République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Bejaïa

Faculté de Technologie

Département Automatique, Télécommunication et Electronique

Mémoire de fin d'études

En vue de l'obtention du diplôme de Master en réseaux et télécommunication

Thème

Mise en place de la téléphonie IP sur un réseau VPN multi site.

Présenté par :

- Melle BOUMERTIT Sarah
- Melle BOUTERCHA Chahinez

Devant le jury composé de :

- Promoteur : Mr BERRAH Smail
- Président : Mme MAMMERI
- Examinateur : Mr GHERBI
- Co-promoteur : Mr khireddine A.karim

Promotion : 2021/2022

Dédicace

J'ai le plaisir de dédier ce modeste travail accompagné d'un profond amour :
A celle qui m'a arrosé de tendance et d'espoir, à la source d'amour inaccessible, qui ma bénie par ces prières…**ma mère**

A mon support dans ma vie, qui m'a appris ma supporté et ma dirigé vers la gloire …**mon père.**

A mon chère frère **« Nour El islem** » et ma chère sœur « **Radhia** » pour leur grand amour et leur soutien.

A Mon fiancé « **saber** » qui n'est pas cessé de me conseiller, encourager et soutenir tout au long de mes etudes.

A tout ma belle-famille : **nihed, aymen, hamza, ma belle-mère, et mon beau père.**

A mon adorable cousine « **Amina** ».

A mon chère oncle **« Farid et A louhab** » pour leur soutien et leur encouragement.

A tout la familles **Aiteur et Boutercha** et a ceux qui me donnent de l'amour et de la vivacité.

A tous mes chers amis qui m'ont encouragé, et qui je souhaite plus de succès

Sans oublier mon binôme **« Sarah »** pour son soutien moral .sa patience et sa compréhension tout au long de ce projet.

Dédicace

Je remercie Allah de m'avoir donné la force et le courage pour pouvoir réalise ce Modest travail.

Je dédie ce travail à mes parents
Pour leur soutien et leur encouragement sans faille tout à long de mon parcours scolaire mais aussi personnel. Aucun mot ne serait exprimé tout mon amour et tout ma gratitude merci pour vos sacrifies le long de ces années merci pour vos présences rassurant et si j'en suis arrivée là c'est grâce à vous. J'espère que le bon dieu les gardes les comble de sante et leur une longue vie.
A mon père « Mohamad » pour son patient avec moi et son encouragement.
A ma source de bonheur la prunelle de mes yeux ma mère « zahia ».
Que le bon ALLAH vous garde en bonne santé.

A mes chères grands-mères maternel et paternelle Que ce modeste travail, soit l'expression des vœux que vous n'avez cessé de formuler dans vos prières.
Que dieu vous préserve santé et longue vie.

Mes très chers frères : Ghiles et Nadjim

A mes chers amis : Nassima, Kahina, Souhila, Ouassila, Yasmine…
Pour leurs aides et supports dans les moments difficiles

A mon cher binôme, chahinez
Pour son entente et sa sympathie

A tout ma famille oncles et tantes cousins et cousines petit et grand sans exception.

A toute personne que je connais de près et de loin a tout la promotion Master 2 RT 2022
pour tous les bons moments passés et à venir.

Table de matière

Chapitre II : le réseau VPN

CHAPITRE III : LA GENERALITE SUR LA VOIX SUR IP

CHAPITRE IV : Organisme D'accueil

CHAPITRE V : LA REALISATION

LA LISTES DES FIGURES

LISTES DES TABLEAUX

Introduction générale :

Le domaine des télécommunications est en constante évolution tous les jours les nouvelles technologies envahissent notre quotidien, dans ces nouvelles révolutions, nous Retrouvez la téléphonie IP, ou plus connue sous le nom de Voice over IP (VoIP, Voice over Internet Protocol), qui représente une technologie récente qui s'impose rapidement
Domaine de la communication vocale. Il utilise le réseau Internet omniprésent
Se propager à l'échelle mondiale et dans un nombre croissant de foyers et d'entreprise
Au lieu de disposer à la fois d'un réseau informatique et d'un réseau téléphonique
Commuté (RTC), l'entreprise peux donc, grâce à la VoIP, tout fusionner sur un même réseau.
Les nouvelles capacités des réseaux à haut débit devraient permettre de transférer de manière fiable des données en temps réel. [4]

Un réseau d'entreprise consiste en l'interconnexion de plusieurs réseaux locaux qui sont
Configuré en fonction de l'infrastructure physique à laquelle ils sont connectés. Subdivision
Les LAN traditionnels ne peuvent pas regrouper les utilisateurs en fonction des groupes d'utilisateurs Travail ou leurs besoins en bande passante. Par conséquent, ils partagent le même segment et se font concurrence Utiliser la même bande passante malgré des exigences de bande passante différentes Tout dépend du groupe de travail ou du département.

Ainsi, pour résoudre ces problèmes, le réseau local virtuel ou VLAN (Virtual Local
Area Networks) sont développés par les fabricants de matériel réseau. En effet, le réseau
Les VLAN vous permettent de créer n'importe quel nombre de réseaux logiques sur un seul réseau Infrastructure physique. La conception des VLAN permet de protéger et d'améliorer le réseau Local (LAN) utilise diverses méthodes pour segmenter le réseau tout en réduisant
Un flot d'informations utiles y circule. Il faut une hiérarchie
Simplifiez sa gestion et résolvez tous les problèmes.

Pour une interconnexion sécurisée entre sites distants partagés par une même entreprise
Les mêmes ressources ou avec des partenaires que nous utilisons Professional Line (LS),
Cette solution, bien qu'efficace, présente des limites du point de vue des coûts.
Construction, maintenance lorsqu'il y a un problème avec le câble... Lorsque cette connexion est rompue Le faire à l'échelle d'un pays voire d'un continent nécessite de penser à une solution

plus souple Tout en minimisant le coût, afin de résoudre ce problème, la technologie VPN (Virtual Private réseau) est configuré pour autoriser les utilisateurs non connectés au réseau Le réseau interne peut encore passer Réseau public (Internet). Le principe du VPN est relativement simple, son but est de créer un réseau à travers un réseau public un tunnel crypté qui permet aux données de transiter vers le réseau privé Avoir une connexion Internet.

L'objectif principal de ce projet est basé sur la mise en place de la téléphone IP sur un réseau VPN multi site en utilisant GNS3 et le VMware afin de permettre un accès à distance vers un réseau LAN.

Afin de présenter notre travail, nous avons structuré notre mémoire comme suit : Dans le premier chapitre nous allons donner une présentation générale sur les réseaux Pour nous initier ensuite à la sécurité réseau et aux VPN - VLAN , dans le second chapitre de ce travail qui se divise en deux parties nous commençons à présenter les différents principes de bases et l'architecture de la TOIP, ces avantages et ces inconvénients, la qualité de service, ensuite, on a détaillé et précis les différents protocoles de la signalisation dédiés à ce genre d'applications. Le troisième chapitre l'organisme d'accueil, apportant quelques notions de base et des informations générales sur les techniques qui seront utilisées tout au long du travail.

Le dernier chapitre aborde les différents outils nécessaires à la mise en place d'une infrastructure Active Directory, suivi du paramétrage et de la mise en place de la solution +

Il est recommandé de commencer par l'implémentation et la configuration d'un contrôleur de domaine Sous Windows Server 2022, mettre en place le serveur de base de données ainsi que le serveur ASTERISK, et enfin, nous allons procéder à la sécurisation du réseau avec le pare-feu pfSense et configurer la connexion VPN au site distant, nous terminerons par une conclusion nous terminerons par une conclusion.

Les télécommunications en particulier occupent une bonne place, dans la mesure où elles constituent le moteur de développement de l'économie et de la société.

Dans l'examen de la réalité qui se passe, il n'en pas le cas, cependant les nouvelles applications réseaux, telle que la VoIP, devait s'apprendre au sein même de l'entreprise.

Face à cette nécessité et par souci d'apporter notre modeste contribution en matière de développement de la communication au sein de l'entreprise SONATRACH Bejaïa, nous pensons que l'implémentation de la VoIP sur ce dernier sera une des solutions appréciables de tous.

De cet ordre d'idées, il convient de se poser quelques questions, telles que :

- **Est-il possible d'améliorer les moyens de communication au sein de Sonatrach Bejaïa ?**
- **Est-il possible d'implémenter la solution VoIP dans un réseau informatique à multi-sites ?**
- **Comment sécuriser la solution VoIP qui sera implémentée ?**

Telles sont les questions auxquelles nous allons tenter de répondre dans la suite de notre travail.

Les difficultés sont multiples au sein de l'entreprise SONATRACH Bejaïa en ce qui concerne le système des communications pour ses personnels.

Ainsi, nous pensons que l'implémentation d'une solution VoIP au sein de son réseau informatique à multi-sites, pourra faire bénéficier au personnel œuvrant au sein de son administration d'effectuer les appels téléphoniques internes, gratuitement sans dépensé de l'argents .

En fonction des besoins réels de l'entreprise, différents arguments plaident en faveur d'une solution VoIP, raison pour laquelle *l'objectif* principal poursuivi dans ce travail est de montrer l'importance de l'intégration de la VoIP dans les entreprises (qu'elles soient multi-sites ou non) en général et à l'entreprise SONATRACH en particulier d'une part, et de proposer l'implémentation de cette technologie au sein du réseau informatique de ce dernier d'autre part.

Tout travail qui se veut scientifique doit être examiné dans le temps tout comme dans l'espace, il doit bien cerner le contour du sujet et faciliter la démarche scientifique pour arriver au résultat escompté.

Dans le cas de ce travail, nous nous limiterons essentiellement à la définition de la théorie se rapportant à la solution VoIP et à la description des matériels de base permettant son déploiement. Nous allons également procéder à une expérimentation d'une communication VoIP à l'aide d'un minimum de matériel à notre disposition.

Au moment où le monde entier connait un essor considérable sur les nouvelles technologies de l'information et de la communication, les entreprises sont appelées à retrouver leurs places dans cet essor afin de jouer le rôle d'élément moteur du progrès social, économique et politique.

Ainsi, trois raisons primordiales justifient le choix et l'intérêt de cette monographie, à savoir :

- Premièrement, nous nous acquittons de notre devoir légitime de finaliste du second cycle, qui oblige à ce que chaque étudiant rédige un travail de fin d'étude, ainsi que le souci permanent d'approfondir nos connaissances dans le domaine de voix sur IP
- Deuxièmement, cette œuvre intellectuelle nous permet de rapprocher les notions théoriques accumulées pendant toute notre formation à la pratique, et constitue une source d'approvisionnement incontestable pour les futurs chercheurs qui aborderont le même thème de la recherche que nous
- Troisièmement, pour l'entreprise SONATRACH, nous voulons par le présent travail, apporter notre modeste contribution tant soit peu aux problèmes de communication qu'il connaît en son sein, dont les questions sont épinglées dans la problématique.

I.1 Introduction :

Les réseaux sont nés du besoin d'échanger des informations de manière simple et rapide entre des machines. En d'autres termes, 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 les stations de travail à leur serveur.

Dans un premier temps, ces communications étaient uniquement destinées au transport des données informatiques, mais aujourd'hui avec l'intégration de la voix et de la vidéo, elles ne se limitent plus aux données mêmes si cela ne va pas sans difficulté. [9]

Dans ce chapitre nous allons voir les réseaux informatiques en général. Ces réseaux permettent le partage de ressources entre ordinateurs : données ou périphériques (imprimantes, connexions internet, scanners, etc.).

I.2 Définition :

Le réseau informatique est un ensemble d'équipements informatiques ou systèmes digitaux interconnecté entre eux via un milieu de transmission de données en vue partage de ressources informatiques et de la communication. [2]

I.3 Classification des réseaux :

Il existe plusieurs types de réseaux selon le réseau distance entre les systèmes informatiques, ou selon la technologie qui permet leur mise en œuvre.

Les réseaux sont plus ou moins vastes et on en distingue 3 catégories :

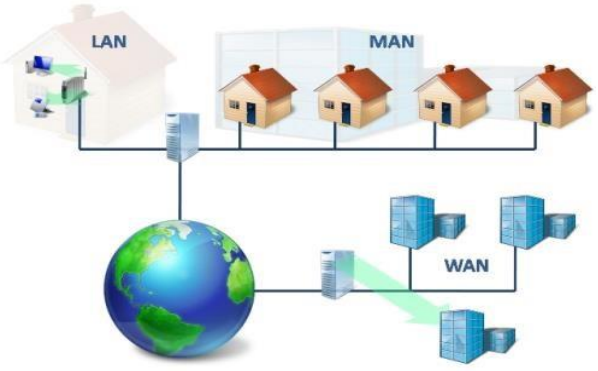


Figure I.1 : les types de réseaux [1]

I.3.1 Les LANs :

LAN signifie Local Area Network (en français Réseau Local). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s (pour un réseau Ethernet par exemple) et 1 Gbit/s (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs [2]

I.3.2 Les MANs :

Les MAN (Metropolitan Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local. Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique) [2].

I.3.3 Les WANs :

Un WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est Internet [2]

I.4Architecture des réseaux :

En élargissant le contexte de la définition du réseau aux services qu'il apporte, il est possible de distinguer deux modes de fonctionnement

- **Architecture d'égal à égal** (peer to peer parfois appelée poste à poste), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur joue un rôle similaire.
- **Architecture de type client-serveur,** ou un ordinateur (serveur) fournit des services réseau aux ordinateurs clients. [7]

I.5 Topologies des réseaux :

La topologie du réseau couvre simplement son chemin Les différents composants et leurs interactions. Nous ne séparons pas les topologies Pour la simplicité, physique et logique.

Nous allons définir ces types :

I.5.1 Topologie en bus :

Un réseau de bus connecte ses composants sur le même câble et envoie des informations sur le bus. La station diffuse sur toutes les stations simultanément. Seule la station de destination est Considérée. Le câble coaxial est souvent utilisé pour réaliser ce type de réseau. Ensuite, il y a une prise à chaque extrémité du câble. Avec le câble coupé, plus de stations. [3].

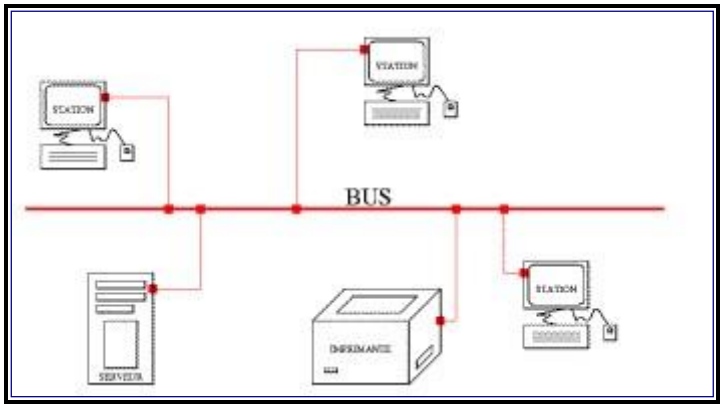


Figure I.2 Topologie en bus.

I.5.2Topologie en étoile

Dans un réseau en étoile, tous les composants sont connectés à un point central, et Les informations ne transitent de l'expéditeur au destinataire que par ce point central. Si ce n'est pas un interrupteur, on met un hub, alors la topologie physique reste en forme d'étoile.

En réalité, un hub ne sait diffuser des informations que sur tous ses ports sans exception. [3].

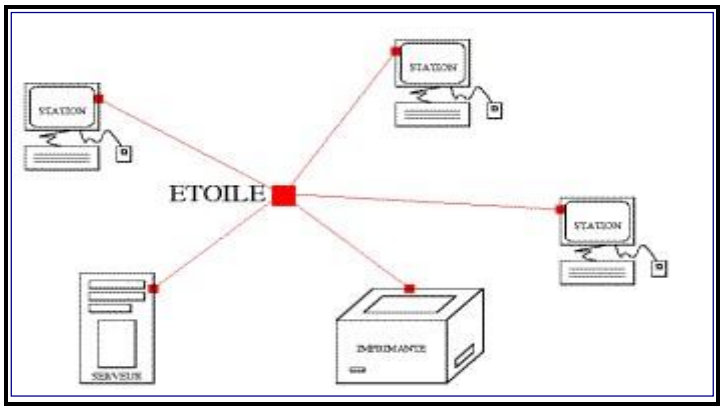


Figure I.3 Topologie en étoile.

I.5.3Topologie en anneau :

Un réseau en anneau a lui aussi tous ces composants liés par le même câble, mais celui-ci n'a pas d'extrémité. De plus, l'information ne circule que dans un sens bien déterminé. Dans le cas du FDDI (Fiber Distributed Data Interface), réseau à base de fibre optique , on a deux anneaux indépendants.

Chaque machine doit donc posséder deux interfaces. En cas de rupture des anneaux entre deux machines, ces dernières reforment un unique anneau en assurant le transit de l'information entre leurs deux interfaces [3].

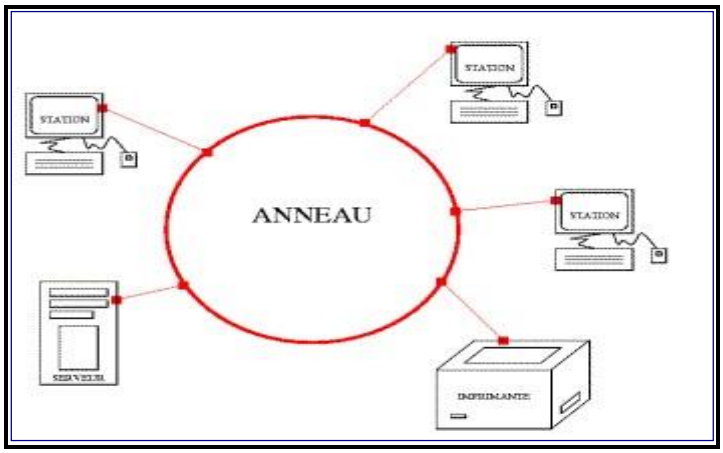


Figure I.4: Topologie en anneau.

I.5.4 Topologie Point à Point :

Dans un réseau point à point, chaque interface possède une liaison spécifique avec chacun des autres points. Ceci n'est utilisé que sur de tous petits réseaux pour des raisons de redondance [3].

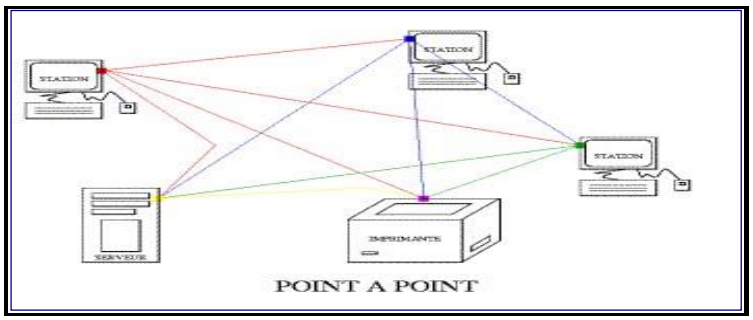


Figure I.5 : Topologie point à point.

I.6 Les équipements réseau :

L'interconnexion des réseaux peut être locale : les réseaux sont au même endroit géographique. Dans ce cas, un équipement standard (répéteurs, routeurs, etc.) est adapté à la connexion physique.

L'interconnexion peut également impliquer des réseaux distants. Il est alors nécessaire de connecter ces réseaux via des liaisons téléphoniques (modems, etc.).

I.6.1 Répéteur :

Les répéteurs permettent d'interconnecter deux segments d'un même réseau.

C'est passif, ça amplifie juste le signal. Il ne permet pas de connecter deux types de réseaux différents, il fonctionne au niveau 1 du modèle OSI.

I.6.2 Ponts :

Un pont ne peut connecter que deux réseaux utilisant le même protocole.

La possibilité de mémoriser un "carnet d'adresses" des machines qui composent le réseau.

Ils identifient la source des données qui leur parviennent et ne traitent que les données passant d'un réseau à l'autre, les trames échangées au sein d'un même réseau ne sont pas transmises, ce qui assure une confidentialité accrue entre les réseaux.

I.6.3 La passerelle (Gateway) :

Les passerelles assurent la connexion de deux réseaux hétérogènes car ce sont des systèmes matériels qui intègrent des applications, transformant les données à transmettre afin de les adapter aux protocoles du réseau cible.

I.6.4 Routeur :

Un routeur peut être assimilé au "carrefour" d'un réseau, contrairement aux deux appareils précédents, qui ne peuvent se connecter qu'à deux réseaux au maximum (ils ont généralement de 4 à 16 ports).

Les chemins empruntés par les données sont prédéfinis dans la table de routage et sont optimisés en fonction de critères de longueur de chemin (nombre de sauts vers la machine de destination) ou de temps (encombrement du réseau).

I.6.5 Concentrateur (HUB) :

Un concentrateur est une boîte avec une fonctionnalité de répéteur. Mais sa fonction principale est la possibilité de regrouper plusieurs lignes en une seule.

Il peut connecter plusieurs sites dont le nombre dépend du type de HUB. Un HUB sera connecté à un autre HUB ou serveur uniquement par une ligne.

I.6.6 le Commutateurs :

C'est un système qui assure l'interconnexion de sites ou de segments LAN en leur allouant toute la bande passant.

Les commutateurs ont été introduits pour augmenter la bande passante globale des réseaux d'entreprise par rapport au concentrateur Ethernet (ou HUB) [2].

I.7 Les techniques de commutation :

I.7.1 commutation de circuit :

Il s'agit de créer un circuit spécifique dans le réseau avant que l'expéditeur et le destinataire ne commencent à échanger des informations. Ce circuit est propre aux deux liaisons communicantes et sera libéré à la fin de la communication.

S'il n'y pas échange pas de données pendant un certain temps, le circuit reste alloué.

Toutes les données suivent le même chemin tout au long du processus de communication.

Exemple : réseau RTC.

I.7.2 La commutation de message :

Un message est une suite d'informations formant un tout, par exemple un fichier ou une ligne de commande tapée au clavier d'un ordinateur.

La commutation de message consiste à envoyer un message de l'émetteur jusqu'au récepteur en passant de nœud de commutation à un nœud de commutation. Chaque nœud de commutation attend d'avoir reçu complètement le message avant de le réexpédier au nœud suivant. [4]

I.7.3 La commutation de paquets :

Un paquet est une suite d'octets, dont le contenu n'a pas forcément une signification et ne pouvant pas dépasser une taille fixée par avance. Apparu dans les années 70 pour résoudre le problème d'erreur de commutation de messages. Un message émis est découpé en paquets. On

parle de segmentation du message, les paquets sont commutés dans le réseau comme dans le cas des messages.

La bonne liaison vers le destinataire est trouvée grâce à une table dite de commutation (ou de routage pour la couche 3). Le message est reconstitué à partir du ré assemblage des paquets reçus par le destinataire [2].

I.8 Technique de Transmission :

I.8.1 la transmission parallèle et série :

Le mode de transmission spécifie le nombre d'unités d'informations de base (bits) qui peuvent être transmises simultanément sur le canal de communication.

• Liaison parallèle signifie que N bits sont transmis simultanément. Ces bits sont envoyés simultanément sur N canaux différents.

• Dans une liaison série, les données sont transmises bit à bit sur le canal de transmission. Cependant, comme la plupart des processeurs traitent les informations en parallèle, les données arrivant en parallèle qui doivent être converties en données série au niveau de l'émetteur et vice versa. [4]

I.9 La pile protocolaire TCP/IP :

La définition : [7]

TCP/IP est une suite de protocoles. Le sigle TCP/IP signifie «Transmission Control Protocol/InternetProtocol». . TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se fonde 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.

* Cette suite est conçue pour répondre à un certain nombre de critères parmi lesquels :

- Acheminement des paquets de données sur le réseau.
- Utilisation d'un système d'adressage.
- Contrôle des erreurs de transmission de données.

TCP/IP est un modèle comprenant 4 couches tel qu'illustré dans la figure I.6.

Le datagramme IP (version 4) : [5]

Lorsque deux machines communiquent en utilisant le protocole IP, elles s'échangent des datagrammes IP qui ont le format ci-dessous :

32 bits (= 4 octets)			
Numéro de version	Longueur en-tête	Type de service	Longueur totale du datagramme
Identificateur (recopié dans chaque segment)			Drapeaux + position du segment
Durée de vie		Protocole couche 4	Somme de contrôle de l'en-tête
Adresse IP source			
Adresse IP destination			
Options			
Données			

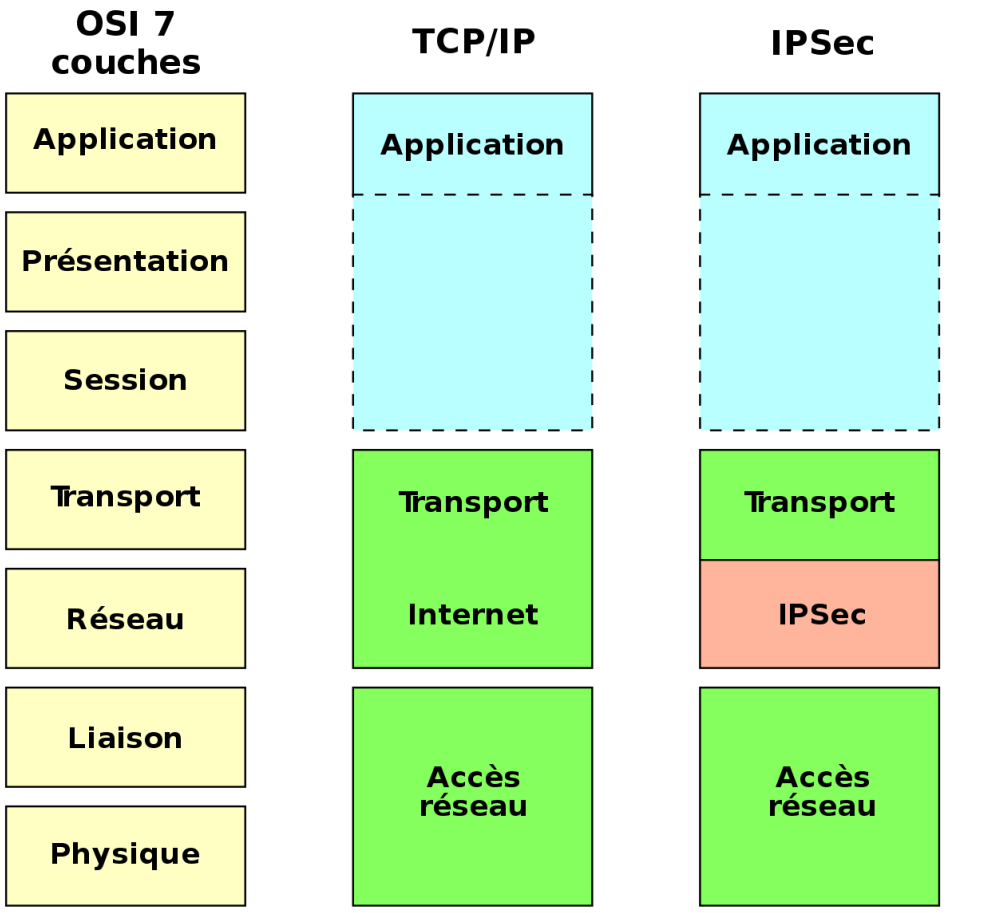


Figure I.6 : La pile TCP/IP et le modèle OSI

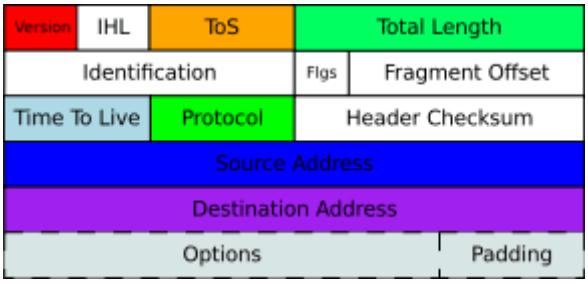


Figure I.7 : L'en-tête IPv4

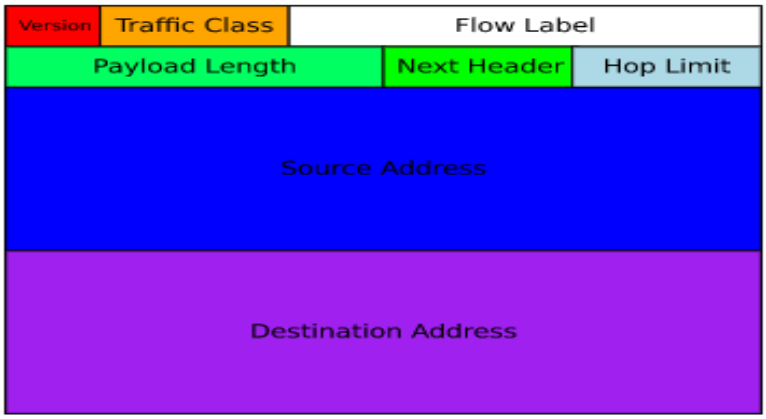


Figure I.8 : L'en-tête IPv6

■ **Version *(4 bits)* :**

le champ version indique la version utilisée du protocole IP. Début 2006, la version de IP la plus fréquemment utilisée est la version 4. La version 6 commence à apparaitre : il n'y aura pas de version 5. Les 4 bits de ce champ sont donc 0100 (codage en binaire de la valeur décimale 4).

■ **IHL = IP Header Length - longueur de l'en-tête IP *(4 bits)* :**

ce champ indique la longueur de l'entête IP. L'unité est le nombre de mots de 32 bits.

Pour la version 4 la longueur de cette entête est de 20 octets soit 5 fois 32 bits : ce champ vaut donc 0101.

■ **Type of service** ***(8 bits)*** **:**

ce champ permet d'indiquer que certains datagrammes IP ont une priorité supérieure à d'autres. Il est peu utilisé sauf par quelques routeurs spécialisés dans la transmission de voix sur IP.

■ **Total length** ***(16 bits)*** **:**

ce champ indique le nombre d'octets du datagramme, en-tête IP comprise. La longueur maximale du datagramme en octets est 2^{16}-1 = 65 535 octets = 64 ko -1 octet

■ **ID (16 bits) :**

ce champ est un identifiant du datagramme IP (le numéro du datagramme).

■ **F = Flags - les drapeaux** ***(3 bits)*** **:**

Le premier bit est inutilisé

Le deuxième bit DF (don't fragments) permet d'interdire ou d'autoriser la fragmentation. Positionné à 1, il est interdit de fragmenter ce datagramme IP.

Le troisième bit MF (more fragment) est utilisé lors de la fragmentation : il indique si le fragment est le dernier fragment du datagramme (MF=0) ou non (MF=1).

■ **TTL = Time to live - temps restant à vivre** *(8 bits)* :

Il s'agit d'une valeur initialisée par l'émetteur et qui est décrémentée de 1 à chaque fois que le datagramme traverse un routeur.

Si le TTL arrive à la valeur 0, le datagramme est détruit : ce mécanisme assure la destruction des datagrammes qui se perdent sur le réseau. Ainsi ces datagrammes perdus n'encombrent pas indéfiniment le réseau.

■ **Protocole** ***(8 bits)*** **:**

Ce champ indique la nature des données transportées par ce datagramme IP. 3 protocoles sont principalement utilisés au-dessus de IP : ICMP (code 1), TCP (code 6) et UDP (code 17).

■ **Header Checksum - somme de contrôle de l'en-tête *(16 bits)* :**

Il s'agit d'un code détecteur d'erreurs qui ne porte que sur l'entête : la somme des octets de l'entête regroupé par paquets de 16 bits (header checksum compris) doit valoir 2^{16}-1 modulo 2^{16}. En cas d'erreur sur l'entête le datagramme est détruit. IP n'est pas un protocole fiable puisqu'on ne garantit pas que les données arrivent, ni de leur fiabilité.

■ **IP source *(32 bits)* :**

Adresse IP de l'expéditeur.

■ **IP destination *(32 bits)* :**

Adresse IP du destinataire.

I.10 Le protocole IP [5] :

Le protocole IP (Internet Protocol) est un des protocoles majeurs de la pile TCP/IP. Il s'agit d'un protocole réseau (niveau 3 dans le modèle OSI). Il n'est pas orienté connexion, c'est à dire qu'il n'est pas fiable. C'est la couche transport qui peut le rendre fiable.

I.11 La conclusion :

Une compréhension des réseaux informatique est une étape nécessaire dans une compréhension globale de l'environnement réseau.

Dans ce chapitre, nous avons présenté les techniques de commutation et transmission, classification des réseaux, ainsi que les équipements d'interconnexion réseau.

II.1 Introduction :

De nos jours, l'utilisation de l'internet n'est plus sûr. Souvent les transmissions de données ainsi que les sites web ne sont pas protégés et sont vulnérables aux attaques des cybers criminels. La sécurité d'un réseau est un niveau de garantie pour que l'ensemble des machines fonctionnent d'une façon optimale.

Dans ce chapitre, nous allons présenter les technologies des VPN son fonctionnement, ses déférentes types, les protocoles qu'il utilise et sécurité de VPN.

II.2 L'étude des technologies des VPN :

II.2.1 Le principe et le fonctionnement des VPN :

Le VPN consiste à relier des lieux géographiques entre eux de manière sécurisée afin de faire communiquer leurs systèmes informatiques. La principale alternative aux VPN consiste à louer des lignes dédiées pour relier les sites d'une entreprise entre eux.

Ces connexions totalement privées sont très intéressantes, car la sécurité est déjà fournie par le loueur. Les données qui y circulent sont intégralement privées et un pirate informatique ne peut en récupérer le contenu. [6]

Le VPN est basé sur Tunneling Protocol, qui est le protocole utilisé pour le cryptage

Les données sont obtenues via un algorithme de cryptage entre les deux réseaux. Le VPN n'est qu'un concept, pas une implémentation. Il se caractérise par

Les obligations suivantes :

* Authentification des entités communicantes : le serveur VPN doit s'assurer que la parole

À un vrai client VPN et vice versa. [7]

II.2.2 Les différents types de VPN :

Concernant les types de VPN, on distingue trois types : les VPN d'accès, les VPN intranet et les VPN extranet :

- **Le VPN d'accès [8] :** Le VPN d'accès est utilisé pour permettre à un utilisateur itinérant ou isolé de se connecter dans un réseau local interne par exemple, de son entreprise. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. A cet effet, cette connexion pourrait être établie de deux manières distinctes :

* L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique à cet effet avec le NAS (Network Access Server) du fournisseur d'accès et ce dernier établit la connexion cryptée.

* L'utilisateur possède son propre logiciel client pour le VPN auquel il établit directement la communication de manière cryptée vers le réseau d'entreprise.
Dans ce cas, il peut avoir son propre client VPN afin de se connecter directement au réseau. Si non, il doit demander à son FAI de lui fournir un serveur isolé et le serveur d'accès n'est pas crypté tel qu'illustré dans la figure II.6 ci-dessous :

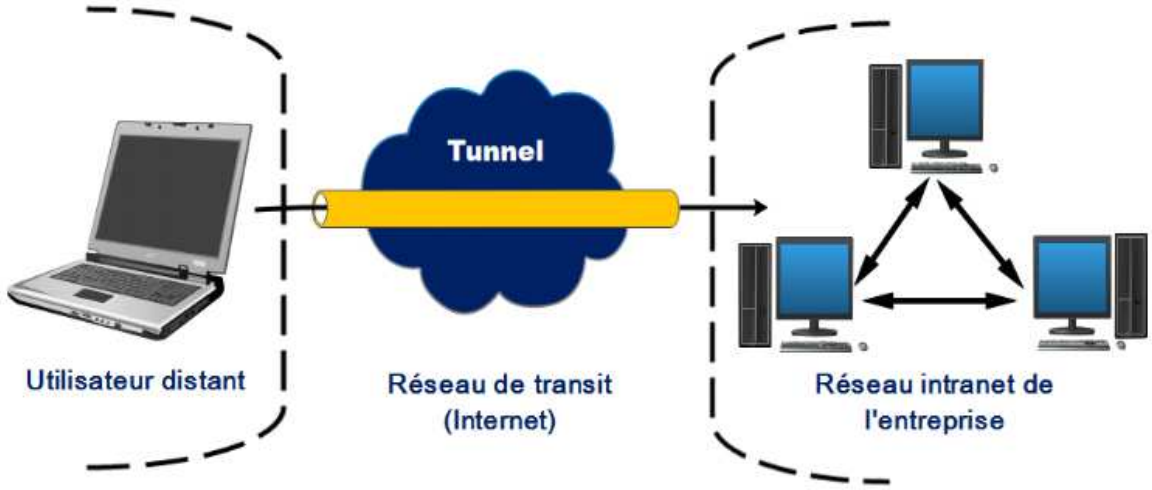


Figure II.1 : Architecture d'un VPN d'accès

- **L'intranet VPN [7] :** Dans une entreprise l'Intranet met à la disposition des employés des documents divers (texte, vidéo, image…), ce qui permet d'avoir un accès centralisé et cohérent aux informations de l'entreprise. L'intranet peut remplir plusieurs fonctions :

- Mise à disposition de documents techniques
- Mise à disposition d'informations sur l'entreprise
- Forums de discussion, listes de diffusion, chat en direct
- Gestion de projets, agenda, aide à la décision
- Un échange de données entre collaborateurs
- Moteur de recherche de documentations

- Portail vers internet
- Messagerie électronique
- Annuaire du personnel
- Visioconférence

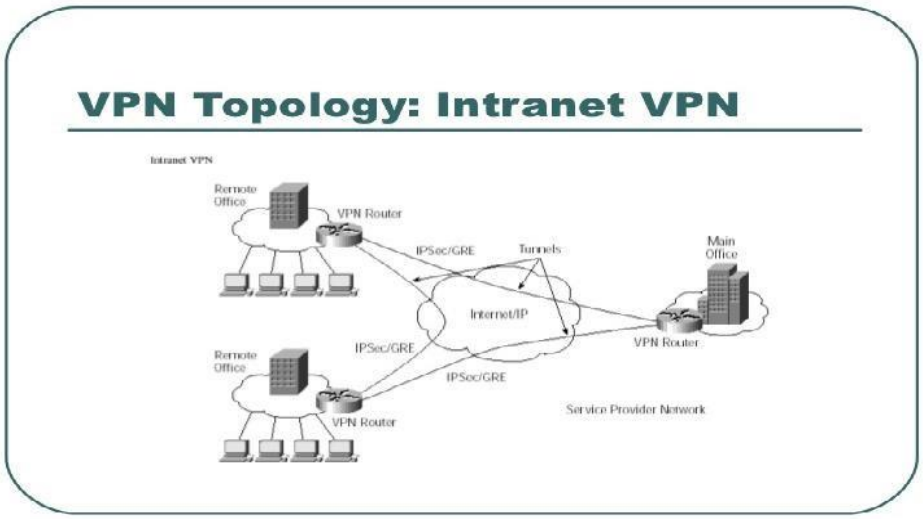


Figure II.2: Intranet VPN

- **L'extranet VPN [8] :** Une entreprise peut utiliser le VPN extranet pour communiquer avec ses clients, les fournisseurs et les partenaires au moyen d'un intranet d'entreprise reposant sur une infrastructure partagée à l'aide de connexions dédiées. Dans ce cas, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

Ci-dessous, la figure I.8 décrit l'architecture d'un VPN Extranet.

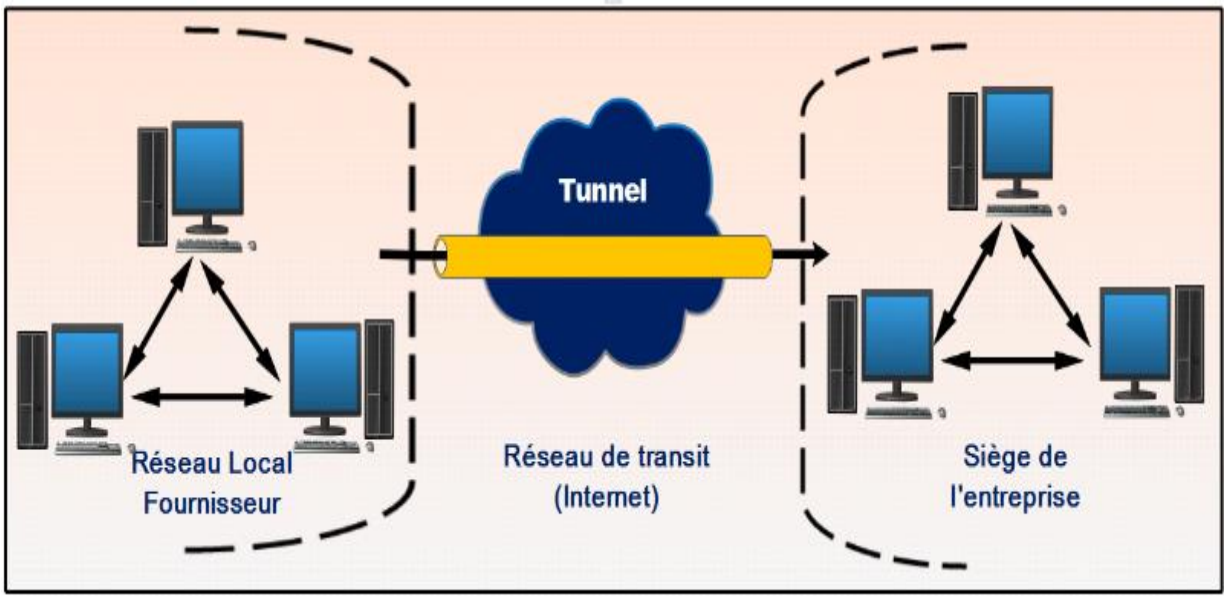


Figure II.3: Architecture d'un VPN Extranet

II.2.3 Open VPN :

Le Protocole Open VPN est une application informatique ouverte pour la mise en place de techniques de réseaux privés virtuels (VPN, en anglais Virtual Private Network), avec des connexions sécurisées point-par-point ou site-par-site, pour des configurations via routage ou pont, ainsi que pour les accès à distance. Il exploite un protocole de sécurité sur mesure qui utilise SSL/TLS pour les échanges clés.

Un protocole Open VPN permet à des homologues de s'authentifier mutuellement en utilisant une clé secrète pré-partagée, des certificats ou un nom d'utilisateur / mot de passe.
Lorsqu'il est utilisé dans une configuration multi client-serveur, il permet au serveur de libérer un certificat d'authentification pour chaque client, en utilisant la signature et l'autorité de certification.
Ce système utilise en grande partie la base de cryptage OpenSSL, ainsi que le protocole SSLv3/TLSv1 et contient de nombreuses fonctionnalités de sécurité et de contrôle [7].

II.3 Les protocoles utilises et sécurité de VPN

Il existe plusieurs protocoles dit de tunnellisation qui permettent la création des réseaux VPN, parmi ces protocoles on va aborder le protocole IP sec :

II.3.1 le protocole IPsec :

II.3.1.1 La définition IPsec :

IPSec (Internet Protocol Security) est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau du modèle OSI. Il assure la confidentialité (grâce au cryptage), l'authentification (qui permet d'être certain de l'identité de l'émetteur) et l'intégrité des données permettant de s'assurer que personne n'a pu avoir accès aux informations.

IPSec permet de protéger les données et également l'en-tête d'une trame, en masquant le plan d'adressage grâce à l'ajout d'un en-tête IPSec à chaque datagramme IP. IPSec de par sa position, agit sur chaque datagramme IP et permet ainsi d'offrir une protection unique pour toutes les applications.

Ce protocole est indissociable d`IPv6 est utilisable aussi sur IPv4 si le fournisseur a choisi de l'implanter dans son produit. [24]

II.3.1.2Le fonctionnement : [25]

Lors de l'établissement d'une connexion IPsec, plusieurs opérations sont effectuées : Échange des clés

- un canal d'échange de clés, sur une connexion UDP depuis et vers le port 500 (ISAKMP (en) pour Internet Security Association and Key Management Protocol).

Le protocole IKE (Internet Key Exchange) est chargé de négocier la connexion. Avant qu'une transmission IPsec puisse être possible, IKE est utilisé pour authentifier les deux extrémités d'un tunnel sécurisé en échangeant des clés partagées.

Ce protocole permet deux types d'authentifications, PSK (secret prépartagé ou secret partagé) pour la génération de clefs de sessions RSA ou à l'aide de certificats.

IPsec utilise une association de sécurité (Security association) pour dicter comment les parties vont faire usage de AH (Authentication header), portant les informations d'authentification, et de l'encapsulation de la charge utile d'un paquet.

• Une association de sécurité (SA) est l'établissement d'information de sécurité partagée entre deux entités de réseau pour soutenir la communication protégée. Elle peut être établie par une intervention manuelle ou par ISAKMP (Internet Security Association and Key ManagementProtocol).

• ISAKMP est défini comme un cadre pour établir, négocier, modifier et supprimer des SA entre deux parties. En centralisant la gestion des SA, ISAKMP réduit la quantité de fonctionnalité reproduite dans chaque protocole de sécurité. Il réduit également le nombre d'heures exigé par l'installation de communications, en négociant tous les services simultanément.

II.3.1.3 Transfert des données : [25]

Un ou plusieurs canaux de données par lesquels le trafic du réseau privé est véhiculé, deux protocoles sont possibles :

• le protocole no 51, AH, (Authentication Header) fournit l'intégrité et l'authentification. AH authentifie les paquets en les signant, ce qui assure l'intégrité de l'information. Une signature unique est créée pour chaque paquet envoyé et empêche que l'information soit modifiée3.

• le protocole no 50, ESP (Encapsulating Security Payload), en plus de l'authentification et l'intégrité, fournit également la confidentialité par l'entremise de la cryptographie.

II.4 Les VLANs :

VLAN (Virtual Local Area Network ou Réseau Local Virtuel en Français Réseau Local Virtuel) Un réseau local qui regroupe un ensemble de machines logiquement plutôt que physiquement. Un VLAN est un réseau commuté qui est logiquement segmenté selon la fonction.

II.4.1 Classification des VLAN : [26]

- **Les VLAN de niveau 1 :**

Chaque port physique du commutateur est configuré par l'administrateur du réseau pour appartenir `à un VLAN, et toute machine (ou ensemble de machines) qui se trouve branchée sur ce port fera partie de ce VLAN. C'est le mode de fonctionnement le plus simple.

Lorsque les équipements réseau étaient simples et fiables, on faisait déjà des VLAN par port tout simplement en construisant des réseaux physiquement séparés, chacun ayant son câblage et ses propres équipements actifs.

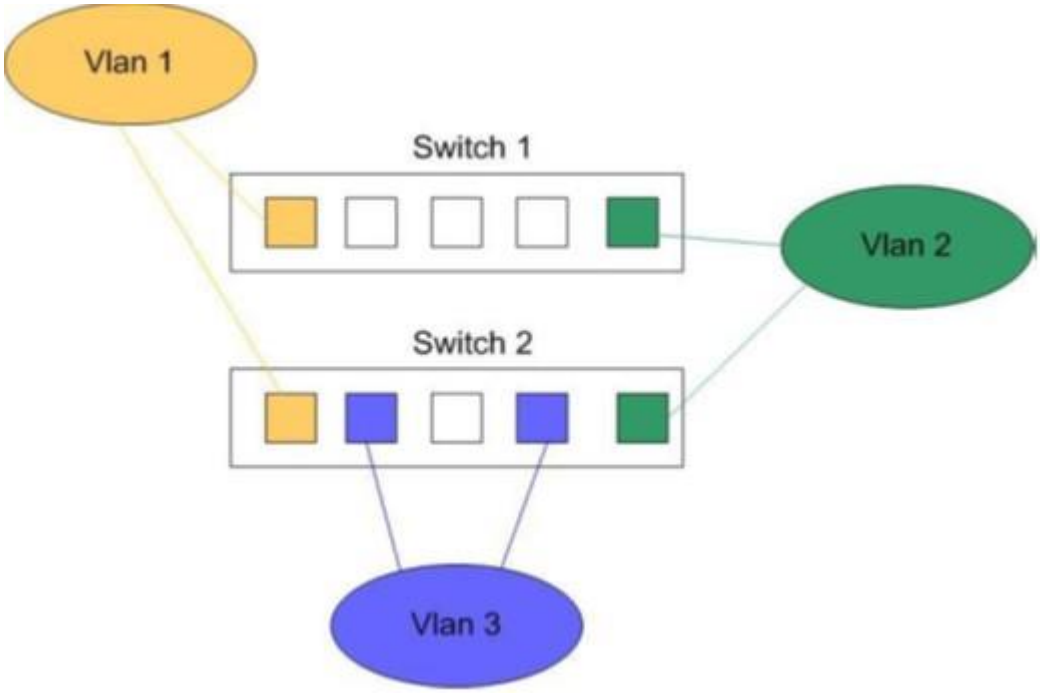


Figure II.4: VLAN par port [27]

- **Les VLAN de niveau 2**

Dans ce modèle, le VLAN auquel appartient une station est déterminé par son adresse MAC. Les adresses MAC étant physiquement liée aux stations, ce modèle permet de conserver la répartition des VLANs même après le déplacement d'une station.

Contrairement au modèle de VLAN basé sur le port, des stations appartenant `a des VLAN différents peuvent être connectées au même port d'un commutateur. Une station peut théoriquement être membre de plusieurs VLANs différents.

Le principal inconvénient de ce modèle est la mise à jour des correspondances entre les VLANs et les adresses MAC, qui peut être ardue dans des réseaux de grande taille.

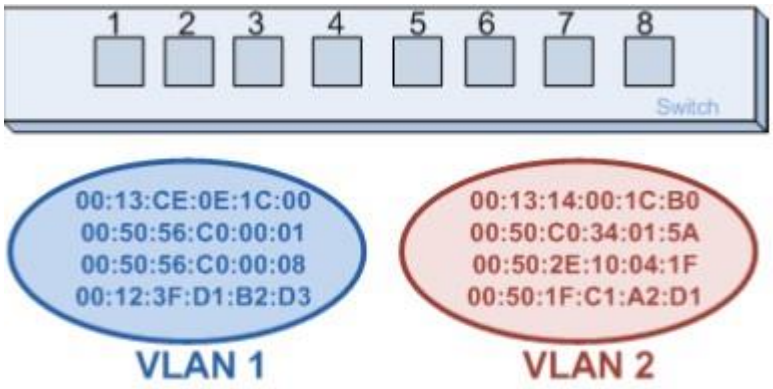


Figure II.5: VLAN par adresse MAC [27]

- **Le VLAN de niveau 3**

On distingue deux types :

* Vlan par sous réseau ou les vlan sont constitué selon les adresse IP.

* Vlan par protocoles ou les vlan sont constitué selon le type de protocole.

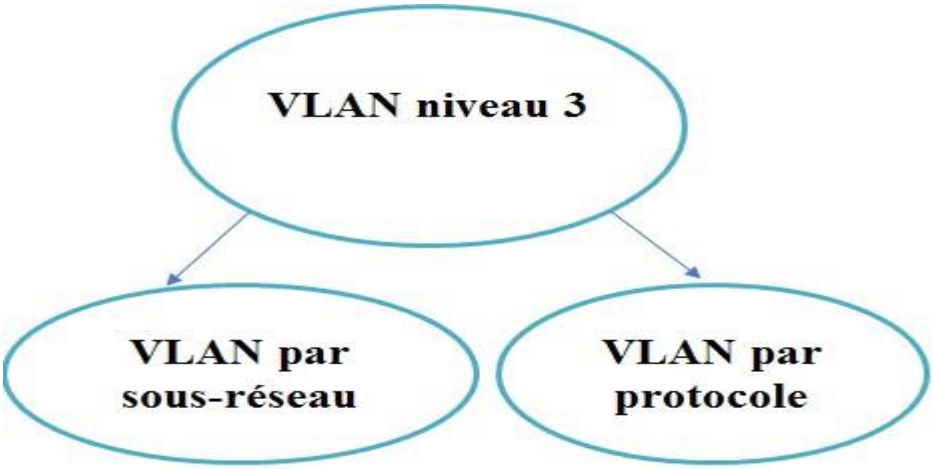


Figure II.6: VLAN de niveau 3

II.4.2 Types des réseaux locaux virtuels [26] :

- **VLAN par défaut**

Au démarrage initial du commutateur, tous les ports du commutateur deviennent membres du VLAN par défaut, ce qui les place tous dans le même domaine de diffusion. Cela permet à tout périphérique réseau connecté à l'un des ports du commutateur de communiquer avec d'autres périphériques sur les autres ports du commutateur.

- **VLAN de données**

VLAN de données qui peuvent également être considérés comme des VLAN utilisateur. Ceci est configuré pour transporter uniquement le trafic généré par l'utilisateur. L'importance de séparer les données utilisateur de tout autre type de VLAN réside dans la gestion et le contrôle des commutateurs appropriés.

- **VLAN natif**

Un port de jonction 802.1Q est attribué au VLAN natif. Les ports de jonction 802.1Q prennent en charge le trafic provenant de plusieurs VLAN ainsi que le trafic ne provenant pas d'un seul VLAN. Les ports de jonction 802.1Q placent le trafic non balisé (trafic qui ne provient pas d'un VLAN) sur le VLAN natif. En résumé, le VLAN natif observe et identifie le trafic de chaque extrémité de la liaison principale.

- **VLAN de gestion**

Un VLAN de gestion est tout VLAN configuré pour accéder aux fonctions de gestion du commutateur. La configuration ddu VLAN de gestion se fait en lui attribuant une adresse IP et un masque de sous-réseau.

- **VLAN voix**

Le VLAN voix est configuré pour transporter le trafic voix. Les réseaux virtuels vocaux sont principalement utilisés pour transporter le trafic réseau de préférence aux autres types. La communication sur le web est incomplète sans téléphone. Plus d'appels sont passés sur le réseau que d'autres formes de messagerie. Les administrateurs réseau envisagent de concevoir un réseau compatible VOIP avec une bande passante garantie pour assurer la qualité de la voix, et la possibilité d'acheminer vers des zones congestionnées sur le réseau avec une latence minimale (150-180 ms).

I.5 Le protocole VTP :

Est un protocole développé par Cisco servant à échanger des informations
VLAN sur des liaisons agrégées, afin de réduire l'administration VLAN et les erreurs de configuration. Il permet de circuler les informations des VLAN sur des différents commutateurs sans avoir besoins de configurer les VLAN sur chaque commutateur. [28]

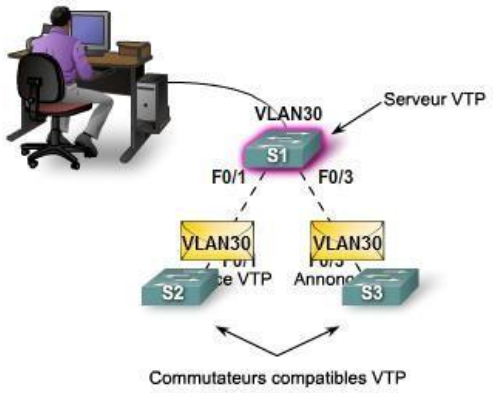


Figure II.7 : ***Principe du VTP***

II.6 La conclusion :

Dans ce chapitre, nous avons présentés les notions de base d'un réseau VPN qui permet donc aux réseaux privés de s'étendre et de de s'étendre et de se connecter les uns aux autres sur internet.

Le chapitre suivant est consacré à la généralité sur la VoIP.

III.1 Introduction

Les Communications Unifiées sont une nouvelle technologie d'entreprise qui intègre la communication interpersonnelle en temps réel (téléphonie, visiophonie) et les outils de travail collaboratif (présence, messagerie instantanée) et bureautique (traitement de texte, agenda, messagerie). La téléphonie IP devient incontournable dans toutes les industries : les entreprises et les fournisseurs d'accès accélèrent la convergence vers les réseaux IP.

TOIP fait référence à tout service de communication qui offre des avantages significatifs en termes de réduction des coûts.

Dans ce chapitre, nous présenterons les concepts de base qui aident à comprendre TOIP, ainsi que les concepts généraux des architectures de réseau nécessaires pour mettre en œuvre un système TOIP.

III.2 La définition et concepts

La téléphonie sur IP correspond à la transmission de la voix et des données sur une seule infrastructure IP. L'objectif donc est d'utiliser un réseau existant IP (intranet, LAN, WAN. etc..) pour effectuer des conversations vocales grâce au protocole IP.

A la différence du réseau RTC qui fonctionne par transmission des signaux sur un réseau de commutation de circuit, la téléphonie sur IP utilise la commutation de paquets.

Ainsi le signal numérique obtenu par numérisation de la voix est découpé en paquets qui sont véhiculés sur le réseau IP jusqu'à sa destination, ou une application se chargera de la transformation inverse (paquets vers voix). Au lieu de disposer à la fois d'un réseau téléphonique commuté (RTC) et d'un réseau informatique, l'entreprise peut donc tout fusionner sur un même réseau. [12]

III.3 Le réseau téléphonique commuté

III.3.1 RTC

Le réseau téléphonique public commuté RTC est un moyen de communication pratique pour de petites applications interactives, comme la téléphonie. Il utilise des commutateurs pour assurer l'interconnexion des abonnées. Le mode transport utilisé est la commutation de circuits. **[10]**

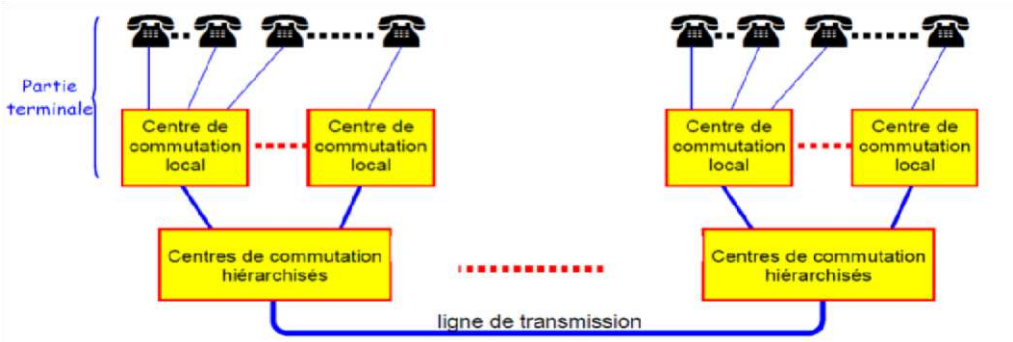


Figure III.1: Le réseau téléphonique commuté (RTC)

Le RTC est composé de nœuds (commutateurs) s'échangeant des informations au moyen de protocoles de communications normalisés par les instances internationales.

Les systèmes réalisant le RTC sont hétérogènes, ils proviennent de fabricants différents et utilisent des technologies différentes. **[11]**

III.4 PABX ET IPBX

- **PABX :** C'est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur et le réseau RTC.

- **IPBX :** C'est lui qui assure la commutation des appels et leurs autorisations, il peut servir aussi de routeur ou de Switch dans certains modèles, ainsi que de serveur

- DHCP. Il peut posséder des interfaces de type analogiques (fax), numériques (postes), numériques (RNIS) ou opérateurs (RTC ou RNIS). Il peut être gérer par IP en intranet ou par un logiciel serveur spécialisé que ce soit en interne ou depuis l'extérieur.
- Il peut s'interconnecter avec d'autres PABX-IP ou PABX non IP de la même marque (réseau homogène) ou d'autres PABX d'autres marques (réseau hétérogène) [2].

III.5 principe de fonctionnement de la TOIP

Le déroulement d'une communication téléphonique sur IP parcourt les cinq grandes étapes suivantes : [13]

a) **Mise en place de la communication**

Une signalisation démarre la session. Le premier élément à considérer est la localisation du récepteur *(User Location).*

Elle s'effectue par une conversion de l'adresse du destinataire (adresse IP ou adresse téléphonique classique) en une adresse IP d'une machine qui puisse joindre le destinataire (qui peut être le destinataire lui-même). Le récepteur peut être un combiné téléphonique classique sur un réseau d'opérateur télécoms

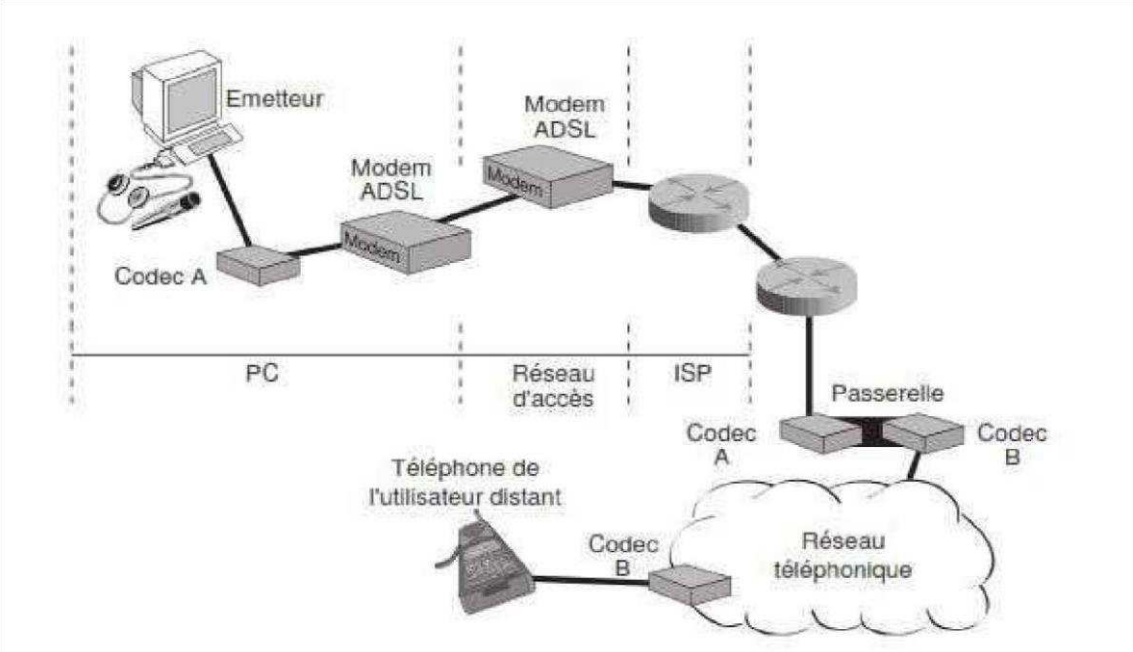


Figure III.2 : Équipement à traverser par une communication téléphonique sur IP.

b) **Établissement de la communication**Cela passe par une acceptation du terminal destinataire, que ce dernier soit un téléphone, une boîte vocale ou un serveur Web. Plusieurs protocoles de signalisation sont utilisés pour cela, en particulier le protocole
SIP (Session Initiation Protocol) de l'IETF. Comme son nom l'indique, SIP est utilisé pour initialiser la session.

c)Transport de l'information téléphonique Le protocole RTP (Real-time Transport Protocol) prend le relais pour transporter l'information téléphonique proprement dite. Son rôle est d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie. C'est un protocole de niveau transport, qui essaye de corriger les défauts apportés par le réseau.

d)Changement de réseau Un autre lieu de transit important de la ToIP est constitué par les passerelles, qui permettent de passer d'un réseau à transfert de paquets à un réseau à commutation de circuits, en prenant en charge les problèmes d'adressage, de signalisation et de transcodage que cela pose.

e) Arrivée au destinataire

De nouveau, le protocole SIP envoie une requête à la passerelle pour déterminer si elle est capable de réaliser la liaison circuit de façon à atteindre le destinataire. En théorie, chaque passerelle peut appeler n'importe quel numéro de téléphone. Cependant, pour réduire les coûts, il faut choisir une passerelle locale, qui garantit que la partie du transport sur le réseau téléphonique.

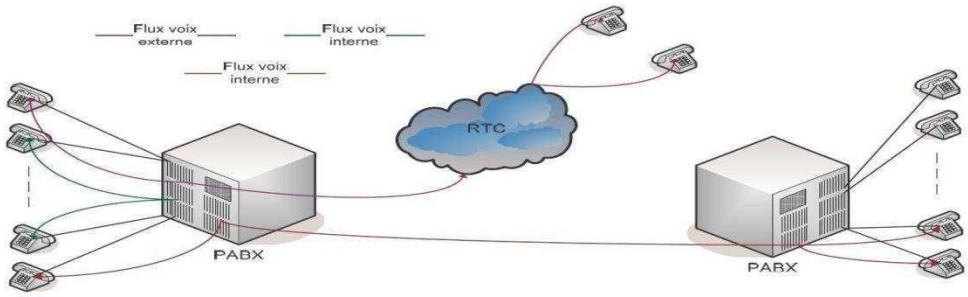
III.6 les architectures de la TOIP [14]

La téléphonie sur IP peut être déployée en entreprise de plusieurs manières, il reflète le degré de convergence entre réseaux. Il existe ainsi trois architectures de mise en œuvre de la téléphonie sur IP en entreprise :

III.6.1. Architecture de la téléphonie classique d'entreprise

Cette architecture consiste à acheminer les fonctions de téléphonie vers un service IP qui est fourni par un opérateur ou autres fournisseurs de solution de VOIP, et qui gère le service de bout en bout. L'ensemble des flux voix et signalisation est centralisé au niveau du PABX de chaque site.

Les architectures de téléphonie sur IP sont conçues, de manière à d'envisager les évolutions qui conduisent vers 'une migration de service full-IP.



FiigureIII.3 : architecture de la téléphonie classique d'entreprise

III.6.2 architecteur de la VOIP (architecteur hybride)

Cette architecture consiste à retenir une architecture hybride (circuit/voix sur IP). Cette solution présente comme avantage de ne pas remettre en cause l'infrastructure existante tout en bénéficiant des avantages du transport de la voix sur IP pour les communications inter- sites.

La mise en œuvre de cette solution peut se faire soit par I 'ajout d'un boitier « Voice Gateway » externe au PABX, soit par un recours aux fonctionnalités de Gateway intégrées aux routeurs de nouvelle génération (sous forme de carte).

III.6.3. L'architecteur de la voip (architecture full-IP)

L'architecture full-IP présente une migration totale vers la téléphonie sur IP, incluant les terminaux téléphoniques utilisateurs. Cette migration s'accompagne de nombreux avantages tels que la convergence entre le système informatique et la téléphonie de l'entreprise.

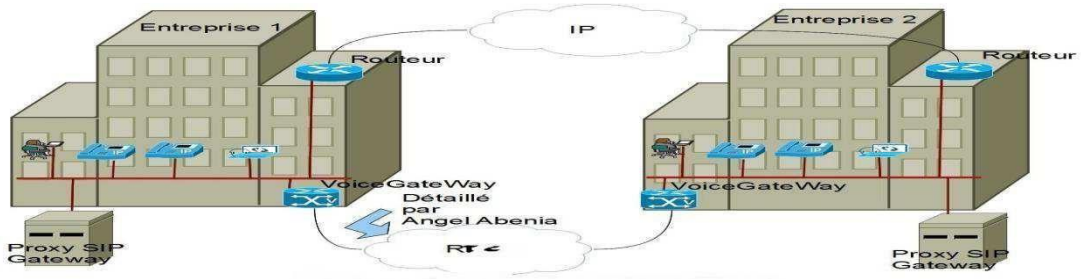


Figure III.4: Architecture VoIP d'entreprise « architecture Full-IP »

La Voice Gateway sera la passerelle d'accès vers le RTC, et lors d'une communication inter ou intra-site. Seuls les flux de signalisation transitent par le Gatekeeper.

Ceci est illustré dans le schéma suivant :

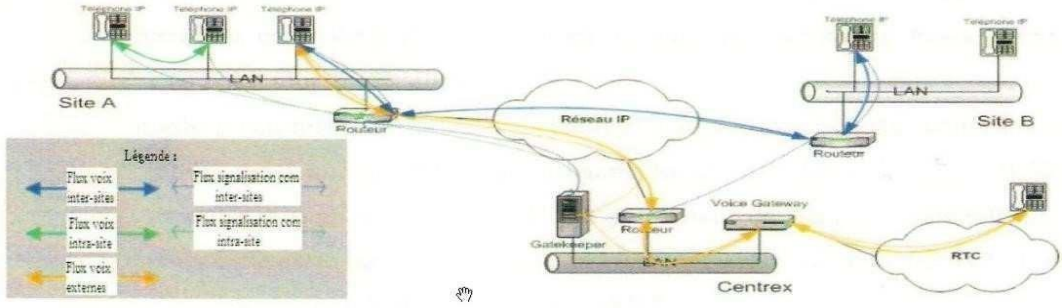


Figure III.5 : Architecture VoIP « architecture type centrex ».

III.7 les composants d'un réseau VOIP

Serveur de communication : Serveur de communication : principalement utilisé pour contrôler la connexion et les échanges avec le monde extérieur.

(Exemple : CISCO Call Manager), qui gère diverses signalisations réseau et autorisation d'appel entre terminaux IP ou soft phone. Il peut avoir une interface réseau opérateur (PSTN ou ISDN), sinon les appels externes passeront par une passerelle dédiée (passerelle).

figureIII.6 serveur de communication

La passerelle (Gateway) : C'est un élément de routage équipé de cartes d'interface analogiques et/ou numériques pour l'interconnexion avec d'autres PABX (en QSIG, ISDN ou E&M) ou avec des opérateurs de télécommunications locaux, nationaux ou internationaux.

figureIII.7 : la passerelle

Getkeeper: est l'élément qui fournit l'intelligence à la passerelle. Getkeeper est le compagnon logiciel de la passerelle qui effectue la traduction des adresses (identifiants H323 et @IP pour les références des endpoints) pour gérer la bande passante et les droits d'accès.

MCU : est un composant optionnel utilisé pour gérer les conférences audio et vidéo.

Routeur : est un dispositif de mise en réseau informatique qui consiste notamment à diriger des données à travers un réseau, il assure le routage des paquets d'un réseau à l'autre.

figureIII.8 : routeur

Le switch : est un commutateur réseau qui permet de connecter plusieurs segments de réseau d'un réseau informatique entre eux. Il garantit ainsi la distribution et la communication de dizaines d'Ethernets à 10/100 voire 1000Mbit/s.

figureIII.9 : le switch

Soft phone : C'est un logiciel qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC. [2].

figureIII.10 : Soft phone

III.8 Les protocoles de signalisation

III.8.1Le protocole H323 :

H.323 est un protocole de communication englobant un ensemble de normes utilisées pour l'envoi de données audio et vidéo sur internet.

Briques d'architecture H.323

L'infrastructure H.323 repose sur des éléments réseaux suivants :

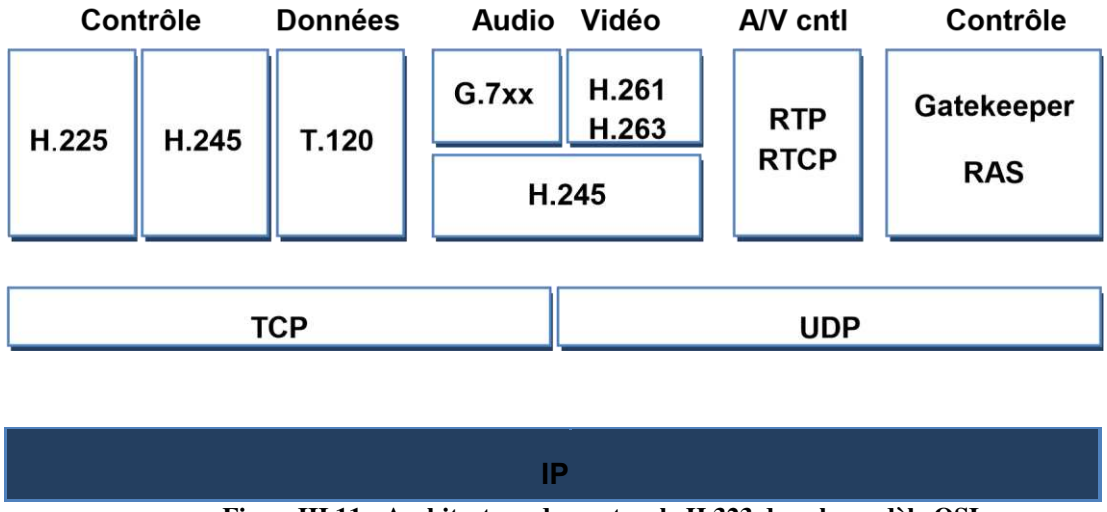
- Les portiers (gk : Gatekeeper)
- Les passerelles (gw : Gateway)
- Les terminaux : Dans un contexte de téléphonie sur IP, deux types de terminaux H.323 sont aujourd'hui disponibles :

*Un poste téléphonique IP raccordés directement au réseau Ethernet de l'entreprise.

*Un PC multimédia sur lequel est installée une application compatible H.323. [3]

Pile protocolaire H.323

Plus qu'un protocole, H.323 ressemble d'avantage à une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories : **la signalisation**, **la négociation de codecs** et **le transport de l'information**. Son architecture est illustrée par la ***figure 6[19]***



FigureIII.11 : Architecture du protocole H.323 dans le modèle OSI.

Le respect du standard H.323 permet de garantir un contrôle sur l'utilisation des ressources réseaux et des contraintes de qualité de service. Tous les terminaux H.323 doivent supporter :

- Le protocole H.245, pour négocier l'ouverture et l'utilisation des canaux ainsi que les paramètres de la communication.
- Le protocole H.225 (SIG) pour la signalisation et l'établissement d'appels.
- Le protocole H.225 (RAS) (Registration/Admission/Status), est le protocole utilisé par le terminal pour communiquer avec le serveur de contrôle d'appels.
- Les protocoles RTP/RTCP (Real Time Protocol/Real Time Control Protocol) pour les flux audio et vidéo.
- Le T.120 pour l'ouverture d'un canal pour le partage d'applications.

III.8.2Le protocole SIP :

La description générale du protocole SIP :

Session initiation Protocol (dont le sigle est SIP) est un Protocole de signalisation appartenant à la couche application du modèle OSI, normalisé et standardisé par l'IETF (internet Engineering Task Force) en 1999. Il a été conçu principalement pour établir, modifier et terminer des sessions multimédia (voix, vidéo, données). Le Protocol SIP permet de supporter de nombreux services tels que la messagerie instantanée, le transfert d'appel, la conférence et les services complémentaires de téléphonie.

Entités du protocole SIP :

Le Protocole SIP dispose des entités qui interagissent entre elles afin de garantir les services SIP, on retrouve particulièrement des entités utilisateurs et des entités réseaux :

***Les entités utilisateurs :** sont appelées des agents utilisateurs (U.A) dont on peut distinguer les UAC (User Agent Client) et UAS (User Agent Server). Le client envoie les requêtes SIP lorsqu'il initialise un appel, l'UAS est une application qui contacte l4utilisateur si un appel lui est destiné.

***Les entités réseaux :** Sont constituées de plusieurs serveurs qui sont :

- **Serveur proxy :** Le serveur Proxy agit comme serveur et client à la fois, c'est-à-dire qu'il peut envoyer et recevoir des requêtes.
- **Serveur d'enregistrement :** Chargé d'enregistrer chaque utilisateur qui rentre dans le réseau SIP, en particulier, il se charge de déterminer l'association client/@IP de chaque UA (User Agent), et permet de garder des traces de localisations des utilisateurs.
- **Serveur redirection :** le rôle de ce serveur est de répondre aux requêtes des UA ou de serveur proxy concernant la localisation de correspondant. Ce serveur se chargera de renvoyer les informations nécessaires au client appelant. Pour qu'il puisse établir une connexion directe avec l'interlocuteur désiré.
- **Serveur de localisation :** les informations recueillies pour le serveur d'enregistrement sont déposées auprès du serveur de localisation.

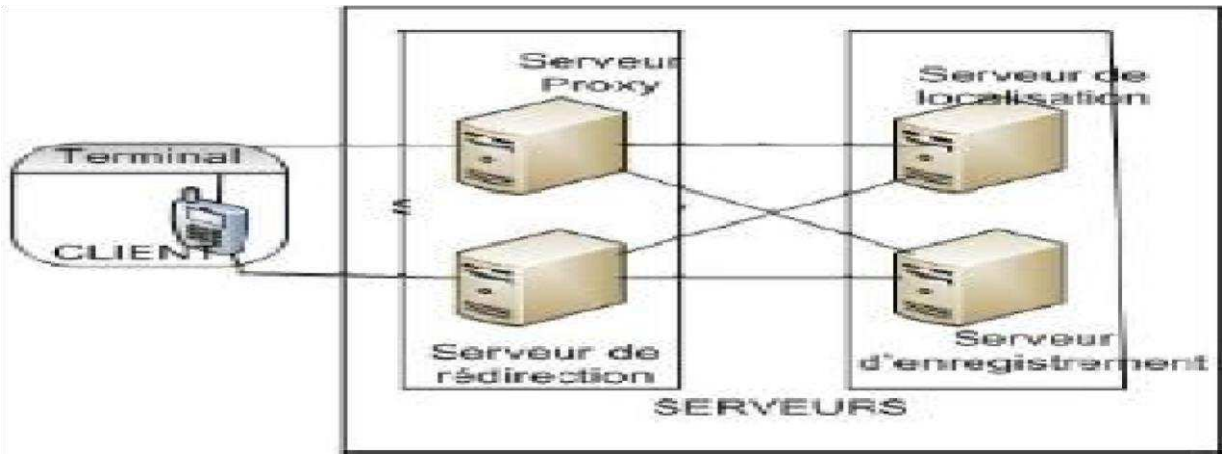


Figure III.12 : architecture de SIP [29]

III.8.3 Le Protocol IAX

- **Définition :**

C'est un protocole de signalisation comme SIP qui utilise un seul port UDP (4569) tant pour le canal de contrôle que pour les flux RTP. La première version (IAX1) utilise le port UDP 5036. [18]

En effet, le protocole SIP, en plus de sa fiabilité, est également célèbre pour sa principale limite qui est la difficulté à l'implémenter derrière un NAT (Network Address Translation).

IAX2 ne rencontre nullement ce problème de NAT d'où son principal succès.

- **Les requêtes IAX :**

Les requêtes IAX fonctionnent exactement comme les requêtes SIP. Les principales requêtes IAX sont : [23]

NEW : c'est une requête qui initie une communication.

REJECT : elle est envoyée pour indiquer qu'une requête **NEW**, **DIAL** ou **ACCEPT** est refusée.

HANGUP : cette requête est envoyée soit par l'émetteur soit par le destinataire pour mettre fin à la communication. Elle est immédiatement suivie d'une réponse **ACK**.

REGREQ : c'est une requête envoyée au serveur pour l'enregistrement. Elle doit obligatoirement contenir le nom de l'utilisateur ***« Username »***.

• **Les réponses IAX**

Il existe plusieurs types de réponses suite à une requête IAX :

ACCEPT : cette réponse est reçue lorsqu'une requête NEW est envoyée. **REGAUTH** : elle est la réponse à une requête REGREQ. Elle est envoyée lorsque l'enregistrement nécessite une authentification

AUTHREQ : elle est envoyée en réponse à une requête NEW. Elle indique que l'authentification nécessaire pour cette communication est acceptée.

ANSWER : Cette réponse est envoyée par le destinataire pour indiquer que la communication est établie.

III.9 Les protocoles de transport de la voix

III.9.1 Le protocole UDP : [20]

Le protocole UDP est un protocole simple, sans connexion, décrit par le document RFC 768.

Il présente l'avantage d'imposer peu de surcharge pour l'acheminement des données. Le protocole UDP est notamment utilisé par des applications de :

- Système de noms de domaine (DNS) ;
- Lecture vidéo en continu ; • Voix sur IP (VoIP).

La figure ci-dessous nous illustre la structure de l'en-tête UDP

Bit (0)	Bit (15)	Bit(16)	Bit (31)
Port source (16)		Port destination (16)	
Longueur (32)		Somme de contrôle (16)	
Données de la couche application (Taille variable)			

Tableau III.1 Structure de l'en -tête UDP

* Définition de différents champs

Champs	Définitions
Port source (16 bits)	Correspond au port relatif à l'application en cour sur la machine de destination
Port destination (16 bits)	correspond au port relatif à l'application en cours sur la machine de destination
Numéro d'ordre (32bits)	Indique le numéro du dernier octet d'un segment
Numéro de reçu (32 bits)	Précise le prochain octet attendu par le destinataire
Longueur (4 bits)	Indique la longueur de l'en-tête du segment en cours
Bits de code (6 bits)	Utilisé dans la gestion de la session et le traitement des segments
Taille de la fenêtre (16 bits)	Il s'agit de la valeur de la fenêtre dynamique c.-à-d. combien d'octets peuvent être envoyés avant d'attendre le reçu
Somme de contrôle (16 bits)	Utilisé pour contrôler les erreurs d'en-tête et de données
Pointeur d'urgence (16 bits)	Uniquement utilisé par un indicateur URG (urgence)
Option	informations facultatives

Tableau III.2 : Définition des champs TCP/UDP

III.9.2 le protocole RTP [14]

Il permet de reconstituer les flux IP multimédias en temps réel. Il se situe au niveau de la couche d'application, il utilise les protocoles se sous-jacents de transport TCP ou UDP.il permet à l'émetteur de moduler son débit de sortie en fonction des ressources disponibles.

III.9.3 Le protocole RTCP [14] :

Le RTCPest un protocole de contrôle utilisé conjointement avec RTP pour contrôler les flux de données et la gestion de la bande passante. Il permet de contrôler le flux RTP, et de véhiculer périodiquement des informations de bout en bout pour renseigner sur la qualité de service de la session de chaque participant à la session.

III.10 Qualité de Service dans la téléphonie sur IP

III.10.1 Définition QoS :

La qualité de service (QoS) est le terme utilisé pour représenter l'ensemble des
Contraintes imposées par un usager (humain ou logiciel) sur la performance d'une application Lors de son exécution. **[15]**

III.10.2 Les problèmes liés au protocole IP

En comparant le réseau IP et le réseau X25, nous avons pu mettre en évidence que la transmission pour le réseau IP n'était pas fiable. De sa propre technologie, nous savons Également que les paquets IP arrivent à destination dans un ordre pouvant être différent de celui De l'émission, donc avec des durées de transmissions variables, à charge pour l'équipement D'arrivée de reconstituer le signal numérique.

Tous ces problèmes inhérents au protocole IP correspondent aux principales causes des Difficultés et des limites à la téléphonie sur IP.

Délai : temps de transmission d'un paquet (doit rester inférieur à 400ms pour respecter Les contraintes d'une conversation interactive)

Gigue : variation de délai (nécessite un buffer de resynchronisation en bout de chemin)

Perte : disparition de paquets au cours de la communication (fait partie de la transmission

IP mais doit être soit réduite, soit inhibée) **Echo**

Bande Passante réduite

Délai de transmission d'un paquet

Le délai de transmission d'un paquet est très important pour bénéficier d'un véritable mode conversationnel et minimiser la perception d'écho. Afin d'avoir une conversation full duplex de bonnes qualités. le délai de transmission ne doit pas dépasser 150ms. Jusqu'à 400ms (limite supérieure). le délai provient de nombreux facteurs. Il y a le délai lié à l'émetteur, celui lié au réseau et bien sûr celui lié au récepteur. **[15]**

Au niveau de l'émetteur, les délais proviennent :

La numérisation et le codage du signal initialement analogique.

La compression du signal comprenant le délai de trame (la compression porte sur une certaine longueur de données.

La mise en paquets (intervalle de temps pendant lequel l'application constitue le paquet : création de l'en-tête, remplissage des données)

La transmission (liaison par un modem ou par un accès direct sur un LAN ou un WAN). **[15]**

Au niveau du réseau, les délais proviennent :

Propagation sur un réseau filaire (la vitesse de propagation est 200000km/s)

Le nombre de routeurs traversés : le temps de traversée d'un routeur étant lui-même fonction de la charge de ce dernier qui fonctionne par file d'attente.

Au niveau du récepteur, ce sont les opérations inverses qu'au niveau de l'émetteur. Le délai provient donc de la réception des paquets.

Perte

Lorsque les routeurs IP sont congestionnés, ils libèrent automatiquement de la bande Passante en se débarrassant d'une certaine proportion des paquets entrant en fonction des seuils prédéfinis.

La destruction par un routeur congestionné n'est pas la seule cause de la perte de paquet : celleci peut en effet provenir de l'épuisement de la durée de vie du paquet IP (TLL=0), du retard à la réception supérieure au buffer de gigue ou à une invalidité du paquet due à des défauts de transmission. **[15]**

La gigue

La gigue correspond à une variation du délai de transmission de l'information. Elle est due au mode de mise en paquets par les codeurs, à l'encapsulation des paquets IP dans des protocoles support tels que le Frame Relay ou l'ATM, et à la variation de routes dans le réseau. **[15]**

L'écho

Les passerelles doivent également traiter l'écho électrique généré localement par le passage 2 fils vers 4 fils (rupture d'impédance) afin de ne pas perturber le terminal distant.

Bande Passante

Sans compression, la voix nécessite 64Kbps de bande passante, avec compression, on peut descendre jusqu'à 5Kbps. Dans ce dernier cas, la qualité du son est moins bonne et le temps de traitement pour la compression et la décompression au départ et à l'arrivée augmente. **[15]**

III.11 les avantages et les inconvénients

Les inconvénients :

Les principaux inconvénients de la téléphonie IP sont les suivants :

-qualité de sonore.

-technologie émergente et constante évolution des normes

-dépendance de l'infrastructure technologique -supports administratif exigeant.

Les avantages : [16]

Les avantages de cette intégration sont, bien sûr, la baisse des frais de communication, mais aussi la simplification de la maintenance de leurs réseaux, qui passent de deux (téléphonie et données) à un seul (données). De façon plus détaillée nous aurons comme avantages :

- **La convergence** : Quel que soit le type de données véhiculées, le réseau est unique : les flux de voix, de vidéo, de textes et d'applicatifs transitent sur le même réseau d'entreprise, la productivité est améliorée. Pour les administrateurs, un seul réseau est à administrer, ce qui simplifie grandement la gestion**.**

- **Le coût de transport** : Grâce à l'intégration de la téléphonie parmi de nombreuses autres applications, le coût du transport devient pratiquement nul.

- **Les services** : La ToIP offre plus de services que la téléphonie classique car certains services sont propres aux réseaux IP**.**

- **L'optimisation des ressources** : la ToIP utilise moins de canaux que la téléphonie classique. Ceci entraine donc une optimisation de la bande passante.

- **La simplification des infrastructures :** les autocommutateurs classiques sont remplacés par des autocommutateurs logiciels (IPBX) plus performants et plus facile à gérer.

III.12 La sécurité de la téléphonie sur IP

III.12.1 la TOIP et la sécurité des appels :

La téléphonie sur IP, malgré ses très nombreux avantages, notamment financiers, comporte des risques majeurs en termes de sécurité des communications voix.

Un appel téléphonique ToIP se décompose en deux phases : la signalisation qui permet d'établir l'appel, et la phase de transport des flux de médias qui transportent la voix. [17]

- Au cours de la phase de signalisation, les messages SIP codés en mode texte sont transmis de façon non chiffrée dans le réseau, ce qui permet à un pirate d'écouter facilement lesmessages SIP et d'accéder aux informations de transport des flux média.
- Il existe de nombreuses attaques possibles sur le réseau ToIP dont les plus répandues sont :

• Dénis de service (attaque DoS) : l'objectif d'une attaque DoS est de rendre un élémentdu réseau indisponible. Des exemples de ce type d'attaque sont :

* l'envoi illégitime de paquets SIP BYE
* interruption de la communication en cours
* rendre la communication inaudible.

• Ecoute clandestine : L'objectif de cette attaque est d'écouter le trafic de signalisationou de données, en utilisant des outils d'écoute réseau tels que VOMIT

(Voice OverMisconfigured Internet Téléphone), SiVuS (SIP Vulnerability Scanner), et WireShark.Des exemples sur ce type d'attaque sont :

* Ecoute de conversation

*Obtention d'informations sur les propriétés et contenu de la communication.

- Détournement du trafic : l'attaquant redirige à son profit le trafic ToIP. Elle se base sur l'envoi d'un message de redirection indiquant que l'appelé s'est déplacé et donne sa propre adresse comme adresse de renvoie, de cette façon tous les appels destinés l'utilisateur sont transférés à l'attaquant. Exemple :

*Détournement d'appel ;

* Détournement de signalisation.

- Usurpation d'identité : Ce type d'attaque consiste à usurper l'identité de l'expéditeur du message SIP en modifiant l'identité de l'expéditeur d'un message.

III.13 la conclusion :

Dans ce chapitre, nous avons passé en revue les concepts liés à la ToIP, ce qui nous a permis de mieux appréhender la technologie et de mieux la comprendre.

TOIP est une technologie émergente, et compte tenu des avantages qu'elle présente, elle a essayé plusieurs entreprises pour en tirer profit.
Certaines applications de cette technologie pourront être déployées au sein d'entreprises multi sites, ce qui permettra de migrer les communications des réseaux RTC vers les réseaux IP. Dans le chapitre suivant, on va aborder la partie environnement matériel et logiciel de ce travail.

IV.1 Introduction :

Dans ce chapitre nous présentons le groupe SONATRACH et sa hiérarchie, après avoir présenté le réseau de télécommunication, nous décrivons les équipements utilisés.

IV.2 Présentation de l'entreprise :

SONATRACH est une société nationale algérienne dédiée à la recherche, au développement, au transport par canalisation, à la transformation et à la commercialisation des hydrocarbures et de leurs dérivés, créée après l'indépendance le 31 décembre 1963.

Le groupe pétrolier et gazier SONATRACH est une société nationale algérienne d'envergure internationale, dont le nom est la Société Nationale de TRAnsport et de Commercialisation des Hydrocarbures.

Fleuron de l'Algérie indépendante, la SONATRACH a été intimement liée au destin de l'Algérie tout au long de son histoire par son envergure et son champ d'activité. Depuis la nationalisation des hydrocarbures le 24 février 1971, érigée en entreprise nationale prépondérante, elle s'est toujours engagée dans une dialectique fructueuse avec les différents stades de développement économique [21].

IV.3 Organigramme :

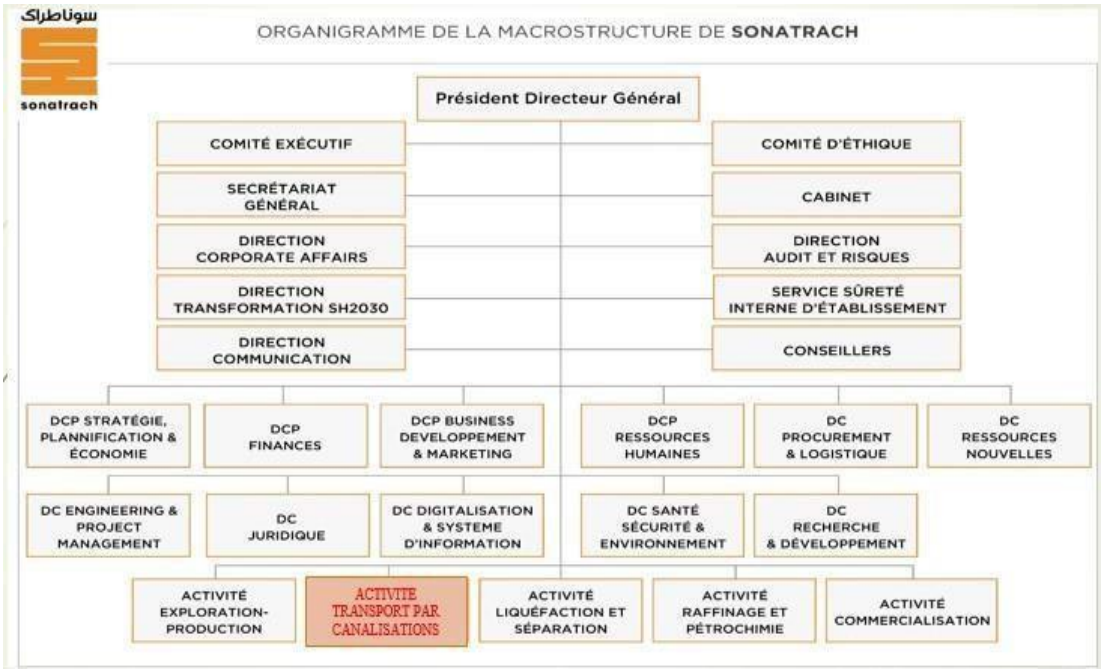


Figure IV.1 : Organigramme de la macrostructure de SONATRACH.

IV.4 Les activités de l'entreprise :

Les activités internationales du Groupe SONATRACH sont les suivantes :

- Exploration et production.
- Transport par canalisation.
- Liquéfaction et séparation.
- Raffinage et pétrochimie
- Commercialisation

Chaque activité développe son industrie, développe son portefeuille d'activités et contribue au développement des activités internationales de l'entreprise dans son domaine d'expertise.

IV.5 Système de Transport par Canalisation (STC) :

Considérée comme l'une des activités les plus importantes de SONATRACH, sa mission est de développer un réseau d'infrastructures de transport par canalisations, de stockage, de chargement et de déchargement à travers les infrastructures portuaires de terminaux et de haute mer.

Il transporte les hydrocarbures des centres de production du sud vers les centres de demande et de traitement du nord

L'activité Transport par Canalisation est regroupée en divisions

- Division Exploitation.
- Division Maintenance.

Depuis la construction du premier pipeline en 1959, le développement du réseau de transport a été porté par la demande toujours croissante de transport, nécessitant ainsi le développement continu de nouvelles capacités de transport.

- Région Transport Centre - Bejaia (RTC),
- Région Transport de Haoud-el- Hamra(HEH),
- Région Transport d'In Amenas (RTI), ➢ Région Transport Est -Skikda (RTE), ➢ Région Transport Ouest Arzew (RTO),

- Gazoduc Espagne/Maroc (GEM), ➢ Gazoduc Tunisie/Italie (GPDF), ➢ Gazoduc Hassi

R'mel (GHR).

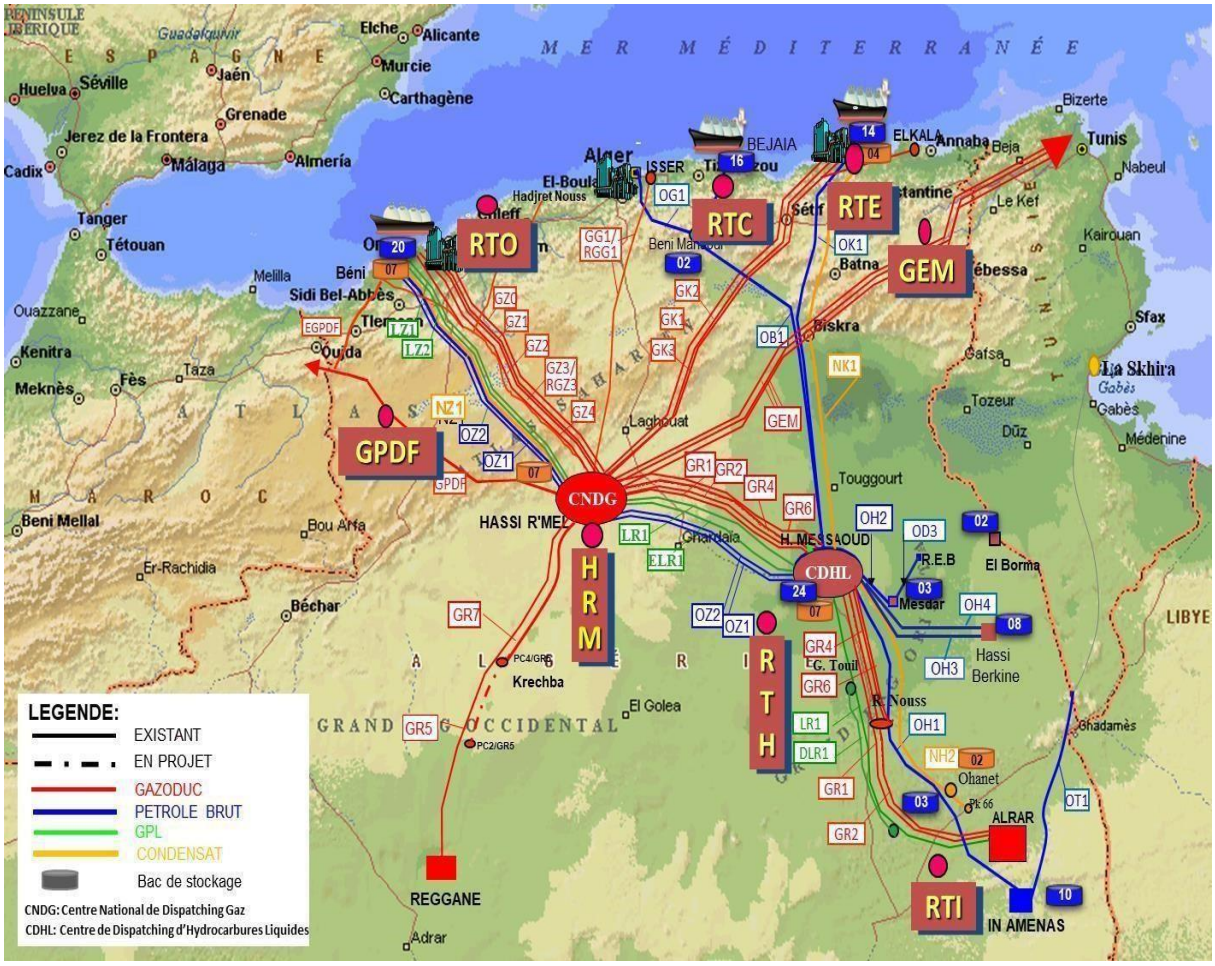


Figure IV.1: Organigramme de la macrostructure de SONATRACH

Cette figure montre **Cartographie actuelle du Réseau de Transport**

IV.6 Présentation de la Région Transport Centre (Bejaia) :

La Région Transport Centre est une région parmi les huit (08) régions composant l'activité de transport par canalisation, Elle est chargée de l'exploitation de deux oléoducs et d'un gazoduc.

C'est une ou plusieurs canalisations transportant des Hydrocarbures des produits pétroliers et de Gaz desservant exclusivement le marché national. [22]

- **L'oléoduc OB1 HEH-TMB :**

  D'une longueur de 668 kilomètres et d'un diamètre de 24 pouces/22 pouces, il transporte le pétrole du centre de stockage de Haoud El Hamra jusqu'au terminal maritime de Béjaïa.

  ✓ **Les Groupes de stations de pompage :**

  - SPA Touggourt / SP1 Bis Djamaa El M'ghair
  - SPB /SP2 El Outaya Biskra ;
  - SPC /SP3 M'sila.
  - Terminal Arrivée Béjaia

- **L'Oléoduc ROB1 SP3-TMB**

  L'opération porte sur 164 kilomètres de canalisation entre la station de pompage SP3 à M'sila et la station d'isolement SP13 à Bejaia Oued-Ghir

  - SP3New M'sila.
  - Terminal Arrivée Béjaïa

- **L'oléoduc DOG1**

  Il mesure 144 kilomètres de long et a un diamètre de 20 pouces pour l'oléoduc H.E.HBejaia et alimente la raffinerie d'Alger à Sidi-Arcine.

  - Beni-Mansour M'sila.
  - Terminal Arrivée Raffinerie d'Alger

- **Le gazoduc GG1 42'' HRM – Bord-Menail**

D'une longueur totale de 437 kilomètres et d'un diamètre de 42 pouces, il alimente en gaz naturel toutes les villes et centres industriels du centre.

- SC3 Moudjebara
- Terminal Arrivée Bordj-Menail
- **Le gazoduc RGG1 42'' Medjdal– Bord-Menail**

  Longue de 210 kilomètres et d'un diamètre de 42 pouces, elle alimente en gaz naturel toutes les villes et centres industriels du centre.

  - TD Medjdel M'sila
  - Terminal Arrivée Bordj-Menail

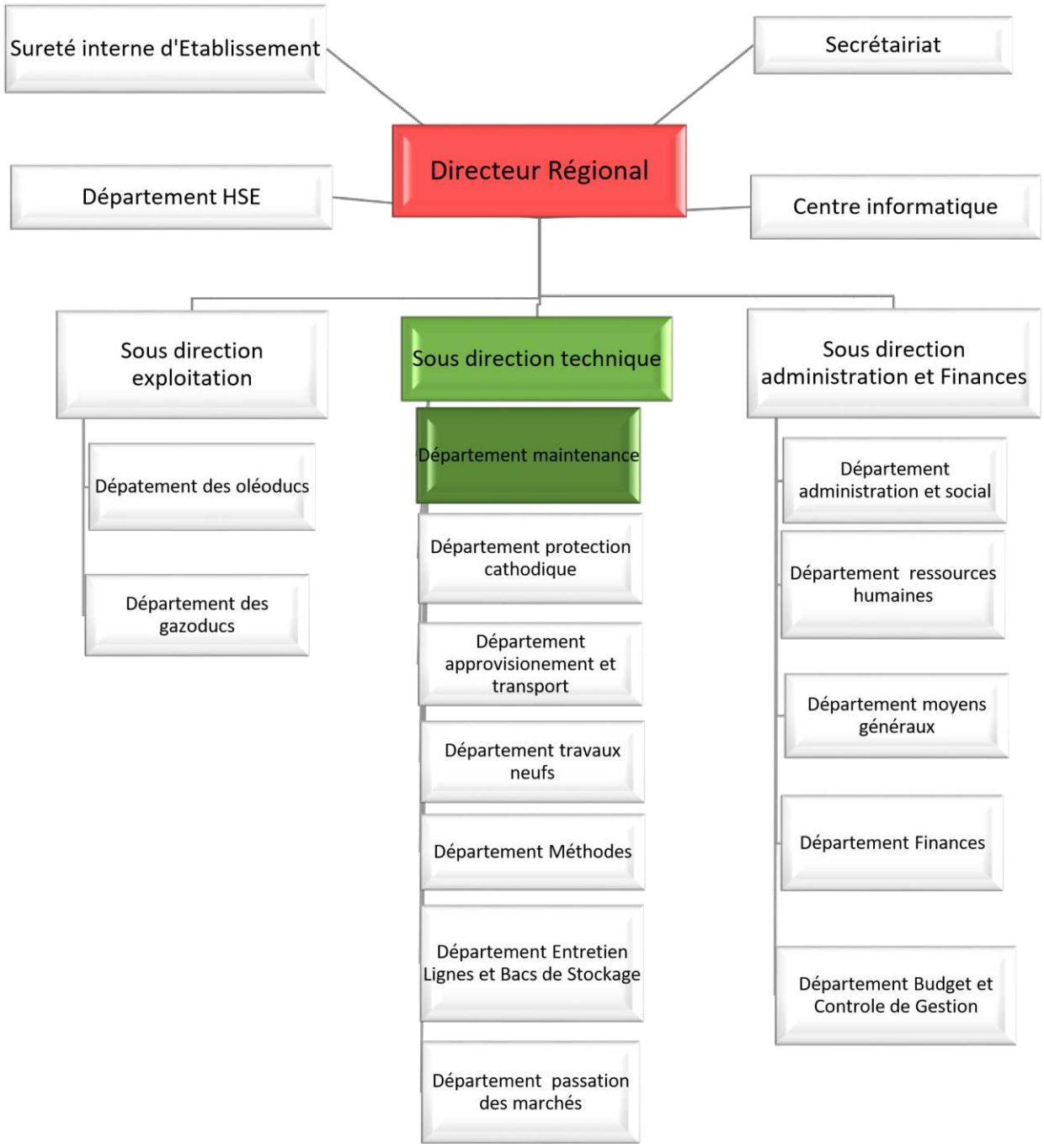
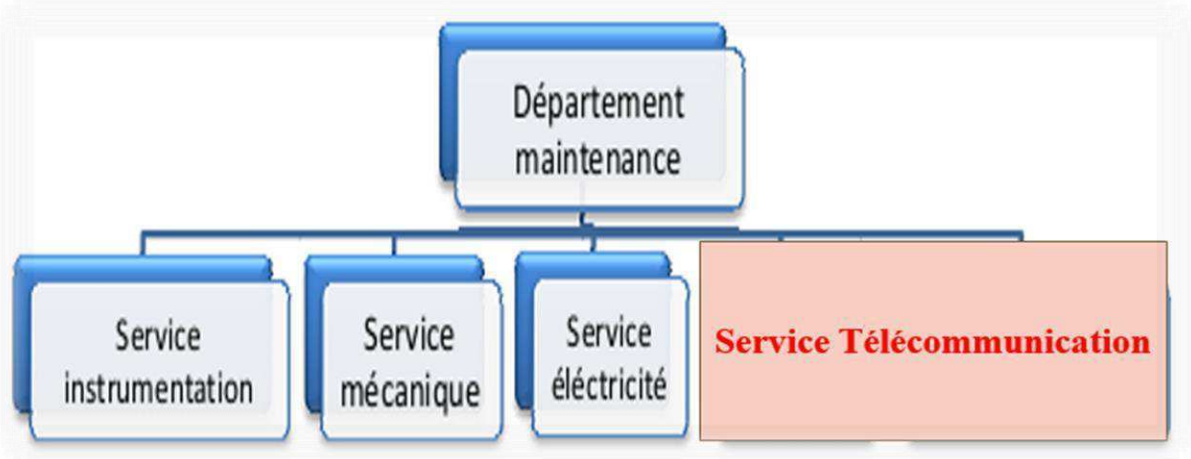


Figure IV.3 Organigramme de la RTC Bejaia

IV.7 Département maintenance

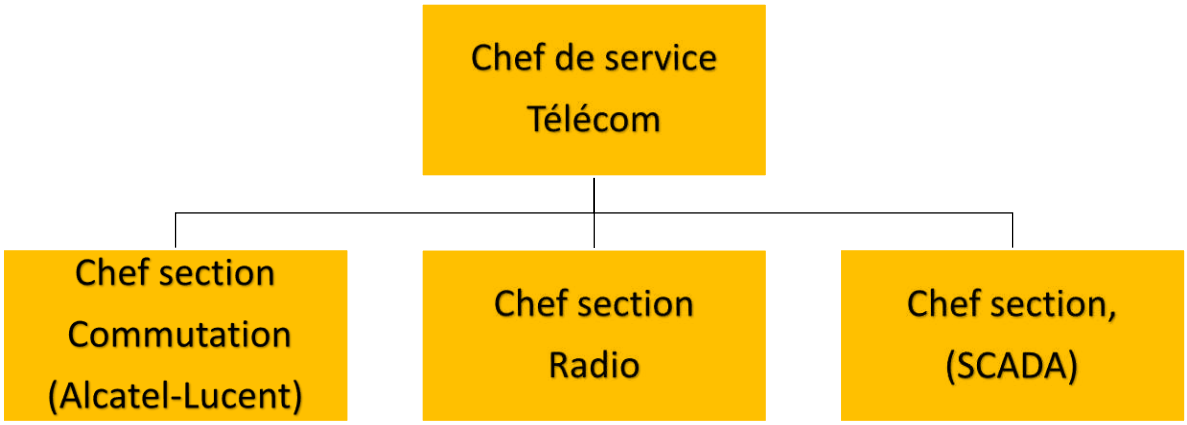
Le service maintenance est une partie très importante de SONATACH. Il regroupe et gère les différents services de l'entreprise. Parce qu'il veille au bon fonctionnement des équipements et installations techniques



FigureIV.4 : Organigramme du département maintenance

IV.7.1 service télécommunications :

Les services de télécommunications sont aujourd'hui des moyens indispensables pour contrôler les mouvements de produits et consolider la gestion au quotidien.



la Figure IV.5 : Les différentes parties des services de télécommunication

IV.7.1.1 Réseau radio :

Les téléphones jouent un rôle important dans une entreprise, c'est pourquoi la radio (sans fil) est un réseau essentiel, en particulier lorsque les lignes téléphoniques sont déconnectées ou difficiles à utiliser.

Elle se compose de :

Un réseau HF

Un réseau radiocommunication VHF

Un réseau radiocommunication UHF

IV.7.1.2 Système de commutation (Alcatel-Lucent)

Le réseau de commutation est constitué de 08 PABX, et les missions assignées à cette section sont :

- Maintenance thérapeutique et préventive de (08) huit PABX installés au siège et dans les gares
- Tester et maintenir diverses liaisons téléphoniques (HEH) liées aux autres entités Élaborer un plan de rénovation du réseau téléphonique.
- Programmation et mise à jour des fichiers de données.
- Maintenance des équipements énergétiques (redresseurs, batteries).
- Suivi de réparation fibre pour OB1 et GG1
- Suivi de la pose des câbles et de la pose de la fibre
- Mise à jour du schéma de câblage du réseau téléphonique.

IV.7.1.3 Système SCADA (supervisory control and data acquisition)

SCADA est un système de télémétrie et de télécommande spécialement utilisé par SONATACH pour répondre aux exigences de la gestion des puits pétroliers, capable de traiter en temps réel un grand nombre de données de mesure et de contrôler à distance les installations pétrolières. Ce dernier peut être exploité pour surmonter les problèmes liés à la production en raison des différentes fonctions offertes par ce système.

IV.8 Présentation des équipements utilisés :

Pour mettre en place notre réseau LAN, nous avons utilisé les équipements résumés dans le tableau ci-dessous :

Périphériques utilisés	Appellation
• Commutateur cœur • Commutateur Accés • CME(call Manager Express) • ISP (Internet Service Provider • Terminal PC • Téléphone IP • Autre devices	• Cisco catalyst 3650 • Cisco catalyst 3560 • Routeur 2811 • Cloud PT • Pc bureau, laptop, Tablet PC-PT • IP Phone 7960 • Serveur, imprimante, AcessPoint

Tableau IV.1 : liste des équipements utilisés

IV.9 Conclusion :

Ce chapitre porte sur l'organisme d'accueil SONATRACH, ainsi la structure de RTC, nous basons sur le service de télécommunication nous étudions les différentes tâches de ce service, les différents équipements utilisés.

V.1 Introduction

On va entamer dans ce chapitre la partie réalisation qui constitue le dernier volet de ce rapport et qui a pour objectif d'exposer le travail réalisé. Pour ce faire, on va commencer tout d'abord par préciser l'environnement matériel et logiciel de ce travail. Ensuite, on va présenter le travail accompli tout au long de ce projet.

V.2 Environnement de travail

L'environnement du travail désigne l'ensemble des moyens matériels et logiciels qui constituent les éléments de base de ce travail.

V.2.1 Logiciel de simulation

Le choix du logiciel est crucial, afin de bien réaliser notre architecture réseau, nous avons opté pour le logiciel GNS3. Ce dernier est un émulateur de périphérique Cisco.il permet une représentation réelle du hardware. Il est utilisé par les ingénieurs réseaux du monde entier pour simuler, configurer, tester et dépanner des réseaux virtuels et réels car il permet de connecter des hyper viseurs à partir de Vmware ou virtualbox. En outre, il permet de construire des réseaux simples et complexes et de les simuler virtuellement. C'est un logiciel gratuit qui fonctionne sur plusieurs plates-formes, telles que Windows, Linux et MacOs.

Figure V.1 : Logo GNS3

VMware : Une machine virtuelle (VM) est un environnement entièrement virtualisé qui s'exécute sur une machine physique. Il exécute son propre système d'exploitation (OS) et bénéficie des mêmes équipements qu'une machine physique à savoir : CPU, mémoire RAM, disque dur et carte réseau. Plusieurs machines virtuelles des systèmes d'exploitation différents peuvent coexister sur un même serveur physique comme : Linux, MacOS, Windows...

Figure V.2 : logo VMware Workstation

V.2.2 Matériel et logiciel (hardware & software) :

V.2.2.1 software :

- **Windows 10**

Windows 10 est un système d'exploitation publié par Microsoft le 29 juillet 2015. Il est hérité de Windows 7 et Windows 8.1. Cette nouvelle version introduit plusieurs changements importants. Premièrement, c'est le premier à fonctionner sur toutes les plateformes existantes : ordinateurs de bureau et portables, Smartphones, tablettes et montres connectées. L'interface de l'OS s'adapte automatiquement au format et au mode de saisie, et Microsoft a déclaré que Windows 10 marquait la fin des mises à jour majeures distribuées sur des supports physiques. Windows évolue désormais en tant que service dans un package distribuer gratuitement sur Internet.

Figure V.3 : logo Windows 10

- **Serveur Windows 2022**

Windows Server 2022 est le système d'exploitation orienté serveur de Microsoft basé sur l'architecture Windows NT qui connecte les environnements sur site avec Azure. Il ajoute de nouvelles couches de sécurité.

FigureV.4 : logo Windows Server 2022

V.2.2.2 hardwares :

- **Pfsense**

Pfsense est un pare-feu avec état open source qui peut être configuré à l'aide de son interface Web ou de ligne de commande, prenant en charge une variété d'avenirs tels que le routage et le NAT. Il comprend des outils et des services équivalents gratuits généralement trouvés sur les routeurs professionnels propriétaires.

Figure V.5 logo Pfsense

Avantages Pfsense :

- Convient pour une utilisation en tant que pare-feu et routeurs
- Il inclut toutes les fonctionnalités d'un pare-feu commercialement coûteux
- Il fournit des options de pare-feu/routage plus avancées qu'IPCOP
- Il permet l'intégration de nouveaux services tels que l'installation de portails captifs, la mise en place de VPN, DHCP et bien d'autres
- Activation/désactivation simple des modules de filtrage
- Système très robuste basé sur le noyau FreeBSD
- Fonctionnalités réseau avancées

FreePBX :

FreePBX est utilisé pour Gérer et contrôler Asterisk. C'est donc un outil de configuration graphique très convivial du logiciel de téléphonie libre Asterisk.

- **Les équipements utilisés dans notre architecture**

Les sites	Les équipements	Les types	Les images
Site Bejaia	Pare-feu (FW-Bejaia)	Pfsense 2.6.0	Free BSD
	Routeur(R1)	Cisco 7200	IOU UNIX
	Switch (SWD1)	Cisco 2690	IOU UNIX
	Switch (SWA1, SWA2, SWA3)	Cisco 3750 N3	IOU UNIX
	FreePBX (ASTERISK1)	16.0.19	CentOS
	Serveur Windows (Serveur AD)	Serveur 2022	Windows
Site Alger	Pare-feu (FW-Alger)	Pfsense 2.6.0	Free BSD
	Routeur(R2)	Cisco 7200	IOU UNIX
	Switch (SWD2)	Cisco 2690	IOU UNIX
	Switch (SWA4, SWA5, SWA6)	Cisco 3750 N3	IOU UNIX
	FreePBX (ASTERISK2)	16.0.19	CentOS

Tableau V.1 : Les équipements utilisés dans notre architecture

V.3. L'adressage

V.3.1 Le plan d'adressage des VLANs

Nom de vlan	ID	Adresse de sous réseau	Passerelle de sous réseau
Vlan data	10	192.168.10.0/24	192.168.10.1
Vlan Voice	20	192.168.20.0/24	192.168.20.1
Vlan gestion	30	192.168.30.0/24	192.168.30.1
Vlan serveur	40	192.168.40.0/24	192.168.40.1
Vlan native	99	…	…

Tableau V.2 : Le plan d'adressage des VLANs

V.3.2 Le plan d'adressage des équipements :

Les équipements	Interface	Adressage
FW-Bejaia	NAT LAN1	192.168.38.129 172.16.1.2
FW-ALGER	LAN2 NAT	172.16.2.1 192.168.38.131
R1	E0/0 E0/1	Interface configurer pour le routage inter-vlan 172.16.1.2
R2	E0/0 E0/1	172.16.2.2 172.16.0.1

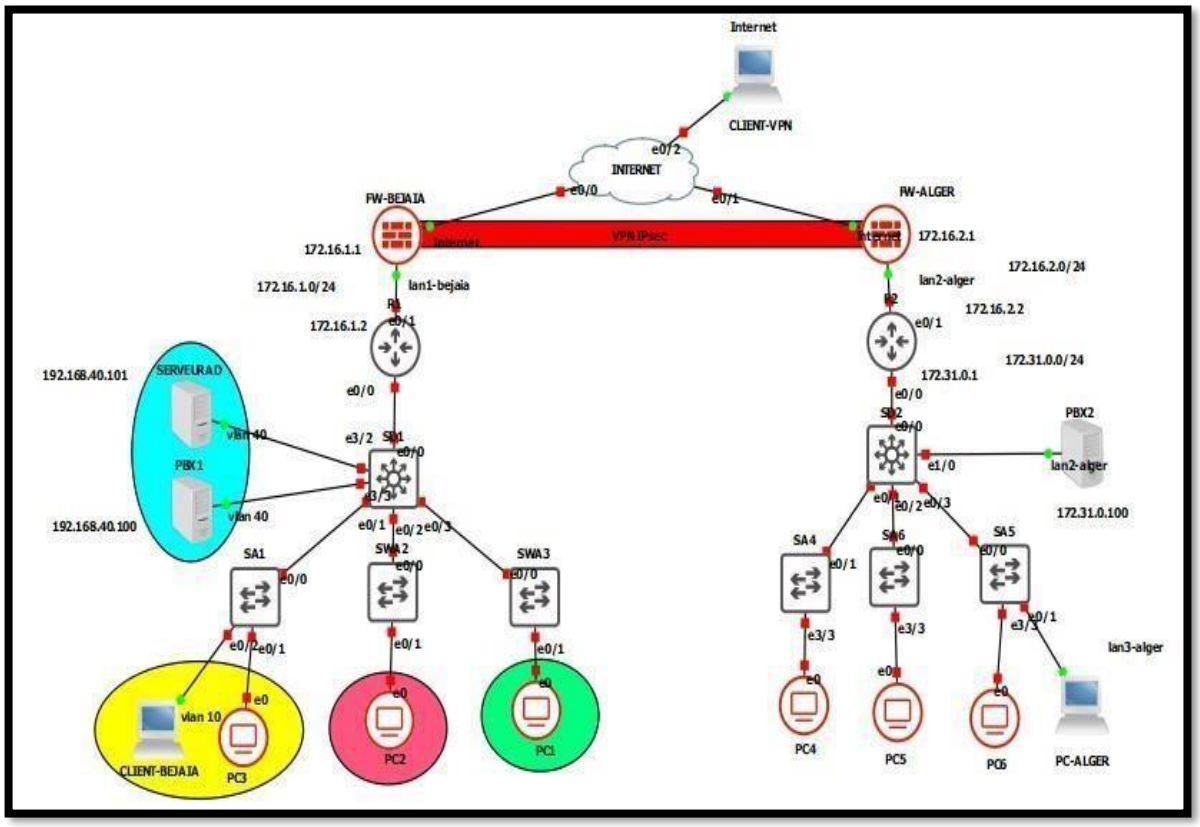
Tableau V.3 Plan d'adressage des équipements

V.3.3 Plan d'adressage des sous interfaces « Routage inter-vlan » routeur Bejaia

Equipement	Sous-Interface	Adresse IP /MASK
Router1(SITE BEJAIA)	Ethernet0/0.10	192.168.10.1/24
	Ethernet0/0.10	192.168.20.1/24
	Ethernet0/0.10	192.168.30.1/24
	Ethernet0/0.10	192.168.40.1/24

TableauV.4 : Plan d'adressage des sous interfaces routeur 1.

V.4 L'architecture proposée :



FigureV.6 : Architecture réseau proposé

Etape 1 : on a implémenté et on a fait connecter notre VPN IPsec

Etape 2 : on a configuré notre client VPN client to site on veut se connecter à distance avec une connexion reliée à l'internet

Etape 3 :la configuration de serveur FreePBX sur le site Bejaïa afin distribuer les numéros locaux

Etape 4 : l'installations de fréeBBX sur le site Alger et la distribution des numéros en local

Etape 5 : l'interconnexion entre les deux sites avec le protocole IAX

Etape 6 : on a routé les appels pour faire la communication vers les deux sites

V.4.1 Le modèle hiérarchique

Le modèle de conception hiérarchique à trois couches, principalement inventé par Cisco, consiste à créer une conception de réseau avec une structure à trois couches, chaque couche ayant un rôle spécifique.

- **La couche cœur :** elle est considérée comme le backbone du réseau, son rôle est de commuter les paquets le plus rapidement possible
- **Couche distribution :** elle fait le lien entre la couche cœur du réseau et la couche accès, elle assure les fonctions du routage et permet la segmentation pour accéder à des départements ou des groupes de travail.
- **Couche accès :** c'est le point d'entrée autorisé dans le réseau, elle permet aux utilisateurs d'accéder aux périphériques du réseau.

V.5 L'installation du Serveur freePBX :

Après avoir ajouté l'image CentOS sur VMware, nous avons créé un serveur :

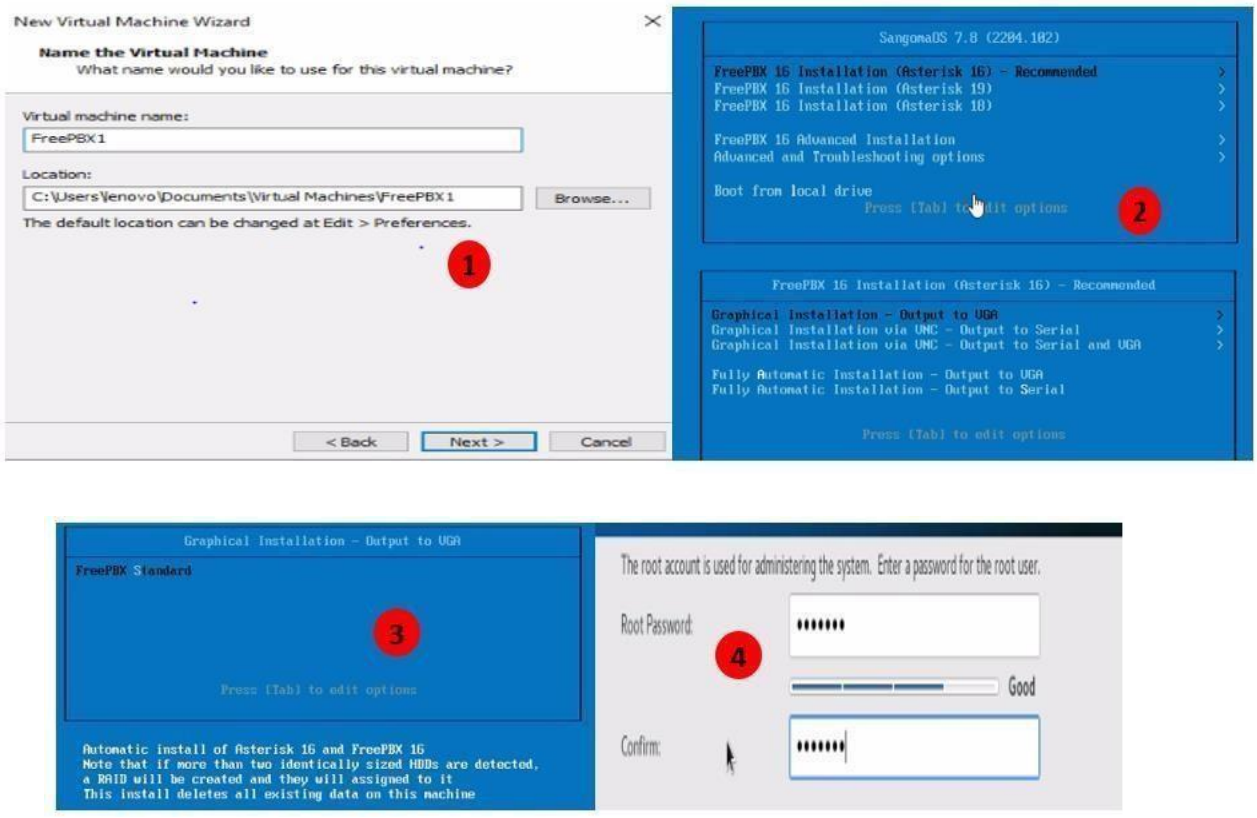


Figure V.7 : Les étapes d'installation FreePBX site 1 « bejaia »

Remarque : pour le FreePBX site 2 « alger » les étapes d'installation sont les mêmes

V.6 Configuration des commutateurs « switchs » :

Nous commençons par la configuration des commutateurs qui permettent l'interconnexion des différents réseaux hétérogène.

V.6.1Configuration et vérification des interfaces truck :

Un trunk est une liaison d'agrégation de VLANs. C'est une connexion physique sur laquelle on transmet le trafic de plusieurs VLANs. Pour configurer les interfaces trunk entre deux switches on suit les étapes suivantes. Vu le nombre de switch à configurer on poursuivra la même procédure.

```
SWD1(config)#interface range ethernet0/1-3
SWD1(config-if-range)#switchport trunk encapsulation dot1q
SWD1(config-if-range)#switchport mode trunk
SWD1(config-if-range)#exit

SWD1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       on               802.1q         trunking      1
Et0/2       on               802.1q         trunking      1
Et0/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094
Et0/2       1-4094
Et0/3       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1
Et0/2       1
Et0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       1
Et0/2       1
Et0/3       1
```

FigureV.8 : Configuration des ports trunk sur le switch distribution SWD1.

```
SWA1#show  interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1
SWA1(config)#interface  ethernet 0/0
SWA1(config-if)#switchport trunk encapsulation dot1q
SWA1(config-if)#switchport mode trunk
SWA1(config-if)#exit
```

Figure V.9 : Configuration et vérification des interfaces au mode trunk sur le switch Access SWA1

V.6.2Configuration et vérification du protocole VTP :

VTP permet d'ajouter, de renommer ou de supprimer un ou plusieurs réseaux locaux Un nœud virtuel sur un seul commutateur qui transmettra cette nouvelle configuration à tous les autres commutateurs du réseau.

Nous avons configuré le serveur VTP sur le commutateur de distribution et le client VTP sur le commutateur client.

```
SWD1(config)#vtp mode server
Device mode already VTP Server for VLANS.
SWD1(config)#vtp domain sonatrach.vtp
Domain name already set to sonatrach.vtp.
SWD1(config)#vtp password cisco
Password already set to cisco
SWD1(config)#vtp version 2
VTP version is already in V2.
SWD1(config)#vtp pruning
Pruning already switched on
SWD1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : sonatrach.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 7-5-22 10:27:37
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 2
MD5 digest                        : 0xC8 0x0E 0x32 0xE5 0x82 0x15 0xA6 0x9D
                                    0x50 0x16 0x25 0x6A 0xB9 0x6E 0x36 0x26
```

Figure V.10 Configuration et vérification VTP serveur sur le switch distribution SWD1

```
SWA1(config)#vtp mode client
Device mode already VTP Client for VLANS.
SWA1(config)#vtp domain sonatrach.vtp
Domain name already set to sonatrach.vtp.
SWA1(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
SWA1(config)#vtp password cisco
Password already set to cisco
```

```
SWA1#show  vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : sonatrach.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0200
Configuration last modified by 0.0.0.0 at 7-5-22 10:27:37

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 2
MD5 digest                        : 0xC8 0x0E 0x32 0xE5 0x82 0x15 0xA6 0x9D
                                    0x50 0x16 0x25 0x6A 0xB9 0x6E 0x36 0x26
```

Figure V.11 : Configuration et vérification VTP client sur le switch access SWA1

V.6.3 Création des VLANs :

Les VLANs sont créés pour regrouper les périphériques d'une part et d'autre part partager les utilisateurs et gérer l'accès et la priorité des utilisateurs individuellement.

Dans notre exemple, nous avons créé cinq VLAN, chaque VLAN est associé à son service.

```
SWD1(config)#vlan 10
SWD1(config-vlan)#name DATA
SWD1(config-vlan)#vlan 20
SWD1(config-vlan)#name voice
SWD1(config-vlan)#vlan 30
SWD1(config-vlan)#name gestion
SWD1(config-vlan)#vlan 40
SWD1(config-vlan)#name serveurs
SWD1(config-vlan)#vlan 99
SWD1(config-vlan)#name native
SWD1(config-vlan)#exit
```

```
SWD1#show  vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et1/0, Et1/1, Et1/2, Et1/3
                                                 Et2/0, Et2/1, Et2/2, Et2/3
                                                 Et3/0, Et3/1, Et3/2, Et3/3
10   DATA                              active
20   voice                             active
30   gestion                           active
40   serveurs                          active
99   native                            active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
SWA1#show  vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/1, Et0/2, Et0/3, Et1/0
                                                 Et1/1, Et1/2, Et1/3, Et2/0
                                                 Et2/1, Et2/2, Et2/3, Et3/0
                                                 Et3/1, Et3/2, Et3/3
10   DATA                              active
20   voice                             active
30   gestion                           active
40   serveurs                          active
99   native                            active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

Vérification de la création des vlan coté serveur

Vérification de la création des vlan coté Clients

Figure V.12 : Création et vérification des VLANs

V.6.4 Affectation des ports mode access au vlan d'accès :

Passons maintenant à la configuration de l'interface Access, ce qui signifie qu'elle ne recevra que les paquets qui lui sont destinés.

La même configuration sera utilisée pour les autres interfaces d'accès.

```
SWA1(config)#interface range  ethernet 0/1-2
SWA1(config-if-range)#switchport mode  access
SWA1(config-if-range)#switchport access vlan 10
SWA1(config-if-range)#switchport voice vlan 20
SWA1(config-if-range)#end
```

```
SWA1#show  vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Et0/3, Et1/0, Et1/1, Et1/2
                                                   Et1/3, Et2/0, Et2/1, Et2/2
                                                   Et2/3, Et3/0, Et3/1, Et3/2
                                                   Et3/3
10   DATA                                active    Et0/1, Et0/2
20   voice                               active    Et0/1, Et0/2
30   gestion                             active
40   serveurs                            active
99   native                              active
1002 fddi-default                        act/unsup
1003 trcrf-default                       act/unsup
1004 fddinet-default                     act/unsup
1005 trbrf-default                       act/unsup
SWA1#
```

Figure V.13 Configuration Access sur le switch Access SWA1

V.6.5 Routage inter-VLANs :

Nous allons configurer l'une des interfaces réseaux du routeur, le principe est toujours le même pour chacune des interfaces réseaux. Pour chaque sous interface on l'encapsule avec le protocole 802.1q

```
R1(config)#interface  ethernet 0/0
R1(config-if)#no shutdown
R1(config-if)#interface  ethernet 0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#ip helper-address 192.168.10.100
R1(config-subif)#interface  ethernet 0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#ip helper-address 192.168.10.100
R1(config-subif)#interface  ethernet 0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#ip helper-address 192.168.10.100
R1(config-subif)#interface  ethernet 0/0.40
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#ip helper-address 192.168.10.100
R1(config-subif)#exit
```

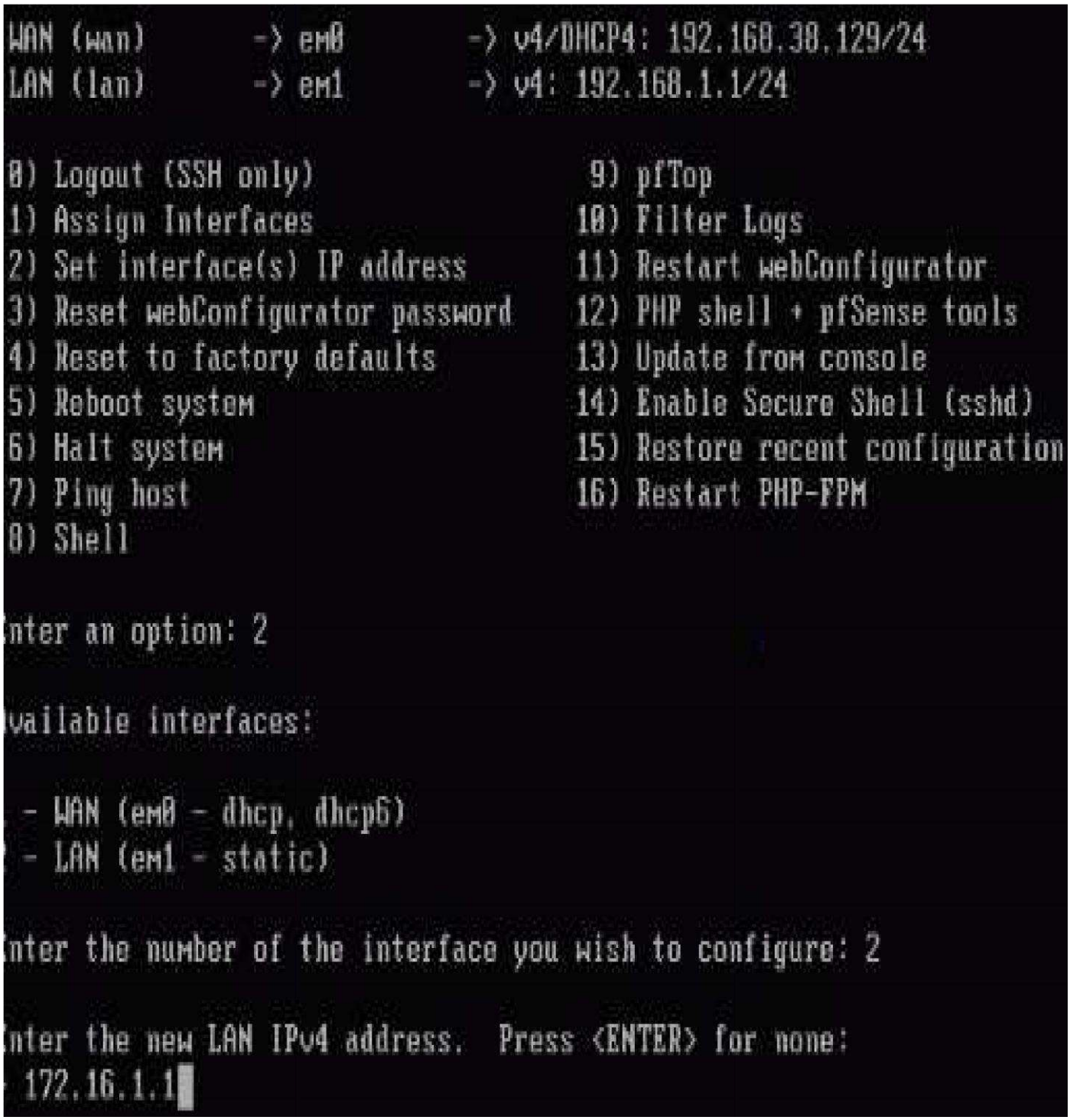
DHCP RELAIS

Figure V.14 Configuration des sous-interfaces « routage inter-vlan » et DHCP relais

V.6.6 Configuration firewall :

- **Les interfaces LAN et WAN :**

On a seulement configuré l'interface LAN, l'interface WAN a été configurée automatiquement à



l'aide du serveur DHCP comme suit :

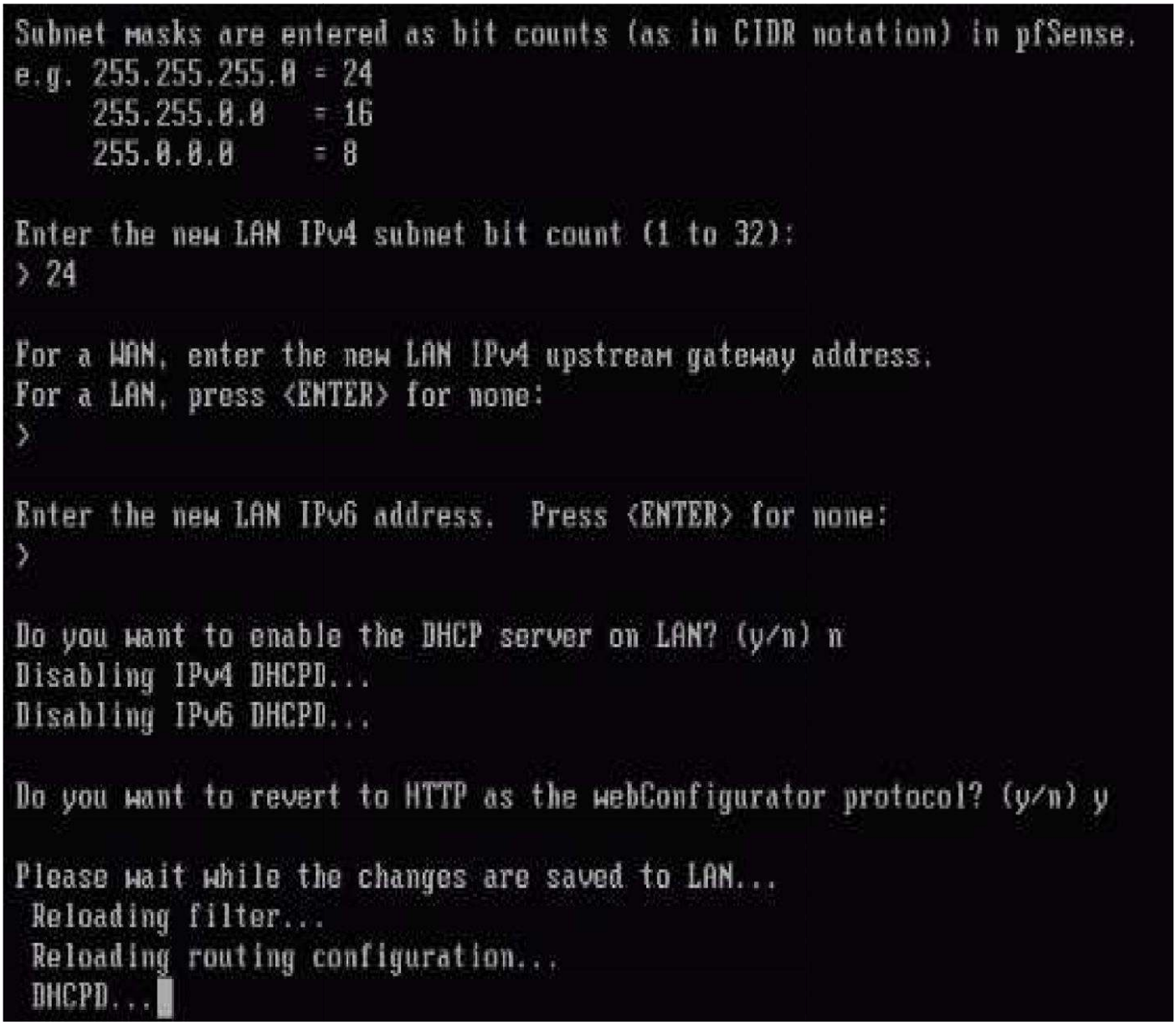


Figure V.15 : les interfaces de pare-feu Bejaia

Remarque : les étapes sont identiques pour le pare-feu Alger

*l'interface WAN :192.168.38.131/24

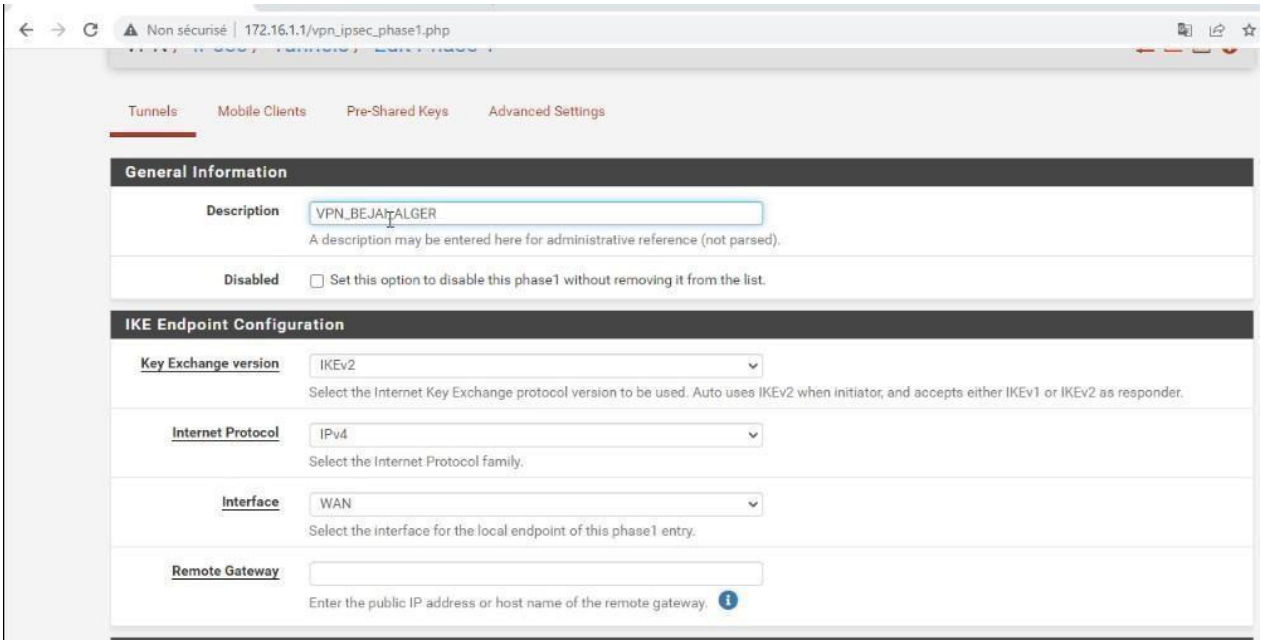
*l'interface LAN :172.16.2.1/24

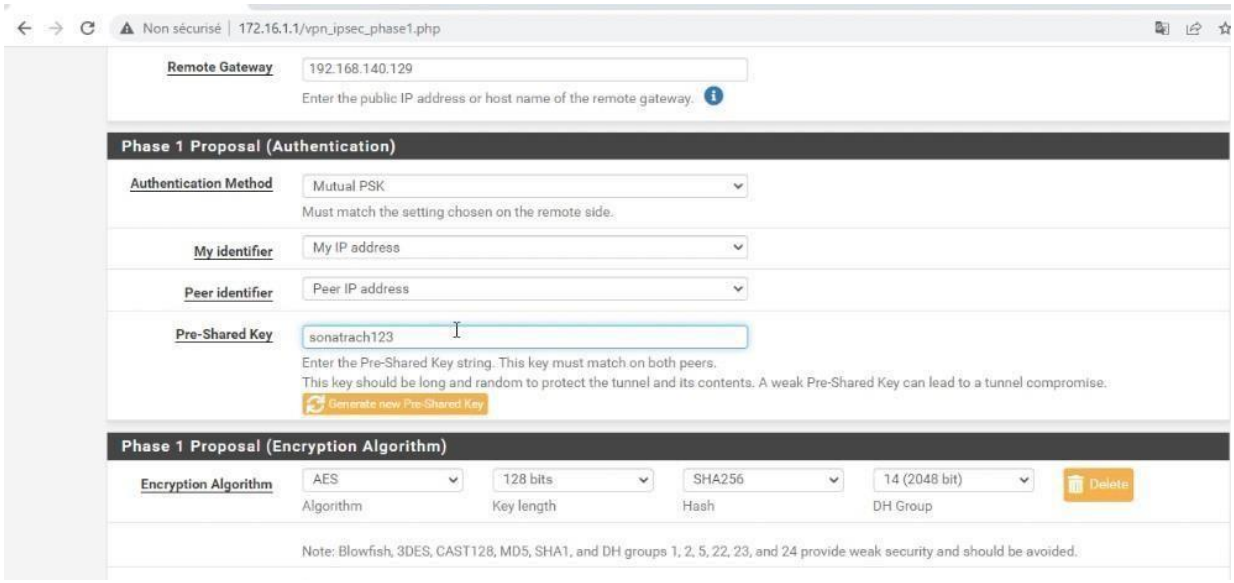
V.6.7 Configuration VPN site to site IPsec :

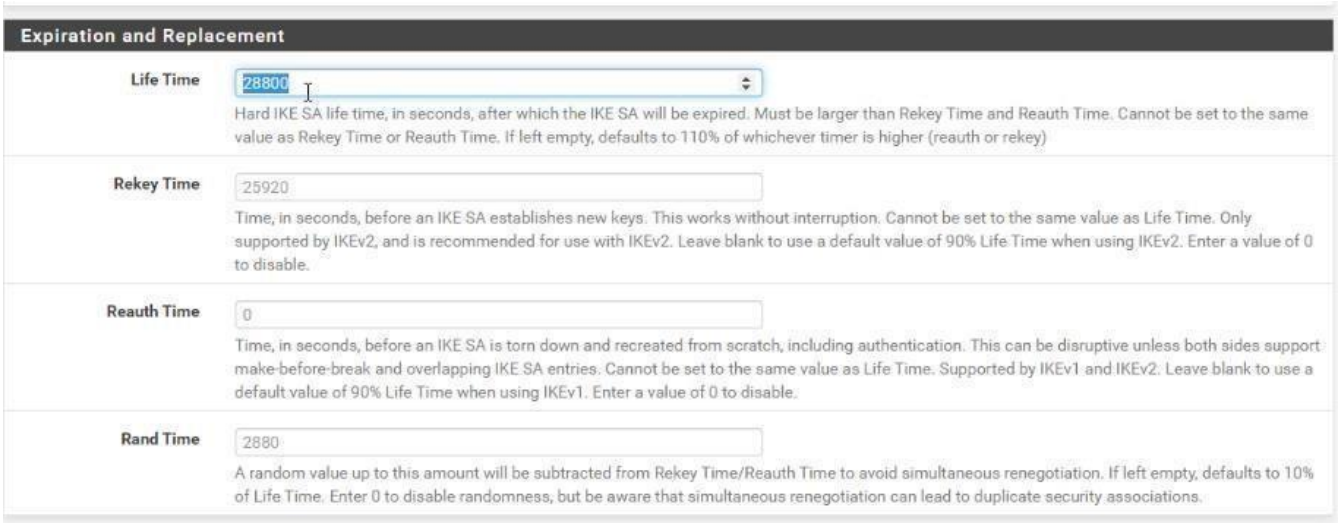
- **Créer une connexion IPsec :**

Pour créer la connexion IPsec on va y'aller au VPN site à site –> IPsec –> Connexions –> Nouvelle connexion IPsec, d'où on va sélectionner la passerelle distante qu'on vient de créer.

L'interface local WAN dont laquelle on va sortir sur ce tunnel et on sélectionnera Réseau LAN local. Nous ferons la même chose sur le site distant (Alger) en sens inverse.





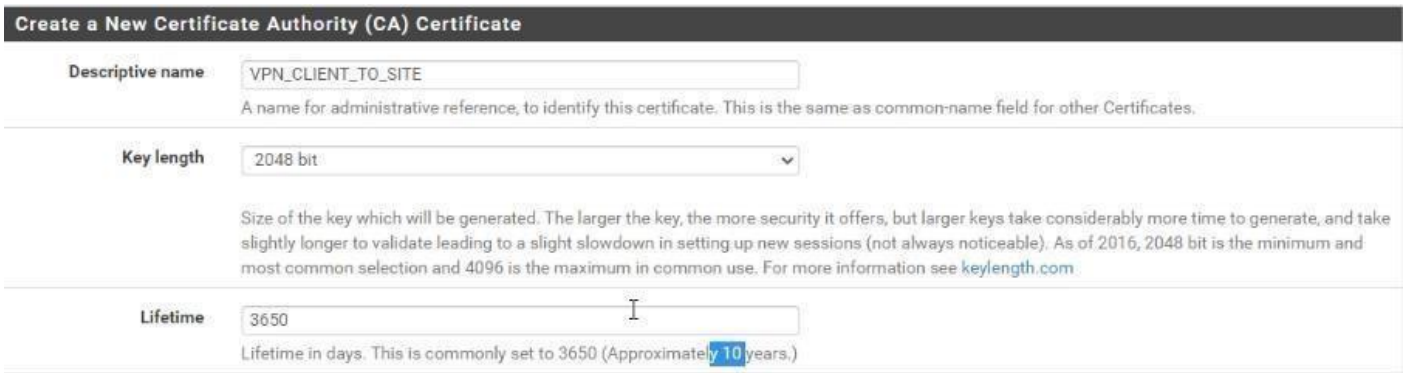


- **Configurer le VPN client à site :**

Le premier élément dont nous avons besoin est de définir une autorité de certification interne,
Avec son propre certificat afin que nous puissions auto-signer les différents certificats créés.
Nous aurons besoin du certificat du serveur, c'est-à-dire au niveau du pfsense et le certificat du client, ceux-ci seront signés par l'autorité de certifications interne que
nous aurons crée

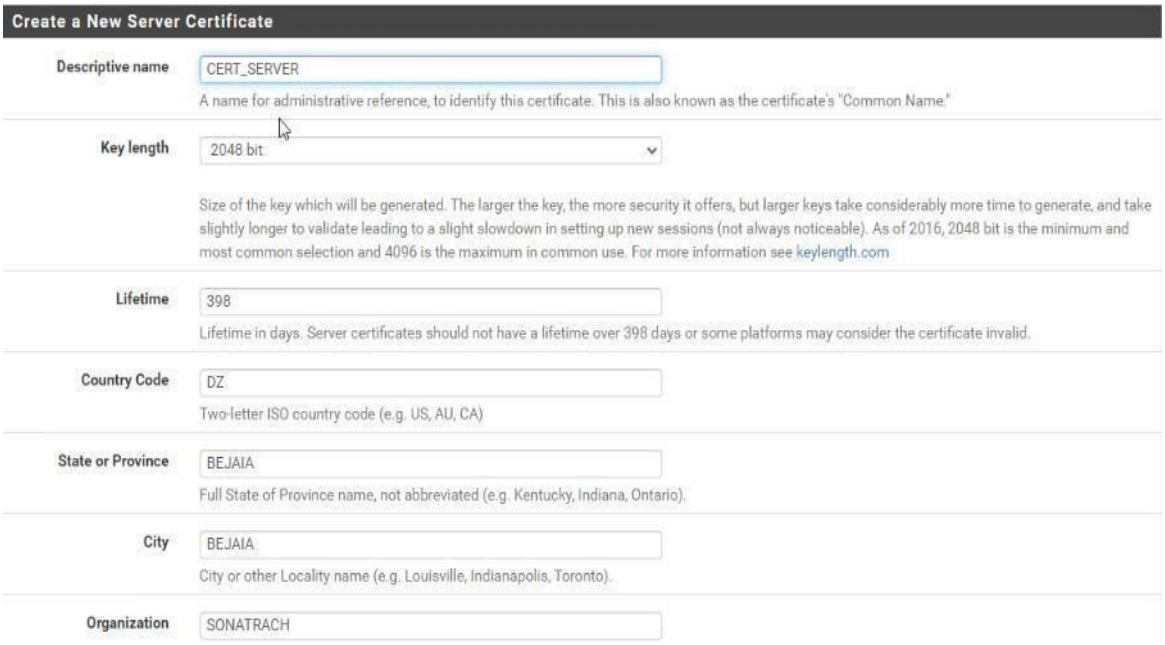
- **Création d'un certificat d'autorité** :

Pour cela, nous allons cliquer sur « Système » puis « certificat manager » dans la fenêtre principale de pfsense.
Nous allons remplir le formulaire ci-dessus en choisissant la méthode « create an internal certificat » pour



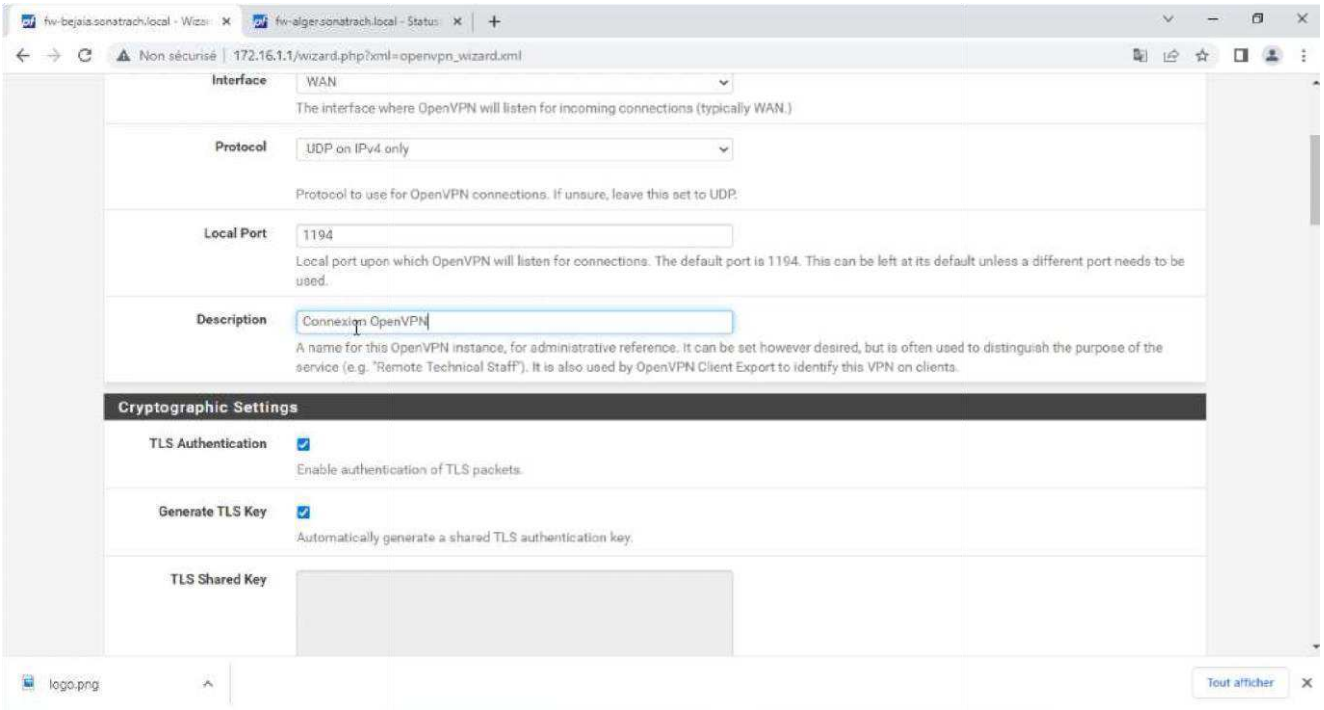
crée une autorité de certificat interne.

- **Création d'un certificat le serveur** :

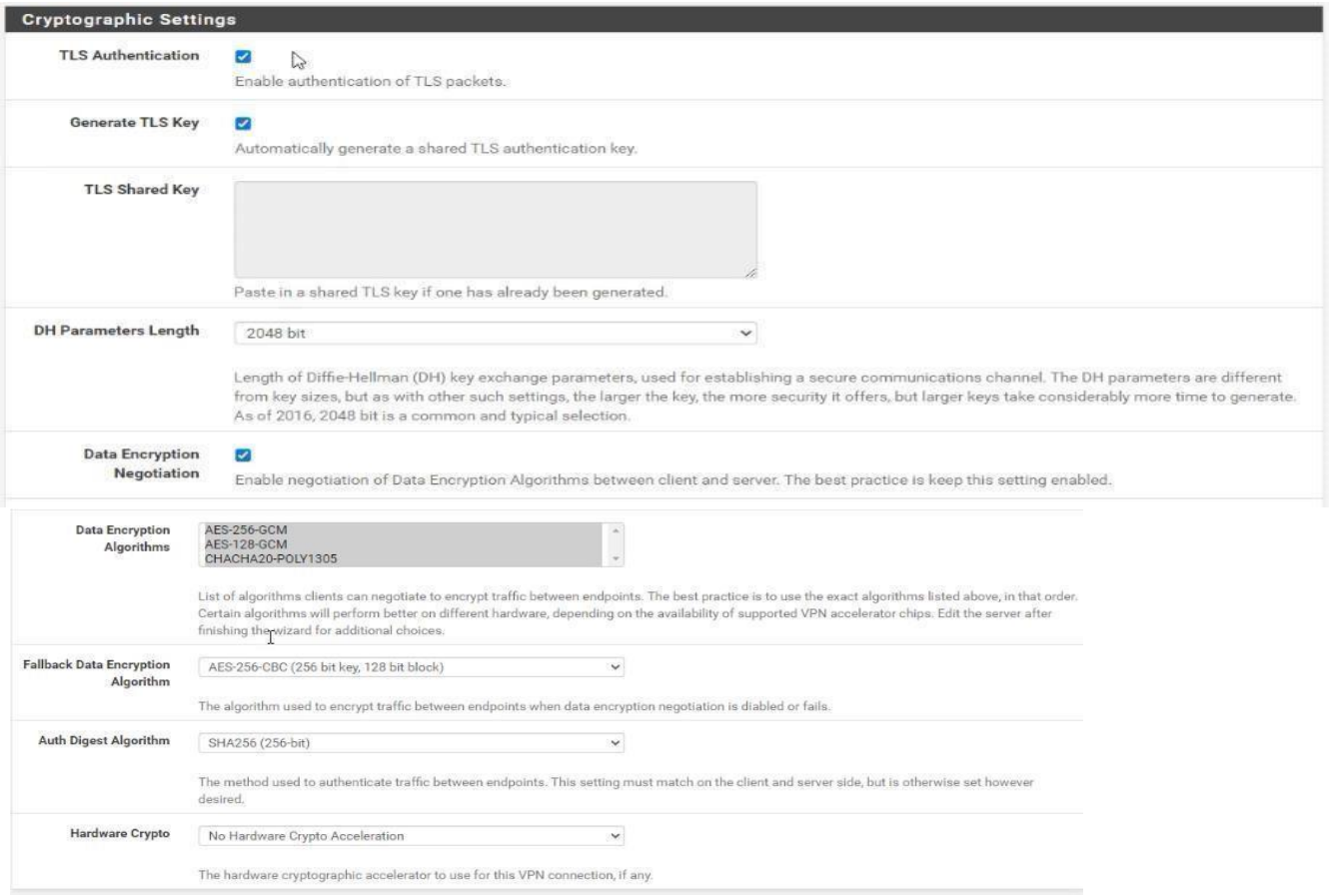


- **Création de certificat openVPN :**

Nous avons également sélectionné l'interface réseau WAN, et précisé le type du protocole de transport (UDP), ainsi que le numéro du port (1194 par défaut).

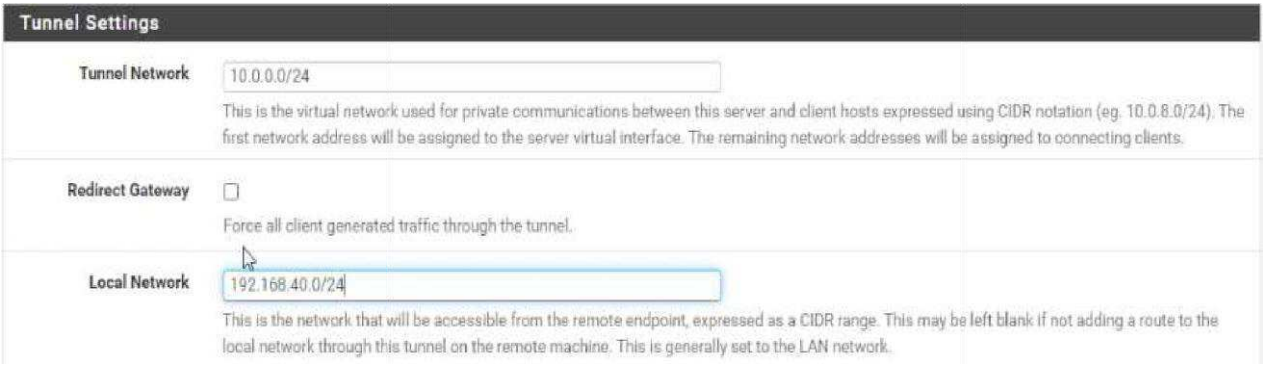


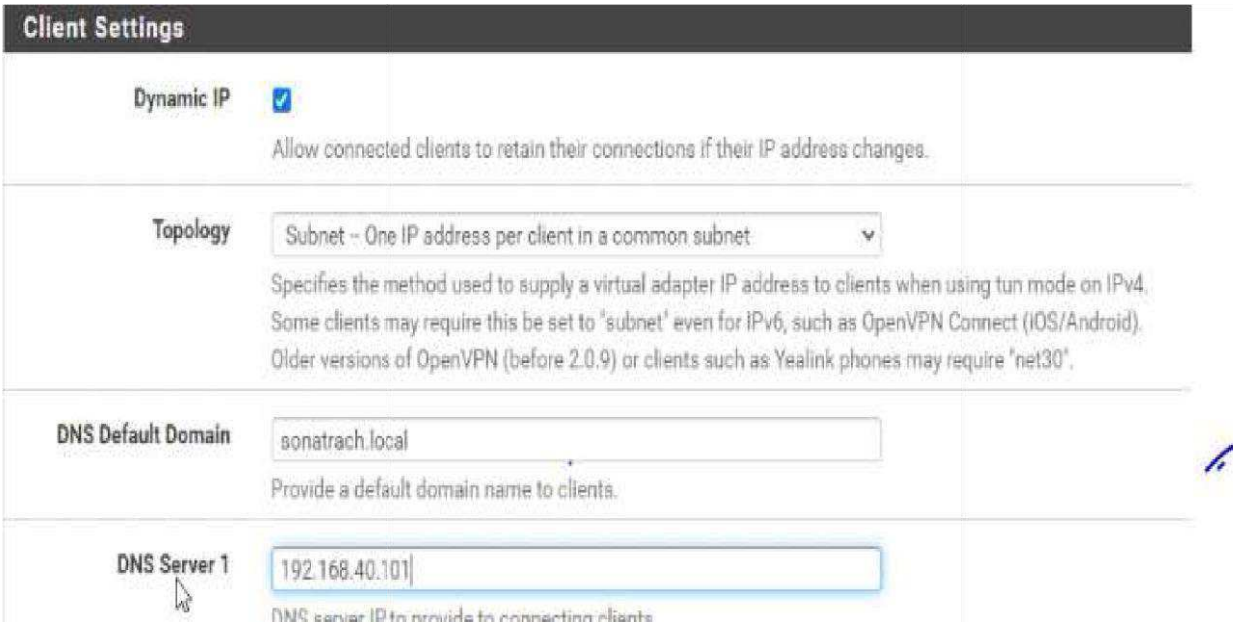
On choisit les algorithmes de cryptographie :



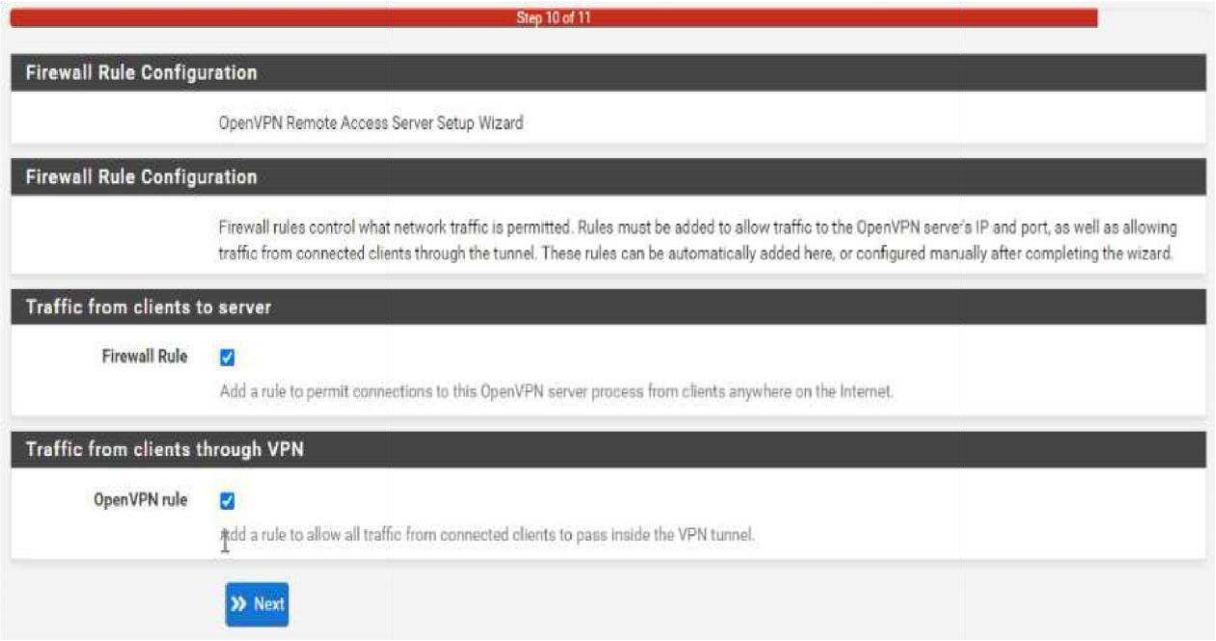
- **Création et configuration du tunnel VPN :**

Le champ réseau du tunnel correspond à l'adresse IP privée dans le tunnel VPN, qui permet d'établir la connexion entre l'utilisateur et le réseau LAN





Pour l'activation des pare-feu par défaut, il faut cocher « Firewall rule »et « OpenVPN rule » :

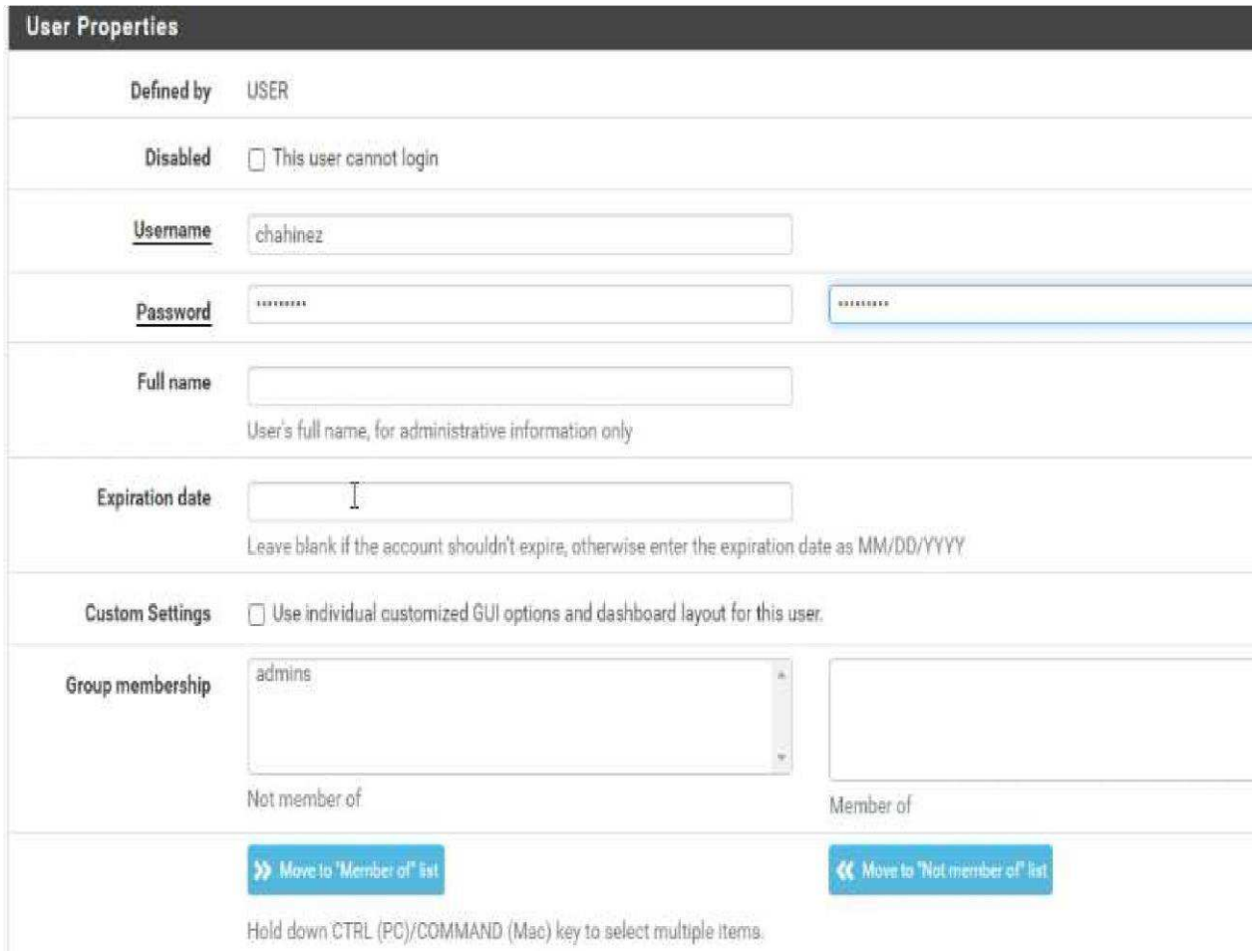


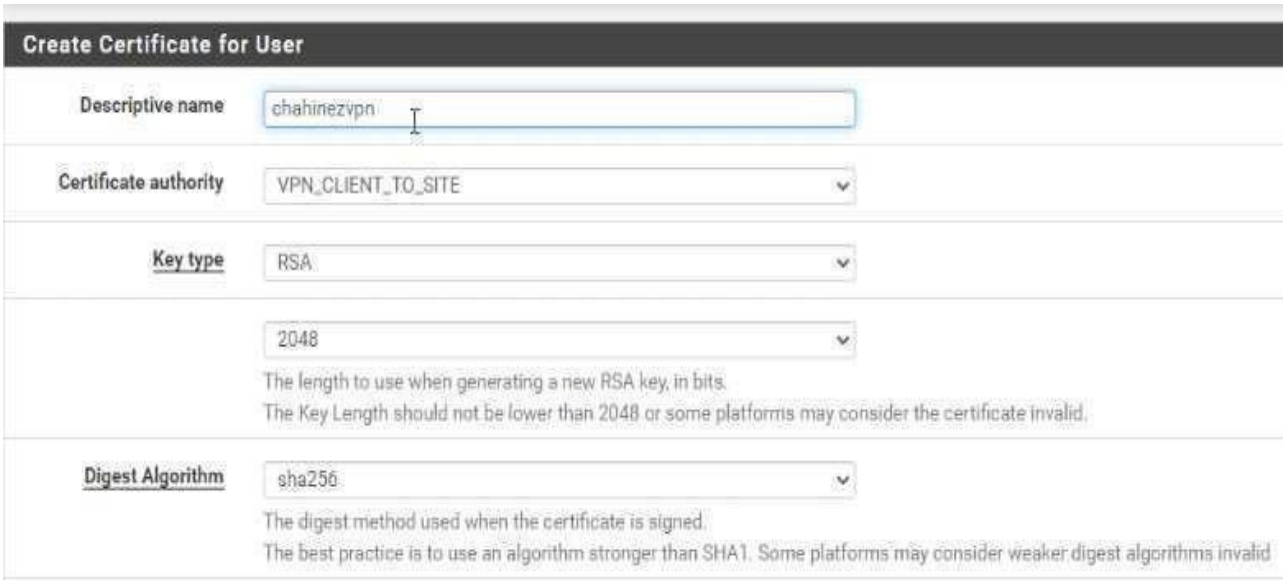
Cliquer sur « next » puis « finish ».

- **Création des utilisateurs ainsi que leurs certificats** :

Dans l'onglet Système, cliquez sur Gestionnaire d'utilisateurs, puis sur Utilisateurs et enfin sur Ajouter un utilisateur autorisé à se connecter au VPN, qui aura son propre certificat Celui-ci sera généré lors de la création de l'utilisateur.

Remplissez le formulaire et cliquez sur "Enregistrer"



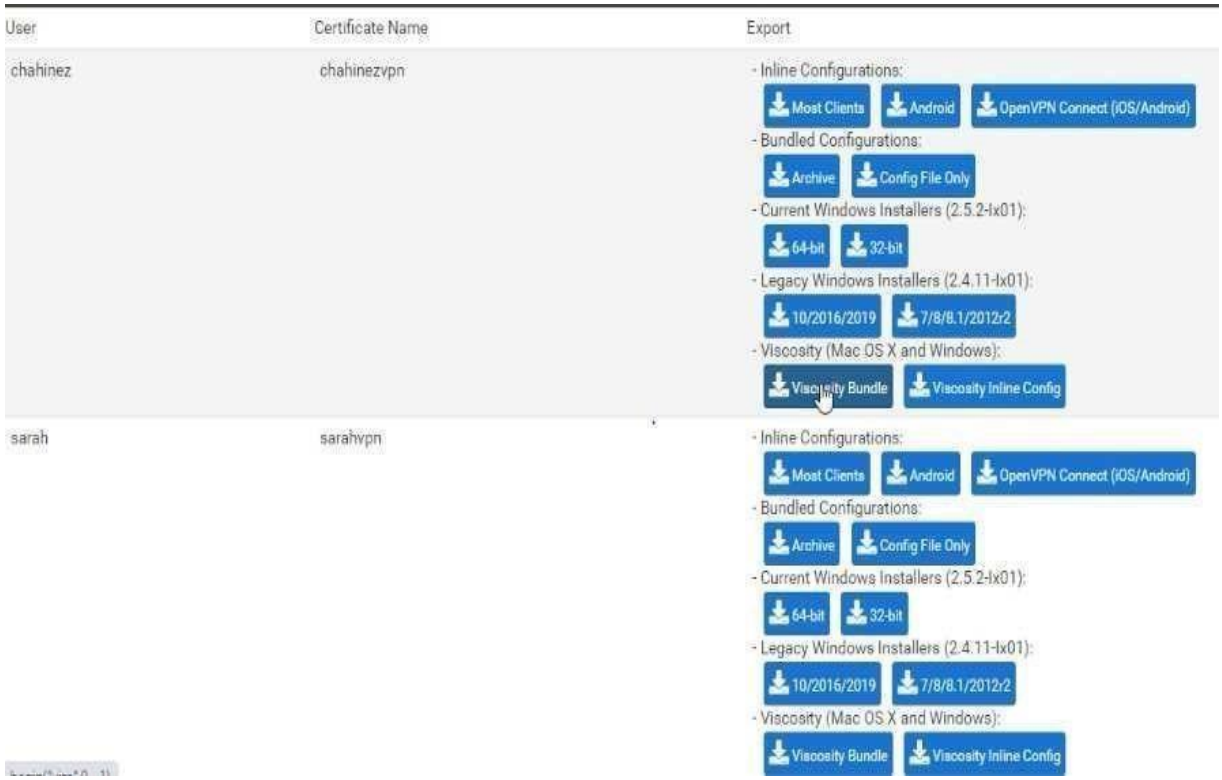


. On a créé deux utilisateurs une pour chahinez et l'autre pour sarah, les étapes sont identiques.

Pour exporter les certificats nous allons installer le paquet Open VPN-client export disponible dans « système » => « backage manager => available packas.

Installation de backage :

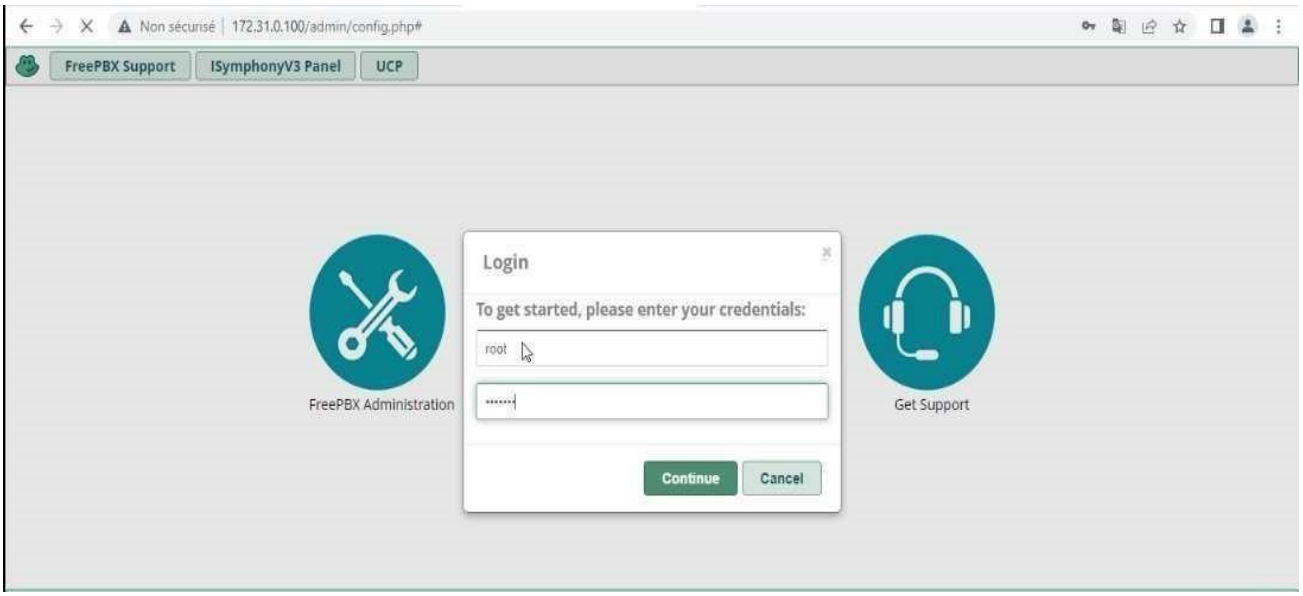
Afin d'exporter les deux clients qu'on a créé, on va y'aller sur OpenVPN puis on télécharge client export :



V.6.8 Configuration de FreePBX :

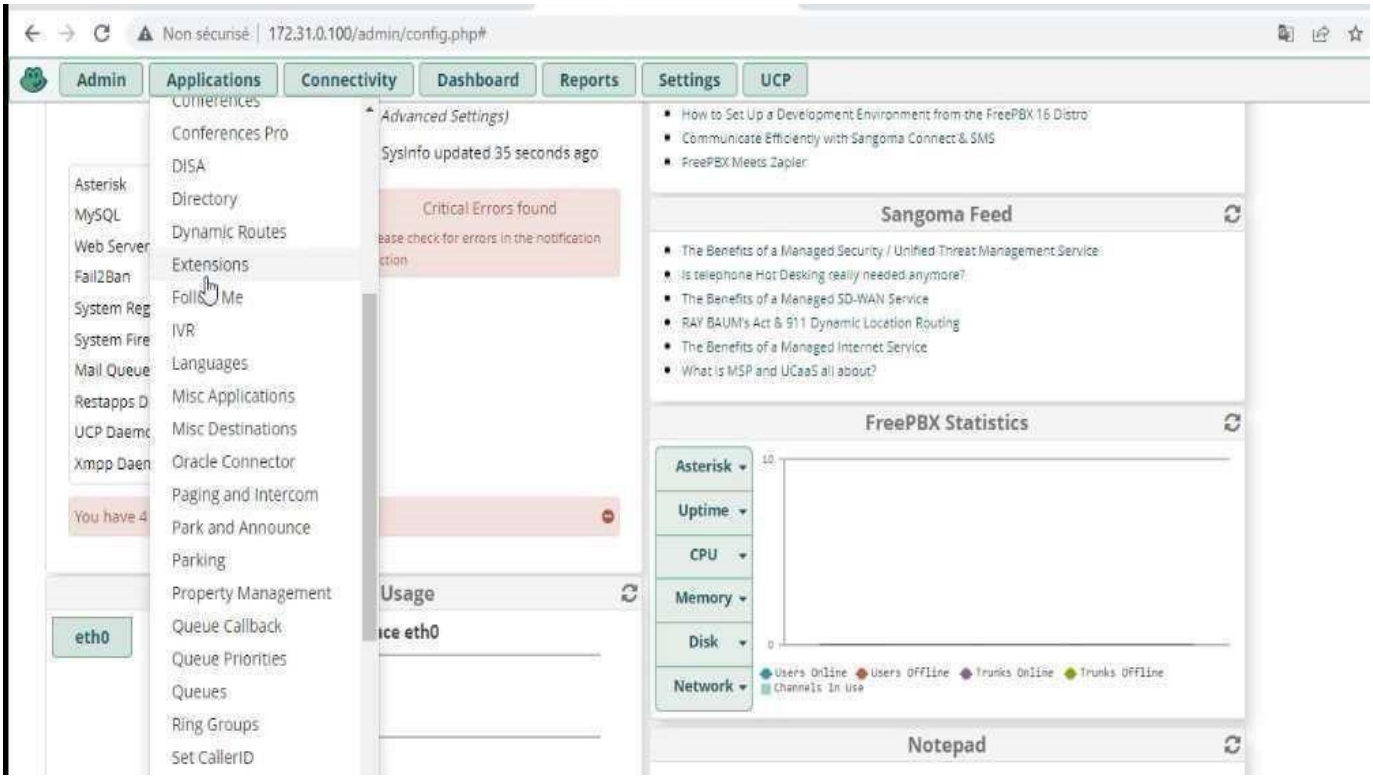
Pour configurer notre FreePBX, nous avons ouvert un navigateur sur un autre PC en réseau avec notre serveur et avons introduit l'adresse IP de notre serveur.

En Cliquant sur « FreePBX administrator », la fenêtre qui permet de nous identifier apparait :



- **Créer des comptes d'utilisateurs :**

Pour créer un compte utilisateur, Pour créer un compte utilisateur il faut aller dans l'onglet « Applications » puis « Extensions », choisir l'outil « Périphérique SIP » et on valide par le bouton « Soumettre ».

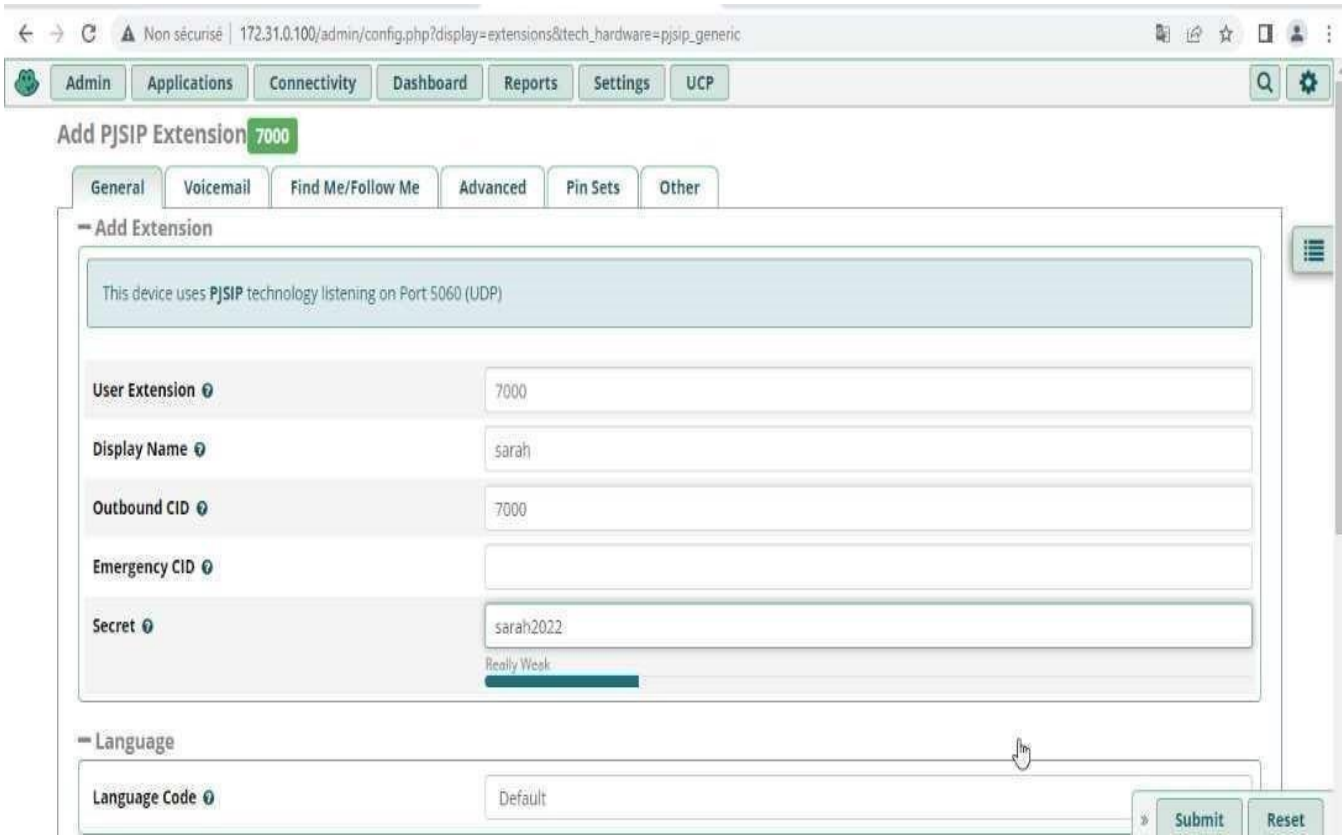


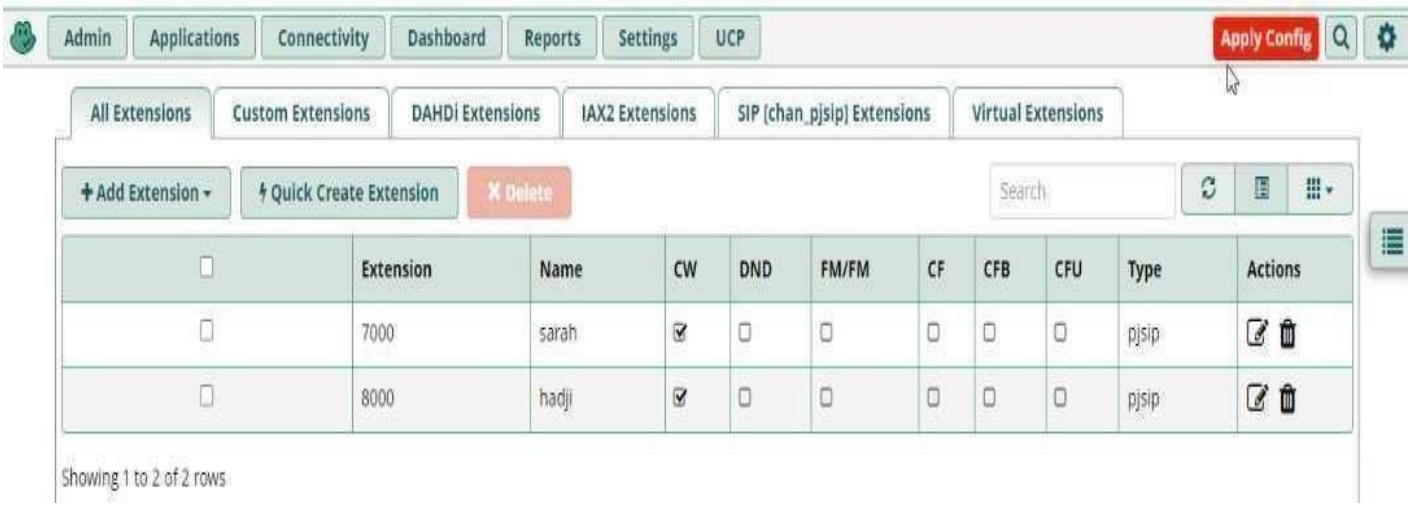
Dans notre cas nous avons besoins de créer quatre comptes (deux comptes sur le site BEJAIA et deux comptes sur le site ALGER). Il suffit de remplir les champs illustrés suivants des quatre utilisateurs :

*Extension Utilisateur : c'est le nom ou le numéro utilisé pour faire les conversations.

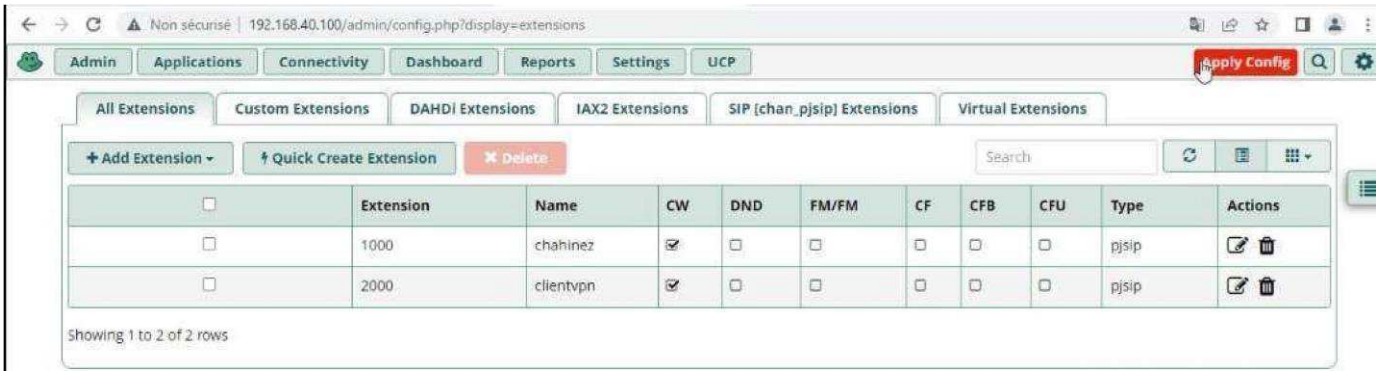
*Nom Affiché : c'est nom de l'extension utilisé pour l'affichage.

*Secret : c'est le mot de passe.



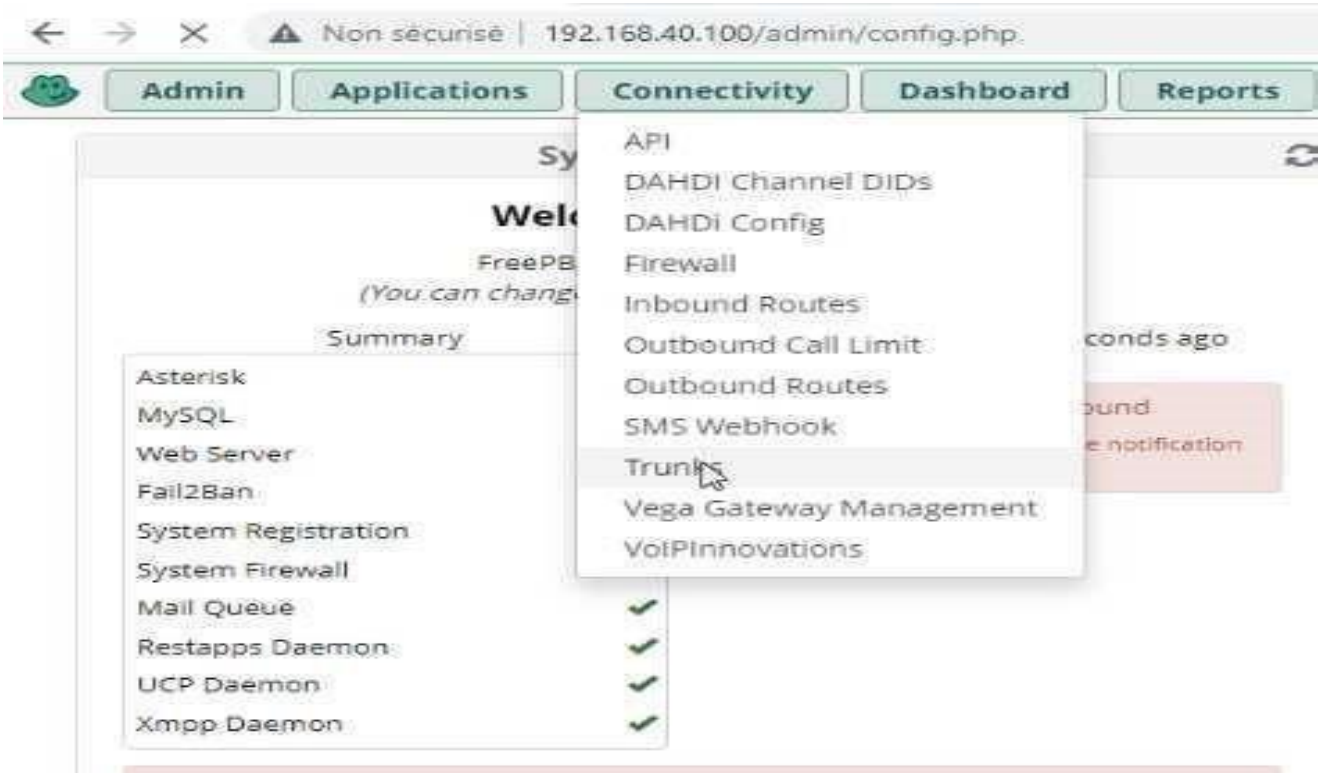


Enfin faire « submit » puis cliquer sur le bouton rouge de rechargement « Apply Config »

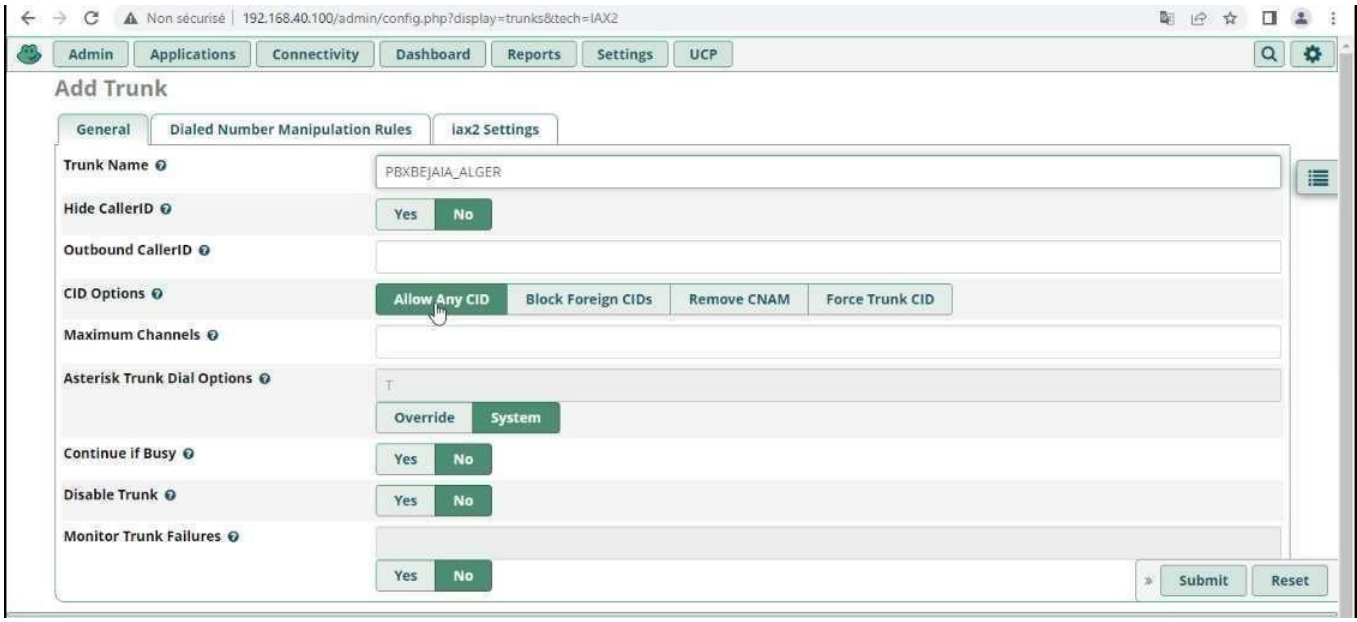


Les extensions site BEJAIA.

- **Configuration d'interconnexion entre deux site**
  Pour configurer l'interconnexion entre de site on suit les étapes suivantes : « connectivity »=> « trunk »

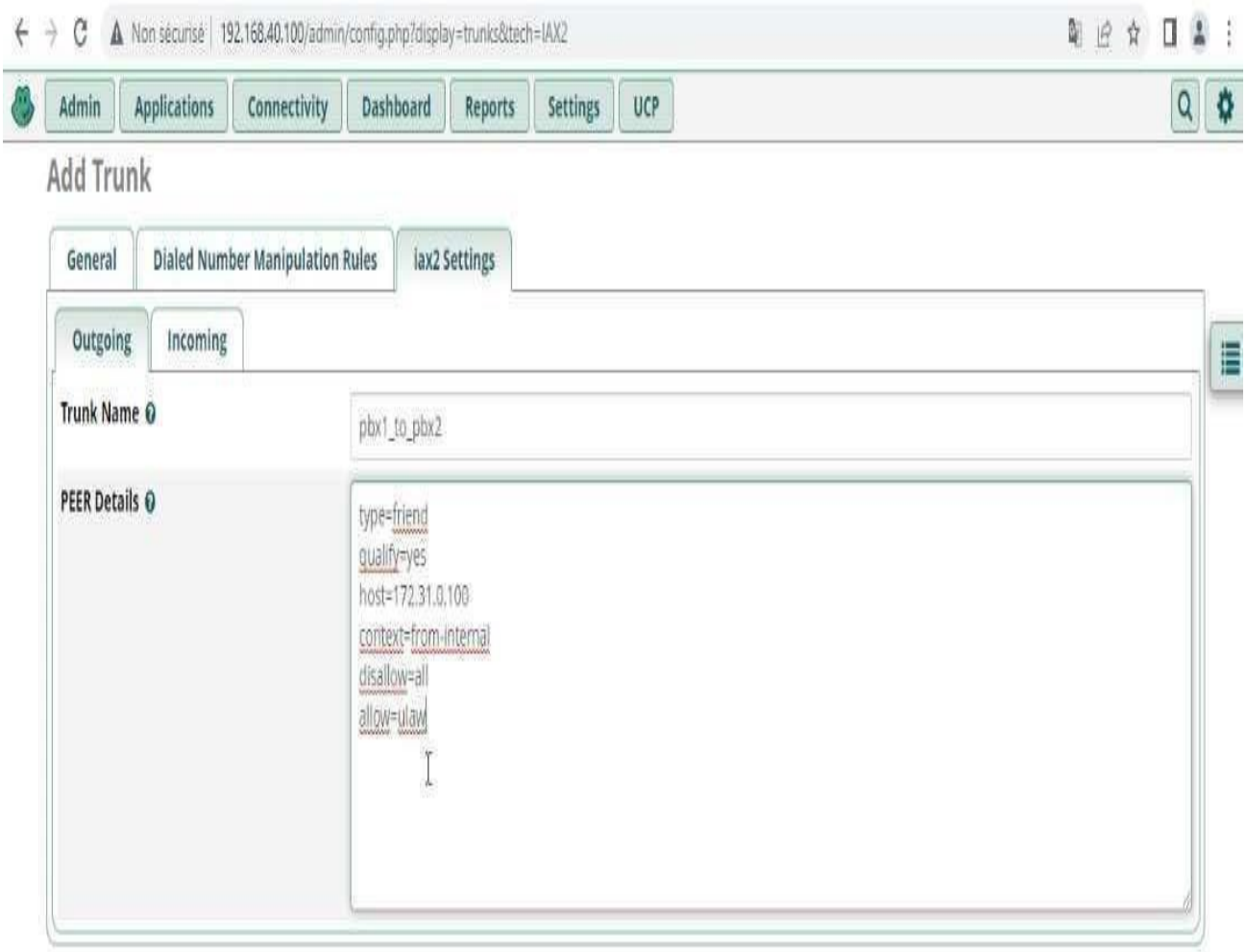


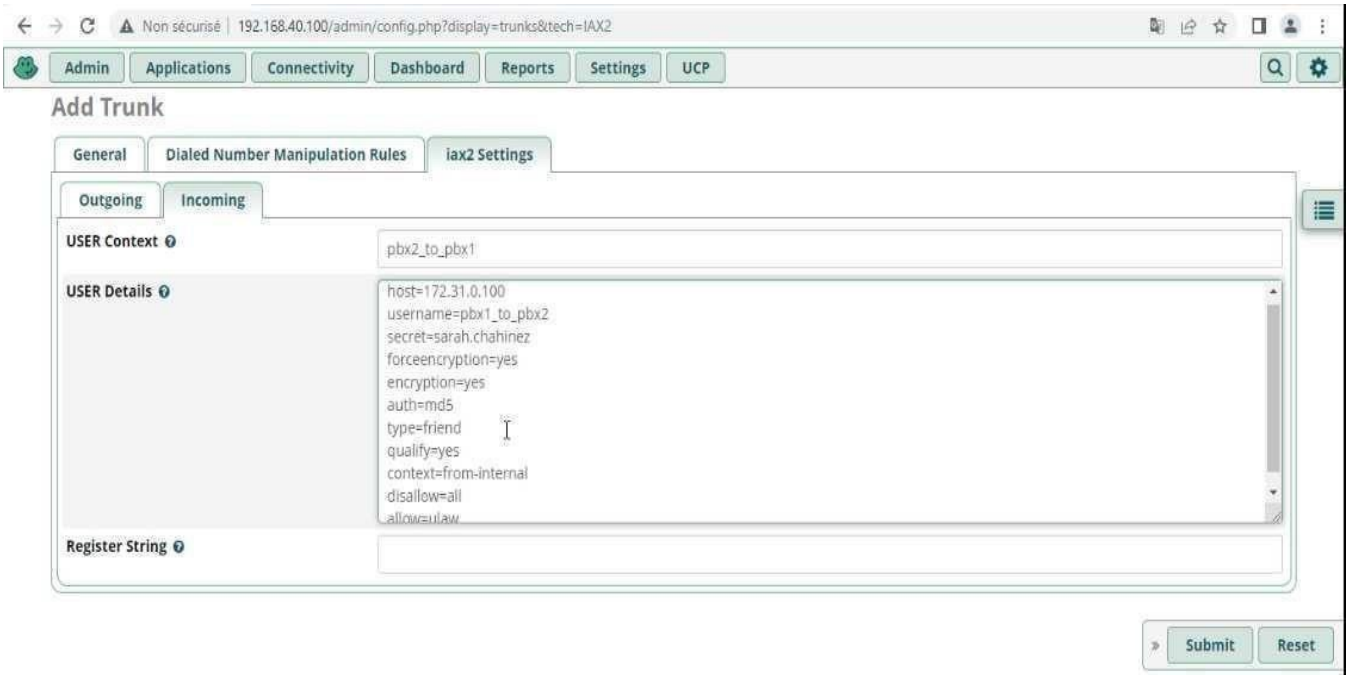
Ensuite « ADD Trunk » => « IAX2 Trunk ». Puis on va remplir le formulaire suivant



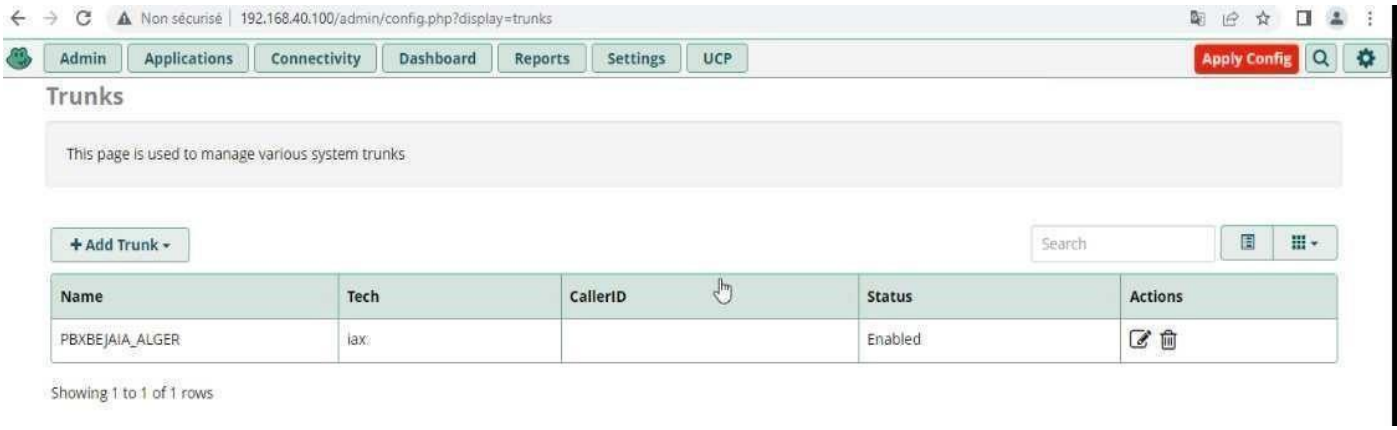
Dans l'onglet iax2 Settings, on doit remplir les champs Trunk Name et Peer Details dans l'onglet Outgoing. ne rien mettre dans l'onglet Incoming.

Sur le PBX1

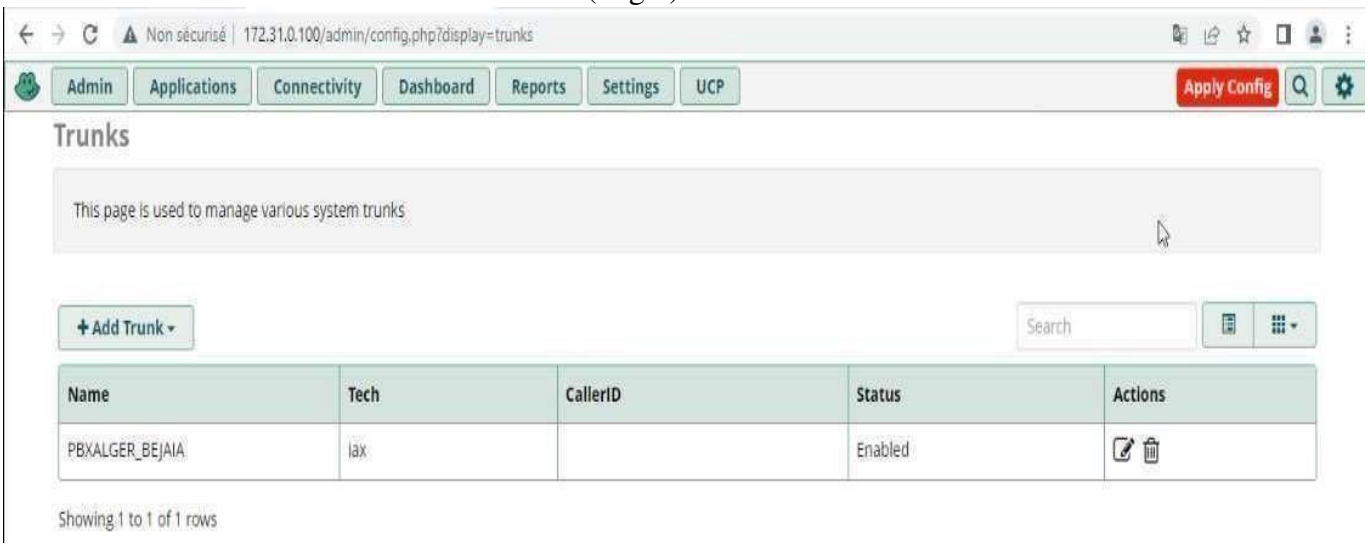




- **Routage des appels site1(1000-2000) vers site2(7000-8000) :**

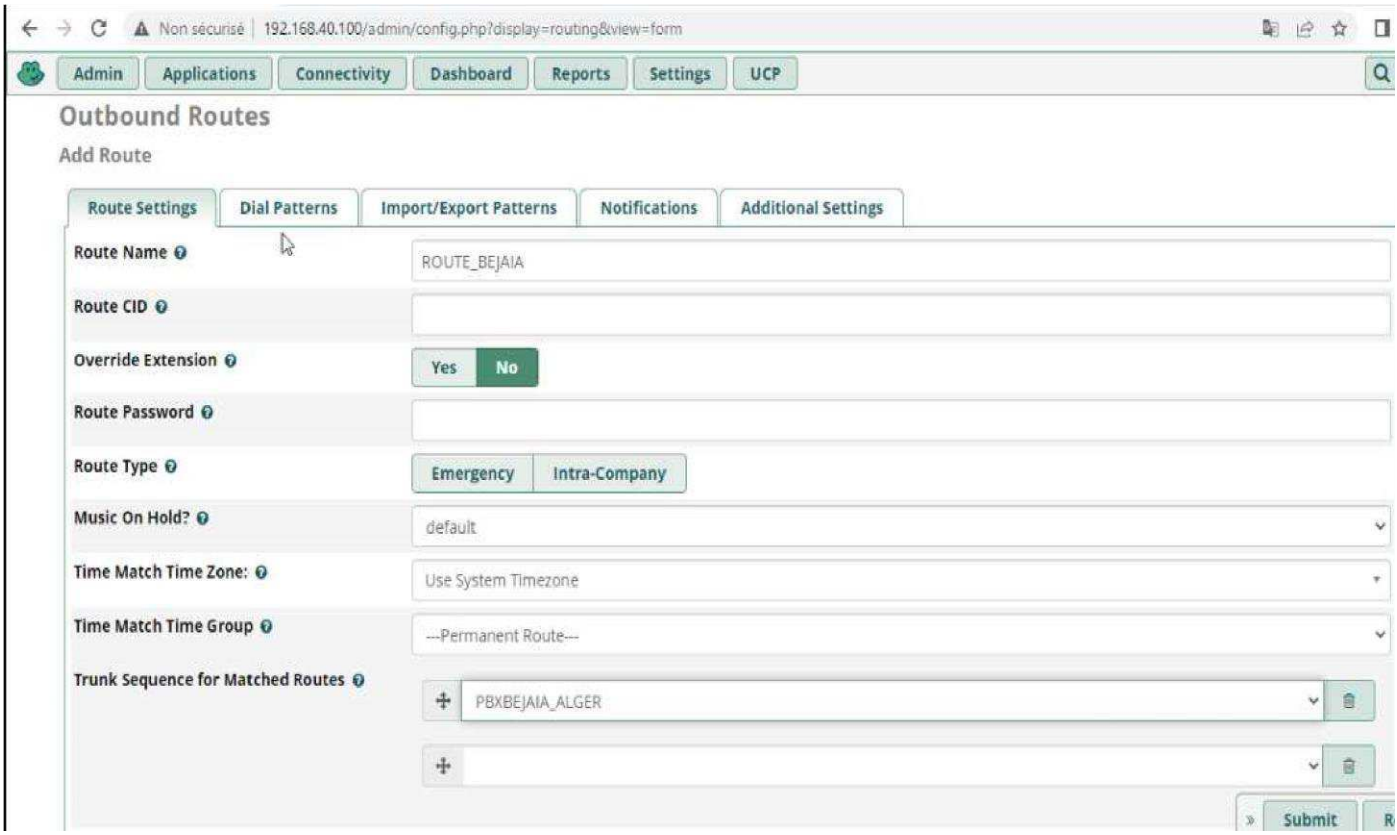


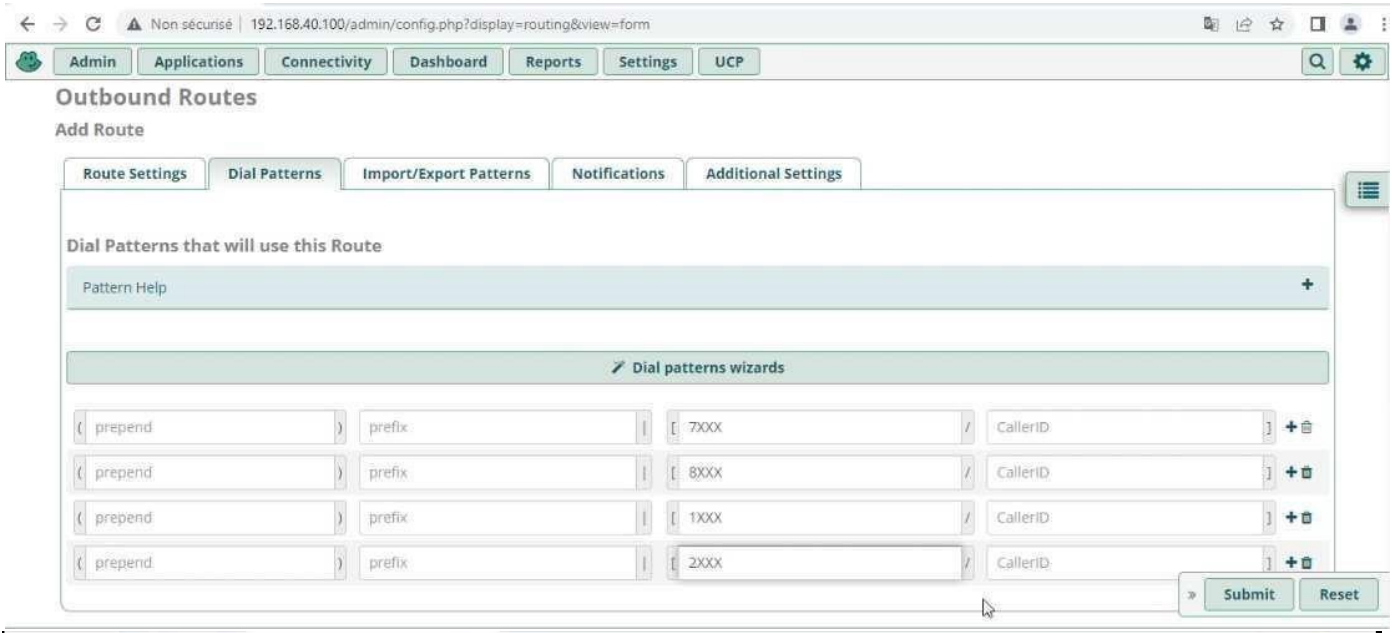
Nous créons la même chose sur le site distant (Alger) en sens inverse.

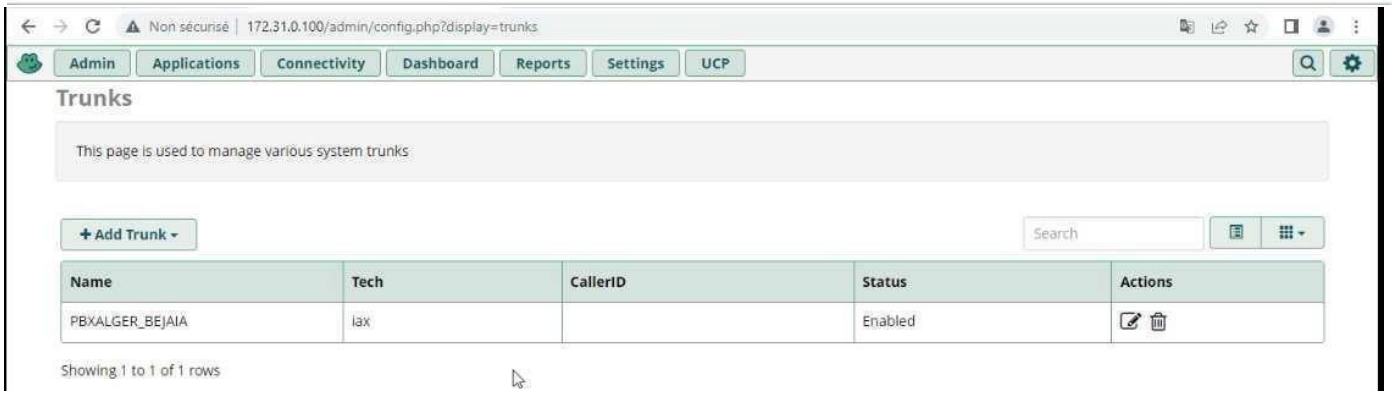


On va y'aller sur « connectivity » pour router les appels avec la commande « outbound Routes » puis « Add outbound trunk »et on va remplir le formulaire suivant :

Dans l'onglet Dial Patterns, on va créer un modèle qui correspond à la gamme d'extensions du PBX opposé. Le site Bejaia PBX1 utilise les extensions 1000 à 2000 et pour le site Alger PBX2 utilise les extensions 7000 à 8000, voici à quoi cela ressemble.


Non sécurisé | 192.168.40.100/admin/config.php?display=routing&view=form
Admin
Applications
Connectivity
Dashboard
Reports
Settings
UCP
Outbound Routes
Add Route
Route Settings
Dial Patterns
Import/Export Patterns
Notifications
Additional Settings
Route Name
ROUTE_BEJAIA
Route CID
Override Extension
Yes
No
Route Password
Route Type
Emergency
Intra-Company
Music On Hold?
default
Time Match Time Zone:
Use System Timezone
Time Match Time Group
---Permanent Route---
Trunk Sequence for Matched Routes
PBXBEJAIA_ALGER
Submit

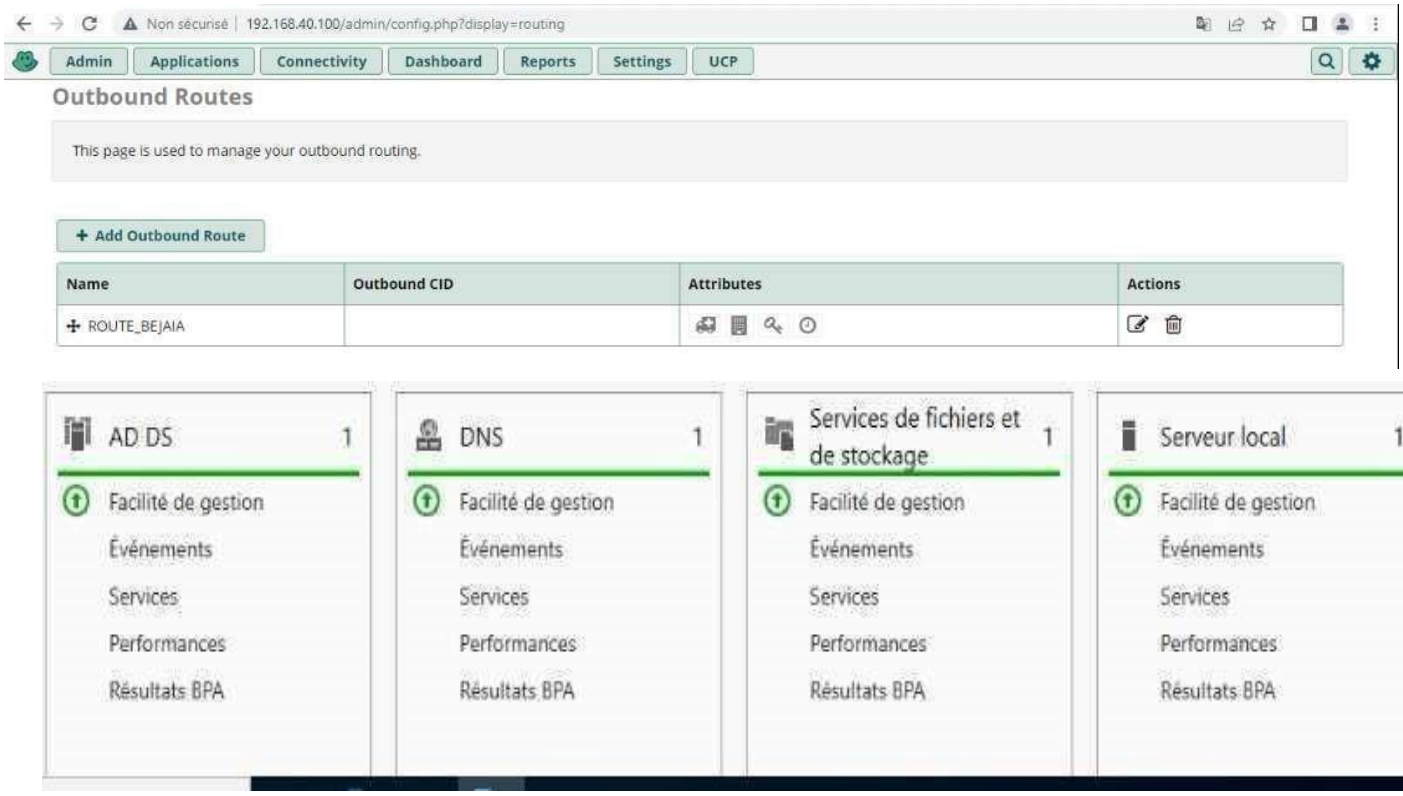




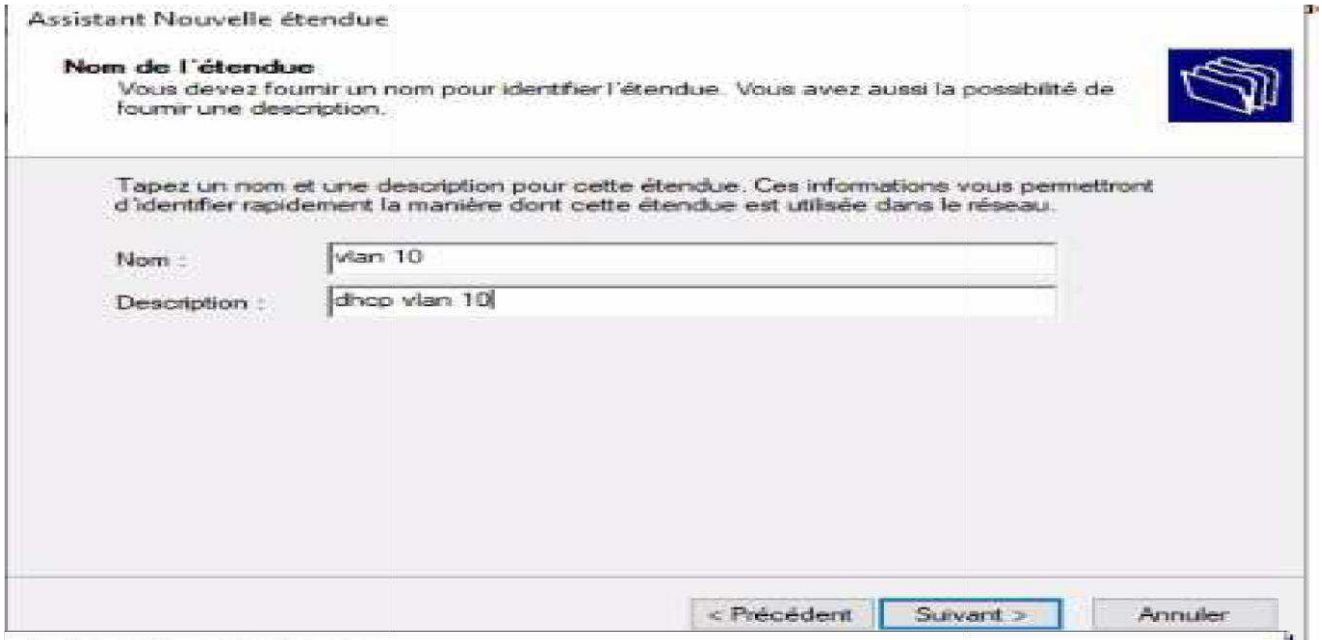
Nous créons la même chose pour le site distant Béjaia en sens inverse

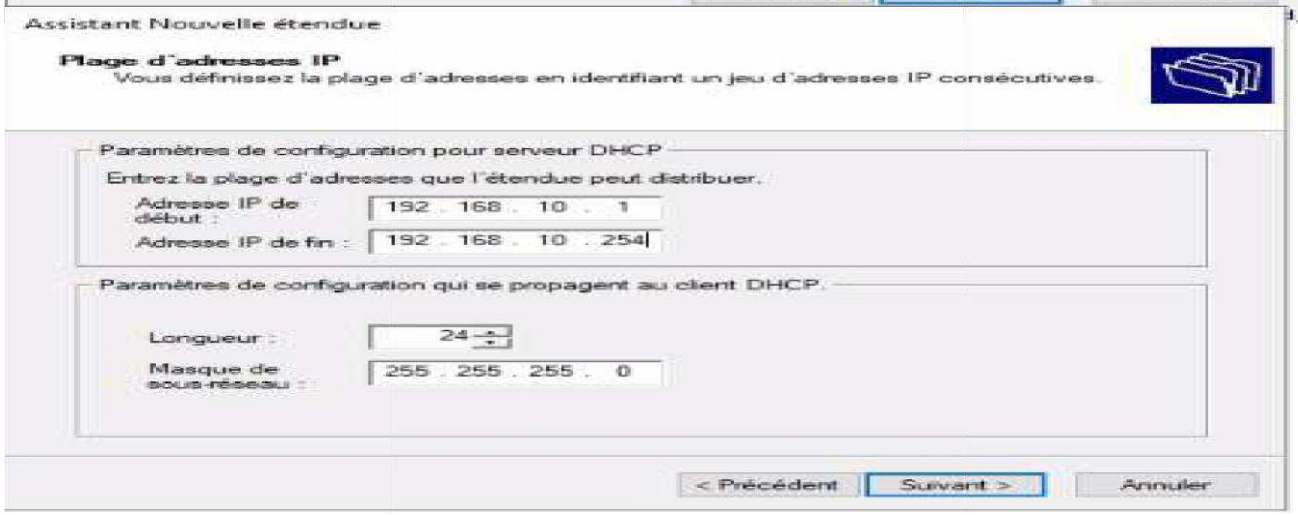
V.6.9 Configuration DHCP :

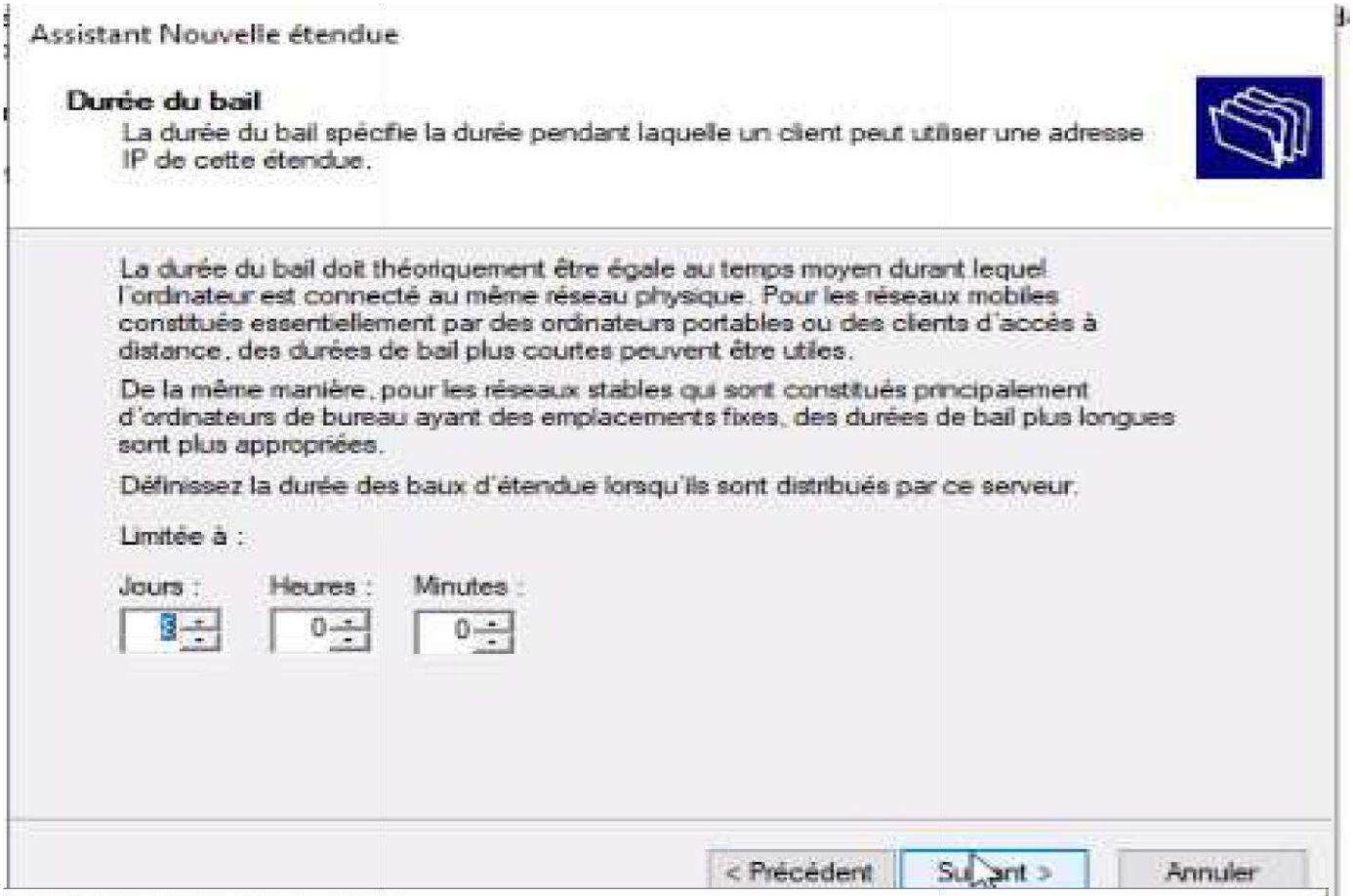
Après l'installation de serveur 2022 on a installé le serveur AD et DHCP sachant que le serveur DNS a été installé automatiquement

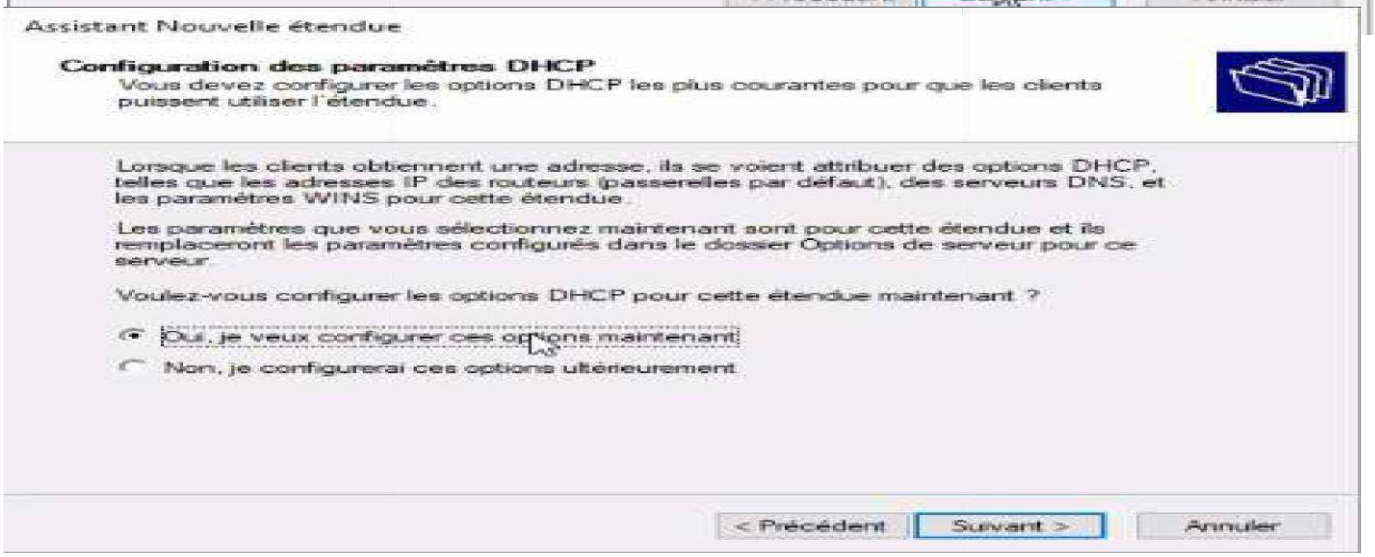


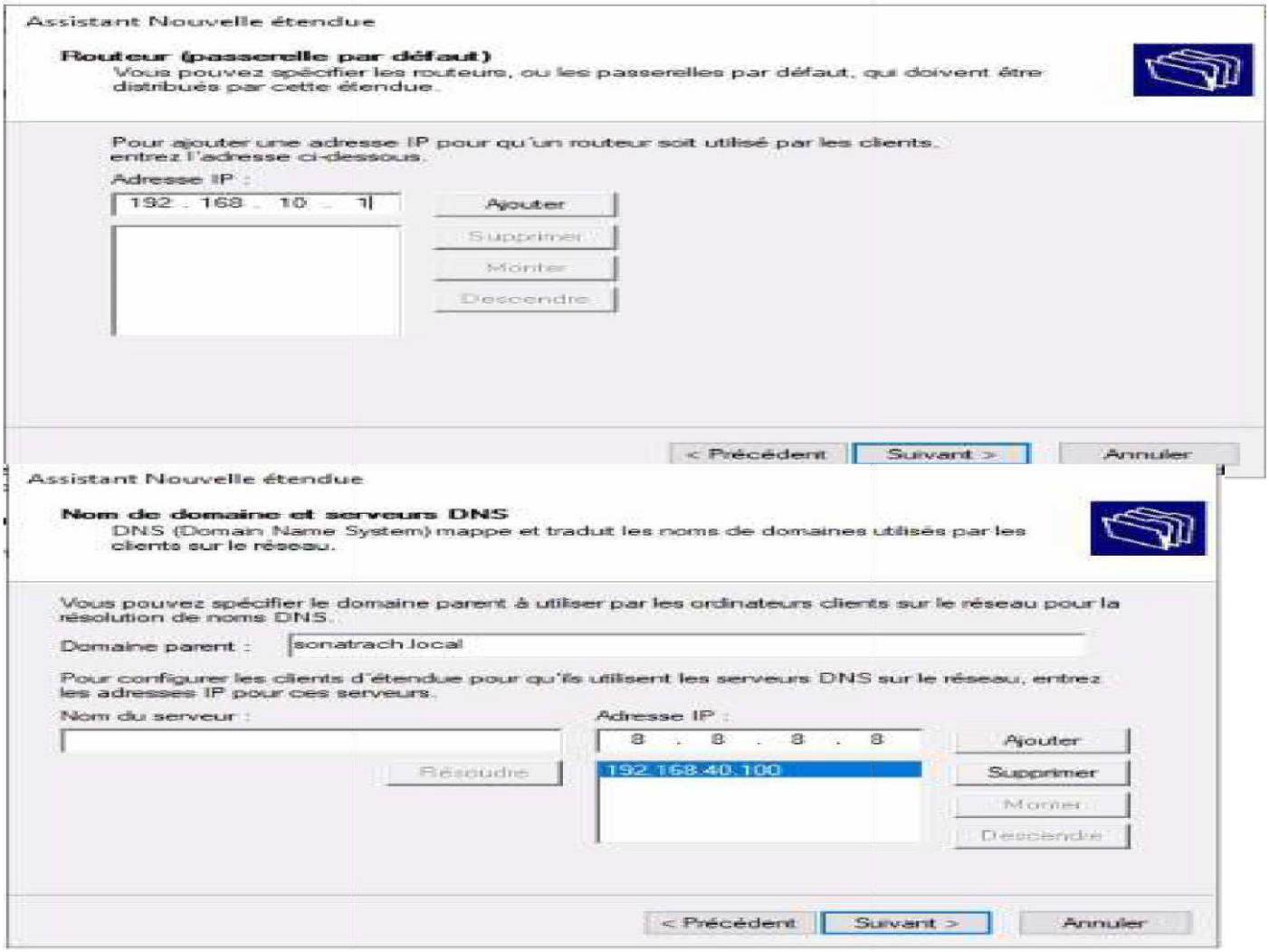
Maintenant, on va passer à la mise en place du DHCP sur le serveur AD

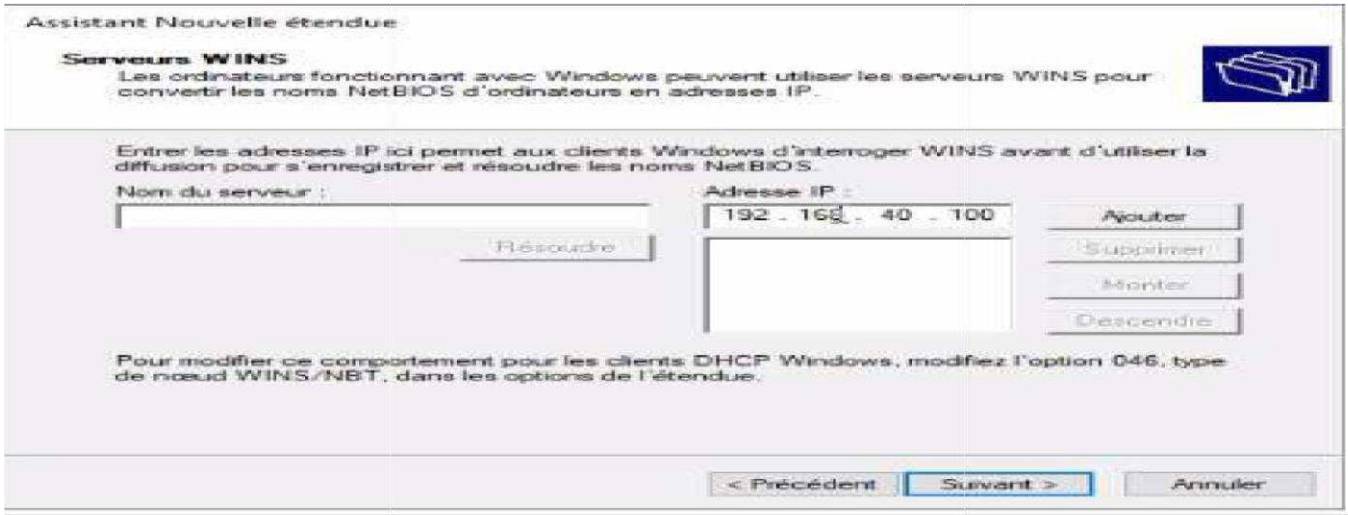

Assistant Nouvelle étendue
Nom de l'étendue
Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.
Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.
Nom :
vlan 10
Description :
dhcp vlan 10
< Précédent
Suivant >
Annuler

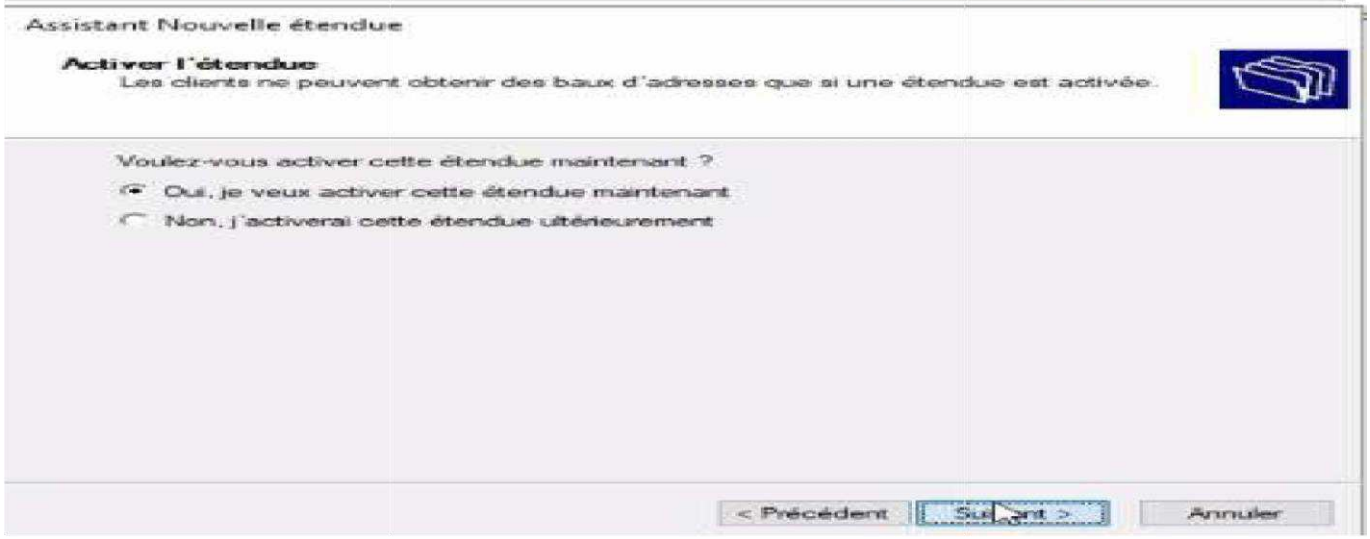

Assistant Nouvelle étendue
Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.
Paramètres de configuration pour serveur DHCP
Entrez la plage d'adresses que l'étendue peut distribuer.
Adresse IP de début :
192 . 168 . 10 . 1
Adresse IP de fin :
192 . 168 . 10 . 254
Paramètres de configuration qui se propagent au client DHCP.
Longueur :
24
Masque de sous-réseau :
255 . 255 . 255 . 0
< Précédent
Suivant >
Annuler


Assistant Nouvelle étendue
Durée du bail
La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.
La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.
De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.
Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.
Limitée à :
Jours :
Heures :
Minutes :
8
0
0
< Précédent
Suivant >
Annuler

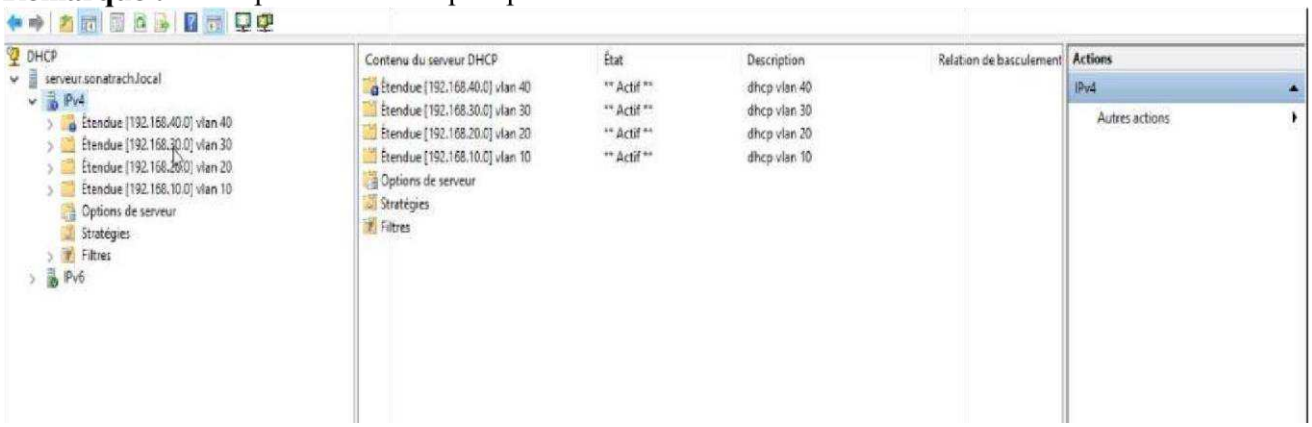

Assistant Nouvelle étendue
Configuration des paramètres DHCP
Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.
Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.
Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.
Voulez-vous configurer les options DHCP pour cette étendue maintenant ?
Oui, je veux configurer ces options maintenant
Non, je configurerai ces options ultérieurement
< Précédent
Suivant >
Annuler


Assistant Nouvelle étendue
Routeur (passerelle par défaut)
Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.
Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.
Adresse IP :
192 . 168 . 10 . 1
Ajouter
Supprimer
Monter
Descendre
< Précédent
Suivant >
Annuler
Assistant Nouvelle étendue
Nom de domaine et serveurs DNS
DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.
Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.
Domaine parent :
sonatrach.local
Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.
Nom du serveur :
Résoudre
Adresse IP :
8 . 8 . 8 . 8
192.168.40.100
Ajouter
Supprimer
Monter
Descendre
< Précédent
Suivant >
Annuler



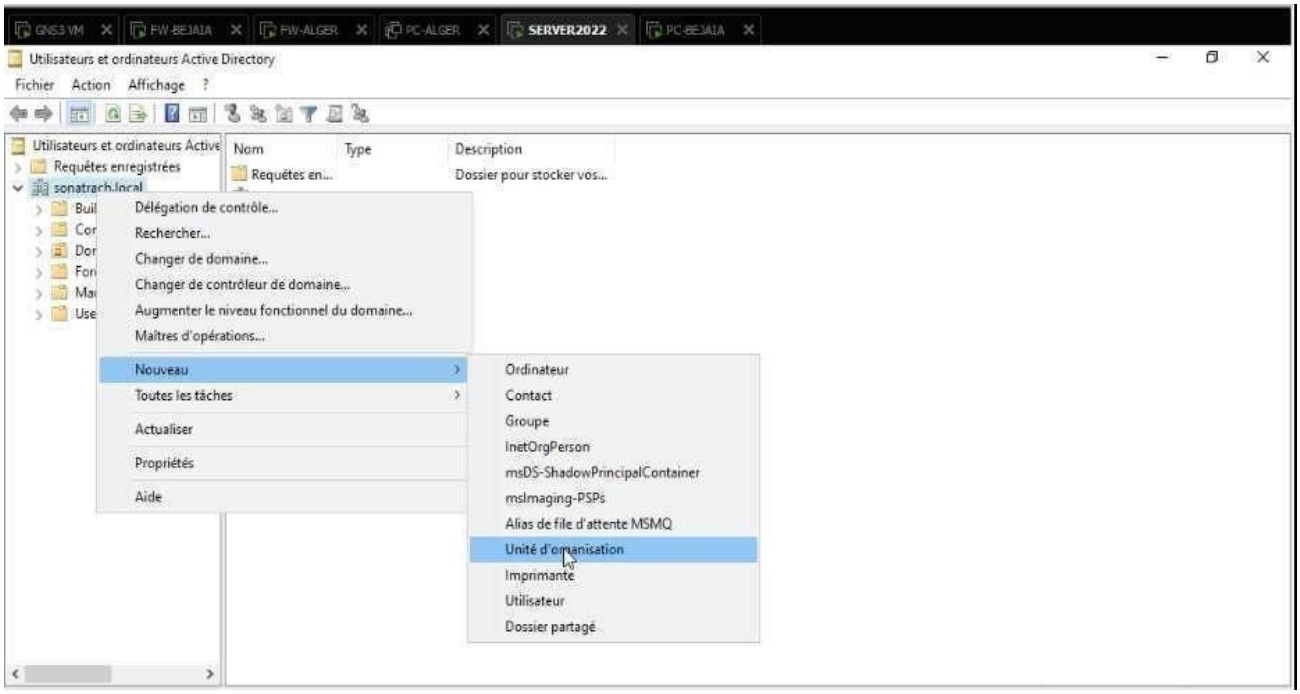


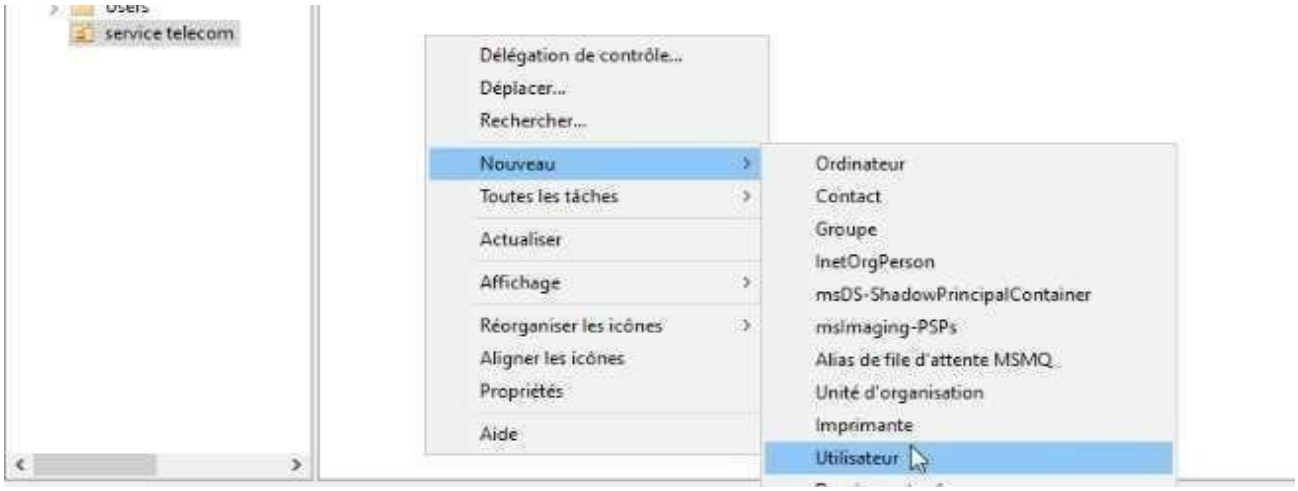
Remarque : les étapes sont identiques pour les autres VLANs.

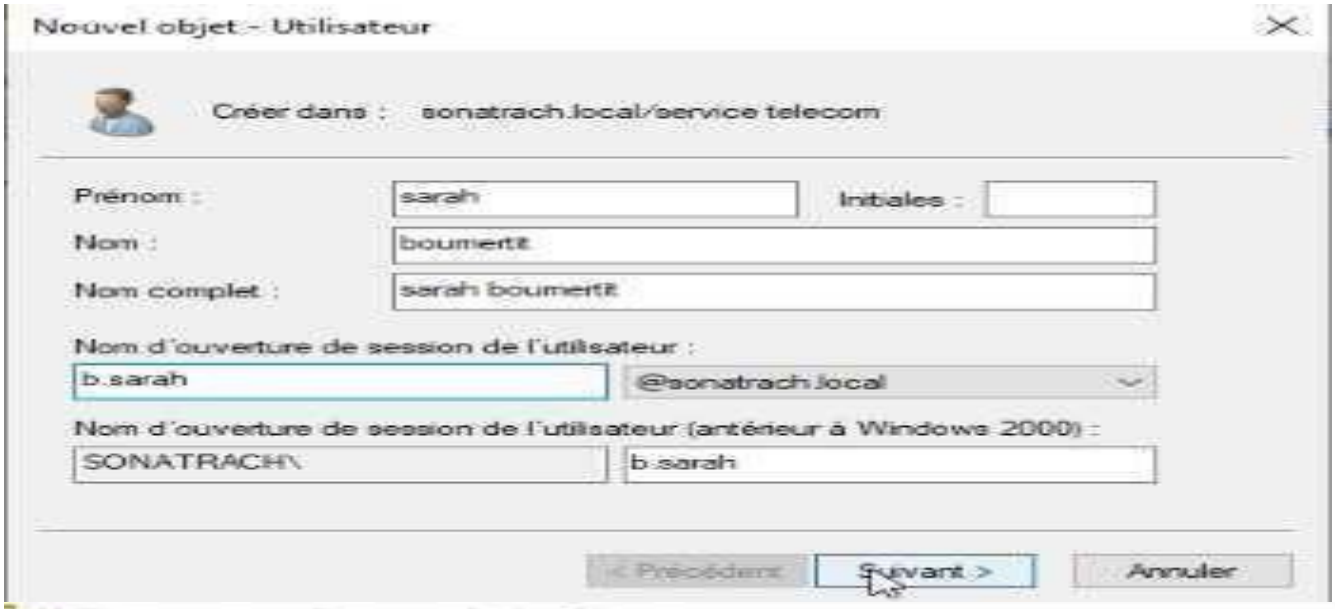


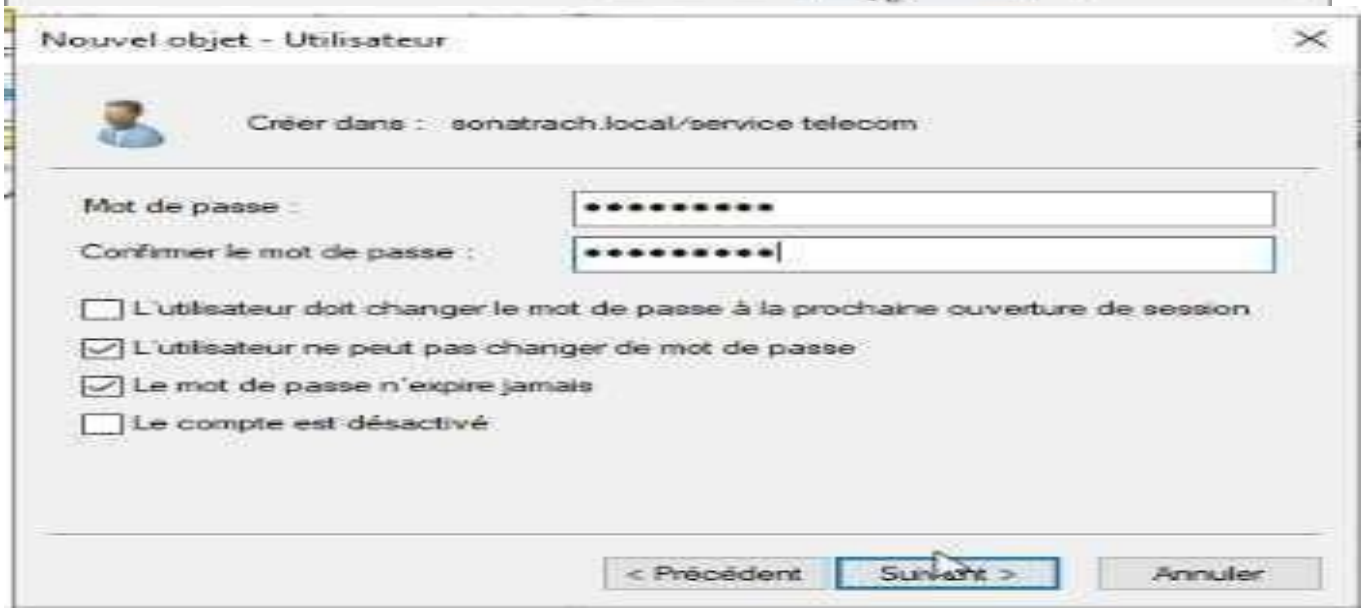
V.6.10 Configuration serveur AD :

On a créé un service « telecom » au-dessous de ce service on a créé deux comptes pour sarah et chahinez en suivant les étapes ci-dessous :

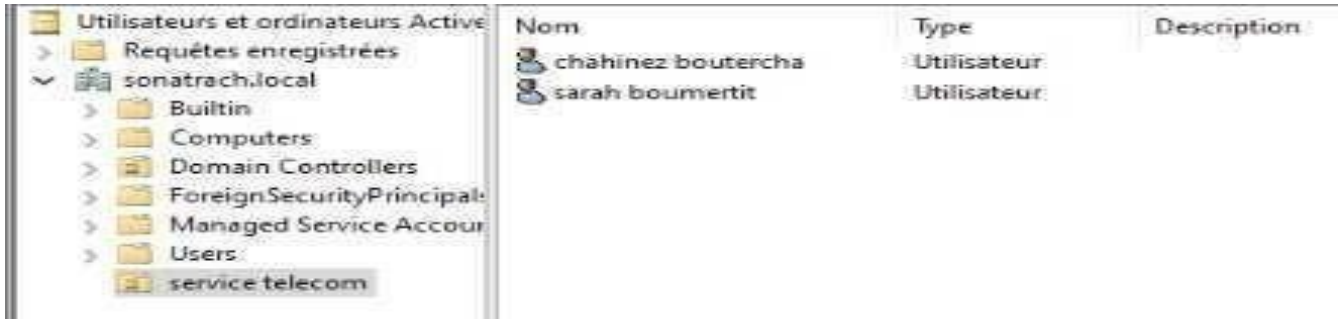

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
sonatrach.local
Nom
Type
Description
Requêtes en...
Dossier pour stocker vos...
Délégation de contrôle...
Rechercher...
Changer de domaine...
Changer de contrôleur de domaine...
Augmenter le niveau fonctionnel du domaine...
Maîtres d'opérations...
Nouveau
Toutes les tâches
Actualiser
Propriétés
Aide
Ordinateur
Contact
Groupe
InetOrgPerson
msDS-ShadowPrincipalContainer
mslmaging-PSPs
Alias de file d'attente MSMQ
Unité d'organisation
Imprimante
Utilisateur
Dossier partagé


service telecom
Délégation de contrôle...
Déplacer...
Rechercher...
Nouveau
Toutes les tâches
Actualiser
Affichage
Réorganiser les icônes
Aligner les icônes
Propriétés
Aide
Ordinateur
Contact
Groupe
InetOrgPerson
msDS-ShadowPrincipalContainer
mslmaging-PSPs
Alias de file d'attente MSMQ
Unité d'organisation
Imprimante
Utilisateur





Remaque : les étapes sont identiques pour le compte de chahinez



V.6.11 les carte réseaux utilisées :

Le nom	Le type	L'adresse
VMnet1	/	192.168.175.0
VMnet8	Nat	192.168.38.0
VMnet10	Vlan 10	192.168.10.0
VMnet11	Vlan 20	192.168.20.0
VMnet12	Vlan 30	192.168.30.0
VMnet13	Vlan 40	192.168.40.0
VMnet14	Lan 1	172.16.1.0
VMnet15	Lan 2	172.16.2.0
VMnet16	Lan3	172.31.0.0

Tableau V.5 les carte réseaux utilisées

V.7 Les tests

- **Vérification de la configuration des ports au mode trunk :**

Pour vérifier la configuration des interfaces trunk entre deux switches on tape la commande.

« Show interfaces trunk »

```
SWD1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       on               802.1q         trunking      1
Et0/2       on               802.1q         trunking      1
Et0/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094
Et0/2       1-4094
Et0/3       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1
Et0/2       1
Et0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       1
Et0/2       1
Et0/3       1
```

- **Vérification de la configuration de VTP :**

Pour vérifier la configuration de serveur VTP sur le commutateur de distribution et le client VTP sur le commutateur client, on tape la commande « **show VTP status** »

```
SWD1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : sonatrach.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 7-5-22 10:27:37
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 2
MD5 digest                      : 0xC8 0x0E 0x32 0xE5 0x82 0x15 0xA6 0x9D
                                  0x50 0x16 0x25 0x6A 0xB9 0x6E 0x36 0x26
```

- **Vérification de la configuration des VLANs :**

Pour vérifier la configuration des VLANs on exécute la commande « show vlan brief ».

```
SWD1#show  vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Et1/0, Et1/1, Et1/2, Et1/3
                                                   Et2/0, Et2/1, Et2/2, Et2/3
                                                   Et3/0, Et3/1, Et3/2, Et3/3
10   DATA                                active
20   voice                               active
30   gestion                             active
40   serveurs                            active
99   native                              active
1002 fddi-default                        act/unsup
1003 trcrf-default                       act/unsup
1004 fddinet-default                     act/unsup
1005 trbrf-default                       act/unsup
SWA1#show  vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Et0/1, Et0/2, Et0/3, Et1/0
                                                   Et1/1, Et1/2, Et1/3, Et2/0
                                                   Et2/1, Et2/2, Et2/3, Et3/0
                                                   Et3/1, Et3/2, Et3/3
10   DATA                                active
20   voice                               active
30   gestion                             active
40   serveurs                            active
99   native                              active
1002 fddi-default                        act/unsup
1003 trcrf-default                       act/unsup
1004 fddinet-default                     act/unsup
1005 trbrf-default                       act/unsup
```

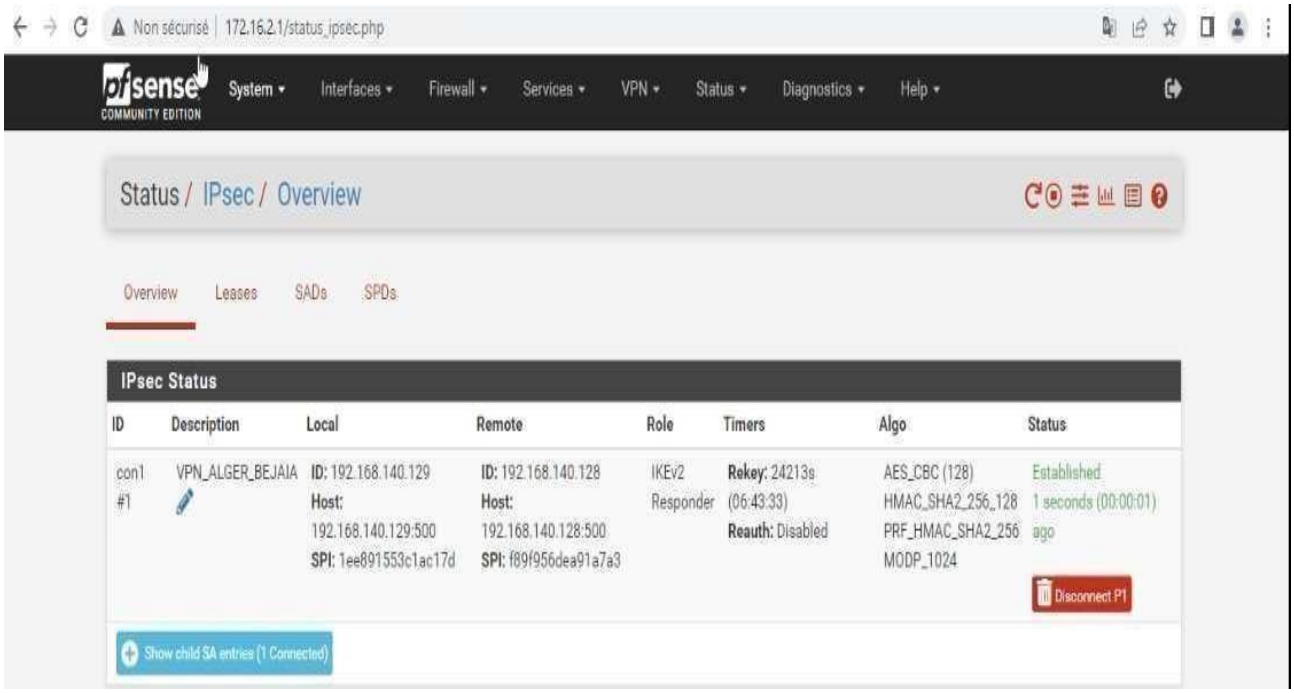
Vérification de la création des vlan coté serveur

Vérification de la création des vlan coté Clients

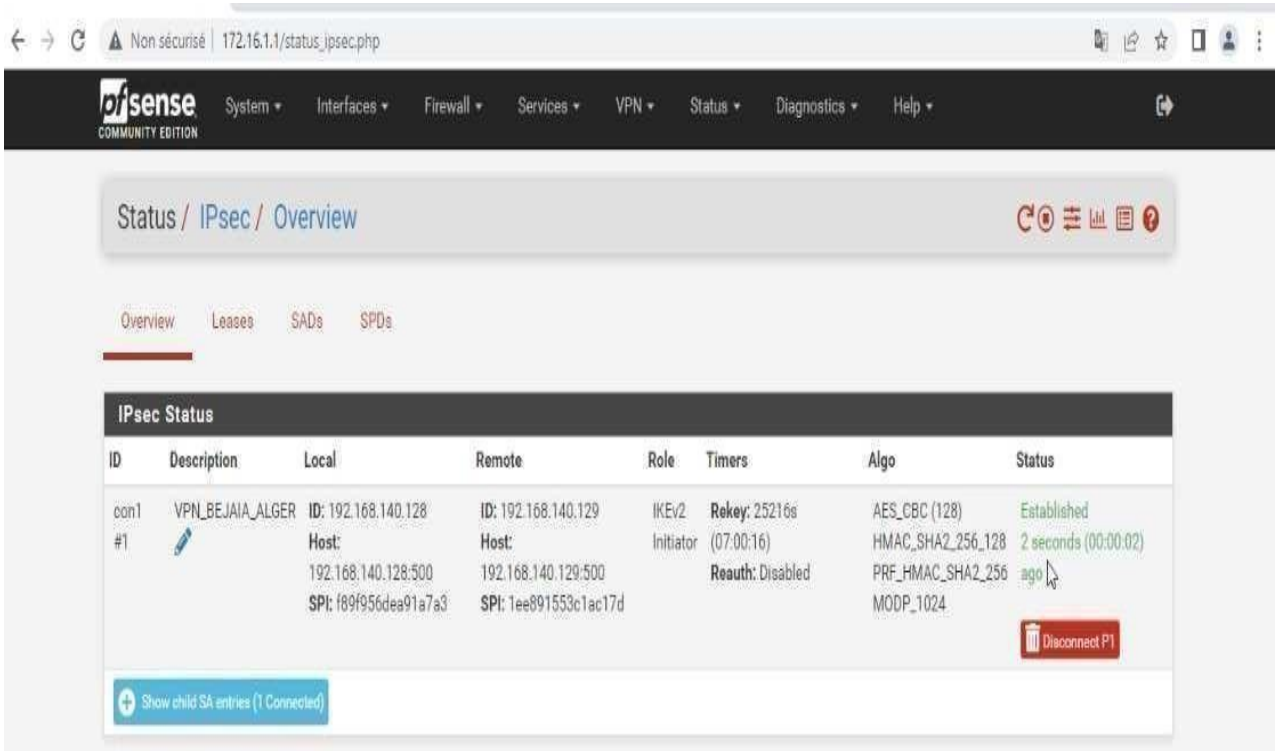
```
SWA1#show  vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Et0/3, Et1/0, Et1/1, Et1/2
                                                   Et1/3, Et2/0, Et2/1, Et2/2
                                                   Et2/3, Et3/0, Et3/1, Et3/2
                                                   Et3/3
10   DATA                                active    Et0/1, Et0/2
20   voice                               active    Et0/1, Et0/2
30   gestion                             active
40   serveurs                            active
99   native                              active
1002 fddi-default                        act/unsup
1003 trcrf-default                       act/unsup
1004 fddinet-default                     act/unsup
1005 trbrf-default                       act/unsup
SWA1#
```

V.7.1 Vérification des pares-feux :

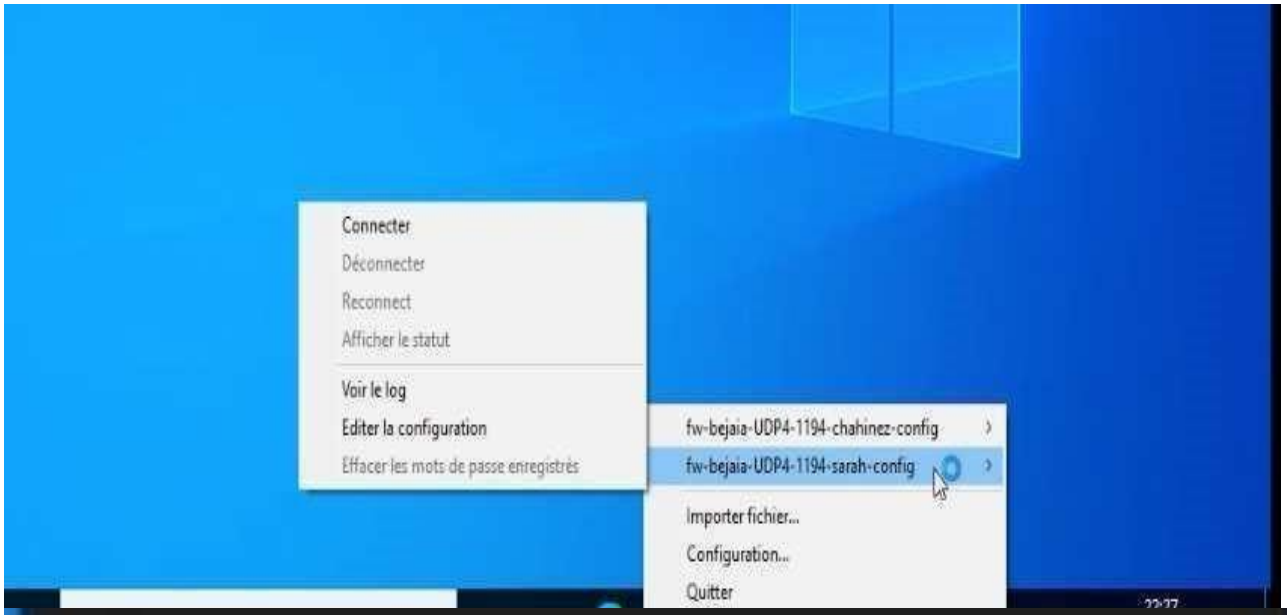
- **IPsec VPN sur PFsense ALGER**

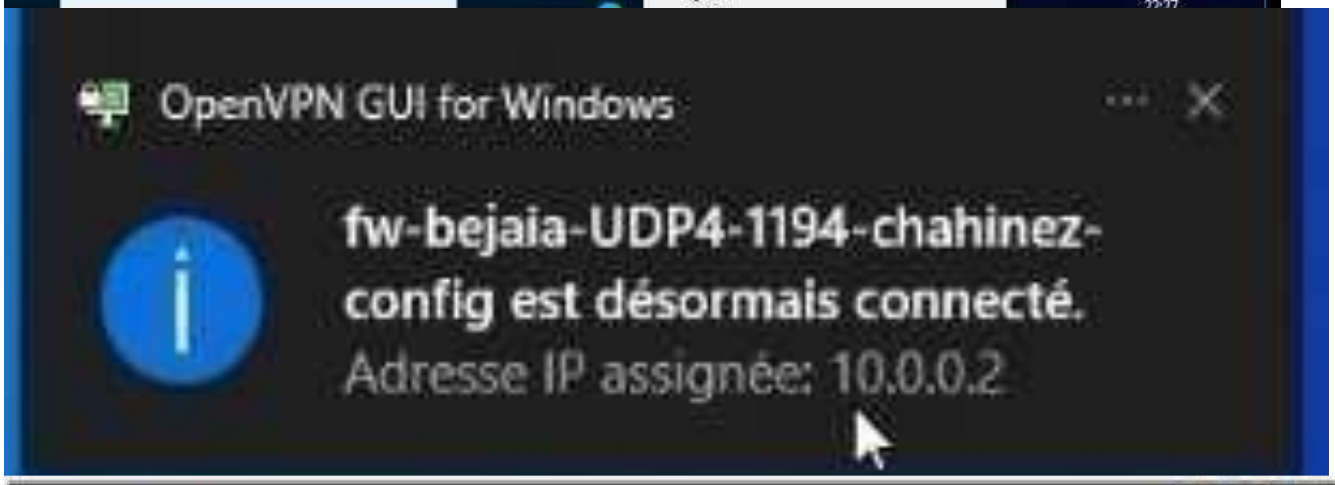


- **IPsec VPN sur PFsense BEJAIA :**



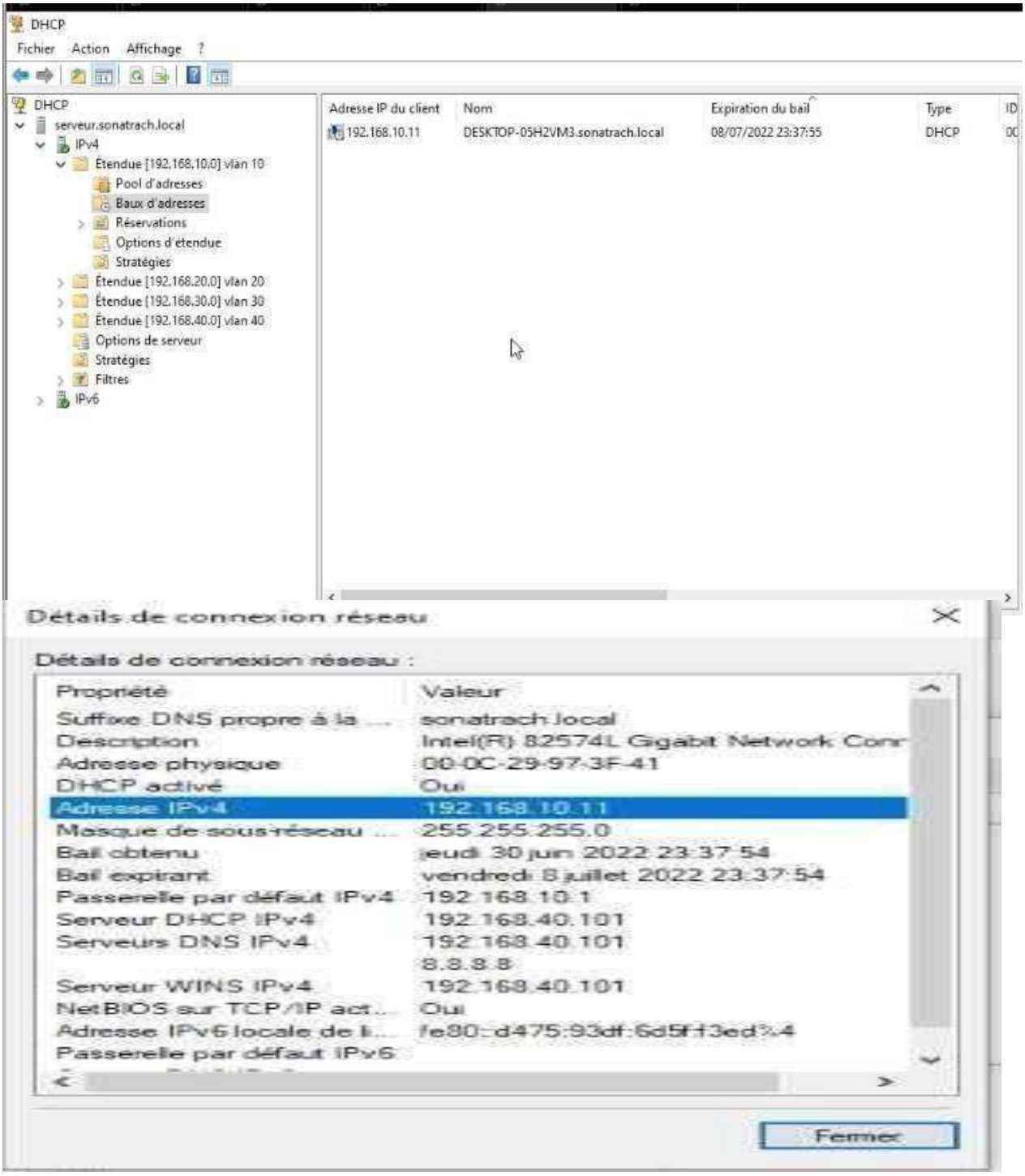
V.7.2 VPN mobile :





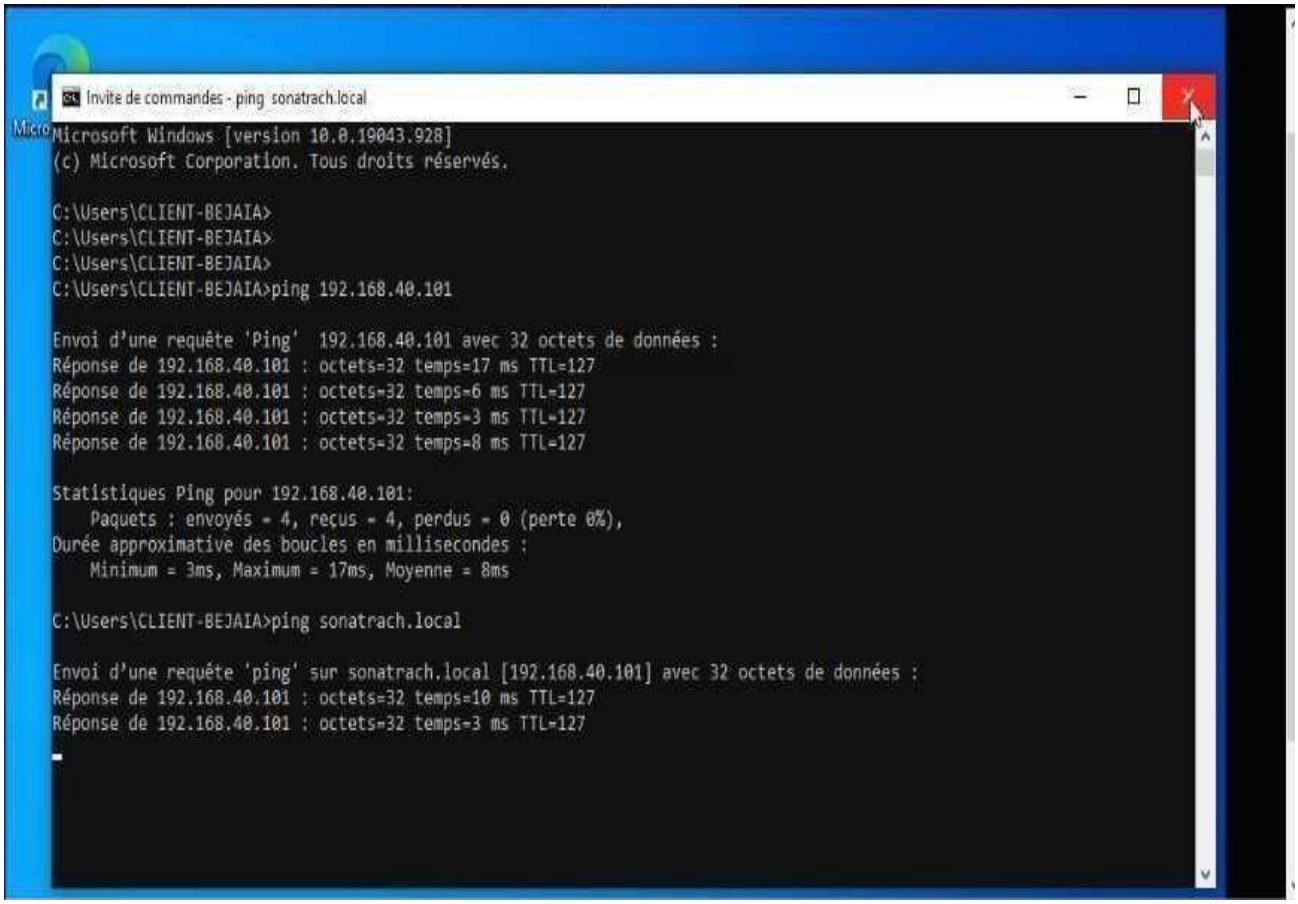
V.7.3 Teste DHCP :

Notre DHCP nous a donné une adresse pour le VLAN 10

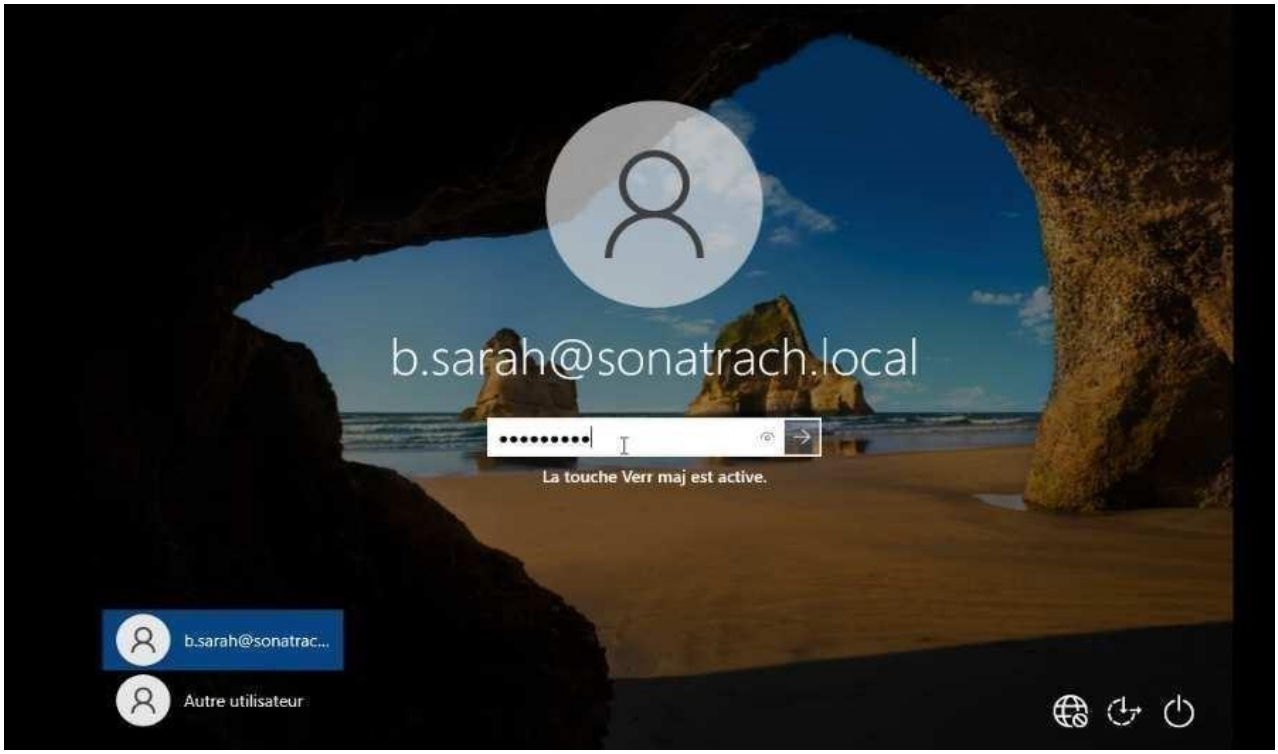


V.7.4 Serveur AD :

- Ping



Après la création des utilisateurs dans le pc BEJAIA on visuelle la figure suivante :



V.7.5 Vérification FreePBX :

V.7.5.1 Ping IAX2 entre deux site

```
[root@freepbx ~]# asterisk -rvv
Asterisk 16.25.0, Copyright (C) 1999 - 2021, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 16.25.0 currently running on freepbx (pid = 2270)
freepbx*CLI> iax2 show peers
Name/Username    Host                                    Mask
     Port          Status      Description
pbx1_to_pbx2/pb  192.168.40.100                    (S)  255.255.255.255
     4569      (E)  OK (22 ms)
pbx2_to_pbx1     192.168.40.100                    (S)  255.255.255.255
     4569          OK (36 ms)
2 iax2 peers [2 online, 0 offline, 0 unmonitored]
freepbx*CLI>
```

V.7.5.2 Interconnexion ente deux site

V.7.5.3 Test en local (site ALGER)

:

V.7.5.4 Test client to (site BEJAIA) :

V.8 Conclusion :

Dans ce chapitre nous avons présenté la phase de réalisation de notre projet en présentant la solution mise en place, la démarche de travail, les configurations et les implémentations effectuées.

Enfin des tests sont effectués avec succès entre deux sites Alger et Bejaia.

Conclusion générale

L'interconnexion des sites via VPN est une technologie en voie de développement, elle est plus qu'une nécessité économique pour les entreprises. En effet, elle permet un accès sécurisé à distance. Elle présente de nombreux avantages tels que, sa facilité d'implémentation et sa transparence vis-à-vis des utilisateurs. Elle peut intégrer divers services comme la téléphonie sur IP.

Cette dernière permet de faire la communication autour d'un seul protocole IP. C'est ainsi que les entreprises optent pour cette solution afin de réduire leurs investissements et également optimiser leur système d'information.

En plus, la VOIP englobe d'autres fonctionnalités que la simple voix. Par conséquent, nous avons fixé comme objectif de faire une étude de trouver les différentes solutions et techniques en tenant compte de l'existant au sein de l'entreprise Sonatrach.

Sonatrach dispose de plusieurs sites distants. Et chaque site possédé deux architectures différents (téléphonique et informatique). C'est pour cela, que nous avons proposé comme solution la mise en place d'une technologie de VPN pour relier les deux sites et en plus solution la mise en place d'une technologie de VPN pour relier les deux sites et en plus l'intégration de la téléphonie sur IP pour unifier le réseau et améliorer les communications.

Notre solution a été testée sur un tunnel VPN IPsec entre les deux sites Alger et Bejaia et avec le logiciel OpenVPN pour les accès à distance via internet, ceci nous a montré qu'il est possible d'implémenter cette solution pour répondre à notre principal problème.

La réalisation de ce projet nous a permis d'acquérir de nouvelles connaissances sur les protocoles de la TOIP telle que le protocole SIP et IAX d'une part et les protocoles de sécurité d'autre part grâce a une étude détaillée sur leurs fonctionnements et leurs principes. Comme perspectives, l'étape suivante sera dédiée à l'application, comme il serait intéressant d'étendre cette étude a d'autres entreprises.

Bibliographie

[1] : Cours-Les-reseaux-profs.pdf-Meutech

[2] : Mr Abed Amine et Mr Guenouna Abdelwahab. (juin 2004) : La voix sur IP. Mémoire d'ingéniorat. Institut des télécommunications Abdelhafid boussouf-Oran

[3] : Maiga Malik et Faye Modou (juin 2004) : Téléphonie sur IP. Mémoire d'ingéniorat.Institut des télécommunications Abdelhafid boussouf-Oran

[4] ABDELLAOUI MOHAMMED EL AMIN,BENHAMOU ABOUBAKR , Application mobile de la voIP sur un réseau Wifi, Mémoire A L'UNIVERSITÉ DE TLEMCEN, en Juin 2014

[5] : https://fr.wikibooks.org/wiki/R%C3%A9seaux_TCP/IP,2020

[6] : STEPHANE SOUBEYRAND, 2016, ÉVOLUTION DU SYSTÈME VPN DE L'ENTREPRISE NETAPSYS, Conservatoire National des Arts et Métiers Centre Régional Rhône-Alpes Centre d'Enseignement de Lyon

[7] : Rahmani Tinhinan Sadaoui Fadhila, 2016/2017, Etude et mise en place d'un réseau VPN, UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU.

[8] Jacob NDWO MAYELE , Déploiement d'un cœur de réseau ip/mpls, cas de la banque centrale du congo,Université de kinshasa – Licence en génie informatique 2017.

[9] Eric BAHATI – SHABANI , Mise en place d'un réseau VPN au sein d'une entreprise . Cas de la BRALIMA Sarl en RDC, Institut supérieur de commerce Kinshasa –Licencé en réseaux informatiques 2011

[10] Romaric K. SOSSA, Etude et Déploiement d'un réseau de téléphonie sur IP. Cas d'utilisation du PABX logiciel Asterisk, MEMOIRE DE FIN DE FORMATION, UNIVERSITÉ D'ABOMEY-CALAVI,2009.

[11] J.Ben Salem, systèmes de communication, support de cours, institut supérieure des études technologies de Nabeul, 2014.

[12] La Telephonie Sur IP , Docstoc.com. , consulté le 24/05/2015 http://www.docstoc.com/docs/109707824/La-telephonie-sur-IP

[13] ,Telephonie_sur_IP , Laurent_Ouakil,_Guy_Pujolle , Groupe Eyrolles, 2007, ISBN : 978-2-212-12099-8 , Accueil - Éditions Eyrolles (editions-eyrolles.com) . consulté le 11/05/2015.

[14] S.BACHIRI, B. BELARBI, Déploiement d'une application de TOIP, Mémoire de fin d'études , Université Abou Bakr Belkaid– Tlemcen ,2015 .

[15] : http://www.frameip.com/voip/#7_-_Probleme_et_Qos/

[16] Romaric K. SOSSA, Etude et Déploiement d'un réseau de téléphonie sur IP. Cas d'utilisation du PABX logiciel Asterisk, MEMOIRE DE FIN DE FORMATION, UNIVERSITÉ D'ABOMEY-CALAVI,2009.

[17] Laurent Ouakil et Guy Pujolle, Téléphonie sur IP, 2ème édition EYROLLES

[18]http://www.architoip.com/toip-open-source/article-hackin9-toipopen-source-frameip-octobre-2008.pdf, Article : « La ToIP Open Source », consulté le 12/6/2009

[19]BEN FREDJ, 2006, « Logiciel de Mesure de la Performance d'un Service de Téléphonie sur IP »

[20] BELKHICHANE Ali ,TOUAHRI Karim,Interconnexion de deux serveurs Asterisk et miseen place de téléphonie et visiophonie sur IP.Cas d'étude : Faculté des sciences exactes et ses départements,Université Abderrahmane Mira de Bejaïa ,mémoire de fin d'étude, juin 2014

[21]: https://sonatrach.com/presentation

[22]: Code-Réseau-de-Transport-par-Canalisation_juin-2018

[23] La norme RFC 5456 de l'IETF définissant les caractéristiques du protocole IAX version 2.

[24] Eric BAHATI - SHABANI **,** MISE EN PLACE D'UN RESEAU VPN AU SEIN D'UNE ENTREPRISECas de la BRALIMA Sarl **,** Mémoire de Fin d'Etudes présenté et défendu en vue de l'obtention du titre de licencié en Informatique de Gestion**,** Institut supérieur de commerce Kinshasa - Licencié en réseaux informatiques 2011

[25] ipsec(internet protocole security , Centre Universitaire Nour Bachir , 2019-2020

[26] : G´enael VALET. Les LANs virtuels. Greta industriel de technologies avanc´ees, 2007.

[27] : type de vlan, . URL http://www-igm.univ-mlv.fr.

[28] : « Commutation et routage intermédiaire », CCNA 3 – Essentiel.

[29]G.PLaurent OUAKIL,Eyrolles,Téléphonie sur IP,2008 ed,paris.

Annexs :

IV.5.1 Installation de GNS3

Pour installer GNS3, vous devez d'abord télécharger l'exécutable, puis
Lancez et suivez les étapes d'installation jusqu'à la fin, puis cliquez sur le bouton Terminer.
La figure ci-dessous montre l'interface GNS3.

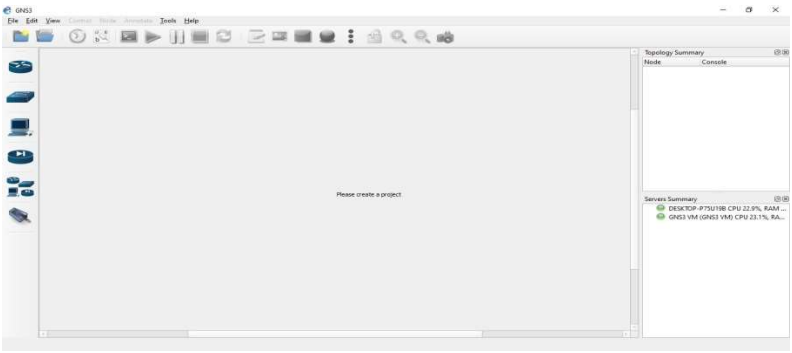


Figure IV.7 : Interface d'accueil GNS3

IV.5.2 Installation de VMware Workstation version 16.1.2

Afin de créer une machine utilisateur virtuelle sur le même ordinateur, nous devons installer VMware Workstation en suivant les étapes ci-dessous

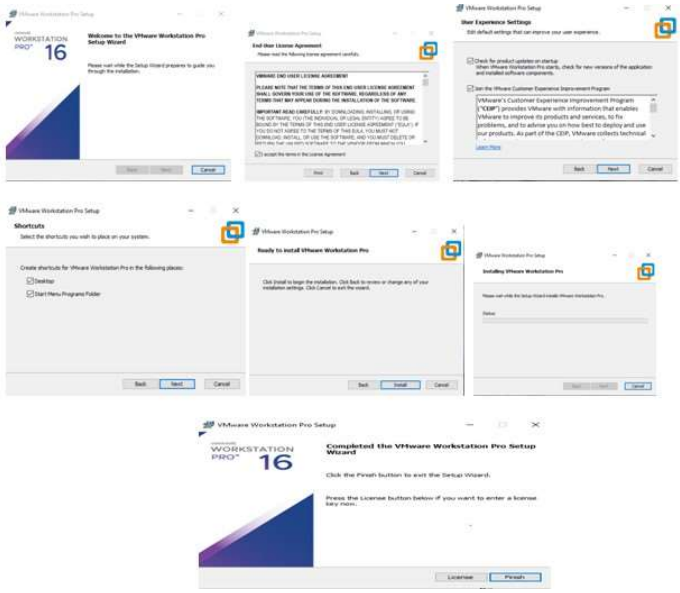
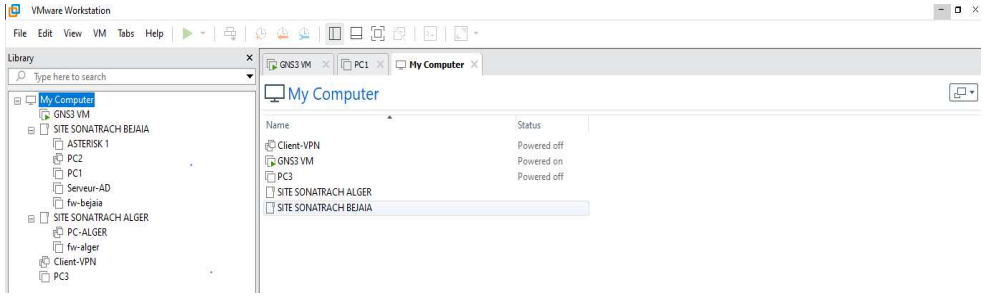


Figure IV.8 : Installation de VMware workstation

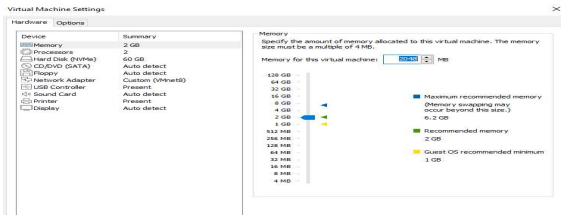
Après l'installation de VMware, la page d'accueil apparaîtra.



IV.5.3 Créer une machine virtuelle

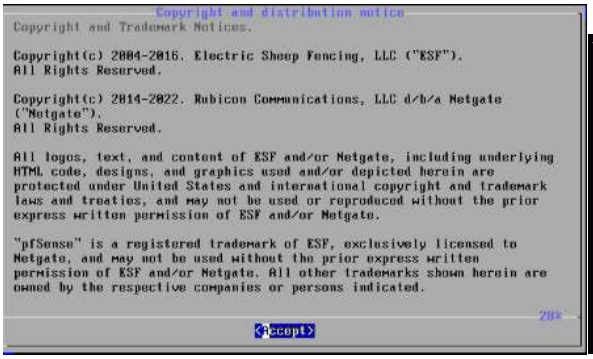
- **Installer Windows 10 sur VMware Workstation ;**

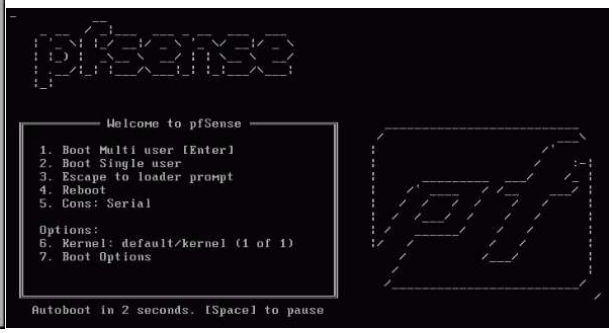
Après avoir ajouté l'image Windows 10 sur VMware, nous avons créé une machine. A qui on a attribué les caractéristiques suivantes :



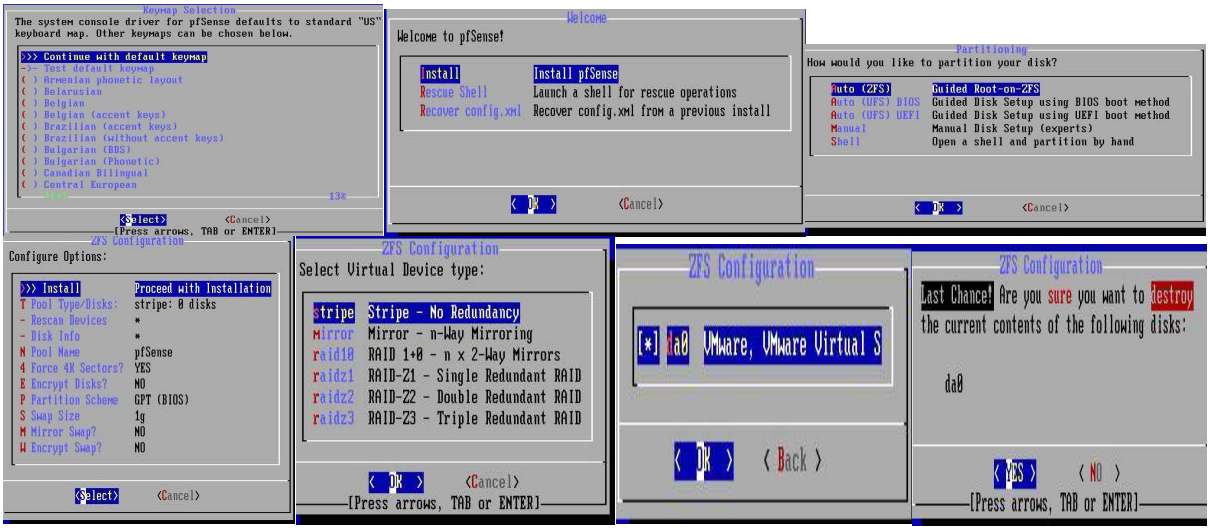
IV.5.4Installation PFSense sur VMware pour les deux site :

Démarrer la VM, Accepter la licence



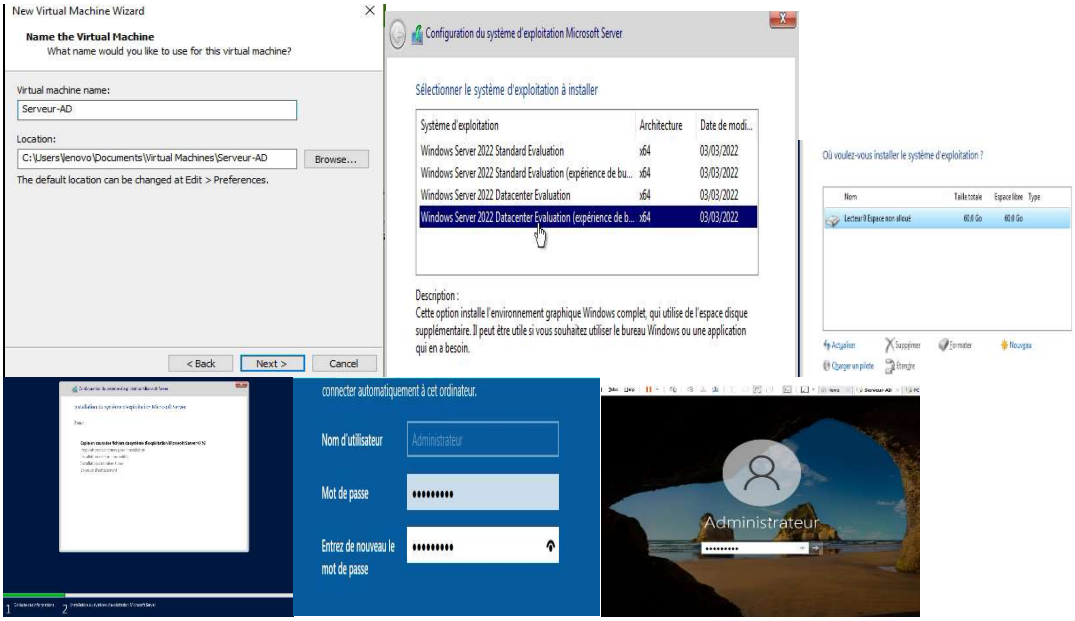


Install PFSense : OK



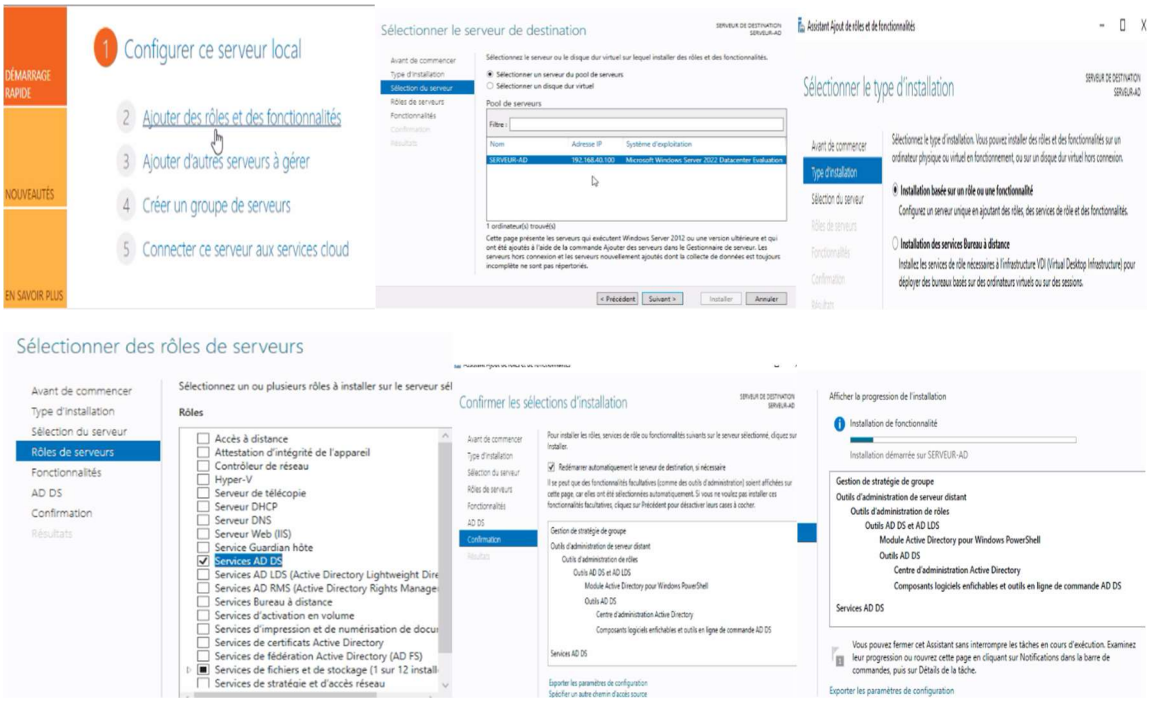
IV.5.6 installation de serveur 2022 :

Dans cette partie nous allons voir les différents étapes d'installation de Windows serveur 2022.



- **Installation de l'Active Directory (AD) :**

Sur la machine Windows serveur 2022 nous avons installé un controlleur de domaine dont le nom de domaine est sonatrach.local.
Pour commencer l'installation, il va falloir ajouter le Service de Role Active Directory.
Lancer l'installation et ajouter les fonctionnalités qui nous manquent.


DÉMARRAGE RAPIDE
NOUVEAUTÉS
EN SAVOIR PLUS
1 Configurer ce serveur local
2 Ajouter des rôles et des fonctionnalités
3 Ajouter d'autres serveurs à gérer
4 Créer un groupe de serveurs
5 Connecter ce serveur aux services cloud
Sélectionner le serveur de destination
Sélectionner le type d'installation
Sélectionner des rôles de serveurs
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Confirmation
Résultats
Rôles
Accès à distance
Attestation d'intégrité de l'appareil
Contrôleur de réseau
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Service Guardian hôte
Services AD DS
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume
Services d'impression et de numérisation de docu
Services de certificats Active Directory
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (1 sur 12 install
Services de stratégie et d'accès réseau
Confirmer les sélections d'installation
Afficher la progression de l'installation
Installation de fonctionnalité
Installation démarrée sur SERVEUR-AD
Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Module Active Directory pour Windows PowerShell
Outils AD DS
Centre d'administration Active Directory
Composants logiciels enfichables et outils en ligne de commande AD DS
Services AD DS
Exporter les paramètres de configuration