1. Les VPN (Virtual Private Network)

Un VPN ou **Virtual Private Network** (Réseau Privé Virtuel) est une technique dont l’objectif est de permettre à plusieurs postes distants de communiquer. Elle est apparue avec la nécessité pour les entreprises de relier leurs différents sites, de façon simple mais aussi peu coûteuse. Avant l’arrivée des VPN, les entreprises devaient utiliser des liaisons appelées TRANSPAC, ou bien des lignes louées. Les VPN ont alors permis de démocratiser ce type de liaison. Le terme VPN sera notamment utilisé dans un contexte de travail à distance, ainsi que pour l’accès à des structures de type [**cloud computing**](https://fr.wikipedia.org/wiki/Cloud_computing).

1. Principes de fonctionnement d’un Virtual Private Network (VPN)

Le principe même des VPN repose sur un protocole appelé “protocole de Tunneling“. Il permet notamment de faire circuler les informations de façon cryptée d’un bout à l’autre du tunnel qui relie deux postes. Une fois identifiés l’émetteur et le destinataire, le principe du Tunneling consiste donc à construire un chemin virtuel entre eux. Par la suite, l’émetteur chiffre les données et les envoie afin que celles-ci soient acheminées grâce à ce chemin virtuel. Simuler ainsi un réseau privé permet d’assurer un accès simple et économique aux intranets ou aux extranets d’entreprise. Mais les échanges reposent en réalité sur une infrastructure d’accès partagée, comme Internet. Concernant leur acheminement, les données transmises sont généralement prises en charge par un protocole différent d’[IP](https://www.cnam-eng221.com/notions-informatiques/). Dans ce cas, le protocole de Tunneling encapsule les données en ajoutant un en-tête. En conclusion, le Tunneling est l’ensemble des processus d’encapsulation, de transmission et de désencapsulation.

1. Plan du mémoire

Ce mémoire s’intéresse aux différentes solutions qui permettent d’échanger des informations au sein des réseaux informatiques de manière sécurisée. La première partie donne une présentation générale des VPN en expliquant le fonctionnement et les objectifs de ces derniers. Puis, le mémoire aborde dans deux parties distinctes, deux solutions VPN très répandues dans le monde de l’entreprise. Le VPN SSL/TLS aussi appelé « clientless », car il ne nécessite pas l’installation d’un logiciel client. Puis le VPN IPsec qui nécessite l’installation d’un logiciel « agent » afin d’établir un tunnel vers un serveur.

Description du sujet choisi :

Les systèmes informatiques étant un outil majeur dans la croissance d'une entreprise ,afin d’améliorer les performances et la sécurité de cette dernière, je me suis penché sur le cas du VPN.

Cette dernière nécessitera une intervention, une bonne compréhension de l'infogérance et les différents moyens de protections.

En autre il permettra :

\*D'accéder au système d'information de l’entreprise à distance rapidement;

\*D'uploader en toute sécurité des données depuis l’extérieur de l’entreprise;

\*De suivre l’activité opérationnelle des équipes.

Cas pratique concret : Déploiement et configuration d'un VPN : solution pour des entreprises Multi-sites pour africa Tech solar

**REMARQUES**

Bien définir :

Les contraintes : https://fr.wikipedia.org/wiki/Contrainte\_technique

Les besoins : établir une liaison réseau à deux entités distantes de AFRICA TECHSOLAR (Cameroun et celui du Congo)

’échanger des informations de manière fiable et sécuriser

Les objectifs : mettre en place une solution qui correspondrait au mieux à leur architecture réseau et en rapport avec leur environnement de travail.