« CONFIGURATION ET MISE EN PLACE D'UN RESEAU VPN DANS UNE ENTREPRISE. CAS DE LA BRALIMA /KISANGANI. »

Christian Nzanzu Mutsuva*

Corresponding Author:

Résumé :

Dans cet article, il est question d'implémenter une solution sécurisée pour permettre une communication sûre et confidentielle entre différents sites distants et le siège de la Bralima Kisangani en utilisant la technologie VPN développée sous l'environnement Windows Server 2012 R2. Le choix technologie qui est fait dans cette étude, se base sur plusieurs protocoles de tunnelisation proposés par l'environnement Windows Server 2012 R2 et offre une facilité de déploiement et de configuration. Deux approches méthodologiques ont été utilisées dans cet article, la première approche étant analytique, s'est focalisée sur la modélisation du système existant en vue de proposer une solution adaptée au besoin de cette entreprise. La dernière approche descriptive, nous a permis de décrire de la manière la plus explicite les technologies VPN implémentées dans l'environnement de Windows Server 2012 R2. Cet article brosse les éléments qui composent un réseau VPN et éclaire le lecteur sur les différentes étapes de configuration de ce dernier.

Abstract

This article looks at the implementation of a secure solution to enable secure and confidential communication between various remote sites and the Bralima Kisangani head office, using VPN technology developed under the Windows Server 2012 R2 environment. The choice of technology made in this study is based on several tunneling protocols offered by the Windows Server 2012 R2 environment, and offers ease of deployment and configuration. Two methodological approaches were used in this article, the first being analytical, focusing on modeling the existing system with a view to proposing a solution adapted to this company's needs. The last approach, descriptive, enabled us to describe in the most explicit way the VPN technologies implemented in the Windows Server 2012 R2 environment. This article outlines the elements that make up a VPN network and explains the various steps involved in configuring it.

INTRODUCTION

Les réseaux composent la structure de base du septième continent qui se forme sous nos yeux. Par l'immense séisme qu'il engendre en ce début de siècle, la planète entre dans une ère nouvelle. Ce nouveau continent est celui de la communication. Constitué de réseaux se parcourant à la vitesse de la lumière, il représente une rupture analogue à l'apparition de l'écriture ou à la grande révolution industrielle. Ces réseaux, qui innervent aujourd'hui complètement la planète, s'appuient sur la fibre optique, les ondes hertziennes et divers équipements qui permettent d'atteindre de hauts débits. Internet incarne pour le moment la principale architecture de ces communications[1].

Mais ces innovations technologiques liées à la communication et aux échanges de données apporteraient également des problèmes de sécurité. C'est ce qui poussa les concepteurs de ces technologies de communications et d'échanges de données à penser aux solutions sûres à adopter. Parmi les mesures prises, nous retrouvons l'usage de la cryptographie[2] qui permet de chiffrer et de déchiffrer chaque message du texte échangé dans la transmission de données d'un émetteur vers un destinataire.

Cette solution aussi efficace soit-elle, pose un problème de lenteur dans la communication car ce processus de chiffrement et de déchiffrement de tous les messages transmis serait gourmand en ressources et ralentit les échanges. L'idéal serait plutôt de chiffrer le flux de l'ensemble du trafic sur un ou plusieurs itinéraires donnés, cela constituerait un *réseau privé virtuel*, ou VPN, comme *Virtual Private Network*. Il s'agirait par exemple d'établir un canal chiffré entre deux nœuds quelconques de l'Internet, ces nœuds pouvant eux-mêmes être des routeurs d'entrée de réseaux. On aurait ainsi établi une sorte de tunnel qui, à travers l'Internet, relierait deux parties éloignées l'une de l'autre du réseau d'une même entreprise pour donner l'illusion de leur contiguïté. C'est ce à quoi nous allons nous investir dans cet article qui vise à expliciter les étapes d'implémentation d'une solution VPN dans une entreprise commerciale. Cas de la Bralima /Kisangani.

Cette étude tire son originalité sur le choix technologique qui se penche sur la solution VPN implémentée au sein de Windows Server 2012 R2 avec une configuration du serveur Radius pour gérer l'authentification et l'autorisation dans le but d'autoriser ou non un accès réseau. Cette fonctionnalité nous permet de communiquer de manière sécurisée. Ainsi, les échanges entre 2 nœuds géographiquement distants de cette même entreprise se feraient en utilisant plusieurs protocoles de tunnelisation et de chiffrement.

L'objectif principal poursuivi dans cette étude est celui d'implémenter un système automatisé devant permettre de relier les différents sites de l'entreprise Bralima de manière sécurisée.
Et dans cette mise, nous nous sommes posé Trois questions Suivantes : Comment permettre à la Bralima Kisangani de transmettre de manière sûre ces données vers les autres sites de la province ou du pays ? Comment implémenter ce VPN au sein de l'entreprise Bralima Kisangani ? Quels sont les protocoles à utiliser dans le cadre d'une solution VPN pour la sécurisation des échanges entre ces différents sites ?

En vue de remédier aux inquiétudes soulevées au travers des questions posées ci-haut, nous pensons que la solution efficace pour permettre à la BRALIMA Kisangani de transmettre de manière sûre ces données entre ces différents sites serait la mise en place d'un VPN. L'implémentation de ce VPN pourrait être réalisée comme rôle serveur dans l'environnement Windows Serveur 2012 R2. Les protocoles de tunnelisation VPN à utiliser pourraient être PPTP, L2TP ou SSTP et celui du chiffrement serait MPPE (Microsoft Point-to-Point Encryptions)

Pour obtenir les résultats attendus, nous avons fait recours à l'approche analytique en vue de modéliser le problème et la méthode descriptive pour ainsi décrire les étapes de cette implémentation.

Sur ce, nous abordons dans la section suivante les différents concepts qui sont liés à la terminologie technique en vue d'éclairer tout lecteur sur les différentes technologies VPN. Ainsi, nous pouvons comprendre par la suite les différents protocoles utilisés et les approches de base qui caractérisent cette technologie.

SECTION I : CADRE THEORIQUE

Dans cette section, nous abordons les concepts théoriques sur les notions des réseaux informatiques et les VPN pour permettre au lecteur une compréhension nette des différentes terminologies employées dans ce domaine. Vu l'immensité des notions que renferme le réseau informatique, nous nous sommes donné le devoir de bien le résumer significativement.

I.1. INTRODUCTION AUX RÉSEAUX INFORMATIQUES

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et enfin des machines terminales, telles que stations de travail ou serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo est généralisée dans les réseaux informatiques, même si cela ne va pas sans difficulté.

[1] Guy Pujolles, Les Réseaux, 6ième édition, Eyrolles 2008.

[2] L'art d'écrire en chiffres ou d'une façon secrète quelconque.

On distingue généralement cinq catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau :

- Les réseaux personnels, ou PAN (Personal Area Network), qui interconnectent sur quelques mètres des équipements personnels tels que téléphone mobile, portables, organiseurs, etc., d'un même utilisateur.
- Les réseaux locaux, ou LAN (Local Area Network), qui correspondent par leur taille aux réseaux intra-entreprise. Ils servent au transport de toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres. Les débits de ces réseaux vont aujourd'hui de quelques mégabits par seconde à plusieurs centaines de mégabits par seconde.
- Les réseaux métropolitains, ou MAN (Metropolitan Area Network), qui permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux des différentes entreprises pour leur donner la possibilité de dialoguer avec l'extérieur.
- Les réseaux régionaux, ou RAN (Regional Area Network), qui ont pour objectif de couvrir une large surface géographique. Dans le cas des réseaux sans fil, les RAN peuvent avoir une cinquantaine de kilomètres de rayon, ce qui permet, à partir d'une seule antenne, de connecter un très grand nombre d'utilisateurs. Cette solution a profité du dividende numérique, c'est-à-dire des bandes de fréquences de la télévision analogique qui ont été libérées après le passage au tout-numérique, à la fin de 2011 en France.
- Les réseaux étendus, ou WAN (Wide Area Network), qui sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, et il utilise en ce cas des infrastructures au niveau du sol, essentiellement de grands réseaux de fibre optique, soit hertzien, comme les réseaux satellite, mais seulement pour des applications particulières à débit faible[3].

I.1.1. TOPOLOGIE D'UN RÉSEAU

La topologie est la manière d'arranger les nœuds (serveur, poste, imprimante, etc.) dans un réseau. Il existe deux types de topologies : les topologies physique et logique[4]. Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication et des éléments matériels. L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelée topologie physique. On distingue généralement les topologies physiques suivantes :

- Topologie en bus,
- Topologie en étoile,
- Topologie en anneau,
- Topologie en arbre,
- Topologie maillée.

La topologie logique, par opposition à la topologie physique, représente la façon dont les choses transitent dans les lignes de communication. Les topologies les plus courantes sont Ethernet, Token Ring et FDDI[5].

I.1.2. SUPPORTS DE TRANSMISSION

Les supports de transmission exploitent les propriétés de conductibilité des métaux (paires torsadées, câble coaxial), celles des ondes électromagnétiques (faisceaux hertziens, guides d'ondes, satellites) ou encore celles du spectre visible de la lumière (fibre optique).

Généralement on classe les supports en deux catégories :

- Les supports guidés (supports cuivre et supports optiques) ;
- les supports libres (faisceaux hertziens et liaisons satellites).[6]

I.1.2.1. Les supports guidés

- **Le câble coaxial**

Un câble coaxial est constitué de deux conducteurs cylindriques de même axe, l'âme et la tresse, séparés par un isolant. Ce dernier permet de limiter les perturbations dues au bruit externe. Si le bruit est important, un blindage peut être ajouté. Quoique ce support perde du terrain, notamment par rapport à la fibre optique, il reste encore très utilisé[7].

- **La paire torsadée**

La paire torsadée ou symétrique est constituée de deux conducteurs identiques torsadés. Les torsades réduisent l'inductance de la ligne (L). Généralement, plusieurs paires sont regroupées sous une enveloppe protectrice appelée gaine pour former un câble. Les câbles contiennent une paire (desserte téléphonique), quatre paires (réseaux locaux), ou plusieurs dizaines de paires (Câble téléphonique).

---

[3] Guy Pujolles, **Les Réseaux,** 9e édition, Eyrolles, 2020, page 53.

[4] Rigobert PEZO NASSUKA BIYO, **Initiation à la théorie et à la pratique du Réseau Informatique**, CRIGED, 2012, page 31.

[5] Jean-François PILLOU et Fabrice LEMAINQUE, **Tout sur les réseaux et Internet**, 4ième édition, DUNOD, 2015, page 5.

[6] Claude Servin, Réseaux et Télécoms, 4ième édition, Dunod, 2013, page 37.

[7] Guy Pujolles, op. cit., page 131.

● **Fibre optique**

Considérée comme le support permettant les plus hauts débits, la fibre optique est une technologie aujourd'hui complètement maîtrisée. Dans les fils métalliques, on transmet les informations par l'intermédiaire d'un courant électrique modulé. Avec la fibre optique, on utilise un faisceau lumineux modulé. Il a fallu attendre les années 1960 et l'invention du laser pour que ce type de transmission se développe.

Une connexion optique nécessite un émetteur et un récepteur. Différents types de composants sont envisageables. Les informations numériques sont modulées par un émetteur de lumière, qui peut être :

- Une diode électroluminescente ou LED (Light Emitting Diode) qui ne comporte pas de cavité laser.
- Une diode à infrarouge.
- Un laser pour les fibres monomodes[8].

I.1.2.2. Les supports libres

Les réseaux hertziens apportent une grande flexibilité de par leur interface, qui permet à un utilisateur de changer de place tout en restant connecté. Les communications entre équipements terminaux peuvent s'effectuer directement ou par le biais de stations de base, appelées encore points d'accès, ou AP (Access Point). Les communications des points d'accès vers le réseau cœur sont effectuées soit par voie hertzienne (relais hertzien ou onde millimétrique), soit par câble (*x*DSL ou fibre optique). Les réseaux hertziens se décomposent en deux grandes catégories : les réseaux dits sans fil et les réseaux de mobiles. À la différence des réseaux sans fil, les réseaux de mobiles permettent de passer d'une cellule à une autre sans couper la communication[9].

I.2. LES RÉSEAUX VPN

Les VPN (Virtual Private Network), ou réseaux privés virtuels, forment une classe particulière de réseaux partagés. Dans de tels réseaux, les ressources d'un réseau réel peuvent se trouver distribuées à un instant donné entre plusieurs réseaux, de telle sorte que chaque sous-réseau puisse croire que le réseau réel appartient à lui seul.

Cette partie décrit les différentes catégories de réseaux privés virtuels permettant d'introduire des fonctions susceptibles d'améliorer la gestion d'une entreprise. Ces catégories proviennent soit du type de réseau mis en place, soit du niveau d'architecture, trame ou paquet, ou encore du type de fonction recherchée (sécurité, qualité de service, etc.). Ces différentes catégories ne sont pas indépendantes, mais se recoupent. Par exemple, un VPN IP est à la fois un VPN permettant de créer un réseau virtuel IP et un VPN de niveau paquet. De même, un VPN IPsec est à la fois un VPN de niveau paquet et un VPN de sécurité. Les VPN MPLS sont plus complexes, car ils appartiennent à la fois aux niveaux trame et paquet.

I.2.1. Architecture des VPN

Un réseau privé virtuel peut être défini comme un ensemble de ressources susceptibles d'être partagées par des flots de paquets ou de trames provenant de machines autorisées. Les VPN peuvent utiliser des technologies et des protocoles quelconques. La gestion de ces ressources nécessite un haut niveau d'automatisation pour obtenir la dynamique nécessaire au fonctionnement d'un VPN. Pour obtenir cette dynamique, les ressources permettant d'acheminer les paquets au destinataire doivent être gérées avec efficacité[10].

I.2.2. Typologie des VPN

La classification des VPN peut se faire en se servant des différents critères comme : le type d'application supporté, l'architecture protocolaire, la personne qui gère le réseau. En fonction de celui qui gère le réseau, il existe deux types de VPN : VPN d'entreprise et le VPN opérateur[11].

Dans le premier type, VPN d'entreprise, nous retrouvons le VPN site à site, VPN poste à site et le VPN poste à poste.

- Le VPN site à site : permet de connecter deux ou plusieurs réseaux distants comme s'ils étaient sur le même LAN.
- Le VPN poste à site : c'est un type de VPN permettant d'interconnecter un utilisateur à un réseau privé distant.
- Le VPN poste à poste : comme son nom l'indique, c'est un type de VPN permettant de connecter un ordinateur à un autre ordinateur distant.

Un VPN repose sur un ou plusieurs protocoles, appelés protocoles de tunnelisation (ou tunneling protocols en anglais). Ces protocoles permettent aux données d'être véhiculées sur plusieurs réseaux physiques en étant sécurisées par des algorithmes de chiffrement.

- **PPP** (Point-To-Point Protocol ou protocole Point à Point) ou protocole point à point permet la connexion entre un client et un serveur distant. Ce protocole est largement utilisé pour la connexion à un fournisseur de service Internet via le

[8] Guy PUJOLLE, op. cit., page 272 - 273
[9] Guy PUJOLLE, op. cit., page 557
[10] Guy PUJOLLE, op. cit., page 835
[11] Jean-Paul ARCHEIER, ***Les VPN -Fonctionnement, mise en œuvre et maintenance des Réseaux Privés Virtuels***, 2e Edition, ENI, 2013, page 200.

réseau téléphonique. PPP offre l'avantage de supporter la compression, le chiffrement ou encore la négociation automatique de paramètres IP [12].

- **PPTP** (Point-To-Point Tunneling Protocol, protocole de tunnel point à point) est un protocole qui permet d'interconnecter des réseaux par l'intermédiaire d'un réseau IP[13]
- **L2TP** (Layer Two Tunneling Protocol) est un protocole standard de tunnelisation très proche de PPTP. Le protocole L2TP encapsule des trames du protocole PPP, encapsulant elles-mêmes d'autres protocoles (par exemple le protocole IP)[14].
- **SSTP** (Secure Socket Tunneling Protocol) est un protocole VPN apparu dans Windows Vista SPA et Windows Server 2008. Il encapsule le protocole PPP dans http sur SSL afin d'éviter les problèmes de passage d'IPSec au travers de pare-feu, voire de proxy[15].
- **IPsec** est un protocole qui permet de sécuriser les échanges entre deux ou plusieurs adresses IP (mode transport). Il intègre deux composantes majeures : AH qui permet de garantir l'intégrité des données et ESP qui permet de crypter les informations transmises[16].

SECTION II : ANALYSE DE L'EXISTANT ET CONCEPTION DU NOUVEAU SYSTÈME

II.1. ANALYSE DE L'EXISTANT

Elle consiste à identifier et à recenser les informations et procédures du Système d'information et de gestion du personnel. L'état du système d'information (matériel et logiciel) actuel est dressé : quelles sont les informations et applications disponibles, celles qui sont utilisées, par qui et pourquoi, quels sont les traitements effectués ?[17]

Dans cette sous-section, nous faisons l'état de lieux de tous les matériels et composantes de traitement de l'information que nous avions trouvé au sein de la Bralima / Kisangani. Le but poursuivi dans cette partie, c'est de recenser les forces et les faiblesses de l'organisation. Pour ce faire, il convient d'examiner l'entreprise selon un point de vue statique en recensant ses moyens (matériel & logiciel), puis d'un point de vue dynamique, en relevant quels types d'activité elle déploie, et d'un point de vue plus synthétique en se préoccupant de son style de gestion.

II.1.1. Matériels recensés à la Bralima / Kisangani

Les postes de travail : ce sont les ordinateurs à partir desquels les utilisateurs accèdent à leurs sessions. Le tableau suivant présente les caractéristiques d'un ordinateur de Bralima / Kisangani. Tous les autres ont presque les mêmes caractéristiques.

N°	Nœuds	Quantité	Place	Description
1	Ordinateurs	55	Site BRALIMA	35 seront affectés dans ce site : - 20 au laboratoire, - 10 au cyber - 5 dans les différents bureaux d'administration
			site CD	10 ordinateurs seront affectés au deuxième site
2	Concentrateur	2	Site BRALIMA	1 sera Placé au Cyber
				Un autre au laboratoire
3	Commutateur	3	Site BRALIMA	Un pour interconnecter les différents bureaux de BRALIMA
			Site CD	Un pour interconnecter les différents bureaux de MIRADOR

Tableau 1 : Recensement des matériels

II.1.2. Logiciels recensés à la Bralima / Kisangani

Lors de notre étude sur terrain, nous avions recensé les logiciels suivants :

- Système d'exploitation client Windows 7 et Windows 8 professionnels tournant sur des postes clients.
- Système d'exploitation de type serveur Windows Server 2012 R2

II.1.3. Diagnostic du système existant

La critique de l'existant appelé aussi bilan de l'existant va nous aider, à l'évaluation du système existant par rapport à l'analyse faite à la Bralima Kisangani, tout en établissant un diagnostic.

---

[12] Philippe Atelin et José Dordoigne, **TCP/IP et les protocoles Internet**, Eni, 2006, page 175

[13] Benoît Lanlard, **Windows Vista: installation et configuration**, Eni 2007, page 240

[14] Jean-François PILLOU et Jean Philipe BAY, **op. cit.**, page 152

[15] Philippe Freddi , **Windows Server 2008 : les services réseaux TCP/IP**, Eni, 2009, page 439

[16] Philippe Atelin, **Wi-Fi: Solutions de sécurisation**, Eni, 2006, page 150

[17] Yves Emery, François Gonin, **Gérer les ressources humaines : des théories aux outils**, 2009, page 416

Ce diagnostic est établi dans le but de recherche de solution future à des problèmes posés. Le but de la critique de l'existant est d'établir un diagnostic précis sur les procédures utilisées, et relever les anomalies et les défauts du système existant. Par ailleurs deux constantes sont dégagées lors de cette critique : le point positif (fort) et le point négatif (faible). Ils méritent d'être soulevés étant donné que les besoins de la perfection seront toujours souhaités par les utilisateurs en vue de bon fonctionnement.

En analysant les ressources logicielles (Software) de l'entreprise Bralima / Kisangani, nous avons pu constater que ce dernier ne dispose que des systèmes d'exploitation client d'où la nécessité d'y intégrer le système d'exploitation réseau (NOS en anglais pour Network Operating System) ; celui-ci aura comme but de contrôler le réseau privé virtuel.

Concernant l'état de matériels, l'entreprise Bralima / Kisangani ne manque pas des ressources matérielles pour mettre en place un réseau privé virtuel. Tout ce que cette institution peut faire, c'est d'organiser leur ressource en termes de réseaux locaux puis interconnecter ces réseaux à l'aide d'un VPN.

II.2. CONCEPTION DU NOUVEAU SYSTÈME

Cette phase consiste à proposer un nouveau système qui va faciliter l'échange des données et la communication entre les partenaires. La conception d'un nouveau système d'information comporte plusieurs tâches, notamment : la conception de la base de données; la conception des flux sortants; la conception des traitements; la conception des flux entrants; la validation du modèle du nouveau système[18].

Dans cette partie, nous allons sur base de l'analyse faite, concevoir un nouveau système qui va prendre en compte les faiblesses et points forts de l'ancien système. Sur ce, nous procédons par la conception de la topologie physique, logique et le plan d'adressage pour ce nouveau système que nous voulons mettre en place.

II.2.1. Topologie physique

Compte tenu de l'emplacement physique des services qui composent la Bralima et tenant compte des services géographiquement éloignés que nous appelons "Centre de Distribution", nous adoptons la topologie en étoile basée sur une architecture client-serveur.

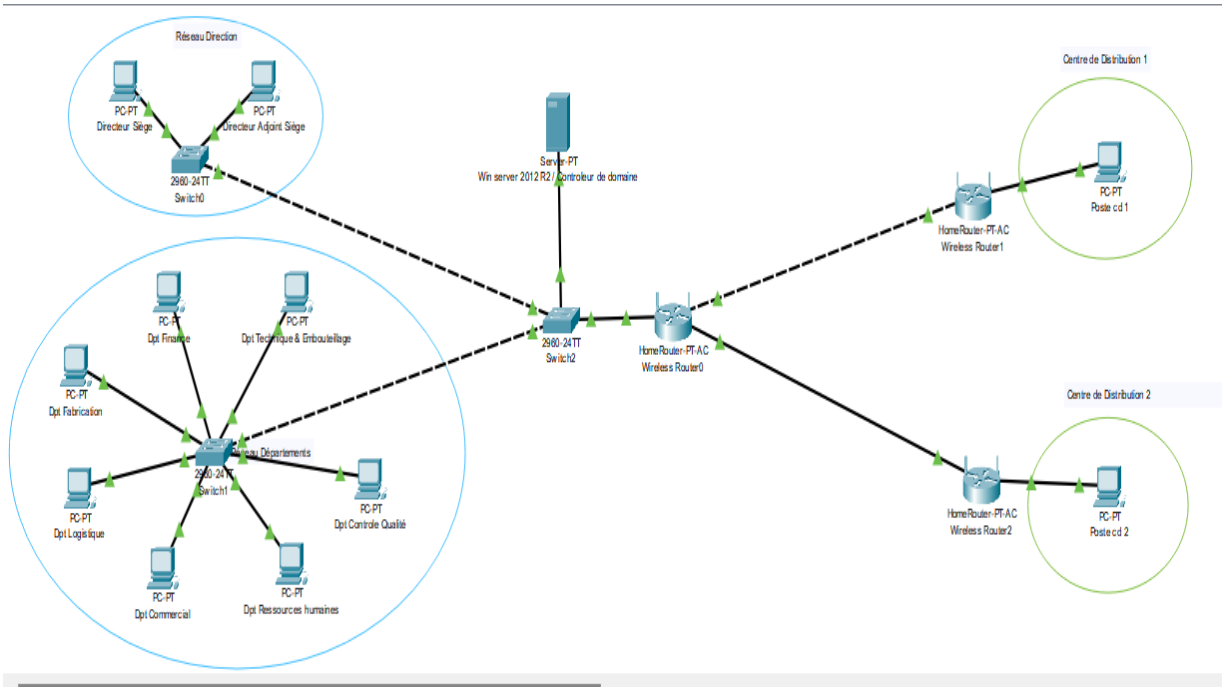

Figure 1 : Schéma global du réseau

II.2.2. Topologie Logique

La topologie logique adaptée à notre réseau serait fondée sur la technologie Fast Ethernet pour permettre des échanges de débits élevés entre différents services au sein de la Bralima et les échanges entre le siège avec le reste de l'infrastructure réseau distante que constituent les CD.

Ainsi, les caractéristiques de cette technologie sont les suivantes : le débit est passé à 100Mbits/s, le câblage est de type « paire torsadée de catégorie 3 » et Le fonctionnement en full-duplex, en permettant à un nœud de transmettre et de recevoir des données simultanément, double le débit.

II.2.3. Plan d'adressage

[18] Fahd M.S. Alduais, Le Système d'information comptable au milieu automatisé, Les éditions du Net 2013, page 65

Pour permettre une meilleure communication de tous les équipements de notre réseau, nous proposons le plan d'adressage suivant :

Matériel	Nom Poste	Adresse IP	Masque réseau	Mode d'Attribution
Server	Administrateur	192.168.0.2	255.255.255.0	Statique
PC	Directeur de siège	192.168.0.100	255.255.255.0	Dynamique
PC	Directeur Adjoint	192.168.0.101	255.255.255.0	Dynamique
PC	Département Logistique	192.168.0.102	255.255.255.0	Dynamique
PC	Département Commercial	192.168.0.103	255.255.255.0	Dynamique
PC	Département de Fabrication	192.168.0.104	255.255.255.0	Dynamique
PC	Département de Finance	192.168.0.105	255.255.255.0	Dynamique
PC	Département de Ressources humaines	192.168.0.106	255.255.255.0	Dynamique
PC	Département de contrôle qualité	192.168.0.107	255.255.255.0	Dynamique
PC	Département Technique et embouteillage	192.168.0.108	255.255.255.0	Dynamique
PC	Centre de Distribution 1	192.168.1.2	255.255.255.0	Statique
PC	Centre de Distribution 2	192.168.2.2	255.255.255.0	Statique
Routeur	Routeur Sans fil 0	192.168.0.1	255.255.255.0	Statique
Routeur	Routeur Sans fil 1	192.168.1.1	255.255.255.0	Statique
Routeur	Routeur Sans fil 2	192.168.2.1	255.255.255.0	Statique

Tableau 2 : Plan d'adressage réseau

II.3 IMPLÉMENTATION DE LA SOLUTION VPN

Dans cette dernière partie, nous détaillons les étapes de l'implémentation de la solution VPN dans le réseau de la Bralima. Puisque l'architecture qui a été retenue est celle de Client-serveur, nous commençons alors la configuration d'abord comme serveur avec Windows Server 2012R2 et ensuite nous terminons côté client avec le système Windows 10.

II.3.1. Configuration côté Serveur

a. Ajout de rôles et fonctionnalités dans le serveur :

- Pour créer un VPN, il faut aller dans le gestionnaire du Serveur, puis cliquer sur « Ajouter des rôles et des fonctionnalités », une fenêtre d'assistance s'affiche. Cliquer sur « Suivant ».
- Après avoir cliqué sur « Ajouter des rôles et des fonctionnalités », une fenêtre d'assistance s'affiche. Cliquons sur « Suivant ».
- Pour créer un VPN, il faut sélectionner « Installation basée sur un rôle ou une fonctionnalité ». Cliquons ensuite sur « Suivant ».
- Nous devons maintenant sélectionner le serveur sur lequel nous allons mettre en place le VPN. Ici un seul choix s'offre à nous. Nous pouvons cliquer sur « Suivant ».
- Il faut à présent déterminer le rôle de l'outil que nous voulons créer. Dans le cas d'un VPN, nous devons sélectionner l'accès à distance. Une fois coché, cliquons sur « Suivant ».
- L'assistant nous décrit à quoi sert un VPN et que faire pour le configurer. Cliquons sur « Suivant ».
- Sélectionnons les services du VPN. Il nous faut donc cocher « DirectAccess et VPN ».
- Une fois cochée, l'assistant nous demande de valider notre choix. Cliquez simplement sur « Ajouter des fonctionnalités » puis sur « Suivant » pour continuer l'installation.
- Nous avons désormais inclus tous les services et toutes les options nécessaires à la création du VPN. Cliquons à présent sur « Installer » pour créer le VPN dans le serveur.
- Une fois l'installation terminée, cliquons sur « Fermer ».
- Nous pouvons donc remarquer que l'accès à distance a bien été créé dans le serveur. Il faut désormais le configurer.

b. Configuration du VPN et accès aux utilisateurs

- Après avoir cliqué sur « Accès à distance », nous pouvons remarquer un message d'alerte nous disant qu'une configuration est requise afin que le VPN soit opérationnel. Cliquez donc sur « Autres… » afin de démarrer la configuration.
- Après cela une nouvelle fenêtre s'ouvre. Cliquez sur « Ouvrir l'Assistant Mise en Route » pour commencer la configuration du VPN.
- Une nouvelle fenêtre s'ouvre. Nous allons déployer le VPN uniquement.
- Ensuite, une nouvelle fenêtre apparaît. Faites un clic droit sur le serveur local puis sélectionnez « Configurer et activer le routage et l'accès à distance » sélectionner « Configurer et activer le routage et l'accès à distance ».
- Un assistant d'installation se met en marche. Nous allons donc suivre ses instructions et cliquer sur « Suivant ».
- Sélectionnez une « configuration personnalisée » et cliquez sur « suivant » Cochez seulement « Accès VPN » et cliquez sur « suivant »
- Cochons uniquement « Accès VPN » et cliquons sur « Suivant ».
- Après avoir cliqué sur « Terminer », une fenêtre d'avertissement apparaît nous informant que le Pare-feu bloque le port 1723, celui du VPN, et qu'il faudra donc l'autoriser à s'ouvrir. Nous nous en occuperons plus tard. Cliquez sur « OK ».

- Vous pouvez maintenant à présent terminer l'installation. Après avoir cliqué sur « Terminer », il ne reste plus qu'à démarrer le service. Il faut cliquer sur « Démarrer le service »
- Le VPN est désormais opérationnel. Nous pouvons fermer cette fenêtre.
- Il faut autoriser les utilisateurs du serveur à se connecter au VPN. Nous allons nous baser sur l'hypothèse selon laquelle il existe des utilisateurs appartenant à l'entreprise Bralima. Dans les outils du serveur, cliquez sur « Utilisateurs et ordinateurs Active Directory »
- Dans les outils du serveur, cliquons sur « Utilisateurs et ordinateurs Active Directory ». Allons dans le dossier Utilisateurs de l'entreprise MS et prenons comme exemple l'utilisateur **Christian Nzanzu**.
- Allez dans le dossier utilisateurs de Bralima et prenez par exemple l'utilisateur **Christian Nzanzu**. Faites un clic droit sur l'utilisateur et allez sur « Propriétés ».
- Une fenêtre se met en marche, allez dans l'onglet « Appel Entrant » Une fois dans cet onglet, sélectionnez « Autoriser l'accès » dans l'autorisation d'accès réseau.
- Une fois dans cet onglet, sélectionnons « Autoriser l'accès » dans l'autorisation d'accès réseau. Appliquons les modifications et cliquons sur « OK ». L'utilisateur est maintenant autorisé à se connecter au VPN.

c. Configurer le pare-feu et les autorisations

- Nous allons maintenant autoriser l'accès au VPN dans le pare-feu de Windows Server.
- Cherchons donc « Autoriser une application via le Pare-feu Windows ».
- Une fenêtre apparaît. Cherchons « Routage et accès distant » et cochons toutes les cases afin d'autoriser tout utilisateur du serveur à se connecter au VPN. Cliquons sur « OK » puis fermons la fenêtre.

II.3.2. Configuration du client Windows 10

- Dans l'ordinateur de l'utilisateur, « Christian Nzanzu » que nous avons pris comme exemple, nous allons mettre les configurations pour qu'il soit en mesure de se connecter au VPN. Il possède une connexion internet chez lui et notons que Christian Nzanzu possède Windows 10. Faites un clic droit sur l'icône du réseau et ouvrez le « Centre de Réseau et Partage ».
- Une fenêtre apparaît, cliquez sur « Configurer une nouvelle connexion ou un nouveau réseau ». Choisissez « Connexion à votre espace de travail » puis cliquez sur « Suivant ».
- Une nouvelle fenêtre s'ouvre et vous demande l'adresse IP ou le nom de domaine du serveur auquel vous voulez vous connecter. Vous pouvez renommer le nom de la connexion. Cliquez ensuite sur « Créer ». Vous pouvez maintenant constater que le VPN est apparu dans la liste de connexion disponible. Cliquez sur connexion VPN. On n'a plus qu'à entrer les identifiants liés au serveur de son bureau et il sera connecté au VPN.
- Après avoir cliqué sur « connexion VPN », on vous demande de renseigner vos identifiants pour vous connecter au réseau de l'entreprise.

CONCLUSION

Dans cet article, il était question de concevoir un nouveau système de communication sécurisé entre le siège de la Bralima / Kisangani et ses centres de distribution géographiquement éloignés. Ainsi, nous avons procédé par la formulation des quelques questions qui ont constitué la quintessence de notre problématique et nous a permis d'émettre les hypothèses selon lesquelles l'implémentation d'une solution sécurisée par la technologie VPN serait opportune et idéale. Pour se faire nous nous sommes fixé comme objectif d'implémenter un réseau sécurisé en vue de permettre à cette entité d'échanger de manière sûre et efficace ses données confidentielles avec le reste de son infrastructure géographiquement distantes.

Pour atteindre cet objectif, nous avions fait recours à l'approche analytique et descriptive qui nous ont permis respectivement d'analyser le système existant de cette entreprise en vue de proposer un nouveau système capable d'assurer une meilleure communication des données entre les différents sites distants de la Bralima et de décrire de manière détaillée les technologies réseaux adaptées aux attentes de nos besoins. Une cartographie nette de la topologie réseau et du plan d'adressage a été dressée tout en s'appuyant sur la structure organisationnelle de la Bralima / Kisangani.

Ainsi, nous avions fait le choix technologique de notre implémentation en nous focalisant sur les fonctionnalités de sécurisation des échanges proposées par le système d'exploitation Windows Server 2012 R2 comme couche serveur de notre architecture et les postes Windows 10 utilisés comme clients. Les différentes étapes de cette implémentation ont été définies clairement pour permettre à tout lecteur de se familiariser à cette configuration.

Compte tenu de la pertinence de cette étude, nous recommandons aux autorités de la Bralima d'intégrer la solution qui a été proposée en vue d'assurer une meilleure communication des échanges de données entre ses différents sites géographiquement éloignés à travers une technologie de sécurité adaptée aux besoins de ladite entreprise.

Sur ce, tout en ne prétendant pas avoir traité ce thème de manière exhaustive, la présente étude renferme probablement des imperfections susceptibles d'être corrigées par toute personne éprise de vérité. Aussi, pensons-nous qu'elle laisse une porte ouverte aux autres chercheurs de pouvoir aborder certains aspects non encore élucidés, et ce dans le seul but de pouvoir avancer la science.

BIBLIOGRAPHIE

[1]. Benoît Lanlard, **Windows Vista : installation et configuration**, Eni 2007, page 240
[2]. Claude Servin, **Réseaux et Télécoms**, 4ième édition, Dunod, 2013.

[3]. Fahd M.S. Alduais, Le Système d'information comptable au milieu automatisé, Les éditions du Net 2013.
[4]. Guy Pujolles, **Les Réseaux,** 9e édition, Eyrolles, 2020.
[5]. Guy Pujolles, **Les Réseaux**, 6ième édition, Eyrolles 2008.
[6]. Jean-François PILLOU et Fabrice LEMAINQUE, **Tout sur les réseaux et Internet**, 4ième édition, DUNOD, 2015, page 5.
[7]. Jean-Paul ARCHEIER, **Les VPN -Fonctionnement, mise en œuvre et maintenance des Réseaux Privés Virtuels**, 2e Edition, ENI, 2013.
[8]. Philippe Atelin et José Dordoigne, **TCP/IP et les protocoles Internet**, Eni, 2006.
[9]. Philippe Atelin, **Wi-Fi: Solutions de sécurisation**, Eni, 2006.
[10]. Philippe Freddi , **Windows Server 2008 : les services réseaux TCP/IP**, Eni, 2009
[11]. Rigobert PEZO et NASSUKA BIYO, **Initiation à la théorie et à la pratique du Réseau Informatique**, CRIGED, 2012
[12]. Yves Emery, François Gonin, **Gérer les ressources humaines : des théories aux outils**, 2009