**République Algérienne Démocratique et Populaire**
**Ministère de l'Enseignement Supérieure et de la Recherche Scientifique**
**Université Abderrahmane Mira**
**Faculté de la Technologie**

**Département d'Automatique, Télécommunication et d'Electronique**

# Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

## Thème

**Etude et mise en place d'un serveur VoIP asterisk sur un réseau multisites sécurisée au sein de l'entreprise NTS**

**Préparé par :**

- BOUYAHIA Sami

**Dirigé par :**

M. BESSAAD Omar

**Examiné par :**

Mme S.GHENNAM(P)

Mme k.MAMMERI

**Année universitaire** : **2023/2024**

# Remerciements

**Avant tout, je remercie Dieu le Tout-Puissant pour la force, la volonté et la connaissance qui ont permis de mener à bien ce travail.**
**Mes sincères remerciements vont à mon encadrant, Mr O.BESSAAD, pour ses précieux conseils et encouragements tout au long de ce projet.**
**Je tiens également à remercier les membres du jury pour avoir accepté d'évaluer ce travail, en leur exprimant ma profonde gratitude et mon respect.**
**Mes remerciements les plus vifs s'adressent à mon encadrant de stage, M. Y. Djebbari, pour son accueil, son suivi et ses conseils durant toute la période de stage pratique.**
**Je remercie chaleureusement ma famille, notamment mes parents, mes sœurs, pour leurs encouragements, leur aide et leur soutien constants tout au long de ce travail.**
**Un grand merci à tous mes amis et collègues pour leur soutien, en particulier.**
**Enfin, je tiens à exprimer ma profonde gratitude à toutes les personnes ayant contribué, de près ou de loin, à la réalisation de ce projet. Leurs conseils, leur soutien et leurs encouragements ont été inestimables tout au long de ce parcours.**

# Dédicace

**J’ai le plaisir de dédier ce modeste travail ;**
**À mes chers parents, qu’ils trouvent ici toute ma gratitude pour leur soutien tout au long de mes études.**
**À mes chères sœurs Imane et Liza, pour leur amour et leur encouragement.**
**À ma chére amie Celia, pour ses conseils avisés et son amitié précieuse.**
**À tout mes amis , pour leur amitié sincère et leur soutien indéfectible.**

# Table des matières

# Table des figures

# Liste des tableaux

# Liste des abréviations

**AH** Authentication Header

**DHCP** Dynamic Host Configuration Protocol

**DNS** Domain Name System

**DoS** Denial of Service

**ESP** Encapsulating Security Payload

**IAX** Inter Asterisk eXchange

**IKE** Internet Key Exchange

**IP** Internet Protocol

**IPBX** Internet Protocol Private Branch eXchange

**IPSec** Internet Protocol Security

**ISAKMP** Internet Security Association and Key Management Protocol

**ISO** International Organization for Standardization

**LAN** Local Area Network

**L2TP** Layer 2 Tunneling Protocol

**NAT** Network Address Translation

**NTS** Nouvelles Technologies de l'information et Sécurité

**OSI** Open Systems Interconnection

**PABX** Private Automated Branch Exchange

**PPTP** Point-to-Point Tunneling Protocol

**PBX** Private Branch eXchange

**QoS** Quality of Service

**RTC** Réseau téléphonique commuté

**RTCP** Real-time Transport Control Protocol

**RTP** Real-time Transport Protocol

**SIP** Session Initiation Protocol

**TCP** Transmission Control Protocol

**ToIP** Telephony over Internet Protocol

**UDP** User Datagram Protocol

**VLAN** Virtual Local Area Network

**VoIP** Voice over Internet Protocol

**VPN** Virtual Private Network

**VTP** VLAN Trunking Protocol

**WAN** Wide Area Network

# Introduction générale

Actuellement, le développement de la technologie de transmission vocale via le protocole IP (Internet Protocol) joue un rôle central dans la transformation du secteur des communications.

Autrefois, la seule option de communication disponible était le service téléphonique traditionnel, ou RTC (Réseau Téléphonique Commuté). L'émergence de la VoIP (Voice over Internet Protocol), une technologie révolutionnaire, a changé la manière dont les communications vocales sont réalisées, en offrant une alternative aux systèmes de téléphonie traditionnels. En utilisant les infrastructures Internet existantes, la VoIP a ouvert de nouvelles possibilités pour les particuliers, les entreprises et les institutions, offrant une flexibilité, une efficacité et des économies sans précédent.

Avec la VoIP, les entreprises peuvent fusionner leurs réseaux informatiques et téléphoniques en un seul réseau. Cette avancée technologique simplifie ainsi les opérations et réduit significativement les coûts de communication.

Les systèmes VoIP proposent une variété de services selon différents modes de communication, tels que PC à PC ou PC à téléphone. En intégrant des outils d'interface pour les réseaux téléphoniques traditionnels, cette technologie est devenue un outil de communication via Internet. Elle utilise des protocoles spécialement conçus pour ce type d'application, comme le RTP (Real-time Transport Protocol), qui fonctionne en conjonction avec des protocoles de signalisation tels que le SIP (Session Initiation Protocol) et l'IAX (Inter-Asterisk eXchange).

Cependant, l'apparition de la VoIP présente des défis en matière de sécurité, car elle combine les vulnérabilités de la téléphonie classique avec celles des réseaux informatiques. Ainsi, lorsqu'une entreprise ou un particulier adopte une solution VoIP, ils peuvent être exposés à de nouveaux risques.

Étant donné l'intégration étroite avec l'infrastructure informatique, il est crucial de sécuriser les flux vocaux lors de la gestion des systèmes et des périphériques. Avec l'émergence des solutions IP, l'importance de la sécurité et de la fiabilité est accrue. En résumé, plus la sécurité est renforcée, moins les risques sont élevés.

Pour approfondir et appliquer mes connaissance théoriques de la VoIP acquises durant mes études, j'ai choisi d'effectuer un stage pratique chez Campus NTS (Nouvelles Technologies de l'Information et Sécurité), une entreprise spécialisée dans l'étude, la conception et la réalisation de solutions pour ses clients.

**Le présent mémoire est structuré comme suit :**

- **Chapitre 1 : État de l'art sur la VoIP** Ce chapitre présente une vue d'ensemble de la technologie VoIP, son fonctionnement, ses avantages et inconvénients, ainsi que les différents protocoles utilisés.
- **Chapitre 2 : Différentes attaques et méthodes de sécurité de VoIP** Dans ce chapitre, nous examinerons les diverses menaces et vulnérabilités auxquelles la VoIP est exposée. Nous aborderons également les méthodes et solutions de sécurité permettant de protéger les communications VoIP.
- **Chapitre 3 : Présentation de l'entreprise d'accueil et du client** Ce chapitre est dédié à la présentation de l'entreprise d'accueil, Campus NTS, ainsi que du client pour lequel le projet a été réalisé. Nous détaillerons leurs besoins, attentes et les solutions proposées.

# Chapitre 1

# Etat de l’art sur la VOIP

## 1.1 Introduction

Dans ce chapitre, nous allons concentrer sur l'étude approfondie de la technologie VoIP et de ses divers aspects. Nous étudierons en détail l'architecture de la VoIP, ses éléments constitutifs et son principe de fonctionnement. Nous décrirons également les protocoles de signalisation et de transport de la VoIP, en expliquant leurs principes de fonctionnement et en identifiant leurs avantages et inconvénients principaux.

### 1.1.1 Définition

La VoIP (Voice over Internet Protocol) est une technologie qui permet de transmettre la voix et méme d'autres données multimédias sur Internet au lieu des réseaux de téléphonie traditionnels, ce qui signifie que les appels téléphoniques sont acheminés via Internet plutôt que par des lignes téléphoniques traditionnelles. Les services de VoIP peuvent inclure des fonctionnalités telles que la possibilité de passer et recevoir des appels vocaux ou appels vidéos, d'envoyer des messages texte et d'autres services de communication en utilisant Internet comme support de transmission. La VoIP est souvent utilisée pour réduire les coûts de communication nationale ou internationale, améliorer la qualité des appels et offrir des fonctionnalités avancées telles que la messagerie vocale, la visioconférence et l'intégration avec d'autres applications informatiques. [1]

### 1.1.2 Avantages

**Coût Réduit :** L'un des avantages les plus évidents de la VoIP est son coût réduit par rapport aux lignes téléphoniques traditionnelles. Les appels internationaux et longue distance sont considérablement moins chers, ce qui peut permettre des économies substantielles, surtout pour les entreprises. [1]

**Flexibilité :** La VoIP offre une grande flexibilité. Vous pouvez effectuer des appels depuis n'importe quel endroit avec une connexion Internet, ce qui est idéal pour les travailleurs à distance et les voyageurs d'affaires. De plus, la plupart des systèmes VoIP offrent des fonctionnalités avancées telles que la messagerie vocale, la vidéoconférence et la messagerie instantanée. [1]

**Fonctionnalités avancées :** La VoIP propose une gamme de fonctionnalités avancées, comme la redirection d'appels, le suivi des appels, la gestion des appels en attente, la conférence téléphonique et plus encore. Ces fonctionnalités peuvent améliorer la productivité et l'efficacité des entreprises. [1]

**Évolutivité :** La VoIP est facilement évolutive. Vous pouvez ajouter ou supprimer des lignes téléphoniques en fonction des besoins de votre entreprise, ce qui en fait une solution idéale pour les petites entreprises en croissance. [1]

### 1.1.3 Inconvénients

**Dépendance à l'Internet :** L'un des principaux inconvénients de la VoIP est sa dépendance à une connexion Internet stable. Si votre connexion est lente ou instable, la qualité des appels peut en souffrir, avec des interruptions et une mauvaise qualité audio. [1]

**Alimentation électrique** Contrairement aux téléphones traditionnels qui fonctionnent même en cas de panne de courant, la VoIP nécessite une alimentation électrique constante. En cas de panne de courant ou de défaillance électrique, vous risquez de perdre la communication. [1]

**Qualité de service** La qualité des appels VoIP peut varier en fonction de divers facteurs, notamment la bande passante, la congestion du réseau et la qualité des équipements. Il est essentiel de s'assurer que votre réseau est configuré pour fournir une qualité de service optimale. [1]

## 1.2 Principe de fonctionnement

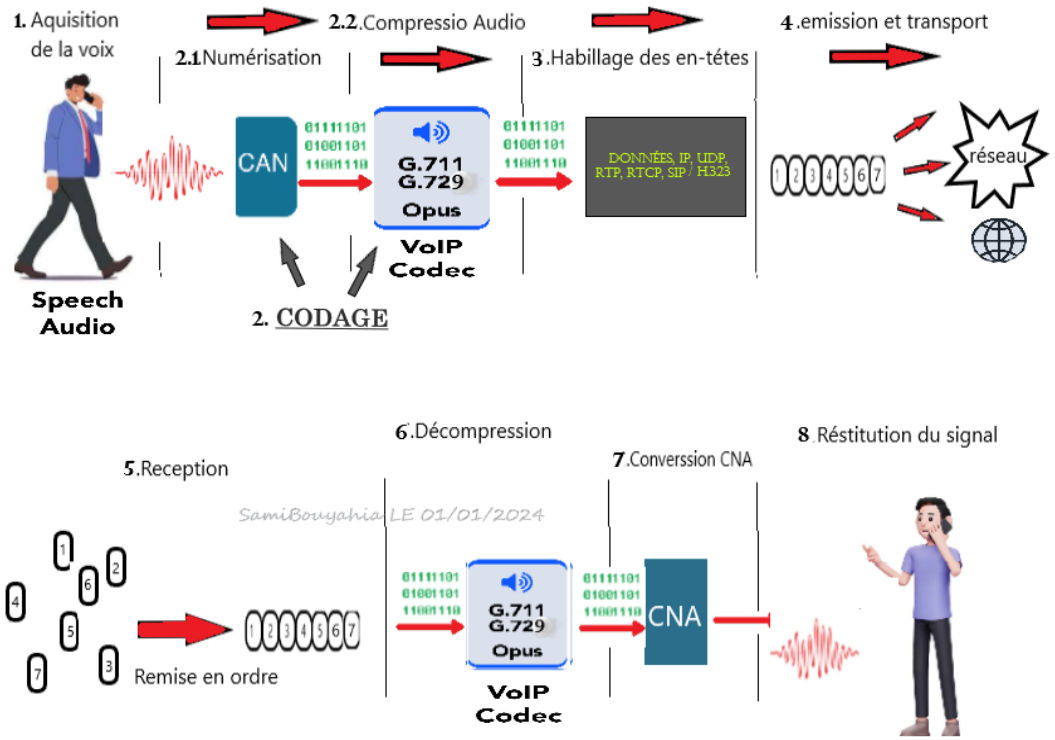


FIGURE 1.1 – Principe de fonctionnement

### 1.2.1 Acquisition du signal

La première étape consiste à capter la voix à l'aide d'un microphone. [2]

### 1.2.2 CODAGE

**Numérisation** La voix passe dans un convertisseur analogique numérique qui réalise deux tâches distinctes [2] :

- Échantillonnage du signal sonore : un prélèvement périodique de ce signal, il s'agit d'enregistrer à des intervalles trés rapprochés la valeur d'un signal afin de pouvoir disposer d'un enregistrement proche de la valeur réelle de ce signal. [2]

- Quantification : qui consiste à affecter une valeur numérique (en binaire) à chaque échantillon. [2]

**Compression du signal** Le signal une fois numérise peut être traité par codecs de compression, c'est-à-dire réduire la quantité d'informations nécessaire pour l'exprimer. L'avantage de la compression est de réduire la bande passante nécessaire pour transmettre le signal. [2]

### 1.2.3 Habillage des-en-têtes

Les données doivent encore être enrichies en informations avant d'être converties en paquets de données à expédier sur le réseau. Càd inclure l'ajout d'informations spécifiques nécessaires pour le routage, le suivi de la qualité, ou d'autres fonctions liées à la transmission audio en temps réel. [2]

### 1.2.4 Emission et transport

Les paquets sont acheminés depuis le point d'émission pour atteindre le point de réception sans qu'un chemin précis soit réserve pour leur transport. Le transport se fait avec des protocoles dédier. [2]

### 1.2.5 Réception

Lorsque les paquets arrivent à destination, il est essentiel de les replacer dans le bon ordre et assez rapidement. Faute de quoi une dégradation de la voix se fera sentir. [2]

### 1.2.6 décompression

Les données vocales compressées sont décompressées après Identification du Codec, en fonction de l'algorithme spécifié par le codec. Cette étape vise à restaurer les données à leur format audio d'origine tout en minimisant la perte de qualité. [2]

### 1.2.7 Conversion numérique analogique

La conversion numérique analogique est l'étape réciproque de la numérisation. [2]

### 1.2.8 Restitution

Le signal analogique est ensuite amplifié et reproduit par des haut-parleurs, permettant à l'utilisateur d'entendre la voix de l'appelant. [2]

## 1.3 Architectures et modes d'accès :

### 1.3.1 Architectures :

**Centrex :** L'architecture Centrex repose sur la centralisation des fonctionnalités de téléphonie IP. Les services de téléphonie sont hébergés sur un serveur distant géré par un fournisseur de services. Les utilisateurs se connectent au serveur à partir de leurs téléphones IP et bénéficient de fonctionnalités avancées telles que la messagerie vocale, le renvoi d'appels et les conférences téléphoniques . [3]

**Hybrid :** L'architecture hybride combine à la fois des éléments de la téléphonie IP et de la téléphonie traditionnelle. Elle permet une transition progressive vers la téléphonie IP en intégrant les systèmes existants. Par exemple, une entreprise peut conserver ses lignes téléphoniques traditionnelles tout en ajoutant des téléphones IP pour profiter des fonctionnalités avancées de la téléphonie IP. Cela offre une flexibilité aux utilisateurs tout en minimisant les perturbations. [3]

**Full IP :** L'architecture Full IP est une approche entièrement basée sur la téléphonie IP, où tous les appareils de communication, y compris les téléphones et les systèmes, sont connectés directement à Internet. Cette architecture offre une flexibilité totale, une évolutivité et une intégration transparente avec d'autres services IP, tels que la visioconférence et la messagerie instantanée. [3]

### 1.3.2 Modes d'accées :

**PC à PC :** L'une des formes les plus courantes d'accès à la téléphonie IP est l'appel de PC à PC. En utilisant un logiciel de téléphonie, les utilisateurs peuvent passer des appels vocaux directs d'un ordinateur à un autre, en utilisant simplement un casque et un microphone. Cette méthode est pratique pour les appels internationaux et les communications entre collègues ou amis. [3]

**De PC à téléphone :** Grâce au logiciel de téléphonie SIP, il est également possible de passer des appels depuis votre ordinateur vers un téléphone traditionnel. En utilisant un adaptateur de téléphonie IP (ATA) connecté à votre ordinateur, les signaux vocaux sont convertis en signaux téléphoniques compatibles, permettant ainsi de communiquer avec des utilisateurs qui n'utilisent pas directement la téléphonie IP. [3]

**De téléphone à téléphone :** Avec la téléphonie IP, il est possible d'établir des appels vocaux d'un téléphone IP à un autre téléphone IP. Ces téléphones sont spécialement conçus pour se connecter directement à Internet et utiliser le protocole SIP pour établir et gérer les appels. Cela permet une communication de haute qualité entre utilisateurs, sans nécessiter d'adaptateurs supplémentaires. [3]

## 1.4 Différence entre VoIP et ToIP (Téléphonie sur IP) :

La ToIP et la VoIP sont deux technologies proches mais pourtant distinctes. Les deux utilisent le protocole internet IP, mais leur mode de fonctionnement diffère. La VoIP transforme la voix en fichiers numériques, qu'elle envoie sous forme de paquets sur un réseau de données (par exemple Internet) au travers de lignes IP. Elle regroupe l'ensemble des techniques permettant ce transit : d'un téléphone IP à un PC ou un téléphone normal, ou encore d'un ordinateur à un autre sur les réseaux internes et externes d'une entreprise.

La ToIP est quant à elle un système de téléphonie basé sur la VoIP, qui se limite au réseau IP local. Elle utilise un simple routeur créant la connexion entre le réseau LAN (société) et le réseau WAN (opérateur) : l'IPBX.

La ToIP regroupe tous les échanges entre deux téléphones IP, ou encore entre deux ordinateurs utilisant le même logiciel.

La VoIP offre des applications et services multiples au-delà de la simple téléphonie : visioconférence sur IP, messageries vocales unifiées, etc. Cette technologie permet une convergence entre la voix, la vidéo et les données. [4]

## 1.5 Différence entre PABX et IPBX :

Le PABX (Private Automatic Branch Exchange) et l'IPBX (Internet Protocol Branch Exchange) sont deux types de systèmes téléphoniques privés utilisés par les entreprises pour gérer automatiquement les appels téléphoniques. La principale différence entre les deux est la technologie utilisée pour acheminer les appels.

Le PABX est un autocommutateur traditionnel qui utilise des lignes téléphoniques analogiques ou numériques pour acheminer les appels, il est installé sur un site et nécessite un câblage dédié pour connecter les téléphones aux lignes téléphoniques. Le PABX offre des fonctionnalités de base telles que la mise en attente des appels, la transfert d'appel et la gestion des files d'attente.

L'IPBX, en revanche, est un autocommutateur qui utilise le protocole IP pour acheminer les appels téléphoniques. L'IPBX peut être installé sur un site ou dans le cloud et permet aux entreprises de connecter des téléphones IP (téléphones qui se connectent directement à Internet) ou des téléphones analogiques via un adaptateur téléphonique IP.

L'IPBX offre des fonctionnalités avancées supplémentaires par rapport au PABX telles que la messagerie vocale unifiée, la visioconférence et la gestion centralisée des téléphones. Il peut être géré à distance, ce qui en fait un choix populaire pour les entreprises qui cherchent à moderniser leur infrastructure téléphonique.

## 1.6 Les protocoles de la VoIP

### 1.6.1 Protocoles de signalisation

**H.323 :** est un protocole de communication en temps réel développé par l'Union internationale des télécommunications (UIT) pour le traitement et la signalisation des données multimédias avec de fortes contraintes temporelles, comme la voix et la vidéo sur des réseaux IP.

Le protocole H.323 utilise un ensemble de protocoles pour permettre la communication entre les terminaux, les passerelles et les réseaux. Les protocoles comprennent le protocole H.225 pour la signalisation de l'appel, la synchronisation, la mise en paquets des données et l'enregistrement auprès d'un Gatekeeper, le protocole H.245 Pour la négociation des codecs ainsi l'ouverture et la fermeture des canaux, le protocole RAS (Registration/Admission/Status) pour la communication avec le Gatekeeper, il permet le contrôle d'admission et la gestion de la bande passante, et enfin les protocoles de transport en temps réel RTP et RTCP pour le transport des données multimédia. [5]

**SIP :** Est un protocole de signalisation qui assure l'établissement, le maintien, la modification, la gestion et la fermeture de sessions interactives entre utilisateurs pour la téléphonie et la vidéoconférence, et plus généralement pour toutes les communications multimédias. Il se situe au niveau de la couche applicative du modèle de référence OSI et fonctionne selon une architecture client-serveur, le client émettant des requêtes et le serveur exécutant en réponse les actions sollicitées par le client. [6]

SIP fournit des fonctions annexes évoluées, comme la redirection d'appel, la modification des paramètres associés à la session en cours ou l'invocation de services. En fait, SIP ne fournit pas l'implémentation des services, mais propose des primitives génériques permettant de les utiliser. De cette manière, l'implémentation des services est laissée libre, et seul le moyen d'accéder aux services est fourni. [6]

**IAX (Inter-Asterisk eXchange) :** Est un protocole de signalisation utilisé dans les systèmes de téléphonie sur IP (VoIP) basés sur le logiciel libre Asterisk. Il a été conçu pour faire transiter voix et vidéo sur des débits plus faibles en utilisant un seul port de communication UDP pour les données et la signalisation. [7]

### 1.6.2 Protocoles de transport

**Protocoles de transport Standards** sont TCP (Transmission Control Protocol) et UDP (User Datagram Protocol)

**TCP** Le protocole TCP implémente plusieurs mécanismes de contrôle :

- **Contrôle de séquence.** [6]
- **Contrôle de flux.** [6]
- **Contrôle d'erreur.** [6]

- **Contrôle de congestion.** [6]

Toutes ces mécanismes assurent un service de transport fiable, mais posent globalement deux problèmes. D'une part, elles engendrent un surplus de données important. D'autre part, ce n'est pas la fiabilité qui est l'élément le plus important dans les communications temps réel, mais le temps. [6]

La figure suivante illustre ce qui ne devrait pas se produire. Alice envoie trois messages à Brigitte, contenant respectivement les mots « bonjour », « à », « tous » (il s'agit bien sûr d'un cas d'école, le découpage réel des trames se faisant à la durée et non au mot). Imaginons que seuls les mots « bonjour » et « tous » soient reçus par Brigitte. [6]

Avec le protocole TCP, une réémission du mot « à » va être effectuée par le terminal d'Alice, une fois le temporisateur de réémission écoulé. Comme il s'agit d'une conversation téléphonique, le terminal de Brigitte doit diffuser les messages reçus immédiatement (en fait un système de cache permet de réduire plus ou moins cet effet, mais sans pallier le problème pour autant puisqu'il n'offre qu'un délai supplémentaire limité). [6]

Si l'application a délivré les deux mots reçus, il ne sert à rien de retransmettre le mot manquant par la suite, car celui-ci sera décorrélé de la conversation. Sa diffusion auprès du récepteur produira une perturbation plutôt qu'une amélioration. En outre, si un message est perdu, il est probable que la cause en soit la forte charge du réseau. En sollicitant une réémission de la trame, on accentue la charge et l'engorgement du réseau Il est donc préférable de perdre définitivement le paquet plutôt que de le réémettre. [6]

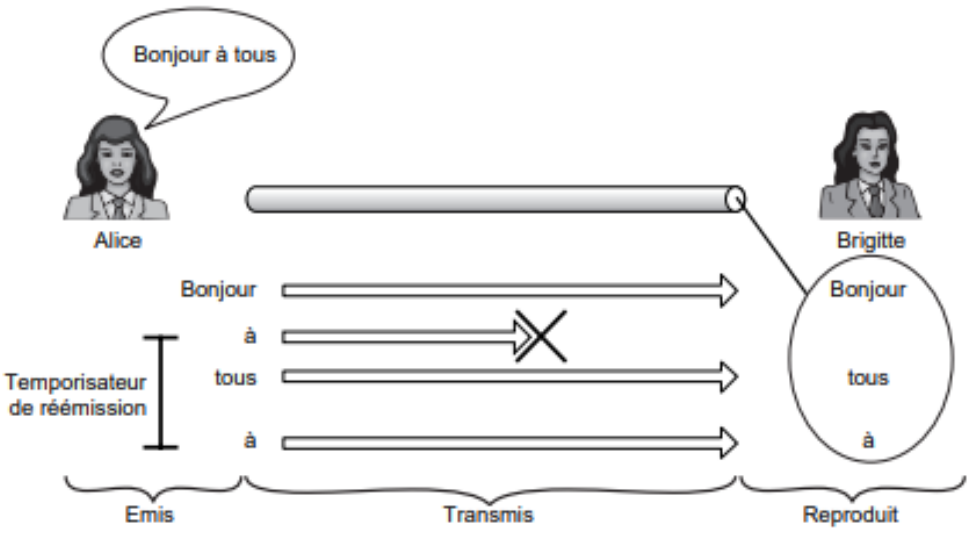


FIGURE 1.2 – Réémission avec TCP [6])

**UDP** Le protocole UDP ne comporte que des fonctionnalités de transport pur, sans aucun mécanisme de contrôle. L'adressage des données avec les ports de communication utilisés est sa seule fonction fondamentale. C'est un atout par rapport aux éléments contraignants mentionnés pour le protocole TCP. UDP est ainsi notablement plus rapide que ne l'est TCP. [6]

Mais la simplicité de ce modèle devient rapidement limitative. En particulier, UDP ne dispose d'aucun mécanisme lui permettant de reconstituer l'ordre des flux auprès du récepteur. Les datagrammes UDP sont totalement épurés, et aucune estampille d'horodatage, ni de numérotation n'y est insérée. Or, dans un réseau IP, les paquets peuvent emprunter des chemins différents. Avec le seul protocole UDP, la séquence temporelle originale ne peut être reconstituée au récepteur. [6]

**En résumé** Des deux protocoles candidats au transport des données multimédias, TCP est « trop complet » et UDP trop limité. Il est cependant possible de partir du protocole UDP et de lui ajouter des fonctionnalités d'ordonnancement. Le protocole RTP a été proposé à cette seule fin de reconstitution de l'ordre du flux d'origine. Pour sa part, RTCP a été conçu pour offrir une vision de l'état du réseau et permettre à une application d'adapter les flux en conséquence. [6]

### Protocoles de transport Multimédia

**Les protocoles RTP et RTCP** Comme indiqué précédemment, le couple de protocoles RTP/RTCP a été conçu dans le but d'enrichir les fonctions d'UDP et de fournir à ce dernier ce dont il a besoin pour gérer efficacement les données multimédias temps réel. [6] Aujourd'hui, ce couple s'utilise systématiquement dans les applications multimédias interactives, à la fois pour la téléphonie, la vidéo, les jeux vidéo et la réalité virtuelle. [6]

**RTP** est utilisé pour le transport de bout en bout de flux ayant des contraintes temporelles fortes, typiquement pour les flux multimédias avec interactivité, tel le service de téléphonie sur IP. Il met en œuvre des numéros de séquence pour chaque paquet afin d'assurer la livraison des données multimédias dans l'ordre correct

**RTCP** est un protocole de contrôle et de supervision du réseau. Il opère comme une sonde qui rend compte aux émetteurs des performances dont la communication en cours bénéficie. Son objectif est d'offrir aux participants d'une session une vision sur l'état du réseau et de s'y adapter de façon dynamique. Il fournit pour cela un rapport sur la qualité de distribution, incluant le délai de bout en bout, la gigue et le taux de pertes. Ce rapport est envoyé de façon périodique de façon que les intervenants disposent d'une mise à jour fréquente de l'état du réseau. [6]

Dans sa spécification, RTCP n'est aucunement indispensable pour le fonctionnement de RTP. La réciproque est vraie également. Néanmoins, leur association apporte une cohérence globale dans le traitement des communications multimédias. Tous deux doivent être pensés et intégrés au niveau applicatif. Les rapports fournis par RTCP peuvent optimiser la qualité de la transmission. [6]

## 1.7 Le protocole RTP

### 1.7.1 Fonctionnalités

assure un contrôle spécifique des données temps réel. Il permet de reconstituer les propriétés temps réel des flux médias en opérant sur deux niveaux, la synchronisation des flux d'un côté et la reconstitution de l'ordre des paquets émis et la détection des pertes de paquets de l'autre :

- Synchronisation des flux : Si l'audio et la vidéo sont transmis séparément, le destinataire doit jouer la séquence audio de façon que cette dernière coïncide avec la séquence vidéo. Pour cela, RTP ajoute aux paquets émis une estampille de date, appelée horodatage, ou timestamp. Cette estampille indique le moment où le paquet a été émis, ce qui permet de reproduire les mêmes délais interpaquet et de jouer les paquets audio et vidéo de manière synchronisée. [6]

- Reconstitution de l'ordre des paquets émis et détection des pertes de paquets : Les paquets IP sont transmis indépendamment les uns des autres. En conséquence, leur ordre d'arrivée chez le destinataire n'est pas forcément conforme à leur ordre d'émission. [6]

  Or cet ordre est indispensable pour reconstituer le message initial et le rendre intelligible à un auditeur. En recevant plusieurs paquets, le destinataire doit savoir lequel jouer avant les autres. Pour cela, un numéro de séquence qui s'incrémente progressivement est affecté à chaque paquet. [6]

  Ce numéro permet de déterminer un ordre de préséance des paquets. Par effet de bord, il permet de déterminer quels sont les paquets qui ont été perdus. [6]

  Si les paquets numérotés i et i + 2 sont reçus, passé un délai d'attente maximal, le terminal récepteur en déduit que le paquet numéroté i + 1 est manquant.

  Un mécanisme de compensation de la perte de paquets est généralement mis en place au niveau applicatif. Ce mécanisme n'est pas spécifié par le protocole RTP, mais son usage est rendu possible par la détection des pertes. Par exemple, un mécanisme classique de compensation consiste à prolonger la durée d'écoute des paquets précédents et suivants (les paquets i et i + 2 dans notre exemple), de façon à combler les pertes et réduire la perception humaine, tout en respectant la synchronisation des données . [6]

### 1.7.2 Inconvénients

Le protocole RTP ne propose pas une garanti de qualité de service. Il ne supporte pas notamment les services suivants : [6]
• Réservation de ressources dans le réseau.
• Fiabilisation des échanges.
• Garantie des délais de transit dans le réseau.

## 1.8 Le protocole SIP

### 1.8.1 Architecture

Le protocole SIP s'appuie sur une architecture purement logicielle. L'architecture de SIP s'articule principalement autour des cinq entités suivantes : [6]

• terminal utilisateur ;
• serveur d'enregistrement ;
• serveur de localisation ;
• serveur de redirection ;
• serveur proxy.

La figure suivante illustre de façon générique les communications entre ces éléments. Un seul terminal étant présent sur cette figure, aucune communication n'est possible. Nous nous intéressons en fait ici aux seuls échanges entre le terminal et les services que ce dernier est susceptible d'utiliser lors de ses communications. [6]

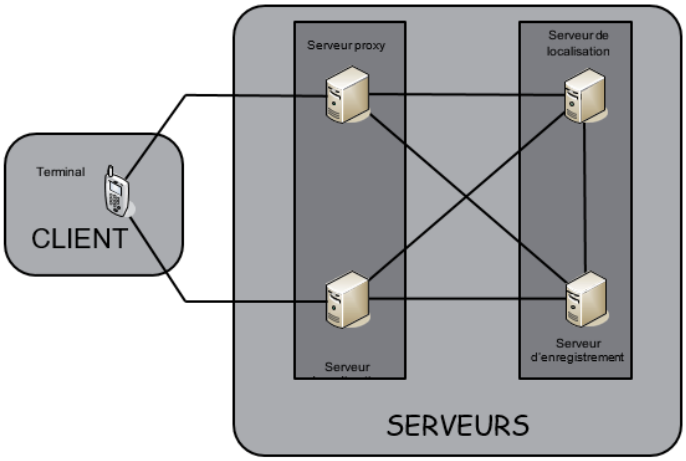


FIGURE 1.3 – architectur sip [6]

**Le serveur d'enregistrement** offre un moyen de localiser un correspon- dant avec souplesse, tout en gérant la mobilité de l'utilisateur. Il peut en outre supporter l'authentification des abonnés. [6]

**Le serveur de localisation** joue un rôle complémentaire par rapport au serveur d'enregistrement en permettant la localisation de l'abonné. [6]

**Le serveur de redirection** agit comme un intermédiaire entre le terminal client et le serveur de localisation. Il est sollicité par le terminal client pour contacter le serveur de localisation afin de déterminer la position courante d'un utilisateur. [6]

**Le serveur proxy** (parfois appelé serveur mandataire) permet d'initier une communica- tion à la place de l'appelant. Il joue le rôle d'intermédiaire entre les terminaux des interlocuteurs et agit pour le compte de ces derniers. [6]

Le serveur proxy remplit les différentes fonctions suivantes :
• localiser un correspondant ; [6]
• réaliser éventuellement certains traitements sur les requêtes ; [6]
• initier, maintenir et terminer une session vers un correspondant. [6]

### 1.8.2 Adressage SIP

Tout utilisateur SIP dispose d'un identifiant unique. Cet identifiant constitue l'adresse de l'utilisateur permettant de le localiser. [6]

Le format d'une adresse SIP (ou URL SIP) respecte la RFC 3986 et se présente sous la forme illustrée à la figure suivante :

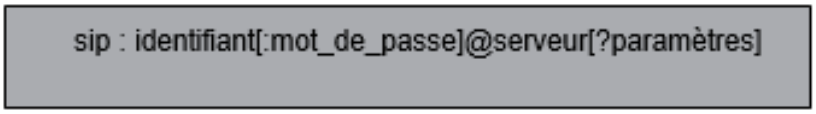


FIGURE 1.4 – Adressage SIP [6]

**On distingue dans cette adresse plusieurs parties :**

**Le mot-clé sip :** spécifie le protocole à utiliser pour la communication. [6]

**La partie identifiant :** définit le nom ou le numéro de l'utilisateur. Cet identifiant est nécessairement unique pour désigner l'utilisateur de manière non ambiguë. [6]

**La partie mot de passe :** est facultative. Le mot de passe peut être utile pour s'authentifier auprès du serveur, notamment à des fins de facturation. C'est aussi un moyen pour joindre un utilisateur qui a souhaité s'enregistrer sur l'équivalent d'une liste rouge : sans la connaissance de ce mot de passe, le correspondant n'est pas joignable. De manière générale, cette possibilité offre le moyen de restreindre l'utilisation de certains services. [6]

**La partie serveur :** spécifie le serveur chargé du compte SIP dont l'identifiant précède l'arobase. Le serveur est indiqué par son adresse IP ou par un nom qui sera résolu par DNS. Des paramètres URI peuvent être associés à ce nom. C'est ce serveur qui sera contacté pour joindre l'abonné correspondant. Un port peut être spécifié à la suite du serveur. [6]

**La partie paramètres :** est facultative. Les paramètres permettent soit de modifier le comportement par défaut (par exemple, en modifiant les protocoles de transport ou les ports, ou encore le TTL par défaut), soit de spécifier des informations complémentaires (par exemple, l'objet d'un appel qui sera envoyé à l'appelé en même temps que l'indication d'appel, à la manière d'un e-mail précisant l'objet du message). [6]

### 1.8.3 Méthode utilisées [7]

Une méthode SIP est une commande utilisée pour établir, modifier ou terminer une session de communication multimédia sur un réseau IP.

- INVITE : utilisée pour initier une session de communication.
- ACK : utilisée pour confirmer la réception d'un message INVITE.
- OPTIONS : permet d'interroger un serveur SIP sur différentes informations
- BYE : utilisée pour terminer une session de communication
- CANCEL : utilisée pour annuler une demande d'invitation qui a été envoyée mais qui n'a pas encore été traitée.
- REGISTER : permet d'enregistrer un utilisateur au niveau d'un serveur d'enregistrement.

### 1.8.4 Codes de réponses [7]

Un code de réponse SIP est une indication numérique envoyée par un serveur SIP à un client SIP pour indiquer le résultat d'une requête envoyée par le client. Les codes de réponse SIP sont généralement regroupés en 6 catégories, en fonction de leur premier chiffre :

- 1xx – Message d'information : Indique que le serveur a reçu la requête du client et continue à traiter la demande.
  Ex : 100 TRYING Tentative d'appel en cours.
- 2xx – Message de succès : La requête a été reçue, comprise et acceptée par le serveur.
  Ex : 200 ok La requête a été exécutée avec succès.
- 3xx – Message de redirection : Indique que la requête du client doit être dirigée vers un autre serveur ou une autre adresse.
  Ex : 301 Moved Permanently la requête du client doit être dirigée vers une nouvelle adresse permanente.
- 4xx – Message d'erreur client : Indique que la demande du client ne peut pas être traitée en raison d'une erreur de la part du client lui-même.
  Ex : 400 BAD REQUEST Le format de la requête est incorrect et ne peut être compris.
- 5xx – Message d'erreur serveur : Indique que la demande du client ne peut pas être traitée en raison d'une erreur de la part du serveur.
  Ex : 500 Internal Server Error Une erreur inattendue s'est produite sur le serveur.
- 6xx – Message d'erreur globale : Aucun serveur ne peut traiter cette requête, car ils sont occupés, inaccessibles ou refusent l'appel.
  Ex : 600 BUSY EVERYWHERE Le destinataire a été joint, mais il est occupé sur tous les postes et ne peut prendre la communication.

### 1.8.5 Communication SIP [7]

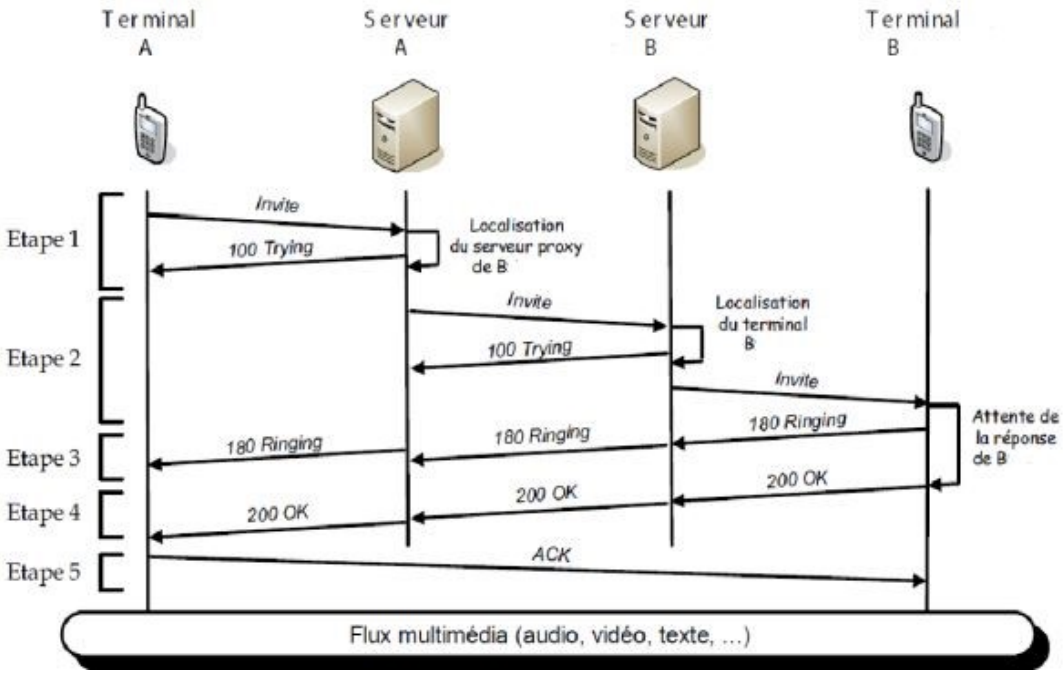


FIGURE 1.5 – Communication SIP [7]

**Explication des différentes étapes**

- **Etape 1 :** Un message d'invitation (requête INVITE) est envoyé du terminal A vers son serveur SIP. À la réception de ce message, le serveur A utilise la partie domaine de l'adresse SIP de B pour déterminer le serveur en charge de la gestion du compte B. À cette fin, un serveur DNS peut être sollicité. En parallèle, le serveur proxy informe A qu'il prend en charge la requête et tente de la mettre en relation. La réponse temporaire 100 TRYING indique que le message a été reçu et qu'il est en cours de traitement.
- **Etape 2 :** Le serveur A transmet l'invitation au serveur B après l'avoir localisé. C'est le message d'invitation original qui est intégralement relayé du serveur A vers le serveur B. Ce dernier informe le serveur A (par un message de réponse temporaire 100 TRYING) de la réception de la requête et de la tentative d'initialisation. Parallèlement, il recherche la localisation du terminal B en utilisant le service de localisation. Une fois la position du terminal dans le réseau trouvé, il lui transmet l'invitation de A.
- **Etape 3 :** Le téléphone B (éventuellement un softphone) reçoit l'invitation et la fait connaître à l'utilisateur B, le plus souvent par une sonnerie. En parallèle, il indique à son serveur (par un message 180 RINGING) que l'appel est en train d'être notifié à B et que la communication est en attente de son acceptation. Ce message informatif est relayé jusqu'à l'émetteur A, qui reçoit généralement un retour audio ou visuel (une tonalité de sonnerie particulière le plus souvent).
- **Etape 4 :** B répond au téléphone. On suppose le cas où B a choisi de répondre à l'appel. À l'instant où il décroche, un message 200 OK est retourné pour l'informer que l'appel est accepté. Ce message est relayé par les différents serveurs. À ce stade, la communication n'a pas encore débuté, et aucun son n'est transmis.

- **Etape 5 :** Le terminal A confirme les paramètres d'appel. En tenant compte des capacités prises en charge par les correspondants, le terminal A envoie un message d'acquittement ACK qui spécifie les paramètres définitifs à utiliser lors de cette session.

### 1.8.6 Avantages [7]

| Avantages | Explications |
|---|---|
| Open source | Les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement. |
| Flexible | SIP peut être utilisé pour tout type de sessions multimédia (voix, vidéo, réalité virtuelle, etc.). |
| Simple | SIP est simple et très similaire à HTTP. En effet, le client envoie des requêtes au serveur, qui lui renvoie une réponse. |
| Standard | L'IETF a normalisé le protocole et son évolution continue par la création ou l'évolution d'autres protocoles qui fonctionnent avec SIP. |

TABLE 1.1 – Avantages du protocole SIP

### 1.8.7 Inconvénients [7]

| Inconvénients | Explications |
|---|---|
| Mauvaise implémentation | une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les USER Agents peut perturber le fonctionnement ou générer du trafic superflu sur le réseau. |

TABLE 1.2 – Inconvénients du protocole SIP

## 1.9 Le protocole IAX/IAX2

IAX /IAX2 (version améliorée d'IAX), est un protocole de signalisation qui est une alternative au protocole SIP.[6] Il s'agit du protocole sur lequel s'appuie Asterisk bien que celui-ci soit en mesure de supporter les autres principaux protocoles VoIP tel que SIP. [7] Il permet la communication entre client et serveur Asterisk ainsi qu'entre deux serveurs Asterisk. Il a été conçu pour le contrôle et la transmission de flux multimédia avec un débit plus faible. [7]

Contrairement à SIP qui utilise 2 paires de flux (l'une pour la signalisation, l'autre pour la voix), IAX utilise une seule paire de flux pour communiquer entre les extrémités de la ligne (téléphone ou central téléphonique). La signalisation comme les données (la conversation vocale) sont transmises sur le même canal, par opposition à SIP qui utilise un second canal pour les flux de données (RTP) transportant la voix. [7]

De plus, IAX2 permet à plusieurs appels d'être rassemblés dans un seul ensemble de paquets IP. Ce mécanisme est appelé « trunking » [7]

### 1.9.1 Caractéristiques

**Compression de données :** IAX2 utilise la compression de données pour réduire la bande passante nécessaire pour les appels vocaux, ce qui peut être particulièrement utile dans les environnements réseau à faible bande passante. [7]

**Transport de données mixtes :** IAX2 peut transporter à la fois des données vocales et des données de signalisation sur la même connexion, ce qui simplifie la configuration réseau et améliore l'efficacité. [7]

**Simplicité de configuration :** Comparé à d'autres protocoles de voix sur IP (VoIP) comme SIP (Session Initiation Protocol), IAX2 est souvent considéré comme plus simple à configurer et à gérer, en particulier dans les environnements Asterisk. [7]

**Sécurité :** IAX2 intègre des fonctionnalités de sécurité telles que l'authentification par mot de passe et le chiffrement des données pour protéger les communications contre les écoutes indésirables et les accès non autorisés. [7]

**Gestion des appels avancée :** IAX2 prend en charge diverses fonctionnalités avancées de gestion des appels, telles que le transfert d'appels, le renvoi d'appels, la mise en attente et la conférence téléphonique. [7]

### 1.9.2 Requêtes et réponses IAX

**Requêtes :**

- **NEW :** est une requête envoyée par un équipement lorsqu'il souhaite initier une nouvelle session IAX avec un autre équipement ou un serveur Asterisk. [7]
- **REGREQ :** est une requête envoyée pour demander l'enregistrement d'un équipement auprès d'un serveur Asterisk. [7]
- **AUTHREQ :** est une requête envoyée pour demander une autorisation d'accès à un serveur Asterisk. [7]

**Réponses :**

- **ACK :** est une réponse pour confirmer la réception d'un message IAX précédent. [7]
- **AUTHREP :** est envoyé en réponse à un message IAX AUTHREQ pour confirmer ou refuser l'autorisation d'accès. [7]
- **REGACK :** envoyé en réponse à une requête REGREQ pour confirmer l'enregistrement d'un équipement auprès d'un serveur Asterisk. [7]
- **ACCEPT :** envoyée pour indiquer qu'une requête NEW est acceptée. [7]
- **REJECT :** envoyée pour indiquer qu'une requête NEW est refusée. [7]

### 1.9.3 Etablissement d'une connexion IAX :

L'établissement d'une connexion IAX (Inter-Asterisk eXchange) implique plusieurs étapes. Voici les principales :

- La première étape consiste à établir une connexion réseau entre le client et le serveur IAX. Cette connexion peut être établie via un réseau local (LAN) ou via Internet. [7]
- Ensuite, le client envoie une requête "AUTHREQ" au serveur pour s'authentifier. Cette requête contient des informations d'identification telles que le nom d'utilisateur et le mot de passe. Le serveur vérifie ces informations et renvoie une réponse "AUTHREP" si l'authentification est réussie. [7]
- Le client envoie ensuite une requête "REGREQ" au serveur pour s'enregistrer. Cette requête contient des informations sur l'identité du client telles que l'adresse IP, le nom d'utilisateur et le mot de passe. Le serveur vérifie ces informations et enregistre le client s'il est valide. [7]
- Une fois que le client est enregistré, il peut envoyer une requête "NEW" pour établir une nouvelle session. Cette requête contient des informations sur l'appel que le client souhaite effectuer, telles que l'adresse IP de destination et le numéro de téléphone. [7]
- Le serveur vérifie si l'adresse IP de destination est disponible et répond avec une réponse "ACCEPT" si elle l'est. Le client peut alors envoyer une requête "ACK" pour confirmer l'établissement de la session. [7]
- Enfin, les données audio et vidéo peuvent être échangées entre le client et le serveur via la session établie. [7]

## 1.10 Conclusion

Dans ce chapitre, nous avons exploré la technologie de la VoIP sous différents angles : ses avantages, ses protocoles, son fonctionnement et son architecture. Nous avons conclu que la VoIP représente la solution la plus économique pour les communications, offrant des services performants à des coûts considérablement réduits, que ce soit pour les entreprises ou les particuliers

# Chapitre 2

# Différents attaques et méthodes de sécurité de VoIP

## 2.1 Introduction

Le passage de la téléphonie classique à la téléphonie IP a présenté de nombreux avantages pour les entreprises, notamment la réduction des coûts, la flexibilité. Cependant, elle expose également les systèmes de communication à une nouvelle gamme de menaces et de vulnérabilités inhérentes aux réseaux IP.
Ce chapitre explorera en détail les différentes menaces pesant sur les systèmes VoIP et les mesures de sécurité à mettre en place pour y faire face. Il fournira une vue d'ensemble des attaques courantes, des solutions techniques disponibles, et des bonnes pratiques à adopter pour assurer la protection des communications VoIP

## 2.2 Attaques contre la VoIP

### 2.2.1 Suivie d'appels

Le suivi d'appels, ou Call tracking, est une attaque visant les terminaux (soft/hard phone) sur un réseau LAN/VPN. Son but est de détecter les communications en cours, d'identifier leur durée et les participants impliqués. Pour cela, l'attaquant intercepte les messages INVITE et BYE en surveillant le réseau afin d'obtenir des informations sur les appels en cours (qui communique, à quelle heure, et pendant combien de temps). [9] .

### 2.2.2 Voice Phishing

Est une technique d'attaque qui vise à tromper les utilisateurs de la VoIP en les incitant à divulguer des informations personnelles ou confidentielles par téléphone. Les attaquants se font souvent passer pour une entité de confiance, comme une banque, une entreprise ou une organisation gouvernementale, afin de convaincre les victimes de leur fournir des informations sensibles, telles que des numéros de carte de crédit, des mots de passe ou des informations d'identification personnelle [10].
Les techniques courantes utilisées pour réaliser le Voice Phishing incluent l'utilisation de messages vocaux automatisés (robocalls), la création de fausses identités, l'enregistrement de messages vocaux préenregistrés, et l'imitation de numéros de téléphone légitimes pour tromper les destinataires. Les attaques de Voice Phishing peuvent également être ciblées, dans lesquelles l'attaquant recueille des informations sur la victime pour personnaliser l'attaque et augmenter les chances de réussite. [10]


FIGURE 2.1 – Voice Phishing attack [10]

### 2.2.3 Sniffing

Le Sniffing en VoIP est une méthode d'espionnage où un attaquant capture et analyse les données vocales échangées lors d'une communication VoIP. Cette technique implique l'interception de paquets de données non cryptés circulant dans le réseau afin d'extraire des informations telles que les numéros de téléphone, les noms d'utilisateur, les mots de passe et les conversations vocales [9].

Cette technique peut être réalisée de différentes manières, par exemple en utilisant des outils de capture de paquets tels que Wireshark ou tcpdump pour intercepter le trafic réseau, ou en utilisant des logiciels malveillants pour infiltrer les systèmes VoIP et collecter les données. [9]

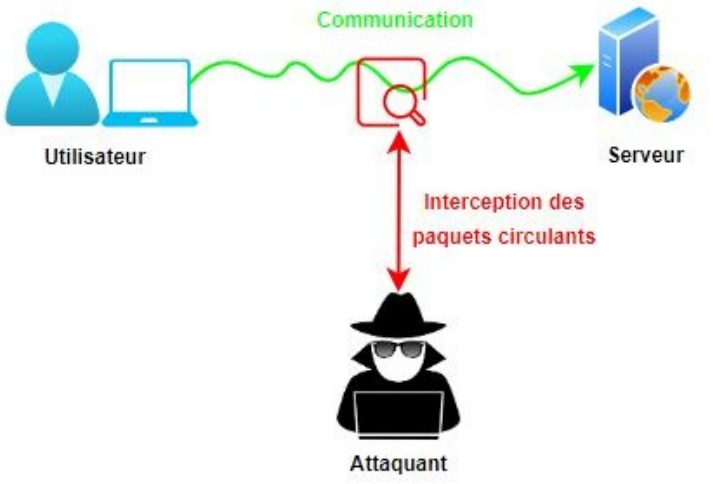


FIGURE 2.2 – Sniffing attackk [9]

### 2.2.4 Déni de service (DoS)

Les attaques de déni de service ont pour but de rendre un service VoIP indisponible en saturant le réseau ou les serveurs VoIP avec un trafic non autorisé. Les attaquants peuvent recourir à des techniques comme l'envoi de paquets de signalisation SIP malveillants ou l'inondation de paquets RTP, afin de surcharger le réseau et les serveurs VoIP.

Dans le cas du protocole SIP, une attaque DoS (SIP flooding) peut être directement dirigée

contre les utilisateurs finaux ou les dispositifs tels que téléphones IP, routeurs et proxy SIP, ou contre les serveurs concernés par le processus, en utilisant le mécanisme du protocole SIP ou d'autres techniques traditionnelles de DoS. Il existe différentes formes d'attaques DoS, on peut citer [9] :

**DoS de type CANCEL :** C'est un type de déni de service lancé contre l'utilisateur.
L'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive pour un utilisateur spécifique.
Une fois que le dispositif de l'utilisateur reçoit la requête INVITE, l'attaquant envoie immédiatement une requête CANCEL.
Cette requête produit une erreur sur le dispositif de l'appelé et termine l'appel.
Ce type d'attaque est employé pour interrompre la communication. [9]

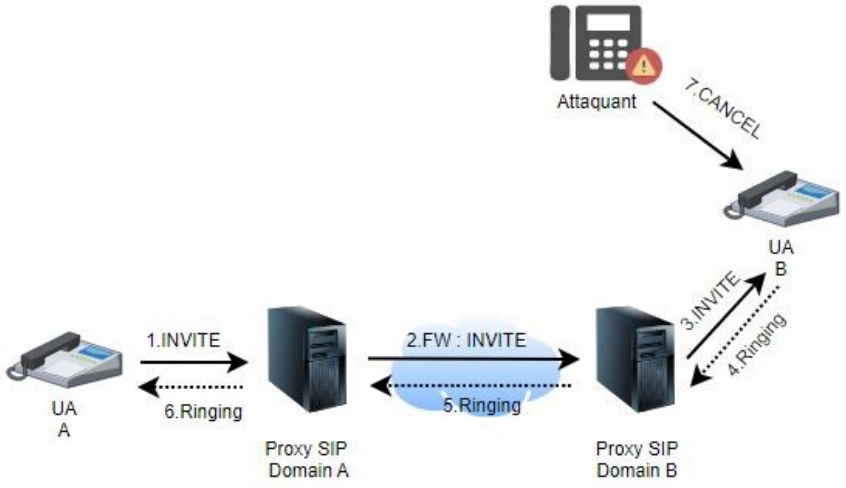


FIGURE 2.3 – DoS de type CANCEL [9]

La figure ci-dessus montre un scénario d'attaque DoS CANCEL, l'utilisateur (UA : User Agent) A initie l'appel, envoie une invitation (1) au proxy auquel il est rattaché. Le proxy du domaine A achemine la requête (2) au proxy qui est responsable de l'utilisateur B. Ensuite c'est le proxy du domaine B qui prend le relais et achemine la requête INVITE (3) qui arrive enfin à destination. Le dispositif B, quand il reçoit l'invitation, sonne (4). Cette information est réacheminée jusqu'au dispositif A. L'attaquant qui surveille l'activité du proxy SIP du domaine B envoie une requête CANCEL (7) avant que B n'ait pu envoyer la réponse OK qui accepte l'appel. Cette requête annulera la requête en attente (l'INVITE), l'appel n'a pas lieu. L'activité du proxy SIP du domaine B envoie une requête CANCEL (7) avant que B n'ait pu envoyer la réponse OK qui accepte l'appel. Cette requête annulera la requête en attente (l'INVITE), l'appel n'a pas lieu. [9]

**DoS de type BYE :** Un autre type d'attaque lancée contre les utilisateurs est le déni de service par requête BYE. Cette dernière est envoyée soit à l'appelant, soit à l'appelé, peut être utilisé pour perturber l'appel à n'importe quel moment de la communication. [9]

C'est exactement le même scénario que DoS de type CANCEL sauf que dans ce cas-ci, l'atta- quant attend qu'une réponse positive acceptant l'appel (4) soit envoyée par B pour lancer son attaque. Dès que la 200 OK est envoyée, l'attaquant envoie une requête BYE à l'un des parti-

cipants ou même aux deux, ce qui terminera l'appel sans que les communiquant n'y puissent rien. [9]

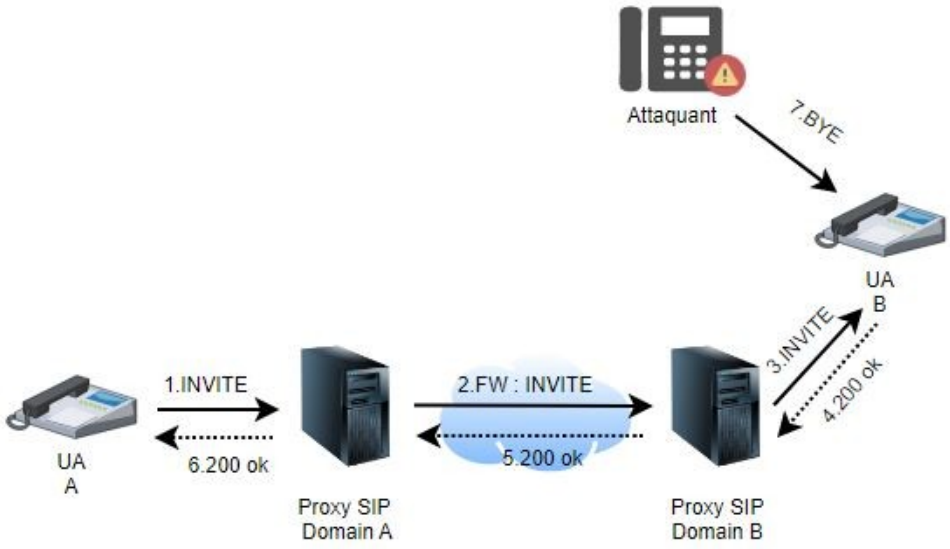


FIGURE 2.4 – DoS de type BYE [9]

### 2.2.5 MITM (Man In The Middle)

L'attaque Man-in-the-Middle (MITM) implique trois acteurs : le client, le serveur et l'attaquant. Le but de l'attaquant est de se faire passer pour le client auprès du serveur et de se faire passer pour le serveur auprès du client, Il devient ainsi l'homme du milieu. Cela lui permet de surveiller et modifier le trafic réseau entre le client et le serveur à sa manière pour obtenir des informations sensibles telles que des mots de passe, des accès au système, etc. La plupart du temps, l'attaquant utilise les techniques de détournement de flux pour rediriger les flux du client et du serveur vers lui [10].

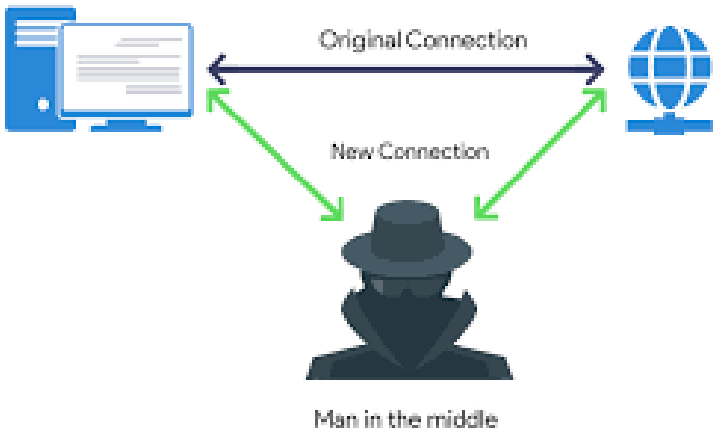


FIGURE 2.5 – Man In The Middle [17]

### 2.2.6 L'écoute clandestine

L'eavesdropping est l'écoute clandestine d'une conversation téléphonique. Un attaquant avec un accès au réseau VoIP peut sniffer le trafic et décoder la conversation vocale. Des outils tels que VOMIT (Voice Over Misconfigured Internet Telephones) permettent de réaliser cette attaque. VOMIT convertit les paquets sniffés en fichier .wav qui peut être réécouté avec n'importe quel lecteur de fichiers son.

## 2.3 Mecanismes de défense

### 2.3.1 Mise en place des VlANs

Un VLAN (Virtual Local Area Network) dans la VoIP est un réseau logique qui est créé à partir d'un réseau physique existant, il permet d'isoler le trafic voix des autres types de trafic sur le réseau. Il s'agit d'une méthode de segmentation logique du réseau qui permet de regrouper des ports de commutateur en fonction de leur utilisation prévue, afin d'optimiser la qualité de service et de simplifier la gestion du réseau [12].
Il exister plusieurs niveaux de vlan : Vlan niveau 1(Vlan par port), Vlan niveau 2(Vlan par adresse MAC) et Vlan niveau 3(Vlan par adresse IP).

### 2.3.2 Mise en place des VPNs

Un VPN (Virtual Private Network) dans la VoIP est un réseau privé qui permet de créer un tunnel crypté dans lequel passent toutes les données (voix et fichiers), ce qui permet de sécuriser et de protéger les communications vocales contre les tentatives d'interception ou d'écoute malveillantes. Cela est particulièrement important lorsque les communications vocales sont transmises sur des réseaux publics ou non sécurisés. [13]

Le fonctionnement des VPN repose sur des technologies appelées protocoles de tunnelisation ou protocoles VPN et parmi eux nous retrouvons [16]

**VPN IPSec :** utilisé pour créer des connexions tunnels chiffrées sur internet. Il fournit un chiffrement de bout en bout. [16]

**VPN PPTP :** Il permet de créer une connexion sécurisée entre deux points sur un réseau public, tel qu'Internet, il est facile à configurer et il offre des vitesses de connexion rapides. [16]

**VPN L2TP :** utilisé en conjonction avec IPSec pour fournir une sécurité accrue. Telles qu'il offre un niveau élevé de confidentialité et de sécurité, et difficile à configurer. [16]

### •Types de VPN

Il existe de différents types de VPN (Virtual Private Network) sont utilisés pour répondre à des besoins spécifiques de connexion sécurisée dans différents contextes. Voici une présentation détaillée de chacun des trois principaux types de VPN : le VPN d'accès, l'Intranet VPN, et l'Extranet VPN. [18]

**Le VPN d'accès :** Le VPN d'accès est principalement utilisé pour permettre aux utilisateurs itinérants (comme les employés en déplacement) de se connecter en toute sécurité au réseau privé de leur entreprise via Internet. [18]

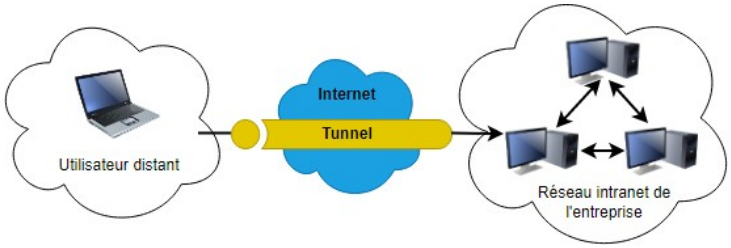


FIGURE 2.6 – VPN d'accés [18]

**Intranet VPN** Dans une entreprise, Un VPN intranet crée une connexion sécurisée entre différentes parties du réseau interne, particulièrement utile pour les bureaux géographiquement dispersés. [19]

**Extranet VPN** L'utilisation d'un VPN extranet permet à une entreprise d'établir une communication sécurisée avec ses clients, fournisseurs et partenaires via un intranet d'entreprise reposant sur une infrastructure partagée et des connexions dédiées. Dans cette configuration, il est essentiel que l'administrateur du VPN ait la capacité de surveiller les clients présents sur le réseau et de gérer les droits d'accès de chacun de manière appropriée. [18]

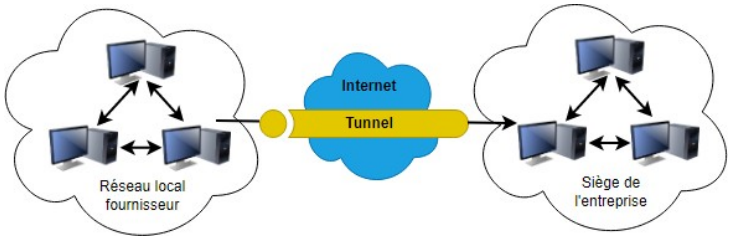


FIGURE 2.7 – Extranet VPN [18]

## •Protocoles VPN

**OpenVpn** OpenVPN est un logiciel open-source qui permet de créer des réseaux privés virtuels (VPN) sécurisés. Il offre une grande flexibilité et peut être utilisé pour différents types de configurations, notamment [18] :

- **Accès à distance :** Les employés distants et les voyageurs peuvent se connecter en toute sécurité au réseau interne de l'entreprise comme s'ils étaient physiquement présents. [18]
- **Site-à-site :** Des connexions sécurisées peuvent être établies entre différents sites d'une même entreprise, permettant ainsi de partager des ressources et de collaborer de manière transparente. [18]
- **Routage et pontage :** OpenVPN peut être configuré pour router le trafic entre différents réseaux ou pour créer des ponts virtuels, permettant ainsi de connecter des réseaux qui ne sont pas directement reliés. [18]

**OpenVPN** utilise un protocole de sécurité sur mesure basé sur SSL/TLS pour le chiffrement des communications et l'authentification des utilisateurs. Cela garantit que vos données restent confidentielles et protégées contre les intrusions. [18] il offre plusieurs options d'authentification pour répondre à vos besoins spécifiques, notamment :

- **Clé pré-partagée :** Une clé secrète partagée entre les utilisateurs est utilisée pour l'authentification. [18]
- **Certificats :** Des certificats numériques délivrés par une autorité de certification de confiance sont utilisés pour vérifier l'identité des utilisateurs. [18]
- **Nom d'utilisateur/mot de passe :** Une combinaison nom d'utilisateur/mot de passe traditionnelle est utilisée pour l'authentification. [18]

**Protocole IPSec** IPSec est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau du modèle OSI [20].

**les principales fonctionnalités d'IPSec sont :**

- **Confidentialité :** Vos données sont chiffrées, les rendant illisibles aux personnes non autorisées. [20]
- **Authentification :** IPSec vérifie l'identité de l'autre appareil pour s'assurer qu'il est bien celui à qui vous souhaitez envoyer vos données. [20]
- **Intègrité :** IPSec garantit que vos données n'ont pas été modifiées en cours de route. [20]

**IPSec est couramment utilisé pour :**

- Réseaux privés virtuels (VPN) : Créez un tunnel sécurisé pour vous connecter à un réseau distant comme si vous y étiez physiquement présent. [20]
- Communications sensibles : Protégez les données confidentielles telles que les informations bancaires ou médicales lors de leur transmission sur Internet. [20]
- Trafic interne d'entreprise : Sécurisez les communications entre les différents sites d'une entreprise. [20]

**IPSec utilise une combinaison de protocoles pour assurer la sécurité des données :**

- ISAKMP (Internet Security Association and Key Management Protocol) : Établit, négocie, gère et supprime les connexions sécurisées entre les appareils. [21]

- IKE (Internet Key Exchange) : Négocier l'échange de clés sécurisées pour le chiffrement et l'authentification. [21]
- AH (Authentication Header) : Garantit l'intégrité des données en les signant numériquement. [21]
- ESP (Encapsulating Security Payload) : Offre la confidentialité en chiffrant les données et, en option, l'authentification et l'intégrité. [21]

**IPSec offre deux modes principaux pour la protection des données :**

- Mode transport : Protège uniquement les données de la couche transport (comme TCP ou UDP), laissant l'en-tête IP inchangé. [22]
- Mode tunnel : Encapsule l'intégralité du paquet IP, y compris l'en-tête, dans un nouveau paquet avec un nouvel en-tête IPSec. [22]

### 2.3.3 Pare-feu

Un pare-feu dédié à la VoIP est conçu pour sécuriser les communications VoIP et protéger le réseau contre les intrusions malveillantes. Il bloque les tentatives d'accès non autorisées, contrôle le trafic entrant et sortant, et filtre les paquets de données afin d'éviter les attaques par déni de service (DoS).

Le pare-feu doit être configuré pour reconnaître et traiter les protocoles VoIP courants, et être régulièrement mis à jour avec les derniers correctifs de sécurité pour assurer une protection optimale contre les menaces. De plus, les règles du pare-feu doivent être testées régulièrement pour garantir leur bon fonctionnement et éviter d'entraver le bon déroulement des communications VoIP.

### 2.3.4 Formation et Sensibilisation des utilisateurs

- **Sensibilisation à la sécurité :** Expliquez l'importance de la sécurité des communications et les conséquences potentielles des violations.

.

- **Pratiques de sécurité :** Enseignez aux utilisateurs les bonnes pratiques, telles que l'utilisation de mots de passe forts, la vérification des identités avant de partager des informations sensibles, et la déconnexion après utilisation.

## 2.4 Conclusion

La VoIP s'impose comme une révolution dans le monde des communications, tirant parti d'Internet pour transmettre des appels vocaux. Ses avantages en termes de flexibilité et de coûts en font une solution de choix pour les entreprises et les particuliers. Cependant, ce succès grandissant attire inévitablement les cybercriminels. La VoIP est devenue une cible privilégiée pour diverses attaques, menaçant la sécurité des réseaux et des communications.

Au cours de ce chapitre, nous avons examiné les attaques les plus courantes et les plus répandues qui peuvent menacer la sécurité des réseaux VoIP ainsi que les différentes solutions de sécurité possibles pour remédier à ces attaques.

# Chapitre 3

# Présentation de l'Entreprise d'Accueil et du Client

## 3.1 Introduction

Ce chapitre sera réservé pour une bréf présentation du campus NTS (New Technologie § Solutions) qui est l'entreprise d'acceuil et une presentation détaillé de sont client groupe COLLABLE (Centre t'éléphonique)où nous effectuons notre stage. Dans un premier temps, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Nous étudierons ensuite l'architecture réseau de cette entreprise et ses composantes afin de pouvoir suggérer d'éventuelles améliorations.

### 3.1.1 Présentation de NTS (New Technologies  Solutions)

NTS, acronyme pour New Technologies  Solutions, est une entreprise spécialisée dans les solutions informatiques avancées et les services de télécommunications. Fondée il y a 4 ans, NTS s'est rapidement affirmée comme un leader dans son domaine, offrant des services innovants et des solutions technologiques sur mesure pour répondre aux besoins variés de sa clientèle. L'entreprise se distingue par son engagement envers l'excellence technique et son approche axée sur la satisfaction client.

### 3.1.2 Présentation de COLLABLE (Centre Téléphonique)

Le Groupe COLLABLE est un centre téléphonique renommé, faisant partie des clients stratégiques de NTS. Spécialisé dans la gestion des communications téléphoniques à grande échelle, COLLABLE joue un rôle crucial dans divers secteurs tels que le service client, le support technique, ressources humaines et le services financiers. L'entreprise se distingue par sa capacité à gérer efficacement un volume élevé d'appels entrants et sortants tout en maintenant des normes élevées de qualité de service.

### Organigramme général de l'organisme d'accueil

L'importance des centres d'appels réside dans la facilitation de l'interaction efficace entre les entreprises et leurs clients. Collable, offre une plateforme centralisée pour gérer les demandes d'assistance, fournir un support technique et résoudre les problèmes liés aux services financiers et aux ressources humaines. Cette présentation offre un aperçu complet des services proposés par Collable.
La figure ci-dessous, represente l'organigramme du centre téléphonique COLLABLE.

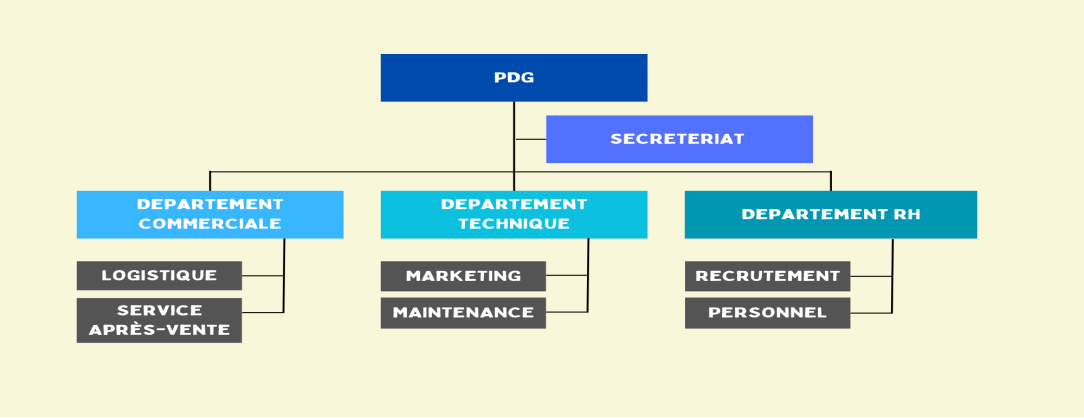


FIGURE 3.1 – L'organigramme de l'entreprise COLLABLE

## 3.2 Etude de l'existant

COLLABLE s'appuie sur une topologie arborescente pour relier ses différents appareils, comme le montre le schéma ci-dessous, avec l'indication que les équipements n'ont reçu aucune configuration préalable.

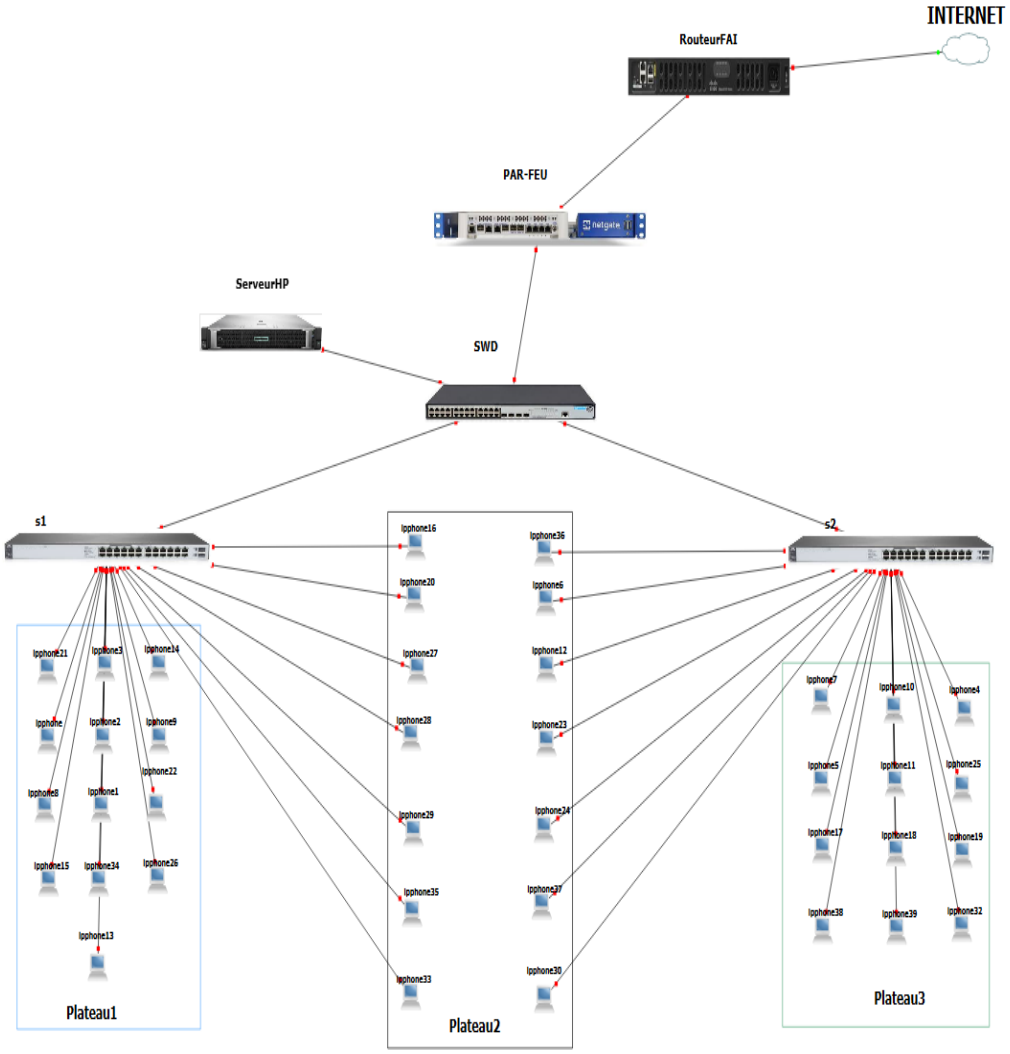


FIGURE 3.2 – Architecture de réseau (COLLABLE).

## 3.3 Analyse du parc informatique

Pour une organisation efficace et sécurisée du câblage réseau, COLLABLE utilise une armoire de brassage. Cette armoire joue un rôle crucial dans la gestion et la distribution des connexions réseau au sein de l'infrastructure.

### 3.3.1 caractéristique de l'armoire de brassage

L'armoire de brassage TOTEN RACK, utilisée par COLLABLE, possède des caractéristiques spécifiques qui répondent aux besoins de l'infrastructure réseau. Le tableau 3.1 ci-dessous détaille ces caractéristiques, telles que la capacité, les dimensions, et les accessoires inclus.

| Équipement | Modèle | Caractéristiques | Prix/unité |
|---|---|---|---|
|  • **N°= 1** | TOTEN RACK | • Capacité 42U(racks)<br>• 700mm × 1100mm × 2000mm<br>• Porte devant et arrière perforée avec poignets rétractables contenant des serrures.<br>• Panneaux latéraux amovibles.<br>• Plaque de fond et de toiture avec des trous de ventilation + Kit de 4 ventilateurs de toit. Rail kit + étagère coulissante + deux étagères fixes.<br>• Bandeau d'alimentation. Entrée de câble sur le dessus et le dessous. 4 pieds ajustables + 4 roulettes. | 70000 DA |

TABLE 3.1 – Caractéristique de l'armoir

### 3.3.2 Présentation d'environnement hard et soft

L'infrastructure informatique de COLLABLE comprend divers équipements matériels et logiciels qui travaillent ensemble pour assurer un fonctionnement efficace et sécurisé. Le tableau 3.2 présente un résumé des principaux équipements matériels (hard) et des logiciels (soft) utilisés.

| Nom de l'équipement | Hardware (hard) | Software (soft) |
|---|---|---|
| Routeur | FAI | IOS (International Organisation For Standardisation) |
| Pare-feu | Pfsense | FreeBSD |
| Serveur | HP ProLiant DL380P génération 10 | Windows server 2012 |
| Switch | Switch Cisco Catalyst 3750-24PS | Switch Cisco Catalyst 3750-24PS IOS (International Organisation For Standardisation) |
| PC portable | Dell i5 VP inside | windows 10 |

TABLE 3.2 – L'environnement hardware et software

### 3.3.3 caractéristiques des équipements par niveaux

Les équipements utilisés dans l'infrastructure informatique de COLLABLE sont répartis par niveaux dans l'armoire de brassage selon leur fonction et leur capacité. Le tableau 3.3 ci-dessous détaille les caractéristiques de ces équipements et leurs prix

| Équipement | Modèle | Caractéristiques | Prix/unité |
|---|---|---|---|
|  • **N°= 1** | ISR 4331 | • RAM : 4 G0 (installé) /16 GO (maximum)<br>• Mémoire Flash :4000 MO<br>• Débit :100 Mb/s<br>• Protocole de liaison de données : Ethernet, fast Ethernet et gigabit-ethernet<br>• Durée de vie de 5 à 10 ans | 270 000 DA |
|  • **N°= 1** | Netgate SG-6100"PFSENSE" | • Débit : 4000 Mbit/s<br>• Débit IPS : 2700Mbit/s<br>• Débit VPN IP sec : 560 Mbit/s<br>• Durée de vie entre 5 et 7 ans | 95 000 DA |
|  • **N°= 1** | Switch HPE 1920 | • Ports : 24 ports<br>• Mémoire Flash : 16MO<br>• Mémoire RAM : 128MO<br>• Capacité de commutation : 32 Gbit/s<br>• Durée de vie 5 à 7 ans ou plus avec un bon entretien | 252 000 DA |
|  • **N°= 2** | Switch HPE 1820 | • Ports : 24 ports<br>• Mémoire Flash : 128MO<br>• Mémoire RAM : 512MO<br>• Capacité de commutation : 56 Gbit/s<br>• Durée de vie 5 à 7 ans ou plus avec un bon entretien | 160 000 DA. |

| | | | |
|---|---|---|---|
|  • **N°= 1** | Serveur HP ProLiant DL380P génération 10 | • Processor Intel Xeon<br>• Silver 4110 (Octo-Core 2.1 GHZ / 3.0 GHZ Turbo-16 Threads-cache 11Mo)<br>• 16 G0 DDR4 RDIMM (1x 16 GO -12 slots)<br>• Durée de vie entre 5 et 7 ans dans des conditions normales d'utilisation | 800 000 DA |
|  • **N°= 40** | PC portable Dell IAER 35 R | • AMD core : i5 8th génération<br>• RAM : 8GO<br>• Disque : 256GO<br>• Ecran : UHD Graphies 620 (1920×1080×32b) | 90000 DA |

TABLE 3.3 – Tableau des équipements

## 3.4 Objectif du stage

Mon stage avait pour but principal de mettre en place une solution VoIP sur l'infrastructure existante afin de gérer les communications du centre téléphonique tout en garantissant une sécurité optimale des communications.

## 3.5 Problématique

Pour mettre en place une solution VoIP efficace et sécurisée pour COLLABLE, nous faisons face à plusieurs défis majeurs.

- Le centre téléphonique cherche une solution Voip sans engager des coûts élevés en matériel et en licences de logiciels. Cette contrainte budgétaire exige une solution qui soit à la fois économique à mettre en place et à maintenir.
- La sécurité des communications est primordiale. Avec une infrastructure existante, il est crucial d'assurer la confidentialité et l'intégrité des appels téléphoniques pour éviter tout risque d'interception ou de piratage. Cela nécessite l'implémentation de mesures de sécurité robustes.
- La qualité de service est un autre aspect critique. La solution VoIP doit garantir une qualité de service optimale pour les utilisateurs finaux, minimisant les délais et interruptions. Cela implique une configuration soignée et une gestion adéquate des ressources réseau pour assurer une performance stable et fiable.

- L'intégration avec l'infrastructure existante est également un facteur essentiel. La solution doit s'intégrer parfaitement avec les équipements et les réseaux actuels, incluant les switches, le serveur et le pare-feu. Toute incompatibilité pourrait entraîner des coûts supplémentaires et des retards dans le déploiement.
- Enfin, la maintenance et l'évolutivité de la solution doivent être prises en compte. La solution choisie doit être facile à maintenir et à faire évoluer, pour répondre aux besoins futurs du centre téléphonique.

## 3.6 Solutions proposées

Pour répondre aux besoins de Collable en termes de mise en place d'un serveur VoIP sécurisé et efficace, plusieurs solutions sont envisagées. Chaque solution est évaluée en termes de coût, avantages et inconvénients afin de choisir la plus adaptée.

### 3.6.1 SOLUTION1 : FreePBX

FreePBX est une solution de téléphonie IP open source basée sur Asterisk, qui offre une interface utilisateur web pour faciliter la configuration et la gestion du système téléphonique. FreePBX permet de créer et de gérer des PBX avec une grande variété de fonctionnalités avancées telles que la messagerie vocale, la gestion des files d'attente, la conférence, l'enregistrement des appels, et bien plus encore. Cette solution s'adapte parfaitement à tout type de serveur, notamment le serveur HP ProLiant DL380P Gen10 existant dans l'infrastructure de COLLABLE. Doté d'un processeur Intel Xeon Silver 4110 et de 16 Go de RAM DDR4 RDIMM, ce serveur offre une puissance de traitement suffisante pour gérer plusieurs appels simultanés, assurant ainsi une performance optimale et une grande fiabilité pour l'ensemble du système téléphonique.

**Avantages :**

- Faible coût initial et d'entretien, car il est open source et gratuit.
- Grande flexibilité permettant des personnalisations étendues pour répondre aux besoins spécifiques du centre d'appel.
- Interface utilisateur web facilitant la configuration et la gestion, même pour les utilisateurs non techniques.
- Large communauté de support offrant une documentation riche et des ressources de dépannage.

**Inconvénients :**

- Nécessite des compétences techniques pour la configuration et la maintenance, ce qui peut nécessiter une formation supplémentaire ou l'embauche de personnel qualifié.
- Moins de support commercial direct comparé à des solutions propriétaires.

## Architecture proposée pour la solution FreePBX

La figure 3.3 représente l'architecture proposée pour la solution 1, sachant que :

- Aucun équipement supplémentaire n'a été ajouté.
- La solution FreePBX sera implémentée sur le serveur existant.
- Les terminaux seront des softphones.

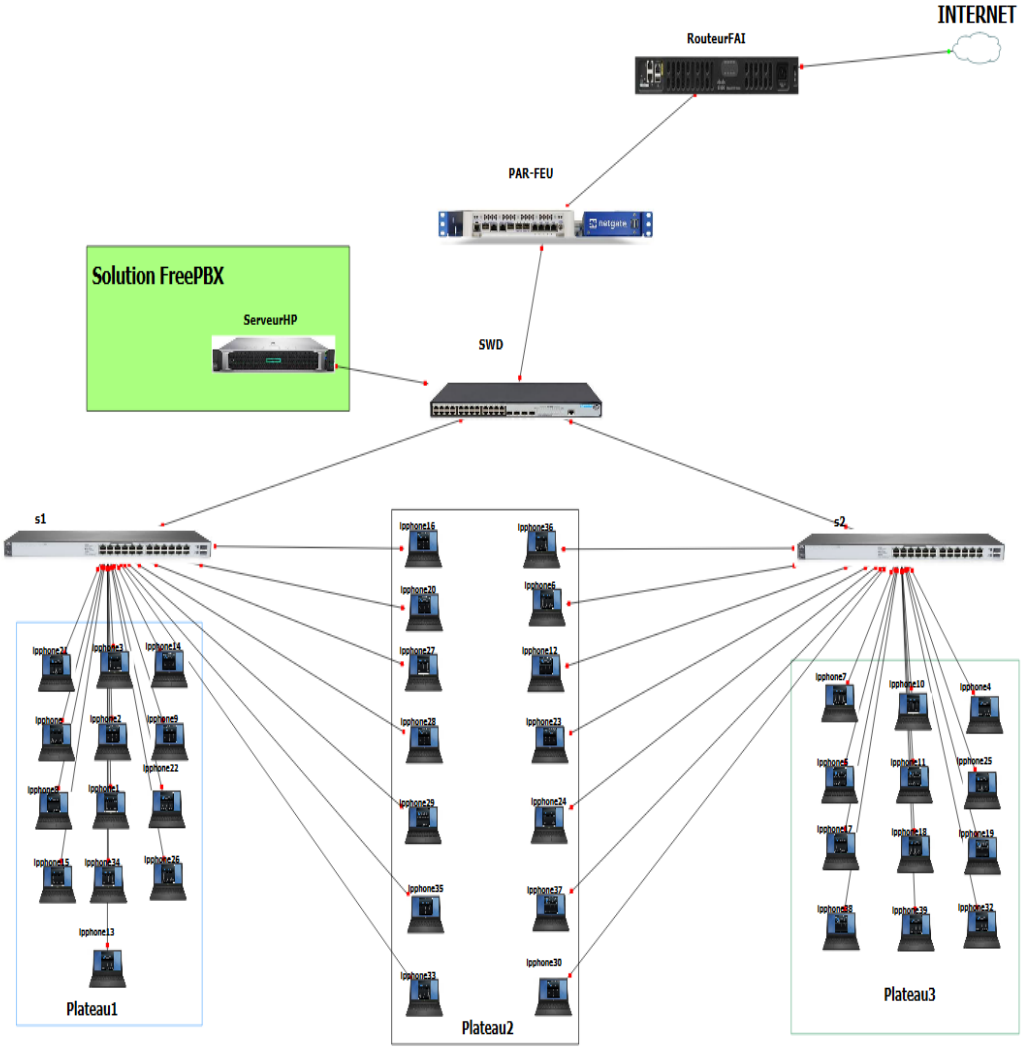


FIGURE 3.3 – Architécture proposée pour la solution FreePBX

### 3.6.2 SOLUTION2 : 3CX

3CX est une solution de téléphonie IP commercial offre une large gamme de fonctionnalités pour la gestion des communications d'entreprise. 3CX permet de gérer les appels, la messagerie instantanée, les conférences vidéo, et plus encore. Cette solution s'adapte parfaitement à tout type de serveur, notamment le serveur HP existant dans l'infrastructure de COLLABLE

**Avantages :**

- Interface utilisateur intuitive, facilitant la gestion et l'utilisation quotidienne.
- Support technique commercial disponible, ce qui peut réduire les temps de résolution des problèmes.
- Intégration facile avec les applications Microsoft, utile si Collable utilise déjà des outils Microsoft.

**Inconvénients :**

- Coût de licence qui peut devenir significatif à long terme.
- Moins flexible qu'Asterisk en termes de personnalisation et d'adaptabilité aux besoins spécifiques.

## Architecture proposée pour la solution 3CX

La figure 3.4 représente l'architecture proposée pour la solution 2, sachant que :

- Aucun équipement supplémentaire n'a été ajouté.
- La solution FreePBX sera implémentée sur le serveur existant.
- Les terminaux seront des softphones.

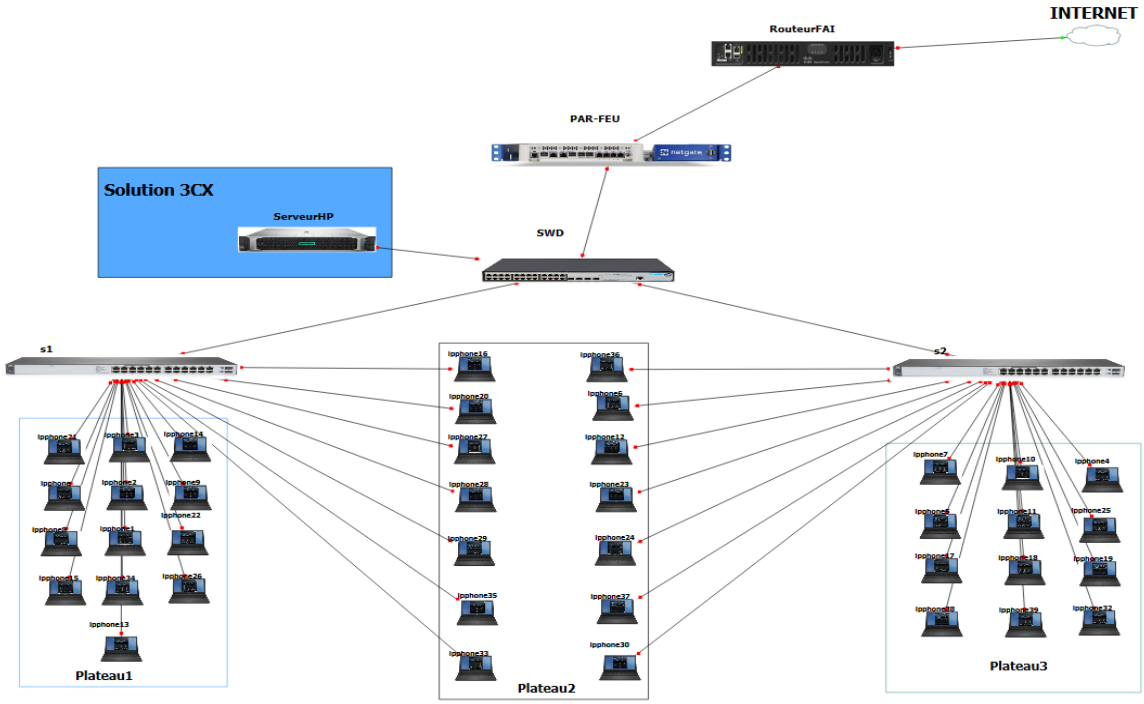


FIGURE 3.4 – Architécture proposée pour la solution 3CX

### 3.6.3 SOLUTION3 : Cisco Unified Communications Manager (CUCM)

Cisco Unified Communications Manager (CUCM) est une solution de téléphonie IP de Cisco conçue pour fournir une gestion centralisée des communications voix et vidéo. CUCM offre une gamme complète de fonctionnalités pour la gestion des appels, la messagerie unifiée, la mobilité, et les conférences.

**Avantages :**

- Très fiable et robuste, adaptée aux environnements de grande envergure et critiques.
- Support et maintenance de niveau entreprise, garantissant une assistance rapide et efficace.
- Intégration avec d'autres produits Cisco, offrant une solution homogène et optimisée pour les infrastructures existantes utilisant des équipements Cisco.

**Inconvénients :**

- Coût très élevé, tant en termes de licences que de matériel.
- Complexité de mise en œuvre, nécessitant des compétences spécialisées et potentiellement des certifications Cisco.

## Architecture proposée pour la solution CUCM

La figure 3.5 représente l'architecture proposée pour la solution 3, sachant que :

- La solution CUCM nécessite d'être implémentée sur un serveur propriétaire CISCO.
- Les terminaux seront des téléphones IP propriétaires CISCO.

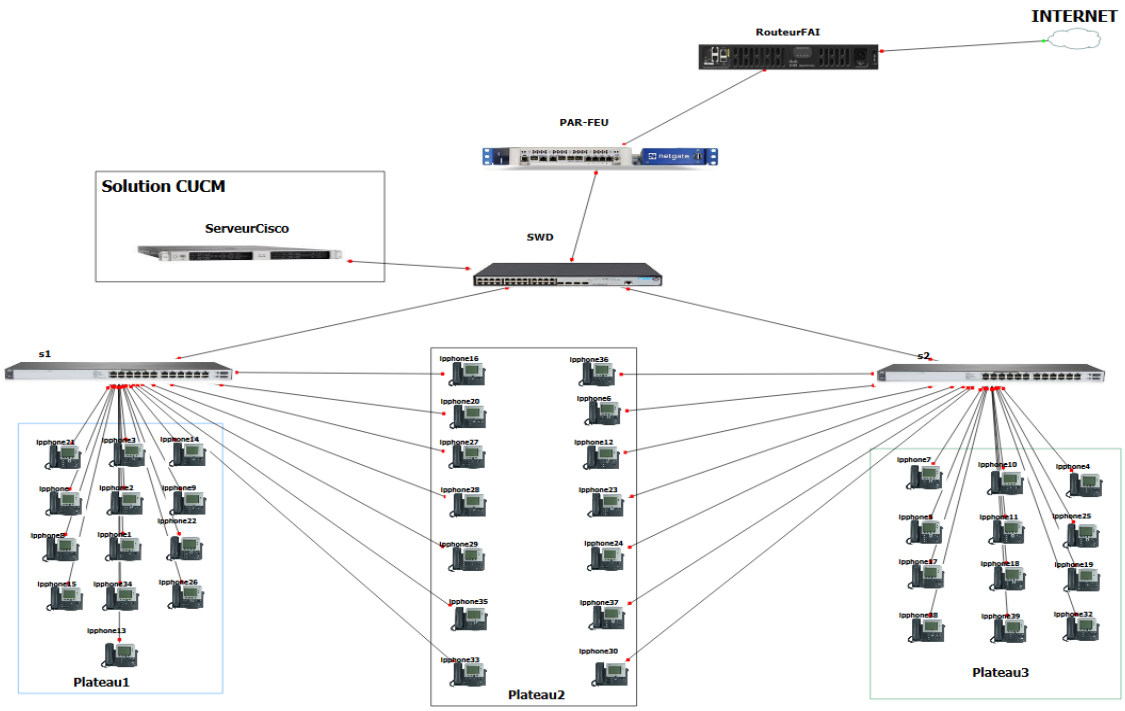


FIGURE 3.5 – Architécture proposée pour la solution CUCM

### 3.6.4 Coût estimé de chaque solution

| Solution | Coût |
|---|---|
| FreePBX | **Logiciel** : Gratuit(0 DZA)<br>**Matériel** : Utilisation du serveur existant (0 DZA)<br>**Softphone** : Gratuit(0 DZA)<br>**Configuration et Maintenance** : entre 200 000 - 300 000 DZA |
| 3CX | **Logiciel** : Licence de 416-500 DZA/Mois pour un utilisateur<br>**Matériel** : Utilisation du serveur existant (0 DZA)<br>**Softphone** : Gratuit(0 DZA)<br>**Configuration et Maintenance** : entre 250 000 - 350 000 DZA |
| Cisco Unified Communications Manager (CUCM) | **Logiciel** : Licence initiale élevée de 10 000 à 15 000 DZA/utilisateur<br>**Matériel** : serveurs Cisco environ 3 375 000 DZD + ip phone de cisco environ 60,000 DZD/ip phone<br>**Configuration et Maintenance** : entre 600 000 - 750 000 DZA |

TABLE 3.4 – Coûts des différentes solutions de serveur VoIP

## 3.7 Comparaison des Solutions

| Solution | Coût | Flexibilité et Personnalisation | Installation et utilisation |
|---|---|---|---|
| FreePBX | Aucun équipement n'a été ajouté, logiciel gratuit, softphone gratuit, ce qui signifie que COLLABLE va payer uniquement les frais d'installation et de configuration. | FreePBX est basé sur Asterisk, un logiciel open source, ce qui offre une grande flexibilité pour les modifications et les intégrations personnalisées, fonctionne avec une large gamme de matériels et de logiciels. | Offre une Interface web intuitive permettant une configuration et utilisation facile, des extensions, des groupes d'appels |
| 3CX | Aucun équipement n'a été ajouté, logiciel payant car c'est une solution commerciale, softphone gratuit, ce qui signifie que COLLABLE va payer les frais d'installation et de configuration + les frais de licences | Moins flexible que FreePBX, fonctionne avec une large gamme de matériels et de logiciels. | Offre une interface utilisateur conviviale, plus facile à configurer |

| | | | |
|---|---|---|---|
| CUCM | Nécessite l'achat d'un serveur propriétaire Cisco et des téléphones IP, logiciel payant car c'est une solution commerciale, ce qui signifie que COLLABLE va dépenser une grande somme pour la mise en place de cette solution. | Moins flexible, fonction uniquement sur des équipements propriétaire Cisco | Complexité de configuration nécessite des compétences certifiées par Cisco |

TABLE 3.5 – Comparaison entre les 03 Solutions

## 3.8 Solution choisie

Après avoir considéré les différentes options, FreePBX a été choisi comme la solution optimale pour Collable. Cette décision repose sur plusieurs facteurs :

- **Coût :** FreePBX est une solution open source, ce qui élimine les coûts de licence. L'utilisation du serveur existant élimine également les coûts matériels.
- **Flexibilité et Personnalisation :** Étant basé sur Asterisk, FreePBX offre une grande flexibilité et une capacité de personnalisation étendue. Cela permet d'adapter le système exactement aux besoins spécifiques de COLLABLE.
- **Interface Utilisateur Web :** FreePBX dispose d'une interface utilisateur web conviviale qui simplifie la configuration et la gestion du système téléphonique. Même pour les utilisateurs non techniques, cette interface intuitive facilite la gestion quotidienne et réduit la dépendance à l'égard de compétences techniques avancées.
- **Support :** Bien que moins robuste que le support commercial, FreePBX bénéficie d'une large communauté d'utilisateurs et de développeurs actifs. Cela signifie qu'il existe une abondance de documentation, de forums et de ressources en ligne pour résoudre les problèmes et obtenir de l'aide en cas de besoin.
- **Coûts de Maintenance :**les coûts de maintenance pour FreePBX sont considérablement réduits par rapport à des solutions commerciales.

Pour assurer la sécurité des communications, nous allons mettre en place des VLANs (Virtual Local Area Networks). En outre, un canal VPN (Virtual Private Network) sera établi entre les sites de COLLABLE et entre les entreprises clientes de COLLABLE en utilisant pfSense, qui intègre le protocole IPsec (Internet Protocol Security). Bien que pfSense soit déjà en place, il n'est pas encore configuré. L'IPsec fournit des mécanismes de cryptage, d'authentification et d'intégrité des données, garantissant ainsi la confidentialité et la protection contre les attaques potentielles.

## 3.9 Conclusion

Dans ce chapitre, nous avons présenté le centre téléphonique COLLABLE qui a besoin d'une implémentation d'une solution VoIP. On a commencé par explorer l'infrastructure, Proposé différentes solutions VoIP et enfin le choix de la solution.

## 3.10 Conclusion générale

La VoIP (Voix sur IP) offre une multitude de fonctionnalités allant bien au-delà de la simple transmission vocale, permettant aux entreprises de centraliser leurs communications via un seul protocole IP. Cette technologie, en plus de réduire les coûts, optimise également le système d'information des entreprises. Notre objectif est donc de mener une étude approfondie pour identifier les différentes solutions et techniques disponibles, en tenant compte de l'infrastructure existante chez groupe COLLABLE.

Le centre téléphonique possède un site unique , mais envisage de s'étendre. Pour que l'entreprise puisse géré ses communications téléphoniques, nous avons proposé d'intégrer la VoIP en installant un serveur PBX. Cette solution inclut également la création de VLANs et la mise en place d'un VPN pour sécuriser les communications, créant ainsi un environnement cohérent et harmonisé.

Le VPN, technologie en pleine expansion, joue un rôle crucial dans l'interconnexion des sites et la sécurisation des accès distants. Il offre un accès distant sécurisé, ce qui en fait bien plus qu'une simple nécessité économique pour les entreprises. Parmi ses nombreux avantages, on note sa simplicité d'installation et sa transparence pour les utilisateurs, ainsi que la possibilité d'intégrer divers services tels que la VoIP.

Des tests ont été effectués en utilisant un tunnel VPN IPsec pour simuler l'extension future et sécuriser les communications. Ces tests ont confirmé la faisabilité de notre solution pour résoudre le problème principal.

La réalisation de ce projet nous a permis d'acquérir de nouvelles connaissances sur les protocoles VoIP, tels que SIP et IAX, ainsi que sur les protocoles de sécurité. Nous avons approfondi notre compréhension de leur fonctionnement et de leurs principes grâce à une étude détaillée. Pour l'avenir, la prochaine étape sera l'application concrète de ces connaissances. Il serait également pertinent d'étendre cette étude à d'autres entreprises pour partager notre expérience et contribuer à l'avancement de ce domaine.

# Bibliographie


[1] https ://zadarma.com/fr/blog/voip-avantages-et-inconvenients/ publié le 20.09.2023 par la société de communication ZADARMA, consulté le 30.04.2024

[2] CUNHA José, VoIP et Asterisk/Trixbox, Métrise en Systèmes Distribués et Réseaux, Université de Franche Comté, 2008.

[3] https ://ami-gestion.fr/acces-telephonie-ip/ publié le le 03/04/2024 par la société AMI GESTION, consulté le 30.04.2024

[4] https ://www.ringover.fr/blog/toip publié le 11 janvier 2021 par RINGOVER GROUPE, consulté le 30.04.2024

[5] Guy PUJOLLE, Les Réseaux, Eyrolles, Paris, 2003.

[6] Laurent Ouakil et Guy Pujolle, Voix sur IP - Réseaux et téléphonie sur IP, Eyrolles, 26 juin 2008, ISBN 978-2-212-12359-3.

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

[8] L. OUAKIL, G. PUJOLLE, Téléphonie sur IP, 2eme édition Eyrolles.

[9] Ahmed Aouadi,Mise en place d'une solution open Source VoIP et Visioconférence multi-sites sécurisée,Université Virtuelle de Tunis ,mémoire de fin d'étude, juillet 2015.

[10] https ://www.rapport-gratuit.com/vulnerabilites-contre-la-voip-et-quelques-moyens-de-securisation/ Consulté le 30/04/2024

[11] Elyazid NOUREDDINE, Sid ali CHAFA, Étude et mise en place d'une solution VoIP sécurisée, Université Mouloud Mammeri De Tizi-Ouzou, mémoire de fin d'étude, 2015.

[12] https ://www.frameip.com/voip/ Consulté le 30/04/2024

[13] https ://www.vpnfreeway.net/eclients/index.php ?rp=/knowledgebase/4/VPN-et-VOIP.html Consulté le 30/04/2024

[14] https ://www.academia.edu/39080897/CHAPITRE III RISQUES ET METHODES DE SECURITE DE La VOIP publié par Rhouma Imen, consulté le 01/05/2024

[15] https ://www.provya.net/ ?d=2019/05/14/15/14/04-asterisk-securiser-efficacement-et-simplement-son-serveur-avec-iptables-et-fail2ban publié le 14/05/2019 par provya, consulté le 01/05/2024

[16] JF. PILLOU, JF.BAY, Tout sur la sécurité informatique, 4eme édition Dunod, 2016.

[17] https ://fr.linkedin.com/pulse/comprendre-et-contrer-les-attaques-man-in-the-middle-harrys-phills publie le 16/07/2023, consulté le 25/05/2024

[18] Jacob NDWO MAYELE , Déploiement d'un coeur de réseau ip/mpls, cas de la banque centrale du congo,Université de kinshasa, Mémoire de Licence en Génie Informatique, 2017.

[19] Rahmani Tinhinan, Sadaoui Fadhila, Etude et mise en place d'un réseau VPN, UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU, Mémoire de Master en Réseaux et Télécommuni- cation, 2017.

[20] Eric BAHATI - SHABANI , MISE EN PLACE D'UN RESEAU VPN AU SEIN D'UNE EN- TREPRISE, Institut supérieur de commerce Kinshasa , Mémoire de Licence en Informatique de Gestion, 2011.

[21] ipsec(internet protocole security) , Centre Universitaire Nour Bachir , 2020.

[22] Nadia BATTAT, Les systèmes de sécurité, cours Sécurité des infrastructures de télécommunica- tion, Université A/Mira Bejaia, 2022.

# Annexe 1

## Implémentation et réalisation

# Présentation de l'environnement de travail

Dans cette section, nous allons décrire en détail l'environnement de travail qui a été mis en place pour mener à bien ce projet. Cette présentation inclura une description des équipements matériels utilisés ainsi que les logiciels et outils spécifiques employés tout au long de notre démarche. Comprendre cet environnement est essentiel pour apprécier pleinement les conditions et les ressources qui ont permis la réalisation des différentes étapes du projet

**GNS3** Est un logiciel de simulation des réseaux informatiques. Il permet aux utilisateurs de créer des topologies réseau virtuelles en utilisant des dispositifs virtuels et des images d'exploitation réelles provenant de divers fournisseurs tel que Cisco. GNS3 est utilisé par les professionnels des réseaux, les ingénieurs système et les étudiants pour concevoir, tester et déployer des ar- chitectures réseau virtuelles avant de les mettre en œuvre dans un environnement réel. C'est un logiciel gratuit qui fonctionne sur plusieurs plates-formes, y compris Windows, Linux et MacOs.

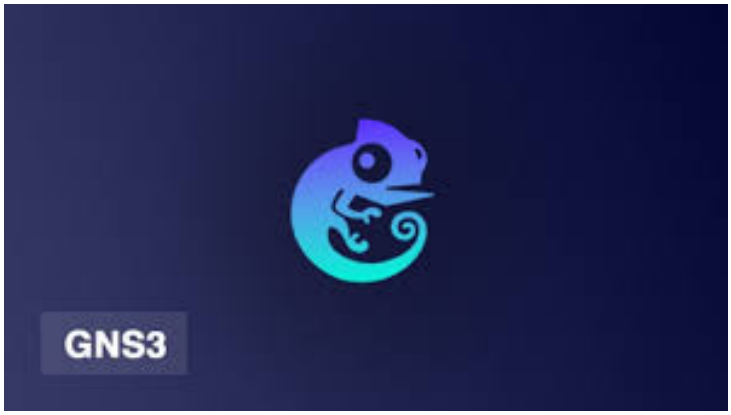


FIGURE 3.6 – GNS3

**VMware** Une machine virtuelle (VM) est un environnement entièrement virtualisé qui s'exécute sur une machine physique. Elle exécute son propre système d'exploitation (OS) et bénéficie des mêmes équipements qu'une machine physique : CPU, mémoire RAM, disque dur et carte ré- seau.Elle permet d'exécuter plusieurs systèmes d'exploitation et applications simultanément sur une même machine physique [25].

FIGURE 3.7 – VMware[25]

**PFsense** Pfsense ou « Packet Filter Sense » est un applicatif qui fait office de routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. Il permet d'analyser, de sécuriser et de gérer le trafic réseau pour empêcher tout accès non autorisé à ce réseau.[26]


FIGURE 3.8 – PFsense[26]

**FreePBX** FreePBX est une interface utilisateur graphique (GUI) open source basée sur le web qui gère le serveur de téléphonie Asterisk. Il a été développé par la société Sangoma en 2004 [27].


FIGURE 3.9 – FreePBX[27]

**Softphone** Est un logiciel de téléphonie utilisé pour effectuer des appels téléphoniques sur Internet à partir d'un ordinateur plutôt que d'un téléphone [28].Nous utilisons les deux softphones 3CX et X- Lite pour tester nos appels téléphoniques.


FIGURE 3.10 – Softphone

# Equipements utilisés

| Site | Equipements | Types | Image |
|---|---|---|---|
| Bejaia | Par-feu | Pfsense | 2.7.2 |
| | Switch SWD | Cisco 3750 N3 | IOU UNIX |
| | Switch access | Cisco 2690 | IOU UNIX |
| | FreePBX | 16.0.19 | Centos |
| Alger | Par-feu | Pfsense | 2.7.2 |
| | Switch access | Cisco 2690 | IOU UNIX |
| | FreePBX | 16.0.19 | Centos |

TABLE 3.6: Equipements de simulation

# Méthodologie du travail

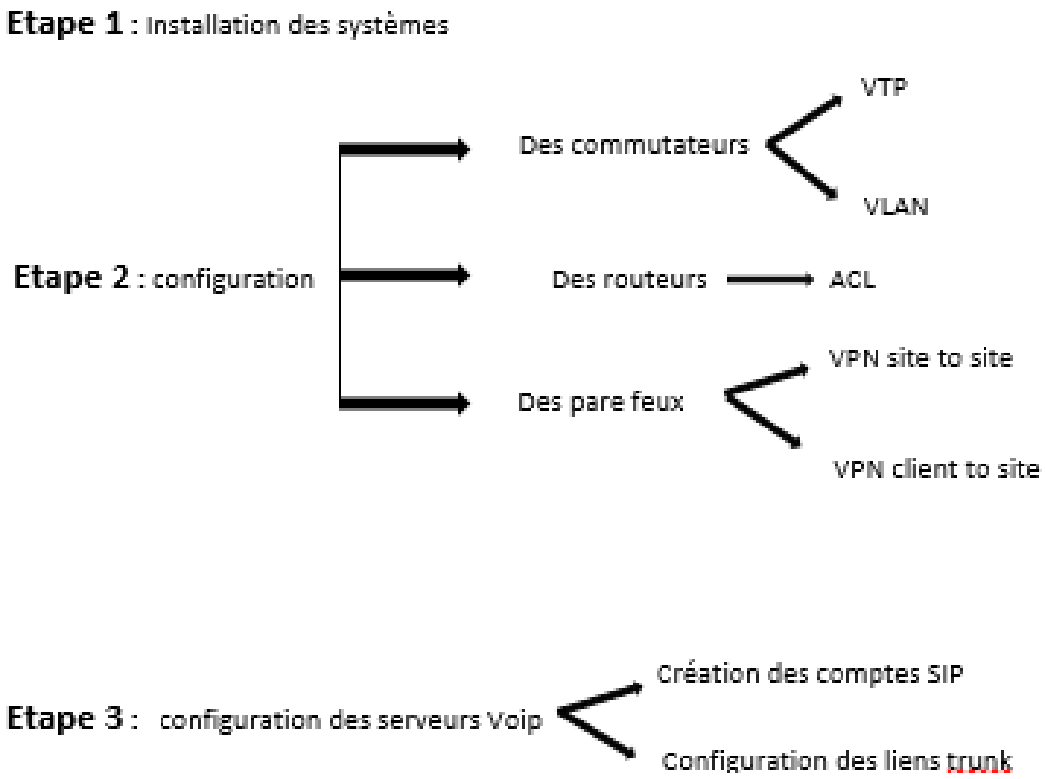


FIGURE 3.11 – Méthodologie du travail

# Architecture de simulation

La figure 3.12 représente l'architecture sur laquelle les configuration seront eféctuées pour gérer les communications VoIP de maniére sécurisées. Sachant que :

- le site COLLABLE d'alger est en cours de construction
- Les étapes de configuration de chaque équipement du site d'ALGER se fera de la méme façon que le site de Bejaia

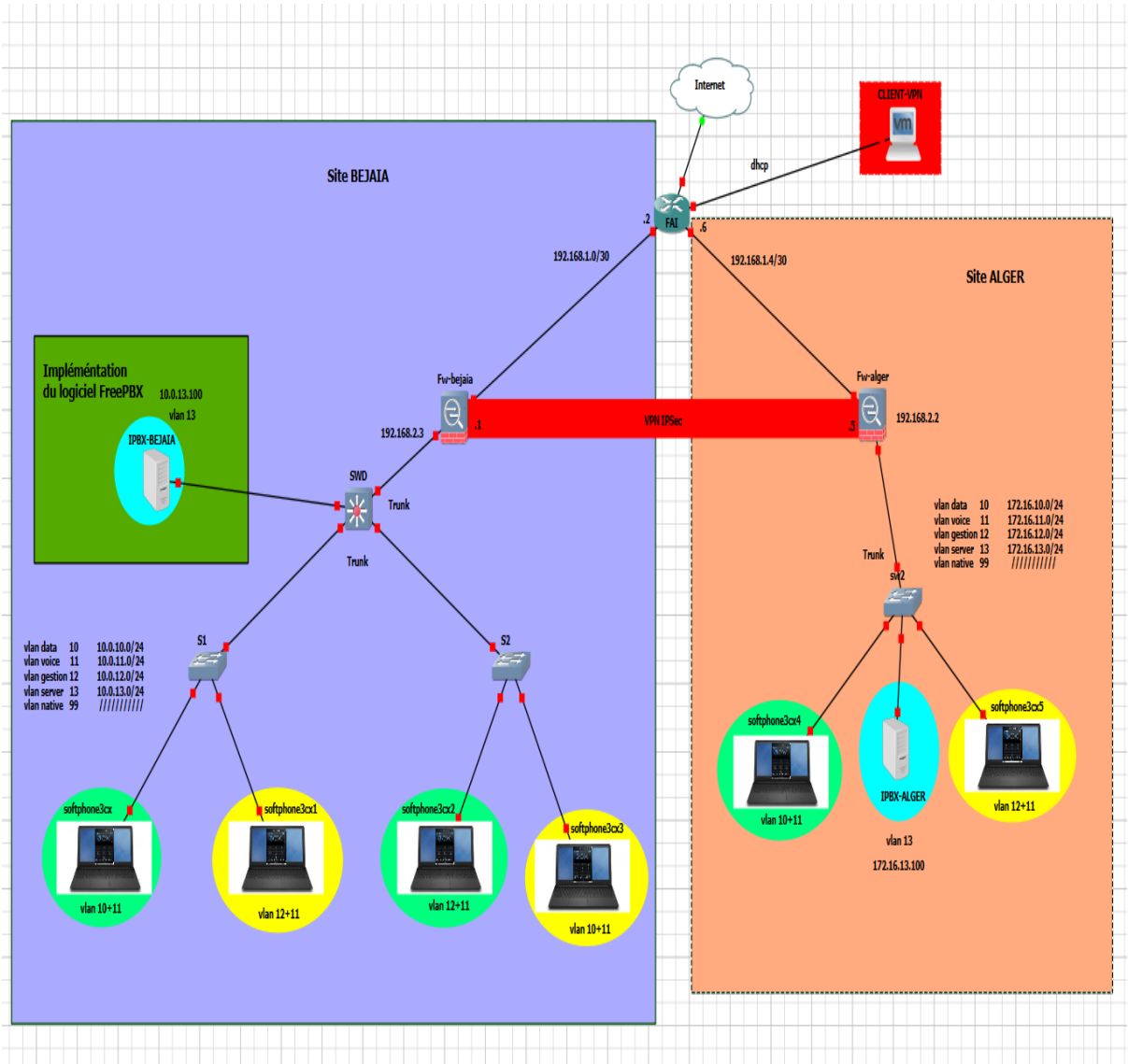


FIGURE 3.12 – Architecture de simulation

# Installation des systèmes

## PFsense

- La figure 3.13représente le lancement de l'installation du PFsense


FIGURE 3.13 – Lancement de l'installation du PFsense

- Une fois qu'on clique sur "Accepter" pour confirmer l'installation et qu'on suit les options par défaut, l'installation de pfSense démarre.


FIGURE 3.14 – Instalation en cours

En suivant ces étapes, pfSense sera installé avec succès, et on bénéficiera de ses fonctionnalités avancées de pare-feu et de routage.

## FreePBX

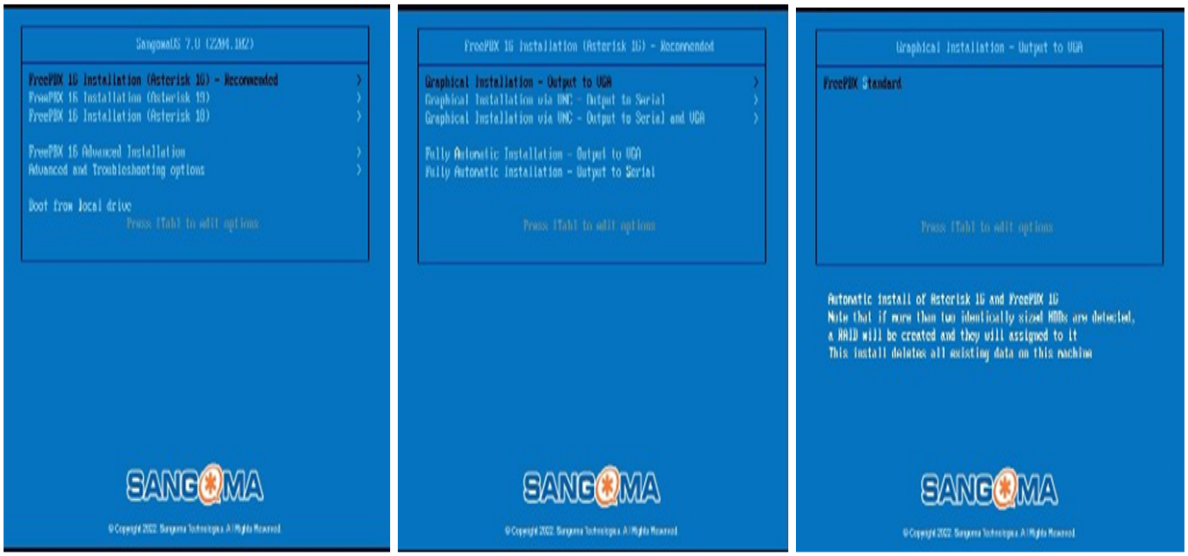


FIGURE 3.15 – Installation de FreePBX

Une fenêtre de paramétrage d'avant installation apparaitra. Nous définissons la date et l'heure, la langue du clavier et le mot de passe qui sera utilisé par l'administrateur pour accéder aux configurations de FreePBX.

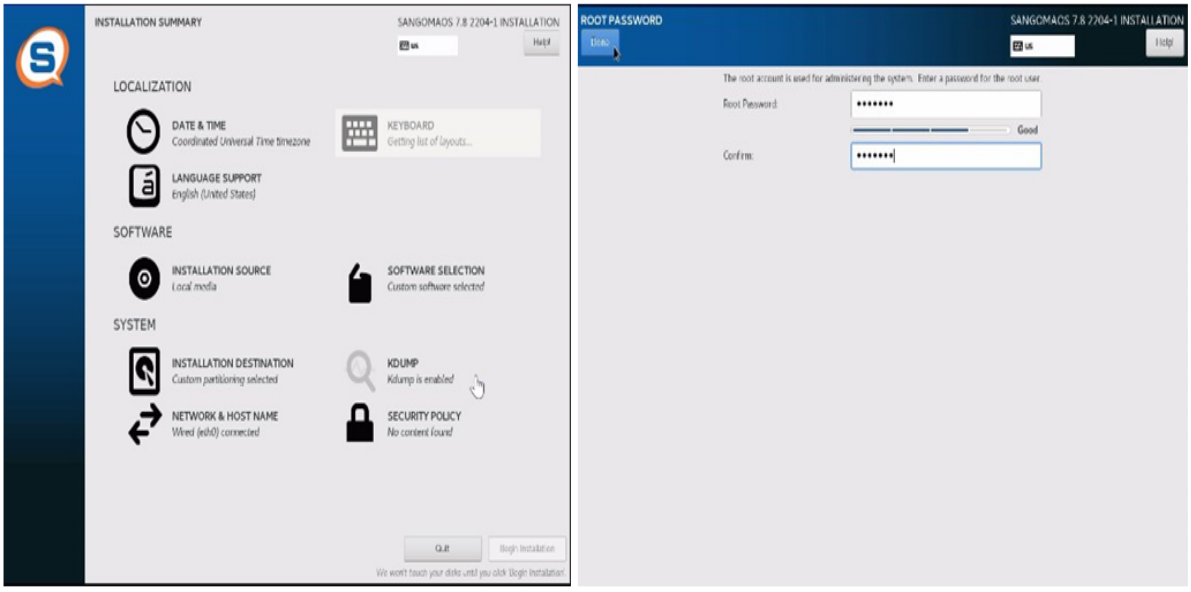


FIGURE 3.16 – Installation de FreePBX

Une fois les configurations enregistrées, l'installation de FreePBX va se lancer. À la fin de l'installation, on obtiendra une adresse IP avec laquelle on accédera à l'interface web de FreePBX.


FIGURE 3.17 – Ligne commande freepbx

# Configurations de base

## Tables d'adressage

## Equipements

| Dispositif | Interface | Adresse IP | Description |
|---|---|---|---|
| FAI | E0/0 | DHCP | Connecté sur internet |
| | E0/1 | 192.168.1.2/30 | Connecté au F-Bejaia |
| | E0/2 | 192.168.1.6/30 | Connecté au F-Alger |
| | E0/3 | DHCP | Connecté au VPN-Client |
| Switch Distribution (SWD) | E0/0 | En mode trunk | Connecté au pfsense Bejaia |
| | E2/1 | En mode trunk | Connecté au S1 |
| | E2/2 | En mode trunk | Connecté au S2 |
| | E3/3 | En acces (VLAN 13) | Connecté aU FreePBX |
| Switch accès (S1) | E0/0 | En mode trunk | Connecté au SWD |
| | E0/1 | En mode access (Vlan 12) | Connecté au PC1 |
| | E0/2 | En mode access (Vlan 10) | Connecté au PC2 |
| Switch accès (S2) | E0/0 | En mode trunk | Connecté au SWD |

| | | | |
|---|---|---|---|
| | E0/1 | En mode access | Connecté au PC3 |
| | E0/2 | En mode acces | Connecté au PC4 |
| Switch Alger | E0/0 | en mode trunk | Connecté au Pfsense Alger |
| | E0/1 | En mode accès | Connecté au Pc5 |
| | E0/2 | En mode accès | Connecté au Pc6 |
| pfsense Alger | Em2 | / | Connecté à S-Alger |
| | Em0 | 192.168.1.5/30 | Connecté au FAI (wan) |
| pfsense Bejaia | Em0 | 192.168.1.1/30 | Connecté au FAI (wan) |
| | Em2 | / | Connecté au SWD |

TABLE 3.7: Tableau d'adressage des dispositifs réseau

## VLANs

| VLAN | Adresse IP (BEJAIA) | Adresse IP (ALGER) |
|---|---|---|
| VLAN10 | 10.0.10.0/24 | 172.16.10.0/24 |
| VLAN11 | 10.0.11.0/24 | 172.16.11.0/24 |
| VLAN12 | 10.0.11.0/24 | 172.16.12.0/24 |
| VLAN13 | 10.0.11.0/24 | 172.16.13.0/24 |

TABLE 3.8: Tableau d'adressage des VLANs

## Configuration des commutateurs

## Création des Vlans

- la figure 3.18 montre les étapes de création des VLANs

```
SWD#Conft
SWD (config)#vlan 10
SWD (config)#name data
SWD (config)#vlan 11
SWD (config)#name voice
SWD (config)#vlan 12
SWD (config)#name gestion
SWD (config)#vlan 13
SWD (config)#name server
SWD (config)#vlan 99
SWD (config)#name native
SWD (config)#end
```

FIGURE 3.18 – Creation des VLANs

## Configuration du VTP

- La figure 3.19 montre les étapes de configuration du VTP mode server au niveau de SWD

```
SWD#Conf t
SWD(config)#vtpmode server
SWD(config)#vtp password collable2024*
SWD(config)#vtp domain collable
SWD(config)#vtp version 2
SWD(config)#vtp pruning
SWD(config)#end
```

FIGURE 3.19 – Configuration du vtp en mode server

- La figure 3.10 montre les étapes de configuration du VTP mode client au niveau de S1

```
S1#Configure  terminal
S1(config)#vtp mode client
S1(config)#vtp domain collable
S1(config)#vtp password collable2024*
S1(config)#vtp version 2
S1(config)#end
```

FIGURE 3.20 – Configuration du vtp en mode client

- La figure 3.21 montre les étapes de configuration du VTP mode client au niveau de S2

```
S2#Configure  terminal
S2(config)#vtp mode client
S2(config)#vtp domain collable
S2(config)#vtp password collable2024*
S2(config)#vtp version 2
S2(config)#end
```

FIGURE 3.21 – Configuration du vtp en mode client

### Configuration des interfaces en mode trunk

- La figure 3.22 représente la configuration des interfaces ethernet 2/1 et 2/2 on mode trunk au niveau de SWD

```
SWD#Configure terminal
SWD(config)#interface range ethernet 2/1-2
SWD(config-if-range)#switchport trunk encapsulation dot1q
SWD(config-if-range)#switchport mode trunk
SWD(config-if-range)#exit
```

FIGURE 3.22 – Interfaces en mode trunk

- La figure 3.23 représente la configuration de l'interfaces ethernet 0/0 on mode trunk au niveau de S1

```
S1#Configure terminal
S1(config)#interface ethernet 0/0
S1(config-if)#switchport trunk encapsulation dot1 q
S1(config-if)#switchport mode trunk
S1(config-if)#end
```

FIGURE 3.23 – Interface en mode trunk

- La figure 3.24 représente la configuration de l'interfaces ethernet 0/0 on mode trunk au niveau de S2

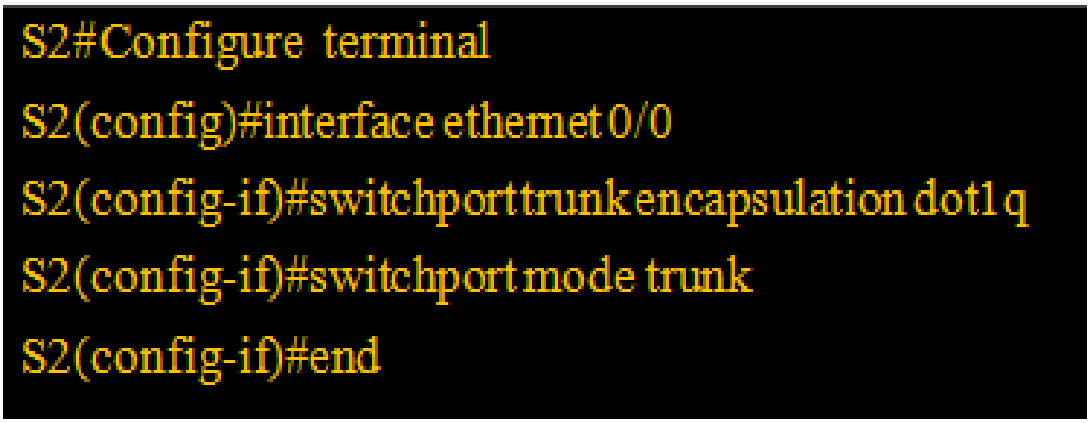


FIGURE 3.24 – Interface en mode trunk

### Configuration des interfaces en mode access

- La figure 3.25 représente la configuration de l'interfaces ethernet 3/3 on mode access au niveau de SWD

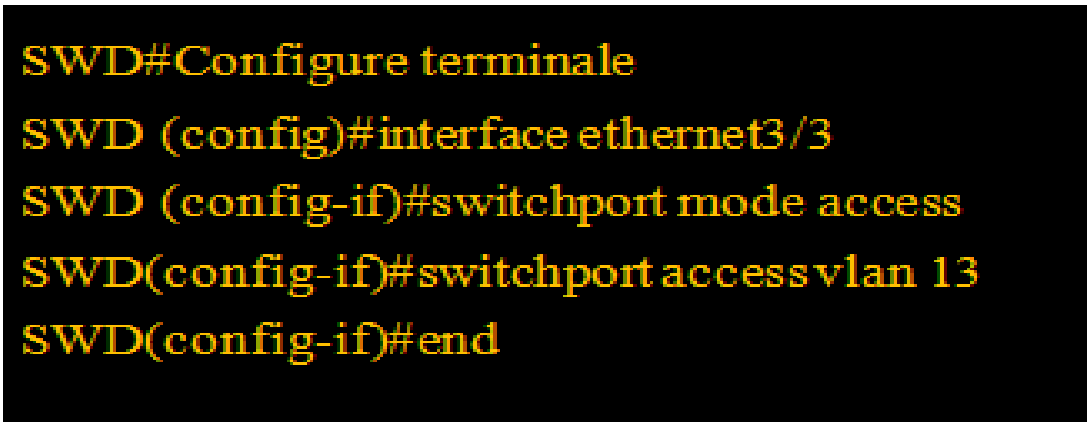


FIGURE 3.25 – Configuration de l'interface ethernet3/3 en mode access

- La figure 3.26 représente la configuration de l'interfaces ethernet 0/2 on mode access au niveau de S1

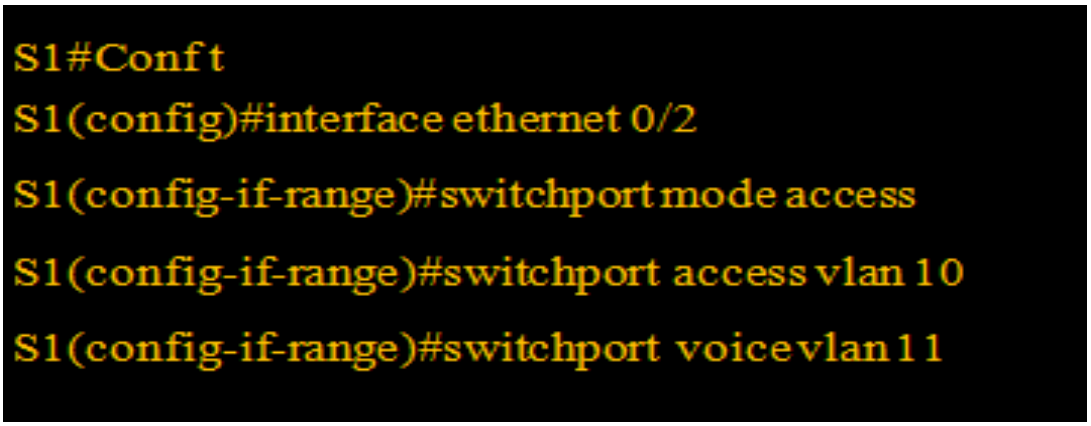


FIGURE 3.26 – Configuration de l'interface ethernet0/2 en mode access

- La figure 3.27 représente la configuration de l'interfaces ethernet 0/1 on mode access au niveau de S1

```
S1#Conf t
S1(config)#interface ethernet 0/1
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 12
S1(config-if-range)#switchport voice vlan 11
```

FIGURE 3.27 – Configuration de l'interface ethernet0/1 en mode access

- La figure 3.28 représente la configuration de l'interfaces ethernet 0/2 on mode access au niveau de S2

```
S2#Conf t
S2(config)#interface ethernet 0/2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#switchport voice vlan 11
```

FIGURE 3.28 – Configuration de l'interface ethernet0/1 en mode access

- La figure 3.29 représente la configuration de l'interfaces ethernet 0/1 on mode access au niveau de S2

```
S2#Conf t
S2(config)#interface ethernet 0/1
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 12
S2(config-if-range)#switchport voice vlan 11
```

FIGURE 3.29 – Configuration de l'interface ethernet0/2 en mode access

## Configuration du routeur

- La figure 3.30 représente la configuration des adresses IP des interfaces WAN.

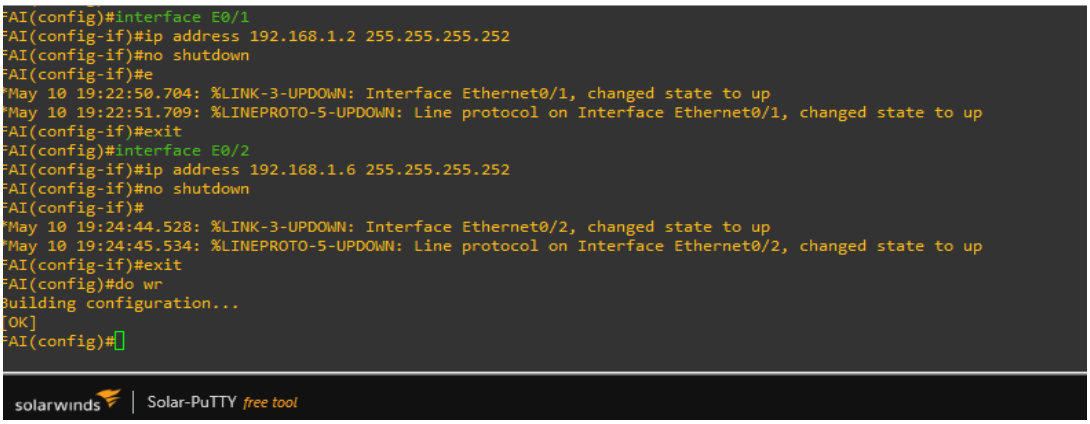


FIGURE 3.30 – Configuration des interfaces WAN E0/1 etE0/2

- La figure 3.31 représente la configuration de l'interface INTERNET

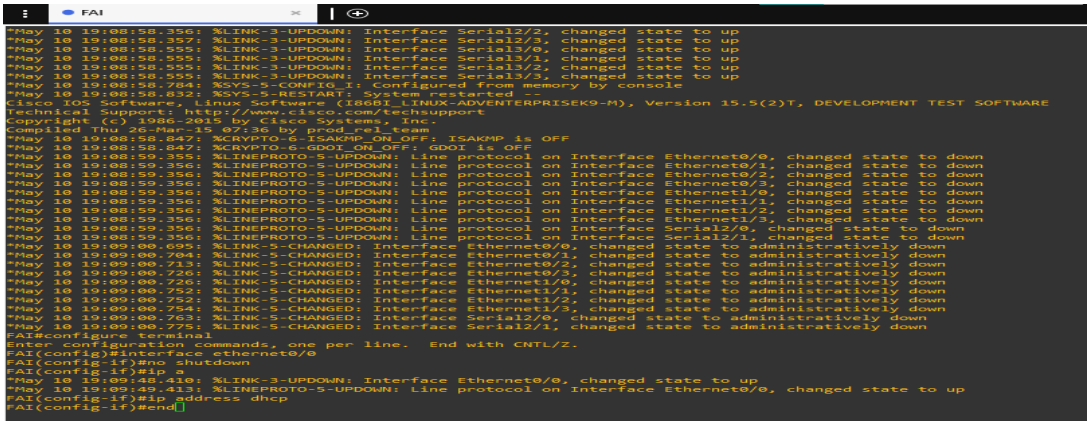


FIGURE 3.31 – Configuration de l'interface INTERNET

# Configuration du pare-feu

## Configuration des interfaces WAN et LAN

- La figure 3.32 représente la configuration de l'interface LAN

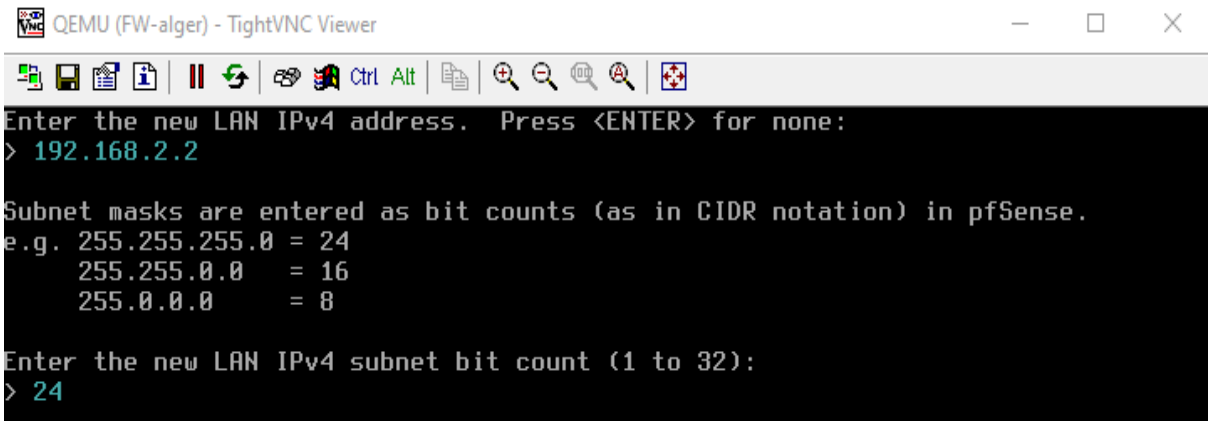


FIGURE 3.32 – Configuration de l'interface LAN

- La figure 3.33 représente la configuration de l'interface WAN

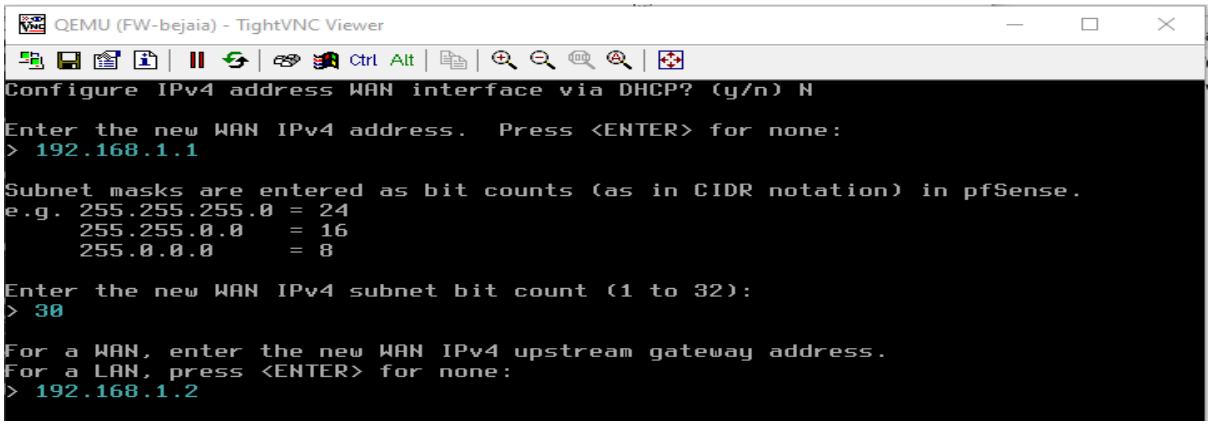


FIGURE 3.33 – Configuration de l'interface WAN

- Une fois que les interfaces sont configurées, il suffit de taper l'adresse LAN du pare-feu dans un navigateur pour commencer les configurations, comme le montre la figure 3.34.

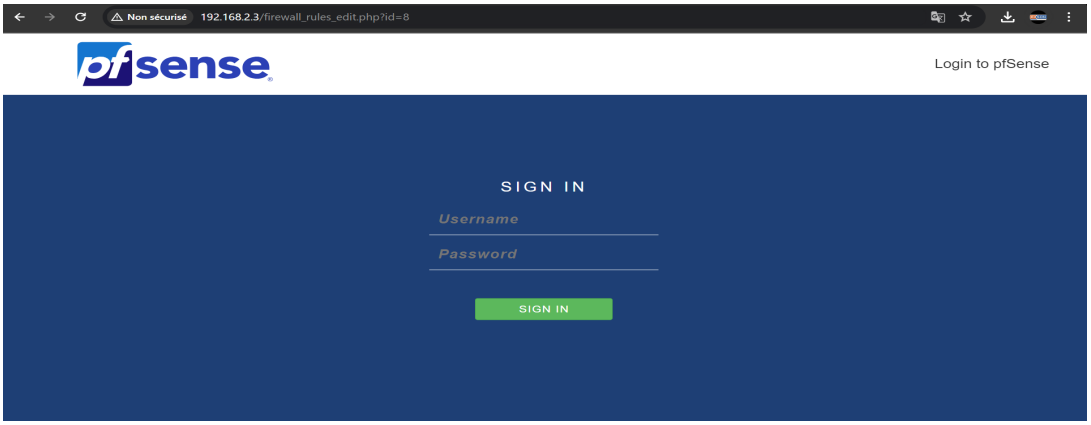


FIGURE 3.34 – Interface web login du PfSense

- Lorsque nous accédons à cette adresse pour la première fois, on voit une page de connexion comme montré dans la figure 3.34. On utilise les informations de connexion par défaut : Nom d'utilisateur : admin Mot de passe : pfsense

## création d'une interface dédier aux VLANs

- Une fois qu'on accède à l'interface web, on se dirige vers la rubrique "Interface Assignement", puis on ajoute l'interface nommée em2 de pfsense comme montré dans la figure suivantes

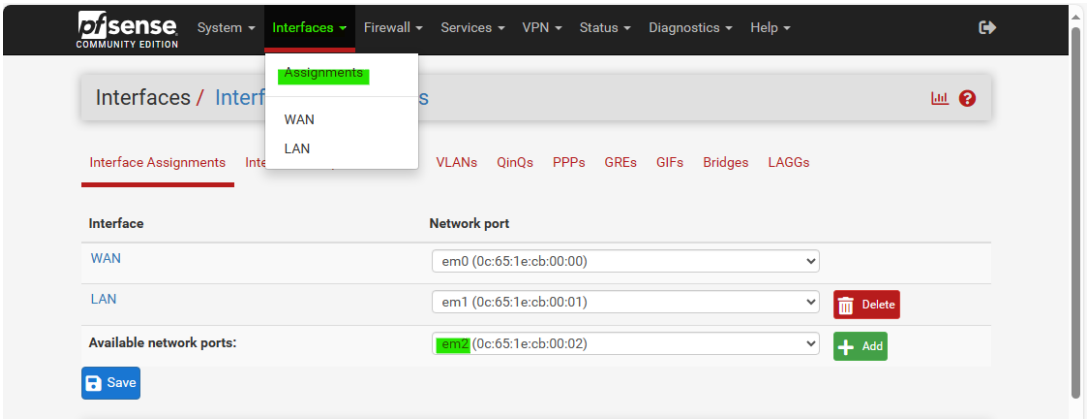


FIGURE 3.35 – ajout de l'interface de em2

- Maintenant, nous allons créer nos VLANs dans pfSense. Pour ce faire, nous allons dans le menu principal, sélectionnons "Interfaces", puis "Assignments", et cliquons sur l'onglet "VLANs" comme le montre la figure 3.36

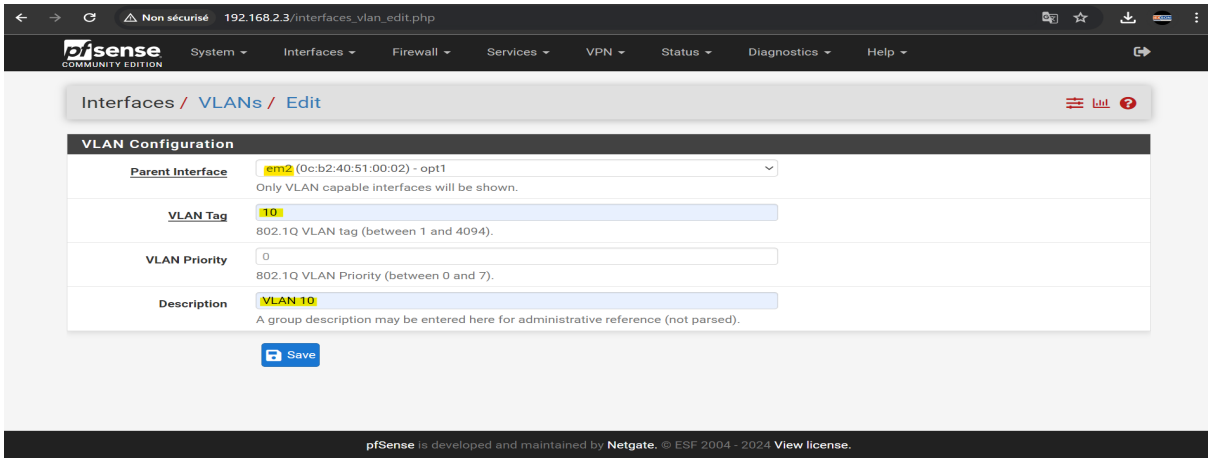


FIGURE 3.36 – Ajout de vlan 10

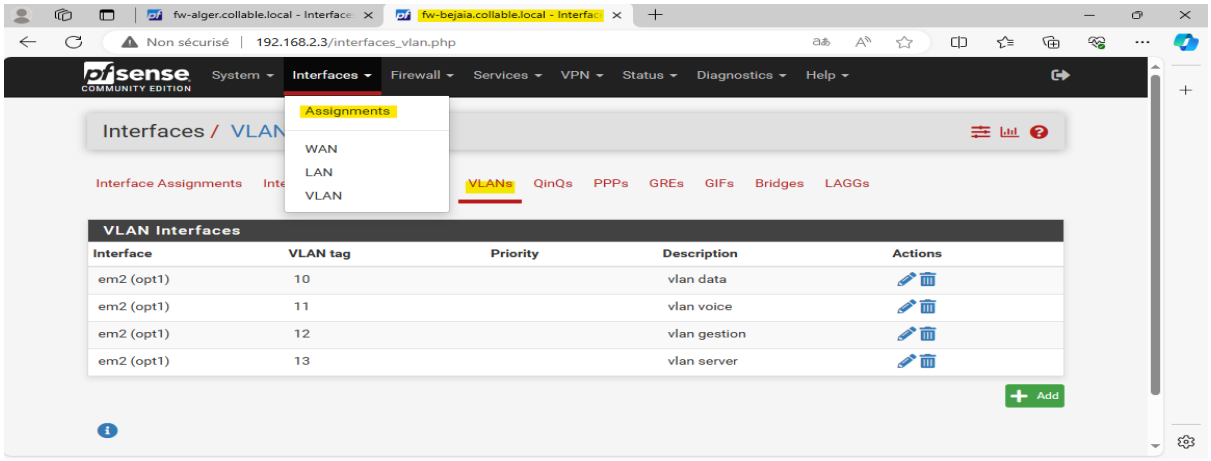


FIGURE 3.37 – Ajoute des VLANs

## Routage inter-VLANs

## Assignation des interfaces aux VLANs

Retournons dans le menu "Interfaces" puis "Assignments". Dans la section "Available network ports", on sélectionne les VLANs que nous avons créés un par un (par exemple, VLAN 10 sur em2), puis on clique sur "Add" pour ajouter cette interface.

Cliquons sur le nom de l'interface nouvellement ajoutée (elle apparaîtra sous un nom comme OPT1).

Cochant la case "Enable Interface". Donnons un nom à l'interface (par exemple, "LAN VLAN10").

Configurer les paramètres IP :

IPv4 Configuration Type : Sélectionnons "Static IPv4" pour attribuer une adresse IP statique. IPv4 Address : Entrant l'adresse IP et le masque de sous-réseau. Enfin, cliquons sur "Save" pour enregistrer les paramètres de l'interface, et sur "Apply Changes" pour appliquer les modifications.

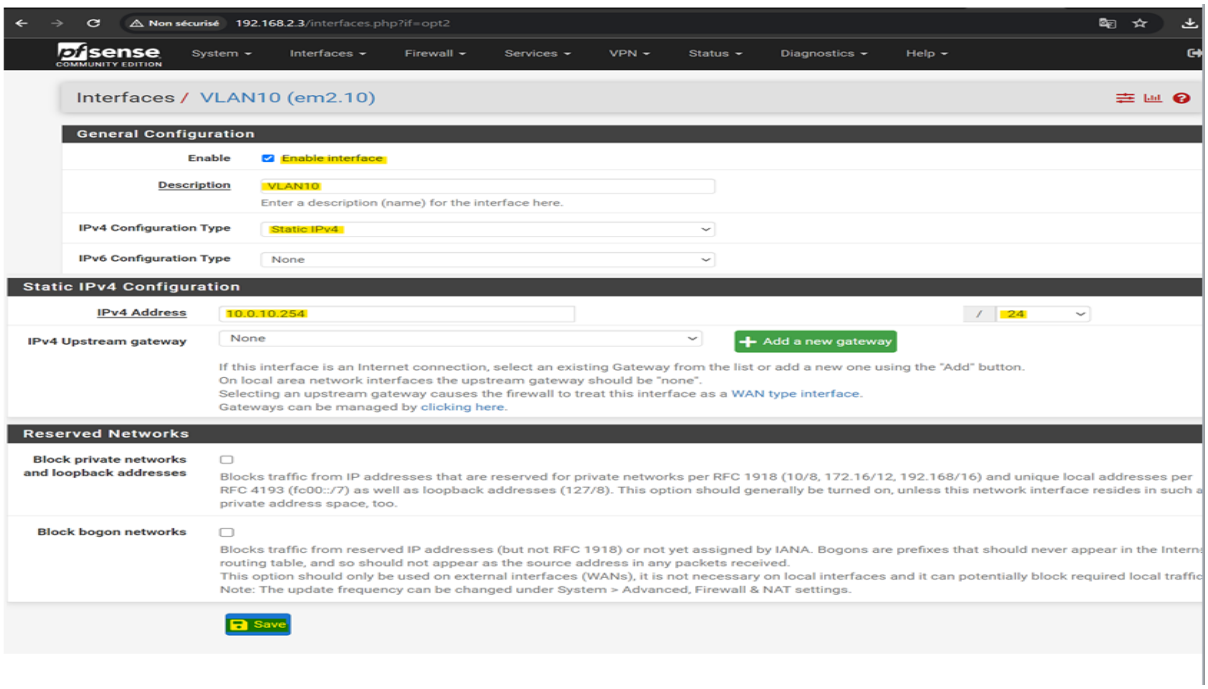


FIGURE 3.38 – Ajout des VLANs

## Configurer les règles de pare-feu pour permettre le routage inter-VLAN

Allons dans le menu "Firewall" puis "Rules". Sélectionnons l'interface VLAN ("VLAN10", "VLAN11", "VLAN12", "VLAN13").

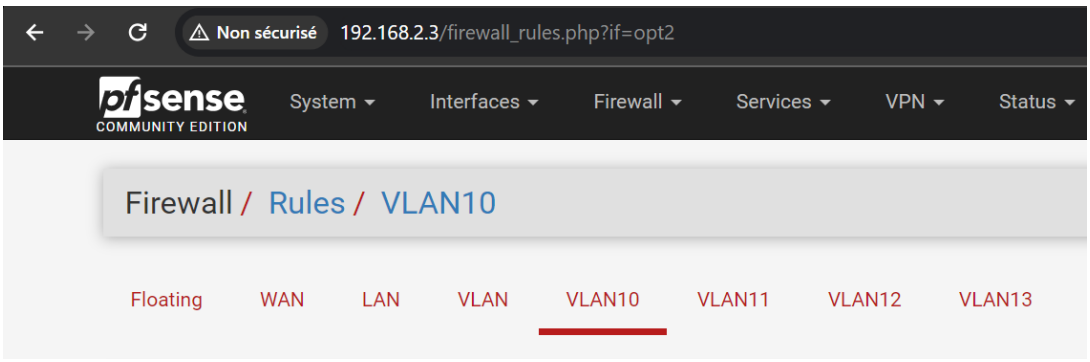


FIGURE 3.39 – Configuration les règles de pare-feu

- Cliquons sur "Add", puis configurons les paramètres suivants :
- Action : Sélectionnons "Pass".
- Interface : Sélectionnons l'interface VLAN.
- Address Family : Sélectionnons "IPv4".
- Protocol : Sélectionnons "Any".
- Source : Sélectionnons "VLAN10 subnet".
- Destination : Sélectionnons "Any".
- Description : Entrant une description pour cette règle.

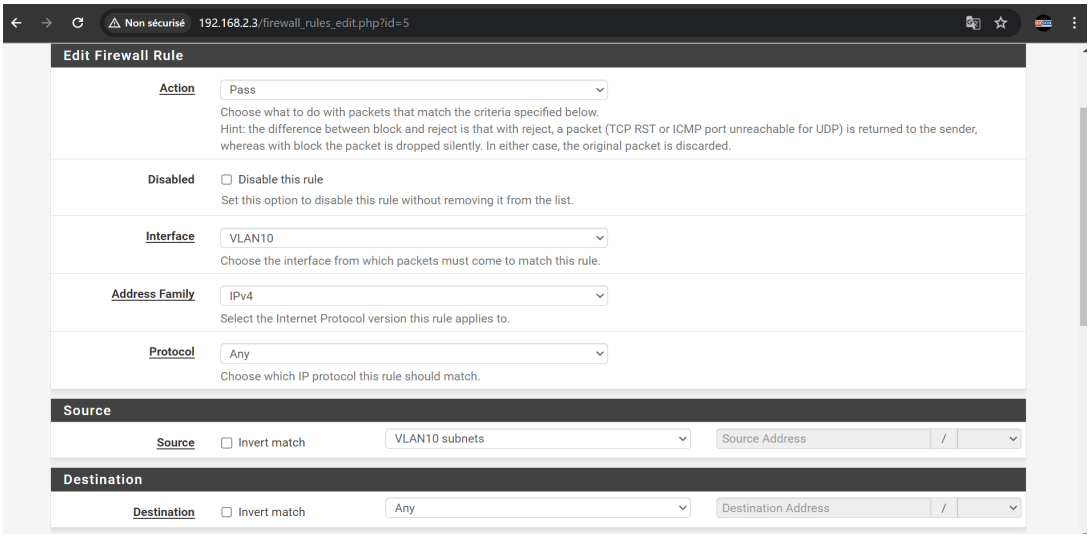


FIGURE 3.40 – Configuration les règles de pare-feu

Cliquons sur "Save" pour enregistrer la règle et répétons les étapes ci-dessus pour chaque interface VLAN, puis cliquons sur "Apply Changes" pour appliquer les modifications.

## Configuration du serveur DHCP dans pfSense

Sélectionnons dans le menu "Services", puis cliquons sur "DHCP Server".

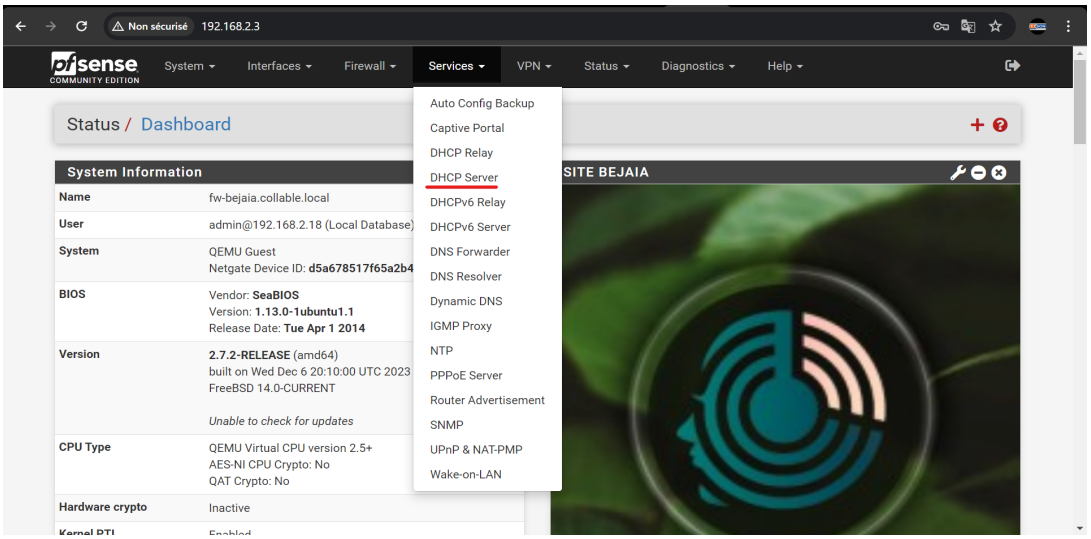


FIGURE 3.41 – accée au serveur DHCP

En haut de la page du serveur DHCP, on trouve des onglets pour chaque interface disponible (WAN, LAN, VLAN, etc.). Sélectionnons l'interface pour laquelle nous configurons le DHCP (VLAN10, VLAN11, VLAN12, VLAN13).

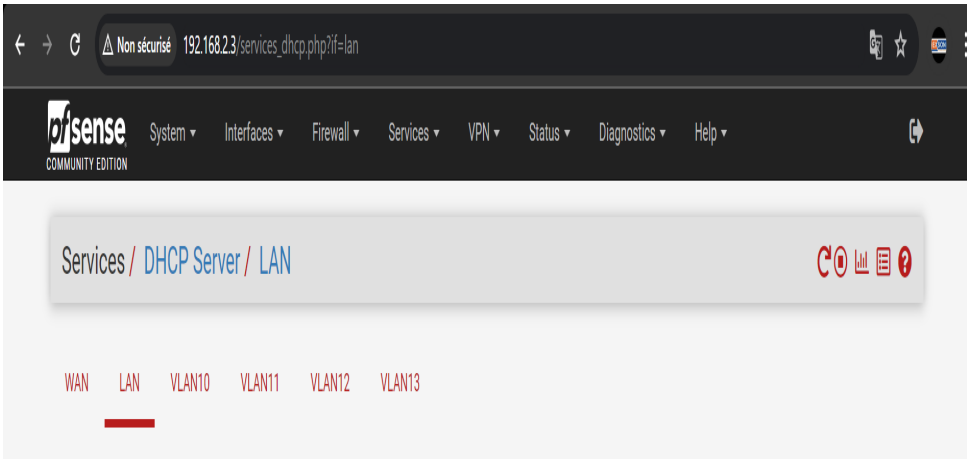


FIGURE 3.42 – interface disponible

- Activons le serveur DHCP pour cette interface en cochant la case "Enable DHCP server".
- Ensuite, configurons la plage d'adresses IP que le serveur DHCP doit attribuer dans les champs "Range".
- Configurons les serveurs DNS en entrant les adresses IP des serveurs DNS que les clients DHCP doivent utiliser.
- Configurons également la passerelle en entrant l'adresse IP de la passerelle que les clients DHCP doivent utiliser.
- Pour le domaine et le nom d'hôte, entrons le nom de domaine que les clients DHCP doivent utiliser dans le champ "Domain Name" et les domaines de recherche DNS dans le champ "Domain Search List" (tous deux facultatifs).
- Après avoir configuré les paramètres DHCP pour l'interface, cliquons sur "Save" en bas de la page pour enregistrer les modifications, puis sur "Apply Changes" en haut de l'interface pour les appliquer.

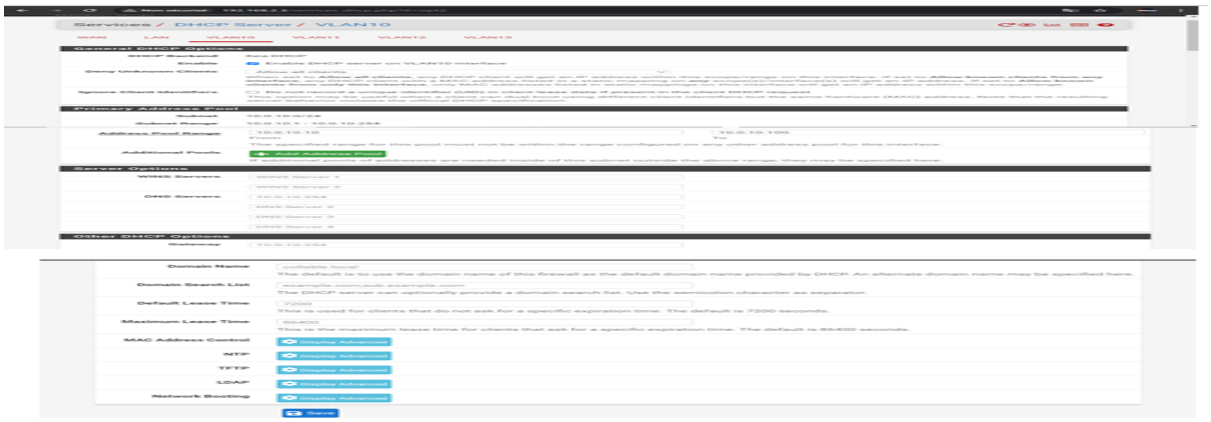

FIGURE 3.43 – configuration DHCP VLAN 10

## Configuration des VPN

## VPN site to site IPSec

Commençons par accéder à l'interface web de pfSense et allons dans VPN > IPsec pour ajouter une nouvelle Phase (Phase 1). Sélectionnons IKEv2 comme version d'échange de clés, choisissons l'interface WAN et entrons l'adresse IP publique de Site d'Alger comme passerelle distante. Utilisons l'authentification par clé pré-partagée (PSK) et définissons une clé partagée sécurisée. Pour les algorithmes de chiffrement et de hachage, sélectionnons AES256 et SHA256 respectivement, et utilisons le groupe DH 2 (1024 bits), puis enregistrons cette configuration.

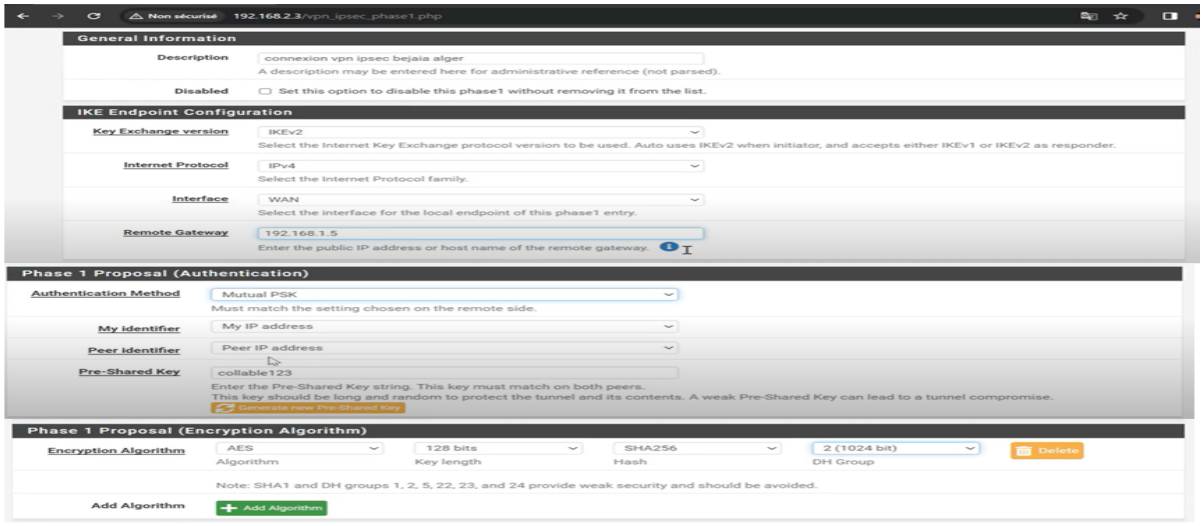


FIGURE 3.44 – phase1

Passons ensuite à la Phase 2, où nous configurerons le tunnel IPsec en sélectionnant le mode Tunnel IPv4 et en spécifiant les réseaux locaux de Site BEJAIA et Site d'Alger. Utilisons AES256 pour le chiffrement et SHA256 pour le hachage, avec le groupe PFS 2. Enregistrons et appliquons les modifications.

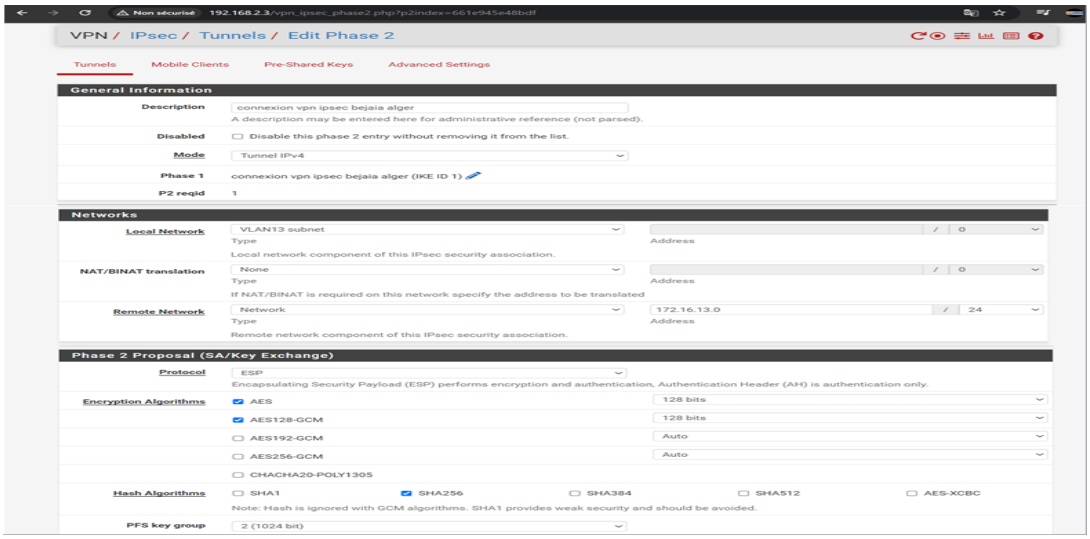


FIGURE 3.45 – phase2

Ensuite, pour permettre le trafic IPsec sur les deux sites, accédons à Firewall > Rules, sélectionnons l'onglet IPsec et créons une nouvelle règle pour autoriser tout le trafic IPsec. Appliquons les modifications.

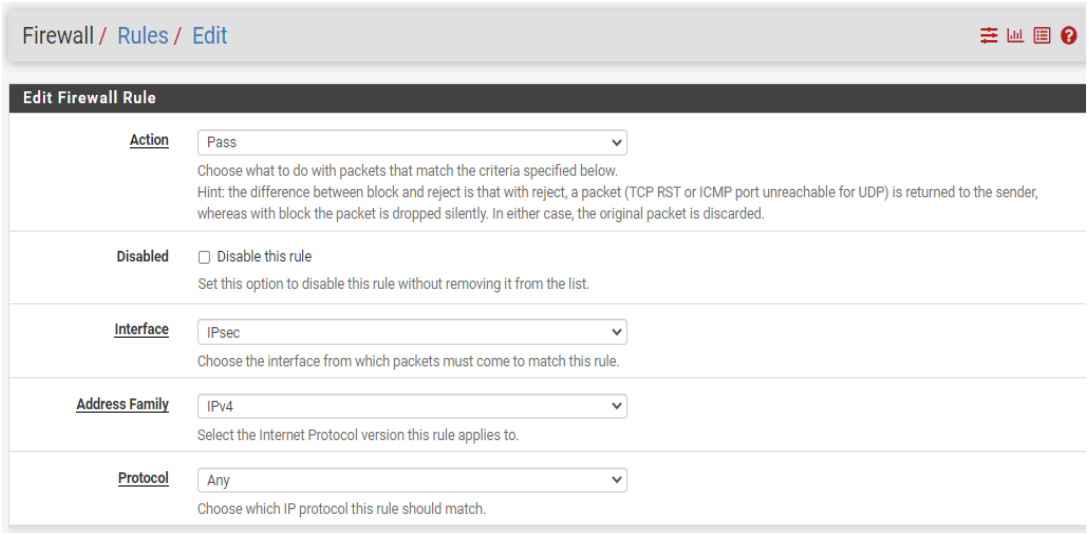


FIGURE 3.46 – Autorisation du trafic dans le tunnel

## VPN client to site

### Etape1 : Création d'un certificat d'autorité interne

- Tout d'abord nous devons créer une autorité de certification interne, dotée de son propre certificat, afin de pouvoir auto-signer les différents certificats créées. Nous aurons besoin de deux certificats en particulier : celui du serveur, qui sera utilisé au niveau du pfSense, et celui du client. Ces certificats seront signés par notre autorité de certification interne que nous allons crée.
- Création d'un certificat d'autorité interne Pour créer un certificat d'autorité, nous allons sur : Système=>Certfificat manager et nous choisis- sons la méthode " authority".

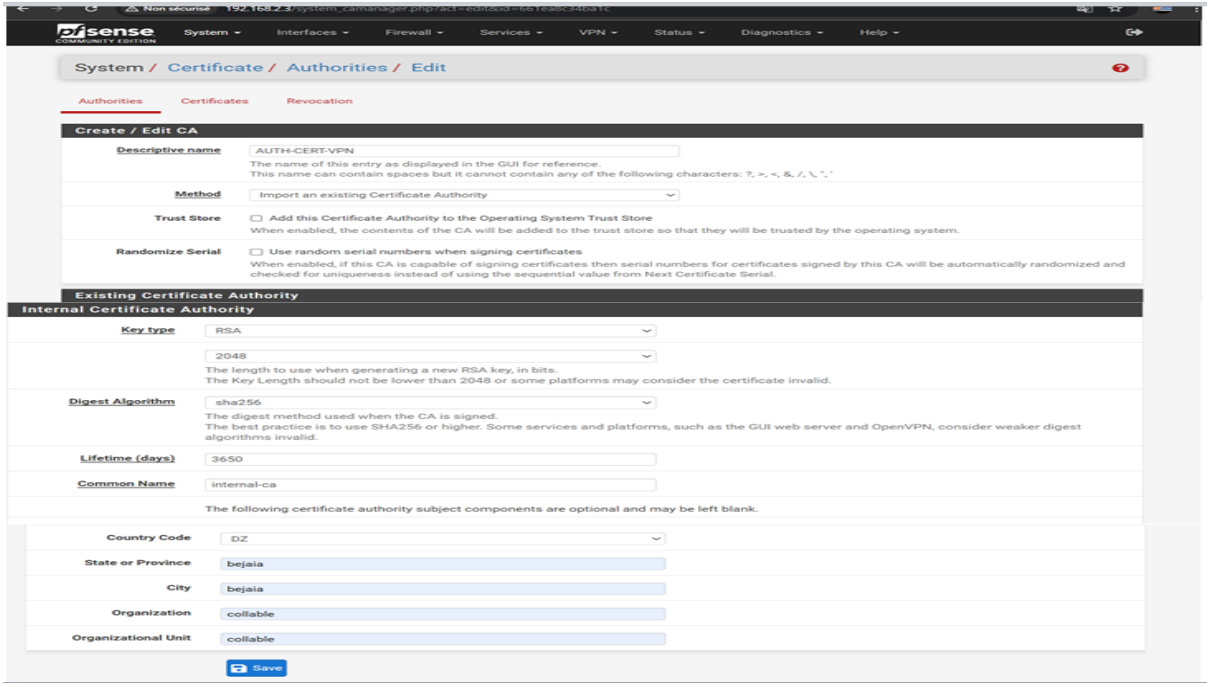


FIGURE 3.47 – Création de certificat d'autorité interne

### Etape2 : Création d'un certificat serveur

- Pour créer un certificat serveur, nous allons sur : Système => Certificate Manager => Certificates, puis remplissons les champs indiqués sur la figure 3.48 en sélectionnant le type "Server Certificate"

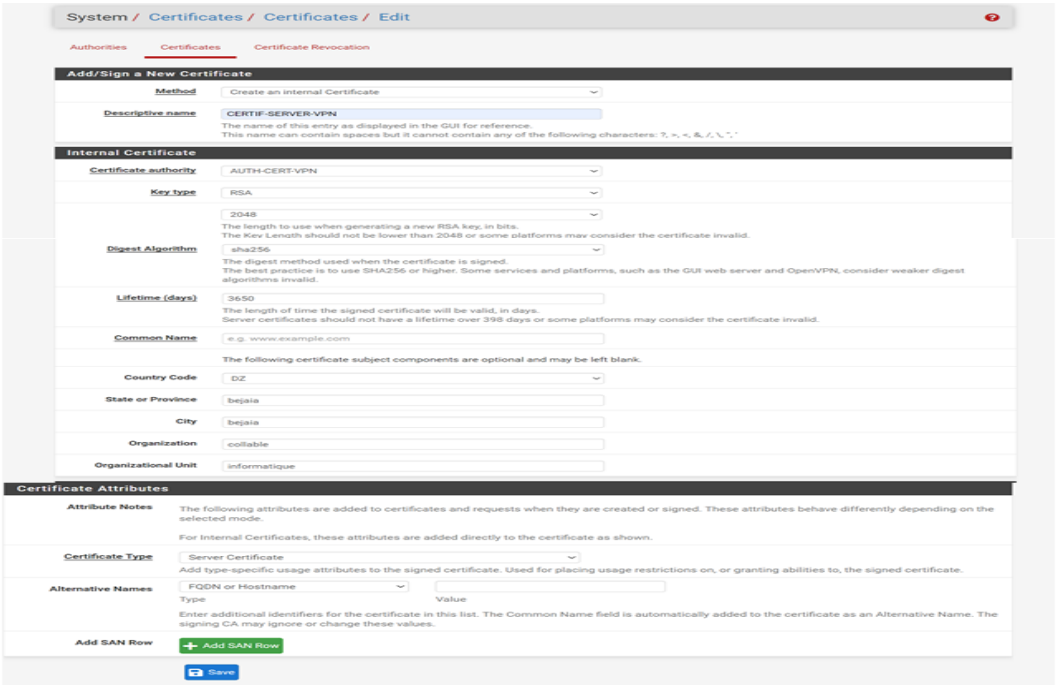


FIGURE 3.48 – Création d'un certificat serveur

### Etape3 : Création d'un certificat openVPN

- Pour créer un certificat OpenVPN, nous allons sur : VPN => OpenVPN => puis remplissons les champs comme indiqués sur les figures 3.49 et 3.50

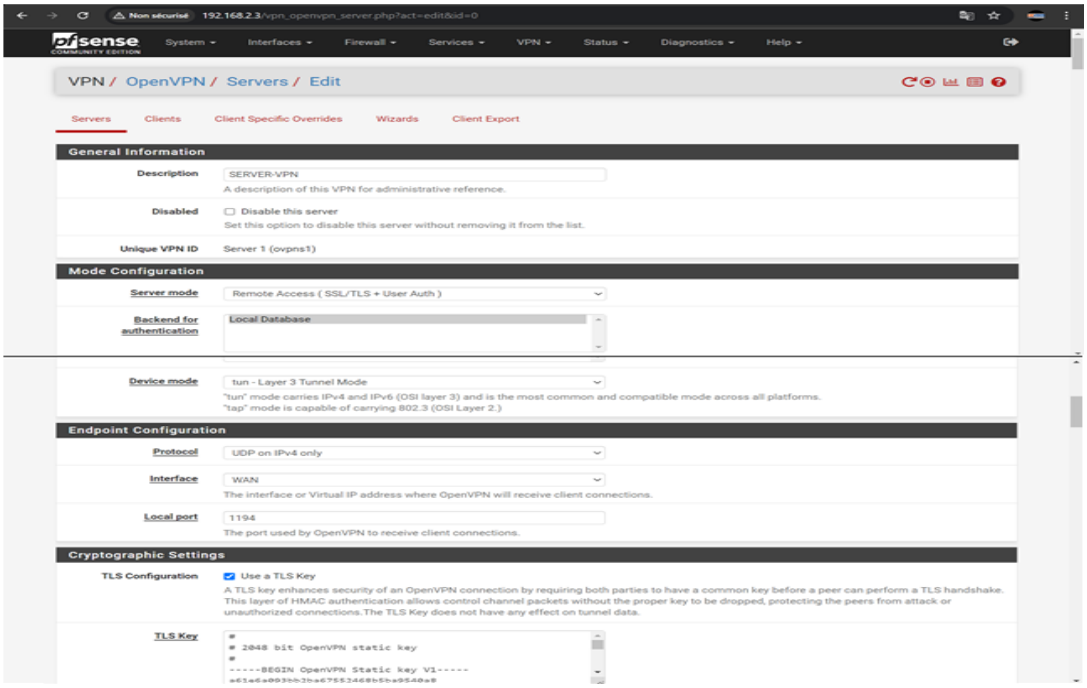


FIGURE 3.49 – Création du certificat OpenVPN

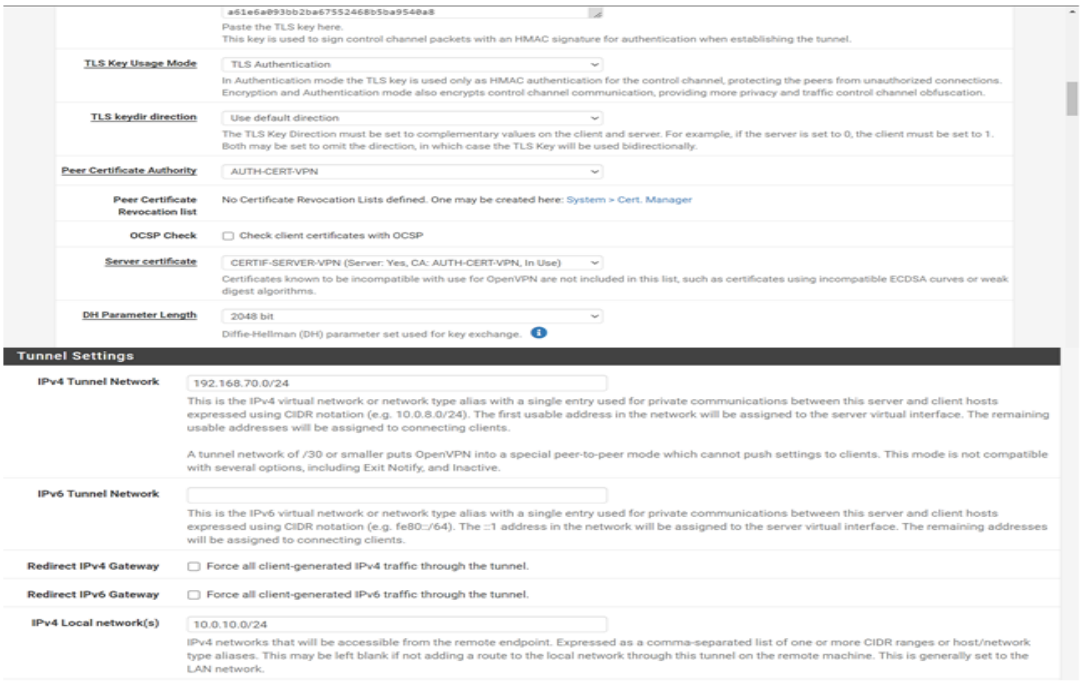


FIGURE 3.50 – Création du certificat OpenVPN

### Etape4 : Création d'utilisateurs VPN

- Pour créer un utilisateur autorisé à se connecter au VPN, nous allons sur : System => User Manager => Add User, puis remplissons les champs comme indiqués sur les figures 3.51

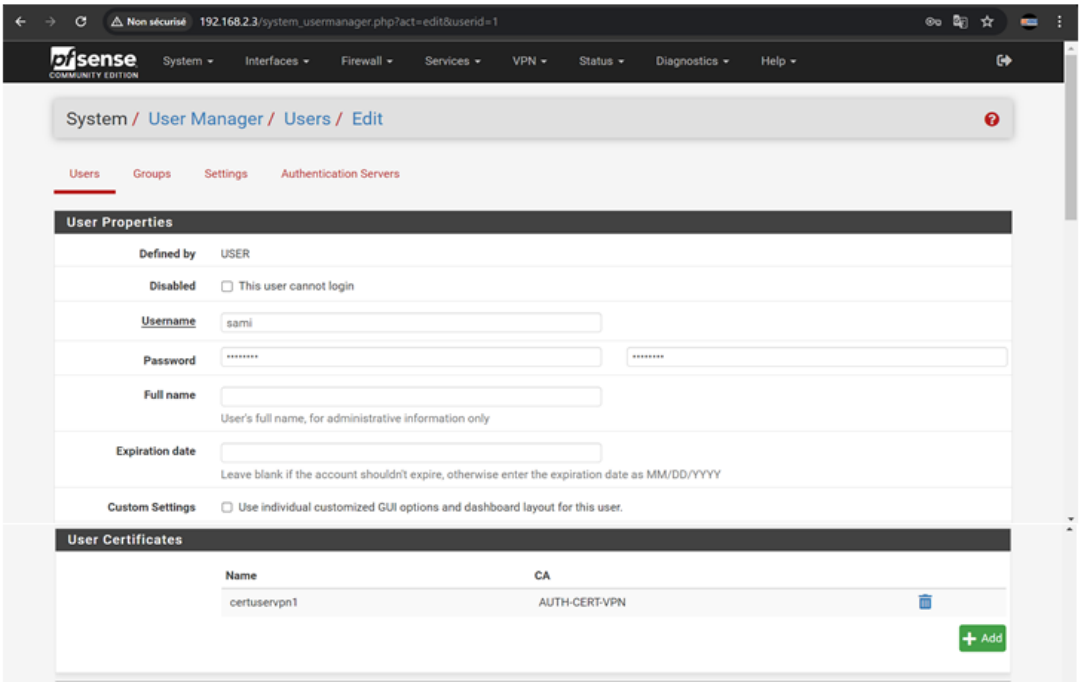


FIGURE 3.51 – Création d'utilisateur VPN

### Etape5 : Exporter le fichier de configuration pour l'utilisateur

- Pour installer le package Open VPN-client-export utilisé pour exporter les certificats, nous allons sur : System=> Package manager=> Available packages.

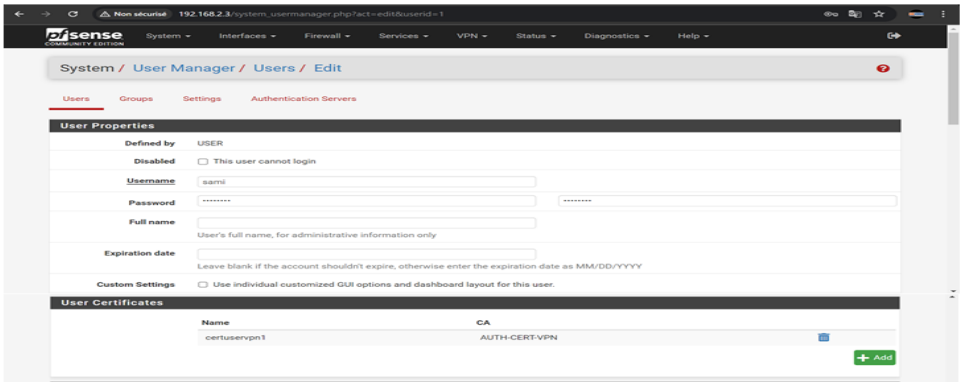

FIGURE 3.52 – Création d'utilisateur VPN

# Configuration de FreePBX

## Création des extensions SIP

Dans le menu principal à gauche, sélectionnons "Applications", puis "Extensions". Ensuite, cliquons sur le bouton "Add Extension". Dans le menu déroulant qui apparaît, choisissons "Ajouter un nouveau poste SIP".

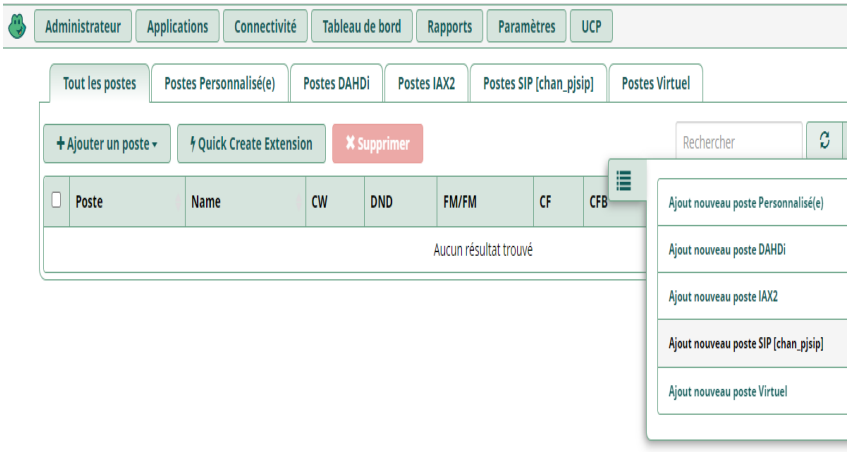


FIGURE 3.53 – Création d'extension

Maintenant, nous devons configurer l'extension. Dans le champ "User Extension", entrons un numéro unique pour l'extension. Dans "Display Name", entrons le nom de l'utilisateur associé à cette extension. Dans "Secret", entrons un mot de passe sécurisé pour cette extension. Ce mot de passe sera utilisé par le téléphone SIP pour s'authentifier auprès du serveur FreePBX.

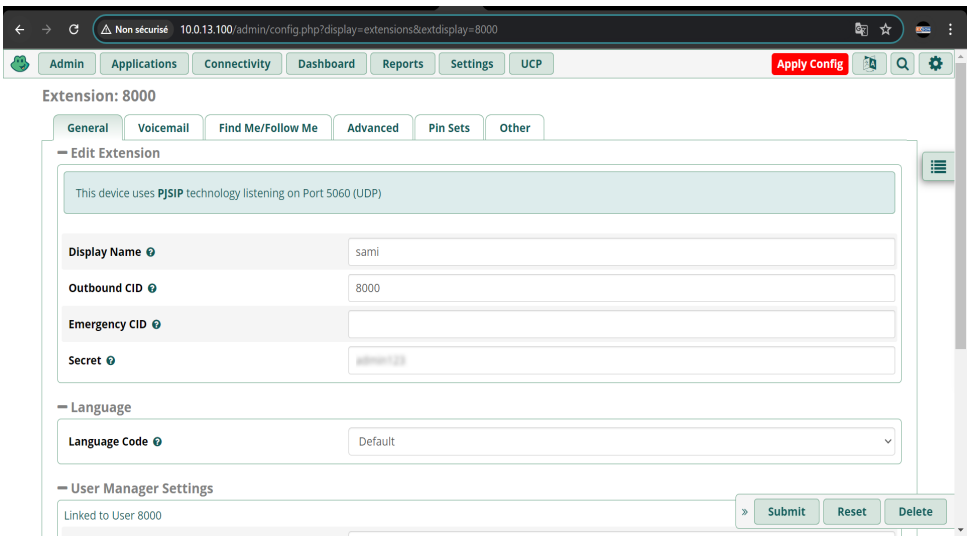


FIGURE 3.54 – configuration de l'extension

Après avoir rempli ces informations, cliquons sur "Soumettre" en bas de la page pour enregistrer l'extension. Une fois cette étape terminée, cliquons sur "Appliquer la configuration" en haut de l'interface pour appliquer les modifications.

## Création des comptes SIP sur les softphones

La prochaine étape consiste à configurer notre téléphone SIP ou softphone. Prenons notre appareil et accédons aux paramètres de compte ou de connexion. Entrons les informations nécessaires : pour le "Serveur", saisissons l'adresse IP de notre serveur FreePBX ; pour le "Nom d'utilisateur", entrons le numéro de l'extension que nous avons créée, et pour le "Mot de passe", utilisons le mot de passe que nous avons défini dans le champ "Secret".

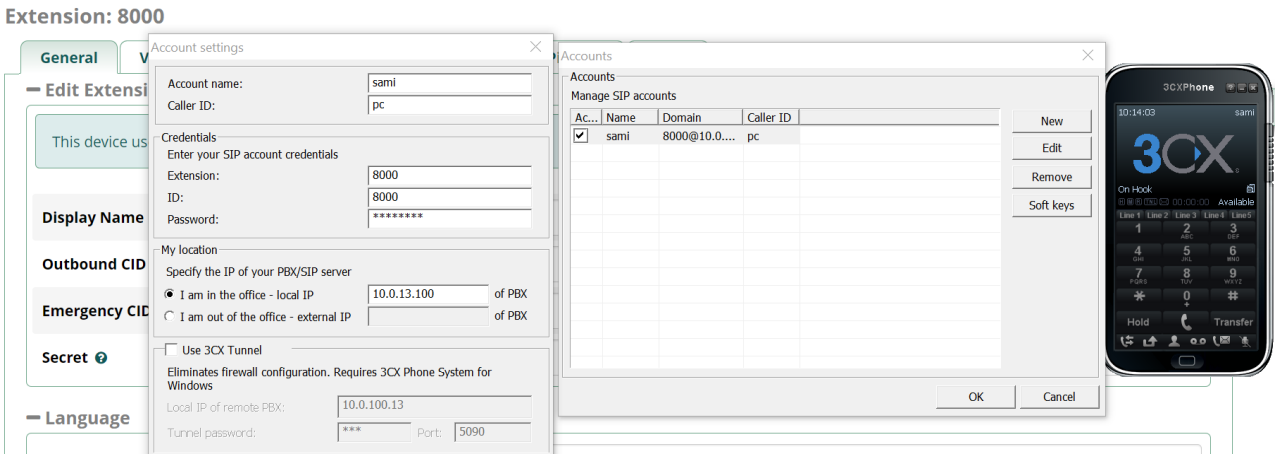


FIGURE 3.55 – configuration téléphone SIP

## Interconnexion des deux serveurs VoIP

## Configuration des liens trunks

Dans le menu principal à gauche, sélectionnons "Connectivity", puis cliquons sur "Trunks". Ensuite, cliquons sur le bouton "Add Trunk" et choisissons "Add IAX2 Trunk". Un trunk IAX2 est une ligne qui permet de transporter les communications entre les deux sites. Pour configurer un trunk, dans le menu principal à gauche, sélectionnons "Connectivity", puis cliquons sur "Trunks". Ensuite, cliquons sur le bouton "Add Trunk" et choisissons "Add IAX2 Trunk".

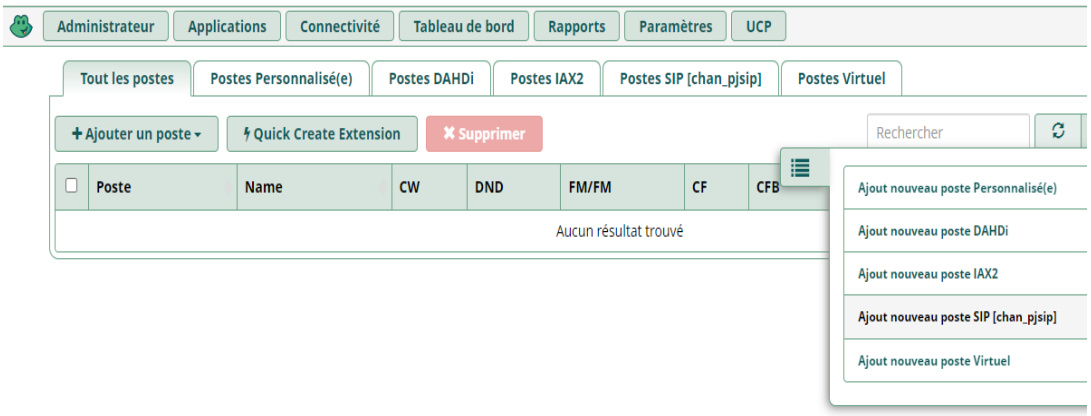


FIGURE 3.56 – Création du trunk IAX

Remplissons les champs nécessaires dans les sections "General"et "iax paramétre ".

- Section "General"

Trunk Name :Nous entrons un nom pour ce trunk

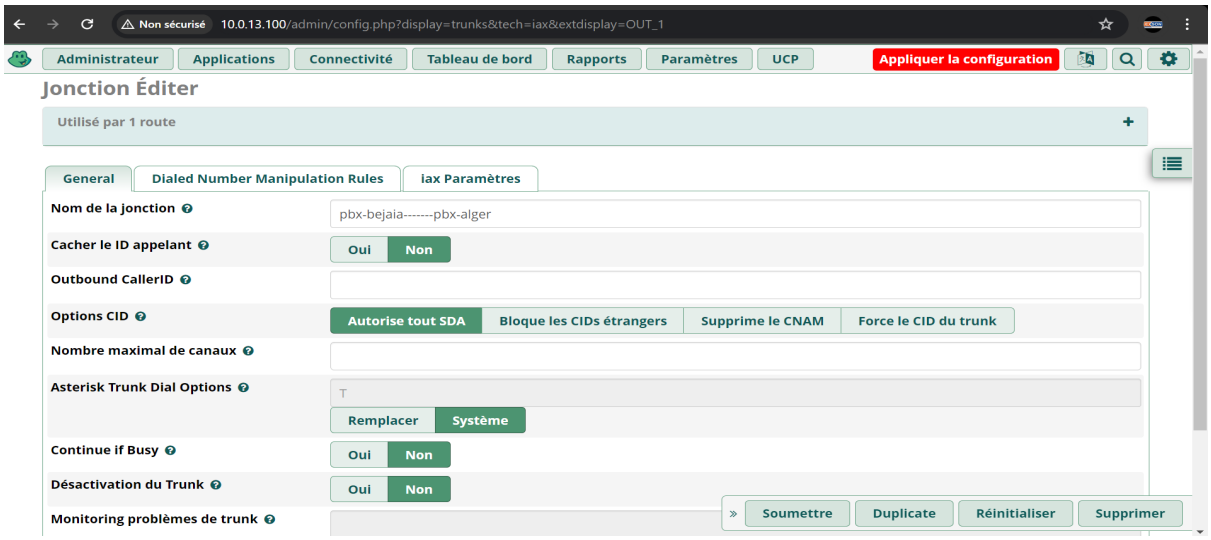


FIGURE 3.57 – Configuration du trunk vers pbx alger

- Dans la section IAX paramétre nous ajoutons les informations nécessaire pour "Outgoing Settings"et "Incoming Settings"

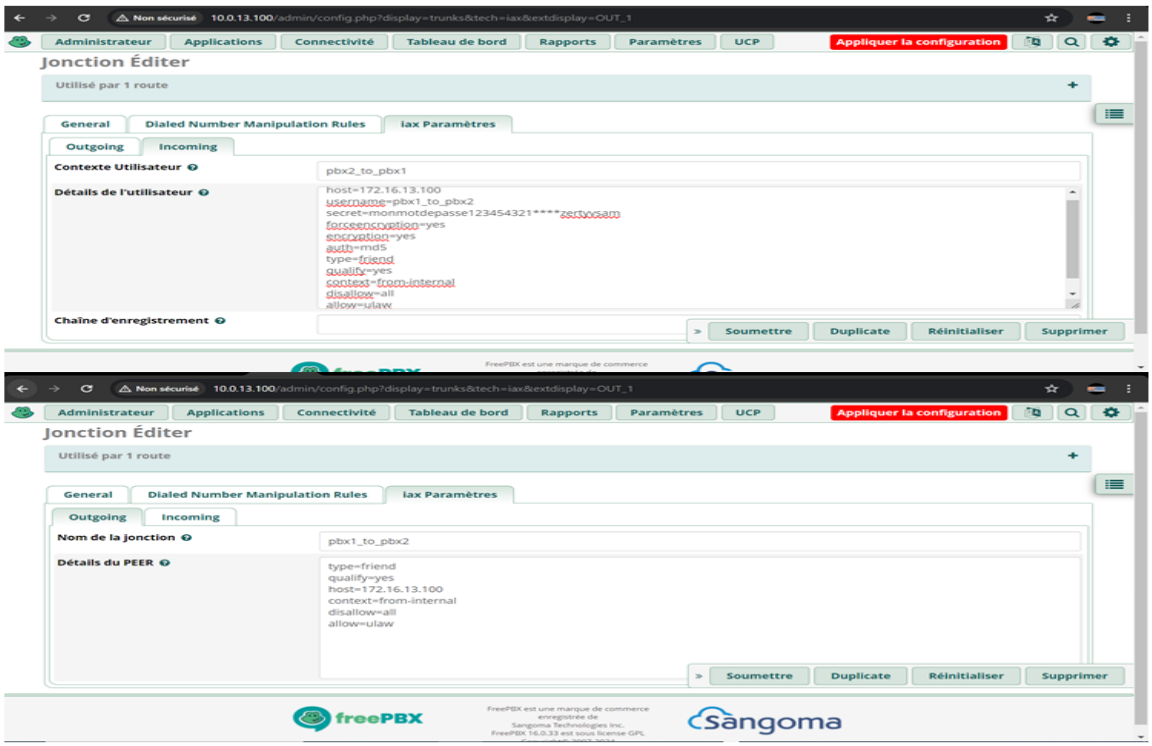


FIGURE 3.58 – trunk IAX

Après avoir configuré toutes les sections nécessaires, cliquons sur "Soumettre" en bas de la page pour enregistrer le trunk IAX. Ensuite, cliquons sur "Appliquer la configuration" en haut de l'interface pour appliquer les modifications.

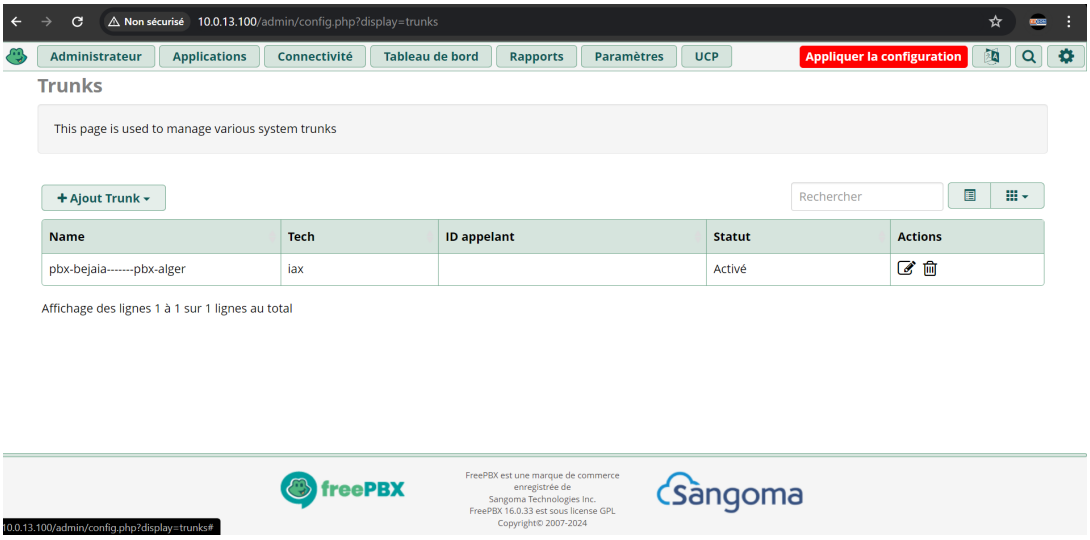


FIGURE 3.59 – enregistrement du trunk IAX

## Routage des appels entre les deux serveurs

Cette étape permet de créer une route de communication entre les deux sites. allons dans le menu principal à gauche, sélectionnons "Connectivity", puis cliquons sur "Outbound Routes". Cliquons ensuite sur "Add Outbound Route". Remplissons les champs nécessaires dans les sections "Route Settings" et "Dial Patterns".

- Dans la section "Route Settings" : Nous allons entrer un nom pour cette route et Sélectionnons le trunk IAX que vous avez configuré précédemment

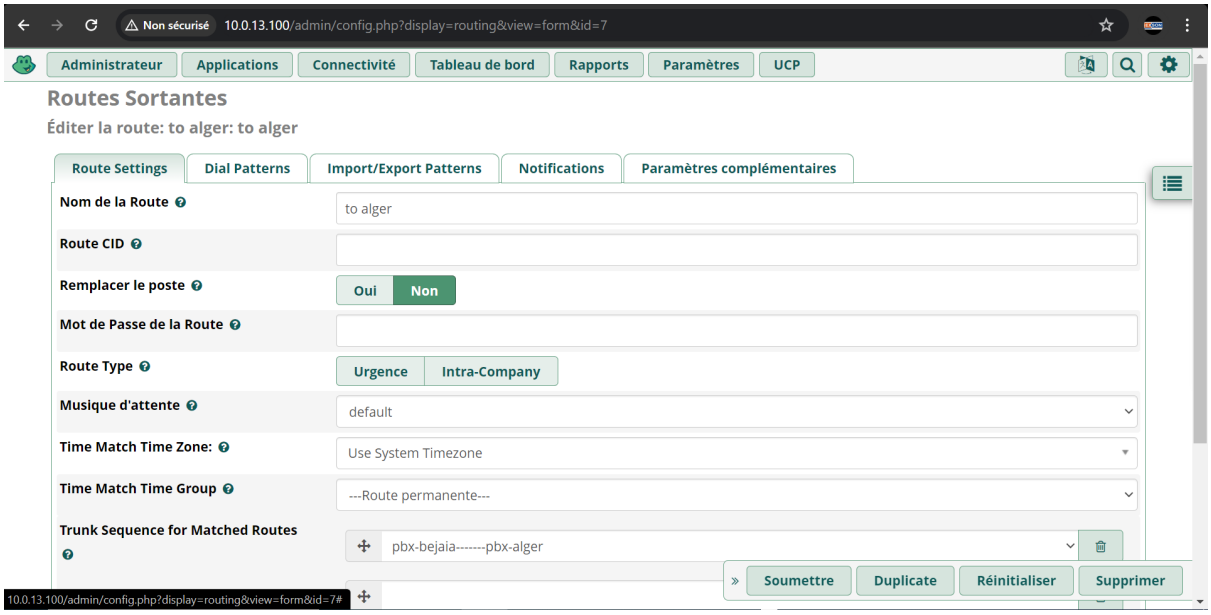


FIGURE 3.60 – Création de route vers alger

- Section "Dial Patterns" : Les dial patterns déterminent quels numéros seront dirigés via cette route.


FIGURE 3.61 – Configuration de la route vers alger

- Après avoir configuré tous les champs nécessaires, cliquons sur "Soumettre" pour enregistrer la route sortante. Ensuite, cliquons sur "Appliquer la configuration" pour appliquer les modifications.

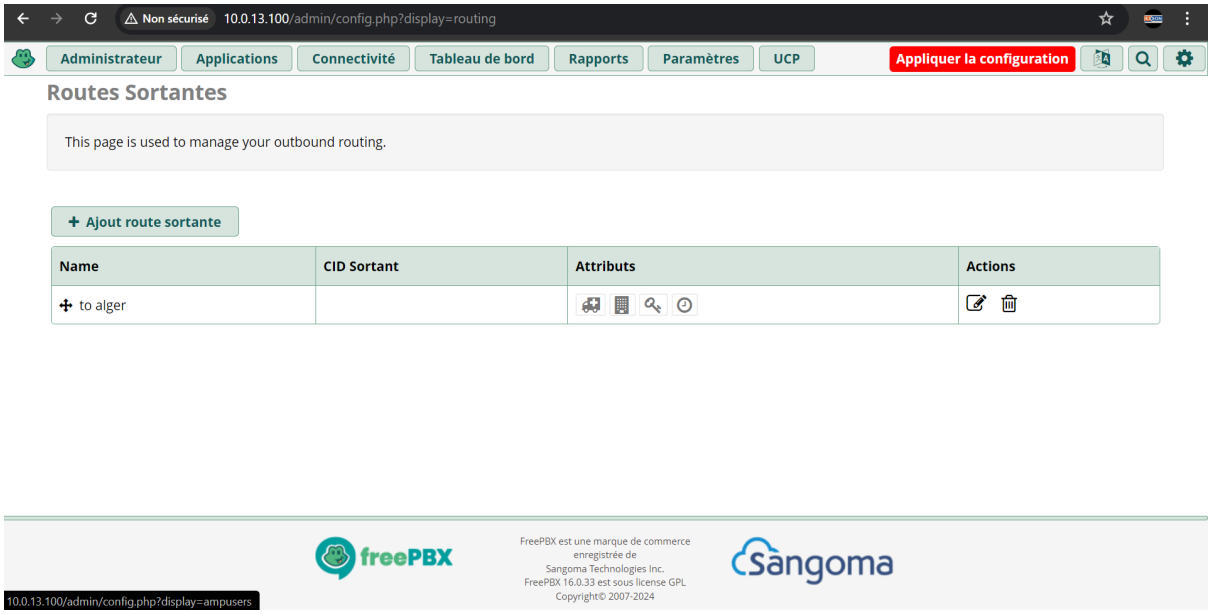


FIGURE 3.62 – enregistrement de la route vers alger

# Configuration du service appels vidéo

## Configurer les extensions pour les appels vidéo

Les extensions doivent être configurées pour permettre les appels vidéo.

- Allons dans Applications > Extensions.
- Éditons l'extension pour laquelle nous souhaitons activer les appels vidéo.
- Nous devons nous assurer que l'option "Allow" pour les codecs vidéo (comme H.264 ou VP8) est activée dans la section "Advanced" ou "Codec" de l'extension.
- Cliquons sur "Submit", puis sur "Apply Config".

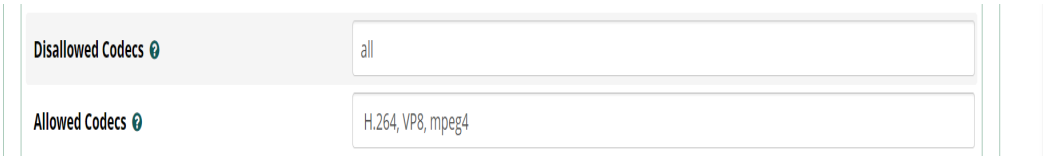


FIGURE 3.63 – Configuration des extensions pour les appels vidéo

## Configuratin des codecs dans les paramètres SIP

- Nous devons nous assurer que les codecs vidéo sont activés dans les paramètres SIP globaux.

dans Settings > Asterisk SIP Settings.

Dans les sections General SIP Settings et Chan SIP Settings, activons les codecs vidéo (comme H.264, VP8).

Cliquons sur Submit puis sur Apply Config.

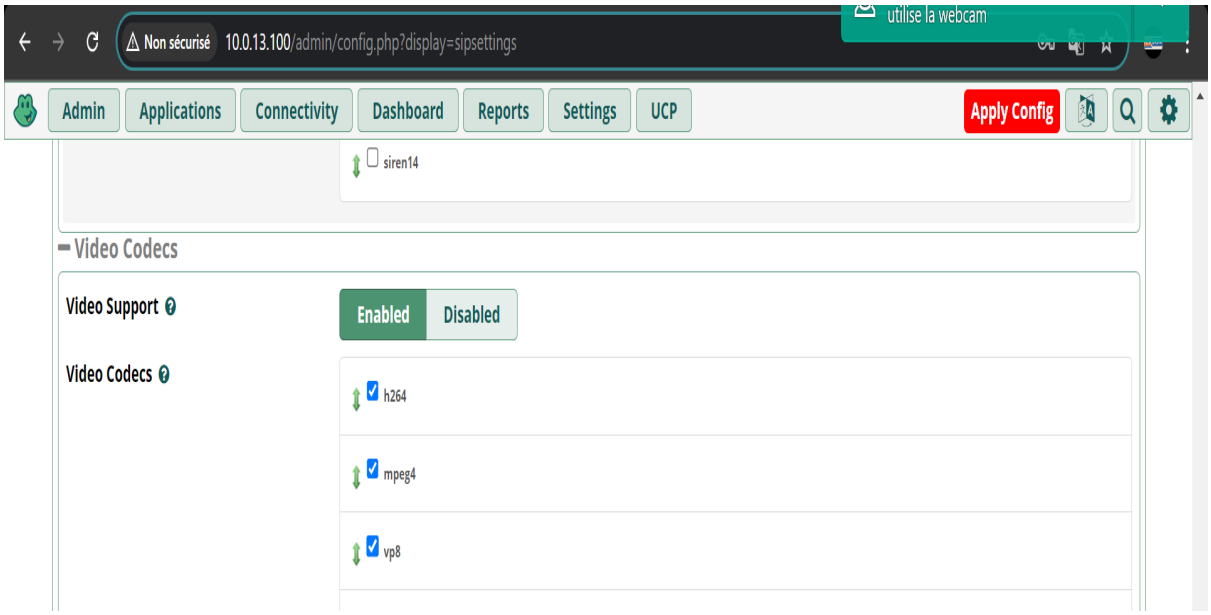


FIGURE 3.64 – Configuration des codecs dans les paramètres SIP

# Méthode de configuration supplémentaire de d'autres services

## File d'attente (Queues)

Les files d'attente permettent de gérer les appels entrants en les plaçant en attente jusqu'à ce qu'un agent soit disponible.

- Allons dans Applications > Queues. Cliquons sur Add Queue.
- Nous allons donner un numéro et un nom à la file d'attente. Configurons les options telles que la stratégie de répartition des appels, les annonces, et les options de temporisation.
- Cliquons sur Submit puis sur Apply Config.

## Messages vocaux (Voicemail)

Configurons les boîtes de messagerie vocale pour les utilisateurs.

- Allons dans Applications > Extensions.
- Éditons une extension et configurez les options de messagerie vocale, telles que les notifications par email et les paramètres de temporisation.
- Cliquons sur Submit puis sur Apply Config.

## Enregistrement des appels (Call Recording)

Configurons l'enregistrement automatique des appels.

- Nous allons dans Admin > Call Recording.
- Définissons les politiques d'enregistrement, y compris les extensions ou les groupes à enregistrer, et les paramètres de stockage.
- Cliquons sur Submit puis sur Apply Config.

## Configuration des IVR (Interactive Voice Response)

Les IVR permettent de créer des menus interactifs pour guider les appelants.

- Allons dans Applications > IVR.
- Cliquons sur Add IVR.
- Donnons un nom à l'IVR.
- Ajoutons des options de menu et définissez les destinations pour chaque option.
- Cliquons sur Submit puis sur Apply Config.

# testes

## Vérification du tunel IPSec

- Pour vérifier si le tunnel est établi, nous allons sur : Status=> IPsec.
- **O**n remaque la connexion VPN est établie entre les deux sites.

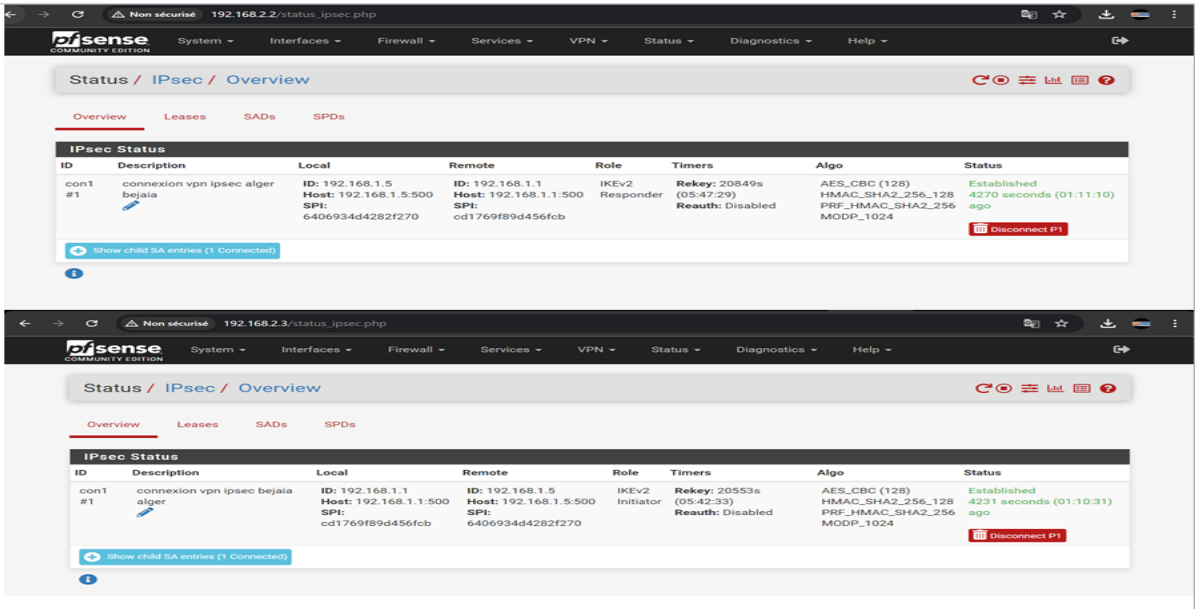


FIGURE 3.65 – Vérification du tunel IPSec

## Test d'appel vocale entre les deux sites

- La figure suivante montre que l'appel entre deux comptes SIP, un de Bejaia et l'autre d'Alger, est établi avec succès, ce qui signifie que les deux serveurs de VoIP sont bien interconnectés


FIGURE 3.66 – Test d'appel entre les deux sites

## Test d'appel vidéo entre les deux sites


FIGURE 3.67 – Test d'appel vidéo entre les deux sites

# Annexe 2

## Installation de VMware Workstation 17

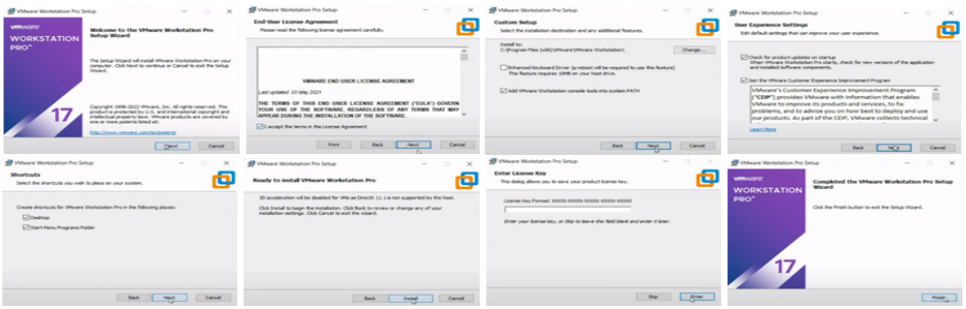

FIGURE 3.68 – Installation de VMware Workstation 17

## Installation de GNS3

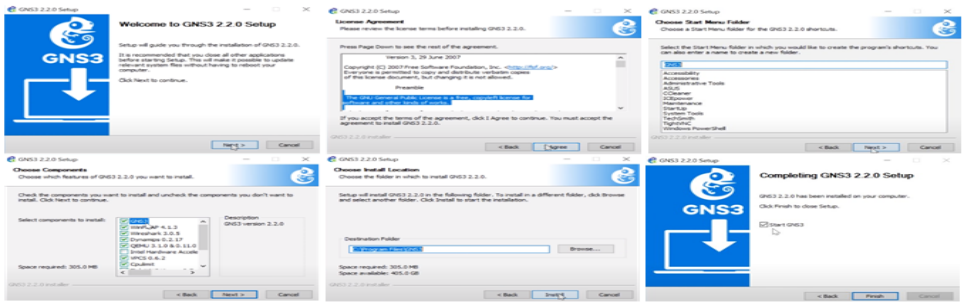


FIGURE 3.69 – Installation de GNS3

## Installation des softphones

## 3CX sofphone

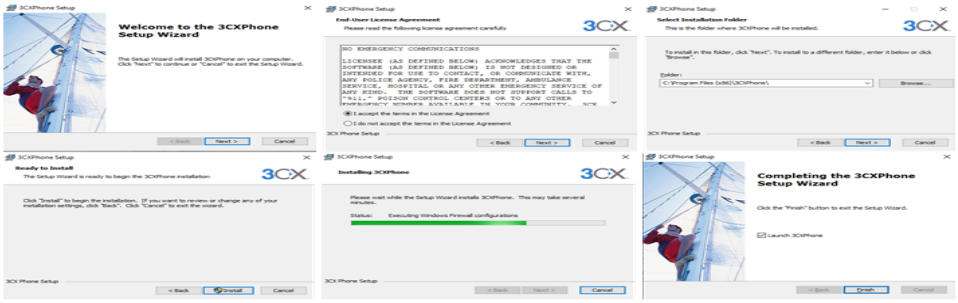


FIGURE 3.70 – Instalation de 3CX sofphone

## X-Lite

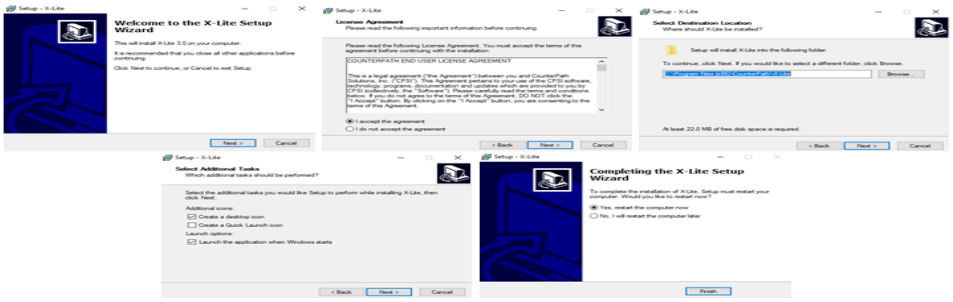


FIGURE 3.71 – Instalation de X-Lite

# Résumé

La Voix sur IP (VoIP) est une technologie en plein essor dans tous les secteurs, offrant aux entreprises une intégration efficace, une fiabilité accrue, une évolutivité optimale et des coûts réduits. Cependant, du fait de sa nouveauté, l'implémentation de la VoIP expose souvent les réseaux d'entreprise à diverses attaques. Ainsi, sécuriser le réseau VoIP devient non seulement nécessaire mais essentiel. Dans ce cadre, nous avons déployé une solution VoIP au sein de l'entreprise Campus NTS en interconnectant deux serveurs PBX et en établissant trois VLANs (data, gestion et voix) entre ses sites distants à Bejaia et Alger. Cette configuration vise à améliorer les communications entre les collaborateurs en utilisant les protocoles de signalisation SIP et IAX. Pour garantir la sécurité, nous avons sécurisé cette infrastructure par un canal VPN IPsec, assurant le chiffrement des données vocales échangées via le protocole ESP, assurant ainsi la confidentialité et l'intégrité des informations transmises.


Mots clés : VoIP, Sécurité, PBX, VLAN, SIP, IAX, VPN IPSec, ESP.



# Abstract

Voice over IP (VoIP) is a technology that is gradually becoming essential across all sectors. It offers businesses effective integration, enhanced reliability, scalability, and cost-effectiveness. However, being a relatively new technology, implementing VoIP can expose a company's network to various attacks. Therefore, securing the VoIP network is not just necessary but imperative. In this context, we implemented a VoIP solution within Campus NTS by interconnecting two PBX servers and establishing three VLANs (data, management, and voice) across its remote sites in Bejaia and Alger. This setup aims to improve communication among company personnel using SIP and IAX signaling protocols. To ensure security, we secured this infrastructure with an IPsec VPN tunnel, encrypting voice data exchanged using the ESP protocol, thereby ensuring confidentiality and integrity of the transmitted information.


Key words : VoIP, Security, PBX, VLAN, SIP, IAX, VPN IPSec, ESP.