République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue d'obtention du diplôme de Master en Informatique.
Spécialité : Adminstration et Sécurité des Réseaux.

Thème

Mise en place d'une solution VoIP sécurisée au sien de l'entreprise

---

Réalisé par :

M. SALAH Mohand et Mlle. BELOUCIF Mouna .

Evalué le 28/09/2022 devant le jury composé de :

Examinateur 1	**Dr. TOUAZI Djoudi**	**U. A/Mira Béjaïa.**
Examinateur 2	**Dr. ALOUI Soraya**	**U. A/Mira Béjaïa.**
Encadrant	**Dr. NAFI Mohammed**	**U. A/Mira Béjaïa.**

Année universitaire 2021/2022

Remerciements

À travers ce modeste travail, nous tenons à remercier notre encadrant pour ses conseils, son orientation et son aide le long de notre projet de fin d'étude.

Nos remerciements s'adressent aussi aux président et membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous exprimons également notre gratitude à tous les professeurs et enseignants qui nous ont aidé à réaliser ce travail, sans omettre bien- sûr de remercier profondément tous ceux qui ont contribué de près ou de loin à la réalisation de ce présent travail.

Nous remercions aussi le personnel de l'entreprise EXSON TELECOM, pour leurs accueils en stage pratique.

Et enfin, que nos chers parents et familles, trouvent ici l'expression de nos remerciements les plus sincères et les plus profonds en reconnaissance de leurs sacrifices, aides, soutien et encouragement afin de nous assurer cette formation dans les meilleures conditions.

Table des matières

Introduction générale 1

1 Généralités sur la voix sur IP et Asterisk **4**

1.1 Généralités sur la Téléphonie IP 5

1.1.1 Introduction 5

1.1.2 Quelques définitions 5

1.1.3 Téléphonie classique vs Téléphonie sur IP 6

1.1.4 Principe de fonctionnement de la VoIP 6

1.1.5 Architectures VoIP 7

1.1.6 Protocoles de signalisation 9

1.1.6.1 Protocole H.323 : 9

1.1.6.2 Protocole SIP 10

1.1.7 Protocoles de transport 14

1.1.7.1 Protocole RTP : 14

1.1.7.2 Protocole RTCP : 15

1.1.8 Avantages et inconvénients de la VoIP 15

1.1.8.1 Avantages de la voip 15

1.1.8.2 Inconvénients de la VoIP 16

1.2 Solution VoIP basée sur Asterisk 16

1.2.1 Présentation d'Asterisk 16

1.2.2 Caractéristiques d'asterisk 17

1.2.3 Protocoles d'asterisk 17

1.2.4 Architecture d'Asterisk 17

1.2.4.1 Vue d'ensemble 17

1.2.4.2 Fonctionnement interne d'asterisk 18

1.3 Conclusion 19

2 Vulnérabilités et attaques contre la VoIP **20**
2.1 Introduction . . . 21
2.2 Vulnérabilités de l'infrastructure . . . 21
2.3 Attaques contre les protocoles VoIP . . . 22
2.3.1 Attaques de déni de service (DoS) . . . 22
2.3.2 Sniffing . . . 25
2.3.3 Attaque de l'homme au milieu . . . 25
2.3.4 Attaque par suivi des appels . . . 26
2.3.5 Injection des paquets RTP . . . 26
2.3.6 Spam . . . 26
2.3.7 Détournement d'appel (CALL HIJACKING) . . . 27
2.4 Technique de sécurisation . . . 27
2.4.1 Sécurisation de l'application . . . 27
2.4.2 Sécurité au niveau du système d'exploitation . . . 27
2.4.3 Sécurisation au niveau des protocoles . . . 28
2.5 Conclusion . . . 29

3 Présentation de l'organisme d'accueil **30**
3.1 Introduction . . . 31
3.2 Présentation de l'entreprise . . . 31
3.2.1 Situation géographique . . . 31
3.2.2 Objectifs, Missions et activités de l'Entreprise . . . 32
3.2.3 Produits disponible dans l'entreprise . . . 33
3.2.4 Organigramme général de l'organisme d'accueil . . . 34
3.2.5 Description de chaque service . . . 34
3.2.6 Architecture réseaux . . . 35
3.2.7 Analyse du parc informatique . . . 36
3.3 Problématique et solution . . . 37
3.3.1 Problématique . . . 37
3.3.2 Solutions proposée . . . 37
3.4 Conclusion . . . 38

4 Réalisation **39**
4.1 Introduction . . . 40
4.2 Environnement de travail . . . 40
4.3 Architecture proposée . . . 41
4.4 Méthodologie . . . 42
4.5 Installation . . . 42

4.5.1 Présentation du server Elastix 42
4.5.1.1 Installation d'Elastix 43
4.5.1.2 Lancement du serveur 45
4.5.1.3 Accès au serveur 45
4.5.1.4 Tableau de bord d'interface Elastix 46
4.5.2 Présentation de PfSense (Firewall) 46
4.5.2.1 Instalation de PfSense 46
4.6 Configuration de base 48
4.6.1 Plan d'adressage IPv4 48
4.6.2 Configuration VTP (Serveur/Client/Transparent) 48
4.6.3 Interface en mode trunk 50
4.6.4 Création des vlan 51
4.6.5 Affectation des port vlan 52
4.6.6 Configuration du routage inter-vlan 53
4.6.7 Configuration du service DHCP sur le routeur 55
4.6.8 Configuration de base de Routeur 56
4.6.9 Configuration de base de firewall 57
4.6.10 Configuration de client VPN 61
4.7 Configuration du PBX et création des compts sip 64
4.7.0.1 Addresse IP en mode statique 64
4.7.0.2 Création d'une nouvelle extension 64
4.7.1 Configuration de logiciel de téléphonie 66
4.8 Scénarios d'attaques contre la VoIP 68
4.8.1 Attaques contre la VoIP 68
4.8.1.1 Localisation des serveurs VoIP 68
4.8.1.2 Attaque MITM"Man-in-the-Middle" 69
4.8.1.3 Attaque par DOS (déni de service) 70
4.8.2 Sécurisation contre les attaques 71
4.8.2.1 Sécurisation du vlan natif 71
4.8.3 Sécurisation des ports 74
4.8.4 Autre aspect de sécurité 76
4.8.4.1 Implémentation d'un pfsense 76
4.8.4.2 Mise en place de la solution VPN 77
4.9 Conclusion 78
Conclusion générale 79

Table des figures

1.1 Processus de communication vocale sur un réseau IP 7
1.2 Architecture du réseau de téléphonie classique d'entreprise. 8
1.3 Architecture VoIP d'entreprise (architecture Full-IP). 8
1.4 Architecture VoIP (architecture type centrex). 9
1.5 Enregistrement d'un terminal SIP. 13
1.6 Initiation d'une communication directe. 14
1.7 Architecture interne d'Asterisk 18

2.1 Attaque Dos avec la méthode CANCEL 23
2.2 Attaque Dos avec la méthode BYE 24
2.3 Attaque de l'homme au milieu 25

3.1 Logo de Exson Telecom 31
3.2 EXSON TELECOM via Google maps. 32
3.3 Organigramme général d'Exson Telecom 34
3.4 Éléments de service technique 34
3.5 Architecture réseaux Exson Telecom 36

4.1 Outiles de travail 40
4.2 Nouvelle architecture réseaux Exson Telecom 41
4.3 Etapes de la méthodologie 42
4.4 Démarrage l'installation Elastix 43
4.5 Différent paremètre d'avant installation 43
4.6 Système d'authentification par mot de passe 44
4.7 Vérification des dépendances 44
4.8 Spécification d'un mot de passe pour l'administrateur de l'interface Web. . . . 44
4.9 Vérification de mot de passe 44
4.10 Adresse IP de server Elastix 45
4.11 Login et mot de passe du server Elastix 45
4.12 Interface Elastix 46

4.13 Démarage de PfSense 46
4.14 Début de processus d'installation 47
4.15 Début d'installation 47
4.16 Lancement de PfSense avec la configuration 48
4.17 Affichage le statu VTP 49
4.18 Affichage d'informations VTP 50
4.19 Affichage d'informations sur les ports 51
4.20 Création des VLANs. 51
4.21 Affichage des VLAN crée 51
4.22 Création des vlan 53
4.23 Affectation des vlan 53
4.24 Autorisation des vlan 54
4.25 Tableau de bord de firewall 54
4.26 Affichage d'informations 55
4.27 Affichage d'informations 55
4.28 Affichage de test DHCP 56
4.29 l'interface d'accueil de PfSense 57
4.30 Édition d'un utilisateur 58
4.31 Graphe de PfSense 58
4.32 Configuration DNS 59
4.33 Application des régles 59
4.34 Création des Vlan 60
4.35 Règles sur LAN 60
4.36 Routage de Firewall 61
4.37 Création de certificat de client 61
4.38 Création de certificat de serveur 62
4.39 Création de la préconfiguration Openvpn 62
4.40 Installation complète de package 63
4.41 Vérsions Openvpn préconfigurer 63
4.42 Ajouter Extension 65
4.43 extension ajouter 65
4.44 logiciel téléphonique 3cx 66
4.45 Interface de configuration de 3CXPhone 67
4.46 Test de communication entre les clients 3CX 67
4.47 Scan le réseau avec svmap 68
4.48 Interface de wireshark 69
4.49 Paquets RTP interceptés par Wireshark 69

4.50 Enregistrements d'un appel voip 70
4.51 Ecoute des conversations enregistrées 70
4.52 Attaque de type DOS avec inviteflood 71
4.53 Appel interrompu entre les deux extensions 71
4.54 Vérification des vlan 72
4.55 Création un vlan natif 72
4.56 Création vlan 99 73
4.57 Vérification vlan natif 73
4.58 Adresse mac d'une machine 75
4.59 Détail de la sécurité 75
4.60 Connexion à l'interface web pfsense 76
4.61 Configuration des regles d'interfaces LAN 76
4.62 Configuration des regles d'interfaces WAN 77
4.63 Installation le client OpenVPN. 77
4.64 Authentification client vpn 78
4.65 Zone autorisée pour les clients vpn 78

Liste des tableaux

3.1 Environnement matériel et logiciel 36

4.1 Plan d'adressage IPv4 48

Liste des abréviations

ACK	ACKnowledged
ADCI	Active Directory Service Interfaces
API	Application Programming Interface
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
GSM	Global System for Mobile Communication
HTTP	Hypertext Transfer Protocol
IAX	Inter Asterisk eXchange
IDS	Intrusion detection System
IMS	IP multimedia subsystem
IP	Internet Protocol
IPBX	Internet Protocol Private Branch eXchange
ISO	International Organization for Standardization
LAN	Local Area Network
MAC	Media Access Control
MCU	Multipoint Control Unit
MGCP	Media Gateway Control Protocol
NAT	Network Address Translation
OSI	Open Systems Interconnection
PABX	Private Automated Branch Exchange
PBX	Private Branch eXchange
RIP	Routing Information Protocol
RTC	Réseau téléphonique commuté
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
WAN	Wide Area Network

Introduction générale

À l'heure actuelle, un élément clé de l'évolution du secteur des communications est le développement de la technologie de transmission vocale basée sur le protocole IP.
Il y a quelques années, le service téléphonique traditionnel, ou RTC, était le seul type de communication disponible, et les offres des opérateurs étaient déterminées uniquement par la concurrence du marché.
La popularité d'Internet l'a rendu possible grâce à la réduction des coûts d'accès et de communication, et les efforts déployés pour faire progresser la technologie dans les domaines des réseaux IP et RTC ont permis la naissance du téléphone IP, également appelé VoIP (Voice Over Internet Protocol), une nouvelle technologie qui envahit rapidement le domaine de la communication vocale. Elle communique avec un grand nombre d'entreprises et le monde entier via les réseaux internet.
Les nombreux services offerts par les systèmes téléphoniques IP reposent sur une variété de scénarios de communication (PC à PC, PC à poste, etc.). En outre, cette technologie s'est transformée en un outil de communication via internet en intégrant des outils d'interface pour les réseaux téléphoniques classiques. Elle utilise des protocoles spécialement conçus pour ce type d'applications, comme le protocole de transport en temps réel (RTP), qui est utilisé conjointement avec les protocoles de signalisation, la norme H323 et le protocole d'initiation de session (SIP).
La possibilité de combiner les réseaux téléphoniques et informatiques entraîne une réduction importante de la logistique nécessaire à la gestion des deux réseaux, ainsi qu'une réduction des coûts des deux communication. Cependant, les caractéristiques techniques de cette nouvelle technologie ne sont pas toujours bien analysées.
Les problèmes de gestion de la bande passante internet, de qualité audio, de sécurité, etc, ne sont que quelques-unes des contraintes qui doivent encore être résolues.

Problématique

La plupart des entreprises aujourd'hui utilisent encore la téléphonie classique basée sur le réseau téléphonique commuté (RTC) dans leurs communications bien qu'elles soient dotées de réseaux informatiques.
Ce type de réseau existe depuis près d'un demi-siècle maintenant donc les pannes se multiplient en raison de l'ancienneté de la technologie, et les équipements nécessaires au fonctionnement du réseau RTC sont plus difficiles d'accès qu'auparavant. De plus l'équipement, l'installation et la maintenance de ces réseaux entraînant un coût d'installation et d'exploitation très élevé. Cette situation qui semblent minimiser plusieurs managers diminue le budget de fonctionnement de ces entreprises. Le problème de coûts élève de communication est d'autant plus important que le transport des données en entreprise est vital pour cette dernière.
Le but est de rechercher la meilleure solution qui permettrait une réduction des coûts de communication en entreprise. L'idéal serait de fusionner tous ces moyens de communication dans une solution intégrée qui offrirait toutes les garanties des services de communications cités ci-dessus. Pour y parvenir, la communication sur IP apparaît comme une solution prometteuse qu'il conviendrait d'explorer.

Objet de l'étude

L'objectif de notre étude est de savoir comment utiliser la téléphonie sur IP pour minimiser les coûts d'installation et d'exploitation tout en optimisant la communication en entreprise. D'autre part, nous allons ésseyer de sécuriser notre réseaux et notre serveur VoIP pour atteindre les objectif de la sécurité informatique.

Structure du mémoire

Ce mémoire est composé de quatre chapitres :

Le premier chapitre intitulé " Généralités sur la VoIP et Asterisk " nous permet d'avoir une idée sur la téléphonie IP et la VoIP, et comprendre les architectures, les différents équipements et les protocoles de transmission sur ces réseaux.
En plus de ça, nous avons fait une présentation du serveur " Asterisk ", plus ces fonctionnalité et son architecture.
Le deuxième chapitre intitulé " Vulnérabilités et attaques contre la VoIP " est consacré à une brève étude sur les attaques sur la VoIP et quelques solutions de sécurisation.
Le troisième chapitre " Présentation de l'organisme d'accueil " présente l'entreprise qui nous a accueilli pour faire notre stage pratique, nous avons donné des informations sur cette entreprise, nous avons cerné quelques les problèmes de réseaux, et proposé des solutions.
Le dernier chapitre présente une étude technique et la mise en place d'une solution VoIP basée sur le serveur Elastix avec le protocole SIP sécuriser.

Chapitre 1

Généralités sur la voix sur IP et Asterisk

1.1 Généralités sur la Téléphonie IP

1.1.1 Introduction

La Voix sur IP est un terme qui fait référence aux protocoles, logiciels et matériels, qui permettent d'envoyer des médias par paquets. L'importance de la voix IP dans les entreprises a augmenté. L'objectif est d'intégrer avec succès les réseaux de données IP et les réseaux téléphoniques existants. La VoIP est une bonne solution en termes d'intégration, de fiabilité et de coût. Dans ce chapitre, nous allons présenter le fonctionnement de la voix sur IP, ses protocoles, ainsi que les éléments nécessaires à sa mise en œuvre. Nous donnerons également une brève présentation sur le logiciel Asterisk.

1.1.2 Quelques définitions

a) Téléphonie sur IP :

TOIP (Telephony Over Internet Protocol) est une technologie qui vise à standardiser divers outils et canaux de communication. Plus précisément, il s'agit d'une technologie qui vise à transporter le trafic vocal et téléphonique sur les réseaux IP, et donc sur Internet[7].

b) Voix sur IP :

VoIP est l'abréviation de Voice over Internet Protocol ou la Voix sur IP. Il s'agit d'une technologie qui permet à la voix d'être transmise via les réseaux numériques ou Internet[7].

1.1.3 Téléphonie classique vs Téléphonie sur IP

a) **Téléphonie classique :** Le service téléphonique traditionnel utilise un réseau téléphonique commuté ou un réseau pour circuits de commutation (PSTN). Chaque communication a son propre circuit logique. Une ressource réservée utilisée lors de la communication. Les informations diffusées au cours d'une même session de communication parcourent le même chemin prévu jusqu'à leur destination.

b) **Téléphonie sur IP :** La téléphonie IP utilise un réseau à commutation de paquets ou un réseau IP. Le message ou l'information à envoyer est découpé en petits morceaux appelés paquets. Chaque colis est livré indépendamment des autres sur le réseau[14]. De plus, la tarification ToIP se généralise gratuitement.

1.1.4 Principe de fonctionnement de la VoIP

L'idée est de numériser la voix analogique et de l'acheminer en paquets IP sur Internet ou tout autre réseau IP[2]. Le processus de communication VoIP est illustré à la Figure I.1 et comprend les étapes suivantes :

1. **Acquisition :** La première étape consiste à utiliser un périphérique pour détecter la voix.
2. **Numérisation (conversion A/D) :** convertir le signal analogique en signal numérique à l'aide d'un convertisseur A/N (analogique/numérique).
3. **Compression :** Consiste à réduire la taille physique des données numériques selon une norme de compression prédéterminée.
4. **Habillage des en-têtes :** Le signal qui a été numérisé et compressé sera ensuite décompressé. Lors de l'ajout d'en-têtes, il est important de considérer l'ordre dans lequel le paquet sera ré-assemblé et le type de trafic de synchronisation.
5. **Emission et transport (transmission et propagation) :** Il s'agit de la transmission de paquets IP au destinataire prévu via des protocoles de routage.

6. **Réception :** recevoir les informations diffusées lors de la transmission.
7. **Conversion D/A :** C'est l'étape inverse de la numérisation.
8. **Restitution :** Résultat final l'écoute de la voix.

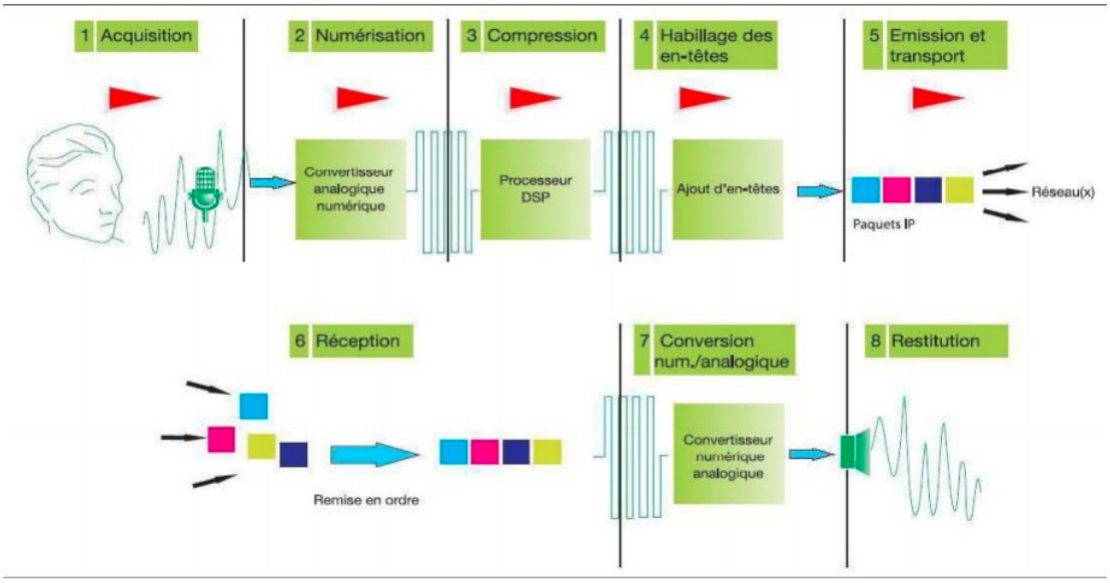

FIGURE 1.1 – Processus de communication vocale sur un réseau IP

[13]

1.1.5 Architectures VoIP

La téléphonie IP peut être déployée dans une entreprise de plusieurs manières, selon le niveau de convergence requis et compte tenu de certaines mesures (budget, équipement,etc.)[10][7].

a) Architecture de la téléphonie classique d'entreprise : Dans une conception téléphonique traditionnelle, tout le trafic vocal et de signalisation est acheminé via le PABX à chaque emplacement pendant la durée de l'appel. Cette conception est la plus répandue dans la grande majorité des environnements "professionnels". La conception de téléphone IP suivante doit être comparée aux réseaux existants à envisager pour le développement dans le cadre de la transition vers le déploiement entièrement IP, comme le montre la figure 1.2 :

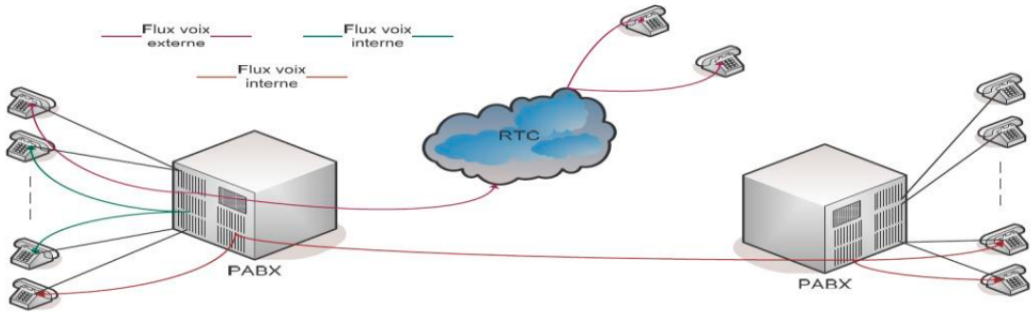

FIGURE 1.2 – Architecture du réseau de téléphonie classique d'entreprise.

[3]

b) Architecture VoIP d'entreprise (architecture hybride : L'avantage de cette approche est qu'elle ne repose pas sur l'infrastructure existante tout en profitant des avantages de la voix sur IP pour la communication de site à site. Cette option peut être mise en œuvre en ajoutant un boîtier "Voice Gateway" à l'extérieur du PABX ou en utilisant la fonction de passage (sous forme de carte) incluse dans les routeurs de nouvelle génération, comme le montre la figure 1.3 :

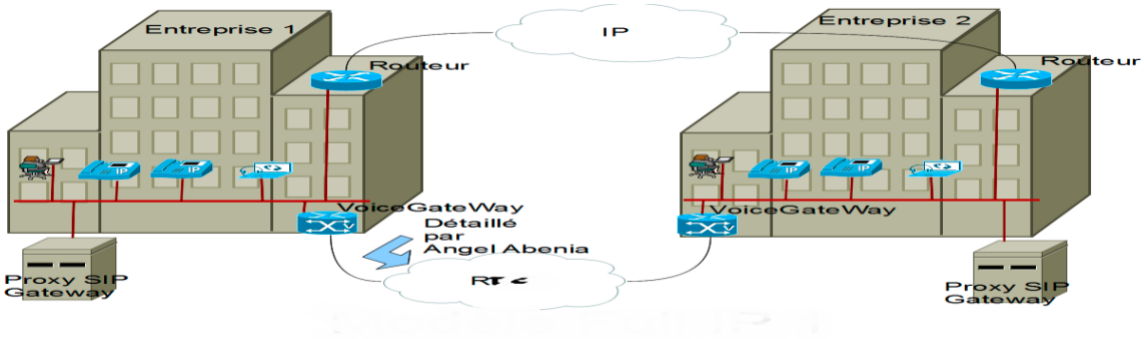

FIGURE 1.3 – Architecture VoIP d'entreprise (architecture Full-IP).

[9]

c) Architecture VoIP d'entreprise (architecture Full-IP : Une conception entièrement IP, plus grande qu'un système hybride, permet une migration complète vers la téléphonie IP pour l'ensemble de l'organisation, y compris les terminaux téléphoniques des abonnés. Ce déménagement a apporté plusieurs avantages en jetant les bases d'une convergence des systèmes informatiques et des systèmes téléphoniques d'entreprise. Lors des communica-

tions inter-sites ou intra-sites, seuls les flux de signalisation transitant par le gatekeeper seront autorisés à accéder au RTC. Afin de réduire les investissements, l'entreprise peut également externaliser la fonction de "gatekeeper/voix gateway" à un fournisseur de centre IP. Après cela, l'intelligence sera expulsée du cœur du réseau, Comme le montre la figure 1.4 :

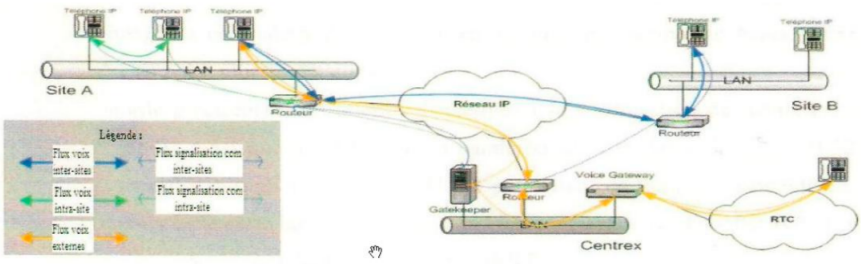

FIGURE 1.4 – Architecture VoIP (architecture type centrex).

[3]

1.1.6 Protocoles de signalisation

Il y a deux types de protocoles VoIP : les protocoles de signalisation et de connexion client (H323, SIP) et les protocoles de transport de données multimédia (RTP, RTCP).

1.1.6.1 Protocole H.323 :

C'est un protocole standard de communication qui définit un ensemble de protocoles pour fournir des sessions de communication audiovisuelle. Il est utilisé pour traiter la signalisation et l'envoi de données audio et vidéo sur internet. L'UIT (Union Internationale des Télécommunications) a développé ce protocole[2].

1. **Composants de réseaux H.323**

   L'infrastructure H.323 repose sur quatre éléments principaux :

   — **Les terminaux :** Un téléphone IP connecté directement au réseau Ethernet de l'entreprise ou un PC avec une application compatible H.323 installée.

   — **Les passerelles (Gateway) :** Assurent l'interconnexion avec les autres réseaux.

- **Les portiers (Gatekeeper) :** Selon H323, le Gatekeeper est le point d'entrée dans le réseau pour un client H.323.
- **Les unités de contrôle multipoint (MCU) :** Il permet aux clients de se joindre à des sessions de conférence téléphonique de données.

2. **Avantages de H323 :** Parmi les avantages, nous citons :
   - **Interopérabilité :** H323 permet aux utilisateurs de ne pas se soucier de la façon dont leurs communications sont effectuées.
   - **Support multipoint :** le protocole H.323 permet des conférences téléphoniques multipoints sans avoir besoin d'un dispositif de contrôle spécialisé.
   - **Support multicast :** H.323 prend en charge la multidiffusion dans les conférences multipoints.
3. **Inconvénients de H323 :**
   - Les documents sont difficiles à obtenir car l'UIT exige un paiement pour accéder aux développements les plus récents de cette technologie.
   - comprend plusieurs choix qui peuvent être mis en œuvre de diverses manières par les constructeurs, posant des problèmes d'interopérabilité.

1.1.6.2 Protocole SIP

Session Initiation Protocol (SIP) est un protocole de signalisation utilisé pour l'ouverture, la maintenance, la modification et la fermeture de sessions utilisateur interactives pour les communications voix et vidéo, ainsi que plus généralement pour toutes les communications multimédias[5]. Ce protocole se distingue principalement par les éléments suivants :

- **Compatibilité :** Il est conçu pour fonctionner avec une variété d'applications, y compris les jeux vidéo, les appels téléphoniques et la réalité virtuelle, la messagerie instantanée, la vidéo-conférence.
- **Modularité :** Il a été créé de manière indépendante de la surface de transport. En conséquence, TCP et UDP sont responsables de la transmission des messages SIP.

— **Simplicité :** Il utilise un langage textuel assez similaire aux protocoles HTTP et SMTP, ce qui facilite son intégration à Internet. Relativement peu de ressources de traitement sont utilisées dans sa mise en œuvre.

1. **Éléments d'une architecture SIP** Le protocole SIP repose entièrement sur une conception logicielle. Elle est soutenue par divers serveurs qui communiquent entre eux et partagent la charge du réseau. Elle est organisée autour de cinq composants :

   — **UA (User Agent) :** Il est composé de deux parties : le composant client, appelé UAC (User Agent Client), qui est en charge de l'envoi des requêtes, et la partie serveur, appelée UAS (User Agent Server), qui traite les demandes.

   — **Serveur d'enregistrement :** Il gère les requêtes REGISTER envoyées par le terminal afin de communiquer la position actuelle de l'utilisateur tout en gérant la mobilité de l'utilisateur.

   — **Serveur de localisation :** Le serveur de localisation complète le serveur d'enregistrement en permettant de déterminer la localisation de l'abonné. Ce serveur dispose de la base de données de tous les abonnés qu'il gère.

   — **Serveur de redirection :** Le serveur de redirection fait le lien entre le terminal client et le serveur de localisation. Le terminal client demande à ce que le serveur de localisation soit contacté afin de déterminer la position courante d'un utilisateur.

   — **Serveur proxy :** Parfois appelé serveur mandataire, Un serveur proxy est en charge du routage des communications SIP. Il existe deux types distincts de serveurs proxy :

   - **Proxy statefull :** qui conserve l'état des connexions au fil des sessions.

   - **Proxy stateless :** qui transmet les messages indépendamment les uns des autres sans conserver l'état des connexions. La vitesse et le poids du proxy stateless sont supérieurs à ceux du proxy statefull.

2. **Adressage SIP**

   C'est l'une des étapes essentielles qui a pour but de localiser les utilisateurs au sein d'un réseau. Les utilisateurs doivent pouvoir être identifiés de manière unique afin d'être localisés[5]. Voici la forme que prend une adresse SIP :

sip : identifiant[:mot-de-passe]@serveur[?paramètres] On distingue dans cette adresse plusieurs parties. Celles qui se trouvent entre crochets sont optionnelles.

sip : le protocole utilisé pour la communication.

identifiant : Cet identifiant doit être unique(le nom d'identification de l'utilisateur).

mot-de-passe : Ce composant facultatif permet une identification au niveau du serveur.

paramètres : Ce composant est également facultatif, donnant à l'utilisateur la possibilité de spécifier plus d'informations ou de modifier le comportement par défaut. Voici un exemple d'adresse SIP : **sip :samy@192.168.10.15.**.

3. **Messages SIP** Le protocole SIP repose sur un modèle Requête/Réponse. Nous allons maintenant examiner les principaux types et formats de messages SIP, qui sont des réponses ou bien des demandes[5] :

   — **Requêtes SIP :** Les principaux types et formats du message SIP :

   • **INVITE :** Pour l'ouverture d'une session.

   • **ACK :** Cette requête confirme que le terminal appelant a reçu une réponse finale à une requête invite.

   • **OPTIONS :** Elle permet d'interroger un serveur SIP, pour initier une communication.

   • **BYE :**Pour terminer l'appel.

   • **CANCEL :** annule un INVITE, la méthode CANCEL doit être suivie d'un message ACK.

   • **REGISTER :** permet d'enregistrer l'adresse IP auprès d'un serveur d'inscription.

   • **UPDATE :**pour la mise à jour des paramètres de la session.

   — **Réponses SIP :**

   Il existe six classes de réponse et donc six codes d'état, qui sont représentés par le premier chiffre :

   • **1xx** =Message d'information.

   • **2xx** =Message de succès.

- **3xx** =Message de redirection
- **4xx** =Erreur du client.
- **5xx** =Erreur du serveur.
- **6xx** =Echec général.

4. **Scénarios de communication :**

— **Enregistrement d'un terminal :**Lorsqu'un terminal se connecte à un réseau, la première chose qu'il fait est d'envoyer une requête "Register" à un serveur d'enregistrement pour l'avertir de sa présence.Le serveur de localisation stocke une entrée dans sa base de données avec l'adresse IP de l'appareil de l'utilisateur et le numéro de port de l'application SIP, qui relie l'identité d'un utilisateur individuel à son emplacement à l'intérieur du réseau.La figure 1.5 décrit l'enregistrement d'un terminal SIP.

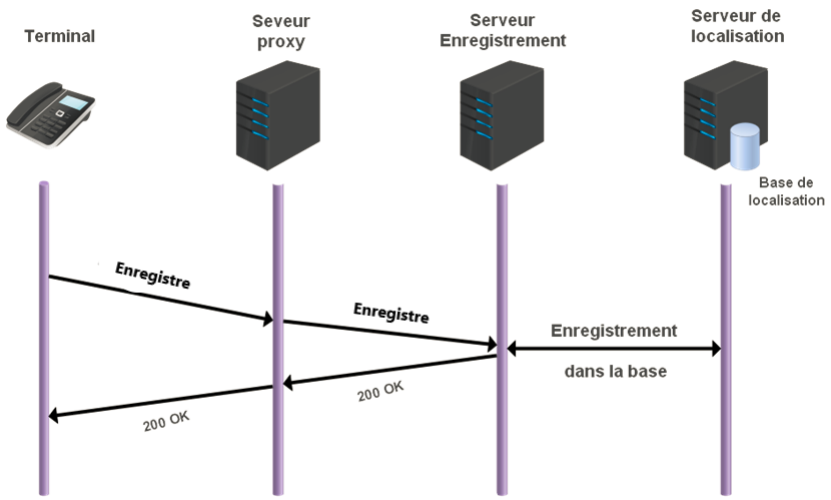

FIGURE 1.5 – Enregistrement d'un terminal SIP.

— **Initialisation d'une communication directe :** Si la personne qui appelle connaît l'emplacement de la personne qu'elle souhaite joindre, une communication directe entre les deux parties est possible. Seules quatre étapes sont nécessaires pour lier les deux utilisateurs, comme le montre la figure 1.6 :

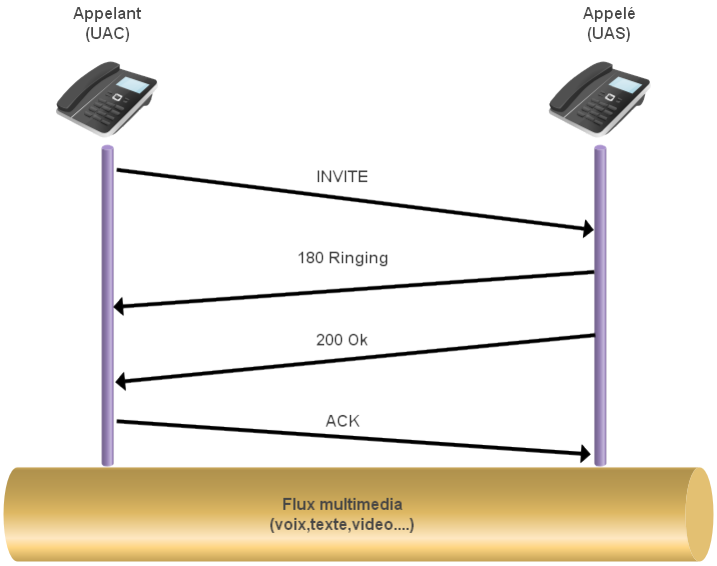

FIGURE 1.6 – Initiation d'une communication directe.

1. L'appelant UAC souhaite contacter l'appelé UAS, pour cela il envoie la requête INVITE.
2. Après avoir reçu ce message, l'appelé renvoie une réponse (180 RINGING).
3. L'appelé accepte la communication et retourne le code d'état 200 OK.
4. L'UAC envoie à l'UAS un message ACK indiquant que l'appel peut commencer.

5. **Avantage et inconvénient du protocole SIP :**
   - Simple à mettre en œuvre, messages écrits en clair.
   - Interopérabilité très bonne grâce à CPL (Call Processing Language) qui utilise XML, il est très facile d'ajouter des services intelligents.
   - possibilité de gestion de la mobilité utilisé pour la téléphonie 3G (UMTS).
   - Pas service supplémentaire de téléphonie.

1.1.7 Protocoles de transport

1.1.7.1 Protocole RTP :

Real time Transport Protocol est un protocole réseau qui gère les flux multimédias, ainsi que le transport en temps réel des données audio et vidéo sur Internet. Il s'appuie sur le

protocole UDP (User Datagram Protocol).
Il est largement utilisé essentiellement pour des appels téléphoniques, la parole numérique ou les applications de visioconférence[6].

1.1.7.2 Protocole RTCP :

Signifie Real Time Transport Control Protocol est un protocole de contrôle qui fonctionne avec le protocole RTP (Real-Time Protocol). C'est l'un des standards de l'UIT, permet de gérer les rapports de qualité de service (QoS) et le contrôle de la session[6].

a) Paquets RTCP : Il existe cinq classes de paquets RTCP : Sender Report, Receiver Report, Source Description, BYE et application (APP)[6].

b) Débit RTCP : Le protocole RTCP ajuste le débit d'envoi des paquets lors d'une session de communication en fonction du nombre de participants. Si ce nombre est très important, RTCP ne pourra pas s'adapter. Le débit maximal de RTCP est de 5% du débit total de la session, dont 25% pour les émetteurs et 75% pour les récepteurs[6].

1.1.8 Avantages et inconvénients de la VoIP

1.1.8.1 Avantages de la voip

— **Réduire les couts :** L'émergence de fournisseurs proposant des appels nationaux et internationaux bon marché a réduit les coûts de communication et permis une communication à faible coût entre les commerciaux.

— **Expansion des services :** Il y a eu une augmentation des services spécifiques à IP, tels que la détection de présence et la détermination si un utilisateur est en ligne ou non. De plus, les services téléphoniques peuvent être intégrés dans les systèmes d'entreprise.

— **Simplification des processus de sélection, d'administration :** Simplification d'exploitation et de configuration, intégration d'applications.

— **Un réseau simultané voix, vidéo et données :** L'utilisation d'un seul transport IP pour gérer trois applications (voix, réseau et vidéo) est simplifiée par l'intégration de la voix comme application supplémentaire dans les réseaux IP.

1.1.8.2 Inconvénients de la VoIP

— Il est impossible de passer un appel urgent par téléphone.

— La qualité de la communication peut être affectée par le niveau de service Internet.

— Les utilisateurs courent le risque de perdre l'accès au réseau téléphonique si un virus infecte un serveur VoIP. L'infection peut également se propager à d'autres ordinateurs liés au système.

1.2 Solution VoIP basée sur Asterisk

Il existe plusieurs logiciels qui peuvent être utilisés pour mettre en œuvre une solution VoIP dans une entreprise, que ce soit dans le monde des logiciels open source ou propriétaires.

1.2.1 Présentation d'Asterisk

Asterisk est un standard téléphonique privé PABX, qui utilise des cartes d'interface téléphonique pour fournir une connexion en temps réel entre des réseaux voix IP et des réseaux téléphoniques traditionnels Asterisk et FreePBX peuvent être trouvés dans une variété de distributions d'applications, dont les plus populaires sont Elastix et Trixbox[8]. Asterisk sert d'intermédiaire entre la téléphonie VoIP (TDM, SIP, etc.) et les applications (conférence, messagerie vocale, etc.). Ce PBX est construit sur le protocole IP. Par conséquent, les conversations et les paquets commutés sont transmis via une variété de protocoles de voix sur IP (SIP, H.323, ADSI, MGCP).

1.2.2 Caractéristiques d'asterisk

Asterisk offre toutes les fonctions d'un PBX et ses services associés[4] :

— La messagerie vocale.

— La gestion des listes d'attente,

— Le stockage et la livraison des appels.

— Transfert, filtrage, enregistrement des appels.

— Messagerie vocale.

— Gestion des conférences.

— Authentification des utilisateurs appelants.

— Les mails vocaux.

— La musique d'attente

1.2.3 Protocoles d'asterisk

Ces protocoles gèrent la communication et le transport entre les correspondants :
H.323 : Et il est rarement utilisé car il est remplacé par SIP.
SIP : Il est beaucoup utilisé pour la voix sur IP, il est apprécié pour sa simplicité.
IAX : Il est développé par Digium pour permettre le dialogue entre serveurs Asterisk. Il est plus simple et rapide que SIP.

1.2.4 Architecture d'Asterisk

1.2.4.1 Vue d'ensemble

Asterisk est composé d'un nœud central pour la communication ainsi que de quatre API (interfaces de programmation d'applications) pour gérer les formats de fichiers et les codecs ainsi que pour moduler le chargement des applications téléphoniques.[8]

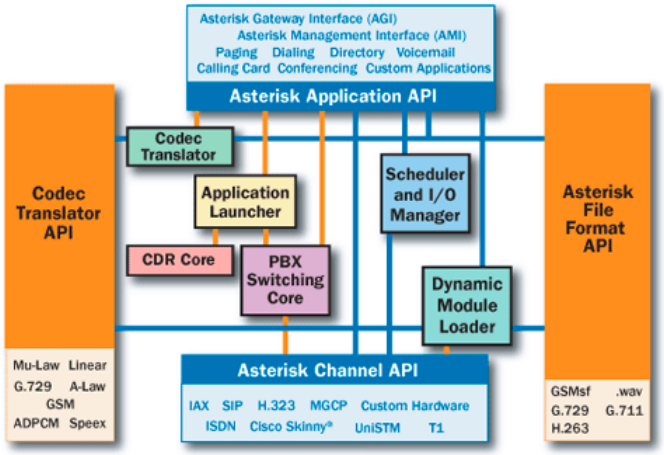

FIGURE 1.7 – Architecture interne d'Asterisk

[8]

1.2.4.2 Fonctionnement interne d'asterisk

1. **nœud central pour la communication :**

   • **Le PBX de banlieue :**Le noeud de communication est construit de manière transparente sur les appels qui entrent via diverses interfaces matérielles et logicielles.

   • **Leader d'applications :**les applications qui fournissent des services pour des programmes.

   • **Le Transcodeur :**Les modules de codec sont utilisés pour coder et décoder les formats de compression audio utilisés dans l'industrie des télécommunications.

   • **Planificateur et Manager d'entrées/sorties :** gère la gestion du système pour des performances optimales à tous les niveaux.

2. **Les APIs (Application Programmming Interface) :**

   • **Canal API :**contrôler le type de connexion utilisé par un appelant.

   • **Application L'API :** permet l'exécution de plusieurs tâches afin de remplir diverses fonctions (la liste des répertoires, la messagerie vocale...).

   • **Transcodeur API :** prendre en charge différent normes de codage.

   • **L'API de formatage de fichier :**permet la lecture et l'écriture de divers formats de fichiers afin que les données puissent être stockées dans le système de fichiers.

1.3 Conclusion

Dans ce chapitre, nous avons présenté le principe de la voix sur IP, ses avantages, ses protocoles. Nous avons également étudié le serveur asterisk pour cette technologie de communication.

Dans le chapitre qui suit, nous allons aborder les aspects liés aux vulnérabilités de la VoIP, ainsi que les mesures de sécurisation de services.

Chapitre 2

Vulnérabilités et attaques contre la VoIP

2.1 Introduction

Dans ce chapitre, nous allons décrire dans la voix IP les attaques et les vulnérabilités au niveau protocolaire, applicatif et système de d'exploitation et détaillerons certaines d'entre elles. Ensuite, nous décrirons les meilleures techniques pour sécuriser les conversations Voix sur IP.

2.2 Vulnérabilités de l'infrastructure

Une application VoIP se compose de serveurs, de passerelles et de téléphones IP. Chaque composant est accessible sur le réseau. Chacun a un processeur qui exécute un logiciel qui peut être utilisé comme point d'entrée pour une attaque plus sophistiquée.

— **Faiblesses de configuration des dispositifs VoIP :** Si les services disponibles ne sont pas configurés avec un mot de passe, un attaquant peut obtenir un accès non autorisé à cet appareil. Les services SNMP (Simple Network Management Protocol) fournis par ces dispositifs peuvent être vulnérables aux attaques de reconnaissance ou de débordement.

De nombreux appareils VoIP sont configurés pour télécharger périodiquement des fichiers de configuration à partir d'un serveur. Un attaquant pourrait détourner ou confondre cette connexion, obligeant l'appareil à télécharger un fichier de configuration malveillant au lieu d'un fichier légitime[16].

— **Le téléphone IP :** Un pirate peut compromettre un système téléphonique IP, tel qu'un téléphone IP, un logiciel téléphonique et d'autres programmes. Dans la plupart des cas, il obtient des autorisations lui permettant de contrôler toutes les fonctions de l'appareil.

Le dernier point (téléphonie IP) peut être interrompu soit à distance, soit en accédant physiquement à l'appareil. Les pirates ont la possibilité de modifier les éléments de fonctionnement de ces appareils : la base du système d'exploitation peut être modi-

fiée. Des micros logiciels modifiés de manière malveillante peuvent également être téléchargés et installés[16].

— **Le serveur VoIP :** Un autre composant vulnérable du réseau est le serveur du fournisseur de réseau IP, qui peut être la cible d'attaques visant à perturber l'ensemble du réseau.

L'attaquant a un contrôle total sur les informations de signalisation pour différents appels, lui permettant de modifier tout paramètre lié à l'appel. Comme le serveur de téléphonie IP est installé sur le système d'exploitation, il est vulnérable aux logiciels malveillants[16].

— **Vulnérabilités du système d'exploitation :** Les éléments VoIP tels que les téléphones IP, les gestionnaires d'appels, les passerelles héritent des mêmes vulnérabilités que le système d'exploitation sur lequel ils fonctionnent.

La majorité de ces vulnérabilités sont liées à un manque de sécurité lors de la phase de développement initiale du système. Les débordements de tampon sont l'une des vulnérabilités de sécurité les plus graves des systèmes d'exploitation. Il permet à un attaquant de prendre le contrôle complet du système.

Quel que soit le degré de sécurité d'un programme VoIP, il est compromis si le système d'exploitation sous-jacent est compromis[15].

2.3 Attaques contre les protocoles VoIP

2.3.1 Attaques de déni de service (DoS)

Une attaque par déni de service consiste à inonder un serveur Web de requêtes jusqu'à ce qu'il ne puisse plus les traiter et cesse de répondre. L'attaquant peut saturer le réseau de l'entreprise, en perturbant les systèmes de communication et d'information internes et externes.

Les lacunes du service se manifestent de diverses façons. Les plus courant sont ceux qui tentent d'utiliser toute la bande passante disponible ou abusent des problèmes TCP/IP in-

hérents, empêchant ainsi les tentatives de communication[12].

Les différentes formes d'attaque de déni de service sont :

a) Attaque par la méthode de CANCEL : Cette forme d'attaque ciblée par déni de service surveille l'activité du proxy SIP et attend un appel entrant d'un utilisateur spécifique. Après la réception de la requête INVITE par l'utilisateur, l'attaquant envoie une requête CANCEL, cette requête provoque une erreur sur l'équipement appelé et annuler l'appel[12].

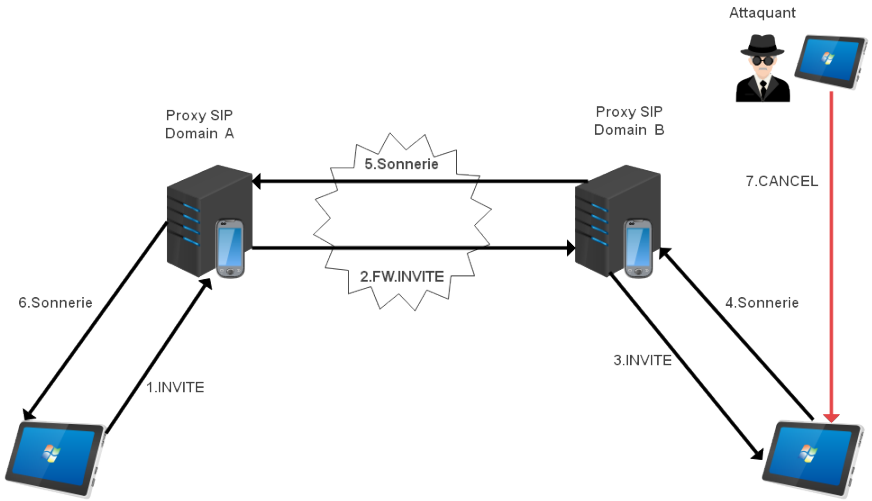

FIGURE 2.1 – Attaque Dos avec la méthode CANCEL

La figure (2.1) décrit un scénario d'attaque Dos utilisant la méthode CANCEL, l'appelant initie l'appel, envoie une invitation (1) au proxy SIP auquel il est affecté.

Le proxy du domaine A achemine la requête (2) au proxy domaine B.

après cela ce dernier achemine la requête INVITE (3) qui arrive enfin à la destination, lorsqu'il reçoit l'invitation (4).

Ces informations sont transmises à l'appareil demandeur. L'attaquant qui surveille l'activité du proxy SIP du domaine B envoie une requête CANCEL (7).

Cette demande annulera la requête en attente (l'INVITE), l'appel n'a pas lieu.

b) Attaque par la méthode BYE : Les utilisateurs sont la cible de l'attaque de la méthode BYE. Une interruption est faite par l'attaquant, qui émet également un BYE. Pour mener à bien cette attaque, le pirate écoute le trafic et rassemble les informations nécessaires pour créer un BYE frauduleux correspondant à la session qui est injectée dans le réseau. Puisque le BYE n'est pas authentifié, la personne qui reçoit l'information l'exécute.

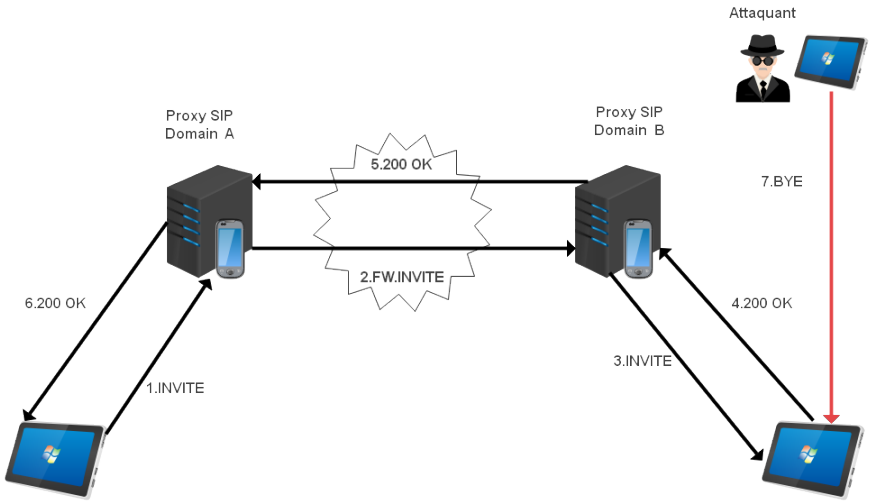

FIGURE 2.2 – Attaque Dos avec la méthode BYE

C'est le même scénario qu'à la figure précédente, sauf que dans ce cas, l'attaquant attend qu'une réponse affirmative acceptant l'invitation (4) soit envoyée par la destination avant de lancer son attaque. Après avoir reçu le 200 OK, l'attaquant envoie une demande BYE à l'un des participants ou aux deux, mettant ainsi fin à l'appel sans permettre aux utilisateurs de communiquer.

2.3.2 Sniffing

C'est une méthode utilisée pour espionner le trafic d'un système en voyant et en copiant tous les paquets non chiffrés qui sont envoyés sur le réseau cible.
Cette attaque peut conduire à l'usurpation d'identité et à la divulgation d'informations confidentielles. Il permet même aux pirates expérimentés d'accéder aux données via les systèmes VoIP, ces informations peuvent être utilisées pour lancer des attaques sur d'autres systèmes[11].

2.3.3 Attaque de l'homme au milieu

L'expression "Man-in-the-Middle" fait référence à l'homme du milieu. Trois acteurs sont impliqués dans cette attaque : le client, le serveur et l'attaquant. Le but de l'attaque est de faire en sorte que le client et le serveur semblent agir différemment l'un de l'autre. Ainsi, il devient l'homme de l'environnement. Cela permet de surveiller tout le trafic réseau entre les clients et les serveurs et même de le reprendre afin de collecter des données[13].

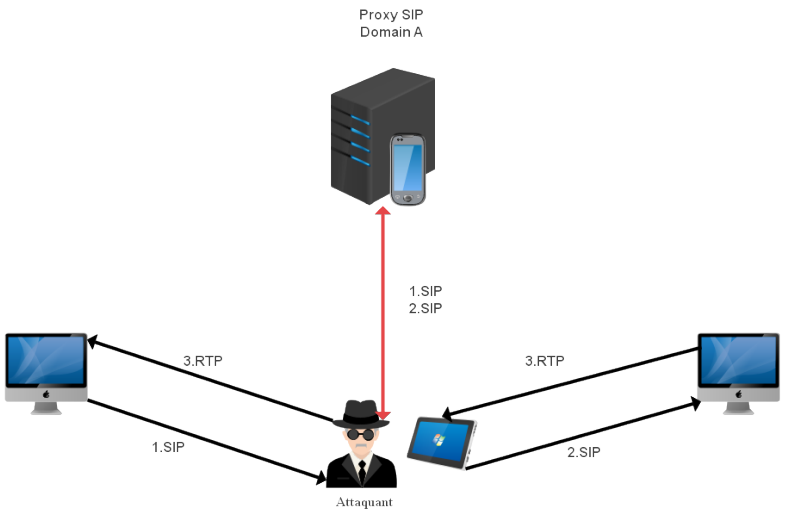

FIGURE 2.3 – Attaque de l'homme au milieu

2.3.4 Attaque par suivi des appels

Cette attaque, également connue sous le nom de call tracking, se produit au niveau du réseau LAN et cible les composants (téléphones logiciels/téléphones). Son objectif est de savoir qui communique et quand la conversation a lieu. L'attaquant doit obtenir les messages INVITE et BYE en écoutant le réseau et en déterminant qui communique, à quelle heure et pendant combien de temps[12].

2.3.5 Injection des paquets RTP

Cette attaque vise à perturber une conversation en ciblant l'enregistrement du serveur. L'attaquant doit pouvoir écouter le réseau afin d'enregistrer les communications et les horodatages des paquets RTP pour mener à bien cette attaque. De plus, il doit pouvoir insérer des messages RTP qu'il a générés avec des horodatages modifiés[12].

2.3.6 Spam

Il existe trois formes de SPAM [12] :

— **Call Spam :** Ce type de spam est décrit comme un grand nombre de tentatives d'ouverture de session non sollicitées. Si l'appel est établi, le programme génère un ACK, répond à une annonce précédemment enregistrée, puis met fin à l'appel.

— **IM (Instant Message) Spam :** Il est décrit comme un grand nombre de communications inattendues et urgentes. La majorité des spams de messagerie instantanée sont transmis via des requêtes SIP.

— **Présence 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.

2.3.7 Détournement d'appel (CALL HIJACKING)

Consiste à dévier un appel entrant. De nombreux fournisseurs de services VoIP utilisent Internet comme interface permettant aux utilisateurs d'accéder à leurs systèmes téléphoniques. Grâce à cette interface en ligne, un utilisateur vérifié peut modifier les paramètres de ses transferts d'appels. Bien que cela puisse être utile, mais un utilisateur malveillant pourrait utiliser la même méthode pour lancer une attaque[14].

2.4 Technique de sécurisation

2.4.1 Sécurisation de l'application

Plusieurs techniques peuvent être utilisées pour sécuriser l'application,Nous citons :

— L'utilisation d'une version stable qui inclut les mises à jour les plus récentes recommandées par le fournisseur pour les parties client et serveur.

— La non installation de softphones sur le serveur.

— La non utilisation de la configuration par défaut, qui manque complètement de défenses contre les attaques.

— La création d'un environnement de test dans lequel les mises à jour logicielles sont testées avant de les installer en production[14].

2.4.2 Sécurité au niveau du système d'exploitation

Il est essentiel de sécuriser le système sur lequel le serveur VoIP est implémenté. Pour le protéger, certaines mesures de sécurité doivent être mises en place, notamment :

— L'utilisation d'un système d'exploitation fiable lors de l'installation des mises à jour les plus récentes. Les nouvelles versions continuent d'avoir des erreurs et des défauts qui doivent être corrigés.

— L'utilisation d'un mot de passe composé de plusieurs combinaisons de lettres, de chiffres et de ponctuation.

— L'augmentation de la sécurité du système d'exploitation en installant des correctifs qui améliorent la sécurité globale du noyau.

— Suppression de tous les programmes, logiciels ou éléments inutiles qui pourraient être utilisés comme cible d'une attaque pour accéder au système[14].

2.4.3 Sécurisation au niveau des protocoles

a) Installer un pare-feu : Si un pirate réussit à se connecter à un réseau sans fil, il peut théoriquement lancer une attaque ARP sur tous les sites de son sous-réseau.
Cependant, les pare-feux sont capables de détecter et de prévenir de telles attaques : L'idée est d'intégrer cette forme de pare-feu dans chaque point d'accès, afin que le pirate ne puisse même pas attaquer d'autres stations connectées au même point d'accès[14].

b) IDS : Pour les systèmes vocaux basés sur IP, il est rare de rencontrer des outils de détection d'intrusion. Le nombre de faux positifs produits par les mesures de flux RTP peut être important. Bien qu'elle permette la détection de dénis de service, la détection d'intrusion aboutit fréquemment à la détection de fraude[14].

c) VoIP VPN : Un VPN VoIP fournit une méthode pour garantir la préservation de la qualité vocale en combinant la technologie vocale IP et la technologie de réseau virtuel privé. Étant donné que la VoIP convertit la voix numérique en un flux de données, la solution VPN VoIP semble être la plus appropriée car elle offre un chiffrement des données via des mécanismes de cryptage et permet d'assurer l'intégrité des paquets VoIP[15].

d) Filtrage des adresses MAC : Pour empêcher quelqu'un de se connecter à l'un des ports d'un commutateur, il est possible de surveiller les adresses MAC des appareils connectés à chaque port[14].

2.5 Conclusion

Ce chapitre a décrit les attaques bien connues qui pourraient compromettre la sécurité VoIP, ainsi que les nombreuses contre-mesures qui pourraient être prises. Afin de mieux protéger le réseau VoIP, une stratégie de sécurité forte doit être mise en place car la voix IP devient de plus en plus ciblée.

Dans le prochain chapitre, nous allons présenter l'organisme d'accueil.

Chapitre 3

Présentation de l’organisme d’accueil

3.1 Introduction

Dans ce chapitre, nous allons présenter l'entreprise EXSON TELECOM avec ses différents services ainsi que l'architecture de son réseau informatique et nous allons énumérer les insuffisances et proposer des solutions qui résoudront les anomalies constatées.

3.2 Présentation de l'entreprise

Exson Telecom est une entreprise créée en 2005 par d'anciens agents de EX-SONatite, dont Mr Ouali, diplômé de l'Institut National des Télécommunications d'Oran et exerçant depuis 1989.

L'équipe technique de cette entreprise comptabilise des centaines d'installations dans de grandes entreprises et institutions (sonatrach, banques, sonelgaz, batimétal, anadarko, hôpitaux, hôtels, université, cours, ministères,etc).

Le logo de l'entreprise est sur la figure 3.1 :

FIGURE 3.1 – Logo de Exson Telecom

3.2.1 Situation géographique

Exson Telecom se situe sur deux addresse, une a Taharacht, Akbou, Béjaia et l'autre sur l'avenue RN 26A, Cité Djama, route de l'université, Bejaia.

FIGURE 3.2 – EXSON TELECOM via Google maps.

3.2.2 Objectifs, Missions et activités de l'Entreprise

— **Services de l'entreprise :** Vente, installation et assurance de maintenance des équipements et matériels de télécom et d'informatique, de réseau informatiques et de sécurité électronique.

— **Installation de réseaux et de centrales électriques et téléphoniques :** Lignes de transport d'énergie électrique, postes de transformation de haut, moyenne et basse tension, centraux téléphoniques, ligne et autre infrastructures.

— **Commerce de détail de machines, matériel et mobilier de bureau :** Machines à écrire, à calculer, reproducteurs, appareils à photocopier, duplicateurs, broyeurs destructeurs de documents, caisses enregistreuses y compris leurs accessoires et pièces détachées.

— **Vente au détail de matériel informatique : ordinateurs, périphériques, consommables et accessoires :** Ordinateurs et imprimantes, scanners, logiciels, disquettes, rubans, boites de rangement.

— **Commerce de détail de matériel de télécommunication** Vente d'équipements de radiocommunications toutes bandes et versions confondues.

— **Commerce de détail de tout matériel et équipements liée au domaine de l'électricité et électronique :** Moteurs, transformateurs, génératrices et convertisseurs, fournitures électrique, matériel de distribution.

— **Traitement de données :** Installation de réseaux informatiques. Traitement de données pour les tiers, saisie de données, conversion de fichier.

— **Installation et réparation de matériel de sécurité et protection contre le vol :**
Réparation et entretien de matériel de protection contre le vol et de tous autres système de détection et d'alarme.
Mise en place de système d'alarme.

3.2.3 Produits disponible dans l'entreprise

Le magazin de l'entreprise vend de différents produits de différents marques (cisco,Alcatel-Lucent, Panasonic, LG-Nortel, Samsung, commax, 3com, D-Link, TeleSystem,Fanvil, nexans, coditel, videx. . ..). Parmi ses produits nous avons :

— Produits télécom :
Standards téléphoniques de déférentes capacités, appareil téléphoniques simples, spécifiques et sans fils, télécopieurs (fax), câbles et accessoires téléphoniques, passerelle GSM, batteries de secours.

— Produits informatiques :
Câbles FTP, UTP, Switches, routeurs, armoires de brassage, onduleurs, Pc, imprimantes, prises et accessoires réseaux.

— Produits de sécurités électronique :
Systèmes de vidéo- surveillance, alarmes, interphones, vidéo-phones, câble RG59, fiches BNC

3.2.4 Organigramme général de l'organisme d'accueil

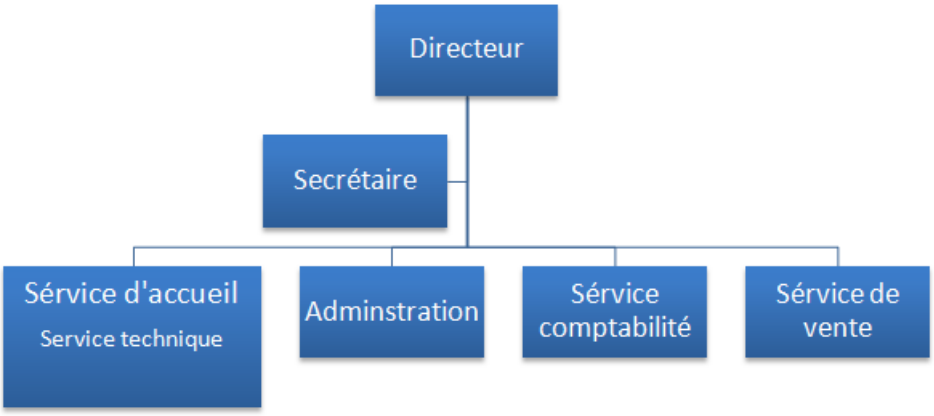

FIGURE 3.3 – Organigramme général d'Exson Telecom

3.2.5 Description de chaque service

A) Service d'accueil :

• **Service technique :** composé d'un technicien supérieur et de deux techniciens ou monteurs avec deux véhicules utilitaire équiper d'outillage nécessaire aux mesures et a la réalisation des services qui sont plusieurs :

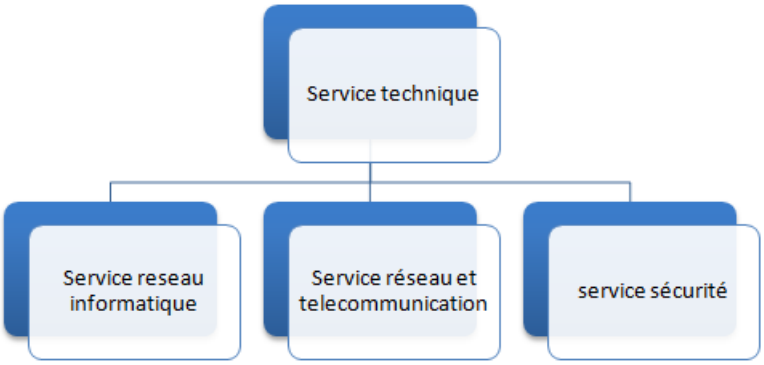

FIGURE 3.4 – Éléments de service technique

— **Service réseau informatique :** Ce service représente toute méthodes afin de partager des ressources ou des informations. En réalité, l'infrastructure du réseau offre un large

éventail de fonctionnalités tant pour les consommateurs que pour les fournisseurs de services, similaire a : limitation du débit, examen, confirmation, surveillance, enregistrement et sécurité du réseau de cette entreprise.

— **Service réseau et télécommunication :** Transmettre des informations en temps réel (synchronisation des informations) sous forme analogique ou numérique.
La plupart de ces services peuvent aider les clients à déterminer leurs besoins en termes d'infrastructure de télécommunications. Voici quelques exemples de services d'infrastructure de télécommunications : pose de fibre optique, emplacement du site de la tour cellulaire, test d'antenne radio, installation d'équipements téléphoniques standards et réseau de données, téléphonie standard.

— **Service sécurité :** Les services d'Exson Telecom comprennent à la fois l'installation et la maintenance de systèmes de sécurité électronique. De plus, elle offre à ses clients des solutions fiables et complètes pour la protection des ressources. Voici les services qu'elle propose : caméras de surveillance, alarme anti-intrusion, détection incendie, pointeuse et Contrôles d'accès, vidéophonie.

B) Service Administration : c'est le service qui s'occupe de la paperasses de l'entreprise ce qui concerne les contrat de travail, les contrats des travailleurs, l'assurance des travailleurs et les équipements de travaille, etc.

C) Service comptabilité : c'est le services qui est occuper par un licencie en économie qui s'occupe de : établissement de devis, facturation, consultation des fournisseurs, passation de commande par email, gestion de stock, retrait et remplissage de cahiers de charges.

D) Service de vente : vend des équipements et matériels de télécom et d'informatique, de réseau informatiques et de sécurité électronique.

3.2.6 Architecture réseaux

L'entreprise dispose d'une architecture multicouches, et pour assurer la communication entre ses différents services, elle connecte son LAN à une connexion FTTH offerte par un

fournisseur d'accès à Internet. L'infrastructure du réseau d'Exson-Telecom est présentée dans le schéma de la figure 3.5 :

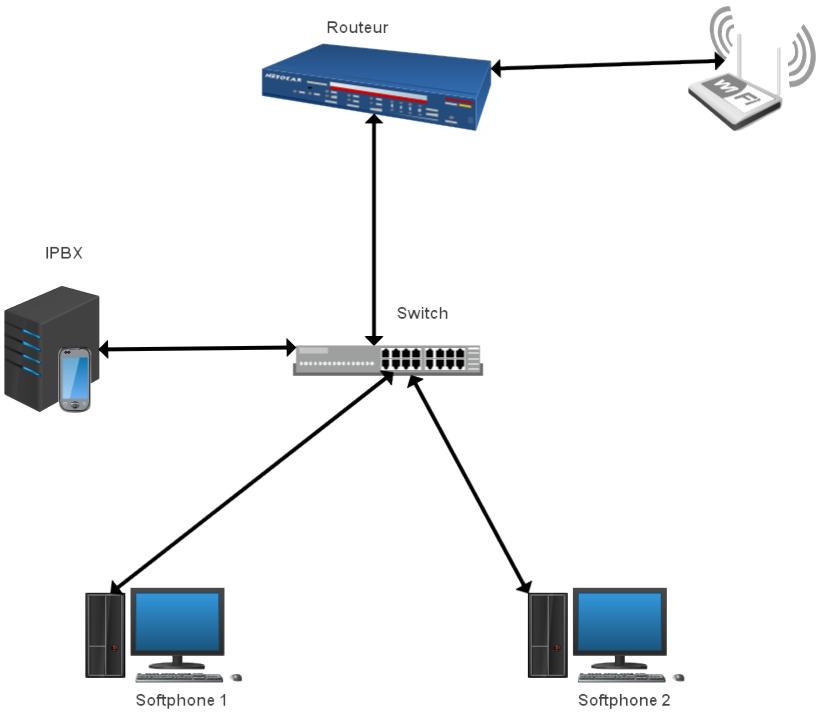

FIGURE 3.5 – Architecture réseaux Exson Telecom

3.2.7 Analyse du parc informatique

Présentation d'environnement matériel et logiciel :

Nom de l'équipement	Le Matériel (hard)	Logiciel (soft)
Modeme	Tp link TD-W9970	Tp Link
Routeur	CISCO 1921 K9	IOS (International Organisation For Standardisation)
Switch	TS-SG1008-P	IOS (International Organisation For Standardisation)
Server	TVS-IPB100	IMS/NGN plateforme
2 PC Bureau	Dell	Windows 7

TABLE 3.1 – Environnement matériel et logiciel

3.3 Problématique et solution

3.3.1 Problématique

Durant notre période de stage au sein du l'entreprise Exson Telecom, nous avons constaté que l'architecture réseaux informatique implémente ne répond pas aux besoins de l'entreprise, et nous avons pu identifier quelques pannes réseau, à savoir :

-Manque d'organisation au niveau de la structure réseaux.

-Les câbles endommagés peuvent provoquer une panne du réseau.

-Sécurité défaillante des données transitant par le réseau.

-Architecture réseaux plate, l'absence d'une segmentation du réseau en vlan ou en sous-réseau favorise l'action des utilisateurs pirates.

-Le dysfonctionnement des applications.

3.3.2 Solutions proposée

Pour répondre aux besoins que nous avons évoqués ci-haut, nous avons proposé l'implémentation d'une solution VoIP, qui est une solution d'entreprise offrant aux agents de EXSON TELECOM, la possibilité d'effectuer les communications vocales sur le réseau unique voix et données, et voire même à l'extérieure en utilisant Internet comme moyen de transport.

Cette convergence des services voix et données sur un réseau unique s'accompagne des avantages liés à la réduction des coûts d'investissement, à la réduction des procédés d'assistance, à l'amélioration de la mobilité des travailleurs et permet aussi de travailler à distance à moindre coût.

L'utilisation de la VoIP conduit à la réduction des coûts d'appels et cela est possible en utilisant un fournisseur de service VoIP pour les appels longues distances et internationaux. Il est très facile interconnecter les systèmes téléphoniques entre bureaux et succursales via internet ou le WAN et de téléphoner gratuitement.

Avec cette technologie, nous n'avons pas besoin d'un câblage indépendant, c.-à-d un réseau informatique à part et un réseau téléphonique aussi à part. Donc, nous avons une seule infrastructure où on peut connecter des téléphones directement à une prise (RJ45) du réseau informatique, peut-être partagée avec un ordinateur adjacent. Les téléphones logiciels peuvent être aussi installés directement sur le PC.

3.4 Conclusion

Après avoir donné un aperçu général de l'activité d'EXSON Telecom dans ce chapitre, nous avons ensuite rencontré un problème qui nous a incité à recherché et à mettre en œuvre une nouvelle conception de réseau sécurisé. Enfin, l'application de la solution proposée fera l'objet du chapitre suivant.

Chapitre 4

Réalisation

4.1 Introduction

Dans ce chapitre nous présentons notre projet avec ces architecture et son environnement de travail et différente configurations de base de réseaux .
En plus de ça nous donnons les techniques de sécurisation convenable à chaque type d'attaque que nous testons.

4.2 Environnement de travail

D'un point de vue logiciel, nous avons travaillé avec de nombreux systèmes d'exploitation, dont Windows 7, kali linux, sur lesquels nous avons installé les outils nécessaires, à savoir :

• **Gns3** (Graphical Network Simulator) est un logiciel libre qui permet de créer et simuler notre architecture[1].

• **Vmware workstation** peut être utilisé pour mettre en place un environnement de test de machines virtuelles[1].

• **Softphone 3cx** est une sorte de logiciel utilisé pour effectuer des appels téléphoniques sur Internet à partir d'un ordinateur plutôt que d'un téléphone.Nous utilisons pour tester nos appels téléphoniques[1].

• **Wireshark** est un analyseur de paquets gratuit et à code source ouvert. Il est utilisé pour le dépannage et l'analyse des réseaux informatiques, le développement de protocoles, l'éducation[1].

FIGURE 4.1 – Outiles de travail

4.3 Architecture proposée

Voici la topologie sur laquelle nous allons travailler. Cette topologie est devisée en trois couches qui sont :

La couche cœur : pour relier les différents segments du réseau entre eux.

La couche distribution : son rôle est de filtrer, router et autoriser ou non les paquets.

La couche d'accès : connecter directement au périphériques du réseau.

• Dans la solution proposé un serveur pfsense et client vpn seront liés.

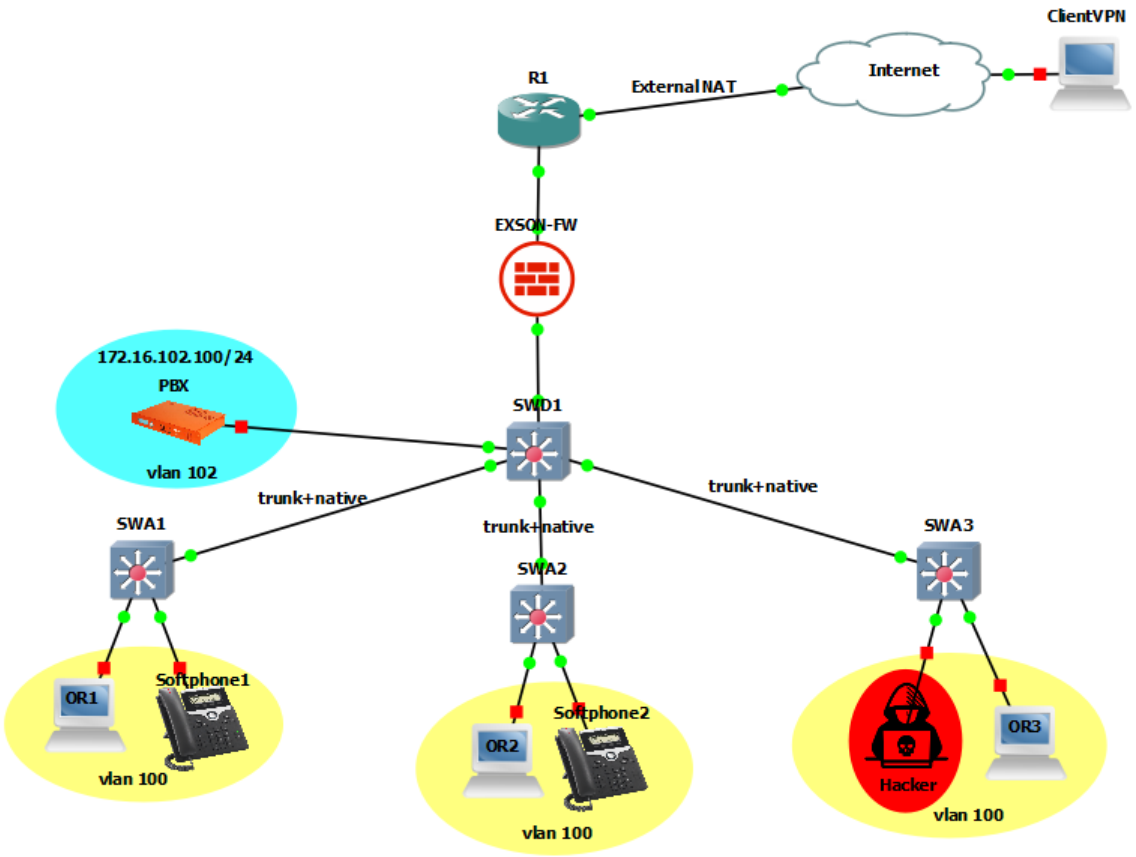

FIGURE 4.2 – Nouvelle architecture réseaux Exson Telecom

Cette topologie comporte quatre VLANs :

• Un premier VLAN pour le trafic de données dénommé "DATA", prenant l'ID 100.

• Un second VLAN pour le trafic de téléphonie IP dénommé "VOICE", prenant l'ID 101.

• Un VLAN serveur qui prend l'ID 102.

• Un Troisième VLAN pour la Gestion des périphériques dénommé "MANAGEMENT", prenant l'ID 103.

4.4 Méthodologie

Le shema de la figure 4.3 montre les étapes suivie pour la réalisation du projet, nous allons les détailler dans ce qui suit :

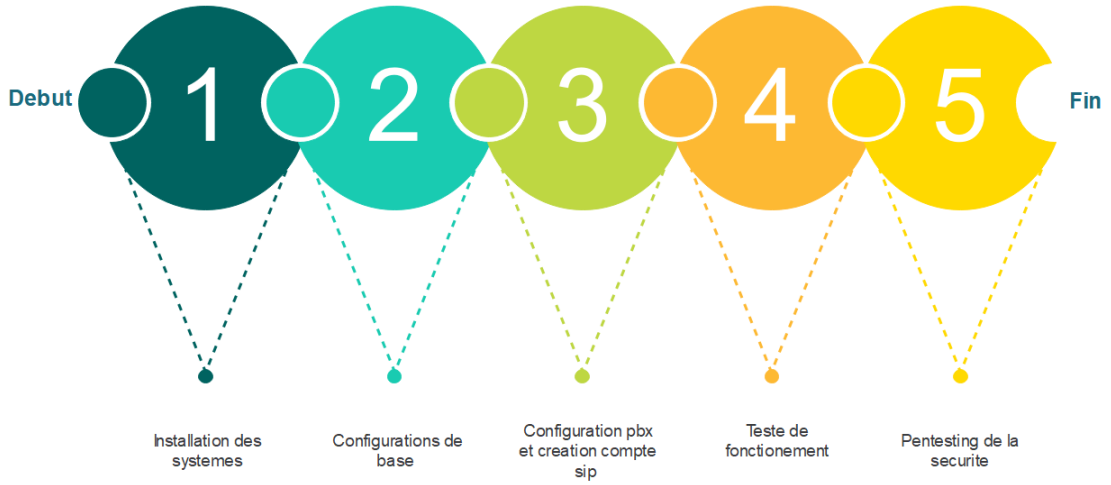

FIGURE 4.3 – Etapes de la méthodologie

4.5 Installation

4.5.1 Présentation du server Elastix

Il s'agit d'un système de communication unifié capable de gérer l'ensemble des besoins de communication d'une organisation. Il possède des fonctionnalités telles que la VOIP (transfert de conversations vocales via un réseau IP), la messagerie électronique et la messagerie instantanée, etc. Un logiciel gratuit permet de construire le PBX idéal pour une entreprise. Elle ajoute également ses propres packages d'utilitaires, ce qui en fait le meilleur logiciel

de téléphonie Open Source actuellement sur le marché. Il est le meilleur choix pour mettre en œuvre un PABX basé sur Asterisk en raison de ces caractéristiques ajoutées à ses solides capacités d'établissement de relations.

4.5.1.1 Installation d'Elastix

FIGURE 4.4 – Démarrage l'installation Elastix

-Après le démarrage, l'écran de la figure 4.4 apparaitra.

-Un petit chargement va se déclancher et nous ramène vers la fenetre figure 4.5.

-Nous sélectionnons la langue et le type de clavier approprié le fuseau horaire.

-Nous définissons les paramètre qui convien la carte reseaux.

-Nous choisissons aussi l'emplacement de l'installation et les mot de passe de sécurite pour le lancement du serveur.

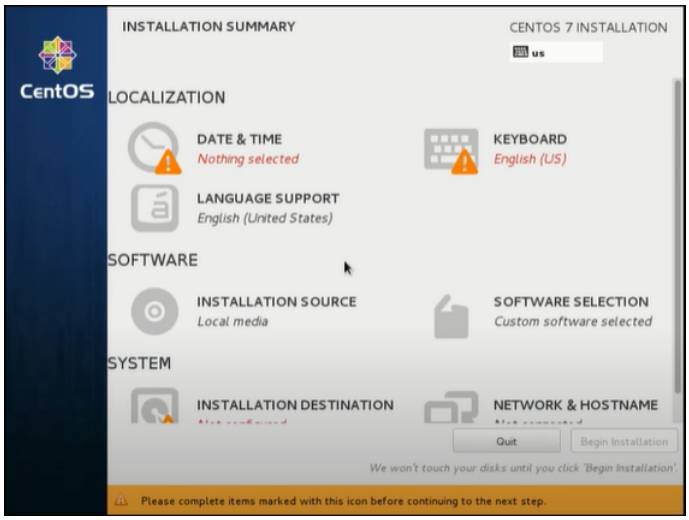

FIGURE 4.5 – Différent paremètre d'avant installation

-Nous entrons le mot de passe qui sera utilisé par l'administrateur Elastix.

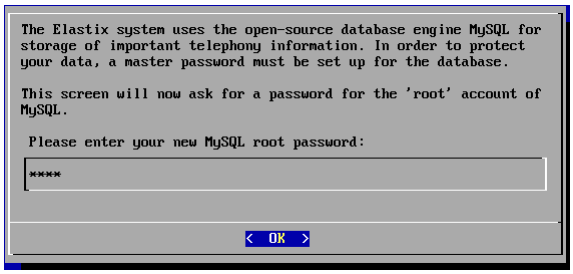

FIGURE 4.6 – Système d'authentification par mot de passe

-Bien sûr il nous demande ensuite la confirmation.

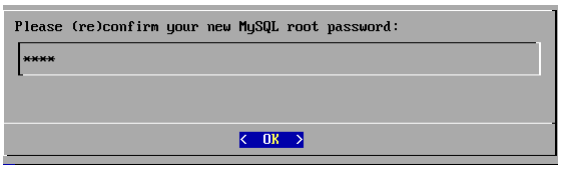

FIGURE 4.7 – Vérification des dépendances

-Ensuite, il nous demandera d'entrer le mot de passe de l'administrateur pour l'interface Web.

FIGURE 4.8 – Spécification d'un mot de passe pour l'administrateur de l'interface Web.

-il nous demande de confirmer le mot de passe. Nous l'indiquons à nouveau et nous validons enfin avec la touche entrée.

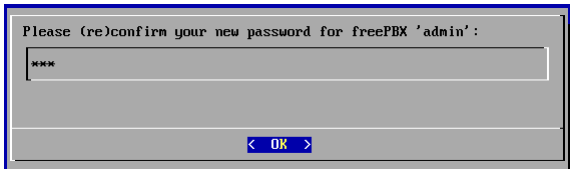

FIGURE 4.9 – Vérification de mot de passe

4.5.1.2 Lancement du serveur

Pour démarrer le serveur, nous entrons le login « root » et le mot de passe « root » crée lors de l'installation d'Elastix.

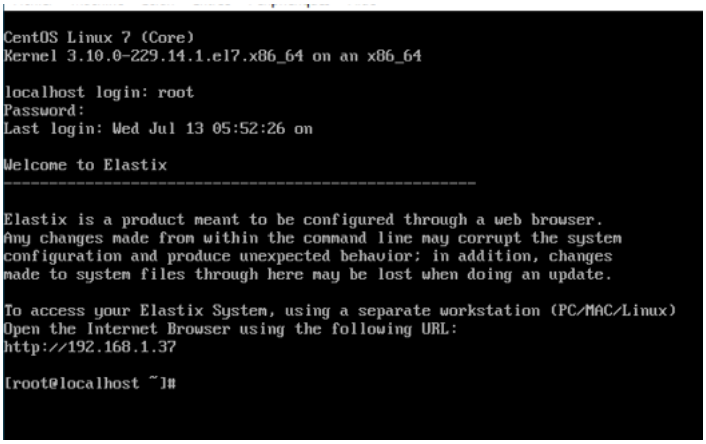

FIGURE 4.10 – Adresse IP de server Elastix

4.5.1.3 Accès au serveur

Pour accéder au serveur, nous tapons son adresse IP « 192.168.1.37 » comme URL dans un navigateur quelconque et la page de connexion au serveur apparaitra.
Nous verrons la figure 4.11 ci-dessous. Le nom d'utilisateur c'est admin et le mot de passe c'est celui que nous avons spécifié lors de l'installation (le dernier mot de passe crée durant l'installation) cliquons ensuite sur le bouton submit.

FIGURE 4.11 – Login et mot de passe du server Elastix

4.5.1.4 Tableau de bord d'interface Elastix

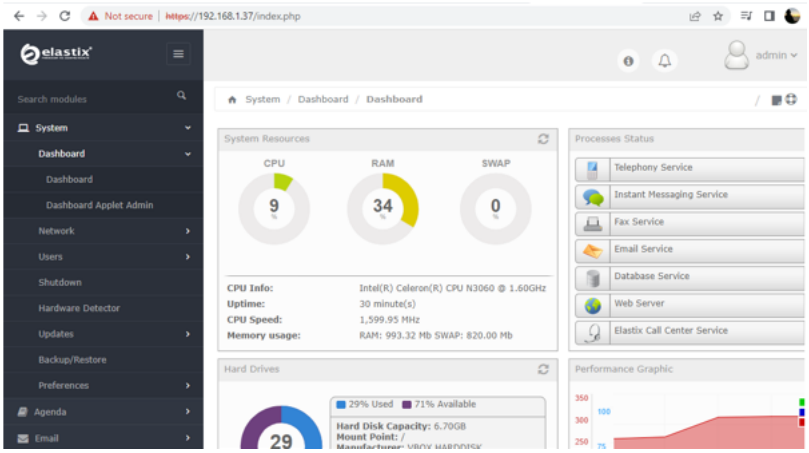

FIGURE 4.12 – Interface Elastix

4.5.2 Présentation de PfSense (Firewall)

Pfsense ou « Packet Filter Sense » est un applicatif qui fait office de routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. Il permet d'analyser, de sécuriser et de gérer le trafic réseau. Et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec les activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données.

4.5.2.1 Instalation de PfSense

- Nous lançons notre installation de PfSense.

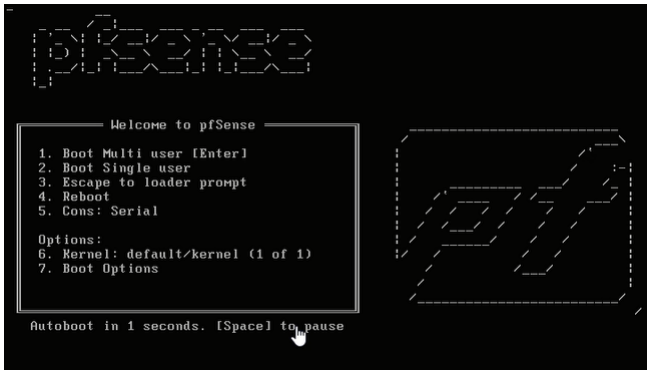

FIGURE 4.13 – Démarage de PfSense

- Après le chargement des données la fenètre va apparaitre.

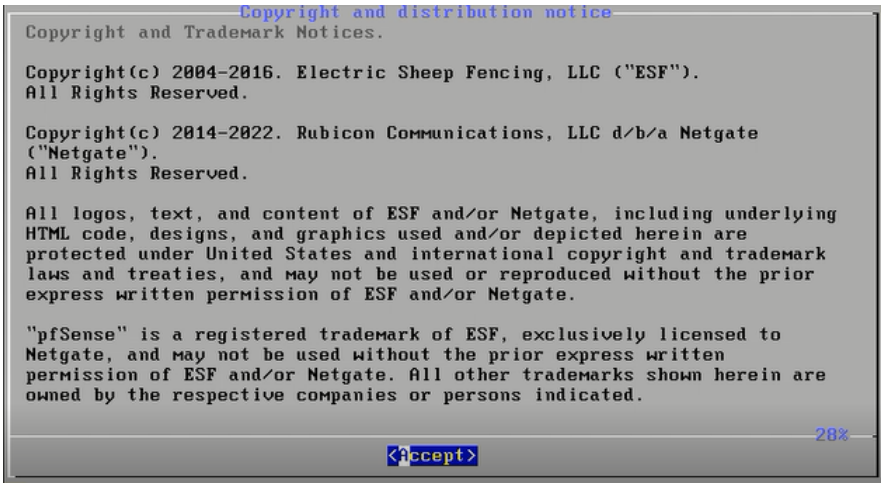

FIGURE 4.14 – Début de processus d'installation

-Nous appuyons sur accepter et nous confirmons l'installation, ensuite nous choisissons la langue de clavier et nous continuons sur les option par défaut jusqu'à la confirmation finale, l'installation se lance.

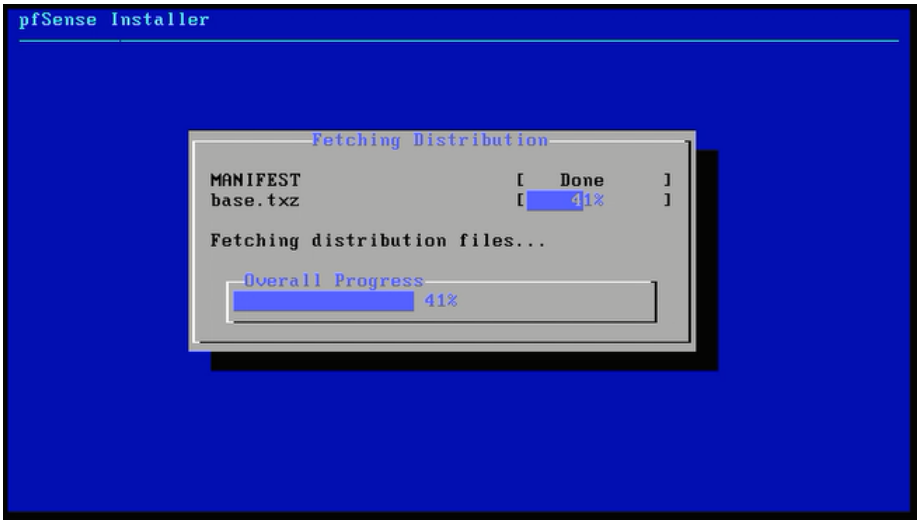

FIGURE 4.15 – Début d'installation

- A la fin de l'installation nous redémarrons le Pfsense pour configurer les interfaces de cette manière :

-interface WAN :192.168.42.129

-interface LAN :10.0.0.1

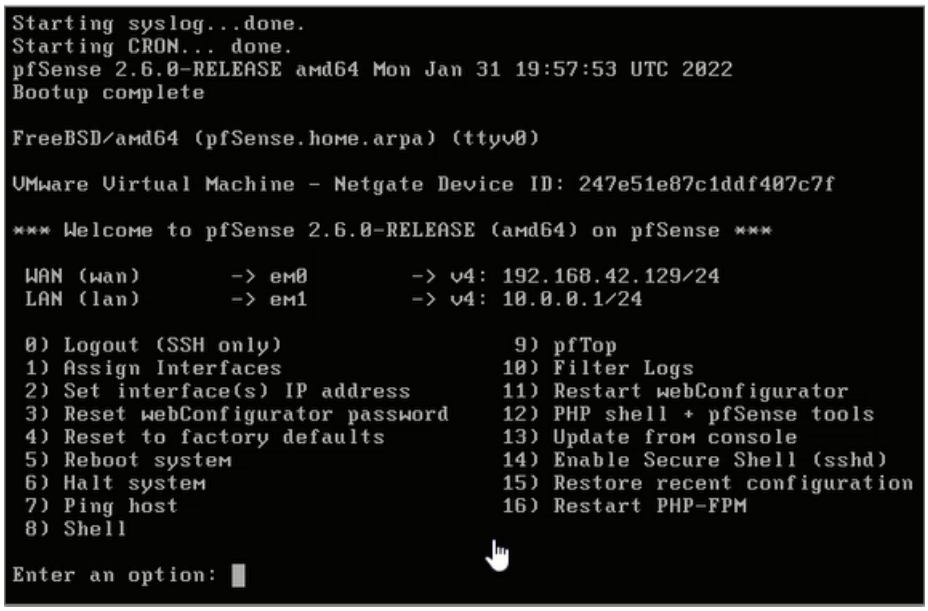

FIGURE 4.16 – Lancement de PfSense avec la configuration

4.6 Configuration de base

4.6.1 Plan d'adressage IPv4

Nom du vlan	Id du vlan	Adress ip	masque	passerelle
Data	Vlan100	172.16.100.0	255.255.255.0	172.16.100.1
Voice	Vlan101	172.16.101.0	255.255.255.0	172.16.101.1
Serveur	Vlan102	172.16.102.0	255.255.255.0	172.16.102.1
Management	Vlan103	172.16.103.0	255.255.255.0	172.16.103.1

TABLE 4.1 – Plan d'adressage IPv4

4.6.2 Configuration VTP (Serveur/Client/Transparent)

Pour faciliter la configuration des VLAN sur plusieurs switchs, il faut configurer le protocole VTP (Virtual LAN Trunk Protocol) : protocoles de niveau 2 permis d'ajouter un ou plusieurs vlans sur le seul switch distribution.

1.Pour configurer SWD1 en tant que serveur VTP, tapons :

```
SWD1>enable
SWD1#configure terminal
SWD1(config)#vtp mode server
SWD1(config)#vtp domain exon-tel.vtp
SWD1(config)#vtp password exon123
SWD1(config)#vtp version 2
SWD1(config)#vtp pruning
```

2.Vérification : En utilisant la commande « Show VTP status » :

```
SWD1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : exon-tel.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0200
Configuration last modified by 0.0.0.0 at 8-20-22 10:56:50
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 2
MD5 digest                      : 0x01 0x21 0x58 0x8B 0xF3 0xA4 0x36 0x4E
                                  0xB9 0xBB 0xCB 0x27 0x5F 0xBC 0xF7 0xF6
```

FIGURE 4.17 – Affichage le statu VTP

3.Les switchs SWA1, SWA2, SWA3 sont configuré de la même manière mais en mode client.

```
SWA1>enable
SWA1#configure terminal
SWA1(config)#vtp mode client
SWA1(config)#vtp domain exon-tel.vtp
SWA1(config)#vtp password exon123
SWA1(config)#vtp version 2
```

4.Vérification VTP :

```
SWA1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : exon-tel.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0300
Configuration last modified by 0.0.0.0 at 8-20-22 10:56:50

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 2
MD5 digest                        : 0x01 0x21 0x58 0x8B 0xF3 0xA4 0x36 0x4E
                                    0xB9 0xBB 0xCB 0x27 0x5F 0xBC 0xF7 0xF6
```

FIGURE 4.18 – Affichage d'informations VTP

4.6.3 Interface en mode trunk

5.Configuration des ports "trunk" dans le SWD1.

```
SWD1#configure terminal
SWD1(config)#interface range ethernet 0/0-2
SWD1(config-if-range)#switchport trunk encapsulation dot1q
SWD1(config-if-range)#switchport mode trunk
```

6.Configuration des ports "trunk" dans le SWA1, et de la même manière pour SWA2, SWA3, R1.

```
SWA1#configure terminal
SWA1(config)#interface ethernet0/0
SWA1(config-if)#switchport trunk encapsulation dot1q
SWA1(config-if)#switchport mode trunk
```

7.Vérification des ports "trunk" :

```
SWD1#show  interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
Et0/1       on               802.1q         trunking      1
Et0/2       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094
Et0/1       1-4094
Et0/2       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1
Et0/1       1
Et0/2       1

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1
Et0/1       1
Et0/2       1
```

FIGURE 4.19 – Affichage d'informations sur les ports

4.6.4 Création des vlan

La création des vlan se fait pour renforcer la sécurite du réseaux en génerale mais dans notre cas c'est pour éviter les Scan facile de détection de serveur sip.

```
SWD1(config)#vlan 100
SWD1(config-vlan)#name Data
SWD1(config-vlan)#vlan 101
SWD1(config-vlan)#name voice
SWD1(config-vlan)#vlan 102
SWD1(config-vlan)#name Serveurs
SWD1(config-vlan)#vlan 103
SWD1(config-vlan)#name management
SWD1(config-vlan)#end
SWD1#
```

FIGURE 4.20 – Création des VLANs.

1.VERIFICATION

```
SWD1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
100  Data                             active
101  voice                            active
102  Serveurs                         active
103  management                       active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

FIGURE 4.21 – Affichage des VLAN crée

4.6.5 Affectation des port vlan

SWD1 :

```
SWD1(config)#interface ethernet 3/3
SWD1(config-if)#switchport mode access
SWD1(config-if)#switchportaccess vlan 102
```

SWA3 :

```
SWA3(config)#interface ethernet0/1
SWA3(config-if)#switchport mode access
SWA3(config-if)#switchport access vlan 100
SWA3(config-if)#switchport voice vlan 101
```

SWA2 :

```
SWA2(config)#interface range ethernet3/2-3
SWA2(config-if-range)#switchport mode access
SWA2(config-if-range)#switchport access vlan 100
SWA2(config-if-range)#switchport voice vlan 101
```

SWA1 :

```
SWA1(config)#interface range ethernet 3/2, ethernet 1/0
SWA1(config-if-range)#switchport mode access
SWA1(config-if-range)#switchport access vlan 100
SWA1(config-if-range)#switchport voice vlan 101
```

4.6.6 Configuration du routage inter-vlan

- Nous allons créer des interfaces de nos vlans.

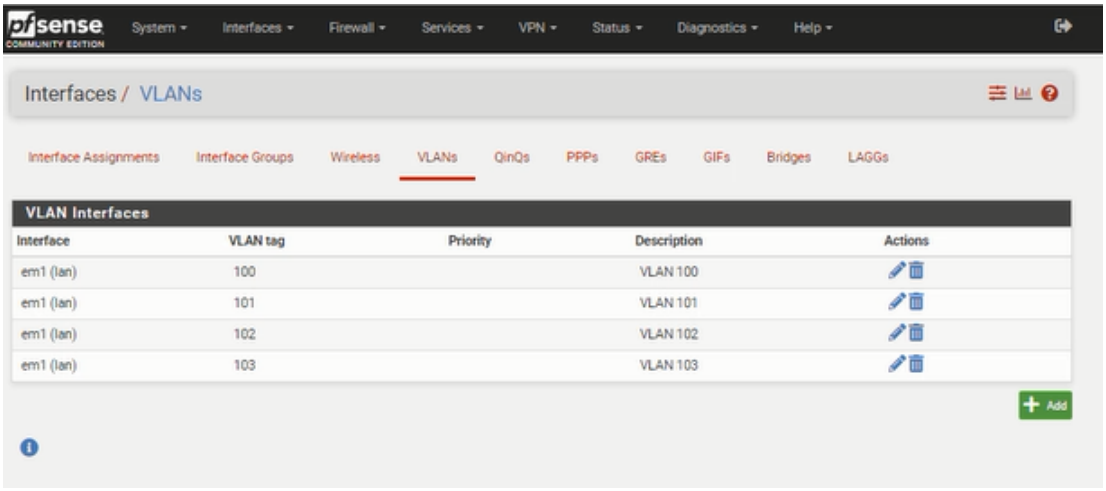

FIGURE 4.22 – Création des vlan

- Nous allons affecter les sous interfaces des vlans.

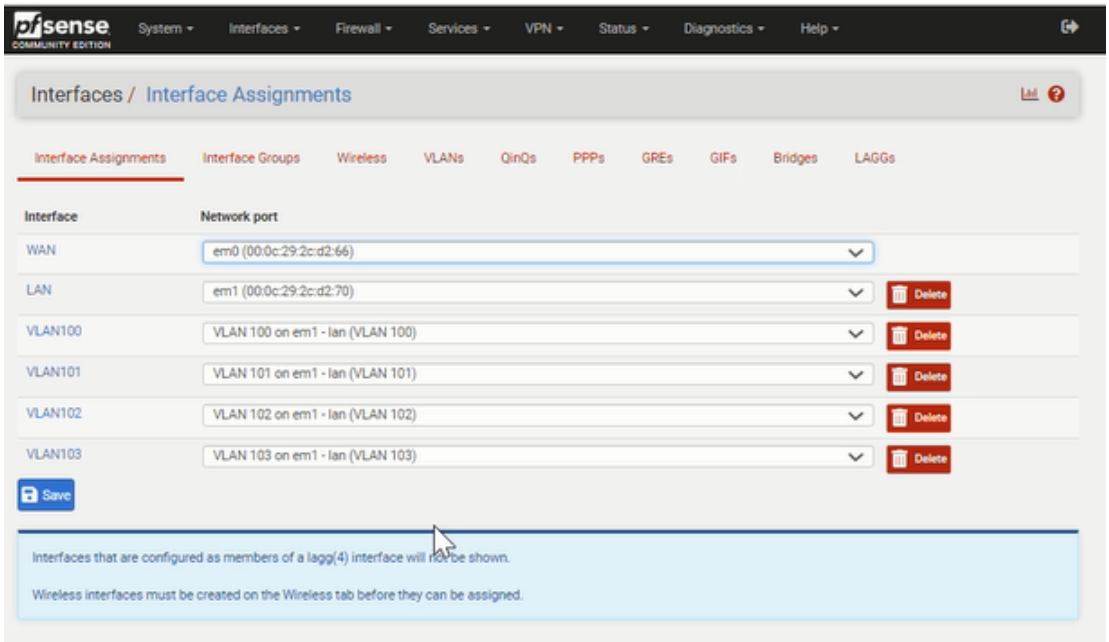

FIGURE 4.23 – Affectation des vlan

- Nous allons autoriser le trafique pour chaque vlans, on ajoutons des règles.

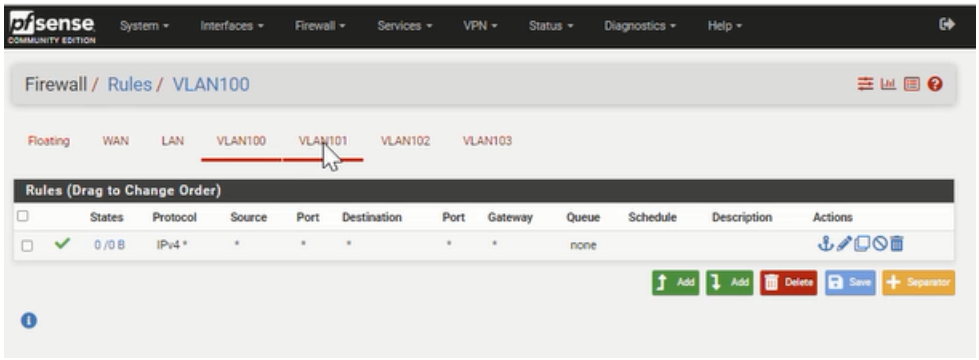

FIGURE 4.24 – Autorisation des vlan

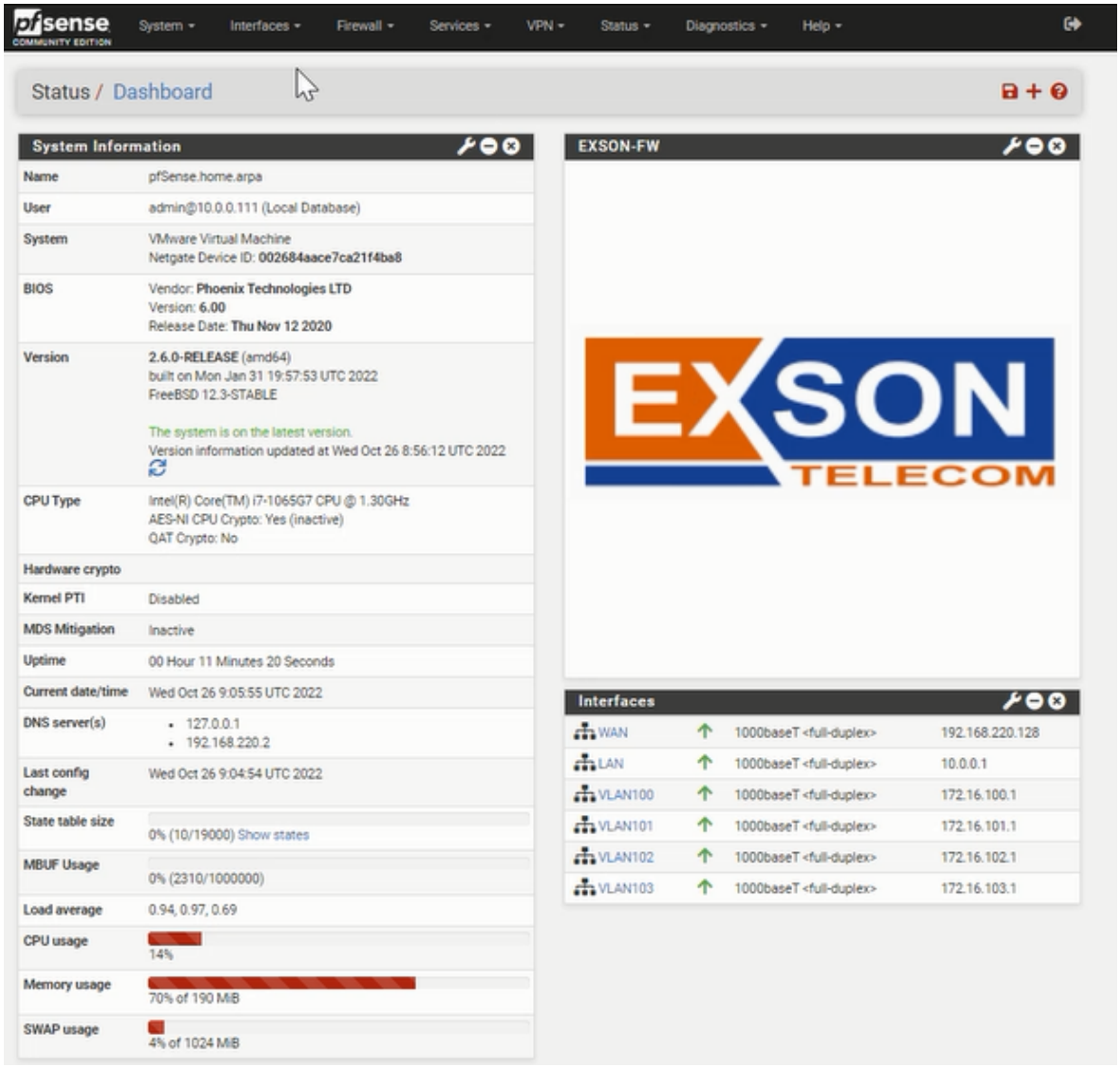

FIGURE 4.25 – Tableau de bord de firewall

4.6.7 Configuration du service DHCP sur le routeur

Un serveur DCHP pour l'obtention d'une adresse IP automatiquement. - Nous allons ajouter une adresse ip de l'un des vlan.

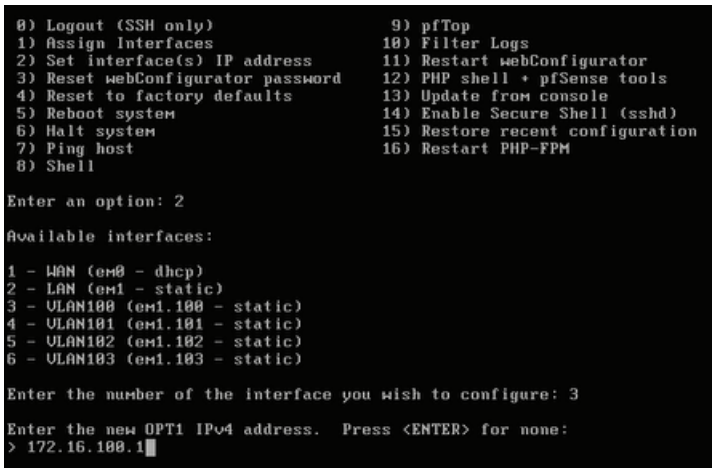

FIGURE 4.26 – Affichage d'informations

- Nous allons configurer les pool d'adresse.

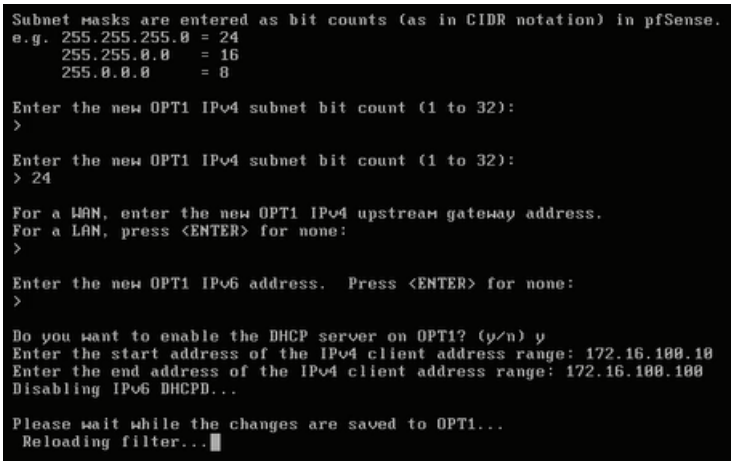

FIGURE 4.27 – Affichage d'informations

Vérification :

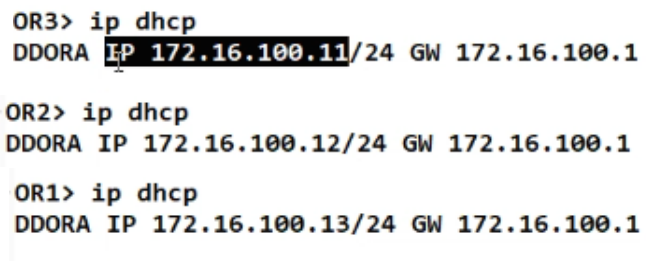

FIGURE 4.28 – Affichage de test DHCP

4.6.8 Configuration de base de Routeur

- Nous allons configurer les interfaces du routeur.

```
R1#conf t
R1(config)#interface ethernet 0/0
R1(config-if)#ip address dhcp
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface ethernet 0/1
R1(config-if)#ip address 192.168.42.130 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
```

- Nous allons router les interfaces du routeur vers internet et vers les vlans que nous avons.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.42.130
R1(config)#ip route 172.16.100.0 255.255.255.0 192.168.42.129
R1(config)#ip route 172.16.101.0 255.255.255.0 192.168.42.129
R1(config)#ip route 172.16.102.0 255.255.255.0 192.168.42.129
R1(config)#ip route 172.16.103.0 255.255.255.0 192.168.42.129
```

4.6.9 Configuration de base de firewall

Après avoir installé et lancé PfSense nous tapons l'adresse 10.0.0.1 dans le navigateur pour accéder à l'interface de notre firewall pour commencer les configuration de base.

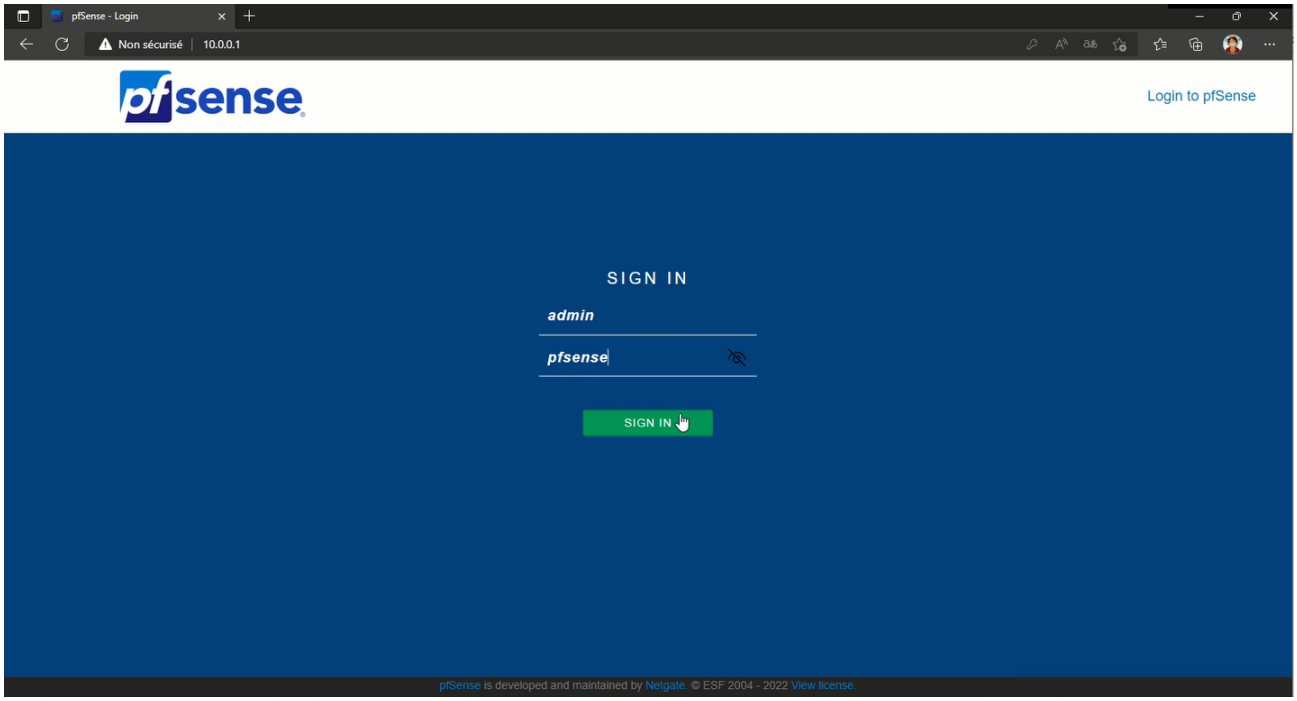

FIGURE 4.29 – l'interface d'accueil de PfSense

-Nous dirigeons vers le routing pour enlever le blocage car on doit indiquer que notre route part sur le port WAN.

-Maintenant nous pouvons créer un utilisateur "salah" avec un mot de passe "Asr2022 " comme administrateur et nous enlevons l'administrateur par défaut pour s'assurer de la sécurité d'accès.

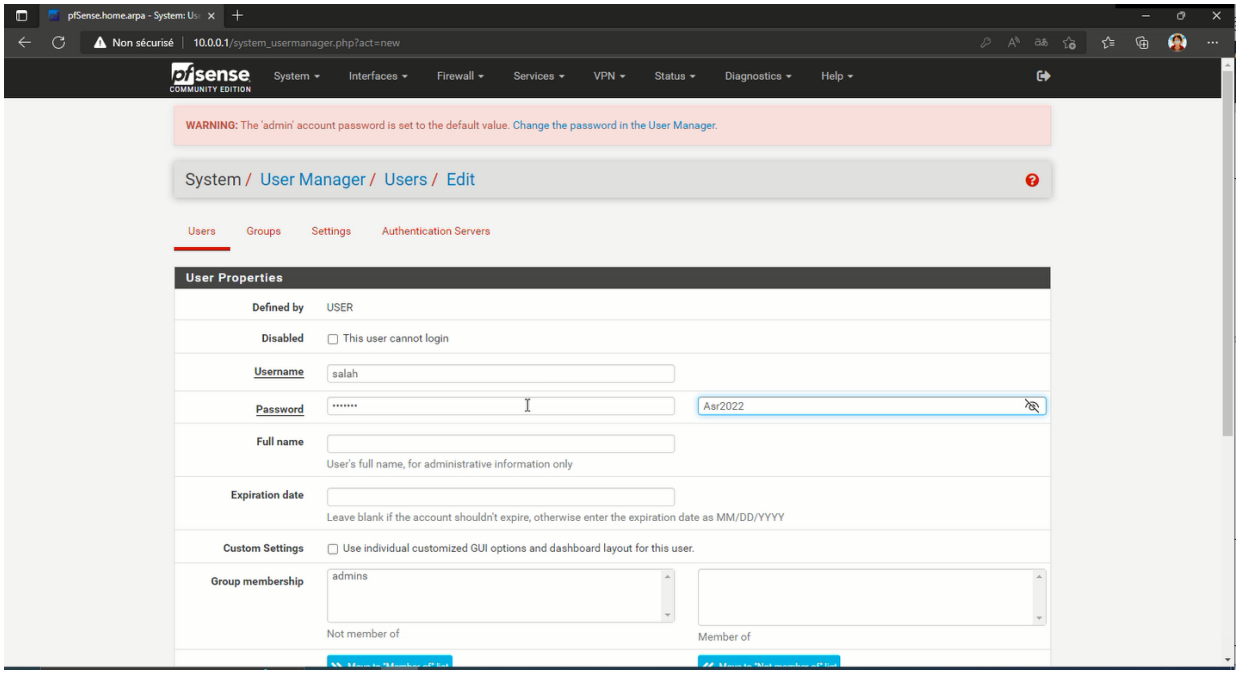

FIGURE 4.30 – Édition d'un utilisateur

- Après cela nous ajoutons le graphe pour surveiller le trafic.

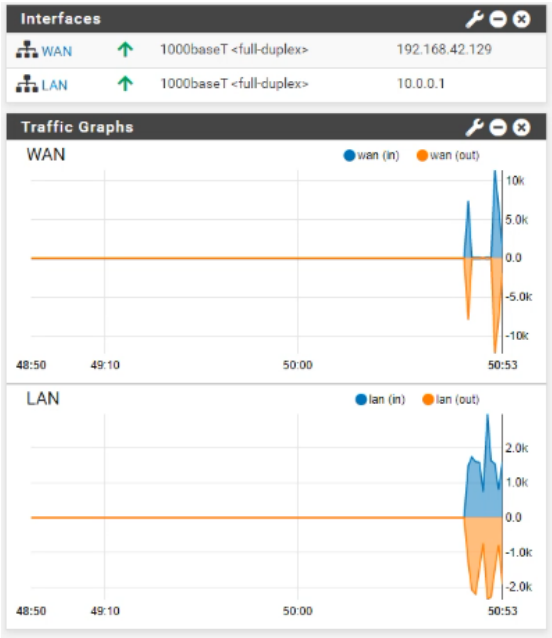

FIGURE 4.31 – Graphe de PfSense

- puisque nous utilisons une adresse privé ou des adresse privés, Nous devons donner accès a l'interface WAN.

-Nous appliquons les règles entrante dans notre firewall.

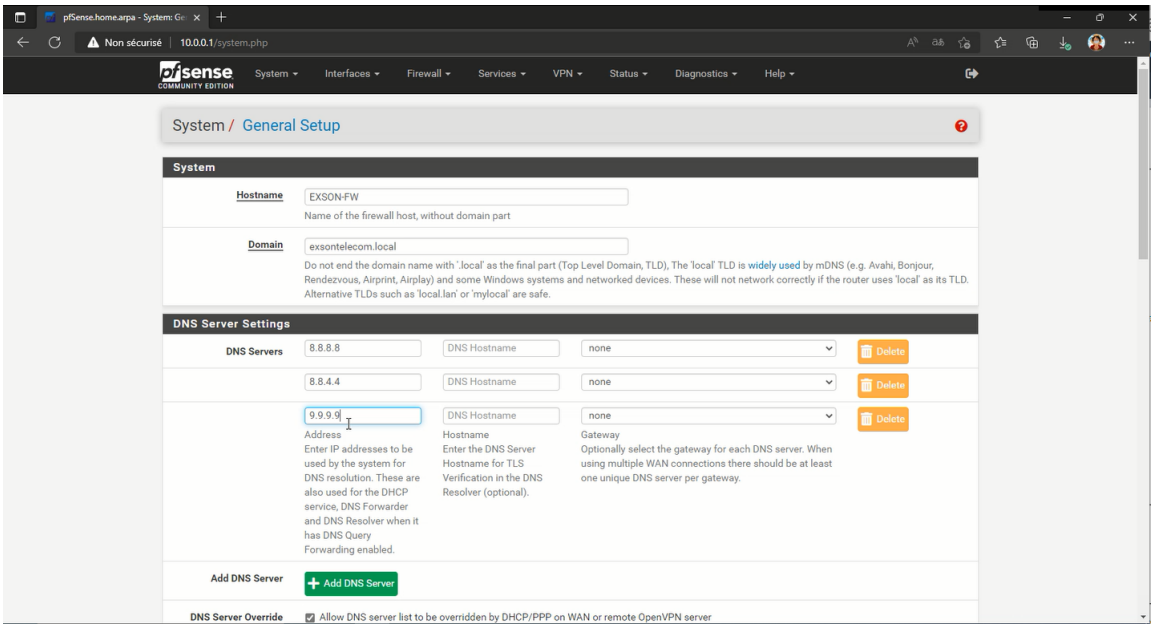

FIGURE 4.32 – Configuration DNS

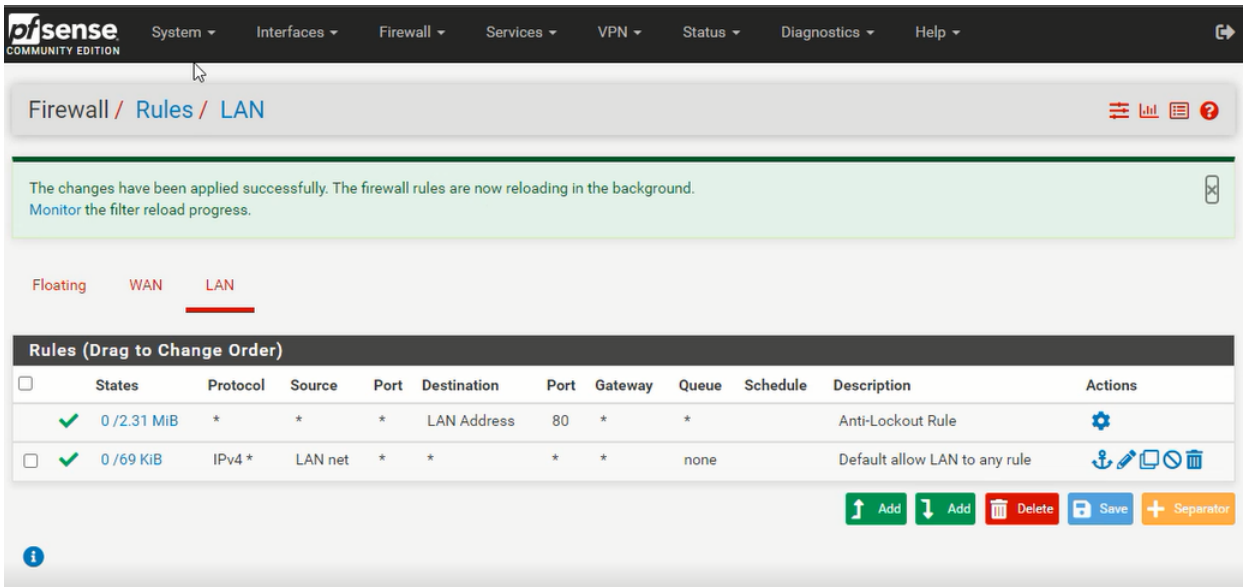

FIGURE 4.33 – Application des régles

- Maintenent nous devons créer et autoriser nos vlan.

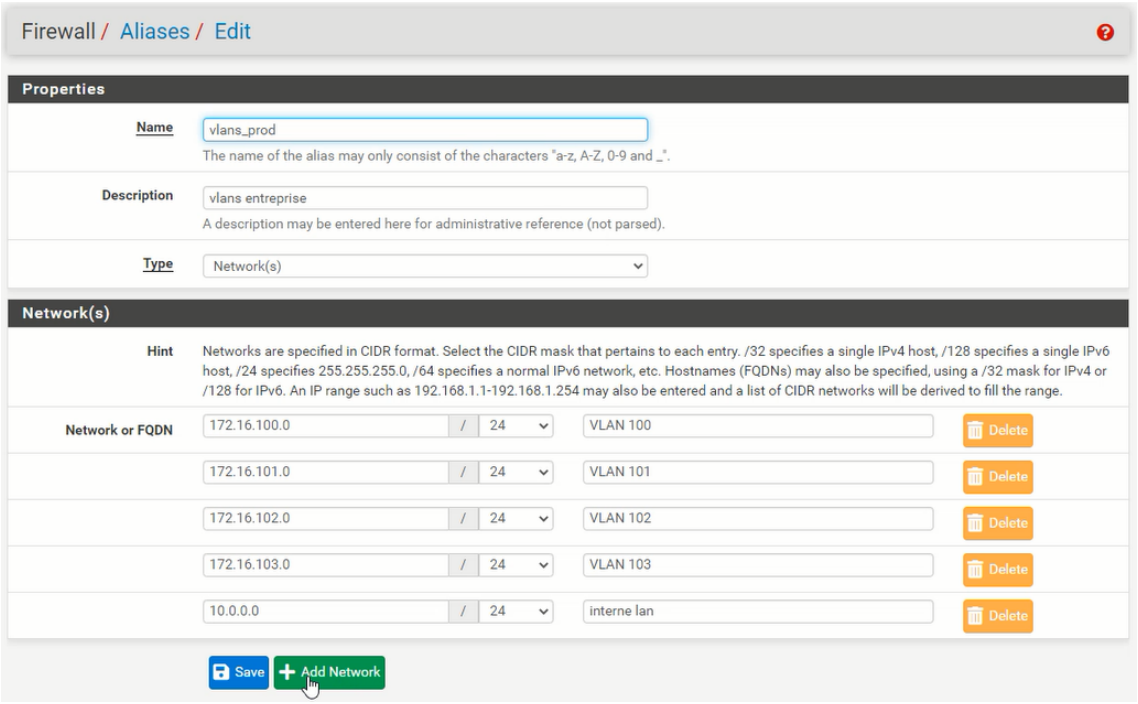

FIGURE 4.34 – Création des Vlan

-Nous ajoutons une regle pour les vlan créer pour les sorties dans l'interface Lan du firewall, et nous supprimons la règle par défaut.

-Au meme temp nous créons une règle de blocage pour les réseaux non pérmis.

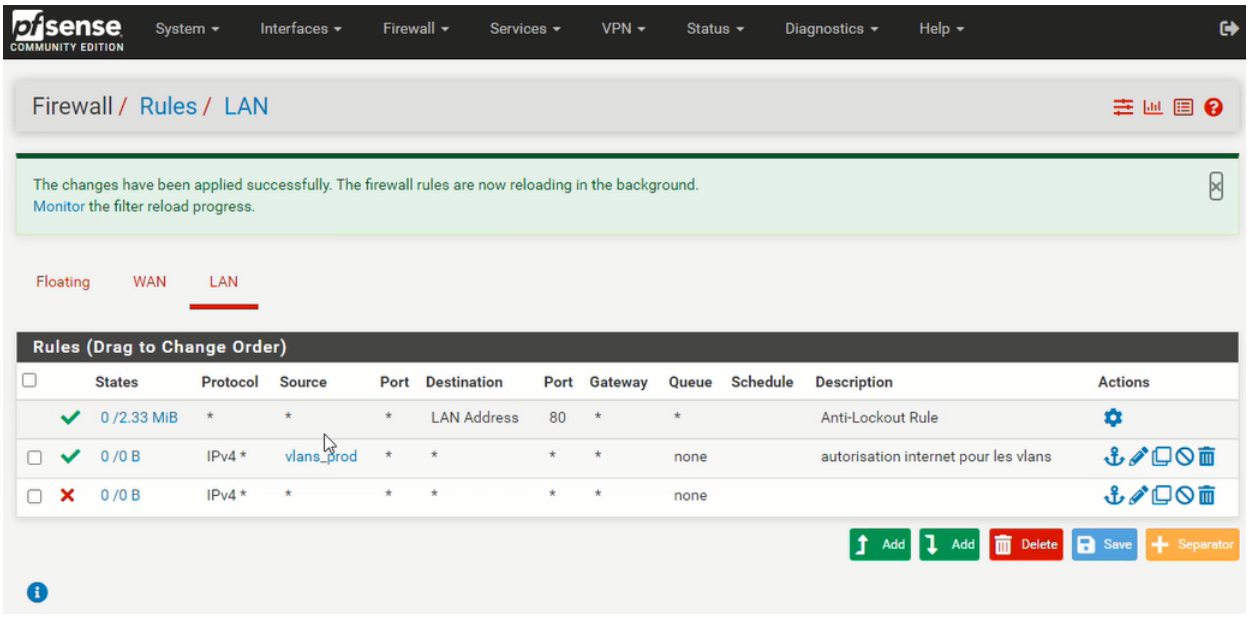

FIGURE 4.35 – Règles sur LAN

-Maintenent nous devons routé notre firewall vers les vlan.

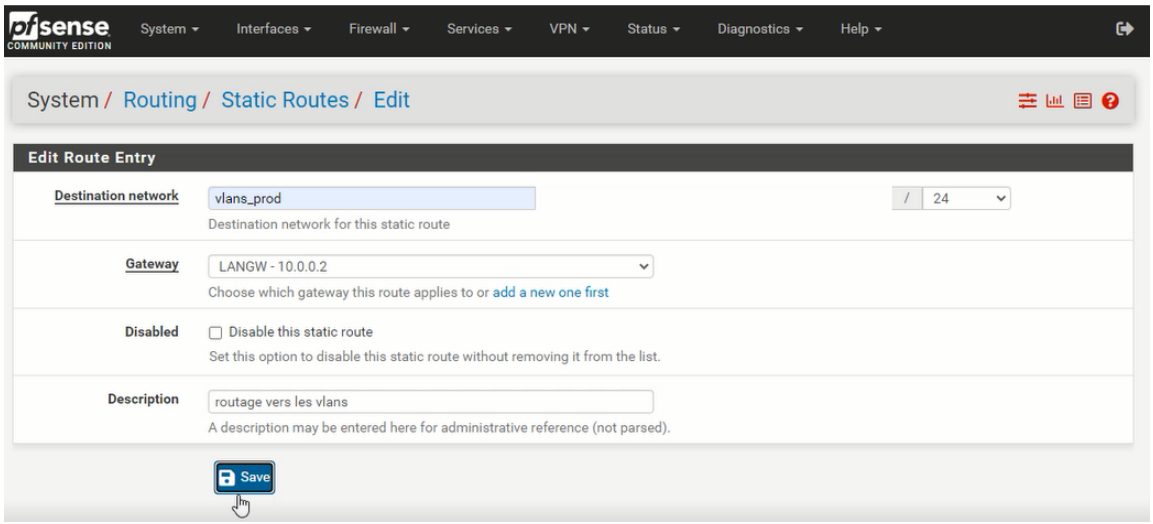

FIGURE 4.36 – Routage de Firewall

4.6.10 Configuration de client VPN

-Nous allons dans le wizard, pour créer un certificat d'authorité pour le client et le serveur.

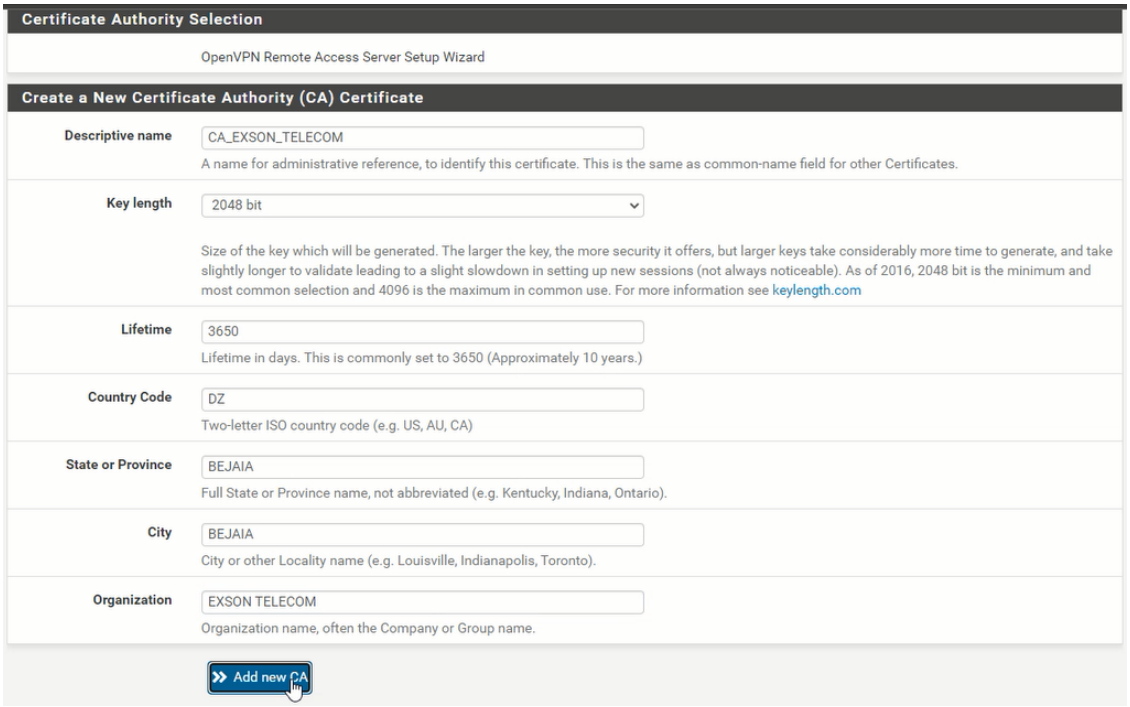

FIGURE 4.37 – Création de certificat de client

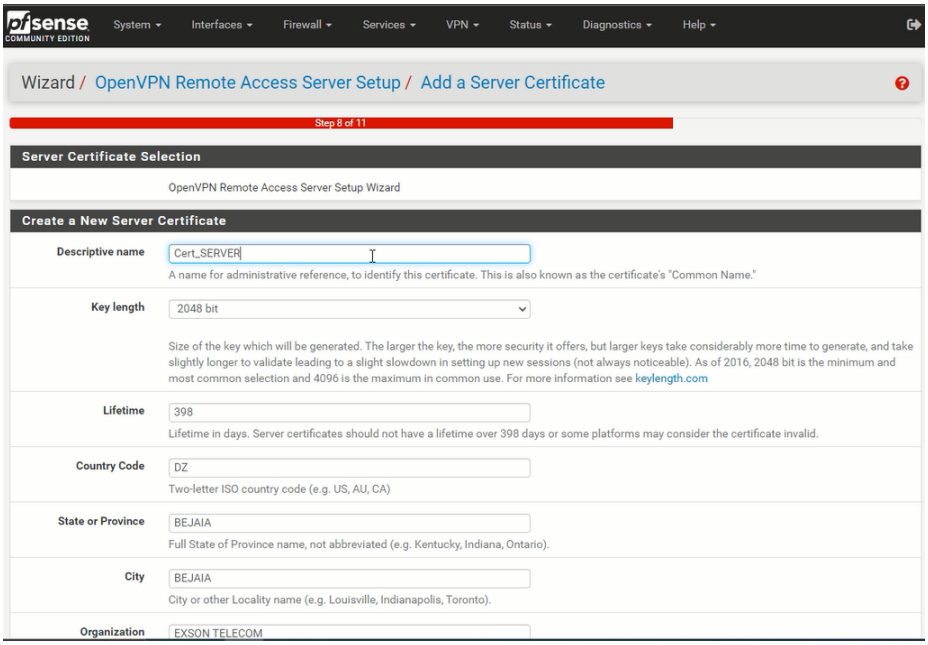

FIGURE 4.38 – Création de certificat de serveur

- Après cela nous allons créer un utilisateur vpn qu'est "mona" avec le mot de passe "123456789" avec sa certification.

- Accorder PfSense d'accepter une préconfiguration de Openvpn .

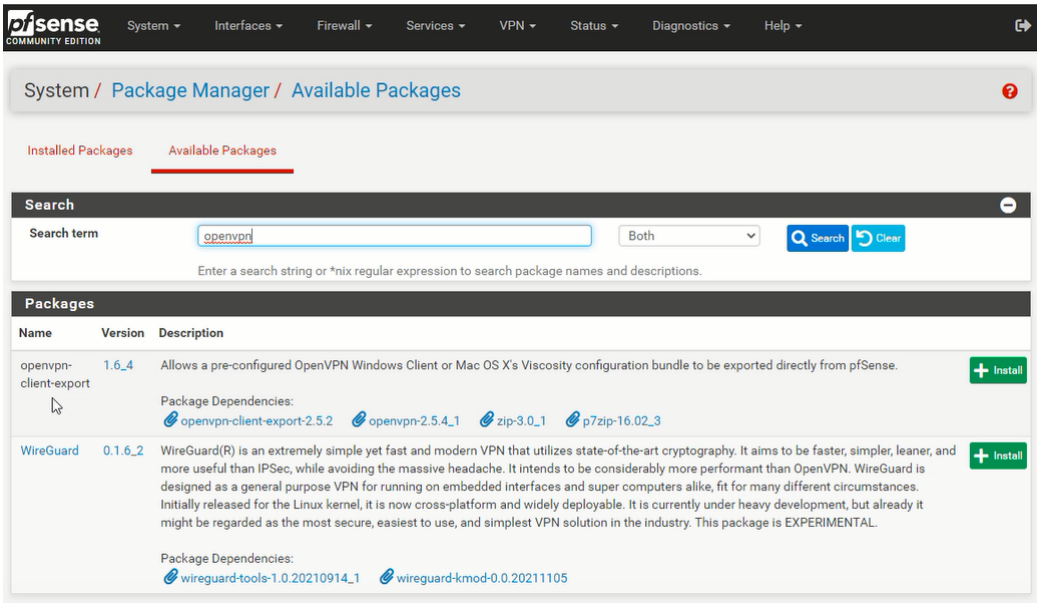

FIGURE 4.39 – Création de la préconfiguration Openvpn

- Après un bon moment le package sera chargé et nous pouvons le télécharger.

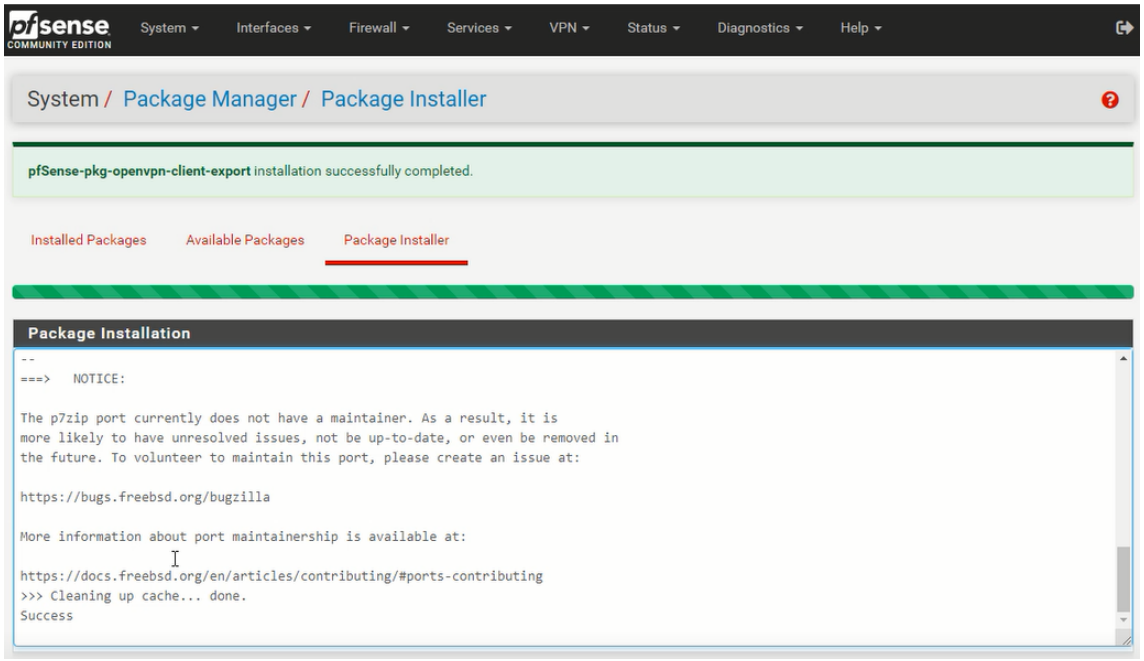

FIGURE 4.40 – Installation complète de package

-Nous avons le choix de version openvpn préconfiguré à télécharger et à installer dans le client vpn afin d'avoir l'accés à distance au firewall.

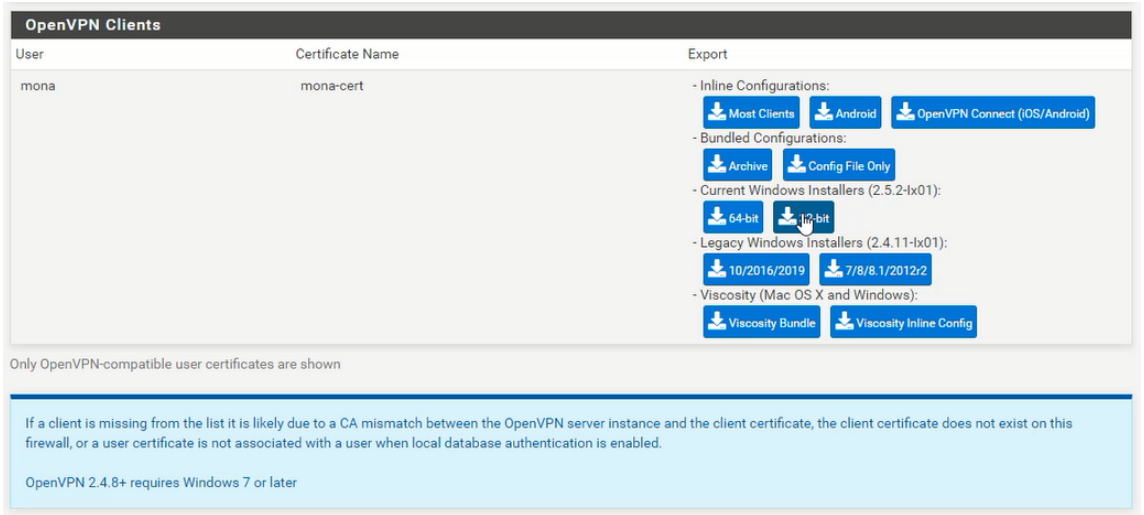

FIGURE 4.41 – Vérsions Openvpn préconfigurer

4.7 Configuration du PBX et création des compts sip

4.7.0.1 Addresse IP en mode statique

-Nous tapons les commande linux suivante :

```
Sudo nano /etc/sysconfig/network -scripts/ifcgfg-enp0s3


BOOTPROTO="static"
IPADDR=172.16.102.100
GATEWAY :172.16.102.1
NETMASK : 255.255.255.0
```

Après avoir terminé, CTRL+O pour sauvegarder et puis CTRL+X pour quitter, et nous redémarrons notre service réseaux pour charger la nouvelle addresse, avec la commande sérvice network restart.

4.7.0.2 Création d'une nouvelle extension

Grâce à l'interface graphique nous n'avons pas besoin de gérer les utilisateurs manuellement avec le fichier sip.conf d'Asterisk, il suffit d'accéder à l'interface elastix d'administration après s'être identifié, l'interface elastix va nous permettre de gérer les utilisateurs.
Pour créer une nouvelle Extension, aller au menu « PBX » qui par défaut, arrive à la section « Configuration PBX » ; dans cette section, choisir l'option « Extensions » sur le panneau gauche. Maintenant nous pouvons créer une nouvelle extension.
a) Tout d'abord, choisir le dispositif parmi les options disponibles. Cliquer sur « Submit » pour procéder aux enregistrements des champs nécessaires pour la création d'une nouvelle extension.

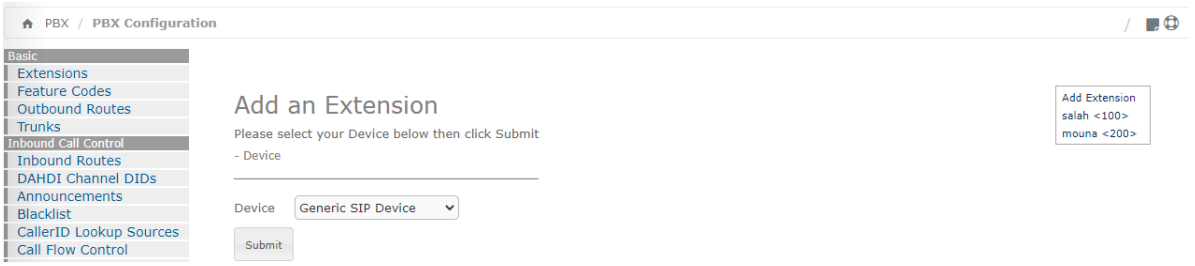

FIGURE 4.42 – Ajouter Extension

b) Créer une nouvelle extension. Continuez à entrer les informations correspondantes :

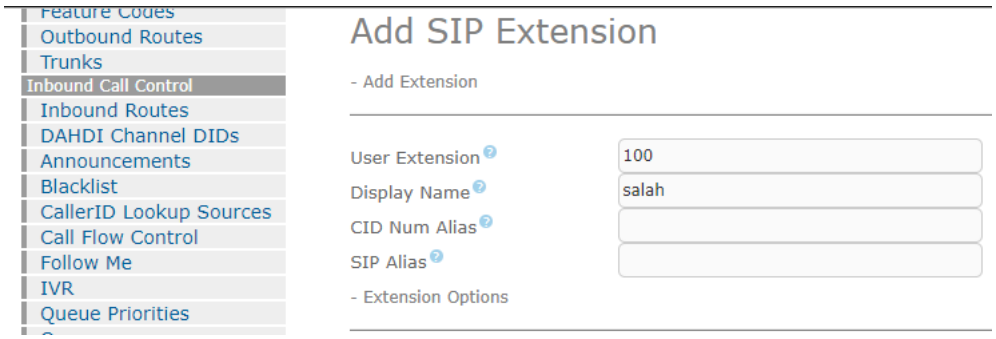

FIGURE 4.43 – extension ajouter

- User Extension : Elle doit être unique. C'est le numéro qui peut être appelé de n'importe qu'elle autre extension, ou directement du réceptionniste numérique s'il est activé. Elle peut être de n'importe qu'elle longueur, mais conventionnellement, un numéro de 3 ou 4 chiffres est utilisé.

- Display Name : Le nom d'identification de l'appelant pour les appels de cet utilisateur affichera ce nom. Entrer seulement le nom, pas le numéro.

- Secret : C'est le mot de passe utilisé par le périphérique téléphonique pour s'authentifier sur le serveur Elastix. Il est habituellement configuré par l'administrateur avant de donner le téléphone à l'utilisateur, Si l'utilisateur utilise un logiciel de téléphonie, alors il aura besoin de ce mot de passe pour configurer son logiciel. Après avoir rempli ces champs nous cliquons sur « submit » pour l'enregistrement et puis on clique sur « apply configuration change here » pour actualiser l'enregistrement.

4.7.1 Configuration de logiciel de téléphonie

En configurant un logiciel de téléphonie, notre but est d'avoir un PC connecté qui autorise les mêmes fonctions qu'un téléphone traditionnel. Pour ceci, nous avons besoin d'installer un logiciel qui convertit le PC en téléphone. Il y a beaucoup de logiciels de téléphonie, dans notre cas nous avons utilisé 3cx.

3CX Softphone est un programme téléphonique basé sur SIP qui permet de passer et de recevoir des appels sur pc.

FIGURE 4.44 – logiciel téléphonique 3cx

Chaque utilisateur à des champs propres à savoir :

- Le champ Profile dans lequel nous ajoutons nom de l'utilisateur
- Le champ Extension dans lequel nous ajoutons numéro du téléphone exemple 200
- Le champ Id dans lequel nous ajoutons un identifiant
- Le champ Password dans lequel nous ajoutons secret mot de passe
- Le champ Adresse IP dans lequel nous ajoutons l'adresse IP du serveur Asterisk.

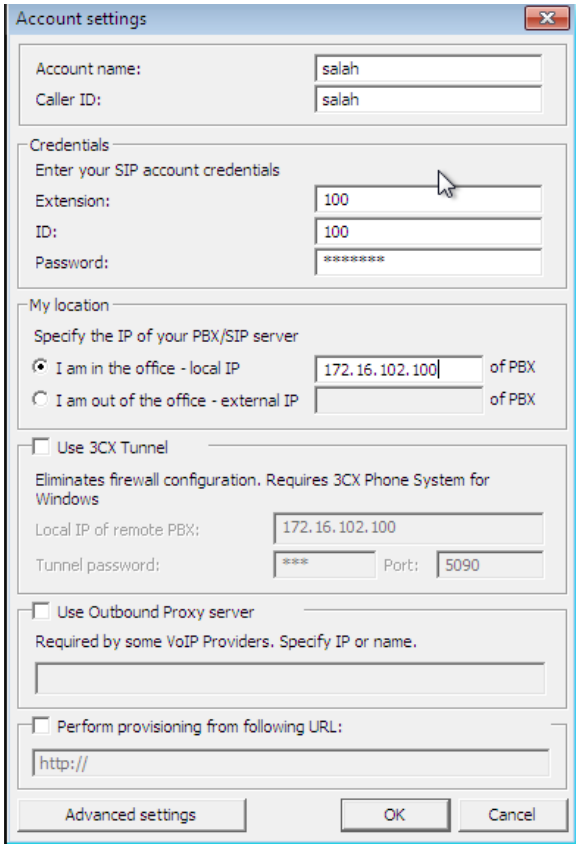

FIGURE 4.45 – Interface de configuration de 3CXPhone

Vérification et Test de communication VoIP :

FIGURE 4.46 – Test de communication entre les clients 3CX

4.8 Scénarios d'attaques contre la VoIP

4.8.1 Attaques contre la VoIP

4.8.1.1 Localisation des serveurs VoIP

Une attaque sans collecte d'informations sur un système distant est totalement inefficace. Pour élargir ses possibilités d'attaque et offrir plus de souplesse dans le choix des méthodes d'attaque, il est impératif de connaître le système cible, la stratégie est tout aussi importante que la manœuvre proprement dite. N'importe qui peut accéder à n'importe quelle connaissance grâce à la collecte de quantités massives de données sur un seul réseau.
Voici quelques méthodes pour la collecte des informations les plusutilisées :
A) Scan des réseaux VoIP Il existe plusieurs méthodes pour scanner le réseau Pour trouver dans le réseau les serveurs IPBX ou des équipements VOIP. Par exemple nous avons utilisé l'un des utilitaires sipvicious que s'appelle svmap pour scanner le réseau. Nous avons trouvé l'IP pbx 172.16.102.100 et le port 5060.

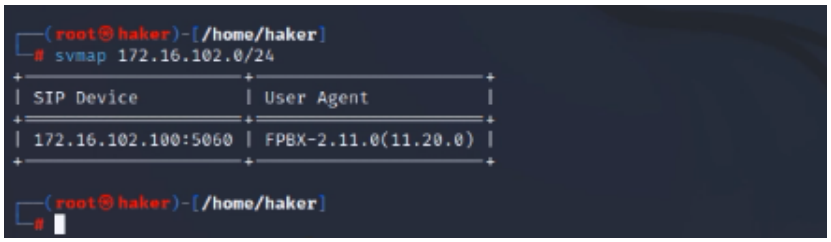

FIGURE 4.47 – Scan le réseau avec svmap

B) Moteurs de recherches L'utilisation des moteurs de recherches et des agents intelligents l'un des plus grands risques de sécurité aujourd'hui pour trouver des informations sur Internet. Un pirate peut utiliser un service tel que les fonctionnalités avancées de Google à son avantage de différentes manières.

C) Utilisation des serveurs Whois Un outil qui vous permet de rechercher dans des bases de données (appelées registres) relatives aux adresses IP et aux noms de domaine.

4.8.1.2 Attaque MITM"Man-in-the-Middle"

Cette attaque est utilisée pour écouter et enregistrer des discussions entre interlocuteurs, ainsi que pour obtenir une collecte d'informations confidentielles.

Analyse de paquets avec Wireshark : C'est l'une des applications logicielles les plus utilisées pour la surveillance et la capture de trafic réseaux, aussi convertir des conversations téléphoniques en fichiers audio.

1. Après le démarrage de Wireshark, nous choisissons l'interface réseau via laquelle nous recevrons les paquets échangès.

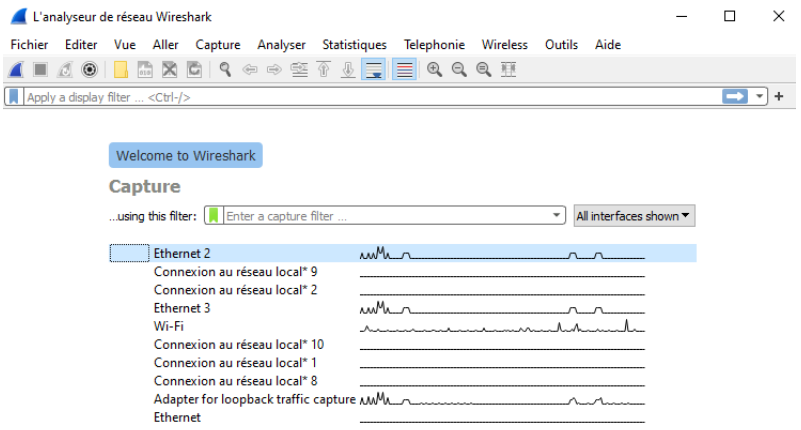

FIGURE 4.48 – Interface de wireshark

2. maintenant, nous allons commencer la capture. Le sniffer du trafic commence lorsque le client 100 appelle le client 200.

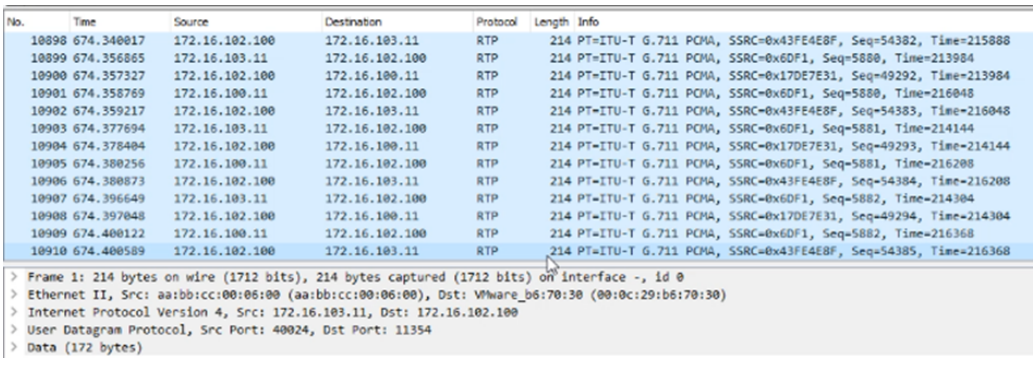

FIGURE 4.49 – Paquets RTP interceptés par Wireshark

3.pour écouter le flux nous cliquons sur "téléphone" après "appels voip".

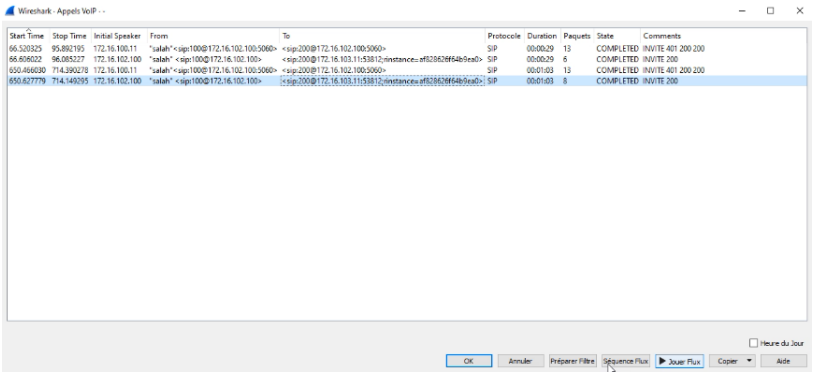

FIGURE 4.50 – Enregistrements d'un appel voip

4. Nous cliquons sur l'appel puis sur 'jouer flux' pour pouvoir écouter.

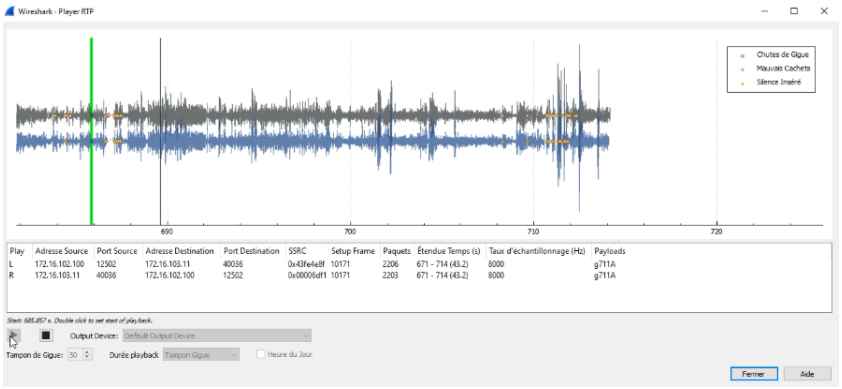

FIGURE 4.51 – Ecoute des conversations enregistrées

En utilisant la technique « man in the middle » pour capter tous les paquets qui passent entre les extensions, pirater toutes les données d'enregistrement qu'utilise les clients SIP distants.

4.8.1.3 Attaque par DOS (déni de service)

Invite flooding : Consiste à envoyer un nombre important de paquets IP inutiles via un réseau d'une manière qui empêche une entité au niveau du réseau de traiter des paquets IP légitimes.

La commande 'Inviteflood' est utilisé pour lancer des attaques DOS contre les extensions sur le réseau VoIP.

Une fois l'attaque lancée, nous remarquons une perturbation dans le réseau du serveur et après un certain temps ce dernier sera hors service.

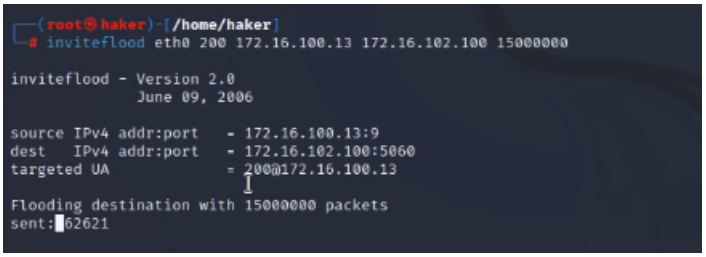

FIGURE 4.52 – Attaque de type DOS avec inviteflood

Avec les requêtes de type INVITE. Nous avons envoyé 15000000 packets vers la cible (serveur voip) ayant l'adresse 192.16.102.100 et nous remarquons que l'appel vers l'extension 200 a été interrompu (hors service).

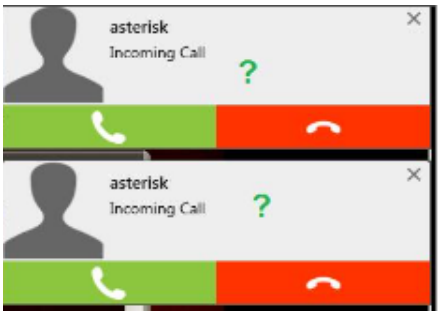

FIGURE 4.53 – Appel interrompu entre les deux extensions

4.8.2 Sécurisation contre les attaques

Nous avons adopté un ensemble de solutions qui peuvent protéger le système contre les attaques réalisées et même d'autres attaques similaires telles que les attaques DOS.

4.8.2.1 Sécurisation du vlan natif

Le VLAN natif par défaut est celui dans lequel les interfaces sont placées par défaut tant qu'elles n'ont été attribuées à aucun VLAN. En configuration par défaut, c'est généralement le VLAN 1 :

-La première bonne pratique consiste donc à modifier la valeur du vlan natif sur le trunk.

Pour empêcher un hacker de capturer son propre trafic ou d'envoyer de faux messages afin de perturber le fonctionnement du réseau.

- Configuration vlan natif :

1. avec la commande « show interface trunk », nous remarquons que vlan 1 contient toutes les interfaces par défaut.

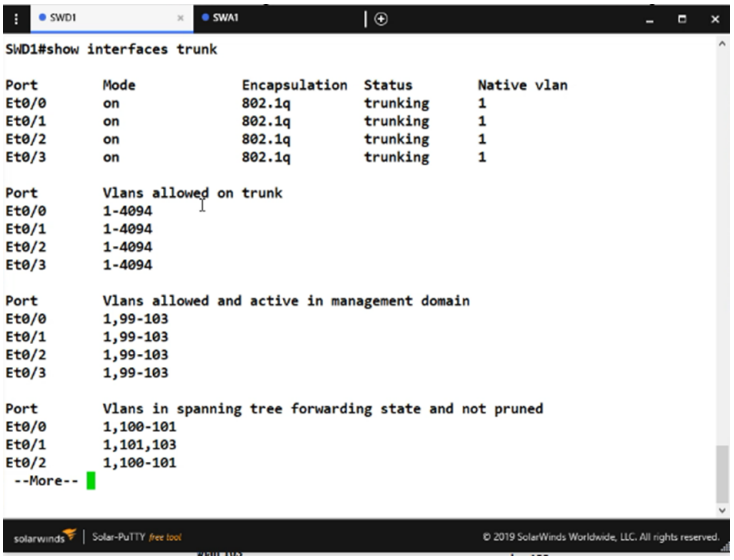

FIGURE 4.54 – Vérification des vlan

2.Création d'un nouveau vlan natif dans le switch SWD1.

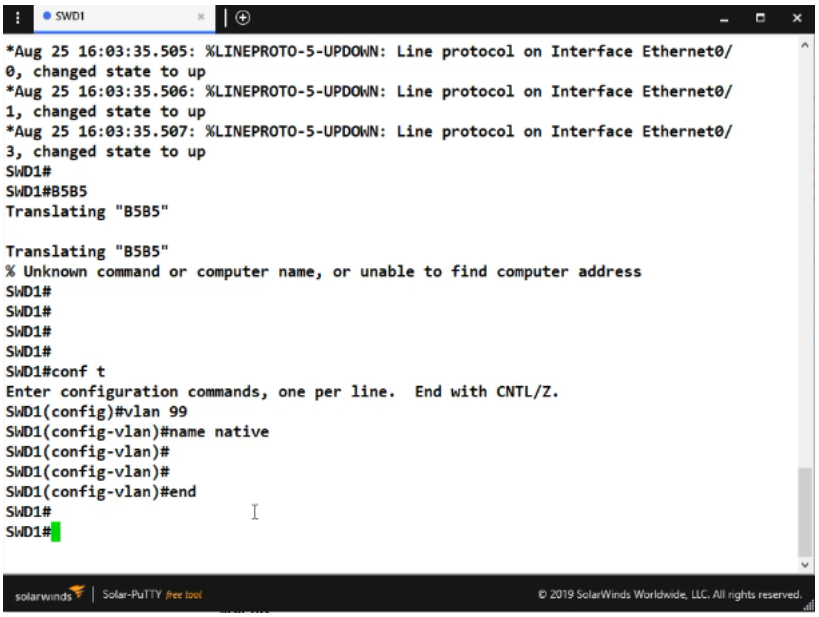

FIGURE 4.55 – Création un vlan natif

3.Verification avec la commande « show vlan brief »

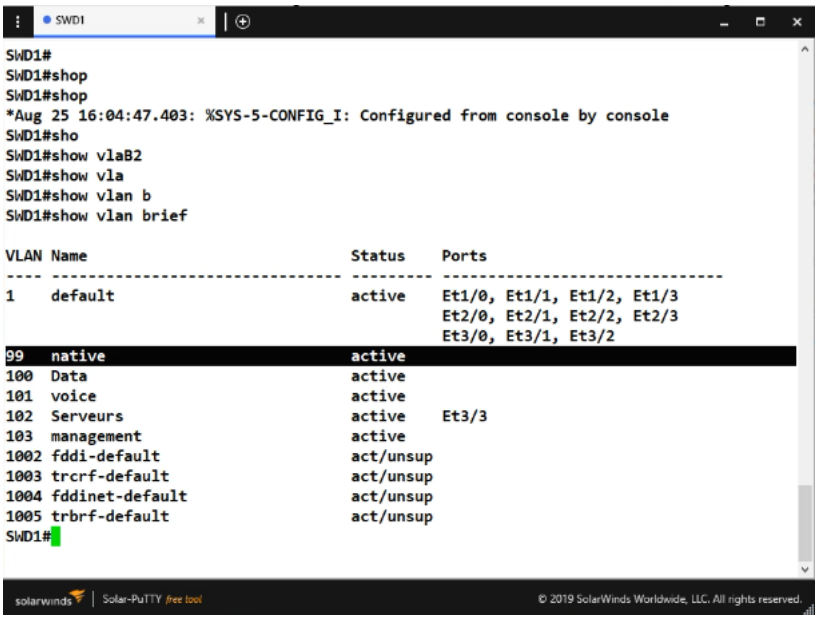

FIGURE 4.56 – Création vlan 99

4.Nous allons modifier la valeur du vlan natif (par défaut le vlan 1 est le vlan natif).

```
SWD1( config )# interface range Ethernet 0/0-2
SWD1 ( config -if)# switchport trunk native vlan 99
SWD1( config -if)# switchport trunk allowed vlan 100-103,99
```

5. Nous remarquons que le 1 est modifié en 99.

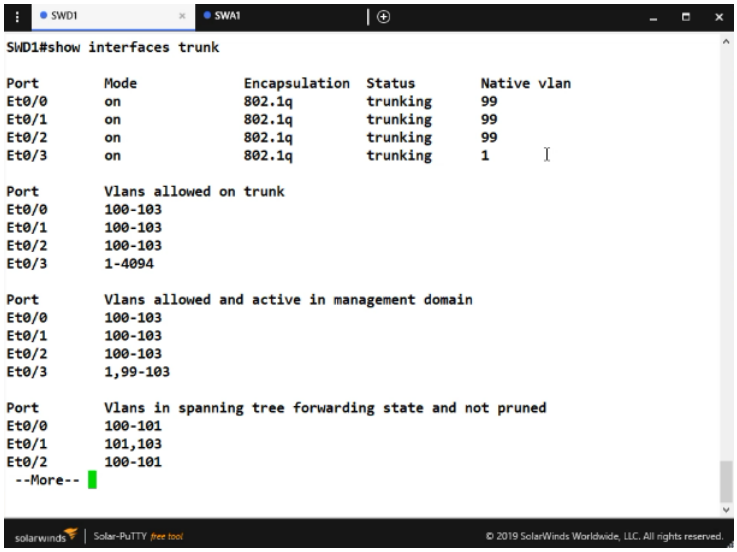

FIGURE 4.57 – Vérification vlan natif

6.Vlan natif doit être le même sur tous les commutateurs du même domaine de diffusion afin d'éviter les comportements inadéquats. Donc nous configurons de la même manière les swa1, swa2, swa3

```
SWA1( config )# interface Ethernet 0/0
SWA1 ( config -if)# switchport trunk native vlan 99
SWA1 ( config -if)# switchport trunk allowed vlan 100-103 ,99
```

```
SWA2( config )# interface Ethernet 0/0
SWA2 ( config -if)# switchport trunk native vlan 99
SWA2 ( config -if)# switchport trunk allowed vlan 100-103 ,99
```

```
SWA3( config )# interface Ethernet 0/0
SWA3 ( config -if)# switchport trunk native vlan 99
SWA3( config -if)# switchport trunk allowed vlan 100-103 ,99
```

4.8.3 Sécurisation des ports

Elle consiste à faire un contrôle sur les ports en limitant l'accès à certaines adresses MAC, cela permet de sécuriser l'accès. Pour cela, il faut spécifié l'adresse MAC de softphone autorisée. En cas de "violation", le port tombe en mode shutdown.

1.Dans le softphone 2 nous allons activer le port-security.

```
SWA2(config)#interface ethrenet 3/3
SWA2(config-if)#switchport port-security
```

2.Définition l'adresses MAC autorisées : L'adresse MAC correspond à l'adresse physique de la machine. Nous avons récupéré l'adresse MAC de softphone2 avec la commande « ipconfig/all »

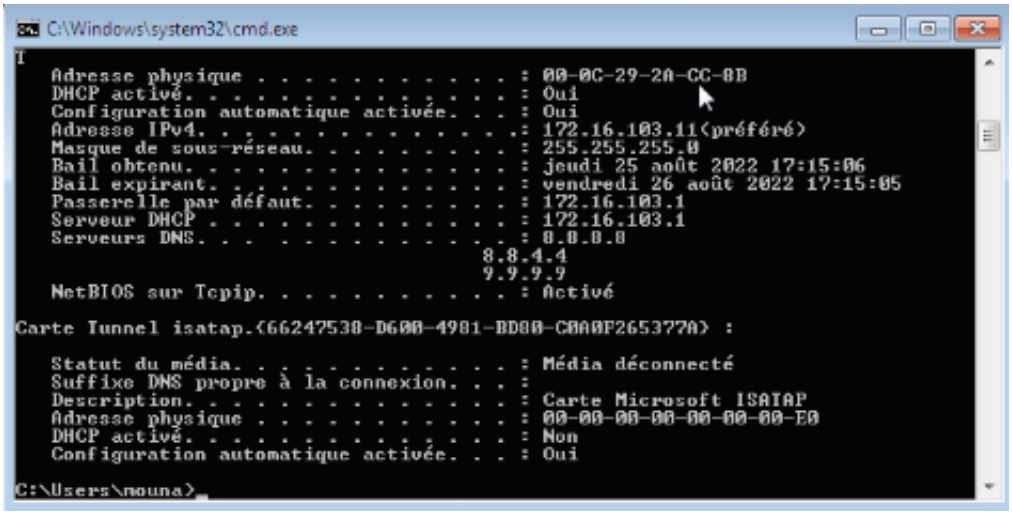

FIGURE 4.58 – Adresse mac d'une machine

3.Ensuite nous selectionnons l'adresses MAC autorisée.

```
SWA2(config-if)#switchport port-security mac-address 000C.292A.CC8B
```

4. dès que la "violation" est constatée, le port passe en état err-disabled (shutdown) et un message de log est envoyé.

```
SWA2(config-if)#switchport port-security violation shutdown
```

5. Pour voir le détail de la sécurité d'une interface

```
SWA2#show port-security interface ethernet 3/3
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.292a.cc8b:103
Security Violation Count   : 1
```

FIGURE 4.59 – Détail de la sécurité

Nous appliquons la même configuration sur chaque port.

4.8.4 Autre aspect de sécurité

4.8.4.1 Implémentation d'un pfsense

- Nous entrerons les informations d'identification suivantes : L'adresse IP dans le navigateur **10.0.0.1**

– Username : **salah** – Password : **Asr2022**

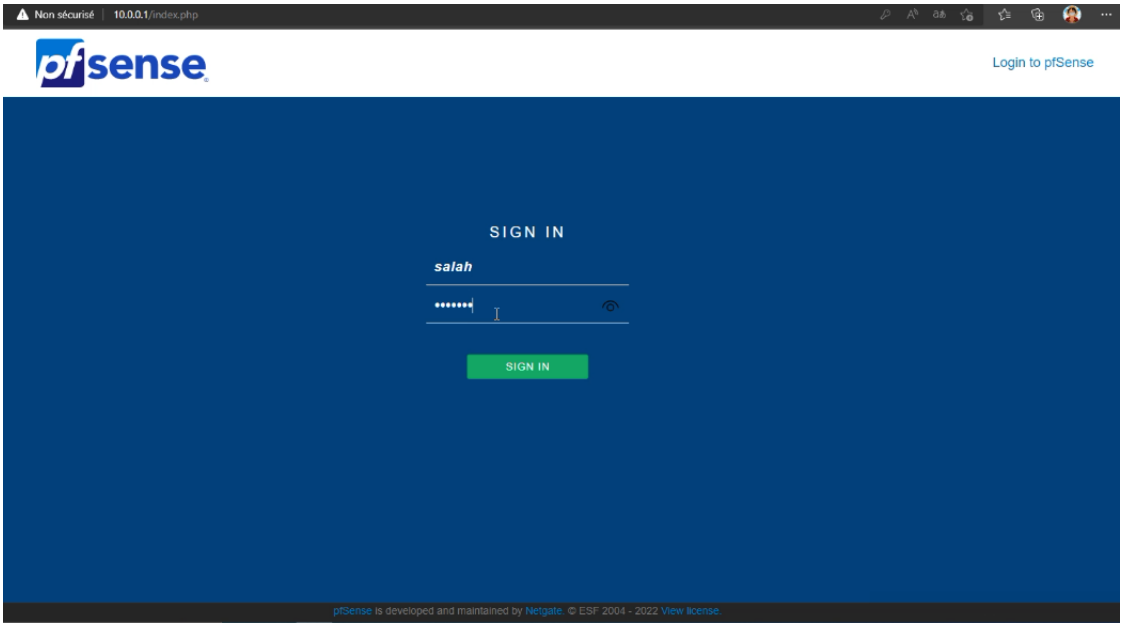

FIGURE 4.60 – Connexion à l'interface web pfsense

Pour avoir le controle de traffic nous accedons au firewall et nous appliquons des régles de controle d'acceé (accorde, blocage,...) soit de l'intèrieur vers l'éxtèrieur ou bien le contraire.

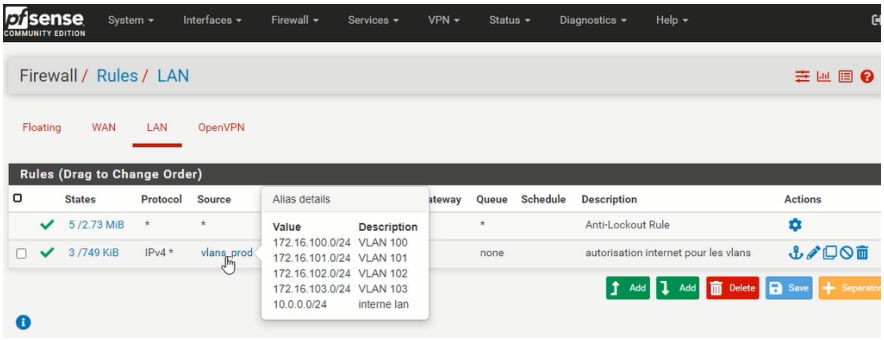

FIGURE 4.61 – Configuration des regles d'interfaces LAN

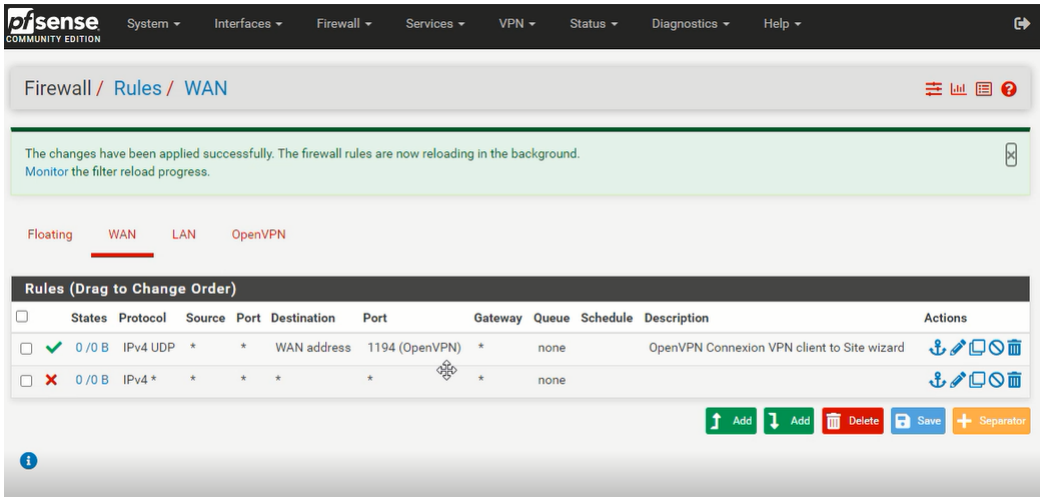

FIGURE 4.62 – Configuration des regles d'interfaces WAN

4.8.4.2 Mise en place de la solution VPN

-Apres avoir télechargé la préconfiguration de Openvpn sur PfSense nous devons l'installer sur notre client vpn.

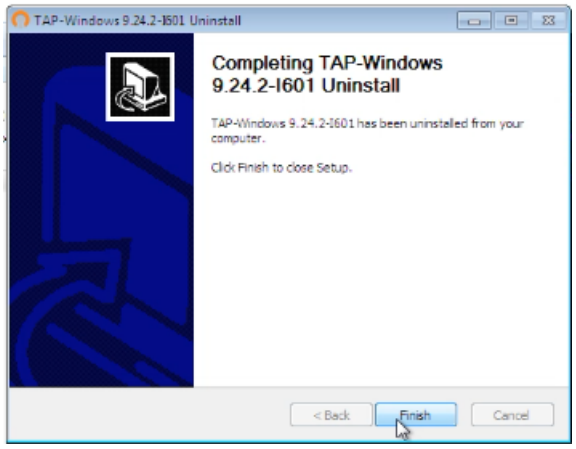

FIGURE 4.63 – Installation le client OpenVPN.

-Nous devons fournir le nom d'utilisateur "mona" et le mot de passe "123456789" pour se connecter.

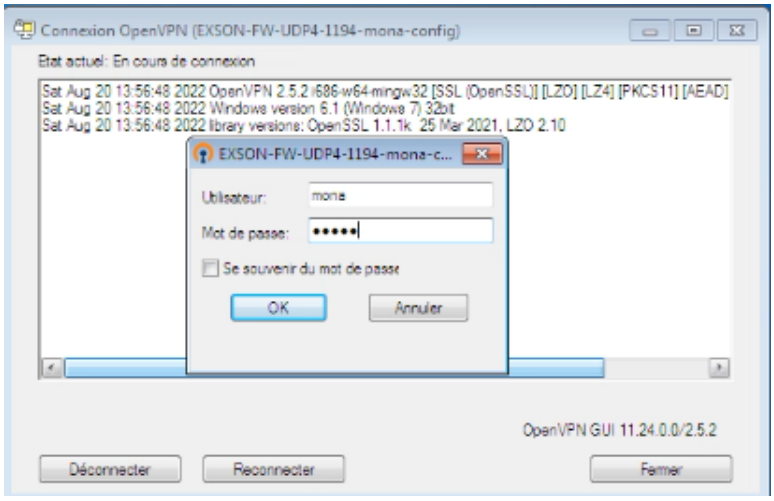

FIGURE 4.64 – Authentification client vpn

-Maintenant nous pouvons voir les utilisateurs connecté au vpn dans la figure 4.59, et cela ségnifie que nous pouvons accèder au par-feu à distance.

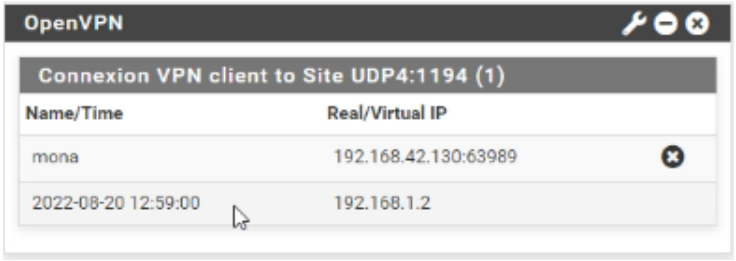

FIGURE 4.65 – Zone autorisée pour les clients vpn

4.9 Conclusion

Tout au long de ce chapitre, nous avons presenté notre environnement de travail, comme nous avons montré la configuration de base de notre architecture proposé, ensuite nous avons simulé un certain nombre de scénarios d'attaque contre notre maquette VoIP et mis en œuvre une variété d'outils pour assurer la sécurité de notre infrastructure.

Conclusion générale

La sécurité de la VoIP est un problème capitale, bien que trop souvent délaissé pour diminuer les coûts d'investissements, et qui pose des problèmes qui ne sont pas toujours simples à résoudre.

L'objectif de notre travail est la mise en place d'une solution open source sécurisée pour les services voix sur ip, pour cela, nous avons utilisé le logiciel Elastix qui possède des fonctionnalités puissantes lui permettant de s'imposer dans l'avenir.

Nous avons entamé le sujet par une étude théorique ciblée et concise pour comprendre les protocoles, les architectures, et le fonctionnement de la technologie VoIP.

Puis, nous avons procédé à une étude comparative de différentes solutions open source disponibles sur le marché afin de choisir la solution la plus adaptée à Exson Telecom.

Ensuite, nous avons étudié les attaques qui peuvent compromettre le serveur VoIP et mis en œuvre les solutions de sécurité nécessaires remédiant à ces attaques.

L'intérêt de mon projet réside dans le fait que les entreprises, bénéficiant de cette solution, seront capables de mettre en place une plateforme de VoIP assez flexible, peu couteuse, et protégée contre les attaques de l'intérieur du réseau comme de l'extérieur.

Ce travail nous a permis d'élargir nos connaissances dans de nombreux domaines en nous initiant au système d'exploitation Linux, en nous apprenant à configurer les outils Asterisk et PfSense ainsi que la configuration des switchs et routeurs, et en nous faisant découvrir le monde professionnel et les technologies émergentes en matière de réseaux Internet. De plus, cette expérience fructueuse nous a permis de mieux comprendre le monde de l'entreprise et d'apprendre à gérer et optimiser notre temps afin d'en tirer le meilleur parti.

Bibliographie

[1] http ://www.wikipédia.org, 2022

[2] “Memoire Online - Etude et Mise Au Point Dun Systeme de Communication VOIP : Application Sur Un PABX-IP Open Source „Cas de Lagence En Douane Getrak - Yannick YANI KALOMBA.” Memoire Online. Accessed May 19, 2014. http ://www.memoireonline.com/08/11/4644/m-Etude-et-mise au-point-dun-systeme-de-communication-VOIP–application-sur-un-PABX-IP open-source10.html.

[3] “AST-InstallingAsteriskNOW-190514-1559-12780.pdf.” Accessed May 19, 2014. https ://wiki.asterisk.org/wiki/download/temp/pdfexport-20140519- 190514-1559-12779/AST-InstallingAsteriskNOW-190514-1559- 12780.pdf?content-Type=application/pdf.

[4] Asterisk ,https ://www.networklab.fr/,2022

[5] ROSENBERG, Jonathan et SCHULZRINNE, Henning. Session initiation protocol (SIP) : locating SIP servers. 2002.

[6] OTT, Joerg, WENGER, Stephan, SATO, Noriyuki, et al. Extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF). 2006.

[7] KUHN, D. Richard, WALSH, Thomas J., FRIES, Steffen, et al. Security considerations for voice over IP systems. NIST special publication, 2005, vol. 800.

[8] Qu’est-ce qu’Asterisk?, https ://ar.21-bal.com/doc/6521/index.html, 2022.

[9] “Patrick papier-Kourou-v2.pdf.” Accessed May 19, 2014. http ://web.univ-pau.fr/ gallon/publis/patrick-papier-kourou-v2.pdf.

[10]] “ToIP.pdf.” Accessed May 19, 2014. http ://web.univpau.fr/ cpham/M2SIR/BIBLIO/DOC04-05/ToIP.pdf.

[11] BOUZAIDA, Rebha. Étude et Mise en place d’une Solution VOIP Sécurisée. 2011. Thèse de doctorat. Université Virtuelle de Tunis, 2022.

[12] attaque sur les protocoles, https ://ts5ri-voip-pfe.fr.gd/Attaques-sur-les-protocoles.htm, 2022.

[13] https ://www.rapport-gratuit.com/vulnerabilites-contre-la-voip-et-quelques-moyens-de-securisation/, 2022.

[14] WERGHUI, Saida. Mise en place d’un outil de monitoring de réseau à base de logiciel libre. 2019. Thèse de doctorat. Université Virtuelle de Tunis, 2022.

[15] Tshimanga, D. "Etude d’implémentation d’une solution VOIP sécurisée dans un réseau informatique d’entreprise." Cas de l’ISTA de Kinshasa Institut supérieur de techniques appliquées de Kinshasa-Ingénieur en génie électrique option informatique appliquée (2012).

[16] https ://www.academia.edu/39080897/CHAPITRE-III-RISQUES-ET-METHODES-DE-SECURITE-DE-La-VOIP, 2022.

Résumé

La téléphonie IP a de nos jours pris beaucoup d'ampleur dans le monde des télécommunications en particulier pour les entreprises qui utilisent des services de centres d'appels. En effet, l'adoption de cette technologie pour avantage d'offrir des services de voix, images ou vidéos tout en minimisant les coûts de communication.

Dans le cadre de notre projet, nous avons réalisé une solution VoIP en utilisant le serveur Elastix. Cette solution est bien sécurisée pour l'utilisation personnelle et professionnelle qui permet de mettre en place un système téléphonique complet et d'établir un centre d'appels pour n'importe quel organisme en utilisant le protocole SIP.

L'implémentation de cette architecture a été faite avec des outils open source dont les softphones, le serveur Elastix et VMware Workstation.

Mots clés : VOIP, Elastix, SIP, VMware workstation, softphones.

Abstract

IP telephony has nowadays taken a lot of importance in the world of telecommunications, especially for companies that use call center services. Indeed, the adoption of this technology has the advantage of offering voice, image or video services while minimizing communication costs.

As part of our project, we have implemented a VoIP solution using the Elastix server. This solution is well secured for personal and professional use and allows to set up a complete telephone system and to establish a call center for any organization using the SIP protocol.

The implementation of this architecture was done with open source tools including softphones, Elastix server and VMware Workstation.

Keywords : VOIP, Elastix, SIP, VMware workstation, softphones.