INTRODUCTION 27](#_Toc206925497)

[2.1. APERÇUS HISTORIQUE DE LA CAISSE NATIONALE DE SECURITE SOCIALE 27](#_Toc206925498)

[2.2 MISSION DE LA CAISSE NATIONALE DE SECURITE SOCIALE 28](#_Toc206925499)

[2.3 CADRE ORGANIQUE ET FONCTIONNEMENT 28](#_Toc206925500)

[2.3.1. Structure organique 28](#_Toc206925501)

[2.3.2. ORGANIGRAMME HIERARCHIQUE DE LA CNSS 33](#_Toc206925502)

[2.4. ANALYSE DE L’EXISTANT 34](#_Toc206925503)

[2.4.1. Le Parc d’ordinateurs et imprimantes 34](#_Toc206925504)

[2.4.2 Analyse des matériels 34](#_Toc206925505)

[2.5 CRITIQUE DE L’EXISTANT 35](#_Toc206925506)

[2.5.1. POINTS FORTS 35](#_Toc206925507)

[1.5.2. POINT FAIBLE 35](#_Toc206925508)

[2.6 CONCLUSION 35](#_Toc206925509)

[CHAPITRE 3 : DEPLOIEMENT DU NOUVEAU SYSTEME 36](#_Toc206925510)

[3.1. INTRODUCTION 36](#_Toc206925511)

[3.2. ÉTUDE TECHNIQUE 36](#_Toc206925512)

[3.3 CHOIX DES MATERIELS INFORMATIQUES 36](#_Toc206925513)

[3.4 CHOIX DES LOGICIELS 37](#_Toc206925514)

[3.5 PLAN D'ADRESSAGE IP 38](#_Toc206925515)

[3.5. SCHEMA DE CABLAGE DU RESEAU 39](#_Toc206925516)

[3.6. SCHEMA DE PRINCIPE DU RESEAU 40](#_Toc206925518)

[3.7. INSTALLATION ET CONFIGURATION DES TERMINAUX 40](#_Toc206925519)

[3.7.2 INSTALLATION ET CONFIGURATION DU PARE-FEU 43](#_Toc206925520)

[3.7.3 TEST DE CONNECTIVITE 48](#_Toc206925522)

[3.8 CONFIGURATION DU DMZ VIA LE ROUTEUR D-LINK 49](#_Toc206925523)

[3.9. Estimation des coûts du projet 51](#_Toc206925524)

[3.9 CONCLUSION 51](#_Toc206925525)

[CONCLUSION GENERALE 52](#_Toc206925526)

[BIBLIOGRAPHIE 53](#_Toc206925527)

[TABLE DES MATIERES 54](#_Toc206925528)

1. IKUMA Célestins : Méthode de recherche scientifique, L1 informatique, ISC-KIN, 2016-2017 P.90 [↑](#footnote-ref-1)
2. Julien TAZI T. KIZEY, Initiation à la recherche scientifique, G2 Tous, ISC-BDD, 2018-2019 P.40 [↑](#footnote-ref-2)
3. RONCE (1971). Méthode des sciences sociales, éd. DALLAZ, Paris, 1971, P.189 [↑](#footnote-ref-3)
4. MUKUNA, C., « *Essaie méthodologique sur la rédaction d’un travail scientifique* » Ed. CRIGED, 2006, p. 28. [↑](#footnote-ref-4)
5. ATELIN P., **Réseau informatique**, Ed. ENI paris, 2009, p.4 [↑](#footnote-ref-5)
6. EVANBLANC O., ***Installer un petit réseau de PC***, Ed. Dunod, Paris, 2003, P. 50 [↑](#footnote-ref-6)
7. LORENZ Pascal, *architectures des réseaux et télécommunications*, Ellipse, paris, 2001, p. 34. [↑](#footnote-ref-7)
8. ATELIN P., **Réseau informatique**, Ed. ENI, Paris, 2009, Page.8 [↑](#footnote-ref-8)
9. DROMARD D. et SERET D., **Architectures des Réseaux**, Ed. Pearson, Paris, 2009, p. 200 [↑](#footnote-ref-9)
10. **PUYOLLE** Guy**, Réseaux informatiques**, Ed. Eyrolles, Paris **2008, p.34** [↑](#footnote-ref-10)
11. LEMAINQUE Fabrice & PILLOU Jean-François, ***Tout sur les Réseaux et Internet***, 3e édition Dunod, Paris 2012 p.100 [↑](#footnote-ref-11)
12. LEMAINQUE Fabrice & PILLOU Jean-François, **Tout sur les Réseaux et Internet**, 3e édition Dunod, Paris 2012 [↑](#footnote-ref-12)
13. DEVANBLANC O., **Installer un petit réseau de PC**, Ed. Dunod, Paris, 2003. [↑](#footnote-ref-13)
14. Supinfo, « les topologies des réseaux informatiques » in www.supinfo.com, consulté le 05/03/2013. [↑](#footnote-ref-14)
15. Alain WIARD, Jean-Marc LEDUC, « ***Les réseaux locaux faciles*** », Marabout, novembre 1994, P.59. [↑](#footnote-ref-15)
16. PEZO NASUKA, **Télématique et Réseaux informatique, L1 Réseaux Informatique**, ISC – Bandundu, 2016 – 2017. P.66 [↑](#footnote-ref-16)
17. Pillou JF, Encyclopédie Comment ça marche, 2009 [↑](#footnote-ref-17)
18. DEVANBLANC O., **Installer un petit réseau de PC**, Ed. Dunod, Paris, 2003. [↑](#footnote-ref-18)
19. Guy PUJOLLE, Les réseaux : L'ère des réseaux Cloud et de la 5G, Edition ENY paris, 2018-2020 Page 36 20 MICHAL ZALEWSKI, Menaces sur le réseau: guide pratique des attaques passives et indirectes, Edition eyrolles paris 2008 pages 28 [↑](#footnote-ref-19)
20. TRABELSI K. & AMARA H., Mise en place des réseaux LAN interconnectés en redondance par 2 réseaux WAN, Rapport de stage de perfectionnement, Université Virtuelle de Tunis-UVT, 2015-2016. [↑](#footnote-ref-20)
21. MAKANGU J. architecture et réseau, notes de cours, GTMR, ISC/BDD, 2020-2021, page 29. (Inédite) [↑](#footnote-ref-21)
22. https://www.commentcamarche.net/contents/539-tcp-ip visité le 24/03/023 à 5h [↑](#footnote-ref-22)
23. MALELA V. Note de cours de réseau informatique 1, G2 TMR ISC/BDD, 2020. Page 40 [↑](#footnote-ref-23)
24. Tandberg, « **MCU Tandberg/Codian** », Version 3.0, Mai 2009, page 56. [↑](#footnote-ref-24)
25. https://www.africmemoire.com/part.10-chapitre-ii-architecture-reseaux-troisieme-partie-714.html consulté le 20/04/2024 à 15h30 [↑](#footnote-ref-25)
26. Hadj Ahmed Hilali Kawther, Administration et sécurité du réseau de l’Institut Supérieur d’Informatique de Mahdia (ISIMa) sous Linux, Mémoire de fin d’études, Université Virtuelle de Tunis-UVT, 2010-211. 28 www.securité\_informatique&pratique\_configuration.fr, consulté le 2/03/2025 [↑](#footnote-ref-26)
27. ITE, Travail de fin cycle, ISC-Bandundu, Page 25 (inédit) [↑](#footnote-ref-27)
28. Guillaume DESGEORGES, La sécurité des réseaux, 2000, PDF.p.25 [↑](#footnote-ref-28)
29. Christophe DUPONT, Technologies & Services protéger les utilisateurs sur la toile. 2011, PDF [↑](#footnote-ref-29)