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

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

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

Mise en place d'une solution VoIP sécurisée cas d'un centre d'appel Candle Call

Préparé par :

- **Mlle** Hamoumou Tin-Hinane & **Mlle** Ghanem Melissa

Dirigé par :

Mme. Gherbi M. **Encadrante**

M. Mili N. **Co-Encadrant**

Examiné par :

M. Kasmi **Président**

Mme Ghennam **Examinatrice**

Année universitaire : **2023/2024**

Remerciement

Avant toute chose, nous souhaitons exprimer notre gratitude infinie ***à Dieu Tout Puissant*** *pour nous avoir donné la force, le courage et la persévérance nécessaires pour mener à bien ce travail. Sans Sa grâce, ce mémoire n'aurait jamais vu le jour.*

Nos plus sincères remerciements vont ***à notre encadrante, Mme GHERBI Meriem,*** *pour son précieux accompagnement, ses conseils avisés et son soutien constant tout au long de ce projet.*

Nous exprimons également notre reconnaissance envers ***notre co-encadreur de l'entreprise, Mr. MILI N,*** *pour sa collaboration tout au long de notre stage.*

Nous adressons également nos sincères remerciements ***aux membres du jury « M. Kasmi*** *et* ***Mme Ghennam »*** *pour l'intérêt qu'ils portent à notre travail et pour leurs futures remarques constructives qui enrichiront notre recherche. Nous apprécions leur engagement et le temps qu'ils consacreront à l'évaluation de ce projet.*

Merci ***à nos professeurs et collègues pour leur soutien académique,*** *ainsi qu'à* ***nos camarades*** *de promotion pour leur camaraderie et encouragement.*

Enfin, nous tenons à exprimer toute notre gratitude ***à nos familles et nos amis,*** *pour leur patience, leur compréhension et leurs encouragements inconditionnels. Leur amour et leur soutien moral ont été une source inestimable de motivation et de réconfort et* ***à toutes les personnes qui ont contribué à l'aboutissement de ce mémoire.***

Dédicace

Au nom d'Allah, le Tout-Puissant, qui m'a guidé et béni tout au long de ce chemin,

Je dédie ce modeste travail :

À mes chers Maman et Papa, *le soleil et la lune de ma vie, qui m'ont porté, soutenu et encouragé avec un amour inconditionnel. Vous êtes mon phare dans la nuit, mon refuge dans la tempête. Votre dévouement, vos sacrifices et vos Dou' as ont été les piliers de ma réussite tout au long de mon parcours académique et ont rendu possible l'accomplissement de ce mémoire. Je vous le dédie avec toute ma gratitude et mon affection.*

À ma grande sœur Siham, *ma confidente et mon âme sœur. Ton affection, ta sagesse et ton soutien indéfectible ont été ma force dans les moments les plus difficiles.* ***À ma petite princesse Inès,*** *ta présence a été ma consolation, et à ma petite compagnonne Mirya. Je vous dédie ce mémoire avec toute mon admiration.*

À mes frères, *mes protecteurs. Votre soutien, votre présence rassurante, votre solidarité fraternelle et votre encouragement ont été précieux. Je vous dédie ce mémoire avec toute mon affection.*

À toute ma famille, *spécifiquement* ***à ma merveilleuse tante Tata Hayat****, qui m'a entouré de son amour et de sa bienveillance sans faille,* ***à ma chère Tata Kouka, à ma douce Hanane*** *et* ***à ma chérie Yasmine*** *pour votre amour et votre soutien constants et sincères,* ***à Khali Nacer****,* ***à Anis*** *pour ta présence inébranlable dans les moments difficiles, ton soutien a été inestimable, et* ***à Babi*** *pour tes encouragements constants, et* ***à tous*** *sans exception. Vous avez été ma force et mon inspiration. Je vous dédie ce mémoire avec tout mon amour.*

À mes adorables nièces et neveux, *vous êtes mes rayons de soleil qui illuminent ma vie de votre joie et de votre innocence. Vous êtes ma source intarissable d'inspiration et de motivation.*

À ma binôme et meilleure amie, *Chaque jour passé ensemble est une nouvelle aventure pleine de défis partagés et de souvenirs inoubliables.*

Ta présence rend tout plus joyeux. Ensemble, nous sommes plus fortes, plus sages, et infiniment plus heureuses.

À mes autres meilleures amies, *ma deuxième famille. Votre amitié sincère, vos rires et votre soutien ont rendu ce voyage plus léger et plus meilleur.*

À la section télécom, mes camarades, mes nouvelles amies et copines, *pour cette aventure partagée et cette ambiance d'entraide.*

À tous nos professeurs, *qui nous ont guidées avec sagesse et patience. Votre enseignement a nourri notre esprit et façonné notre réflexion. Nous vous dédions ce mémoire avec toute notre reconnaissance et notre respect.*

À tous les Palestiniens, *qui souffrent et résistent chaque jour. Votre courage, votre résilience et votre esprit indomptable sont une source d'inspiration pour le monde entier. Free Palestine. Ce mémoire est dédié en hommage à ceux qui ont perdu leur vie dans cette lutte pour la liberté et la justice. Puissent vos sacrifices ne jamais être oubliés et puisse votre souffrance bientôt cesser. Que la paix et la justice règnent sur la Terre Sainte.*

Que Dieu vous bénisse tous, mes chers bien-aimés, pour avoir fait de ce mémoire une œuvre imprégnée de vos précieuses contributions.

Hamoumou Tin-Hinane.

Dédicace

Quelles que soient mes paroles et mes actions, elles ne sauraient exprimer pleinement ma gratitude envers vous. Ce travail est dédié comme une humble reconnaissance de vos efforts et une expression sincère de mon profond amour.

À ma chère maman,

Ton amour inconditionnel, ta patience infinie et tes encouragements constants ont été les piliers de ma réussite tout au long de ce parcours académique. Ce mémoire est le fruit de ton soutien inestimable et de ton dévouement sans limite. Merci pour tout ce que tu as fait et continue de faire pour moi.

À mon cher papa,

Pour ta persévérance, ton soutien et tes conseils précieux. Tu es un exemple de force et de détermination. Merci d'avoir toujours cru en moi.

À mes frères,

Nabil, dont l'aide précieuse et le soutien constant ont été essentiels à chaque étape de ce mémoire. Adel et Nadir, pour votre soutien inconditionnel.

À ma binôme et meilleure amie,

Hinane, complice de cette aventure académique et amie précieuse, pour notre collaboration enrichissante et notre amitié sincère qui ont fait de ce mémoire une expérience inoubliable.

À mes meilleure amies,

Mely et Lydia, Pour votre amitié précieuse qui a enrichi ma vie. Ce mémoire est dédié à notre amitié sincère.

GHANEM Mélissa

Table des matières

Chapitre 2 : Compréhension des Risques et Solutions de Sécurité en Voix sur IP

Chapitre 3 : Étude de l'existant et choix de la solution VoIP

Chapitre 4 : Sécurisation de la solution mise en place

Liste des figures

Liste des tableaux :

Liste des abréviations

	A
ACL	Access Control List
ACE	Access Control Entries
ACD	Automatic Call Distributor
AH	Authentication Header
	C
CRM	Customer Relationship Management
CPU	Central Processing Unit
	E
ESP	Encapsulating Security Payload
	I
IDS/IPS	Intrusion Detection/Prevention Systems
IM	Instant Message
IP	Internet Protocol
IPBX	Internet Protocol Private Branch Exchange
IPsec	Internet Protocol Security
	L
LAN	Local Area Network
	M
MIKEY	Multimedia Internet Keying
MKI	Master Key Identifier
MMUSIC	Multiparty Multimedia Session Control
	O
OSI	Open Systems Interconnection
	P
PBX	Private Branch Exchange
PABX	Private Automatic Branch Exchange
	R
RAM	Random Access Memory
RFC	Request for Comments
RTP	Real-time Transport Protocol
RTCP	Real-time Control Protocol
RTC	Real-Time Communication
	S
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SRTP	Secure Real-time Transport Protocol
	T
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TFTP	Trivial File Transfer Protocol

U

UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URI	Uniform Resource Identifier

V

VPN	Virtual Private Network
VOIP	Voice Over Internet Protocol
VOIP VPN	Voice Over IP Virtual Private Network

Introduction générale

Dans un monde où la communication est au cœur de toutes les activités, les entreprises sont constamment à la recherche des solutions innovantes pour optimiser leurs échanges tout en garantissant la sécurité de leurs données.

La VOIP, la technique de la voix sur IP, est devenue une option incontournable pour remplacer les systèmes téléphoniques traditionnels, offrant ainsi plus de flexibilité et de rentabilité. Néanmoins, avec l'avènement de la VOIP, les enjeux liés à la sécurité des communications deviennent de plus en plus importants. Dans ce contexte, ce mémoire de fin d'études vise à créer une solution VOIP sécurisée au sein du centre d'appel Candle Call.

La VOIP, ou Voice over Internet Protocol, permet de transmettre la voix sous forme de données numériques via les réseaux IP, offrant ainsi une alternative économique et flexible aux systèmes téléphoniques classiques.

Cependant, cette technologie présente un grand nombre de failles et expose les communications à diverses menaces, comme l'écoute illégale, l'usurpation d'identité ou encore les attaques par déni de service. Pour faire face à ces risques, il est crucial que les entreprises mettent en place des solutions VOIP sécurisées, garantissant la confidentialité, l'intégrité et la disponibilité des échanges.

Ce mémoire vise principalement à concevoir, implémenter et analyser une solution VOIP sécurisée qui répond aux besoins spécifiques du centre d'appel Candle Call. Pour parvenir à cet objectif, nous allons adopter une méthodologie en quatre étapes qui correspond aux quatre chapitres de ce document.

Ce mémoire est organisé en quatre chapitres :

Pour commencer, nous établirons les bases théoriques indispensables à la compréhension de la VOIP et de ses enjeux sécuritaires.

Le premier chapitre, intitulé **Généralités sur la voix sur IP**, présente les principes fondamentaux de cette technologie, son architecture et les protocoles associés.

Le deuxième chapitre, **Compréhension des Risques et Solutions de Sécurité en VoIP**, examine les menaces spécifiques auxquelles la VoIP est confrontée et propose des stratégies de sécurité pour les atténuer.

Le troisième chapitre, **Étude de l'existant et choix de la solution VoIP**, analyse un centre d'appel réel pour identifier ses besoins en communication et décrit le choix et l'implémentation d'une solution VoIP adaptée.

Enfin, le quatrième chapitre, **Sécurisation de la solution mise en place**, détaille les mesures de sécurité adoptées pour renforcer la solution VoIP, incluant la configuration de fail2ban, l'implémentation d'un pare-feu, le chiffrement TLS et l'utilisation du protocole SRTP.

À travers ce mémoire, nous démontrerons qu'il est possible de concilier les avantages de la VOIP avec les impératifs de sécurité, en proposant une solution adaptée aux besoins d'un centre d'appel tel que Candle Call. Cette étude se veut une contribution à la réflexion sur la sécurisation des communications dans un contexte professionnel, et une aide à la décision pour les entreprises souhaitant adopter la VOIP de manière sûre et efficace.

Chapitre 0 1

Généralité sur la voix sur IP

1. Introduction

Ce chapitre introductif vise à poser les bases de la compréhension de la VOIP. Nous commencerons par définir précisément cette technologie et expliquer son principe de fonctionnement fondamental. Ensuite, nous décrirons l'architecture réseau typique sur laquelle repose un système VoIP, en soulignant les différents composants clés impliqués. Nous aborderons ensuite les avantages et les inconvénients liés à l'utilisation de cette technologie. Enfin, nous examinerons en profondeur les protocoles clés utilisés pour la signalisation et le transport des communications VoIP.

2. Définition et concept de la voix sur IP

La Voix sur IP est une technologie qui permet d'acheminer, grâce au protocole IP, des paquets de données correspondant à des échantillons de voix numérisée. Cette technologie convertit les signaux vocaux en signaux digitaux qui voyagent par Internet. Par la suite, ces paquets doivent être acheminés dans le bon ordre et dans un délai raisonnable pour que la voix soit correctement reproduite. [1]

3. Principe de fonctionnement de la Voix sur IP

La transmission de la voix sur IP (VoIP) implique plusieurs étapes clés pour convertir et transmettre les signaux vocaux à travers un réseau IP. Voici les étapes essentielles du processus :

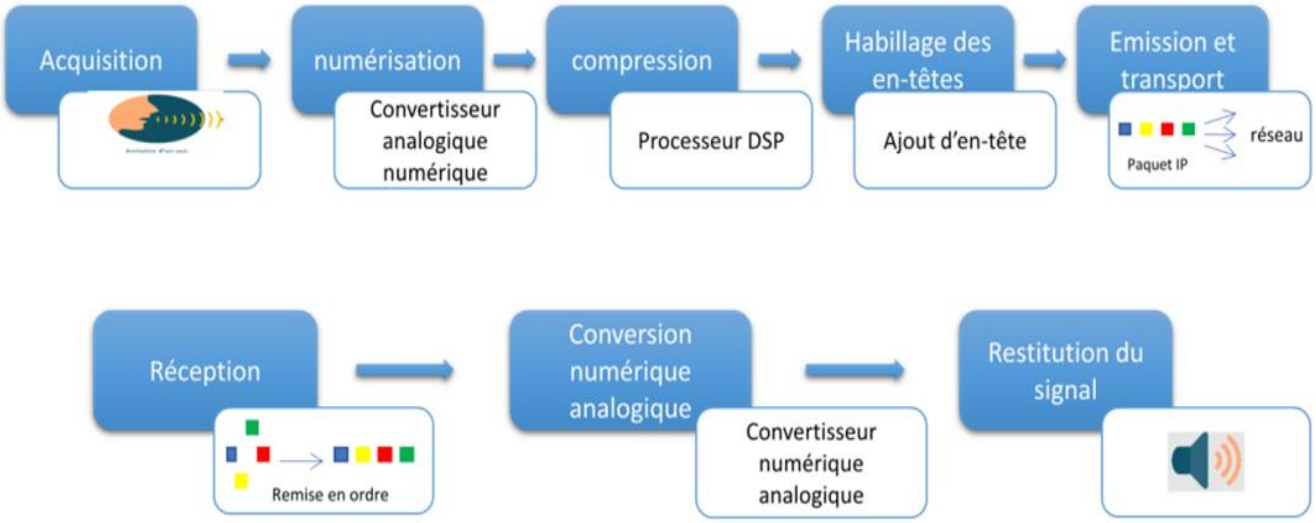


Figure 1.1 : Principe de transmission VoIP [2].

- **L'acquisition :**

La première étape de la VOIP consiste à acquérir le signal vocal analogique à l'aide d'un microphone. Pour être transmis via le réseau IP, ce signal doit être converti en format numérique.

- **La numérisation :**

Dans le cadre de la numérisation, on utilise deux processus principaux : l'échantillonnage et la quantification.

➢ **Echantillonnage :**

Le signal analogique est converti en un flux numérique lorsqu'on extrait des échantillons à une fréquence d'échantillonnage particulière.

➢ **Quantification :**

La quantification consiste à convertir chaque échantillon en une valeur numérique après l'échantillonnage. Pour ce faire, il est nécessaire de mesurer l'amplitude de chaque échantillon et de l'assigner à la valeur numérique la plus proche dans une échelle prédéfinie. Cette procédure repose sur la précision de la représentation numérique du signal vocal, en fonction du nombre

de bits utilisés. Pour illustrer, une quantification sur 8 bits autorise 256 niveaux de quantification différents.

- **La compression :**

La compression des données vocales numériques est une étape essentielle dans la VoIP, étant donné qu'elles peuvent occuper une large bande passante. Les techniques de compression permettent de réduire la taille des données tout en maintenant la qualité de la voix. Il existe plusieurs codecs de compression couramment utilisés dans la VOIP, tels que G.711. Afin de réduire la quantité de données à transmettre, ces codecs utilisent des techniques de compression, qu'elles soient avec ou sans perte.

- **L'habillage des entêtes :**

Une fois les données vocales compressées, elles sont encapsulées dans des paquets de données compatibles avec le réseau IP. Les paquets renferment des en-têtes qui intègrent des informations comme l'adresse IP source et de destination, et d'autres métadonnées inévitables pour router les paquets à travers le réseau. On utilise généralement RTP (Real-time Transport Protocol) et UDP (User Data gram Protocol) comme protocoles d'encapsulation pour la VOIP.

- **L'émission et transport :**

Lors de cette phase, les paquets de données VoIP sont envoyés sur le réseau IP. Les paquets parcourent différents nœuds du réseau, comme des routeurs, pour parvenir à leur destination. L'acheminement des paquets de manière efficace et flexible est assuré par le protocole IP.

- **La réception :**

À l'extrémité réceptrice, les paquets VoIP sont reçus et rassemblés en fonction de leur numéro de séquence. Les paquets peuvent arriver dans un ordre différent ou avec des délais variables en raison de la nature du réseau IP. Le protocole RTP, est utile pour gérer la synchronisation et l'ordre des paquets.

- **La conversion numérique/analogique :**

Une fois que les paquets de données VoIP ont été reçus et réassemblés, le signal vocal numérique doit être transformé en signal analogique pour être audible. Lors de cette étape, les

valeurs numériques sont transformées en signaux électriques analogiques, ce qui permet de les reproduire par un haut-parleur ou un casque.

- **La restitution :**

Enfin, l'utilisateur destinataire reçoit le signal analogique, ce qui lui permet d'entendre la voix de l'appelant. À ce stade, la transmission de la voix via la VOIP est terminée.

4. Architecture VOIP [3]

La voix sur IP (VOIP), en tant que technologie de communication émergente, ne dispose pas encore d'un standard unique établi. Chaque fabricant apporte en effet ses propres normes et fonctionnalités spécifiques à ses solutions VOIP. Le schéma suivant décrit de manière générale la topologie typique d'un réseau de téléphonie IP dit VOIP. Celle-ci comprend invariablement des terminaux, un serveur de communication et une passerelle permettant l'interconnexion avec d'autres réseaux. L'intelligence du réseau est par ailleurs déportée, soit au niveau des terminaux, soit au niveau des passerelles/contrôleurs d'admission d'appel (Gatekeeper).

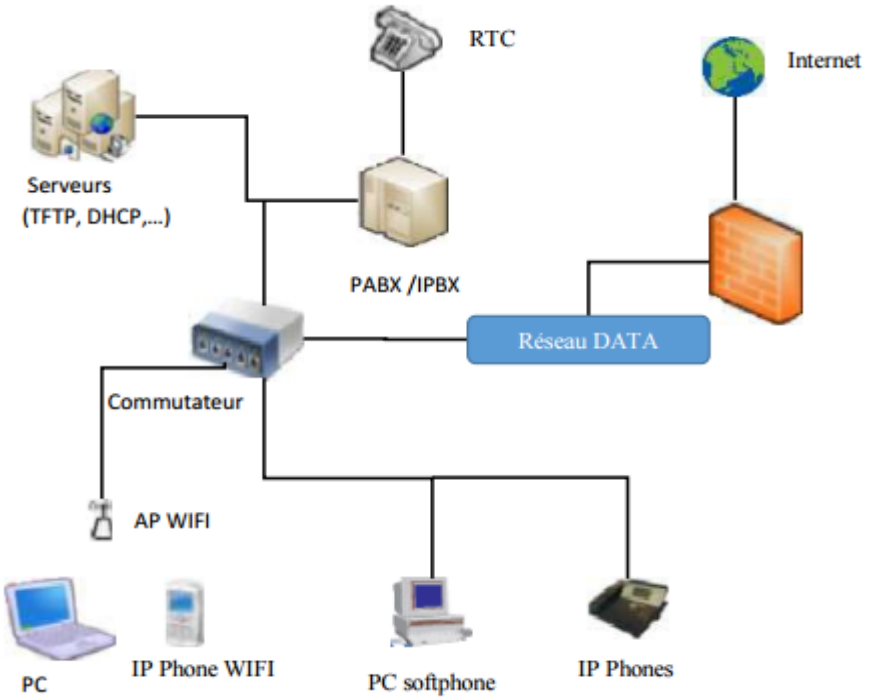


Figure 1.2 : Architecture VoIP [4].

On retrouve généralement les éléments constitutifs suivants :

- **Le routeur :** Il permet d'aiguiller les données et le routage des paquets entre deux réseaux, jouant un rôle clé dans l'acheminement des communications VOIP à travers différents réseaux.
- **Le PABX (autocommutateur téléphonique privé) :** C'est le commutateur du réseau téléphonique classique, assurant la liaison entre la passerelle ou le routeur et le réseau téléphonique commuté (RTC). une mise à jour du PABX traditionnel est nécessaire. Si tout le réseau devient IP, le PABX conçu pour la téléphonie commutée classique n'est plus adapté. Il doit être remplacé par un IPBX, qui est l'équivalent IP du PABX, spécifiquement conçu pour acheminer la voix et les communications unifiées sur un réseau IP/Ethernet.
- **Les Terminaux :** Parmi les terminaux VOIP, on distingue principalement deux catégories. La première consiste en des applications logicielles (softphones) installées sur les ordinateurs des utilisateurs, leur permettant d'émettre et de recevoir des appels via l'interface du logiciel. La seconde catégorie regroupe les terminaux matériels dédiés, communément appelés téléphones IP. Ceux-ci intègrent directement la technologie VOIP et se connectent au réseau IP pour transmettre la voix numérisée, sans passer par les réseaux téléphoniques traditionnels.
- **Gateway et Gatekeeper :** Les passerelles ou gateways en téléphonie IP sont des ordinateurs qui fournissent une interface où se fait la convergence entre les réseaux téléphoniques commutés (RTC) et les réseaux basés sur la commutation de paquets, assurent les fonctions de codage, décodage et la mise en paquet de la voix et disposent d'interface d'interconnexion analogique et numérique. C'est une partie essentielle de l'architecture du réseau de téléphonie IP. Le gatekeeper est l'élément qui fournit de l'intelligence à la passerelle. Le gatekeeper est le compagnon logiciel de la Gateway. Le gatekeeper répond aux aspects suivant de la téléphonie IP :

- **Le routage des appels :** en effet, le gatekeeper est responsable de la fonction de routage. Non seulement, il doit tester si l'appel est permis et faire la résolution d'adresse mais il doit aussi rediriger l'appel vers le bon client ou la bonne passerelle ;
- **Administration de la bande passante :** le gatekeeper alloue une certaine quantité de bande passante pour un appel et sélectionne les codecs à utiliser ;

- **Tolérance aux fautes, sécurité :** le gatekeeper est aussi responsable de la sécurité dans un réseau de téléphonie IP. Il doit gérer les redondances des passerelles afin de faire aboutir tout appel. Il connaît à tout moment l'état de chaque passerelle et route les appels vers les passerelles accessibles et qui ont des ports libres ;
- **Gestion des différentes gateways :** dans un réseau de téléphonie IP, il peut y avoir beaucoup de gateways. Le gatekeeper, de par ses fonctionnalités de routage et de sécurité, doit gérer ces gateways pour faire en sorte que tout appel atteigne sa destination avec la meilleure qualité de service possible.

5. Avantages et inconvénients de la VOIP

➢ Avantages de la VOIP

- **Réduction des coûts :** La VOIP offre la possibilité de réaliser des économies importantes, notamment pour les appels longue distance ou internationaux, car elle utilise des réseaux IP au lieu des réseaux téléphoniques traditionnels.
- **Mobilité et flexibilité :** Grâce à la VOIP, les utilisateurs bénéficient d'une liberté de mouvement accrue, pouvant passer et recevoir des appels depuis pratiquement n'importe quel endroit disposant d'une connexion Internet, que ce soit au bureau, à domicile ou en déplacement. Les numéros de téléphone VOIP sont facilement transférables, offrant une grande souplesse.
- **Fonctionnalités avancées intégrées :** la VOIP est dotée de nombreuses fonctionnalités avancées, notamment la messagerie vocale visuelle, le transfert d'appel, la conférence à plusieurs, identification de l'appelant et bien d'autres, sans frais supplémentaires.
- **Convergence des communications :** La VOIP permet de regrouper voix, données et vidéo sur une seule infrastructure réseau**.**

➢ Inconvénients de la VOIP

- **Dépendance envers la connexion Internet** : Pour fonctionner correctement, la VOIP nécessite une connexion Internet haut débit stable et performante. En cas de problèmes réseau, la qualité des appels vocaux VOIP peut être sérieusement dégradée, avec des coupures, des échos ou des voix déformées.
- **Sensibilité aux pannes d'électricité et aux coupures d'Internet :** les systèmes VOIP dépendent à la fois d'une alimentation électrique continue et d'un accès permanent à

Internet. Ainsi, en cas de coupure de courant ou d'interruption du service Internet, il devient impossible d'émettre ou de recevoir des appels VOIP.

- **Enjeux de sécurité et de confidentialité accrus**: En transitant sur le réseau IP ouvert, les communications VOIP sont exposées à des risques supplémentaires tels que le piratage, l'écoute illégale ou les attaques malveillantes, nécessitant des mesures de sécurité renforcées.

6. Protocoles de signalisation

6.1 Protocole SIP

6.1.1 Description générale du protocole SIP

Le protocole SIP (Session Initiation Protocole) a été initié par le groupe MMUSIC (Multiparty Multimedia Session Control) et désormais repris et maintenu par le groupe SIP de l'IETF. SIP est un protocole de signalisation appartenant à la couche application du modèle OSI. Son rôle est d'ouvrir, modifier et libérer les sessions. L'ouverture de ces sessions permet de réaliser de l'audio ou vidéoconférence, de l'enseignement à distance, de la voix (téléphonie) et de la diffusion multimédia sur IP. [3]

6.1.2 Architecture de SIP

L'architecture fonctionnelle de SIP s'articule autour de plusieurs entités logicielles interagissant de manière coordonnée pour assurer l'établissement, le contrôle et la terminaison des sessions multimédias sur IP. Les principaux éléments constitutifs sont :

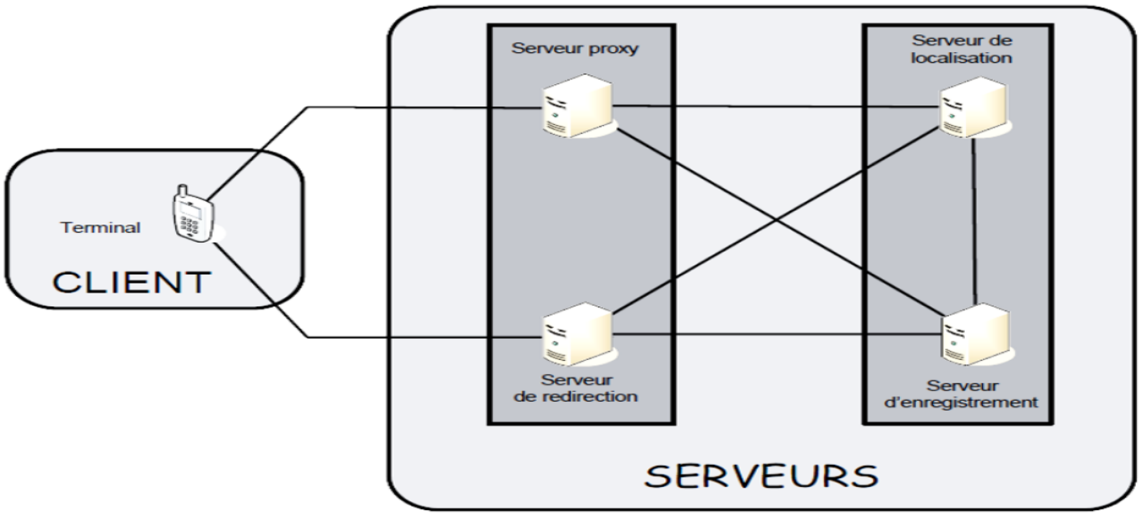


Figure 1.3 : Architecture de SIP [5].

- **Terminal :**

Un terminal, aussi appelé "user agent" (UA), est un composant logiciel ou matériel situé aux extrémités d'une session de communication. Son rôle est d'initier, recevoir et terminer des sessions multimédias. Il permet aux utilisateurs de passer et de recevoir des appels. Les terminaux SIP peuvent se présenter sous deux formes distinctes: une implémentation matérielle dédiée (hardphone) ou une application logicielle (softphone) installée sur un équipement informatique. Un user agent se compose de deux parties :

- User Agent Client (UAC) : la partie cliente du terminal qui émet des requêtes SIP comme INVITE, ACK, CANCEL, BYE etc. C'est l'entité qui initie la session SIP.
- User Agent Server (UAS) : la partie serveur du terminal qui reçoit les requêtes SIP provenant d'un UAC et renvoie les réponses appropriées. C'est l'entité qui reçoit la demande de session.

- **Serveur d'enregistrement :**

Le serveur d'enregistrement, ou Registrar Server, est un composant clé de l'infrastructure SIP chargé de la gestion des informations de localisation des utilisateurs. Son rôle principal consiste à traiter les requêtes d'enregistrement REGISTER émises par les terminaux utilisateurs (User Agents) lors de leur connexion au réseau SIP. Lorsqu'un utilisateur se connecte au réseau SIP, il envoie une requête d'enregistrement au serveur d'enregistrement pour l'informer de son URI (Uniform Resource Identifier) et de l'adresse IP ou de l'adresse du domaine où il peut être joint. Le serveur d'enregistrement enregistre alors ces informations dans une base de données, appelée généralement un registre SIP ou un serveur de localisation (Location Server).

- **Serveur de localisation :**

Le serveur de localisation (Location Server) joue un rôle essentiel en permettant la localisation des abonnés dans le réseau. Ce serveur centralisé héberge une base de données contenant les informations de localisation de tous les abonnés qu'il gère. Cette base de données est mise à jour par le serveur d'enregistrement à chaque fois qu'un utilisateur s'enregistre ou change de localisation. Celui-ci transmet ces données actualisées au serveur de localisation.

- **Serveur de redirection :**

Le serveur de redirection est utilisé pour rediriger les requêtes SIP (comme INVITE) vers le serveur de localisation sans se charger lui-même de l'établissement de la communication. Lorsqu'un terminal utilisateur émet une invitation, comme pour initier un appel, cette requête est d'abord transmise au serveur de redirection. Ce dernier n'a pas accès direct aux informations de localisation, il se charge alors de transmettre cette requête au serveur de localisation qui détient la base de données des adresses IP associées à chaque utilisateur enregistré sur le réseau. Le serveur de localisation transmet les informations de localisation de l'appelé au serveur de redirection. Ce dernier peut alors renvoyer ces informations au terminal utilisateur à l'origine de la requête initiale sans avoir à connaitre l'adresse du serveur de localisation.

- **Serveur proxy : [6]**

Le serveur proxy (parfois appelé serveur mandataire) permet d'initier une communication 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. Le serveur proxy remplit les différentes fonctions suivantes :

- localiser un correspondant ;
- réaliser éventuellement certains traitements sur les requêtes ;
- initier, maintenir et terminer une session vers un correspondant.

Lorsqu'un utilisateur demande à un serveur proxy de localiser un correspondant, ce dernier effectue la recherche, mais, au lieu de retourner le résultat au demandeur (comme le serveur de redirection), il utilise cette réponse pour effectuer lui-même l'initialisation de la communication en invitant le correspondant à ouvrir une session.

6.1.3 Messages SIP :

Le protocole SIP repose sur un modèle de communication requête/réponse basé sur un échange de messages entre les différents éléments du réseau. Ces messages SIP se divisent en deux catégories principales :

➢ Les requêtes :

INVITE : Cette requête est utilisée pour initier une session multimédia,

ACK : Après la réception d'une réponse finale (200 OK) à une requête INVITE, l'expéditeur envoie un message ACK pour confirmer la réception de cette réponse et finaliser l'établissement de la session,

BYE : Cette requête est envoyée par l'un des participants pour mettre fin à une session multimédia en cours. Elle indique à l'autre partie que la communication doit être terminée.

CANCEL : Si une requête INVITE est en attente, le message CANCEL permet à l'expéditeur d'annuler cette requête avant qu'elle ne soit acceptée ou rejetée par le destinataire.

REGISTER : Un client utilise cette requête pour s'enregistrer auprès d'un serveur d'enregistrement. Cela permet au serveur de connaître l'emplacement du client pour acheminer les futures requêtes.

OPTIONS : Cette requête est utilisée pour interroger les capacités d'un serveur ou d'un client SIP. Elle permet de découvrir les fonctionnalités prises en charge par l'entité cible.

➢ Les réponses :

Classe	Définition de la famille de réponse	Principales réponses
1xx	Informative : Ces réponses indiquent que la requête est en cours de traitement.	-100 Trying: Accusé de réception initial de la requête. -180 Ringing: La destination est alertée de l'appel entrant.
2xx	Succès : Elles confirment que la requête a été traitée avec succès.	-200 OK: Réponse positive pour une requête réussie.
3xx	Redirection: Le client doit effectuer une autre action pour compléter la requête.	-302 Moved Temporarily: L'utilisateur a été redirigé temporairement vers une autre adresse.
4xx	Erreur client: La requête comporte une erreur et n'a pas pu être traitée.	-400 Bad Request: La syntaxe de la requête est incorrecte.

		-403 Forbidden: La requête n'est pas autorisée sur le serveur. -404 Not Found: L'utilisateur demandé est introuvable.
5xx	Erreur serveur: Le serveur a rencontré une erreur et n'a pas pu traiter la requête.	-500 Server Internal Error: Une erreur interne empêche le serveur de répondre. -501 Not Implemented: Le serveur ne prend pas en charge la fonctionnalité requise.
6xx	Echec global: La requête ne peut être traitée en aucun point final.	-600 Busy Everywhere: Tous les utilisateurs possibles sont actuellement occupés.

Tableau 1.1 : Description et signification des réponses SIP

6.2 Protocole H323

6.2.1 Description générale de protocole H323

L'UIT a établi H.323 comme une norme pour les systèmes de communication multimédia sur les réseaux à commutation de paquets, tels que l'Internet. Ce protocole fournit un cadre pour le transfert d'informations audio, vidéo et autres sur les réseaux IP. Il décrit les éléments, les protocoles et les procédures nécessaires pour organiser et gérer des sessions de communication multimédia en temps réel. Basée sur une architecture décentralisée, H.323 utilise des mécanismes de signalisation pour repérer, discuter des capacités et établir des appels.

6.3 La comparaison entre SIP et H323

SIP et H.323 sont tous deux des protocoles de signalisation utilisés dans les réseaux VoIP (Voice over IP) pour établir, contrôler et terminer les sessions multimédias. Cependant, ils diffèrent dans leur conception, leur architecture et leur implémentation.

Voici un aperçu sous un tableau de leurs divergences :

Aspect	**SIP**	**H.323**
Origine	IETF (Internet Engineering Task Force)	ITU (International Télécommunication Union)

Architecture	Client-serveur	Décentralisée avec Gatekeeper et MCU
Simplicité	Connu pour sa simplicité	Plus complexe
Déploiement	Plus facile	Nécessite une expertise supplémentaire
Interopérabilité	Adapté aux protocoles Internet	Souvent utilisé dans les réseaux traditionnels
Types de médias supportés	Audio, vidéo, données	Audio, vidéo, données
Gestion de la QoS	Moins avancée, nécessite des extensions	Meilleure gestion de la QoS et de la bande passante
Adoption	Large	Moins répandu

Tableau 1.2 : comparaison entre SIP et H323

En somme, SIP est favorisé en raison de sa simplicité et d'une adoption généralisée, tandis que H.323 offre des fonctionnalités plus avancées mais nécessite une expertise supplémentaire pour être mis en œuvre.

7. Protocoles de transport (RTP, RTCP)

Dans le cadre de notre projet visant à mettre en place une solution VOIP sécurisée, nous examinons attentivement deux protocoles de transport fondamentaux : RTP (Real-time Transport Protocol) et RTCP (Real-time Control Protocol).

7.1 Protocole RTP

7.1.1 Description générale de RTP

Le protocole RTP a été conçu dans le dessein de transporter des données en temps réel, notamment la voix et la vidéo, à travers les réseaux IP. Il offre une approche normalisée pour acheminer des contenus multimédias synchronisés, tout en offrant une compatibilité avec une gamme variée de codecs de compression audio et vidéo. Ce protocole représente un pilier

fondamental dans le domaine des communications VOIP, garantissant un transfert efficace des flux multimédias entre les participants.

7.1.2 Les fonctions de RTP

Les principales fonctions de RTP incluent :

1. **Numérotation des paquets :** Chaque paquet reçoit un numéro de séquence pour détecter les pertes ou duplications.
2. **Estampillage temporel :** Chaque paquet contient une marque temporelle pour une reconstruction précise.
3. **Identification des sources :** Attribution unique de l'origine du flux multimédia.
4. **Multiplexage des flux :** Combinaison de plusieurs flux dans une même session.
5. **Contrôle de la livraison :** Détection des pertes de paquets pour des actions correctives.

7.1.3 Avantages et inconvénients

➢ Avantages

- Adapté à la transmission en temps réel sur des réseaux peu fiables.
- Intègre des mécanismes de synchronisation et de détection des pertes.
- Permet le regroupement de flux multimédias.
- Complémentaire à RTCP pour le contrôle de la transmission.

➢ Inconvénients

- Manque de fiabilité et de contrôle de congestion intégrés.
- Sécurité non garantie (nécessite SRTP pour la sécurisation).
- Nécessite une coordination avec d'autres protocoles de signalisation.

7.2 Protocole RTCP

7.2.1 Description générale de RTCP

Le protocole de contrôle du transport en temps réel RTCP est utilisé en parallèle avec RTP pour surveiller et contrôler les flux multimédias en temps réel. Son rôle vital est de s'assurer

que le service fourni est de qualité (QOS) lorsqu'il transmet des données multimédias sur les réseaux IP.

7.2.2 Les fonctions de RTCP

RTCP s'occupe principalement de ces fonctions :

1. **Rapports d'envoi :** Les participants envoient régulièrement des statistiques sur les paquets envoyés, y compris le nombre de paquets et les pertes éventuelles.
2. **Rapports de réception :** Les rapports des récepteurs fournissent des détails sur la qualité de la réception, comme le pourcentage de perte de paquets.
3. **Description des sources :** RTCP transmet des informations détaillées sur les sources participant à la session, telles que les identifications et les adresses.
4. **Paquets de rapport spécifiques à l'application :** Les applications peuvent échanger des paquets de rapport adaptés à leurs besoins spécifiques, améliorant ainsi les fonctionnalités.
5. **Contrôle de la bande passante :** RTCP surveille l'utilisation de la bande passante par les flux RTP pour garantir une utilisation efficace de la bande passante disponible.

7.2.3 Avantages et inconvénients

➢ Avantages

- Fournit des renseignements cruciaux sur la qualité de transmission des flux RTP, comme le délai, la gigue et la perte de paquets.
- Permet aux applications d'intervenir rapidement en cas de détérioration de la qualité.
- Assure une surveillance continue de la session RTP, permettant une évaluation constante des performances.
- Offre une flexibilité grâce aux ensembles de rapports APP spécifiques aux applications.

➢ Inconvénients

- Engendre un trafic de contrôle RTCP supplémentaire, augmentant ainsi la charge sur le réseau.
- Manque de mécanismes intégrés de sécurité pour la confidentialité et l'intégrité des données (nécessitant l'utilisation conjointe avec SRTP).

8. La qualité de service

8.1 Définition

La Qualité de Service (QoS) est un ensemble de technologies et de mécanismes utilisés pour garantir que les services de communication, tels que la Voix sur IP (VoIP), fonctionnent de manière optimale et satisfaisante pour les utilisateurs.

Comme JAQUE HEROVITZ la définit: « La qualité de service est le niveau d'excellence que l'entreprise a choisi d'atteindre pour satisfaire sa clientèle cible, c'est en même temps, la mesure dans laquelle elle s'y conforme. » [7]

La QoS est essentielle pour la mise en place d'une solution VoIP sécurisée, car elle assure que les appels vocaux sont clairs, fiables et exempts d'interruptions, même dans des environnements réseau complexes et chargés, en se concentrant sur plusieurs paramètres clés :

- ✓ **Latence :** Le délai de transmission des paquets de données d'un point à un autre. Pour les appels VoIP, une latence inférieure à 150 millisecondes est généralement acceptable pour une conversation de bonne qualité.
- ✓ **Gigue :** La variation de la latence des paquets de données. Une gique élevé peut causer des interruptions et une dégradation de la qualité audio. La gestion de la gigue est essentielle pour maintenir la fluidité des communications.
- ✓ **Perte de Paquets :** Le pourcentage de paquets de données qui sont perdus pendant la transmission. Une perte de paquets supérieure à 1% peut affecter significativement la qualité audio des appels VoIP.
- ✓ **Bande Passante** : La capacité du réseau à transmettre des données. Une bande passante insuffisante peut entraîner une congestion du réseau, augmentant ainsi la latence et la gigue.
- ✓ **Priorisation du Trafic :** La capacité à prioriser le trafic VoIP par rapport aux autres types de trafic sur le réseau. Cela permet de s'assurer que les appels vocaux reçoivent la priorité nécessaire pour maintenir une qualité audio élevée, même en cas de forte utilisation du réseau.

Pour garantir une QoS optimale dans une solution VoIP, il est crucial de mettre en œuvre des mécanismes de gestion de réseau tels que :

- ✓ **Marquage des Paquets :** Utilisation de protocoles comme DiffServ (Differentiated Services) pour marquer les paquets VoIP afin qu'ils soient traités avec une priorité plus élevée.
- ✓ **Contrôle de la Congestion :** Utilisation de techniques pour gérer la bande passante et éviter la congestion du réseau, comme la mise en place de files d'attente spécifiques pour le trafic VoIP.
- ✓ **Surveillance et Gestion Proactive :** Surveillance continue de la performance du réseau et des appels VoIP pour détecter et corriger rapidement les problèmes de QoS.

9. Conclusion

La compréhension de la technologie VOIP repose en grande partie sur ce premier chapitre. Nous avons exploré ses principes fondamentaux, son architecture et les protocoles qui l'encadrent. Nous avons dévoilé les principaux mécanismes de cette technologie qui évolue sans cesse, de la numérisation de la voix à la transmission des paquets de données sur le réseau IP.

Néanmoins, la mise en place d'une solution VOIP nécessite une compréhension approfondie de ses aspects techniques. Dans le contexte de la VOIP, la sécurité est un enjeu majeur pour tout système d'information. C'est la raison pour laquelle, en se basant sur les connaissances acquises dans ce chapitre, nous allons maintenant nous concentrer sur les aspects de sécurité liés à la VOIP et explorer les solutions pour la sécuriser.

Chapitre 2 :

Compréhension des Risques et Solutions de Sécurité en Voix sur IP

1. Introduction

Ce chapitre examine les vulnérabilités de sécurité qui mettent en péril les communications vocales sur Internet. Nous étudions les points faibles des protocoles, des applications et des systèmes d'exploitation, ainsi que les attaques courantes à chaque étape. Notre objectif est d'offrir une compréhension approfondie des enjeux sécurité et des solutions adaptées, en mettant l'accent sur les bonnes pratiques et les moyens de renforcer. Les recherches approfondies et les exemples concrets utilisés pour cette analyse fournissent un guide essentiel pour renforcer la sécurité des communications vocales sur Internet.

2. Les vulnérabilités des protocoles de communication

Les vulnérabilités des protocoles de communication dans le contexte de la VoIP se réfèrent aux points faibles inhérents aux protocoles utilisés pour la transmission des données vocales sur Internet. Étant donné que la VoIP utilise des protocoles tels que SIP et RTP, elle est sujette à diverses failles de sécurité, telles que le détournement de session pour les flux TCP ou la mystification pour les paquets UDP, etc.

Les attaques les plus fréquemment rencontrées contre un système de VoIP sont :

2.1 Sniffing

2.1.1 Définition

Le sniffing est une technique qui consiste à capturer et analyser le trafic de données circulant sur un réseau à l'aide d'un outil appelé sniffer. L'objectif du sniffing est souvent d'obtenir un accès non autorisé à un système ou un réseau, de voler des données sensibles ou de perturber le fonctionnement normal du système.

2.1.2 Problématique de sécurité

En ce qui concerne la VoIP, le sniffing peut être utilisé pour écouter les conversations téléphoniques, compromettant ainsi la confidentialité des communications. Les attaquants peuvent intercepter les paquets de données VoIP pour obtenir des informations sensibles ou pour surveiller les activités des utilisateurs.

2.1.3 Recommandations de sécurité

Utilisez le chiffrement des communications VoIP en implémentant des protocoles comme TLS pour protéger le trafic contre l'interception. Assuré également de segmenter le réseau et de restreindre l'accès aux données sensibles.

2.2 Suivie d'appel

2.2.1 Définition

Appelé aussi Call tracking, cette attaque se fait au niveau du réseau LAN/VPN et cible les terminaux (soft/hard phone). Elle a pour but de connaître qui est en train de communiquer et quelle est la période de la communication. L'attaquant doit récupérer les messages INVITE et BYE en écoutant le réseau et peut ainsi savoir qui communique, à quelle heure, et pendant combien de temps. Pour réaliser cette attaque, L'attaquant doit être capable d'écouter le réseau et récupérer les messages INVITE et BYE [8].

2.2.2 Problématique de sécurité

Dans le contexte de la VoIP, le suivi d'appel peut être exploité par des individus malintentionnés pour surveiller les activités des utilisateurs, compromettant ainsi leur vie privée et leur sécurité. Les attaquants peuvent recueillir des informations sensibles telles que les numéros composés, les identifiants d'appelants, ou même enregistrer les conversations téléphoniques à l'insu des participants. Cela peut avoir des implications graves, notamment en matière de confidentialité des données et de conformité réglementaire.

2.2.3 Recommandations de sécurité

Met en place des mécanismes d'authentification forte, comme l'authentification à deux facteurs, pour empêcher les accès non autorisés. Utiliser également des techniques de chiffrement pour protéger les informations d'identification et les données de l'appel.

2.3 Les spams

2.3.1 Définition

Le spam dans les communications VoIP fait référence à l'envoi massif et non sollicité de messages, d'appels ou de demandes de présence sur les réseaux VoIP. Tout comme dans d'autres domaines de communication, le spam VoIP est généralement associé à des tentatives de publicité indésirable, des escroqueries ou des tentatives de phishing.

Il existe trois formes de spams [8] :

- **Call Spam :** Ce type de spam est définit comme un grand nombre de tentatives d'ouverture de session non sollicitées. Une fois l'appel établi, le programme génère un ACK, répond à une annonce précédemment enregistrée, puis interrompt la communication.
- **IM (Instant Message) Spam :** consiste en un envoi massif de messages instantanés non sollicités, généralement sous forme de requêtes SIP (INVITE) contenant de grands en-têtes ou corps de messages indésirables.
- **Presence Spam :** Ce type de spam est comparable au spam de messagerie instantanée. Il est décrit comme un grand nombre de demandes de présence non sollicitées. L'attaquant fait cela afin d'être inclus dans la "liste blanche" d'un utilisateur afin qu'il puisse lui envoyer des messages instantanés.

2.3.2 Problématique de sécurité

Le spam dans les communications VoIP crée des problèmes de sécurité, de gestion et d'expérience utilisateur. Il peut provoquer une surcharge du réseau, une perte de productivité et une exposition à des contenus indésirables. De plus, il expose les utilisateurs à des risques de sécurité comme les escroqueries ou les logiciels malveillants. Pour contrer ces menaces et préserver la qualité de service, des mesures de protection appropriées sont nécessaires.

2.3.3 Recommandations de sécurité

Met en place des filtres anti-spam pour identifier et bloquer les appels provenant de sources non autorisées. Utiliser également des listes de blocage pour bloquer les numéros de téléphone connus pour être utilisés à des fins de spam.

2.4 Détournement d'appel (Call Hijacking)

2.4.1 Définition

Le détournement d'appel, également connu sous le nom de Call Hijacking, se réfère à une technique utilisée par des individus malveillants pour prendre le contrôle d'un appel en cours. L'attaquant peut intercepter la communication ou modifier sa trajectoire afin d'écouter les conversations, d'injecter du contenu malveillant ou de rediriger l'appel vers un autre destinataire sans que les parties concernées ne le sachent.

Exemple : quand un agent SIP envoie un message INVITE pour initier un appel, l'attaquant envoie un message de redirection 3xx indiquant que l'appelé s'est déplacé et par la même occasion donne sa propre adresse comme adresse de renvoi. A partir de ce moment, tous les appels destinés à l'utilisateur sont transférés et c'est l'attaquant qui les reçoit. [8]

2.4.2 Problématique de sécurité

Le détournement d'appel dans les communications VoIP pose des risques graves pour la confidentialité, la sécurité et l'intégrité des communications. Les attaquants peuvent écouter des conversations privées, collecter des informations sensibles ou usurper l'identité des parties impliquées pour mener des activités frauduleuses. Cela peut compromettre la confiance des utilisateurs dans le système VoIP et entraîner des conséquences financières ou juridiques pour les organisations victimes de telles attaques.

2.4.3 Recommandations de sécurité

Renforcer les mécanismes d'authentification et d'autorisation pour empêcher les attaques de détournement d'appel. Surveiller également le trafic réseau pour détecter les comportements suspects et les tentatives d'interception.

2.5 Injection des paquets RTP

2.5.1 Définition

L'injection des paquets RTP est une technique utilisée par les attaquants pour intercepter, modifier ou insérer des paquets de données dans le flux de trafic RTP d'une communication VoIP. Ces paquets peuvent contenir des informations malveillantes, telles que des données

corrompues, des enregistrements audio frauduleux ou des instructions de redirection, compromettant ainsi l'intégrité, la confidentialité et la disponibilité de la communication.

Cette attaque sur un réseau LAN/VPN cible le serveur d'enregistrement dans le but de perturber une communication en cours. L'attaquant doit d'abord écouter le flux RTP entre l'appelant et l'appelé, analyser son contenu, puis générer un paquet RTP avec un en-tête similaire mais un numéro de séquence et un timestamp plus élevés afin que ce paquet soit traité en priorité. Cela perturbera la communication et empêchera l'appel de se dérouler correctement.

Pour réussir, l'attaquant doit pouvoir écouter le réseau pour détecter une communication et les timestamps RTP, ainsi qu'injecter des paquets RTP qu'il a généré ayant un timestamp modifié [8].

2.5.2 Problématique de sécurité

L'injection des paquets RTP dans les communications VoIP présente des risques sérieux pour la sécurité. Les attaquants peuvent altérer le contenu des conversations, écouter des informations sensibles, perturber la qualité de la communication ou même rediriger le trafic vers des destinations non autorisées. Cela peut entraîner des conséquences graves, telles que la divulgation de données confidentielles, les pertes financières ou les interruptions des activités commerciales.

2.5.3 Recommandations de sécurité

Utiliser des pare-feu et des systèmes de détection des intrusions pour surveiller et filtrer le trafic entrant. Assuré également de maintenir les logiciels et les équipements à jour pour corriger les vulnérabilités connues.

2.6 Le déni de service (DoS)

2.6.1 Définition

Le déni de service est une attaque informatique visant à rendre indisponible un service, serveur ou équipement en le submergeant de requêtes fictives afin de saturer ses ressources et l'empêcher de répondre aux demandes légitimes des utilisateurs.

Les failles du service se présentent de différentes façons. Les plus courantes cherchent à monopoliser toute la bande passante disponible ou tirent profit des vulnérabilités inhérentes aux protocoles TCP/IP, bloquant par conséquent toute tentative de communication [8].

Les diverses méthodes d'attaque de déni de service sont :

a) Attaque par la méthode du cancel :

Il s'agit d'une attaque ciblant spécifiquement un utilisateur. L'attaquant surveille l'activité du proxy SIP et attend qu'un appel entrant arrive pour l'utilisateur visé. Dès que le dispositif de l'utilisateur reçoit la requête INVITE pour établir l'appel, l'attaquant envoie immédiatement une requête CANCEL, cette requête provoque une erreur sur le dispositif de l'appelé et met fin à l'appel de façon prématurée [8].

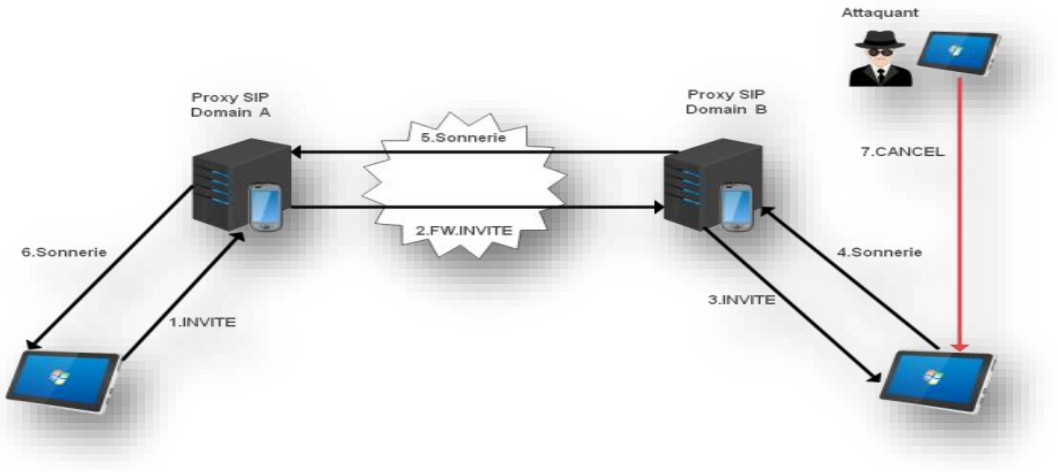


Figure 2.1 : Attaque Dos avec la méthode CANCEL [9]

La figure suivante montre un scénario d'attaque DoS CANCEL, l'utilisateur A initié un appel et envoie une requête INVITE (1) à son proxy SIP. Celui-ci la transmet (2) au proxy du domaine B responsable de l'utilisateur B. Le proxy B achemine ensuite l'INVITE (3) vers B, qui reçoit l'appel entrant (4). Pendant ce temps, un attaquant surveille l'activité du proxy B. Avant que B n'ait pu accepter l'appel avec une réponse OK, l'attaquant envoie une requête CANCEL (7) au proxy B. Cette requête CANCEL annule la requête INVITE en attente avant son acceptation, empêchant ainsi l'établissement de l'appel entre A et B.

b) Attaque par la méthode de BYE :

L'attaque par la méthode BYE cible les utilisateurs de services de communication. Un attaquant intercepte une session établie et récupère les informations nécessaires pour générer un message BYE (de fin de session) frauduleux. Comme ce message n'est pas authentifié, lorsqu'il est injecté dans le réseau, le destinataire l'accepte, ce qui entraîne une interruption involontaire de la session légitime. En écoutant le trafic réseau, un pirate peut ainsi provoquer la fermeture de sessions en cours en usurpant l'identité d'un des correspondants. Cette attaque exploite le manque d'authentification du message BYE dans certains protocoles.

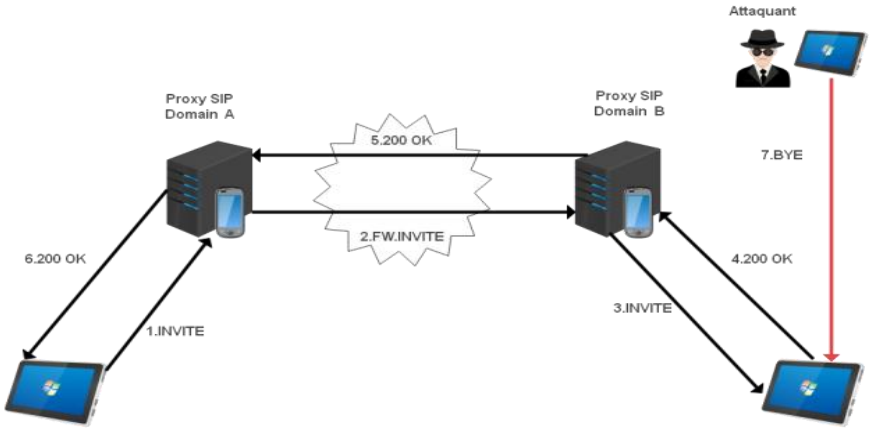


Figure 2.2 : Attaque Dos avec la méthode BYE [9]

Dans ce scénario, similaire au précédent, l'attaquant attend qu'une session soit établie avec succès entre deux utilisateurs. Il laisse passer les messages d'invitation et d'acceptation (1, 2, 3, 4) sans intervenir. Cependant, dès que la réponse "200 OK" confirmant l'établissement de la session (4) est envoyée, l'attaquant envoie un message frauduleux "BYE" à un ou aux deux participants. Ce message "BYE" non authentifié est interprété par le(s) destinataire(s) comme une demande légitime de fin de session. La session est alors brutalement interrompue par cette fausse demande, empêchant les utilisateurs de pouvoir communiquer.

c) Register :

Cette méthode consiste à surcharger le serveur d'enregistrement (registrar) avec un grand nombre de requêtes d'enregistrement malveillantes. L'objectif est de saturer les ressources du serveur, le rendant ainsi incapable de traiter les requêtes légitimes des utilisateurs. Cette méthode d'attaque DoS cible spécifiquement le processus d'enregistrement des clients VoIP sur le réseau, empêchant de nouveaux utilisateurs de se connecter et perturbant le service.

2.6.2 Recommandations de sécurité

Mettre en place des mécanismes de limitation de bande passante pour atténuer les effets des attaques DoS. Utiliser également des filtres anti-spoofing pour identifier et bloquer le trafic malveillant.

2.7 Attaque d'écoute clandestine « Eavesdropping »

2.7.1 Définition

L'attaque d'écoute clandestine, ou eavesdropping, est une forme d'espionnage visant à capturer illégalement les données circulant sur un réseau VoIP. Les attaquants interceptent furtivement les communications vocales, compromettant ainsi la confidentialité des échanges. Des techniques logicielles et matérielles permettent cette interception non autorisée menaçant la sécurité des réseaux VoIP non chiffrés.

a) Attaque Man in the Middle

L'attaque Man in the Middle consiste en l'interception malveillante d'une communication entre deux parties, sans que celles-ci ne s'en rendent compte. Un attaquant se positionne comme un intermédiaire transparent, relayant les échanges tout en ayant la possibilité de les lire, les modifier ou les supprimer à sa guise. Cette forme d'attaque permet à un pirate informatique de se faire passer pour une entité légitime auprès des deux interlocuteurs, tout en restant dissimulé. L'objectif principal est de compromettre la confidentialité et l'intégrité des données échangées, en violant la confiance établie entre les participants. En gros, c'est comme si quelqu'un écoutait une conversation téléphonique sans que les interlocuteurs ne le sachent, mais en ayant la possibilité d'influencer ce qui est dit.

b) Espionnage des communications VOIP avec Wireshark

L'espionnage des communications VoIP avec Wireshark consiste à intercepter et analyser de manière malveillante les flux de données vocales transitant sur un réseau IP. Wireshark est un puissant outil d'analyse de trafic réseau qui permet de capturer les paquets circulant sur le réseau physique. Dans le cadre d'une attaque par espionnage, un pirate informatique peut utiliser Wireshark pour cibler spécifiquement les paquets RTP qui transportent le contenu audio des conversations VoIP. En analysant et reconstituant ces paquets RTP, l'attaquant parvient à écouter et éventuellement enregistrer les conversations téléphoniques confidentielles.

2.7.2 Recommandations de sécurité

Utilise le chiffrement des communications VoIP pour protéger la confidentialité des données. Assure également de sécuriser l'accès aux équipements VoIP et de surveiller activement le réseau pour détecter toute activité suspecte.

3. Les vulnérabilités de l'infrastructure

Une infrastructure VoIP comprend divers éléments comme les téléphones IP, passerelles et serveurs, accessibles via le réseau. Chaque composant exécutant des logiciels peut présenter des failles exploitables par des attaquants. Tout équipement connecté représente ainsi un vecteur d'attaque potentiel vers l'infrastructure. Une approche de sécurité globale, couvrant l'ensemble des composants, est donc essentielle pour protéger le système VoIP contre les menaces internes et externes. [10]

3.1 Faiblesses dans la configuration des dispositifs de la VoIP

De nombreux équipements VoIP, dans leur configuration d'usine, disposent de multiples ports TCP et UDP ouverts pour divers services. Si ces services ne sont pas correctement sécurisés, ils peuvent être vulnérables à des attaques par déni de service, dépassement de tampon mémoire, etc. En outre, la plupart des dispositifs VoIP embarquent un serveur web pour l'administration à distance, lequel peut être la cible d'attaques par dépassement de tampon ou de divulgation d'informations sensibles en l'absence de mots de passe robustes.

Les services SNMP, souvent activés par défaut, représentent également un risque en cas d'exploitation malveillante à des fins de reconnaissance ou de dépassement de tampon.

Enfin, de nombreux équipements VoIP sont configurés pour télécharger périodiquement des fichiers de configuration à partir d'un serveur, généralement via TFTP. Un attaquant peut détourner cette connexion pour faire télécharger un fichier de configuration malveillant au dispositif. [10]

3.2 Les téléphones IP

Un attaquant peut compromettre un dispositif de téléphonie IP comme un téléphone IP, un logiciel de téléphonie ou d'autres équipements clients. Généralement, il obtient un niveau de privilèges élevé lui permettant de contrôler entièrement les fonctionnalités du dispositif. Ce compromis peut être réalisé à distance ou par un accès physique au terminal.

L'attaquant pourrait alors modifier plusieurs aspects opérationnels du dispositif compromis :

- La pile du système d'exploitation peut être altérée pour dissimuler la présence de l'attaquant.
- Un firmware modifié de manière malveillante pourrait être téléchargé et installé. La configuration des logiciels de téléphonie IP pourrait être changée pour permettre :

  - ✓ Le détournement des appels entrants vers une autre destination à l'insu de l'utilisateur.
  - ✓ L'interception et l'enregistrement des appels.
  - ✓ Le routage et l'altération des données de signalisation et des flux voix.
  - ✓ La dégradation de la disponibilité en rejetant les appels, désactivant les notifications et l'interruption soudaine des communications en cours.
- Des portes dérobées (backdoors) pourraient être installées pour un accès pérenne.
- Toutes les informations personnelles concernant l'utilisateur stockées sur l'appareil pourraient être exfiltrées.

L'accès non autorisé à un dispositif de téléphonie IP peut résulter d'une autre faille sur le réseau IP ou d'informations récoltées sur celui-ci. Les softphones sont plus vulnérables que les téléphones IP physiques en raison des multiples vecteurs d'attaque liés au système d'exploitation hôte, aux applications, aux services, aux virus/vers, etc. De plus, résidant sur le réseau données,

ils sont exposés aux menaces visant ce segment, pas seulement l'hôte. En revanche, les téléphones IP autonomes exécutent leur propre système d'exploitation minimaliste avec moins de services exposés, réduisant leurs surfaces d'attaque. [10]

3.3 Les serveurs

Les pirates peuvent également viser les serveurs qui fournissent le service de téléphonie IP. Le compromis d'un tel serveur met en danger l'ensemble du réseau de téléphonie IP dont il fait partie. Par exemple, si un serveur de signalisation est compromis, un attaquant peut prendre le contrôle total des données de signalisation des appels qui transitent par ce serveur. Cela lui permet de modifier n'importe quel paramètre relatif aux communications. De plus, lorsqu'un serveur de téléphonie IP est installé sur un système d'exploitation classique, il devient vulnérable aux menaces visant ce système, comme les virus, vers et autres codes malveillants. [10]

4. Les vulnérabilités du système d'exploitation

Les systèmes d'exploitation sont vulnérables à diverses failles, notamment le buffer overflow qui permet à un attaquant de prendre le contrôle partiel ou total de la machine. Bien que ce ne soit pas la seule vulnérabilité, elles varient selon le fabricant et la version, mais découlent principalement d'un manque de sécurité lors du développement initial. Ces failles ne sont souvent découvertes qu'après le lancement du produit.

Les dispositifs VoIP tels que les téléphones IP, Call Managers, Gateways et serveurs proxy héritent des mêmes vulnérabilités que le système d'exploitation ou le firmware sur lequel ils s'exécutent. Des centaines de vulnérabilités exploitables à distance existent sur Windows et même Linux, avec de nombreux exploits disponibles gratuitement sur Internet, prêts à être téléchargés.

Peu importe la sécurité apparente d'une application VoIP, celle-ci devient discutable si le système d'exploitation sous-jacent est compromis. Ainsi, la sécurité de ces applications dépend grandement de la robustesse du système d'exploitation sur lequel elles reposent. [10]

5. Sécurisation et bonne pratique

Les vulnérabilités peuvent se situer au niveau des protocoles, des applications ou des systèmes d'exploitation. Par conséquent, une sécurisation à ces trois niveaux protocolaire, applicatif et système d'exploitation est nécessaire pour une protection complète.

5.1 Sécurisation protocolaire

La protection de la confidentialité des communications vocales sur IP est essentielle, en particulier face à la facilité avec laquelle les paquets peuvent être interceptés ("sniffés") sur le réseau. Le chiffrement s'avère donc indispensable pour sécuriser ces échanges entre utilisateurs interconnectés. Bien que certains protocoles doivent compter sur leurs propres mécanismes de sécurité intrinsèques, le recours à IPsec offre une solution efficace pour deux objectifs majeurs.

D'une part, IPsec permet d'authentifier mutuellement l'identité des points terminaux impliqués dans la communication. D'autre part, il assure le chiffrement des flux vocaux, une fois que les paquets quittent le réseau intranet de l'entreprise. Cette combinaison de la voix sur IP avec IPsec, appelée VoIPsec, réduit les menaces liées à l'analyse du trafic vocal et à l'utilisation de sniffers de paquets. Associée à un pare-feu, cette approche renforce la sécurité de la voix sur IP par rapport aux lignes téléphoniques classiques. En effet, IPsec n'est pas une solution universelle applicable à l'ensemble des applications. Certains protocoles disposent de leurs propres fonctionnalités de sécurité intégrées, sur lesquelles ils doivent continuer à se reposer afin de garantir leur sécurité de manière appropriée.

5.1.1 VoIP VPN

La VoIP VPN est une solution qui combine la technologie de la voix sur IP et celle des réseaux privés virtuels pour assurer une communication vocale sécurisée. La VoIP numérise la voix en paquets de données, tandis que le VPN crée un tunnel crypté entre les points d'extrémité du réseau, protégeant ainsi les données transmises contre les accès non autorisés.

Dans cette approche, le mode tunnel du VPN est privilégié, car il encapsule et chiffre l'intégralité des paquets, y compris les en-têtes (contrairement au mode transport qui ne sécurise que la charge utile IP), garantissant ainsi la confidentialité et l'intégrité des communications. Le protocole ESP est souvent choisi en conjonction avec le mode tunnel, car il assure le

chiffrement des données en plus de l'authentification des paquets (Contrairement au protocole AH, qui se limite à authentifier les paquets).

L'implémentation de la VoIP VPN est généralement déployée au niveau des routeurs ou des points de terminaison de la voix IP, minimisant ainsi le nombre de machines impliquées dans le traitement de sécurité et réduisant le nombre de clés cryptographiques nécessaires. Cette solution offre une méthode robuste pour préserver la confidentialité et l'intégrité des communications vocales sur IP, en les acheminant à travers un tunnel VPN sécurisé. [11]

5.1.2 Secure RTP ou SRTP

Le SRTP est un protocole de sécurité conçu spécifiquement pour protéger les communications multimédias en temps réel. Il vise à combler les lacunes des protocoles de sécurité existants, comme IPsec, dont le mécanisme d'échange de clés est considéré comme trop lourd pour les applications en temps réel. SRTP est étroitement lié au protocole RTP, sur lequel il se base pour transporter les données multimédias. Il comprend également un ensemble de protocoles complémentaires, notamment le protocole MIKEY qui gère la distribution et la mise à jour des clés de chiffrement.

L'un des avantages clés du SRTP est sa compatibilité avec les protocoles de signalisation utilisés dans la VoIP, tels que SIP, ainsi qu'avec le protocole RTSP pour la diffusion de contenu multimédia en temps réel. Cette compatibilité permet une intégration transparente de la sécurité dans les applications multimédias existantes. [11]

a) Services de sécurités offerts par SRTP

Les principaux services offerts par SRTP sont :

Confidentialité des données RTP : SRTP permet de chiffrer l'en-tête et la charge utile des paquets RTP, ou seulement la charge utile, afin de garantir la confidentialité des données transmises. Cette fonctionnalité empêche toute interception non autorisée du contenu du flux multimédia ;

Authentification et intégrité des paquets RTP : SRTP calcule une empreinte numérique (hash) du message à transmettre et l'inclut avec le paquet, permettant au récepteur de vérifier

l'authenticité et l'intégrité des données reçues. Cela prévient contre les attaques de type "homme du milieu" ou les altérations malveillantes des paquets ;

Protection contre le rejet de paquets : Chaque récepteur SRTP maintient une liste des indices de séquence des paquets reçus et authentifiés avec succès. Cela permet de détecter les éventuelles tentatives de rejeu (rejouer un paquet capturé précédemment) et de les rejeter. [11]

b) Principe de fonctionnement de SRTP

SRTP est une extension sécurisée du protocole RTP. Son objectif principal est d'offrir une solution de chiffrement et d'authentification des flux multimédias en temps réel, tout en minimisant l'impact sur les performances et la consommation de ressources.

Le fonctionnement de SRTP repose sur une gestion de clés cryptographiques et l'utilisation de primitives cryptographiques légères. Les composants clés de SRTP sont :

- **Clé maîtresse :** Une clé principale aléatoire utilisée pour dériver les clés de session ;
- **Fonction de dérivation de clés :** Un algorithme permettant de générer de manière sécurisée les clés de session à partir de la clé maîtresse et d'autres paramètres ;
- **Clés de salage (salt keys) :** Des clés aléatoires introduites pour renforcer la sécurité et prévenir les attaques par rejeu ou par force brute.

SRTP utilise deux types de clés : les clés de session et la clé maîtresse. Les clés de session sont utilisées directement dans les opérations de chiffrement et d'authentification des paquets RTP. La clé maîtresse, quant à elle, est une chaîne de bits aléatoires à partir de laquelle les clés de session sont dérivées de manière sécurisée à l'aide de fonctions cryptographiques. [11]

c) Format du paquet SRTP

Dans le protocole SRTP, les paquets RTP sont transformés et renforcés avec des mécanismes de sécurité supplémentaires. Cette transformation implique l'ajout de deux champs spécifiques au paquet RTP d'origine.

Le premier champ ajouté est l'identifiant de clé maîtresse (MKI). Cet identifiant permet au récepteur de retrouver la clé maîtresse appropriée dans le contexte cryptographique utilisé. Il facilite ainsi la gestion du renouvellement des clés, lorsque cela est nécessaire.

Le second champ introduit est un code d'authentification (Authentication Tag). Ce code est calculé et inséré lorsque le message a été authentifié. Son utilisation est fortement recommandée, car il fournit une authentification des en-têtes et des données RTP, ainsi qu'une protection indirecte contre le rejet de paquets en authentifiant le numéro de séquence. [11]

5.1.3 TLS (Transport Layer Security)

a) Description

TLS est un protocole de chiffrement qui sécurise la communication entre le client et le serveur. Il utilise des certificats pour authentifier les parties et chiffre les données en transit, protégeant ainsi contre l'interception et les attaques de type "man-in-the-middle".

Le protocole TLS (Transport Layer Security) assure la confidentialité, l'intégrité et l'authentification des communications sur un réseau. En chiffrant les données échangées, TLS empêche les interceptions non autorisées. Il garantit l'intégrité des données en utilisant des mécanismes de hachage pour vérifier qu'elles n'ont pas été altérées où modifiées. De plus, TLS authentifie les parties communicantes à l'aide de certificats numériques, assurant que les deux parties sont bien celles qu'elles prétendent être, protégeant ainsi contre les attaques de type "man-in-the-middle" et d'autres cyberattaques, assurant une connexion sécurisée et fiable.

b) Fonctionnement du Protocole TLS

Le fonctionnement de TLS (Transport Layer Security) peut être décrit en quatre étapes principales :

1. Négociation de la Version et des Paramètres : Le client et le serveur s'entendent sur la version de TLS à utiliser et les paramètres de sécurité tels que les algorithmes de chiffrement et les méthodes d'authentification.
2. Authentification du Serveur : Le serveur présente un certificat numérique contenant sa clé publique et des informations d'identification. Le client vérifie la validité du certificat pour s'assurer de l'identité du serveur.
3. Échange de Clés : Le client et le serveur utilisent des techniques de chiffrement asymétrique pour échanger secrètement une clé de session symétrique. Cette clé de session est utilisée pour chiffrer et déchiffrer les données pendant la communication.

4. Chiffrement des Données : Une fois la clé de session établie, les données échangées entre le client et le serveur sont chiffrées à l'aide de cette clé, assurant ainsi la confidentialité des informations transitant sur le réseau.

5.1.4 Pare-feu (Firewall)

a) Définition

Un pare-feu, également appelé firewall, est un composant de sécurité informatique conçu pour surveiller et contrôler le trafic réseau entrant et sortant selon des règles prédéfinies. Son objectif principal est de protéger un système informatique ou un réseau contre les menaces potentielles en filtrant et en autorisant sélectivement le flux de données en fonction de critères tels que l'adresse IP, le port, le protocole, etc. En agissant comme une barrière virtuelle, le pare-feu aide à prévenir les attaques malveillantes, les intrusions et les fuites de données en empêchant l'accès non autorisé et en filtrant le trafic réseau suspect.

b) Principe de Fonctionnement

- **Filtrage des Paquets :** Le pare-feu examine chaque paquet de données en fonction de règles prédéfinies, bloquant ou autorisant le trafic basé sur l'adresse IP, le port et le protocole utilisé.
- **Inspection de l'État :** Le pare-feu suit l'état des connexions réseau actives pour décider de bloquer ou d'autoriser le trafic, empêchant ainsi les attaques courantes contre les systèmes VoIP, telles que les attaques par déni de service (DoS).

5.2 Sécurisation au niveau application

Plusieurs méthodes peuvent être appliquées pour sécuriser l'application, ces méthodes varient selon le type d'application (serveur ou client). Pour sécuriser le serveur, il faut :

- ✓ L'utilisation d'une version stable, Il est bien connu que toute application non stable contient surement des erreurs et des vulnérabilités. Pour minimiser les risques, il est impératif d'utiliser une version stable ;
- ✓ Tester les mises à jour des softwares dans un laboratoire de test. Il est très important de tester toute mise à jour de l'application dans un laboratoire de test, avant de les appliquer sur le système en production ;

- ✓ Ne pas tester les correctifs sur le serveur lui-même ;
- ✓ Ne pas utiliser la configuration par défaut qui sert juste à établir des appels. Elle ne contient aucune protection contre les attaques ;
- ✓ Ne pas installer une application cliente dans le serveur. [11]

5.3 Sécurisation du système d'exploitation

Sécuriser le système d'exploitation sur lequel est déployé le serveur VoIP est crucial, car si ce système est compromis, l'attaque peut se propager à l'application serveur et affecter les fichiers de configuration contenant des informations sensibles sur les clients enregistrés. Pour renforcer la sécurité du système, il est recommandé de suivre ces bonnes pratiques :

- ✓ **Utiliser un système d'exploitation stable et éprouvé:** Les nouvelles versions peuvent contenir des bugs et des failles de sécurité non corrigés. Il est préférable d'opter pour une version stable et de bien maîtriser son environnement avant de mettre à jour.
- ✓ **Appliquer régulièrement les mises à jour et correctifs de sécurité:** Suivre les recommandations des éditeurs et installer les dernières mises à jour de sécurité pour corriger les vulnérabilités connues.
- ✓ **Utiliser des mots de passe robustes:** Éviter les mots de passe simples, dates de naissance, noms ou numéros de téléphone. Les mots de passe doivent être suffisamment longs et combiner des lettres, des chiffres et des caractères spéciaux pour une meilleure protection contre les intrusions.
- ✓ **Exécuter le serveur VoIP avec des privilèges restreints:** Si un attaquant exploite une vulnérabilité du serveur VoIP, il n'héritera que des privilèges limités de l'utilisateur exécutant le service, réduisant ainsi l'impact potentiel de l'attaque.
- ✓ **Minimiser l'installation des composants non essentiels:** Limiter les applications et services installés sur le système à ceux strictement nécessaires au fonctionnement du serveur VoIP. Cela réduit la surface d'attaque potentielle.
- ✓ **Utiliser des pare-feux (firewalls) :** Un pare-feu, qu'il soit logiciel ou matériel, permet de filtrer le trafic réseau entrant et sortant en analysant les en-têtes des paquets IP échangés entre les machines. Il sécurise ainsi le réseau ou l'ordinateur contre les intrusions provenant d'autres systèmes.
- ✓ **Implémenter des listes de contrôle d'accès (ACL) :** Les ACL sont des listes d'entrées de contrôle d'accès (ACE) qui définissent les droits d'accès à accorder ou à refuser à des

personnes ou des groupes spécifiques. Elles peuvent être implémentées au niveau du pare-feu, des routeurs ou directement dans le système d'exploitation. Pour un serveur VoIP, il est crucial d'utiliser les ACL afin de limiter l'accès aux seules personnes autorisées, comme les agents enregistrés, et de refuser l'accès aux utilisateurs indésirables. Les ACL permettent de n'autoriser que les requêtes provenant des agents enregistrés auprès du serveur.

En combinant l'utilisation de pare-feux et d'ACL, il est possible de fermer les ports inutilisés et de n'autoriser l'accès qu'aux ports nécessaires au fonctionnement du serveur VoIP, tels que 5060, 5061, 4569, etc. Cela renforce considérablement la sécurité du serveur en limitant les surfaces d'attaque potentielles. [11]

6. Conclusion

En conclusion, ce chapitre nous a permis de comprendre les risques et les solutions de sécurité en voix sur IP. Nous avons exploré les vulnérabilités du protocole, de l'infrastructure et du système d'exploitation, ainsi que les bonnes pratiques pour sécuriser les communications VoIP. En mettant en place des solutions telles que le chiffrement des données, l'authentification robuste et la surveillance du trafic, il est possible de réduire efficacement les risques et d'assurer une communication VoIP sécurisée. La sécurité des communications VoIP reste un enjeu crucial, nécessitant une attention continue et une mise en œuvre proactive des mesures de sécurité pour garantir l'intégrité, la confidentialité et la disponibilité des communications.

Chapitre 3 :

Étude de l'existant et choix de la solution VoIP

1. Introduction

Ce chapitre se concentre sur l'analyse d'un centre d'appel existant pour identifier ses besoins et défis en matière de communication. À partir de cette étude, nous choisirons une solution VoIP adaptée, en utilisant VMware Workstation pour la virtualisation et Issabel PBX pour la gestion des communications.

Nous détaillerons ensuite le processus d'installation et de configuration de ces outils, fournissant un guide pratique pour déployer une solution VoIP sécurisée et efficace. Cette approche vise à garantir une transition en douceur et une optimisation des performances du centre d'appel, tout en assurant la sécurité des communications.

2. Etude de l'existant

2.1 Présentation du Centre d'Appel

Le centre d'appel que nous avons étudié est une infrastructure essentielle au sein de l'organisation, dédiée à la gestion des interactions téléphoniques avec les clients. Il est structuré pour répondre à un volume élevé d'appels entrants et sortants, et pour offrir un service client de qualité supérieure.

« Le centre d'appels est une structure basée sur le couplage de la téléphonie et de l'informatique qui établit une communication directe, à l'inverse du serveur vocal interactif, entre un interlocuteur " (client, usager, etc.) et le téléopérateur qui représente son entité (entreprise, association, etc.) et dont la mission est de gérer la relation clientèle. » [12]

Dans le domaine de la relation client, le Centre d'Appel Candle Call est un pilier essentiel, proposant une gamme étendue de services et de solutions pour répondre aux multiples besoins des entreprises modernes. Les points essentiels à connaître sont regroupés dans ce tableau :

Section	**Contenu**
Historique et Mission	Fondé en 2013, Candle Call vise à fournir des services de gestion de la relation client de haute qualité. Il se distingue par son engagement à offrir une expérience client exceptionnelle, tout en

	respectant des normes strictes de qualité, d'efficacité et de sécurité. Le centre d'appel est stratégiquement situé, doté d'une infrastructure moderne et capable de s'adapter aux besoins croissants du marché. Son équipe est hautement qualifiée, et l'environnement de travail favorise l'efficacité et la productivité.
Vision	Candle Call s'efforce d'améliorer continuellement l'expérience client grâce à des solutions innovantes et adaptatives. Il aspire à être le leader incontesté des services de gestion de la relation client en Algérie, en mettant l'accent sur l'innovation et l'excellence opérationnelle.
Fonctionnalités Clés	Réception et distribution des appels, traitement des appels sortants, ACD, IVR , enregistrement et surveillance des appels, gestion des appels en file d'attente, intégration CRM, rapports et analyses, support multicanal, assistance personnalisée.
Services Offerts	Le centre d'appel propose une gamme complète de services : support technique, gestion de la relation client, télémarketing, prise de rendez-vous, et sondages/études de marché. Ces services visent à répondre efficacement aux besoins des entreprises, en offrant une assistance personnalisée, une promotion proactive et des données stratégiques pour favoriser la croissance commerciale.

Tableau 3.1 : Présentation de l'Entreprise et de ses Services.

2.2 Objectif d'un Centre d'Appel

« Les centres d'appels sont des sociétés de services qui ont pour objet de gérer la communication des entreprises qui sont leurs clientes, grâce aux innombrables numéros verts fournis par les entreprises. » [13]

D'une autre façon, un centre d'appel vise principalement à offrir un service de qualité à la clientèle en répondant efficacement aux besoins, questions et préoccupations des clients. Cela peut impliquer de résoudre des problèmes techniques, de gérer les demandes d'information, de promouvoir des produits ou services, et de prendre des rendez-vous, entre autres.

En outre, les centres d'appel visent à améliorer l'expérience client en assurant une communication fluide, professionnelle et personnalisée à chaque interaction. Pour notre partie pratique sur la mise en place d'une solution VoIP sécurisée, l'objectif est d'intégrer cette technologie pour améliorer l'efficacité opérationnelle du centre d'appel tout en garantissant la sécurité et la confidentialité des communications. Cette initiative devrait permettre une meilleure connectivité entre les agents et les clients, ainsi que des fonctionnalités améliorées pour un service encore plus réactif et sécurisé.

2.3 Architecture d'un Centre d'Appel

L'architecture d'un centre d'appel est conçue pour gérer efficacement les communications entre les clients et les agents. Voici les principaux composants de cette architecture :

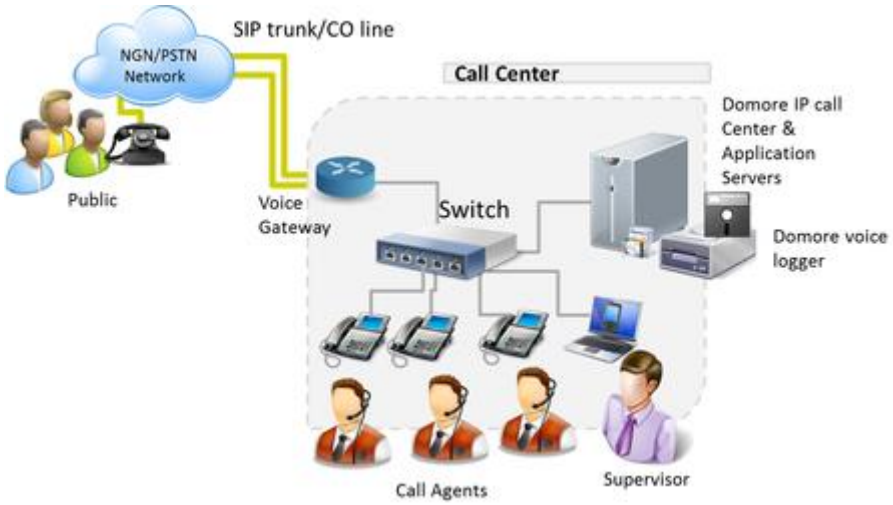


Figure 2.1 : Architecture d'un centre d'appel [14]

a. Serveurs de Communication :

- Hébergent les logiciels de gestion des appels et les bases de données clients.

b. Commutateurs et Routeurs :

- Gèrent le trafic réseau interne et externe, assurant une distribution fluide des connexions.

c. Equipements Téléphoniques :

- Téléphones IP et casques utilisés par les agents pour communiquer avec les clients.

d. Systèmes de Gestion des Appels :

- PBX : Système de commutation téléphonique qui gère les appels internes et externes.

- ACD : Distribue automatiquement les appels entrants aux agents disponibles.

- IVR : Permet aux appelants d'interagir avec un menu vocal automatisé pour accéder aux services spécifiques.

e. Systèmes CRM :

- Centralisent les informations sur les clients et leurs interactions pour offrir un service personnalisé.

f. Sécurité:

- Pare-feu : Protègent contre les accès non autorisés.

- Systèmes IDS/IPS : Surveillent et réagissent aux activités suspectes pour prévenir les intrusions.

Cette architecture intégrée permet aux centres d'appel de fonctionner de manière efficace et sécurisée, offrant une qualité de service élevée aux clients.

3. Problématique

Les centres d'appel jouent un rôle crucial dans la gestion des interactions clients pour de nombreuses entreprises. Ils permettent de centraliser les communications, d'améliorer la satisfaction client et de renforcer la productivité des agents. Grâce à des outils avancés comme les systèmes de gestion des appels, les ACD et les logiciels CRM, les centres d'appel peuvent offrir un service rapide et personnalisé, gérer efficacement un grand volume d'appels, et collecter des données précieuses pour analyser les performances et identifier les domaines d'amélioration.

Cependant, malgré ces nombreux avantages, les centres d'appel présentent également des limitations importantes. Ils peuvent souffrir de problèmes de vulnérabilités en matière de sécurité, de difficultés d'intégration entre différents systèmes, et de défis liés à la qualité du

service. De plus, la maintenance et les coûts associés à ces infrastructures peuvent être prohibitifs, rendant nécessaire l'exploration de solutions plus modernes et efficaces.

Face à ces défis, la question qui se pose est la suivante : **comment les centres d'appel peuvent-ils surmonter leurs limitations actuelles en adoptant des technologies modernes tout en garantissant la sécurité et l'efficacité opérationnelle ?**

- **Objectif :**

Pour répondre à cette problématique, nous nous focalisons sur la mise en place d'une solution VoIP sécurisée. La VoIP offre une flexibilité accrue, des coûts réduits et des options de sécurité avancées, répondant ainsi aux besoins actuels des centres d'appel. En intégrant des outils de virtualisation pour une gestion efficace des ressources et des systèmes de gestion des communications unifiées, nous visons à transformer les opérations du centre d'appel en améliorant la qualité des communications et en renforçant la sécurité.

- **Hypothèse :**

L'adoption d'une solution VoIP sécurisée permettra d'améliorer significativement la sécurité, l'intégration des systèmes et la qualité du service dans les centres d'appel, tout en réduisant les coûts de maintenance et d'exploitation.

- **Perspective Future :**

Bien que notre étude se concentre sur la mise en place d'une solution VoIP sécurisée, nous reconnaissons l'importance d'explorer d'autres solutions et technologies à l'avenir. Notre recherche continuera afin d'identifier et d'intégrer des approches innovantes pour relever les défis des centres d'appel, assurant ainsi une communication client optimale et sécurisée sur le long terme.

4. Choix de la solution voip

Pour moderniser et sécuriser le centre d'appel Candle Call, nous avons envisagé de passer à une solution VoIP. Cette technologie offre flexibilité, réduction des coûts, et sécurité accrue. Avant de choisir une solution spécifique, il est crucial de comprendre les besoins du centre d'appel et d'évaluer les options disponibles. Cette section examine les critères de sélection, les

fonctionnalités recherchées et les étapes nécessaires pour une transition réussie vers la VoIP, afin de choisir la meilleure technologie pour améliorer les opérations et la sécurité du centre d'appel.

4.1 Etude des technologies de virtualisation

La virtualisation est une technologie qui permet à un seul ordinateur de faire fonctionner plusieurs systèmes d'exploitation simultanément, en créant des machines virtuelles. Ces machines virtuelles permettent de simuler plusieurs ordinateurs physiques au sein d'un même système. La virtualisation couvre diverses ressources informatiques, telles que les applications, les serveurs, le stockage et les réseaux. Pour garantir une virtualisation efficace, il est crucial de choisir un logiciel de virtualisation performant.

Avant de sélectionner la solution à utiliser pour notre projet, nous allons effectuer une étude comparative des différentes solutions de virtualisation disponibles sur le marché :

Critère	**VMware**	**Citrix**	**Microsoft**	**Oracle**
Solution principale	vSphere	Citrix Hypervisor (anciennement XenServer)	R2 avec Hyper-V	Oracle VM
Caractéristiques	VMware est le leader du marché de la virtualisation côté serveur avec ses produits phares tels que vSphere et vCenter. Il propose une large gamme de solutions de virtualisation	Citrix propose une solution de virtualisation côté serveur avec son produit phare, Citrix Hypervisor. Il offre également des solutions de virtualisation des postes de	Microsoft propose une solution de virtualisation côté serveur avec son produit phare, Hyper-V. Il est intégré à Windows Server et offre également des solutions de	Oracle propose une solution de virtualisation côté serveur avec son produit phare, Oracle VM. Il offre également des solutions de virtualisation des postes de travail et des applications.

	pour les entreprises de toutes tailles.	travail et des applications.	virtualisation des postes de travail et des applications	
Prix	Varie selon les versions et les fonctionnalités	Les prix sont compétitifs par rapport à VMware, mais peuvent varier en fonction des fonctionnalités et des besoins spécifiques.	Moins cher, avec une version gratuite disponible	Gratuit, avec des options payantes pour extensions

Tableau 3.2 : une étude comparative de la différente technologie de virtualisation disponibles sur le marché.

Ce tableau comparatif met en évidence les principales différences entre les acteurs majeurs de la virtualisation côté serveurs. Il est important de noter que chaque solution à ses forces et ses faiblesses, et le choix dépendra des besoins spécifiques de notre projet, en ce qui concerne la mise en place d'une solution VoIP sécurisée, il est important de choisir une solution de virtualisation qui offre des fonctionnalités de sécurité intégrées et une bonne gestion de la sécurité.

4.2 Choix de la technologie de virtualisation

VMware est le choix populaires pour les entreprises qui ont besoin d'une solution de virtualisation côté serveur hautement sécurisée.

4.2.1 Présentation de VMware Workstation

4.2.1.1 Définition

VMware Workstation est une plateforme de virtualisation de bureau qui facilite la création et la gestion de machines virtuelles sur un seul ordinateur physique. Cette solution de virtualisation permet d'installer et de tester divers systèmes d'exploitation et applications dans

un environnement isolé et sécurisé. Ce qui le rend parfait pour mettre en place une solution de VoIP sécurisée dans le cadre de notre mémoire de fin d'étude.

4.2.1.2 Principales Caractéristiques

- **Virtualisation :** Permet de créer des machines virtuelles (VM) avec différents systèmes d'exploitation.
- **Virtualisation du Matériel :** Virtualise les composants matériels, permettant aux VM d'accéder à ces ressources comme si elles étaient physiques.
- **Support Multi-OS :** Prend en charge une variété de systèmes d'exploitation, offrant la possibilité d'exécuter plusieurs OS sur une seule machine.
- **Instantanés et Clonage :** Permet de prendre des instantanés des VM et de cloner les VM, facilitant ainsi la gestion et la sauvegarde des configurations.
- **Réseau :** Offre un éditeur de réseau virtuel intégré pour configurer les paramètres réseau de chaque VM.
- **Sécurité :** Propose des fonctionnalités de sécurité telles que le chiffrement et le démarrage sécurisé, assurant la sécurité et l'intégrité des VM.

4.2.1.3 Pourquoi Utiliser VMware Workstation pour l'Implémentation de la Solution VoIP ?

- **Flexibilité :** Facilite la création et le déploiement de différentes solutions VoIP en offrant des environnements isolés pour chaque configuration.
- **Isolation :** Offre un haut niveau d'isolation entre les VM, garantissant la sécurité et la fiabilité des environnements de test.
- **Adaptabilité :** Permet une adaptation facile des ressources allouées à chaque VM aux exigences changeantes de la solution VoIP.
- **Coût-Effectivité :** Élimine le besoin de plusieurs machines physiques, réduisant ainsi les coûts matériels et en faisant une solution économique pour l'implémentation de la solution VoIP.

4.2.1.4 Avantages de l'Utilisation de VMware Workstation pour notre projet

- **Déploiement Facile :** Simplifie le déploiement et les tests de solutions VoIP, permettant de se concentrer sur la conception et les tests.
- **Sécurité Améliorée :** Fournit un environnement sécurisé pour tester et déployer la solution VoIP, assurant la sécurité et la fiabilité.
- **Flexibilité et évolutivité :** Facilite l'adaptation aux exigences changeantes et permet d'évoluer selon les besoins, offrant une plateforme idéale pour la réalisation du mémoire.

4.3 Étude des différents serveurs de communication Open Source

La VoIP a véritablement transformé nos interactions à distance dans le monde numérique contemporain. Les serveurs de VoIP ne se contentent pas seulement de permettre des appels téléphoniques via Internet à moindre coût, mais ils offrent également une panoplie de fonctionnalités avancées comme la messagerie vocale, les conférences, et l'intégration avec d'autres services de communication. Les solutions open source dans ce domaine sont particulièrement plébiscitées pour leur flexibilité, leur coût abordable, et la communauté active qui les soutient.

Cette étude met en lumière les serveurs de VoIP open source les plus prisés et analyse leurs caractéristiques, avantages, et inconvénients afin de nous aider à sélectionner le meilleur pour notre projet de mémoire de fin d'études.

Voici une présentation des différents serveurs de communication open source dans un tableau pour offrir un aperçu succinct des caractéristiques principales de chaque IPBX open source, permettant une comparaison rapide pour identifier celui qui correspond le mieux à nos besoins spécifiques :

Critère	**Issabel**	**FreePBX**	**Xivo**
Éditeur	Issabel.com. Mexique	Sangoma (ex-Digium). USA	Avencall (anciennement Proformatique). France
Caractéristique	Bien adapté pour les utilisateurs cherchant une solution tout-en-un incluant la téléphonie, la	Très populaire pour les petites et moyennes entreprises grâce à sa flexibilité et à son	Convient aux utilisateurs cherchant une solution basée sur Debian avec une interface de gestion

	messagerie et le CRM. L'utilisation d'une version plus ancienne de FreePBX peut poser des problèmes de compatibilité avec les nouvelles fonctionnalités.	large écosystème de modules. Cependant, la gestion des modules payants peut être compliquée pour les débutants.	unique. La communauté active depuis 2009 offre un support et des mises à jour régulières, rendant Xivo une option solide pour ceux qui préfèrent Debian à CentOS.
Commentaire	Fork d'Elastix offrant un IPBX basé sur Asterisk, ainsi que des solutions de messagerie et CRM. Le module de provisioning est inclus en standard et open source. Basé sur une ancienne version de FreePBX (2.11) maintenue par Issabel.	Distribution phare d'Asterisk. Modulaire avec de nombreux modules, certains open source, d'autres propriétaires. Attention aux modules payants par défaut. Le module de provisioning open source n'est pas bien maintenu ; la solution payante (EndPoint Manager) est plus complète.	Projet initialement non communautaire devenu open source en 2009. Utilise sa propre interface de configuration Web au lieu de FreePBX. Basé sur Debian, ce qui est unique parmi les distributions Asterisk.

Tableau 3.3 : comparaison des solutions ipbx Open Source les plus connu

4.4 Choix de la solution IPBX open source

Issabel est une solution IPBX open source riche en fonctionnalités, sécurisée, et soutenue par une communauté active, ce qui en fait un excellent choix pour notre projet centré sur la mise en place d'une solution VoIP sécurisée.

4.4.1 Présentation d'Issabel

4.4.1.1 Définition

Issabel est une plateforme de communication open source basée sur Asterisk, qui intègre des fonctionnalités d'IPBX, de messagerie unifiée et de CRM (Customer Relationship Management). C'est un fork d'Elastix, une autre solution IPBX, et est maintenu par **Issabel.com**, une société basée au Mexique. Issabel utilise un fork de FreePBX 2.11 comme interface de gestion et fonctionne sur le système d'exploitation CentOS.

4.4.1.2 Pourquoi choisir Issabel ?

1. **Nature Open source :**

   - Entièrement gratuit et open source, ce qui permet aux utilisateurs de personnaliser et de modifier le système selon leurs besoins sans frais de licence.
   - permet aux étudiants de plonger dans le code source pour mieux comprendre le fonctionnement interne d'un IPBX, offrant une transparence totale.

2. **Richesse Fonctionnelle :**

   - Issabel intègre de nombreuses fonctionnalités comme la messagerie unifiée, la gestion des appels, la conférence, les files d'attente, et bien plus encore.
   - Supporte divers protocoles et peut être étendu avec des modules supplémentaires pour répondre à des besoins spécifiques.

3. **Expérience Pratique :**

   - Utiliser Issabel (comme notre cas) dans un projet de fin d'études permet aux étudiants d'acquérir une expérience pratique précieuse dans la mise en place et la gestion d'un système VoIP.
   - La possibilité de configurer et de tester divers scénarios d'utilisation réelle (entreprises, centres d'appels, etc.) enrichit la pertinence et l'applicabilité du projet.

4. **Communauté Active et Documentation :**

   - Une large communauté d'utilisateurs et de développeurs permet de bénéficier de support, de conseils et de solutions à des problèmes communs.
   - La disponibilité de documentation détaillée et de tutoriels facilite l'apprentissage et la mise en œuvre de la solution.

5. **Sécurité :**

   - Issabel inclut des fonctionnalités de sécurité comme le cryptage des appels (SRTP), la sécurisation des connexions (TLS), et des outils pour la gestion des pare-feu et des politiques de sécurité.
   - Des mises à jour régulières et des patches de sécurité sont disponibles pour protéger le système contre les vulnérabilités.

6. **Interopérabilité et Intégration :**

- Issabel peut être intégré avec d'autres systèmes et applications, permettant ainsi une solution VoIP complète et multifonctionnelle.
- Supporte une large gamme de matériels (téléphones IP, passerelles, etc.), ce qui permet une flexibilité accrue dans le choix des équipements.

7. **Exemples et Références :**

- Il existe de nombreux exemples de mise en place réussie d'Issabel dans diverses organisations, ce qui peut servir de référence et d'inspiration pour notre projet.

5. Installation et configuration d'Issabel PBX

5.1 Les étapes d'installation d'Issabel

- Avant de procéder à l'installation d'Issabel PBX, il est indispensable d'obtenir l'image disque ISO du logiciel, en se rendant sur le site officiel **https://www.issabel.org/** et en téléchargeant la dernière version stable disponible et l'importer dans le data store de VMware Workstation Pro.
- On crée une nouvelle machine virtuelle dans VMware Workstation Pro on cliquant sur ''Create a New Virtual Machine''.

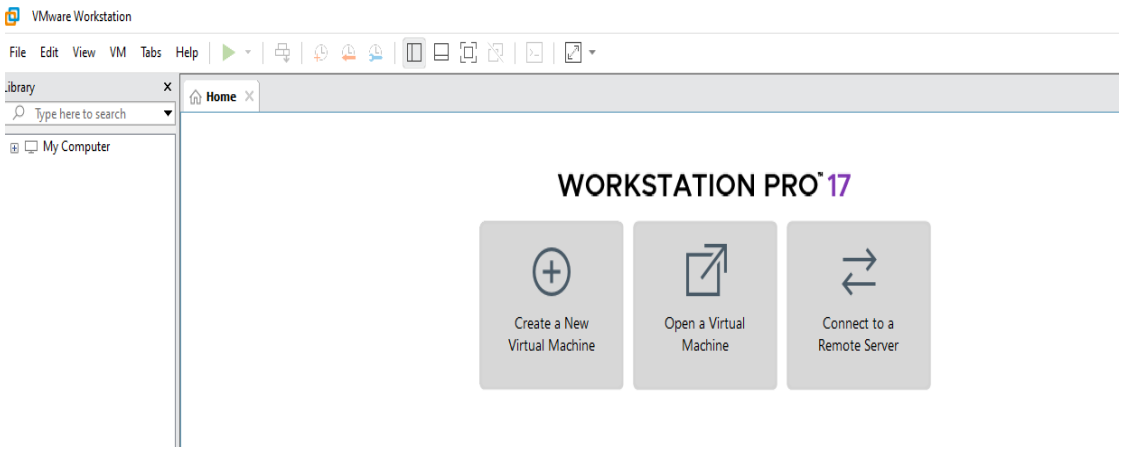


Figure 3.2 : Page d'accueil de VMware Workstation

- On choisit l'option Installer disc image file (ISO) et on sélectionne l'image ISO téléchargée d'Issabel.

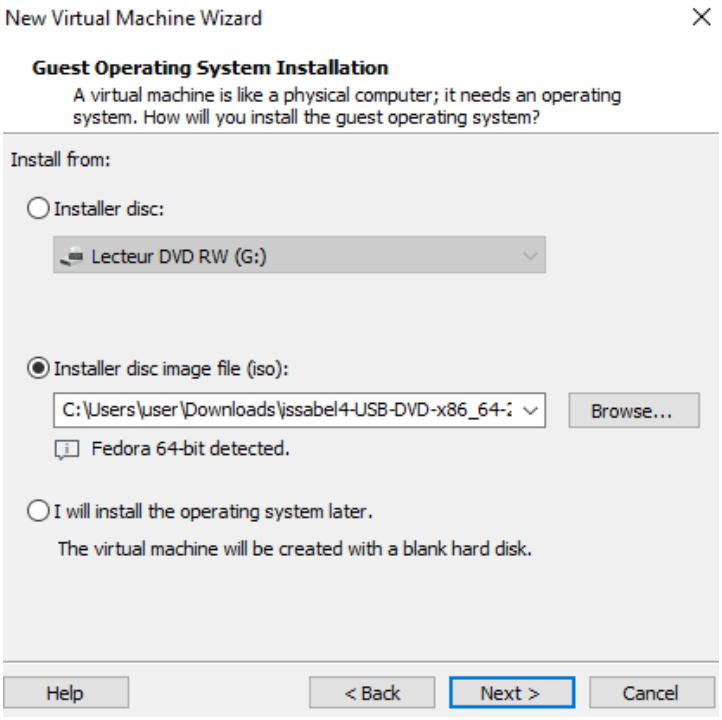


Figure 3.3 : Pré-installation au système d'exploitation

- On choisit linux comme système d'exploitation et centOS 7 comme version du système.

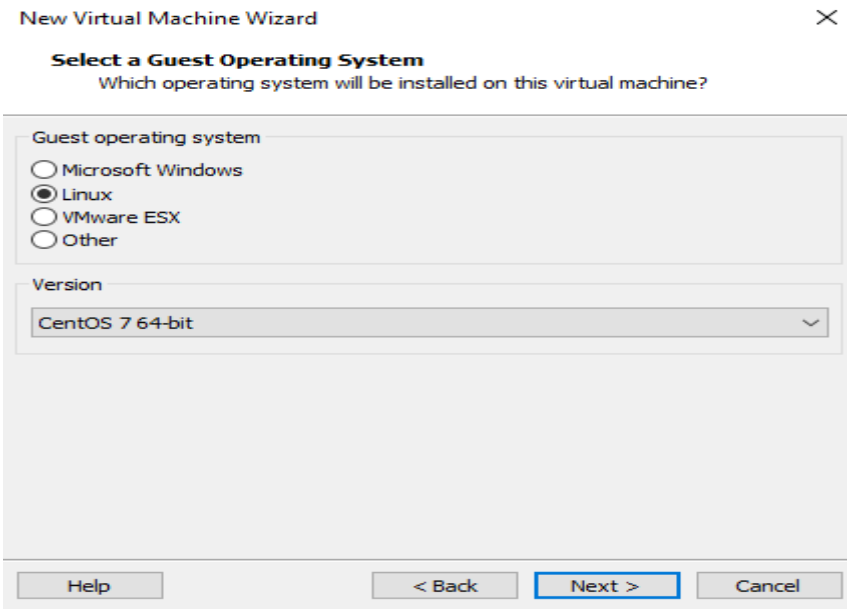


Figure 3.4 : Le choix et la version du système d'exploitation

- On donne Issabel_PBX comme nom pour notre machine virtuelle.

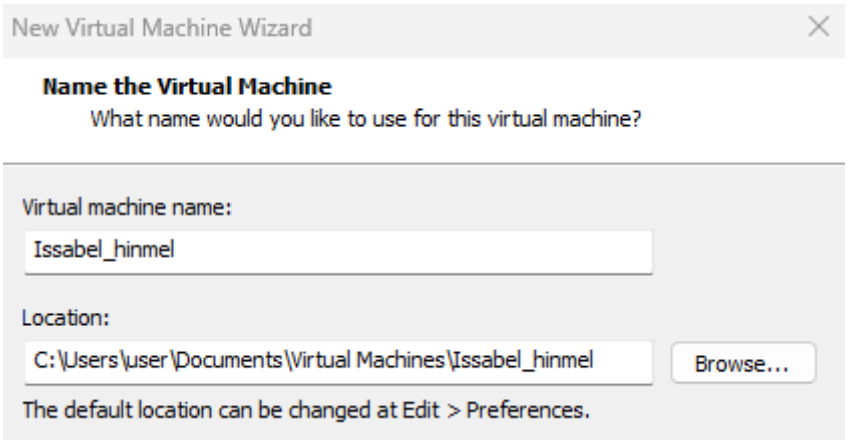


Figure 3.5 : Le nom de la machine virtuelle et son emplacement

- À partir de là, VMware Workstation nous guide à travers les différentes étapes de personnalisation des paramètres matériels de la machine virtuelle. On peut ajuster la quantité de mémoire vive allouée, le nombre de processeurs virtuels, la taille du disque dur virtuel, ainsi que d'autres périphériques. Une fois ces réglages effectués on clique sur ‘’Finish’’ pour démarrer l'installation.

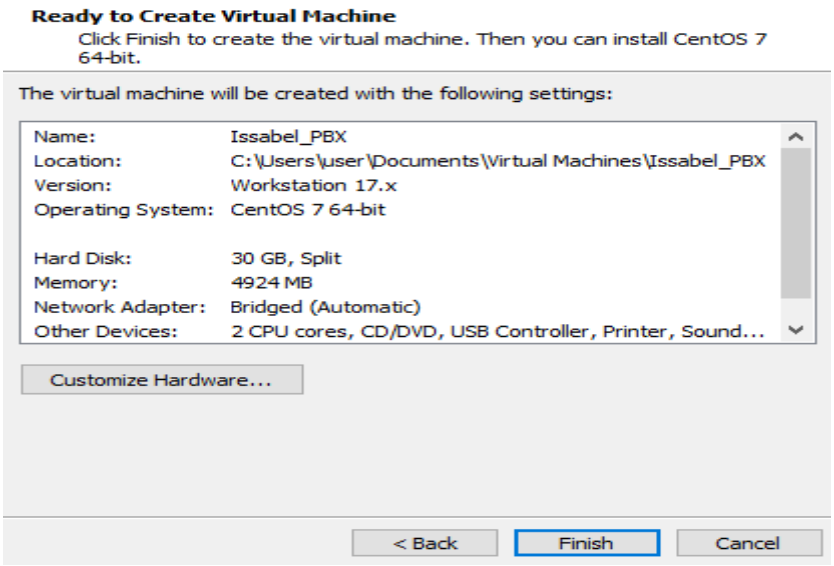


Figure 3.6 : Les paramètres matériels de la machine virtuelle

- Nous procéderons maintenant au lancement de notre machine virtuel, en vue d'initier le processus d'installation du système Issabel PBX. Après le démarrage de la machine virtuelle, nous sélectionnerons l'option "Install" du menu d'installation. Pour confirmer notre choix, nous appuierons sur la touche Entrée.

Figure 3.7 : Ecran d'accueil de l'installation d'Issabel

- Après avoir terminé l'installation, notre machine effectuera un redémarrage automatique. Une fois redémarrée, on se connecte en utilisant le nom d'utilisateur (root) et le mot de passe administrateur pour accéder à notre machine.

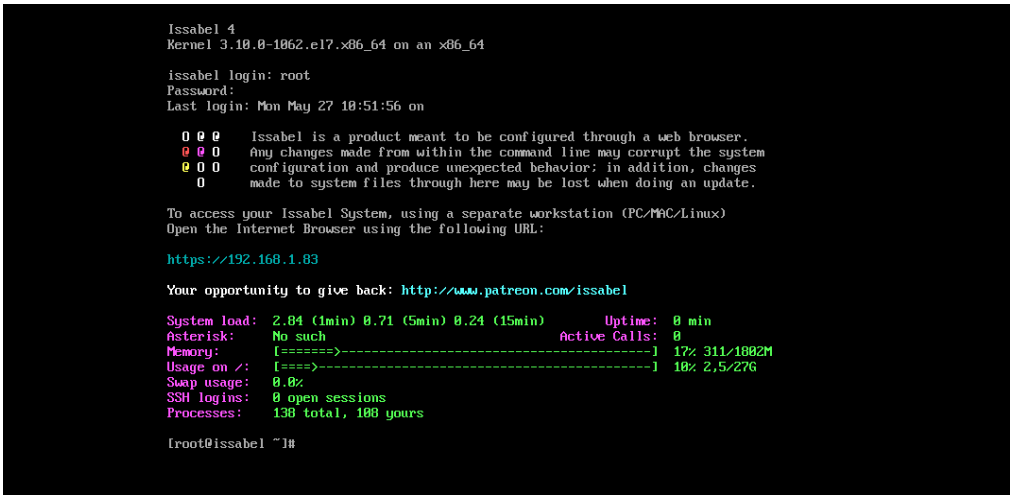


Figure 3.8 : L'interface de configuration D'issabel

- Nous allons maintenant ouvrir un navigateur web et saisir l'adresse IP de notre serveur Issabel dans la barre d'URL, http://192.168.1.83, afin d'accéder à l'interface web d'administration d'Issabel.

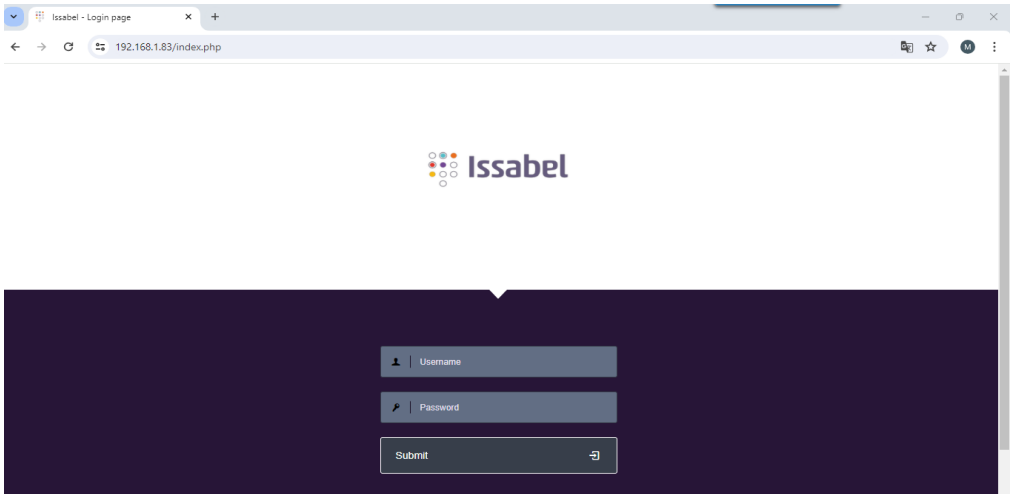


Figure 3.9 : Page de connexion à l'interface web d'Issabel

- Une fois les informations d'identification validées, on accède au tableau de bord principal d'Issabel qui nous offre un aperçu complet du système, affichant des détails tels que l'utilisation du processeur (CPU) et de la mémoire vive (RAM), ainsi que l'état des services intégrés comme la téléphonie, la messagerie instantanée, le fax, le service mail, les bases de données et les services web. On a également accès aux différents outils d'administration. Ceux-ci nous offriront un contrôle complet sur la configuration, la personnalisation et le dépannage de notre plateforme Issabel.

5.2 Configuration d'Issabel PBX

5.2.1 Création des extensions

- Pour commencer à passer des appels, nous allons attribuer des "extensions" (identifiants qui définissent l'appareil utilisé par un numéro) à nos utilisateurs. Pour ce faire, il est nécessaire de se rendre dans PBX > Configuration PBX > Ajouter une nouvelle extension.

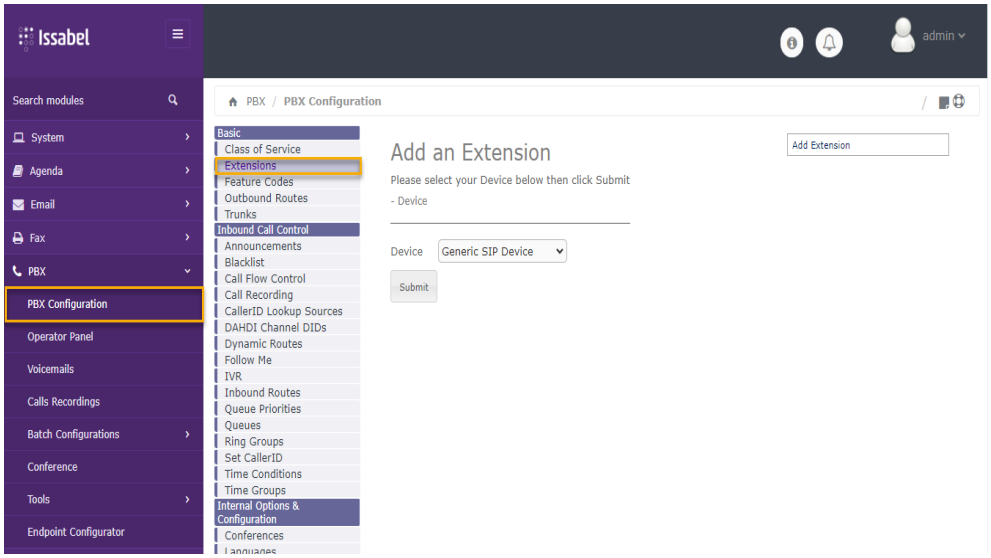


Figure 3.10 : Création des extensions

- Nous allons maintenant définir l'extension pour chaque utilisateur, en spécifiant user extension (numéro unique) et display name (nom associé à l'extension).

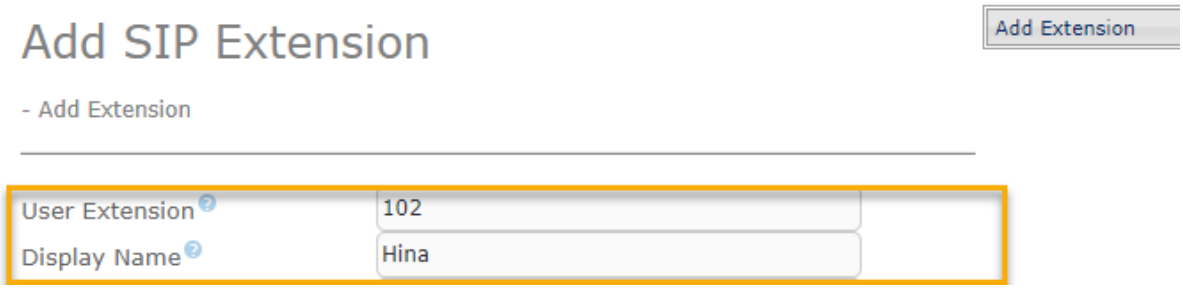


Figure 3.11: L'ajout de l'extension et son nom

- Dans cette étape, nous procédons à la configuration des fonctionnalités supplémentaire de notre solution VoIP. Nous allons définir un ‘’outbound CID’’ qui permet de définir l'identifiant de l'appelant pour les appels sortants, ici nommé "candle call". Et on laisse ‘’tr’’ pour Asterisk Dial Options pour inclure les options de connexion et de transfert.

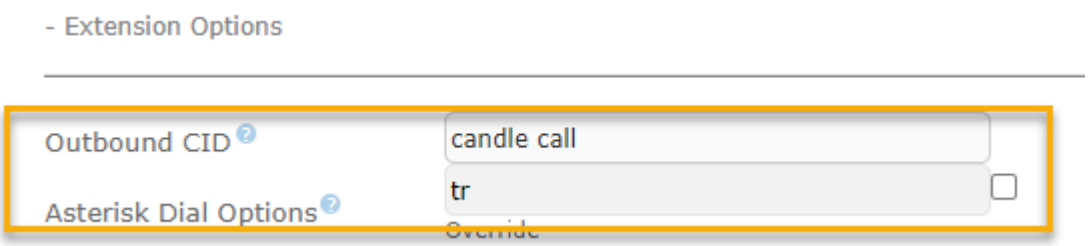


Figure 3.12 : L'identifiant de l'appelant sortant et l'Option de numérotation Asterisk

- Et maintenant nous allons définir un temps de 20s pour ''Ring Time'' (Durée avant qu'un appel soit non répondu), et 25s pour 'Call Forward Ring Time' (Durée avant qu'un appel soit transféré).

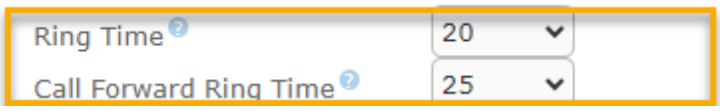


Figure 3.13 : choix de temps de sonnerie et le temps de passage aux autres extensions

- Cette fois on va fixer Outbound Concurrency Limit (nombre maximal d'appels sortants autorisés à être actifs simultanément) à 5, on active l'option d'appel en attente (Call Waiting) et on désactive Internal Auto Answer pour qu'il ne réponde pas automatiquement aux appels internes.

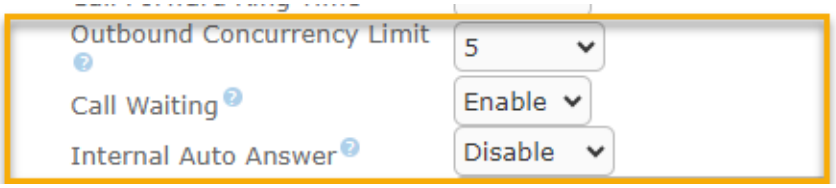


Figure 3.14 : Configuration des Limites de Concurrence des Appels Sortants, de l'Attente et de la Réponse Automatique Interne

- Dorénavant on choisit ''screen caller : Memory'' pour ''Le call screening'' qui permet de vérifier les appels entrants avant de les accepter ou de les rejeter, et on désactive le ''pinless dialing'' pour ne pas permettre de passer des appels sans saisir de code PIN.

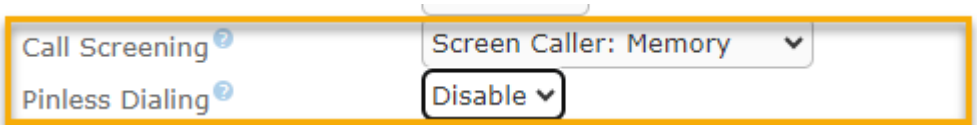


Figure 3.15 : Paramètres d'écran d'appel et de numérotation sans code PIN.

- A présent, on attribue le numéro 114 pour ''Emergency CID'' qui sera affiché lors d'un appel d'urgence et enfin on sélectionne use state pour la détection de l'état des files d'attente (queues) dans le système de gestion des appels.

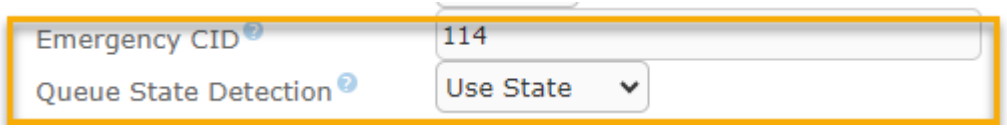


Figure 3.16 : Configuration de l'identifiant d'appel d'urgence et détection de l'état de la file d'attente.

- Le mot de passe doit être spécifié dans le champ ‘’secret’’. ‘’Dtmfmode ‘’ est utilisé pour la signalisation des touches sur un téléphone. Pour permettre l'émission d'appels, il est également nécessaire d'activer le NAT.

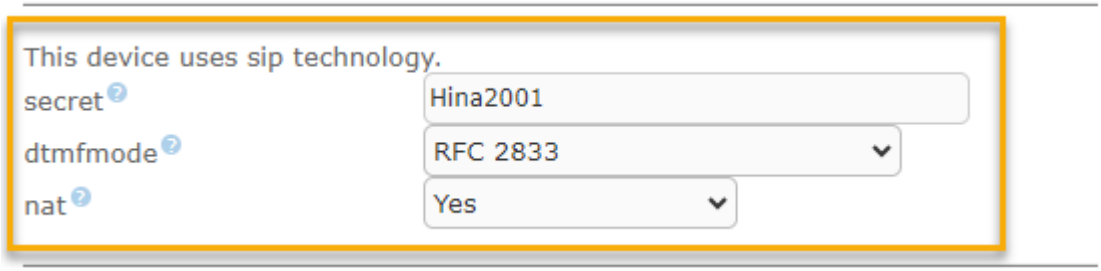


Figure 3.17 : Paramètres SIP pour un dispositif.

- Voici la liste des extensions qu'on a créées.

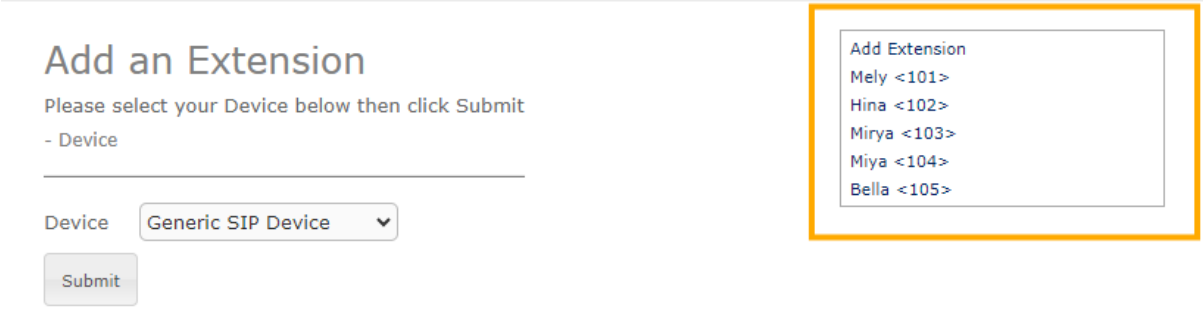


Figure 3.18 : Les extensions créées.

5.2.2 Création des utilisateurs

- La prochaine étape consiste à associer les comptes utilisateurs avec les extensions correspondantes. Pour ce faire, nous devons initialement créer ces utilisateurs en accédant à la section ‘’Users’’ et en choisissant l'option de création d'un nouvel utilisateur.

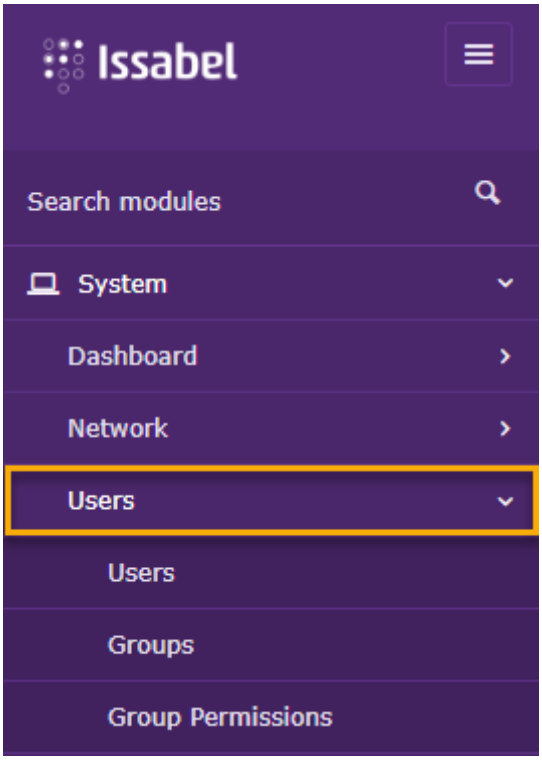


Figure 3.19 : Menu de gestion des utilisateurs dans l'interface Issabel.

- Il est à noter que le système inclut par défaut le compte ‘'admin’', qui est déjà listé parmi les utilisateurs existants.

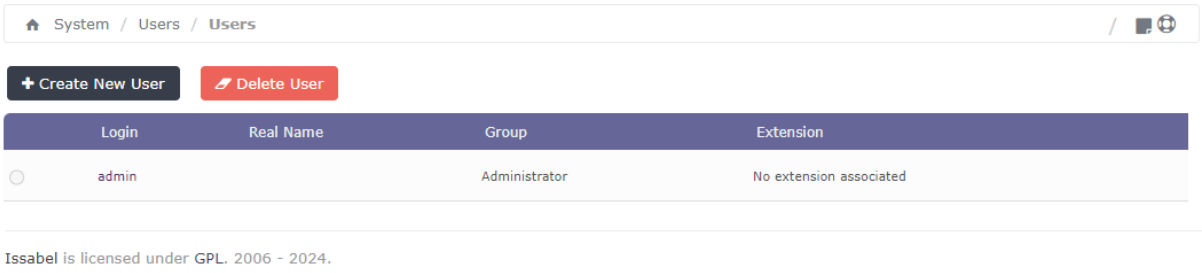


Figure 3.20 : tableau de liste des utilisateurs.

- Pour créer un nouvel utilisateur, on doit définir les informations suivantes : l'identifiant de connexion (Login), le nom complet (Name), le mot de passe, le groupe auquel appartient l'utilisateur et l'extension qui lui sera associée. Une fois toutes ces informations renseignées, on clique sur "Save" pour enregistrer le nouveau compte utilisateur.

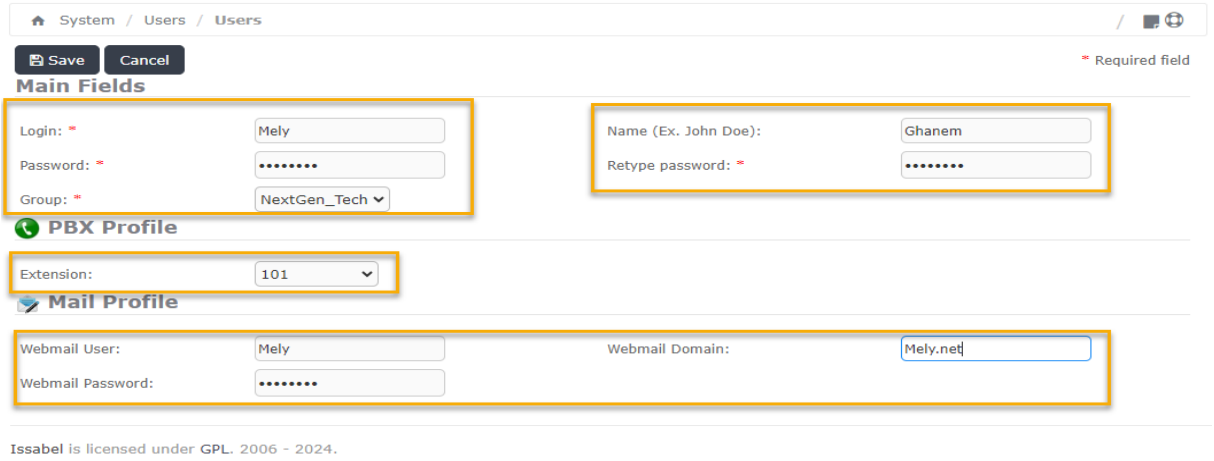


Figure 3.21 : Création d'un nouvel utilisateur avec les détails de connexion.

- Après avoir créé les comptes utilisateurs souhaités, nous disposerons d'une liste complète d'utilisateurs liés à leurs extensions respectives.

Figure 3.22 : Liste des utilisateurs avec leurs détails de connexion.

5.2.3 Gestion du Transfert et du Suivi d'Appels

- Pour configurer une redirection d'appels, on accède à la section PBX > PBX Configuration > Follow Me (dans Inbound Call Control). Ensuite, on peut choisir une extension spécifique à configurer telle que 101.
- On choisit un temps initial de 20s pendant lequel l'extension principale sonne avant de suivre la "Liste de Suivi".

- On sélectionne '' Hunt'' comme stratégie d'appel ("Ring Strategy") cela signifie que les extensions seront appelées de manière séquentielle. Par exemple, si l'extension 101 ne répond pas, l'appel sera transféré vers l'extension 102.
- ''Ring Time'' est le temps pendant lequel chaque extension de la liste va sonner avant de passer à la suivante. Ici, il est réglé à 30 secondes.
- ''Follow-Me List '' C'est la liste des extensions vers lesquelles les appels seront redirigés (dans notre cas on a les extensions 102, 103, 104, 105).

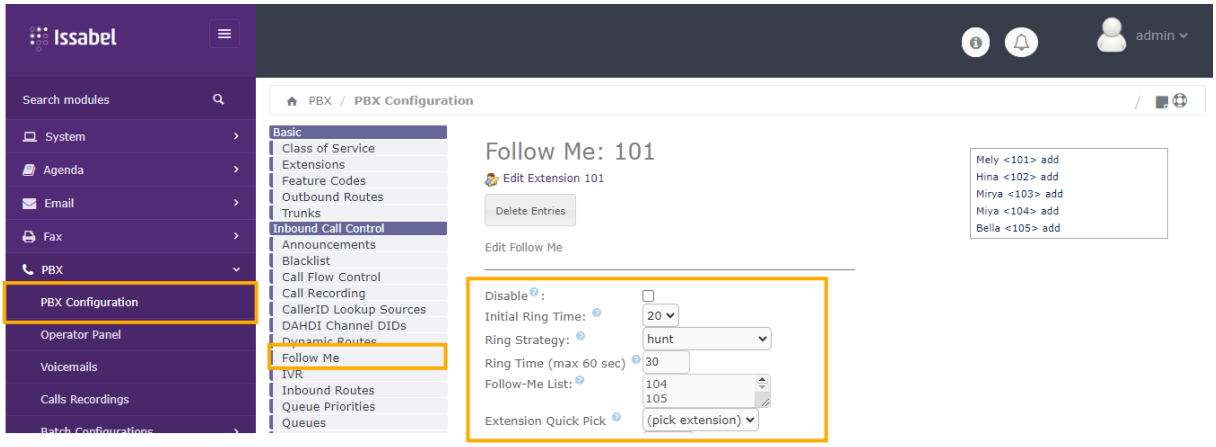


Figure 3.23 : Configuration de l'option "Follow Me" pour l'extension 101.

- Pour mettre en place une redirection d'appels, Il est important de spécifier l'action à réaliser si aucune des extensions ne répond. Pour notre scenario, nous choisirons de terminer l'appel puis de raccrocher.

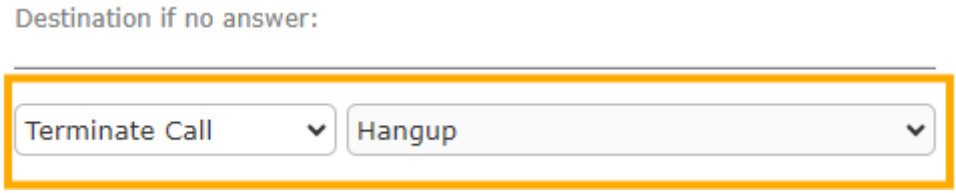


Figure 3.24 : Paramètre de destination en cas de non-réponse.

5.2.4 Gestion des Groupes d'Appels

Il faut se rendre dans le menu "PBX Configuration" puis sélectionner l'option "Ring Groups" sous "Inbound Call Control". Ensuite, on clique sur "Add Ring Group" pour créer un nouveau groupe. On doit alors renseigner les champs suivants :

- On attribue un numéro de groupe (Ring group number), dans ce cas le 600, et un nom qui décrit le groupe qui sera "SupportClient".
- on sélectionne ‘’ringall’’ comme Stratégie d'appel pour que toutes les extensions sonnent en même temps jusqu'à ce qu'un membre décroche, et une période (Ring time) de 30s pendant lequel les extensions du groupe vont sonner.
- On ajoute les numéros d'extensions qui doivent faire partie du groupe, dans ce cas 101 et 102.
- On sélectionne ‘’None’’ pour ‘’Announcement’’ pour qu'aucun message audio ne soit joué avant que les extensions ne commencent à sonner.
- On sélectionne ‘’Ring’’ pour ‘’Play Music On Hold’’ pour que les appelants entendent une sonnerie pendant l'attente.

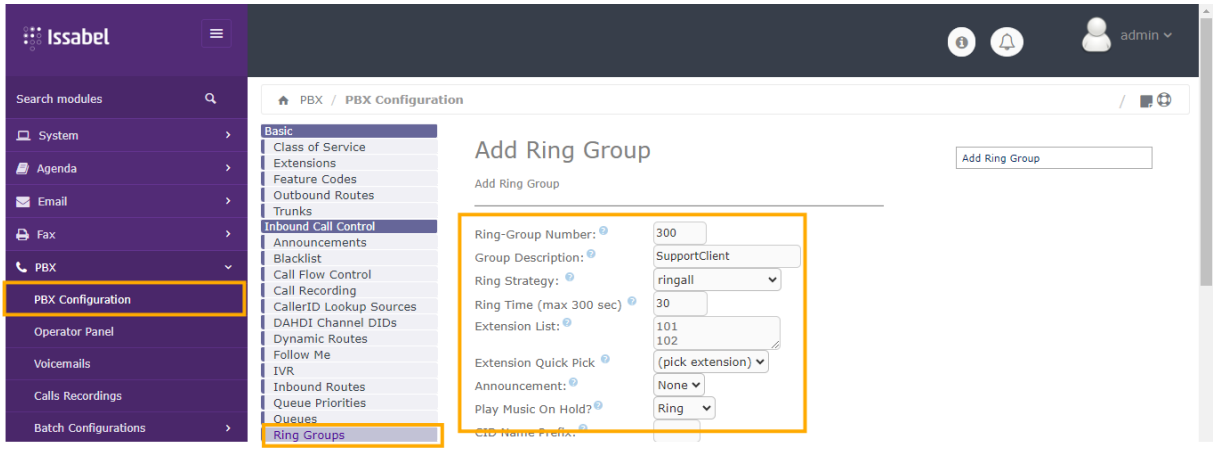


Figure 3.25 : Ajout d'un groupe de sonnerie.

- Et pour finir, On sélectionne ‘’Hangup’’ pour ‘’Terminate Call’’ pour que l'appel soit raccroché si personne ne répond.

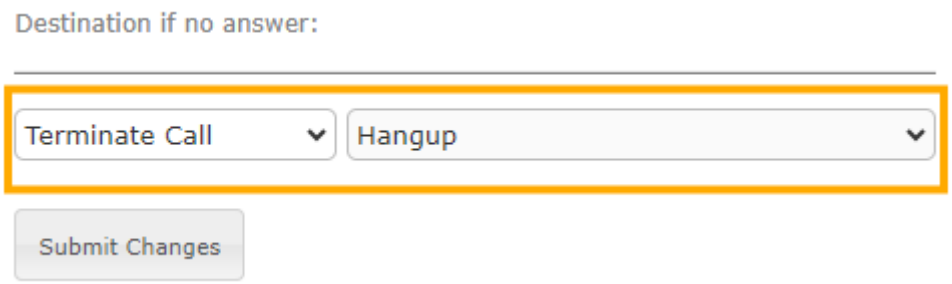


Figure 3.26 : Paramètre de destination en cas de non-réponse.

5.2.5 Configuration de Linphone

- Pour commencer, il est nécessaire de télécharger Linphone depuis son site officiel, accessible à l'adresse https://www.linphone.org/download. Une fois téléchargé, nous avons configuré Linphone sur notre PC et smartphone. Lors du premier lancement, Linphone nous invite à créer un compte. Nous sélectionnons l'option ‘’utiliser un compte SIP’’ pour procéder.

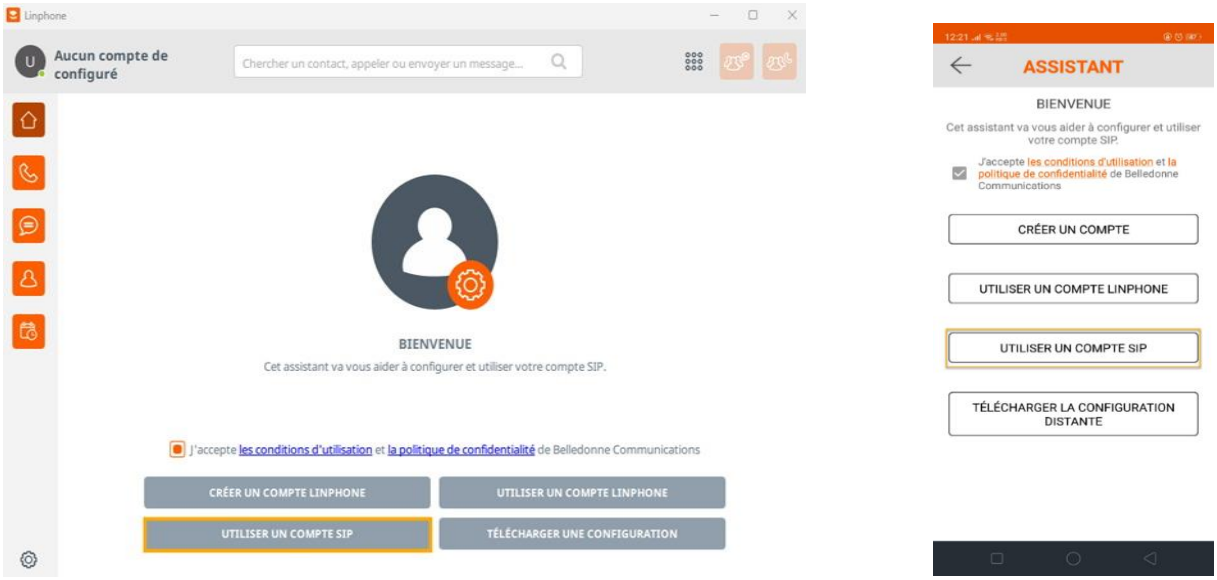


Figure 3.27 : Interface de de l'application Linphone sur ordinateur et smatphone.

- Ensuite, nous allons saisir les informations nécessaires pour configurer notre compte sip, et on sélectionne udp comme protocole de transport, puis on clique sur ‘terminer’ pour valider notre compte.

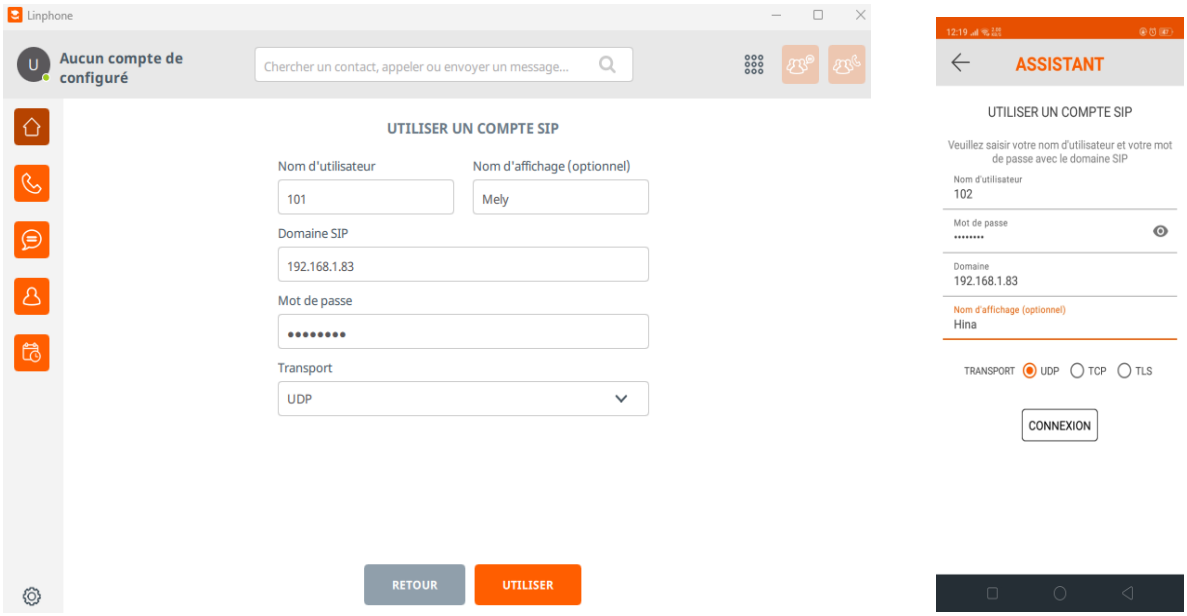


Figure 3.28 : Configuration des comptes SIP sur PC et smartphone.

- Une fois validé, notre compte sera créé et nous pourrons effectuer et recevoir des appels.

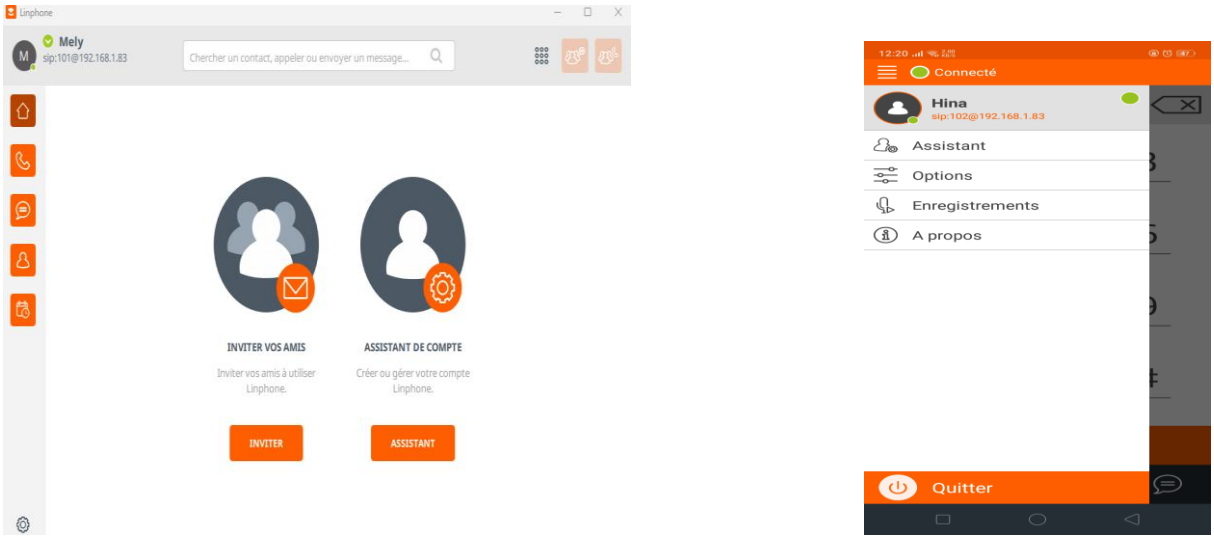


Figure 3.29 : la connexion sur pc et smartphone

- Désormais, nous allons initier un appel depuis l'utilisateur 101 (Mely) vers l'utilisateur 102 (Hina).

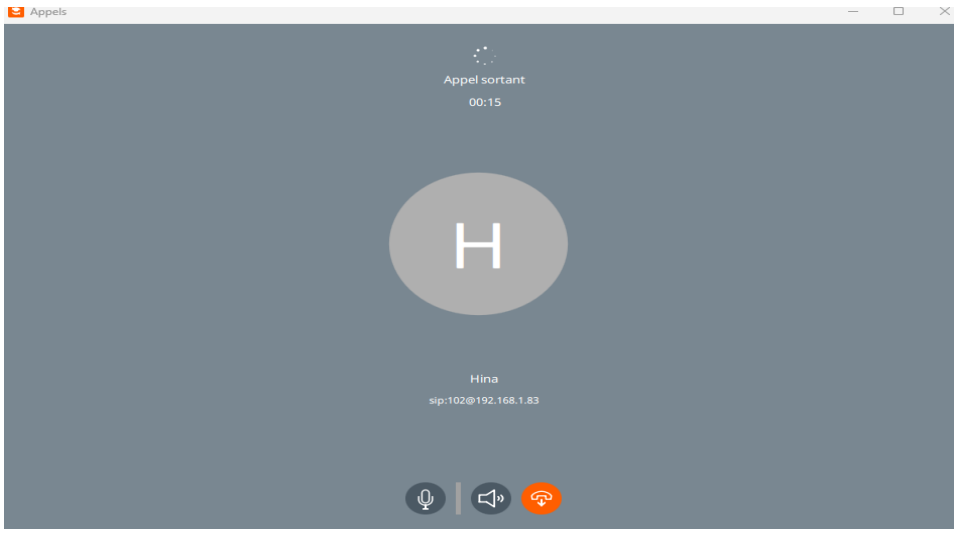


Figure 3.30 : Lancement d'un appel.

- Et l'utilisateur 102 décroche.

Figure 3.31 : Prise d'un appel entrant.

6. Conclusion

Dans ce chapitre, nous avons étudié l'infrastructure existante du centre d'appel, identifié ses faiblesses et défini les besoins pour une solution VoIP sécurisée. Nous avons choisi VMware Workstation pour la virtualisation et Issabel pour la gestion des communications, en raison de leurs fonctionnalités et fiabilité. Ensuite, nous avons installé et configuré la solution VoIP, incluant le softphone Linphone pour améliorer la flexibilité des agents. Ces actions établissent une base solide pour une communication efficace et sécurisée. La prochaine étape est de mettre en place les mécanismes de sécurité pour protéger et garantir l'intégrité des communications VoIP.

Chapitre 04 :

Sécurisation de la solution mise en place

1. Introduction

La sécurité est un pilier fondamental pour assurer la fiabilité de notre solution de communication VoIP. Dans ce chapitre, nous nous concentrerons sur quatre stratégies essentielles que nous avons mises en œuvre pour renforcer cette sécurité : la configuration de fail2ban, l'implémentation d'un pare-feu, le chiffrement TLS, et le protocole SRTP. Ces mesures visent à protéger l'infrastructure contre les accès non autorisés, à sécuriser les communications et à garantir l'intégrité des données échangées.

2. Pourquoi est-il crucial de sécuriser les communications VoIP ?

Pour comprendre l'importance de sécuriser les communications VoIP, nous allons utiliser Wireshark pour démontrer à quel point ces communications peuvent être vulnérables lorsqu'elles ne sont pas protégées.

2.1 Définition de Wireshark

Wireshark est un logiciel d'analyse de protocole réseau open-source. Il permet de capturer, d'analyser et de visualiser le trafic réseau en temps réel. Wireshark offre des fonctionnalités avancées de filtrage, d'analyse détaillée et de génération de statistiques sur le trafic réseau.

2.2 Surveillance et analyse de réseau avec Wireshark

Pour commencer, il faudra lancer Wireshark et sélectionner l'interface réseau appropriée pour démarrer la capture du trafic.

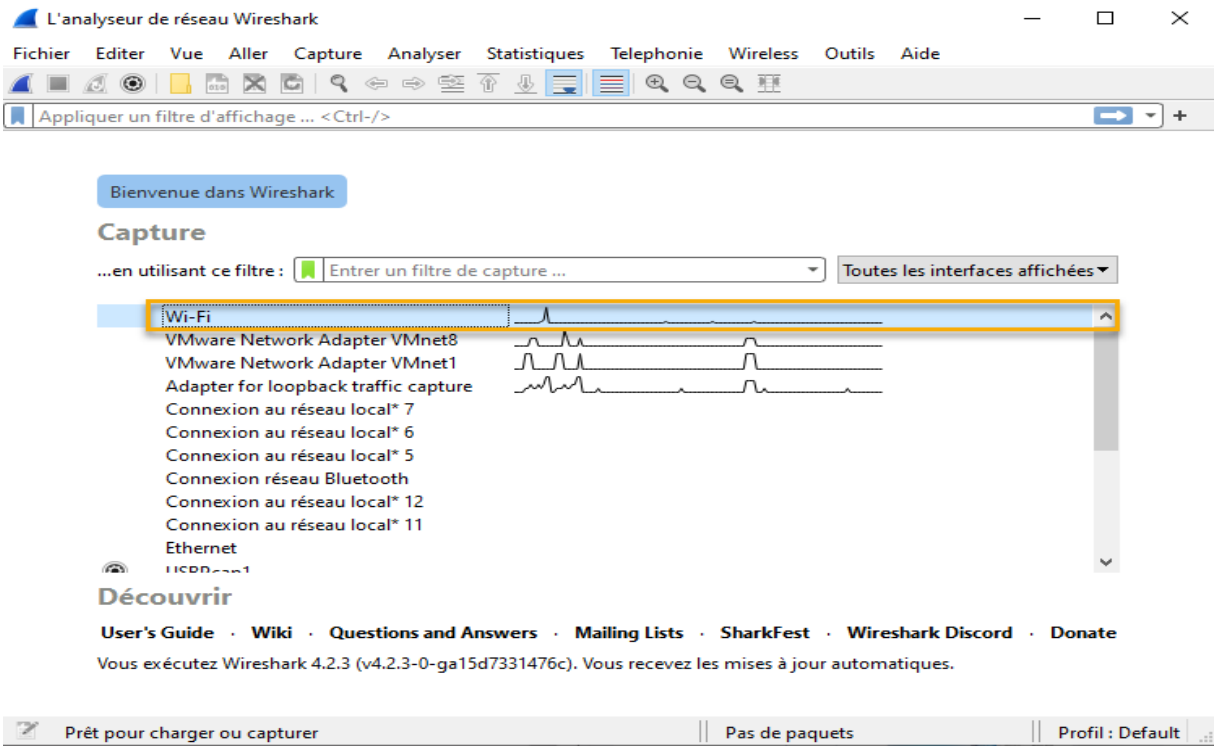


Figure 4.1 : Sélection de l'interface réseau

Et maintenant, nous lancerons la capture de paquets. Par défaut, Wireshark enregistre toutes les données circulant sur cette interface, capturant ainsi tous les protocoles de communication.

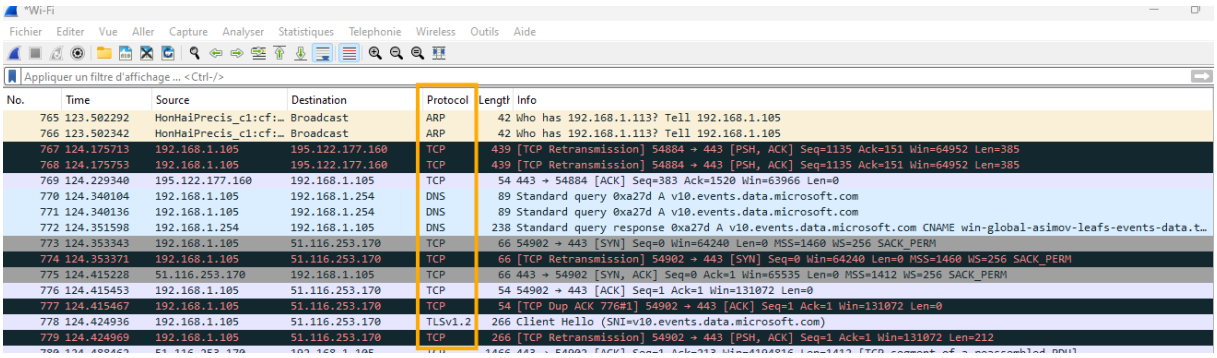


Figure 4.2 : Capture des paquets par Whireshark

Après avoir effectué un appel VoIP, on a appliqué un filtre sur le protocole SIP pour étudier les échanges de signalisation.

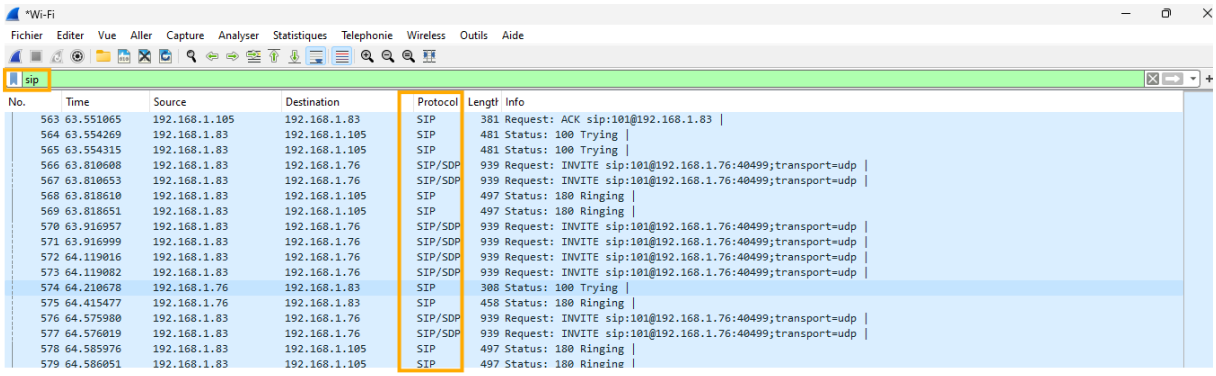


Figure 4.3 : Application d'un filtre sur le protocole SIP

Puis, sur le protocole RTP pour inspecter les flux audio.

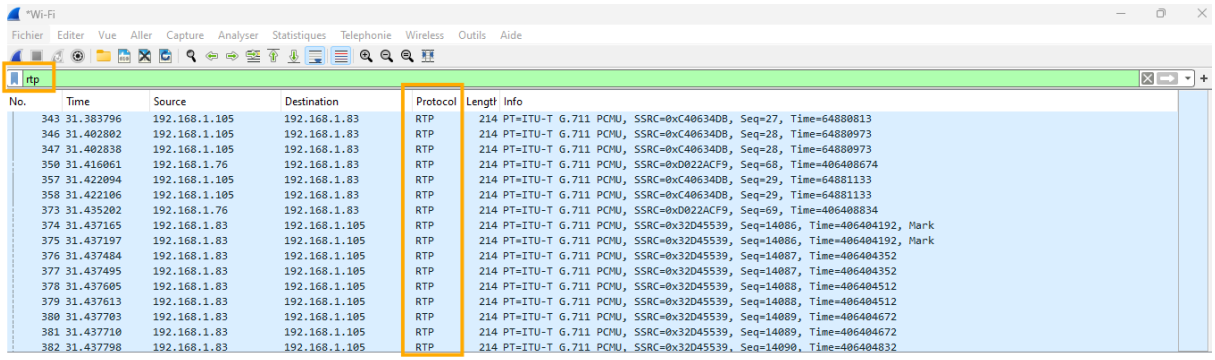


Figure 4.4 : Application d'un filtre sur le protocole RTP

Maintenant on va dans Téléphonie > Appels VoIP pour visualiser tous les appels détectés.

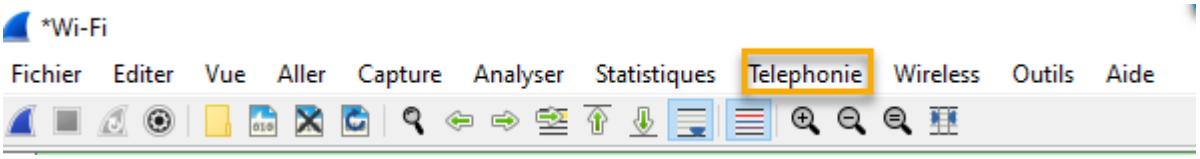


Figure 4.5 : Sélection de téléphonie pour visualiser les appels VoIP

En accédant à l'interface de gestion des appels, il est possible de visualiser une liste détaillée de toutes les conversations actives. Pour chaque appel, nous avons accès à des informations complémentaires telles que la durée de l'appel, les numéros de téléphone ou les adresses IP des interlocuteurs...etc. Pour écouter le contenu d'une conversation, il suffit de sélectionner l'appel concerné et de cliquer sur ‘’lire les flux ‘’.

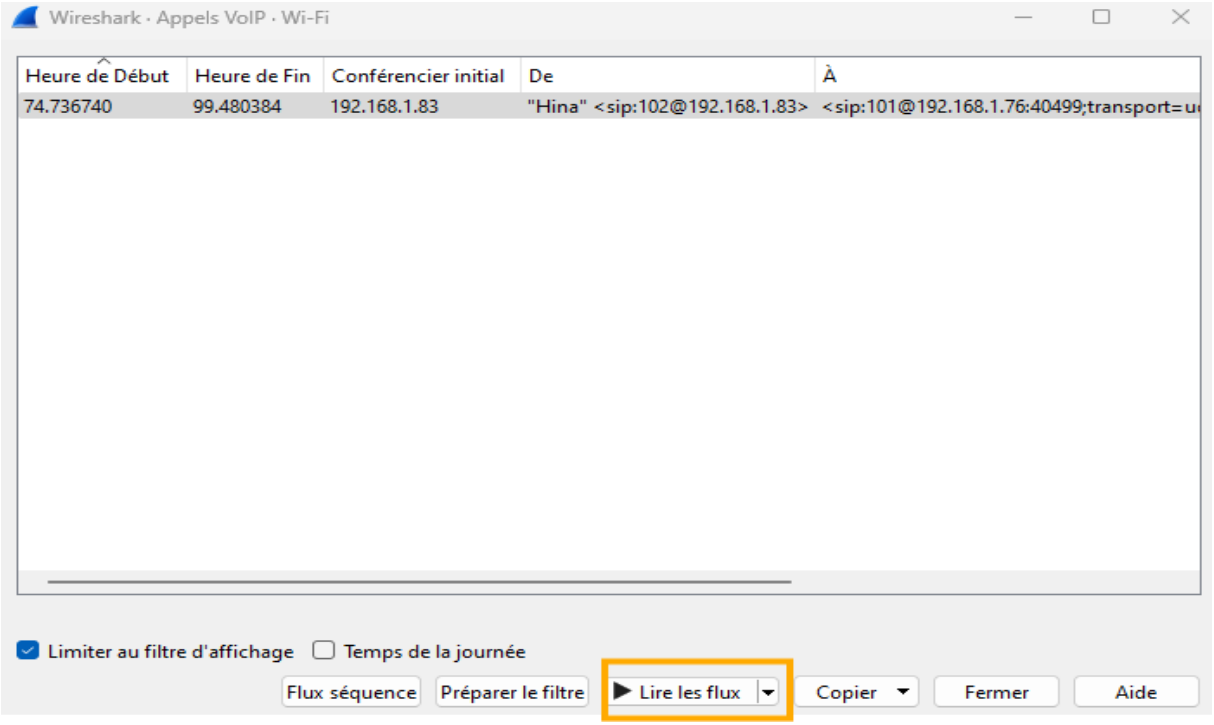


Figure 4.6 : Listes des flux RTP

Grace à Wireshark, nous avons la capacité de capturer et d'inspecter les paquets RTP qui transportent les flux audio des conversations téléphoniques entre deux clients SIP. Comme illustré dans la figure ci-dessous.

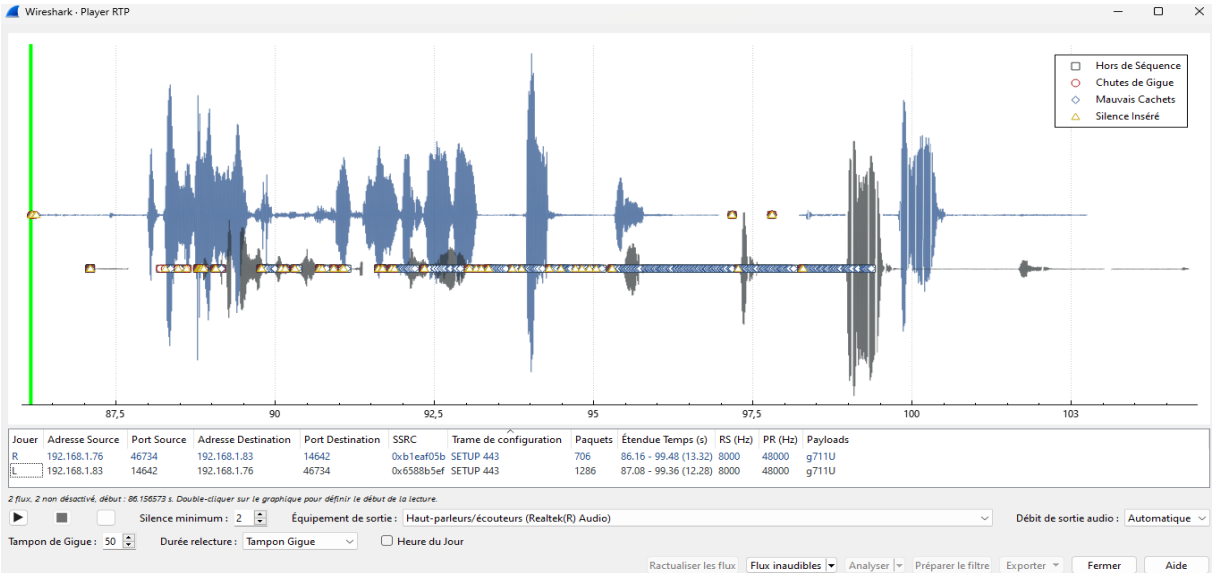


Figure 4.7 : Ecoute d'une conversation téléphonique entre deux utilisateurs avec Wireshark

Après avoir montré la facilité avec laquelle les communications VoIP non sécurisées peuvent être interceptées, il devient impératif de discuter des mesures de sécurité nécessaires pour protéger ces communications.

3. Solutions avancées de sécurité

Nous allons explorer l'implémentation de mesures de sécurité essentielles pour garantir la confidentialité et l'intégrité des communications VoIP dans notre solution. Parmi ces mesures, nous utiliserons Fail2ban, Firewall, protocole SRTP et TLS, des outils indispensables pour renforcer la sécurité de notre système Issabel PBX.

3.1 Optimisation de la Sécurité du Serveur avec Fail2ban

Pour renforcer la sécurité du serveur, nous abordons maintenant l'utilisation de Fail2ban, un système de prévention des intrusions efficace et configurable.

3.1.1 Définition de fail2ban

Fail2ban est un logiciel de sécurité qui protège les systèmes en surveillant les fichiers de logs pour identifier les tentatives répétées de connexion échouées. Lorsqu'une adresse IP tente à plusieurs reprises de se connecter sans succès, Fail2ban la bloque en ajoutant une règle au pare-feu iptables, empêchant ainsi toute nouvelle tentative de cette adresse pendant une période définie. Ce mécanisme améliore la sécurité globale du système en bloquant automatiquement les tentatives de connexion malveillantes, réduisant ainsi les risques d'intrusions non autorisées et de perturbations du service.

3.1.2 Configuration de fail2ban

Issabel offre une interface utilisateur graphique qui facilite la configuration de services comme Fail2ban sans avoir besoin d'entrer des commandes dans le terminal. Pour cela, nous allons accédez à l'interface web d'Issabel et nous diriger vers Security>Fail2ban>Admin.

Figure 4.8 : Sélection de Fail2ban dans les Paramètres de Sécurité

Maintenant, nous pouvons voir les différents paramètres des jails qui sont déjà configurer par défaut pour offrir une sécurité de base dès le départ. Cependant, ils peuvent être personnalisés pour répondre aux besoins spécifiques de notre environnement.

Figure 4.9 : Configuration des jails

Pour adapter ces jails à nos besoins, nous allons personnaliser certains paramètres en commençant par celle d'Asterisk, qui est cruciale pour la sécurité de notre système de téléphonie VoIP. Il est important de définir une liste blanche pour éviter de bannir par erreur nos propres adresses IP.

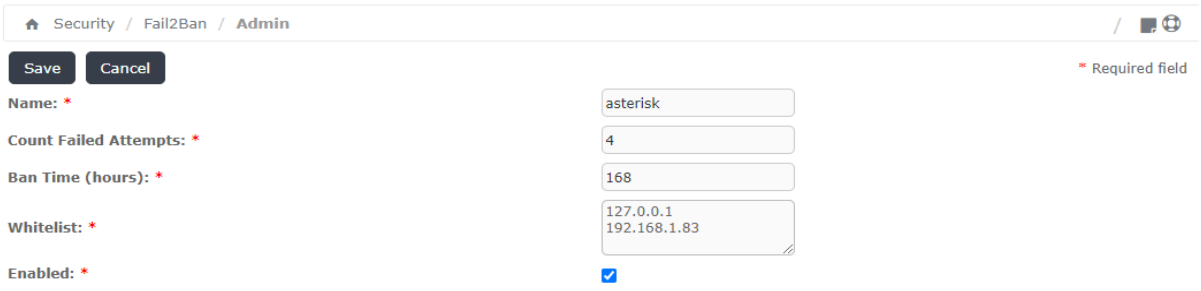


Figure 4.10 : Configuration des jails pour Asterisk

Nous allons refaire cette même action pour chacun de nos services afin de garantir une protection complète. Après avoir fini, notre configuration ressemblera à ceci

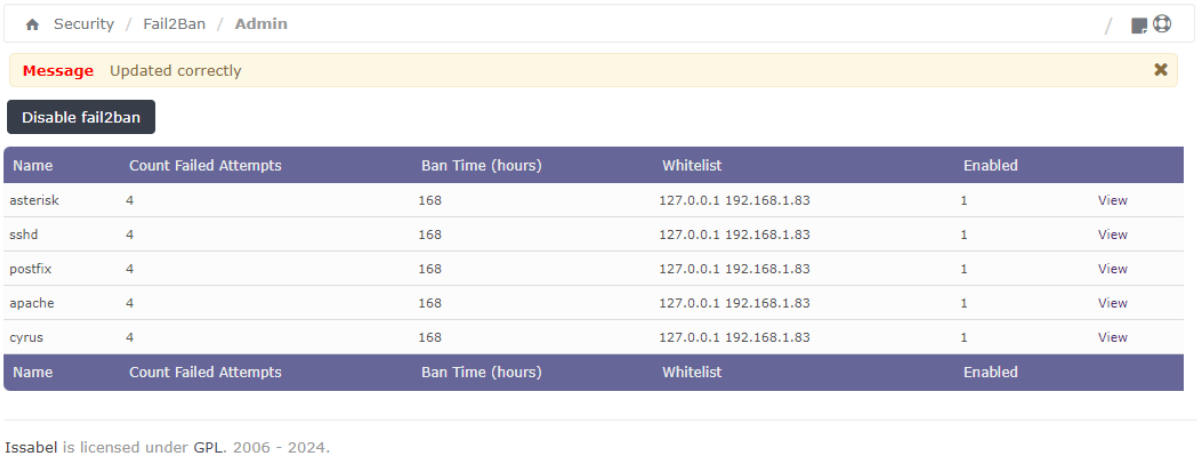


Figure 4.11 : Liste des jails des services

3.2 Renforcement de la Sécurité du Pare-feu

Dans cette section, nous nous concentrerons sur le renforcement de la sécurité du pare-feu à travers la configuration détaillée du Firewall.

3.2.1 Configuration du Firewall

Pour gérer les règles d'accès et renforcer la sécurité de notre système, nous allons configurer le pare-feu en allant dans le menu ‘’Security’’, nous sélectionnerons l'option ‘’Firewall’’ pour ouvrir les paramètres associés. Ensuite, nous pourrons définir les ports autorisés à communiquer en choisissant la section ‘’Define ports‘’.

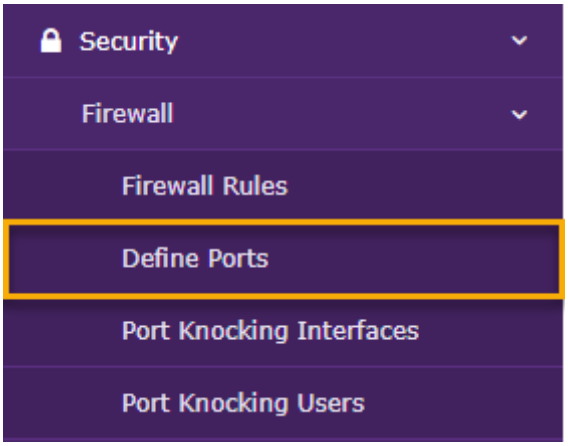
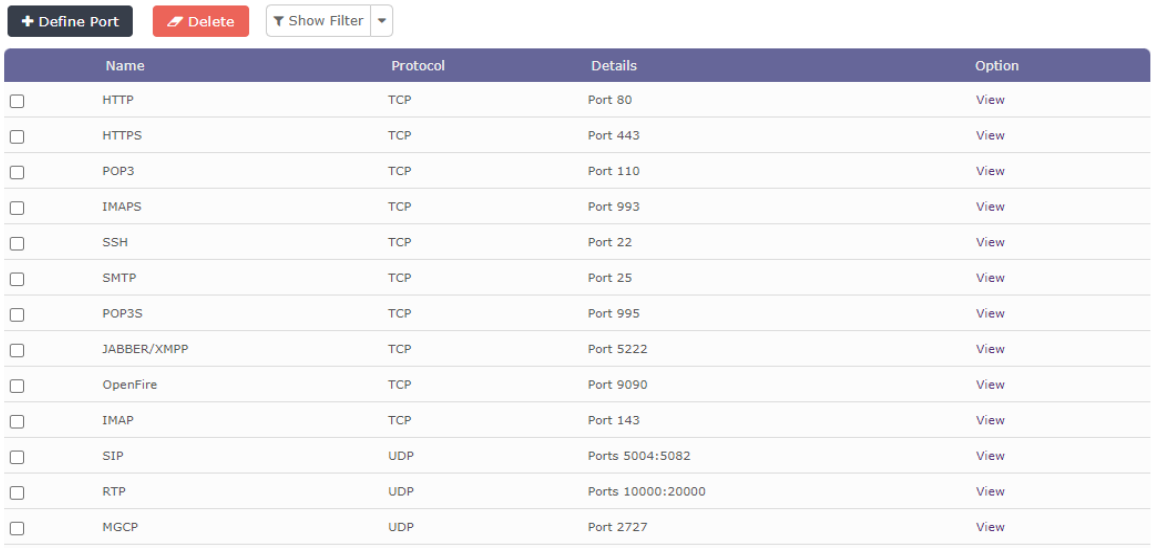


Figure 4.12 : Sélection de Firewall dans les Paramètres de Sécurité

Avant toute chose, on détermine les ports qui nécessitent un accès entrant ou sortant.



	Name	Protocol	Details	Option
☐	HTTP	TCP	Port 80	View
☐	HTTPS	TCP	Port 443	View
☐	POP3	TCP	Port 110	View
☐	IMAPS	TCP	Port 993	View
☐	SSH	TCP	Port 22	View
☐	SMTP	TCP	Port 25	View
☐	POP3S	TCP	Port 995	View
☐	JABBER/XMPP	TCP	Port 5222	View
☐	OpenFire	TCP	Port 9090	View
☐	IMAP	TCP	Port 143	View
☐	SIP	UDP	Ports 5004:5082	View
☐	RTP	UDP	Ports 10000:20000	View
☐	MGCP	UDP	Port 2727	View

Figure 4.13 : Définition des ports

Après avoir configuré les ports réseau, il est essentiel de mettre en place des règles de sécurité du pare-feu. Pour ce faire, on accède à la section Security > Firewall >Firewall Rules, puis on active le pare-feu en cliquant sur ‘’Activate Firewall’’.

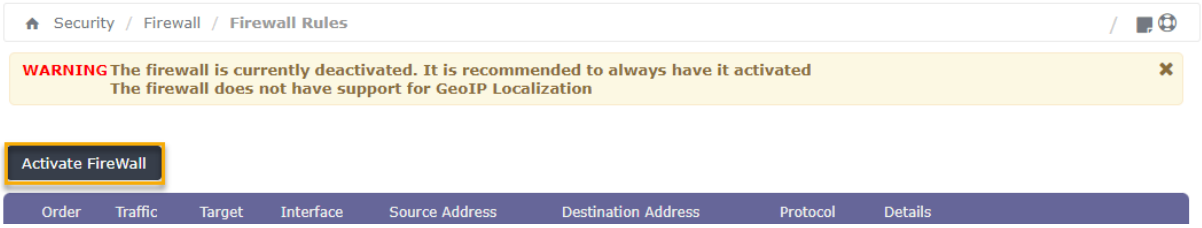


Figure 4.14 : Activation du pare-feu

Pour définir une nouvelle règle, nous allons cliquer sur le bouton ‘’New Rule’’ dans l'interface du firewall.

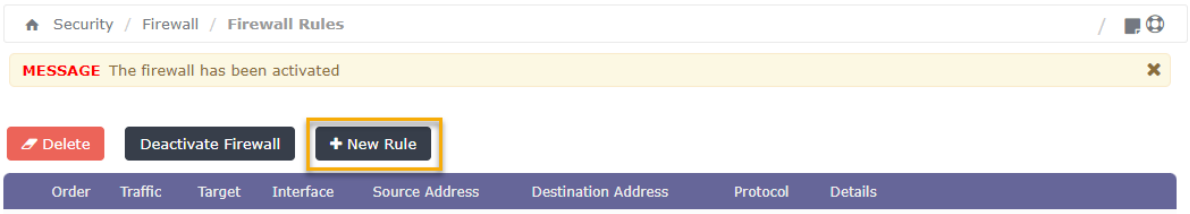


Figure 4.15 : Définition d'une nouvelle règle dans le firewall

Ainsi, nous pouvons procéder à la définition de notre règle.

Figure 4.16 : Définition des règles du pare-feu

Nous allons élaborer des directives spécifiques pour chaque protocole, permettant ainsi une filtration précise du trafic des paquets. Une fois ce processus finalisé, nous obtiendrons ce résultat.

Order	Traffic	Target	Interface	Source Address	Destination Address	Protocol	Details
1			IN: lo	0.0.0.0/0	0.0.0.0/0	ALL	
2			IN: ANY	0.0.0.0/0	0.0.0.0/0	ICMP	Type: ANY
3			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: DHCPD
4			IN: ANY	0.0.0.0/0	0.0.0.0/0	TCP	Source Port: ANY Destination Port: FOP2
5			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: SIP
6			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: IAX2
7			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: IAX1
8			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: RTP
9			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: ANY Destination Port: MGCP
10			IN: ANY	0.0.0.0/0	0.0.0.0/0	UDP	Source Port: DNS Destination Port: ANY

Figure 4.17 : Liste des règles du pare-feu

Et maintenant, nous adopterons une approche restrictive en autorisant uniquement les protocoles nécessaires à nos besoins spécifiques, tout en bloquant tous les autres. Cette mesure vise à réduire la surface d'attaque en n'autorisant que les communications essentielles, renforçant ainsi la sécurité de notre réseau contre les menaces potentielles.

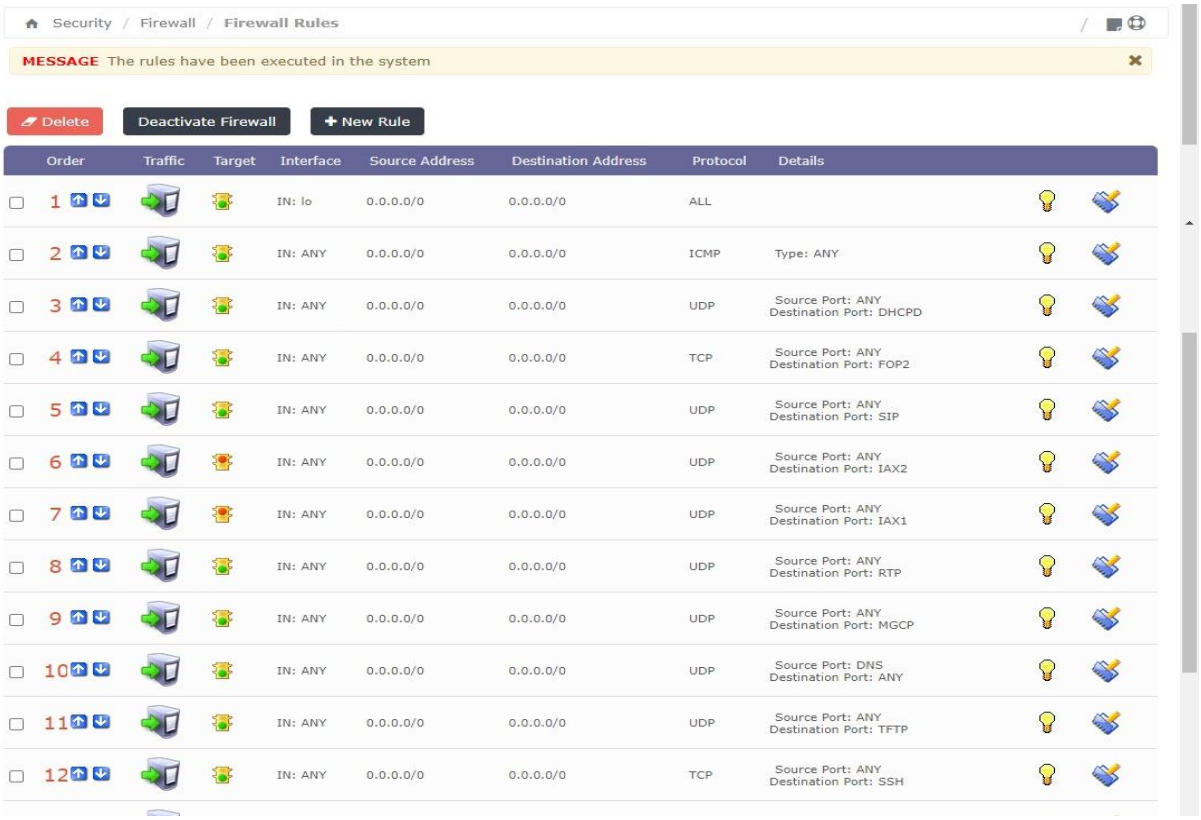


Figure 4.18 : Blocage de certaines règles du firewall

3.3 Configuration de SRTP

Le protocole SRTP permet de chiffrer les appels VoIP, renforçant ainsi la protection des données sensibles.

Pour configurer SRTP, on se rend dans l'interface web, dans la rubrique "PBX", puis dans la section "Extensions" sous " IBX Configuration ". On sélectionne ensuite l'extension concernée et on active SRTP.

Figure 4.19 : Configuration de SRTP dans l'interface web

3.4 Configuration de TLS

La configuration appropriée de TLS dans Issabel offre une couche supplémentaire de sécurité pour les communications VoIP. En établissant des connexions sécurisées entre les clients et le serveur, TLS garantit que les données échangées sont cryptées et protégées contre toute tentative d'interception ou de manipulation par des tiers non autorisés.

Pour sécuriser les communications VoIP dans notre système Asterisk. Voici comment nous allons procéder :

- Tous d'abord, nous intégrons le script « ast_tls_cert » afin de générer des certificats TLS. La commande suivante permet de télécharger ce script depuis le référentiel GitHub officiel d'Asterisk :

```
[root@issabel ~]# wget -O /root/ast_tls_cert https://raw.githubusercontent.com/asterisk/asterisk/mas
ter/contrib/scripts/ast_tls_cert_
```

Figure 4.20 : Téléchargement du script ast_tls_cert

- Ensuite, on utilise le script ast_tls_cert pour créer une autorité de certification (CA) locale, générer des certificats pour le serveur, et combiner ces certificats en un fichier utilisable par Asterisk.

```
[root@issabel ~]# /root/ast_tls_cert -C issabel.hopto.org -O "LesllCommandements" -d /etc/asterisk/k
eys/
No config file specified, creating '/etc/asterisk/keys//tmp.cfg'
You can use this config file to create additional certs without
re-entering the information for the fields in the certificate
Creating CA key /etc/asterisk/keys//ca.key
Generating RSA private key, 4096 bit long modulus
...............................++
......++
e is 65537 (0x10001)
Enter pass phrase for /etc/asterisk/keys//ca.key:
Verifying - Enter pass phrase for /etc/asterisk/keys//ca.key:
Creating CA certificate /etc/asterisk/keys//ca.crt
Enter pass phrase for /etc/asterisk/keys//ca.key:
Creating certificate /etc/asterisk/keys//asterisk.key
Generating RSA private key, 2048 bit long modulus
.....................+++
.....................................+++
e is 65537 (0x10001)
Creating signing request /etc/asterisk/keys//asterisk.csr
Creating certificate /etc/asterisk/keys//asterisk.crt
Signature ok
subject=/CN=issabel.hopto.org/O=LesllCommandements
Getting CA Private Key
Enter pass phrase for /etc/asterisk/keys//ca.key:
Combining key and crt into /etc/asterisk/keys//asterisk.pem
[root@issabel ~]#
```

Figure 4.21 : Génération des certificats

- Dans le répertoire /etc/asterisk/keys, nous avons rassemblé les certificats nécessaires à la configuration sécurisée de la VoIP via TLS. Avant d'aller plus loin, examinons attentivement les fichiers que nous avons créés.

```
[root@issabel ~]# cd /etc/asterisk/keys/
[root@issabel keys]# ls -la
total 48
drwxrwx--x  2 root     root      4096  8 juin  10:17 .
drwxrwxr-x. 3 asterisk asterisk 12288  9 juin  03:33 ..
-rw-------  1 root     root      1415  8 juin  10:18 asterisk.crt
-rw-------  1 root     root       940  8 juin  10:17 asterisk.csr
-rw-------  1 root     root      1675  8 juin  10:17 asterisk.key
-rw-rw-r--  1 asterisk asterisk  3090  8 juin  10:18 asterisk.pem
-rw-------  1 root     root       164  8 juin  10:13 ca.cfg
-rw-------  1 root     root      1777  8 juin  10:17 ca.crt
-rw-------  1 root     root      3311  8 juin  10:16 ca.key
-rw-------  1 root     root       131  8 juin  10:13 tmp.cfg
[root@issabel keys]#
```

Figure 4.22 : Listes de clés générées

- Après nous configurons le module PJSIP d'asterisk pour utiliser tls. Cette étape consiste à ouvrir le fichier de configuration principal (pjsip.conf) afin d'ajouter les paramètres nécessaires pour TLS

```
[root@issabel ~]# sudo nano /etc/asterisk/pjsip.conf_
```

Figure 4.23 : Ouverture du fichier pjsip.conf

- Par la suite on ajoute la configuration de transport TLS, cette configuration définit un transport nommé 'transport-tls' qui utilise le protocole TLS sur le port 5061. Il spécifie également les emplacements des fichiers de certificat et de clé privée, ainsi que la méthode TLS à utiliser (TLS v1.2).

```
[transport-tls]
type = transport                                ; Spécifie le type comme étant un transport
protocol = tls                                  ; Protocole utilisé
bind = 0.0.0.0:5061                             ; Port d'écoute pour les connexions TLS
cert_file = /etc/pki/tls/certs/asterisk.crt     ; Chemin vers le certificat SSL
priv_key_file = /etc/pki/tls/private/asterisk.key ; Chemin vers la clé privée SSL
method = tlsv1_2                                ; Méthode de chiffrement TLS à utiliser
~
~
~
-- INSERT --
```

Figure 4.24 : Configuration du fichier pjsip.conf

- Après cela, on redémarre le service Asterisk pour appliquer les modifications de configuration.

```
[root@issabel ~]# sudo systemctl restart asterisk
```

Figure 4.25 : Redémarrer Asterisk

- Et maintenant on accède à l'interface web d'Issabel, puis dans la rubrique 'PBX', et ensuite dans 'IBX Configuration' sous 'Extensions'. On sélectionne l'extension appropriée et on ajuste plusieurs paramètres pour activer TLS.

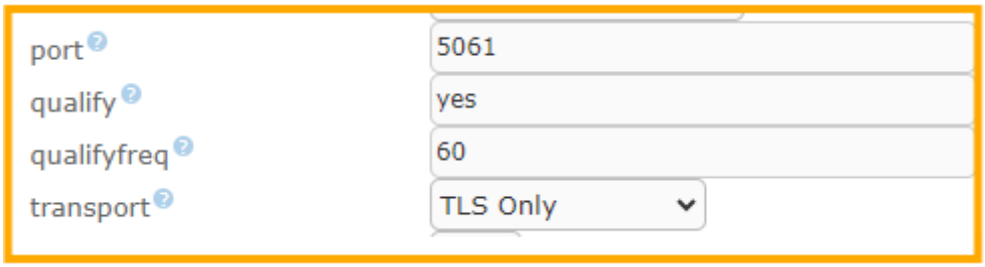


Figure 4.26 : Configuration de TLS sur l'interface web

4. Conclusion :

Dans ce chapitre dédié à la sécurité, nous avons exploré diverses méthodes visant à renforcer la protection de notre infrastructure de communication. Du déploiement de pare-feu pour contrôler le trafic réseau à l'utilisation de File2ban pour bloquer les accès non autorisés, en passant par la mise en place de TLS pour sécuriser la signalisation SIP et l'activation de SRTP pour chiffrer les flux de médias, nous avons examiné plusieurs approches essentielles pour garantir la sécurité de notre système VoIP.

Bien que ces mesures offrent une protection précieuse contre un large éventail de menaces, il est important de reconnaître que la sécurité absolue reste un objectif difficile à atteindre. Aucune mesure de sécurité n'est infaillible, et la vigilance continue demeure essentielle pour détecter et prévenir les éventuelles vulnérabilités ou attaques.

Conclusion Générale

Dans un monde de plus en plus connecté, où la communication instantanée est essentielle, la Voix sur IP (VoIP) se présente comme une technologie révolutionnaire. Cependant, cette révolution n'est pas exempte de défis, notamment en termes de sécurité.

La mise en place d'une solution VoIP sécurisée est une tâche complexe qui requiert une compréhension approfondie des aspects techniques, des risques de sécurité et des solutions existantes. À travers ce mémoire, nous avons exploré ces dimensions de manière exhaustive pour offrir une vision claire et pratique de l'intégration d'une solution VoIP dans un environnement de centre d'appel.

Dans le premier chapitre, nous avons présenté les généralités de la VoIP, en soulignant son importance croissante dans les communications modernes et ses avantages notables en termes de coût et de flexibilité. Ce cadre de base nous a permis d'aborder, dans le deuxième chapitre, les divers risques de sécurité inhérents à la VoIP, ainsi que les solutions pour les atténuer. Nous avons identifié les menaces telles que les interceptions, les attaques DDoS et la fraude, et avons proposé des contre-mesures efficaces comme l'utilisation de TLS, de pare-feu et de mécanismes de détection d'intrusions.

Le troisième chapitre s'est concentré sur l'étude de l'existant dans un centre d'appel, le choix de la solution VoIP (en utilisant VMware Workstation, Issabel et linphone), ainsi que l'installation et la configuration de cette solution. Nous avons formulé la problématique centrale de notre étude : **"Comment les centres d'appel peuvent-ils surmonter leurs limitations actuelles en adoptant des technologies modernes tout en garantissant la sécurité et l'efficacité opérationnelle ?"**. En répondant à cette question, nous avons démontré que l'intégration de technologies modernes, bien que complexe, permet une amélioration significative de l'efficacité opérationnelle tout en assurant une sécurité robuste.

Enfin, dans le quatrième chapitre, nous avons entrepris une analyse approfondie de notre solution VoIP en utilisant Wireshark, un outil de surveillance et d'analyse de réseau. Cette analyse initiale a révélé plusieurs failles de sécurité dans notre système. Pour répondre à ces vulnérabilités, nous avons mis en œuvre des mesures de sécurité robustes, incluant la configuration de fail2ban, l'implémentation d'un pare-feu, le chiffrement TLS et l'utilisation du

protocole SRTP. Ces mesures assurent que la solution VoIP est résiliente et capable de résister aux diverses menaces de sécurité.

En conclusion, ce mémoire a démontré que les centres d'appel peuvent non seulement adopter des technologies modernes comme la VoIP pour surmonter leurs limitations actuelles, mais aussi garantir un haut niveau de sécurité et d'efficacité opérationnelle. La clé réside dans une compréhension approfondie des risques et des solutions, une planification rigoureuse, et l'application de bonnes pratiques de sécurité. Ainsi, les centres d'appel peuvent évoluer vers des infrastructures de communication plus agiles, sécurisées et performantes, répondant ainsi aux exigences du monde numérique moderne.

Les perspectives futures incluent l'intégration de technologies émergentes comme l'intelligence artificielle pour améliorer l'efficacité des centres d'appel, l'implémentation de systèmes de détection d'intrusion basés sur l'apprentissage automatique pour renforcer la sécurité, et l'exploration de solutions VoIP basées sur le cloud pour une plus grande flexibilité et évolutivité. Notre étude ne s'arrête pas là : elle ouvre la voie à des recherches continues et à des innovations qui permettront d'améliorer encore la sécurité et l'efficacité des solutions VoIP. En continuant à innover et à adapter les solutions de communication, les centres d'appel pourront non seulement améliorer leurs opérations, mais aussi offrir un service client de meilleure qualité tout en garantissant la sécurité et l'intégrité des données.

Résumé

La téléphonie sur IP (VoIP) représente une solution moderne et efficace pour les communications vocales en réseau. Ce mémoire se concentre sur l'implémentation d'une solution VoIP sécurisée en utilisant Issabel, une plateforme intégrant Asterisk. Nous explorons les protocoles de VoIP, les vulnérabilités inhérentes à cette technologie, et les stratégies de protection efficaces. La section pratique couvre l'installation et la configuration d'Issabel, la gestion des utilisateurs. L'analyse initiale avec Wireshark a permis de mettre en évidence des failles de sécurité dans notre système, ce qui nous a incités à renforcer notre solution avec des mesures de protection avancées telles que le chiffrement TLS/SRTP, la configuration d'un pare-feu robuste, et l'utilisation de fail2ban pour prévenir les intrusions.

Mots clés : VoIP, Voix sur IP, Issabel, Asterisk, IPBX, SIP, H.323, RTP, RTCP.

Abstract

Voice over IP (VoIP) represents a modern and efficient solution for network voice communications. This thesis focuses on implementing a secure VoIP solution using Issabel, a platform integrating Asterisk. We explore VoIP protocols, inherent vulnerabilities of this technology, and effective protection strategies. The practical section covers Issabel's installation and configuration, as well as user management. Initial analysis with Wireshark highlighted security flaws in our system, prompting us to enhance our solution with advanced protection measures such as TLS/SRTP encryption, robust firewall configuration, and the use of fail2ban to prevent intrusions.

Keywords: VoIP, Voice over IP, Issabel, Asterisk, IPBX, SIP, H.323, RTP, RTCP.

Bibliographie

[1] Centre d'expertise des grands organismes, *La téléphonie sur IP*, 2007.

[2] BENACHOUR.L, DJABALI.Kh, Implémentation d'une solution VoIP sécurisée dans un réseau d'entreprise, MEMOIRE MASTER, Université SAAD DAHLAB de BLIDA, 2021/2022.

[4] BOUZID.R, CHABANA.D, Etude d'un système de communication VoIP, MEMOIRE MASTER, Université Abderrahmane Mira de Béjaïa, 2018,2019.

[5] O. Laurent, G Pujolle, Téléphonie sur IP, Eyrolles, Paris, 2008.

[6] NDAYISABA.E, NIYONKURU.D, VoIP : Réalisation d'un standard téléphonique, MEMOIRE MASTER, Université IBN Khaldoun de Tiaret, 2011/2012.

[7] HEROVITZ (J). op.cit, P.46.

[9] SALAH M, BELOUCIF M, Mise en place d'une solution VoIP sécurisée au sien de l'entreprise, MEMOIRE MASTER, Université Abderrahmane Mira de Béjaïa, 2021/2022.

[10] K. Lalaina, VoIP & Security: IPS, Rapport Technique 2020

[11] Rebha BOUZAIDA, Etude et Mise en place d'une solution, Faculté de nouvelle Technologie Département de communication, Université de LORRAINNE, 2015

[12] Institut des métiers de France Télécom, mars 1999.

Webographie

[3] https://www.frameip.com/

[8] https://ts5ri-voip-pfe.fr.gd/Attaques-sur-les-protocoles.htm

[10] https://www.e-xpertsolutions.com/images/pdf/Rapport_Kuhn.pdf

[13] https://wikimemoires.net/?p=1497

[14] https://engsoftgroup.com/pabx-call-centercontact-centrecomplete-call-analysis-and-voice-recording/