International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 8 Issue 10 October - 2024, Pages: 67-76

Setting up a VPN for managing connection time and bandwidth in the Ndesha health zone.

Trésor BANANTAMBA KALUNDE and Franck MUNAKEBE MPINDA

Trésor BANANTAMBA KALUNDE
Sciences informatiques
Université de Kananga, UNIKAN
Kananga, République Démocratique du Congo
banantambatresor02@gmail.com
Franck MUNAKEBE MPINDA
Sciences informatiques
Université de Kananga, UNIKAN
Kananga, République Démocratique du Congo
francklinkebe@gmail.com

Abstract: The implementation of a VPN for connection time and bandwidth management at the Ndesha Health Zone is a crucial step towards a more efficient and secure digital health infrastructure. This project responds to pressing needs in terms of connectivity, while guaranteeing the protection of sensitive health data. With the implementation of a VPN, healthcare professionals will benefit from secure and reliable access to the resources needed for their daily work. Connection time and bandwidth management mechanisms will optimize the use of network resources, reducing the risk of congestion and improving user experience with a focus on security, with measures such as data encryption and multi-factor authentication, increasing user trust in the system. The deployment of a VPN in Ndesha represents a significant step forward in improving healthcare, while serving as a model for other facilities facing similar connectivity and security challenges.

Keywords–Virtual Private Network, connection time management, bandwidth
.

Résumé

La mise en place d'un VPN pour la gestion du temps de connexion et de la bande passante à la zone de santé de Ndesha constitue une étape cruciale vers une infrastructure de santé numérique plus efficace et sécurisée. Ce projet répond à des besoins pressants en matière de connectivité, tout en garantissant la protection des données sensibles sanitaires. Grâce à l'implémentation d'un VPN, les professionnels de la santé bénéficieront d'un accès sécurisé et fiable aux ressources nécessaires pour leur travail quotidien. Les mécanismes de gestion du temps de connexion et de la bande passante permettront d'optimiser l'utilisation des ressources réseau, réduisant ainsi le risque de congestion et améliorant l'expérience utilisateur en mettant l'accent sur la sécurité, avec des mesures telles que le chiffrement des données et l'authentification multi-facteurs, renforçant la confiance des utilisateurs dans le système.

Le déploiement d'un VPN à Ndesha représente une avancée significative vers l'amélioration des soins de santé, tout en servant de modèle pour d'autres établissements confrontés à des défis similaires en matière de connectivité et de sécurité.

0. INTRODUCTION

Les Nouvelles Technologies de l'Information et de la Communication (NTIC) ont rendu l'espace planétaire en un village via les réseaux informatiques qui sont en train de bouleverser la sphère du développement car elles ouvrent des nouveaux horizons des individus en créant les conditions qui permettent de réaliser dans une courte période un travail qui posait des difficultés jadis.

De nos jours, la sécurité informatique est trop indispensable pour le bon fonctionnement d'un réseau, aucune entreprise ou organisation ne peut prétendre vouloir mettre en place une infrastructure réseau quel que soit sa taille sans envisager une politique de sécurité. Pour ce faire nous ne prétendons pas dire que nous avons constitué une sécurité informatique parfaite mais néanmoins nous avons mis en œuvre un ensemble d'outils nécessaires pour minimiser la vulnérabilité de notre système contre des menaces accidentelles ou intentionnelles.

Grace aux échanges des données sécurisées avec gestion de temps de la connexion, il est possible d'interconnecter les structures éloignées qui ont une petite difficulté ou risques de collectes et d'encodage des données. Il est import de noter qu'il y a toujours des risques lors des collectes et encodage des données car les superviseurs, les secrétaires,

Administrateur Gestionnaire, et d'autres personnes animés de mauvaise foi peuvent créer de dysfonctionnement au sein de cette structure sanitaire car certains défis formidables peuvent être entre autre la modification des données, perte et vol d'informations, lourdeur lors de la connexion, …

En plus, la Zone de Santé de la Ndesha en tant structure sanitaire destinée à décentraliser certaines opérations dans les aires de santé afin de minimiser les risques et mobilité des superviseurs d'une aire de santé à l'autre avec les canevas SNIS. Notre choix sur ce spectacle est de nous plonger dans l'investigation et proposition des solutions à la problématique de la gestion de temps de connexion et de la bande passante pour l'échange des données à la zone de santé de Ndesha.

1. DEFINITION

1.1. Réseau Privé

Couramment utilisés dans les entreprises, les réseaux privés entreposent souvent des données confidentielles à l'intérieur de l'entreprise. De plus en plus, pour des raisons d'interopérabilité, on y utilise les mêmes protocoles que ceux utilisés dans l'Internet. On appelle alors ces réseaux privés « intranet ». Y sont stockés des serveurs propres à l'entreprise en l'occurrence des portails, serveurs de partage de données, etc. ... Pour garantir cette confidentialité, le réseau privé est coupé logiquement du réseau internet.

En général, les machines se trouvant à l'extérieur du réseau privé ne peuvent accéder à celui-ci. L'inverse n'étant pas forcément vrai. L'utilisateur au sein d'un réseau privé pourra accéder au réseau internet.

1.2. Réseau privé virtuel

L'acronyme VPN correspond à *Virtual Private Network*, c'est-à-dire un réseau privé virtuel. Dans les faits que cela correspond à une liaison permanente, distante et sécurisée entre les différents sites d'une organisation**.** Cette liaison autorise la transmission de données cryptées par le biais d'un réseau non sécurisé, comme Internet. En d'autres termes, un réseau privé virtuel est l'extension d'un réseau privé qui englobe les liaisons sur des réseaux partagés ou publics, tels qu'Internet.

1.3. Concept de VPN

Ce concept est utilisé pour des connexions sécurisées (souvent cryptés au niveau des protocoles les plus bas) afin de mettre en place un sous-réseau privé sur une infrastructure non sécurisée (exemple : Internet). Abrégé VPN qui signifie Virtual Private Network (réseau privé virtuel). Il arrive ainsi que des entreprises éprouvent le besoin de communiquer avec des clients ou même des personnels géographiquement éloignés via internet. Sur ce, les données transmises sur internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne d'une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. [1]

Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser internet comme support de transmission. Un bon compromis consiste à utiliser internet comme support en utilisant un protocole d'encapsulation" (en anglais *tunneling*, d'où l'utilisation impropre parfois du terme "tunnelisation"), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (noté *RPV* ou VPN, acronyme de *Virtual Private Network*) pour désigner le réseau ainsi artificiellement créé.

Ce réseau est dit *virtuel* car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable qui est internet et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent se partager les données. Le système de VPN permet donc d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux.

1.4. Fonctionnement [2]

Le VPN repose sur un protocole de tunnelisation (*tunneling*), c'est-à-dire un protocole qui permet le passage de données cryptées d'une extrémité du VPN à l'autre grâce à des algorithmes. On utilise le terme « tunnel » pour symboliser le fait que les données soient cryptées et de ce fait incompréhensible pour tous les autres utilisateurs du réseau public (ceux qui ne se trouvent pas aux extrémités du VPN).

Dans le cas d'un *VPN* établi entre deux machines, on appelle client VPN ce qui permet de chiffrer et de déchiffrer les données du côté utilisateur (client) et *serveur* VPN dans un réseau d'une organisation. De ceci, lorsqu'un utilisateur désire accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée.

L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A la réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur. Pour émuler une liaison point à point, les données sont encapsulées à l'aide d'un en-tête qui contient les informations de routage pour leur permettre de traverser le réseau partagé ou public jusqu'à leur destination finale [3]. Pour simuler une liaison privée, les données sont cryptées à des fins de confidentialité. Les paquets interceptés sur le réseau privé ou

International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 8 Issue 10 October - 2024, Pages: 67-76

public restent indéchiffrables sans clé de décryptage. La liaison servant à l'encapsulation et au cryptage des données privées est une connexion VPN. Etant donné que chaque point d'un réseau VPN est relié au réseau central par le biais d'un tunnel, reliant la machine à un gateway. Ainsi, tous les utilisateurs passent par le même "portail", ce qui permet de gérer la sécurité des accès, ainsi que le trafic utilisé par chacun.

1.5. Méthode de connexion

1) **Le VPN d'accès**

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion Vpn. Il existe deux méthodes :

- Le client demande au fournisseur l'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS du fournisseur d'accès, le NAS établit la connexion cryptée et présente certains avantages et inconvénients dans lesquels elle permet au client de communiquer sur plusieurs réseaux tout en créant plusieurs tunnels, qui nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise.
- Le client ou utilisateur possède son propre logiciel pour le VPN auquel il établit directement la communication de manière cryptée vers le réseau de la structure sanitaire. Sur cette deuxième méthode ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs.

2. **L'intranet VPN**

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...).

Il s'agit d'une authentification de paquets pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation Ip dans Ip pour assurer une sécurité raisonnable.

3. **Topologie des VPN**

Les VPN s'appuient principalement sur Internet comme support de transmission, avec un protocole d'encapsulation et un protocole d'authentification, au niveau des topologies, on retrouve des réseaux privés virtuels en étoile, maillé.

- Dans cette première topologie toutes les ressources sont centralisées au même endroit et c'est à ce niveau qu'on retrouve le serveur d`accès distant ou serveur VPN, dans ce cas de figure tous les employés du réseau s'identifient ou s'authentifient au niveau du serveur et pourront ainsi accéder aux ressources qui se situent sur l'intranet.
- Dans la seconde topologie les routeurs ou passerelles présents aux extrémités de chaque site seront considérés comme des serveurs d'accès distant, les ressources ici sont décentralisées sur chacun des sites autrement dit les employés pourront accéder aux informations présents sur tous les réseaux.

4. ***Internet d'un VPN***

La mise en place d'un réseau privé virtuel permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local. Ce procédé est utilisé par de nombreuses entreprises afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise hors de leur lieu de travail. On peut facilement imaginer un grand nombre d'applications telles que :

- Les connexions VPN offrent un accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les travailleurs nomades.
- Les connexions VPN permettent de partager des fichiers et programmes de manière sécurisés entre une machine locale et une machine distante avec facilité d'administrer efficacement un réseau local à partir d'une machine distante.
- Les connexions VPN permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure de réseau public, telle qu'Internet.
- Les connexions VPN permettent également aux entreprises de disposer de connexions routées partagées avec d'autres entreprises sur un réseau public, tel qu'internet, et de continuer à disposer les communications sécurisées, relier, par exemple des bureaux éloignés géographiquement. Une connexion VPN routée via internet fonctionne logiquement comme une liaison de réseau étendu (WAN, Wide Area Network) dédiée.

International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 8 Issue 10 October - 2024, Pages: 67-76

1.6. PROTOCOLES UTILISES ET SECURITE DES VPN

Il existe plusieurs protocoles dit de tunnelisation qui permettent la création des réseaux VPN :

a) PPP (Point To Point Protocol)

Le protocole PPP (Point To Point Protocol) est un ensemble de protocoles standard garantissant l'interopérabilité des logiciels d'accès distant de divers éditeurs qui prend en charge plusieurs méthodes d'authentification, protocoles de réseau local ainsi que la compression des données et leur cryptage. Nous pouvons utiliser TCP/IP comme protocole réseau. PPP est le fondement des protocoles PPTP et L2TP utilisés dans les connexions du Réseau Privé Virtuel sécurisées.

b) PPTP (Point To Point Tunneling Protocol)

Nous pouvons accéder à un réseau privé par l'intermédiaire d'Internet ou d'un autre réseau public au moyen d'une connexion à un réseau privé virtuel utilisant le protocole PPTP (Point To Point Tunneling Protocol) qui autorise le transfert sécurisé des données d'un ordinateur distant vers un serveur privé en créant un réseau privé virtuel entre les réseaux de données TCP/IP. Il est développé en tant qu'extension du protocole PPP (Point To Point Protocol), PPTP lui confère un niveau supplémentaire de sécurité et de communication multi protocoles sur internet, et il encapsule (fait passer par un tunnel) les protocoles IP ou IPX dans des datagrammes PPP.

c) L2TP (Layer Two Tunneling Protocol)

Nous pouvons accéder à un réseau privé par l'intermédiaire de l'internet ou d'un autre réseau public au moyen d'une connexion à un réseau privé virtuel (VPN) utilisant le protocole L2TP (Layer Two Tunneling Protocol). Il est un protocole de tunneling standard utilisé sur internet qui possède pratiquement les mêmes fonctionnalités que le protocole PPTP. Sur la base des spécifications des protocoles L2F (Layer TwoForwarding) qui est quasiment de nos jours obsolète et PPTP (Point To Point Tunneling Protocol), nous pouvons utiliser le protocole L2TP pour configurer des tunnels entre les réseaux concernés.

d) IPSec (Internet Protocol Security)

1) Présentation et fonctionnement d'IPsec

IPSec (Internet Protocol Security) est un protocole de la couche 3 du modèle OSI utilisé pour sécuriser le transport des données lors d'échanges internes et externes, la stratégie IPSec permet à l'administrateur réseau d'assurer une sécurité efficace pour son entreprise contre toute attaque venant de l'extérieur.

2) Concept de base d'IPSec

Le protocole IPSec est destiné à fournir différents services de sécurité. Il permet grâce à plusieurs choix et options de définir différents niveaux de sécurité afin de répondre de façon adaptée aux besoins de chaque entreprise. Le protocole IPSec permettant d'assurer la confidentialité, l'intégrité et l'authentification des données entre deux hôtes est gérée par un ensemble de normes et de protocoles :

- **Authentification des extrémités :** Elle permet de s'assurer que l'identité de chaque machine comme IPSec fonctionne au niveau de la couche 3.
- **Confidentialité des données échangées** : elle permet que chaque paquet IP soit chiffré afin qu'aucune personne non autorisée ne puisse le lire.
- **Authenticité des données** : ce protocole permet de s'assurer que chaque paquet a bien été envoyé par l'hôte et qu'il a bien été reçu par le destinataire souhaité.
- **Intégrité des données échangées :** il permet de vérifier qu'aucune donnée n'a été modifiée lors du trajet.
- **Protection contre les écoutes et analyses de trafic :** Le mode tunneling permet de chiffrer les adresses IP réelles et les entêtes des paquets IP de l'émetteur et du destinataire. Ce mode permet ainsi de contrecarrer toutes les attaques de ceux qui voudraient intercepter des trames afin d'en récupérer leur contenu.
- **Protection contre le rejeu** : IPSec intègre la possibilité d'empêcher un pirate d'intercepter un paquet afin de le renvoyer à nouveau dans le but d'acquérir les mêmes droits que l'envoyeur d'origine. Ces différentes caractéristiques permettent à l'hôte X de crypter ses données et de les envoyer vers l'hôte Y via le réseau qui reçoit et les décode afin de les lire sans que personne ne puisse modifier ou récupérer ces données.

3) Application de l'IPSec au modèle OSI

Le mode tunneling d'IPSec est un protocole de couche 3 fournissant ses services pour sécuriser l'IP qui est de même couche. Il a pour avantage d'offrir la protection des protocoles de couches supérieurs TCP/IP comme HTTP pour FTP. En plus ces protocoles, il regorge également les protocoles de couches 2 comme PPTP et L2TP.

4) Modes de transmission des données : transport et tunnelisation

Ces deux modes permettent de sécuriser les échanges réseau lors d'une communication. Néanmoins, le niveau de sécurité le plus élevé est le mode tunnelisation.

- Le mode transport offre essentiellement une protection aux protocoles de niveaux supérieurs. En effet, ce

mode ne modifie pas l'en-tête initial dans la mesure où il ne fait que s'intercaler entre la couche IP et la couche transport.

- Le mode tunnel intègre les fonctionnalités du mode transport et permet de protéger un ou plusieurs flux de données entre utilisateurs internes ou connectés via un VPN (Virtual Private Network). Lorsqu'un paquet de données est envoyé sur le réseau, le paquet est lui-même encapsulé dans un autre paquet. On crypte alors le corps de ce nouveau paquet à l'aide d'algorithmes de sécurités adéquats et on ne laisse en clair que l'entête contenant les adresses IP publiques de l'émetteur et du destinataire.

5) Le mode tunnel propose 2 protocoles de sécurité :

- ***PPTP*** (Point to Point Tunneling Protocol) : Ce protocole standard dans l'industrie a été pris en charge pour la première fois par Windows NT 4.0. PPTP est une extension du protocole PPP (Point to Point Protocol) qui s'appuie sur les mêmes mécanismes d'authentification, de compression et de cryptage que PPP.
- ***L2TP / IPSec* :** Celui-ci gère tous les types de trafic pour assurer l'encapsulation des données. Il encapsule les paquets d'origine dans une trame PPP, en effectuant une compression d'entête si possible, puis encapsule de nouveau dans un paquet de type UDP. IPSec et L2TP sont associés afin d'assurer la sécurité et la tunnelisation des paquets sur n'importe quel réseau IP. Leur association représente également une option garantissant la simplicité, la souplesse d'utilisation, l'interaction et la sécurité.

1.6.1. Principe d'échange de clés Internet (IKE) [4]

Une des spécificités d'IPSec est l'IKE (Internet Key Exchange) qui gère la négociation des protocoles et des algorithmes basés sur la stratégie de sécurité locale pour produire les clés de chiffrage et l'authentification à employer. Ce protocole est un dérivé de plusieurs protocoles. Cette pile de protocoles permet l'échange automatique des clés.

Le protocole IKE gère la sécurité en établissant un premier tunnel entre les 2 machines (le tunnel IKE la deuxième phase consiste à établir d'autres tunnels secondaires pour la transmission de données utilisateur entre les 2 machines.

1.6.2. Administration de clé ISAKMP/Oakley

Les 2 protocoles ISAKMP et Oakley ne fonctionnent que si l'agent de stratégie IPSec n'est pas en cours d'exécution. Ce service doit être implanté sur chaque poste Windows Client et permet lors de la communication IPSec de générer des clés et définir les propriétés de sécurité entre 2 hôtes.

- ***Internet Security Association and Key Management Protocol*** : Gère l'administration des associations de sécurité.
- ***Oakley*** : Génère les clés qui permettront de chiffrer et de déchiffrer les données transitant sur le canal sécurisé.

L'association des 2 protocoles permet de créer un canal sécurisé entre les deux hôtes en se servant de l'authentification des ordinateurs, et, de faire l'échange des données qui permettra de créer la clé secrète partagée. Cette clé sera utilisée pour crypter et décrypter les données envoyées via le réseau. ISAKMP/Oakley crée ainsi un contrat de confiance entre les deux ordinateurs puis envoie la clé et ce contrat au pilote IPSec.

1.6.3. Le pilote IPSec

Nommé IPSEC.sys, le pilote IPSec doit également être présent sur chaque poste Windows Client. Il permet de contrôler les paquets IP et d'effectuer les vérifications avec les stratégies de sécurité locale et les filtres IP mis en place.

a) Processus d'établissement d'une connexion

Afin de mettre en place un processus d'établissement d'une connexion, faisons l'étude d'un cas d'égal à égal : L'hôte A est un utilisateur itinérant qui se connecte via une liaison spécialisée vers l'hôte B qui est un serveur de base de données interne à son entreprise. Cette connexion pour des raisons de confidentialité et de sécurité doit être protégée. La sécurité IPSec est alors déployée afin de garantir le cryptage des données et l'authentification des 2 hôtes. La connexion va donc se dérouler en 6 étapes :

***1ère étape* :** L'hôte A cherché à télécharger des données situées sur le serveur FTP. Pour ce faire, il lance une transaction vers ce dernier. Le pilote IPSec de l'hôte A signale au service ISAKMP/Oakley que la stratégie de sécurité nécessite l'IPSec. On utilise alors les stratégies utilisées par l'agent de stratégie dans la base de registre.
***2ème étape* :** Le Service ISAKMP/Oakley des deux hôtes génère une clé partagée et une association de sécurité (contrat de confiance).
3ème étape : Les pilotes IPSec des deux hôtes prennent chacun la clé et l'association.
4ème étape : Les données envoyées par l'hôte A sont cryptées grâce à la clé (processus géré par le pilote IPSec).
5ème étape : Le serveur hôte B reçoit les données et les décrypte grâce au pilote IPSec qui connaît la clé partagée et l'association de sécurité.
***6ème étape* :** Les données sont ensuite transmises à la couche d'application (couche 7 du modèle OSI).

1.7. LA SECURITE DE FONCTIONNEMENT [5]

1.7. 1. Généralité

L'indisponibilité d'un système peut résulter de la défaillance des équipements de traitement(panne), de la perte d'information par dysfonctionnement des mémoires de masse, d'un défaut des équipements réseau, d'une défaillance involontaire (panne) ou volontaire (grève) de la fourniture d'énergie mais aussi d'agressions physiques comme l'incendie et les inondations.

1.7.2. Système de tolérance de panne

La fiabilité matérielle est obtenue par sélection des composants mais surtout par le doublement des éléments principaux, ces derniers systèmes sont dits à tolérance de panne (*faulttolerant*). La redondance peut être interne à l'équipement (alimentation...) ou externe. Les systèmes à redondance utilisent les techniques de mirroringet/ou de duplexing.

- **Le mirroring :** est une technique dans laquelle le système de secours est maintenu en permanence dans le même état que le système actif (miroir). Le *mirroring* disques consiste à écrire simultanément les données sur deux disques distincts. En cas de défaillance de l'un, l'autre continue d'assurer les services disques.
- **Le duplexing :** est une technique dans laquelle chaque disque miroir est relié à un contrôleur disque différent. Le *duplexing* consiste à avoir un équipement disponible qui prend automatiquement le relais du système défaillant.

1.7.3. Sûreté environnementale

L'indisponibilité des équipements peut résulter de leur défaillance interne mais aussi des événements d'origine externe. Le réseau électrique est la principale source de perturbation (coupures, microcoupures, parasites, foudre...). Des équipements spécifiques peuvent prendre le relais en cas de défaillance du réseau (onduleur *off-line*) ou constituer la source d'alimentation électrique permanente du système (onduleur *on-line*). Ces équipements fournissent, à partir de batteries, le courant électrique d'alimentation du système.

1. 8. Gestion de temps de connexion

Elle permet d'équilibrer productivité et la consommation des ressources en ligne tout en établissant les règles dans le but d'optimiser le temps et l'utilisation des outils de suivi pour surveiller la bande passante. Pour gérer le temps de connexion, nous devons prendre en compte certains préalables :

1.Fixation des limites qui aidera à définir les plages horaires spécifiques pour naviguer sur Internet ou utiliser les réseaux sociaux.

2.Utilisation des outils de suivi avec l'application comme RescueTime peut aider à suivre le temps passé sur différentes activités.

3.Établissement des priorités c'est-à-dire avant de se connecter, il serait important d'établir une liste des tâches à accomplir et se concentrer sur les plus importantes. Et évitez les distractions c'est-à-dire désactiver les notifications et créez un environnement propice pour une bonne concentration.

4.Programmez des pauses permettra non seulement pour rafraîchir les équipements mais aussi des pauses régulières pour éviter la fatigue mentale et rester productif dans la consommation de temps en ligne pouvant donner une nouvelle énergie qui permettra de se ressourcer. Et appliquer des techniques de gestion du temps comme la méthode Pomodoro, qui par exemple consiste à travailler par intervalles de quelques minutes, suivis de courtes pauses.

1. 9. **Bande passante**

La gestion de la bande passante est cruciale pour assurer un accès Internet fluide et efficace, surtout dans un environnement avec plusieurs utilisateurs ou appareils. Nous présentons certaines stratégies pour bien gérer la bande passante et garantir une expérience internet plus fluide pour tous les utilisateurs :

1. Priorisation du trafic : une Qualité de Service (QoS) : Configurez des règles QoS sur votre routeur pour donner la priorité à certaines applications (comme la vidéoconférence) par rapport à d'autres (comme le téléchargement).

2. Limitation de la bande passante : il suffit de limiter la bande passante pour certaines applications ou utilisateurs afin de garantir que tous aient un accès équitable.

3. Planification des téléchargements : établir un horaire de faible utilisation en programmant les téléchargements lourds (comme les mises à jour de logiciels) pendant les heures où l'utilisation est minimale.

4. Surveillance de l'utilisation Outils de surveillance : Utilisez des outils comme PRTG ou NetWorx pour surveiller et analyser l'utilisation de la bande passante.

5. Optimisation des applications : vous assurez que toutes les applications sont à jour pour bénéficier les nouvelles versions qui peuvent être plus efficaces en termes de bande passante.

6. Utilisation de câbles Ethernet ou connexion filaire : si nécessaire, il serait important d'utiliser la connexion câblée pour une connexion plus stable et rapide, surtout pour les activités gourmandes en bande passante.

7. veiller aux applications lourdes en simultané : c'est-à-dire faire le planning des activités qui permettra de prévenir la connectivité des plusieurs utilisateurs ou appareils qui

International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 8 Issue 10 October - 2024, Pages: 67-76

consomment beaucoup de bande passante en même temps aux jeux, réseaux sociaux, ….

8. Configuration du réseau Wi-Fi : qui demandera la sécurité la sécurité du réseau pour éviter que des utilisateurs non autorisés ou authentifiés ne consomment la bande passante.

2. Champ d'investigations

L'objectif de cette étude est de comprendre le système actuel, déceler ses points forts et faibles, et arriver à proposer des solutions adéquates pour améliorer son côté négatif tout en se basant sur d'autres systèmes de suivi des malades déjà présents.

2.1. Définition globale du problème

En dépit des multiples outils et matériels informatiques dotés à cette zone de santé (NDESHA) en vue de faciliter la communication (tant en interne qu'en externe) et le traitement harmonieux de données, le système de communication en ce lieu reste encore à nos jours une préoccupation. Constituée de 8 airs de santé, le réseau informatique installé au siège de la zone de santé de NDESHA, ne sert qu'à faciliter le transfert de données SNIS vers le niveau provincial et national.

Il se pose ainsi un vrai problème qui oblige à ce que les superviseurs se déplacent de temps à autre pour collecter les données devant être encodées au bureau central pour leur transfert. Qu'adviendra-t-il alors pour ces Superviseurs en cas d'intempéries (pluie par exemple) ou autre cause liée à l'insécurité ?

Les nouvelles technologies de l'information et de communication, ne peuvent-elles pas permettre l'encodage de ces données dans les aires de santé, puis faciliter leur transmission à qui que l'on désire, aussi longtemps que la structure dispose déjà d'un réseau ?

Ces grands questionnements définissent d'ailleurs le problème fondamental que connaissent les utilisateurs et dirigeants de la zone de santé de NDESHA.

A. Système de communication utilise pour communiquer avec les airs de sante

La communication se fait d'une manière classique, autrement dit les méthodes utilisées pour faire transiter les messages que la zone désire passer se présentent comme suit :

- **Les notes de service**

Premier outil de communication utilisé au bureau central de ladite zone sont les notes écrites ; en effet elles ont pour objectif de diffuser au sein de la zone, des informations précises et utiles pour le bon fonctionnement.

- **Les communications électroniques**

Les agents de la DPS et ceux de cette zone de santé font recours aux réseaux sociaux comme Facebook, whatsapp, mail pour communiquer, partager certaines informations et débattre sur certains sujets.

- **La ligne téléphonique**

C'est un moyen de communication utilisé par le MCZ, les superviseurs, la DPS pour rester en interaction dynamique avec le bureau central. La ligne téléphonique reste l'un de moyen indéfectible que les IS s'en servent pour centraliser les plus importantes données de différents airs de santé que gère cette zone.

B. Présentation du réseau existant au bureau central

Ce réseau qui ne facilite que le transfert de données SNIS vers le niveau plus haut, se présente de la manière ci-après :

Figure 1 : Présentation du Réseau existant

2.2. Critiques de l'existant

Ce système présente un certain nombre d'insuffisances qu'on va essayer d'énumérer, notons néanmoins que ces difficultés ne peuvent être réglées d'une manière définitive qu'à travers une refonte du système existant. Les principales insuffisances et limites du système existant se présentent comme suit :

- ✓ L'acheminement toujours tardif des rapports à la ZS qui à son tour prend aussi une décision tardive sur l'accompagnement des airs de santé.
- ✓ Les rapports envoyés parfois par les structures sanitaires sont des fichiers Word ou Excel jointent aux messageries électroniques est une perte de temps, car parfois certains ne s'ouvrent plus (mauvais format, impossible d'ouvrir ce fichier,…)
- ✓ L'utilisation abusive du carburant dans les taches de la récolte de canevas SNIS et l'utilisation négative du réseau en téléchargeant les films et chansons.
- ✓ Le besoin incessant d'accès à l'Internet afin de pouvoir communiquer et manipuler le logiciel DHS2 pour encoder en temps réel les données SNIS.

International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 8 Issue 10 October - 2024, Pages: 67-76

✓ Les notes de service ne parviennent pas forcément à toutes les structures concernées ce qui engendre certaines failles quant à l'application de ces notes.

✓ L'utilisation des réseaux sociaux comme FACEBOOK à des fins de communication à caractère administratif ou professionnel peut encourir la zone à un vrai danger.

✓ La circulation de nouveautés au sein de la zone se fait à l'aide de la bouche qui parfois déforme l'information ou par la ligne téléphonique ce qui engendre un mauvais partage des informations entre les Infirmiers Superviseurs.

✓ Insuffisance voire même inexistence du service informatique au bureau central ce qui pèse sur les Infirmiers Titulaires et le Superviseur de manipuler l'outil informatique rend le travail lourd.

2.3. Propositions des solutions

Afin de pallier aux défaillances observées, on se propose d'informatiser le processus de communication interne et externe au sein du bureau central. Ce qui se traduit par le développement d'un ***réseau informatique opérationnel***, une fois mis en place et exploité par tous les personnels de la zone, celui-ci va permettre une communication assez fluide et efficace.

La création d'un portail réseau permet au personnel : l'accès à l'information en temps opportun et également une mise à jour régulière et efficace ; l'archivage, la sécurité et la confidentialité des données ; Une évaluation quantitative et qualitative des soins de chaque structure. Un Portail peut servir à fournir tout genre d'informations utiles au sein de la zone.

3.CONCEPTION E DE LA NOUVELLE ARCHITECTURE RÉSEAU

3.1. Analyse des besoins

Dans cette section du chapitre, seront exposés les besoins des utilisateurs à travers les spécifications fonctionnelles et non fonctionnelles afin d'aboutir à une application performante et satisfaisante a la hauteur de l'attente des utilisateurs.

Pour les besoins fonctionnels, nous allons élucider deux aspects spécifiques du réseau : d'autre part le réseau pour informer qui doit rassembler toutes les informations utiles au personnel dans l'exercice de ses fonctions et pour se situer dans son environnement de travail : les nouveautés, les nouveaux services, actualités sur la vie de la zone, l'annuaire téléphonique, rapports d'activités de la vaccination et les notes de services et d'autre part le réseau pour collaborer ou communiquer par messagerie avec tout le personnel, pour échanger et s'exprimer sur le sujet dans le plateforme interne, chercher un agent par l'annuaire.

Les besoins non fonctionnels sont importants car ils agissent de façon indirecte sur le résultat et sur le rendement de l'utilisateur d'où leurs importances. Pour cela il faut répondre aux exigences suivantes :

✓ *Fiabilité* : le réseau doit fonctionner de façon cohérente sans erreurs.

✓ *Les erreurs* : le réseau doit les signaler par des messages d'erreurs.

✓ *Sécurité* : le réseau doit être sécurisé au niveau des données : authentification et contrôle d'accès.

3.2. CAHIER DE CHARGE

Le cahier de charge peut être défini comme un acte, un document de référence qui permet au dirigeant d'entreprise, d'une organisation de préciser les exigences ou conditions d'un projet qu'il faut réaliser ou une tâche à exécuter par un consultant en vue d'améliorer une situation donnée tout en précisant les résultats. Pour ce faire, nous allons présenter ici ces exigences du Concepteur que nous sommes :

a) Coût matériels

N°	Nom matériel	Caractéristique	Qté	PU	Prix Total
1	Serveur	8Go RAM, 500Ghz carte réseau	3	1500$	4500$
2	Switch	2 LINK	3	100$	300$
3	Imprimante	HP laser	4	300$	1200$
4	Ordinateur	HP 250Go HD	40	500$	20000$
5	Antenne CPE	55 cm	3	300$	900$
6	Routeur	2 ports WAN	3	450$	1350$
4	câble UTP	UTP simple	500m	1$	500$
5	Connecteur RJ45		2000	0,5$	200$
6	Ventilateurs	2500W	4	50$	200$
7	Câble SSTP	Blindé	40m	10$	400$
8	Modem	ADSL	3	120$	360$
				Total Partiel	29450$

Tableau. 1 : Coût matériels

b) Coût personnel

N°	Description	Montant prevue	Montant reçu
1	Acheminement des matériels au BCZ	450$	450$
2	Acheminement de matériels dans le site	100$	100$
3	Restauration	500$	350$
4	Transport	80$	50$

International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 8 Issue 10 October - 2024, Pages: 67-76

5	Communication	100$	70$
6	Logement	150$	150$
	Total Partiel	1380$	1170$
	Coût global	**30.830$**	
	Main d'œuvre	**3.083$**	

Tableau 2 : Coût personnel

*3.3. **Planning previsionnel de la realisation du projet***

Accessibilité géographique

Il ressort de ce tableau ici-bas que **:**

- Quelques Aires de Santé sont situées à plus de 15 Km du bureau central et deux Aires de Santé ont plus de 30% de leur population au-delà de 5Km de Centre de Santé.
- 69% des Aires de Santé ont en outre le Centre de Santé de responsabilité, une autre structure des soins améliorant ainsi, l'accessibilité géographique de leur population au PMA.

En déduisant ce tableau nous sommes conduits à ressortir les sites suivant pour notre réseau :

1. *Site NDESHA BCZ* qui s'étend sur distance de 100m
2. *Site MUSANGILAYI* qui s'étend sur une distance de 35 Km.
3. Site *CHRIST-ROI* qui s'étend sur une distance de 4 Km

3.4. Conception du réseau

Un réseau informatique étant un ensemble d'ordinateurs qui communiquent entre eux en utilisant les différentes technologies telles que les ondes radio ou par câble, du réseau Ethernet. Il permet de relier tous les personnels dans le but de faciliter leur communication, leur collaboration et la gestion de leur travail. Il s'agit d'un moyen simple de partager et de valider les informations à l'intérieur d'une structure. Cela est d'autant plus important que le personnel est assez éparpillé géographiquement sur tout le territoire. Facile à mettre en œuvre de façon décentralisée, le réseau informatique offre l'avantage d'une interface identique quel que soit le poste de travail auquel l'utilisateur est connecté.

1) *Identification des acteurs*

Le but de ce projet étant de permettre aux employés de la zone de santé rurale de santé de disposer d'une plateforme de communication et de partage de données. Chaque employé de la zone est un acteur interagissant avec le réseau ce qui lui attribue certains rôles spécifiques au poste occupé.

Voici le tableau présentant les différents acteurs du système et leurs rôles :

Admin/ Secrétaire	Représente les développeurs et les techniciens responsables de la gestion du réseau. L'administrateur peut : Donner le droit à l'utilisateur de gérer les services, Gérer les utilisateurs et les groupes, Gérer les accès au réseau, Auditer le système
Directeur	Représente les chefs de centres de santé(IT), les sous-directeurs(IS), Le directeur Adjoint (AG) Le directeur (MCZ). Cet acteur : Gère les services de la direction
Utilisateur	Représente tous les agents de la zone, y compris les administrateurs et les directeurs Hiérarchiques, qui peuvent : Gérer la messagerie interne, Consulter le stock, demander un service au bureau central de la zone, direction...etc., recevoir les notifications et les informations sur l'état des demandes.
Responsable services	Représente les gestionnaires des directions qui peuvent : Gérer les canevas SNIS, Gérer les demandes de produit pharmaceutique en rupture aux centres, postes et aires de santé.

Tableau 3 : tableau des acteurs

C. Logiciels nécessaires

Nous avons opté pour ce projet avec les logiciels ci-après :***Edraw Network diagramm*** et ***Cisco Packet Tracer.***

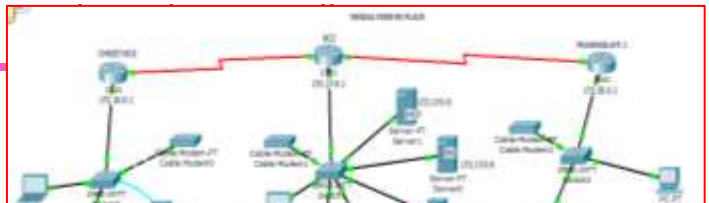
3.6. MAQUETTE DU RESEAU A METTRE EN PLACE

Figure 2 : Maquette du réseau

L'ordinateur connecté au réseau est la cible de plusieurs menaces ainsi pour protéger notre réseau contre les virus et des programmes malveillants, nous avons pensé à cet antivirus pour multiples raisons entre autre il incorpore le logiciel anti-espions et la mise à niveau rapide.

3.5. Configuration et déploiement du réseau

La configuration et déploiement d'un réseau sont des processus essentiels pour favoriser le fonctionnement des



International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 8 Issue 10 October - 2024, Pages: 67-76

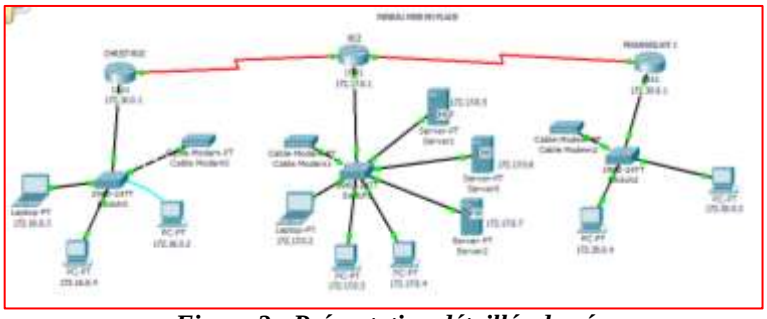


Figure 3 : Présentation détaillée du réseau

3.6. PLAN DE NOMMAGE ET D'ADRESSAGE

Il est très bénéfique pour assurer une gestion efficace et cohérente des différentes ressources réseau dans une entreprise.

Adresse générale du réseau : 172.16.0.0/24
Masque de sous réseau : 255.255.0.0

Adresse du réseau du site de du BCZ : 172.16.1.0/24
Plage d'adresses utilisables :
De 172.16.1.0 à 172.16.1.254

Adresse du réseau du site Christ-roi : 172.16.2.0/24
Plage d'adresses utilisables :
De 172.16.2.0 à 172.16.2.254

Adresse du réseau de Musangilayi : 172.16.3.0/24
Plage d'adresses utilisables :
De 172.16.3.0 à 172.16.3.254

Conclusion

Après les larges horizons, nous atterrissons en disant que ce projet de fin d'études nous a permis de confronter l'acquis théorique à l'environnement pratique. Tenant compte de ce qui précède, notre projet présente plusieurs avantages notamment sur le plan de rapprochement des différentes aires de santés et du bureau central de la zone de santé de NDESHA, la plus grande des solutions que ce projet apporte sera celle de faciliter la communication entre le MCZ et les infirmiers responsables de différentes aires de santés en consacrant du temps pour l'étude et le recensement des fonctionnalités de notre système à mettre en place. Nous avons pris en compte les besoins actuels de ladite Zone de Santé pour le bon fonctionnement de son réseau informatique et sa sécurité sans oublier les insuffisances relevées dans l'existant pour concevoir une nouvelle architecture du réseau sécurisé basée sur le VPN en utilisant le protocole IPSec qui garantit un échange de données et le partage des ressources d'une manière sécurisée.

En effet, la mise en place d'un réseau permet aux réseaux privés de cette Zone de Santé de s'étendre et de se relier entre eux via internet.

Nous souhaitons que ce travail soit un pas qui servira à d'autres chercheurs de mener à bien leurs recherches afin de trouver et de démontrer encore d'autres avantages que peut apporter l'utilisation d'un réseau informatique. Nous ne croyons pas avoir tout fait, ainsi nous restons ouverts à toute remarque.

Références

[1] Dictionnaire Jargon Informatique, 20-10-2004
[2] ELLISPSES, Technosup, éd. Dunod, Paris 2001, P. 56
[3] L. MONTAGIERJ, Pratique des réseaux d'entreprise, Eyrolles, Paris, 1997, P. 125
[4] L-L. MONTAGIER, Pratique des réseaux d'entreprise : du câblage à l'administration, du réseau local aux réseaux de télécommunication, Eyrolles, Paris, 1997, P. 303.
[5] Claude Servin, Réseaux et télécoms ; Cours et exercices corrigés, Dunod, Paris, 2003,p.56