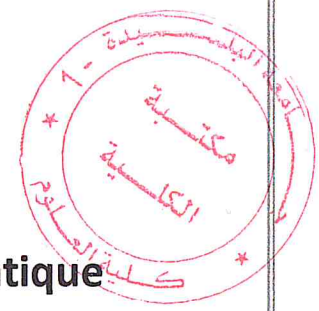
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de laRecherche Scientifique

Université de Saad Dahleb – Blida

Faculté des Sciences
Département d'informatique



Mémoire de MASTER
Domaine : Mathématique et Informatique
Spécialité : Informatique
Option :(Sécurité des systèmes d'information SSI)

THEME

Etude et mise en œuvre d'une architecture de téléphonie sur IP sécurisée Au sein du NAFTAL

Proposé et dirigé par :
Mme. Otman Saida

Promoteur:
Djillali Nehal

Soutenu le 27 /09/2018
Devant le jury composé de :
Présidente de jury : Mlle.Arkam Meriem
Examinatrice : Mme.Aroussi Sana

Présenté par :
Mlle. Dahri Meriem
Mlle. Djemai Karima

Promotion : 2017-2018

Remerciment

Louange à notre créateur qui nous a incités à acquérir le savoir. C'est à lui que nous adressons toute notre gratitude en premier lieu.

Ce travail est l'aboutissement d'un long cheminement au cours du quel nous avons bénéficié des encouragements et du soutien de plusieurs personnes, à qui on tient à dire profondément et sincèrement merci.

Nous remercions nos parents et nos frères à qui nous devons beaucoup de respect et d'admiration, et nous leurs disons mille mercis.

Nos sentiments de reconnaissance vont en premier lieu à l'endroit de notre promoteur

Mr. Djillali Nehal

Nous tenons à présenter nos salutatier erfons et notre gratitude envers lui, pour son soutien, sa patience et son aide précieuse.

Aussi nous exprimons notre profonde gratitude à nos encadreurs Mr Kasmi Med(رحمه الله), Mme Otman Saida d'avoir dirigés ce travail.

Nos remerciements s'adressent également à Madame la présidente et les membres du jury pour l'honneur d'avoir assisté à notre soutenance et jugé ce modeste travail.

Finalement, nous voudrons adresser nos vifs remerciements à tous les amis, enseignants, et personnels de l'Université Saad Dahleb Blida-1 qui ont contribué à notre formation.

Dédicace

A celle qui m'a donné la vie, le symbole de tendresse, qui s'est sacrifiée pour mon bonheur et ma réussite, A ma mère

A mon père, école de mon enfance, celui qui a été mon ombre durant toutes les années des études, Que Dieu les garde et les protège.

A mes adorables soeurs Imen , salma Siham ,linda et à mon frère mourad

Je dédie ce travail.

Meriem...

Je dédie ce travail à ma chère famille pour leur priare : ma mère, pour les sacrifices pendant mes longues années d'étude et mon père pour son effort son soutien . Je témoigne ma reconnaissance pour leurs encouragements.

A mes belles sœurs Nassima, Fatima , Fatiha, Ilham.

A mes chérs Badreddine , Alaa ,Dina , Youness ,adem , Mohamed ,Yasser, Abd-elrahman

A mes amis qui contribuent à l'achèvement de ce projet, pour leurs soutiens moraux et leurs encouragements illimités.

Karima...

Résumé

Ces dernières années, la téléphonie est considérablement connaît une grande révolution avec émergence de la téléphonie sur IP. Cette dernière fournit des services de télécommunications flexibles tout en réduisant les coûts opérationnels.

Cependant, la VoIP doit également faire face à plusieurs risques comprenant des vulnérabilités liées aux niveaux des protocoles et aux dispositifs réseau.

Ce travail vise à se concentrer sur les menaces de sécurité spécifiées à la VoIP et les contre-mesures. Afin de réduire les risques et renforcer le niveau de sécurité de cette dernière.

Mots Clés : VOIP, Sécurité, Vulnérabilité, Protocole, menaces

Abstract

In recent years, telephony is experiencing a major revolution with the emergence of IP telephony, which provides flexible telecommunications services while reducing operational costs.

However, VoIP also faces several risks including vulnerabilities related to protocol levels and network devices.

This work aims to focus on the specified security threats to VoIP and countermeasures, to reduce the risks and enhance the level of security of the latter.

Key Words: VOIP, Security, Vulnerability, Protocol, Threats.

ملخص

في السنوات الأخيرة ، شهدت المهاتفة ثورة كبيرة مع ظهور المهاتفة عبر بروتوكول الإنترنت ، التي توفر خدمات اتصالات مرنة مع تقليل التكاليف التشغيلية.

ومع ذلك ، فإن VoIP يواجه أيضًا العديد من المخاطر بما في ذلك نقاط الضعف المتعلقة بمستويات البروتوكول وأجهزة الشبكة.

يهدف هذا العمل إلى التركيز على التهديدات الأمنية المحددة لنقل الصوت عبر بروتوكول الإنترنت (VoIP) والتدابير المضادة، وذلك للحد من المخاطر وتعزيز مستوى أمن هذا الأخير.

الكلمات المفتاحية VOIP، الأمن ، الضعف ، البروتوكول ، التهديدات.

Table des matières

Liste des figures

CHAPITRE I : GENERALITE SUR LA TELEPHONIE SUR IP

CHAPITRE II : VULNERABILITES ET MESURES DE SECURITE DE LA TOIP

CHAPITRE III: PRESENTATION DE L'ORGANISME D'ACCEUIL

CHAPITRE IV: MISE EN ŒUVRE D'UNE ARCHITECTURE TOIP SECURISEE

Liste des tableaux

CHAPITE I GENERALITE SUR LA TELEPHONIE SUR IP

CHAPITE IV MISE EN ŒUVRE D'UNE ARCHITECTURE TOIP SECURISEE

Introduction Générale

La téléphonie a récemment connu à une grande révolution avec l'apparition et l'émergence de téléphonie IP, ce qui pose certains problèmes de sécurité, comme d'autres technologies dans le monde de l'informatique.

La téléphonie IP combine les vulnérabilités de la téléphonie traditionnelle et celles des réseaux informatiques.

Avec l'intégration de la VoIP dans les systèmes d'information et dans le monde des réseaux IP, la sécurité de ce service est vraiment complexe. Les exigences relatives à l'authentification, à la confidentialité, à l'intégrité, au respect de la vie privée et à la non-répudiation doivent être prises en compte.

La question est donc comment mettre en œuvre une solution vigoureuse avec les infrastructures actuelles.

L'objectif de ce travail est de définir les risques liés à une session de communication VoIP et de mettre en œuvre une architecture de téléphonie sur IP en proposant des solutions de sécurité robustes.

Ce mémoire se décompose en quatre chapitres :

- Le premier chapitre présente l'organisme d'accueil NAFTAL.
- Le deuxième chapitre introduit en générale la téléphonie sur IP et le fonctionnement de ces protocoles.
- Le troisième chapitre cite les failles de sécurités liées à la VoIP, et les différentes solutions pour déterminer une architecture sécurisée.
- Le dernier chapitre, fournit un aperçu sur les outils choisis, en illustrant la configuration mise en place pour établir l'architecture sécurisée.
- On terminera ce mémoire par une conclusion générale et des perspectives de sécurisation de la ToIP.

CHAPITRE I

Généralité sur la Téléphonie sur IP

Introduction

La téléphonie sur IP est apparue grâce à la démocratisation des connexions Internet Haut-débits et des réseaux Ethernet pour les réseaux locaux. Dans ce chapitre, nous allons définir la T-VoIP et également ses protocoles de fonctionnement.

I.1. Présentation de la VoIP (Voice Over IP)

La VoIP (Voice Over IP) est une technologie de communication vocale concerne le cœur du système de téléphonie, qui comprend tous les éléments assurant le transport de la voix : PABX[1], passerelles de communication, réseaux opérateurs, communication intersites, protocole de communication. [19]

I.2. Présentation de la ToIP (Telephony Over IP)

La téléphonie sur IP ou ToIP (Telephony over IP) concerne uniquement la partie correspondante aux téléphones IP(materiel),les softphones ou logiciels téléphonique, qui s'installent sur PC et qui « émulent » un téléphone IP, rentrent tout à fait dans cette catégorie.[19]

D'où, la ToIP est un service de téléphonie qui transporte les flux voix des communications téléphoniques sur un réseau IP. A la différence de la VoIP où l'on ne fait qu'établir une communication « voix », la ToIP intègre l'ensemble des services associés à la téléphonie : double appel, messagerie, renvoie d'appel, FAX, etc. [5]

I.3 La différence entre la ToIP et la VoIP

Nous faisons souvent un amalgame entre la téléphonie sur IP et la voix sur IP. Cela est normal, car les deux concepts sont très proches. La nuance réside dans le fait que la VoIP est inclue dans la ToIP. La VoIP représente seulement la technologie de transport de voix sur le protocole Internet. La ToIP, représente la VoIP en addition de toutes les applications téléphoniques qu'il peut y avoir. [20]

Le schéma ci-dessous explique cette différence:

[1] PABX : C'est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur et le réseau RTC. Toutefois, si tout le réseau devient IP, ce matériel devient obsolète.

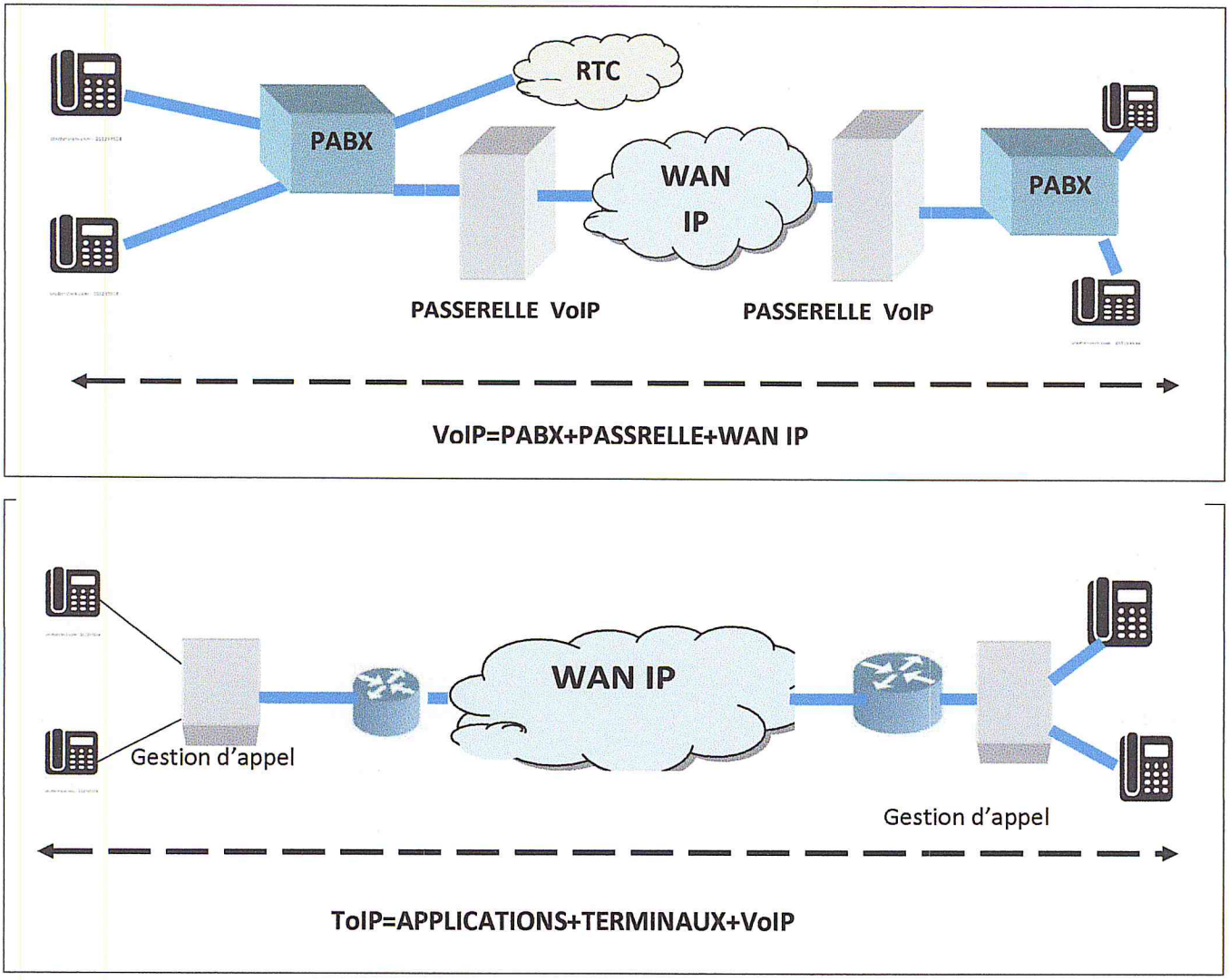


Figure I.1 : La différence entre la ToIP et la VoIP.

La VOIP est ainsi une technique qui permet la communication par la voix (audio ou vidéo), sur des réseaux compatibles IP, que ce soit un réseau privé ou Internet, filaire (câble, ADSL, fibre optique), ou non filaire (satellite, wifi, GSM). La VOIP comprend donc les communications de PC à PC, dans lequel chaque utilisateur utilise le logiciel adéquat. Si la communication passe par Internet, on parle de TOIP, la téléphonie par Internet. Les communications peuvent également passer entre un PC et un téléphone, dans lesquelles le PC se « transforme » en téléphone, grâce à des logiciels spécifiques, et le PC est appelé « softphone ». [21]

I.4. Fonctionnement technique

Contrairement au RTC, qui utilise le fil de cuivre traditionnel pour arriver chez le correspondant, la VoIP utilise le réseau maillé du web pour effectuer ses transmissions. En effet, elle utilise le protocole TCP/IP pour faire voyager les données (ici entièrement numériques [0 et 1]) entre les correspondants, et ce par n'importe quel chemin. [21]

Les données (voix) sont coupées en petits paquets et compressées à l'aide d'un programme de codec avant d'être transmises. Une fois que les données sont parvenues au destinataire, l'opération inverse est appliquée sur la voix, à savoir la décompression et la restitution sonore.

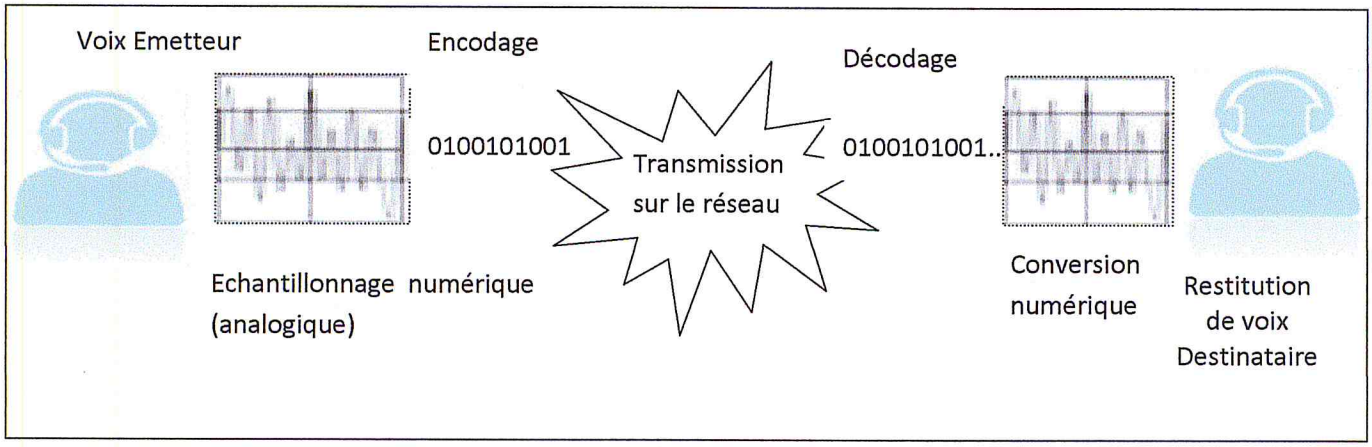


Figure I.2 -La transmission de la voix sur le réseau IP

I.5. Les avantages et les inconvénients de la téléphonie sur IP

La téléphonie sur IP dispose de nombreux avantages et inconvénients

I.5.1. Avantages de la téléphonie sur IP

La téléphonie sur IP dispose de nombreux avantages par rapport à la téléphonie classique :

- **La réduction des coûts opérationnels :** Les entreprises ont la possibilité de réduire leurs propres coûts de communication en transférant le trafic vocal de la téléphonie traditionnelle vers un réseau IP. En outre, des réductions de coûts importantes sont mises en évidence pour les communications internationales, car elles ne nécessitent pas de déploiement à l'image de la téléphonie classique.

- **Accessibilité** : Un système téléphonique IP, est nettement différent d'un système téléphonique traditionnel. La distance ou l'emplacement ne fait aucune différence pour un système de téléphonie IP, que ce soit pour appeler un siège social à l'autre bout du pays ou pour appeler à l'autre bout du monde. Tant qu'il y a une connexion Internet, la communication est possible.

- **Adaptabilité :** Les anciens systèmes propriétaires ne sont pas faciles à développer. En fait, l'ajout de lignes téléphoniques ou d'extensions nécessite des mises à jour matérielles souvent très coûteuses et, dans certains cas, une remise à neuf complète du réseau téléphonique.

- **Qualité de la voix :** S'il existe une connexion Internet fiable avec une bonne bande passante, l'utilisateur bénéficiera d'une qualité vocale équivalente ou même supérieure à une connexion téléphonique traditionnelle. mais si c'est dans une zone rurale sans lien fort, les qualités en souffriront

I.5.2. Inconvénients de la téléphonie sur IP

La téléphonie sur IP possède les mêmes contraintes temps réel que la téléphonie classique. Etant donné que cette technologie basée sur une commutation de paquets, elle est fortement liée aux contraintes suivantes :

- **La latence :** En raison des besoins en bande passante, certains appels peuvent sembler différer, différer ou disparaître complètement. En effet, les paquets d'informations ont besoin de temps pour être réassemblés afin de pouvoir

effectuer un appel efficace. Ce problème devient moins problématique à mesure que de nouveaux algorithmes de données plus sophistiqués sont utilisés.

- **le temps de numérisation de la voix** : la voix téléphonique est un signal analogique, impossible à coder sur un l'ordinateur, il faut donc la numériser avec un codeur, généralement, Le temps de numérisation est négligeable, mais le codec va déterminer la vitesse à laquelle les données sont émises. [22]

- **le temps de remplissage des paquets** : les données envoyées sont assemblées en paquets. Ces derniers, comportent des en-têtes, qui sont placées une fois le paquet constitué. On peut définir le temps de remplissage comme le temps utilisé par le codec pour remplir un paquet de taille fixée (la taille ne prend pas en compte les en-têtes qui sont ajoutés automatiquement et indépendamment du codec). [22]

- **le temps de propagation :** il se définit comme le rapport de la distance à parcourir entre l'émetteur et le récepteur sur la vitesse de propagation du signal. On prend généralement une vitesse de propagation d'un signal de 200 000 Km/s. [22]

- **le temps de transmission** : Le temps de transmission peut être défini comme le rapport entre la quantité de données à envoyer et le débit de la liaison considérée, les données arrivant d'un point à un autre en fonction de la quantité de données transmise et du débit des liaisons entre l'expéditeur et le destinataire.
- **La sécurité** : Les communications téléphoniques rencontrent divers problèmes, dont le plus important est la sécurité.

  Le piratage téléphonique a été une préoccupation majeure à cet égard. Les performances du pare-feu sont moins satisfaisantes en raison du temps réduit consacré à l'analyse des paquets de données. La téléphonie IP est également affectée par les vers et les virus. Tous ces éléments constituent une menace pour la sécurité.

I.6. Les Protocoles de ToIP

Une communication VoIP requiert plusieurs protocoles, certains servent à la signalisation, d'autres aux flux médias.

I.6.1.Les Protocoles de signalisation

La signalisation indique l'envoi d'un ensemble de signaux et d'informations de contrôle mutuel entre les intervenants d'une communication.

I.6.1 .1. Le protocole H.323

H.323, standard de (UIT-T) Union internationale des télécommunications -Secteur de la normalisation des télécommunications est un protocole de signalisation très commun utilisé sur les réseaux VoIP. H.323 rassemble trois catégories de protocoles : la signalisation, la négociation de codec et le transport de l'information.

La signalisation s'appuie sur le protocole RAS (Registration, Administration and Status) pour l'enregistrement et l'authentification, et le protocole Q.931 pour l'initialisation et le contrôle d'appel. Ce protocole est une spécification du système comprenant plusieurs autres sous- protocoles UIT-T, y compris H.225 (gère l'enregistrement, l'admission et le statut), H.245 (le protocole de contrôle), H.450 (offre des services supplémentaires), H.235 (fournit des services de sécurité pour les canaux de signalisation et de média), H.239 (offre une diffusion en double) et H.460 (permet la traversée du pare-feu).

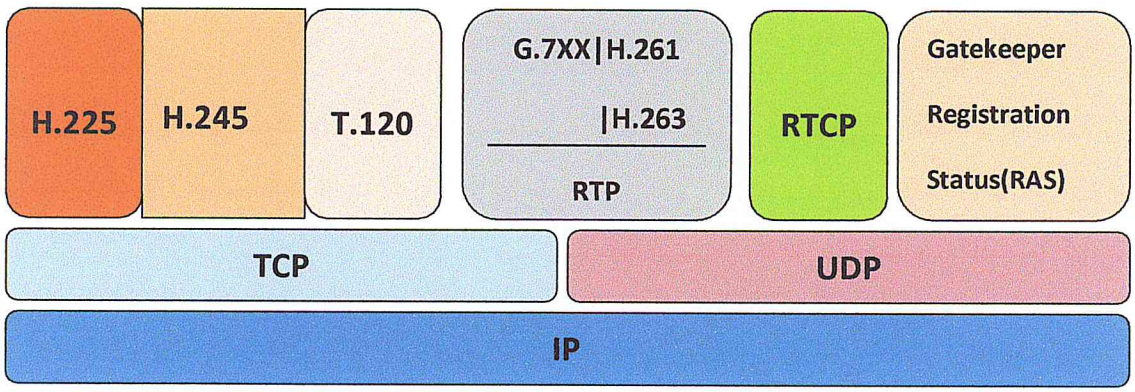


Figure I.3. Association de protocoles H323

De nombreux déploiements VoIP utilisent H.323 car ils s'intègrent mieux avec les systèmes PBX existants offrent une grande fiabilité. Cependant, ce protocole ne garantit pas l'interopérabilité.

I.6.1.2. Le protocole SIP

SIP (Session Initiation Protocol) est un protocole de signalisation défini par l'IETF (Internet Engineering Task Force) permettant l'établissement, la libération et la modification de sessions multimédias [RFC 3261].

Aujourd'hui, SIP a donné son nom à l'ensemble de la structure TOIP, basée sur ses propres fonctionnalités de signalisation. De plus, il est important de noter que SIP n'est pas spécifique à la téléphonie sur IP, et peut être utilisé dans toutes les technologies utilisant le concept de session.

Le protocole SIP dispose d'une grande capacité d'intégration à d'autres protocoles standards du monde IP. Ce qui lui confère son caractère modulaire, lui permettant ainsi de fonctionner avec différentes applications telles que la téléphonie, la messagerie instantanée, la vidéo conférence, la réalité virtuelle et même le jeu vidéo. [22]

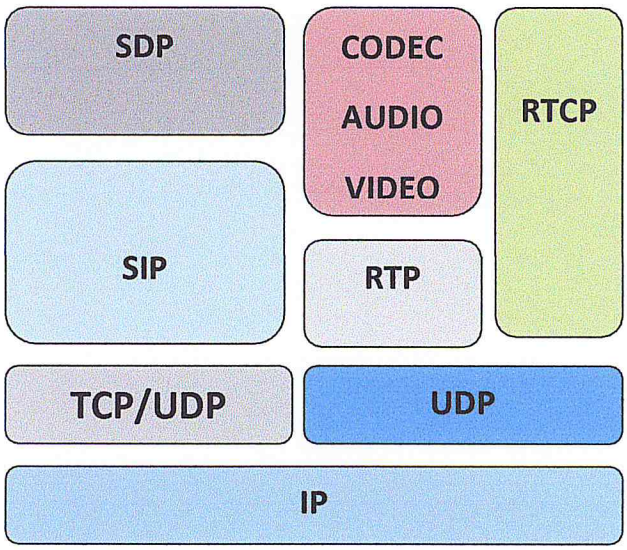


Figure I.4-La pile protocolaire de SIP

L'établissement d'une communication se fait a travers l'échanges des messages entre les différentes entités du réseau.Une fois la session établie, les échanges de données (voix,

images, vidéo) se font entre les deux extrémités. La voix est quant à elle transportée par le protocole RTP [RFC3550].

A. Entités SIP

Il existe deux familles d'entités SIP, les usagers et les serveurs. L'usager ou UA (User Agent) émet et reçoit les appels. Chaque UA est associé à un identifiant appelé URI SIP (Uniform Resource Identifier). Les URIs contiennent normalement le nom d'utilisateur et le domaine d'appartenance.

À propos des serveurs, il en existe de 4 types :

Le Serveur	Description
Registrar Server	Il s'occupe exclusivement de l'enregistrement des terminaux SIP. Il reçoit les messages de type REGISTER. Il identifie les utilisateurs. Il doit être relié à un Proxy Server ou à un Redirect Server qui sera en charge de l'appel.
Proxy Server	Il sert de relais aux messages SIP. Il joue le rôle de serveur d'un côté et de client de l'autre. Il interprète, transforme ou traduit un message avant de le transférer.
Redirect Server	Il gère la signalisation d'appel comme le Poxy Server, mais il ne relaie pas les messages. Il redirige directement l'UA vers la destination requise en lui indiquant l'adresse IP et le port à contacter.
Location Server	Il est utilisé par les deux types de serveur précédents pour obtenir des informations sur les différentes localisations possibles d'un utilisateur.

Tableau I.1: les serveurs SIP

B. Méthodes SIP

Les méthodes SIP sont des requêtes et des réponses SIP pour constituer un appel.

Messages SIP

Les communications SIP se font au moyen d'une série de messages qui peuvent être de deux natures des requêtes qui Permet d'invoquer une opération particulière, ou bien des réponses qui permet d'informer l'initiateur d'une requête que cette dernière a bien été reçue, traitée, et voir aussi du résultat obtenu après le traitement. Chaque message est

composé d'une première ligne qui indique le type de message, de l'en-tête du message (en-tête SIP) et optionnellement du corps du message. Les deux derniers sont séparés par une ligne vide. Le corps du message peut être de plusieurs types. Le plus courant est un message SDP inclus dans une requête INVITE. La grande malléabilité du protocole SIP provient entre autres de la liberté de créer des requêtes et/ou réponses personnalisées. Il est donc possible de créer des services supplémentaires [4]. Voici un exemple de message SIP :

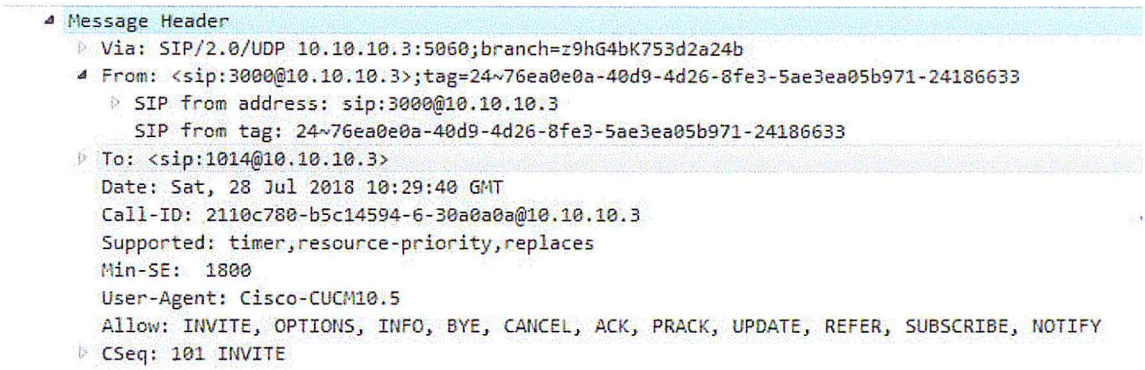


Figure I.5. Exemple de message SIP

En-tête SIP

L'en-tête SIP est écrit sous la forme d'une succession de champs, dont voici les principaux :

Champ d'en-tête	Description
Call-ID	Identifiant unique pour un échange d'établissement particulier.
CSeq	Identifie une requête à l'intérieur d'une session.
From	Initiateur de la requête.
Content- Type	Indique le type de média du corps du message envoyé
To	Précise le destinataire de la requête.
User- Agent	Chaîne de caractères stipulant le terminal utilisé pour envoyer ce message
Content- Length	Indique la taille du corps du message

Tableau I.2- Les principaux champs d'en-tête des messages SIP

Voici un exemple de message INVITE envoyé :

```
INVITE sip:3000@10.10.10.3:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.10.60:54350;branch=z9hG4bK-d8754z-
2276ea7078368225-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:1410@10.10.10.60:54350;rinstance=bbd5caed8ad84b18>
To: <sip:3000@10.10.10.3:5060>
From: "MeriemDahri"<sip:1410@10.10.10.60:5060>;tag=f33afb19
Call-ID: MzY4YzAwY2ZlZDhiMjgwZTQ5ZjZiOTYzZGRhZDNkNTQ.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE,
NOTIFY, REFER, INFO, MESSAGE
Content-Type: application/sdp
Supported: replaces
User-Agent: 3CXPhone 6.0.26523.0
Content-Length: 398
```

Figure I.6. Exemple de message INVITE

Requêtes SIP

Il existe plusieurs types de requêtes SIP. Néanmoins, les plus importantes sont décrites ci dans ce Tableau suivant :

Requête	Définition
INVITE	Requête d'établissement d'une session invitant un usager à participer à une communication téléphonique ou multimédia ; l'émetteur de cette requête y indique les types de media qu'il souhaite et peut recevoir, en générale au travers d'une description de session SDP. [RFC4566]
ACK	Requête d'acquittement, émise pour confirmer que le client émetteur d'un INVITE précèdent a reçu une réponse finale ; cette requête peut véhiculer une description de session qui clôt la négociation.
BYE	Requête de clôture d'un appel.
CANCEL	Requête d'annulation, signifiant au serveur de détruire le contexte d'un appel en cours d'établissement (cette requête n'a pas d'effet sur un appel en cours).
OPTIONS	Cette requête permet à un client d'obtenir de l'information sur les capacités d'un usager, sans pour autant provoquer l'établissement d'une session.
REGISTER	Requête à destination d'un serveur SIP et permettant de lui faire parvenir de l'information de localisation (machine sur laquelle se trouve l'utilisateur).

Tableau I.3: Les requêtes SIP

Réponses SIP

Les réponses sont identifiées par un code définit par la version 2 du protocole SIP. Le code consiste en une valeur allant de 100 à 699, ces dernières étant classées en 6 catégories de réponses :

Code	Définition de la famille de réponse	Principales Réponses
1XX	Réponse intermédiaire d'information (traitement en cours)	- 100 Trying - 180 Ringing
2XX	Succès	- 200 OK
3XX	Redirection	301Moved permanently - 302 Moved temporarily
4XX	Erreur client	- 400 Bad Request - 401 Unauthorized
5XX	Erreur serveur	- 500 Server Internet Error - 501 Not Implemented
6XX	Echec global du traitement	- 603 Decline

Tableau I.4 : Les réponses SIP

Un exemple d'appel SIP illustré par le diagramme suivant :

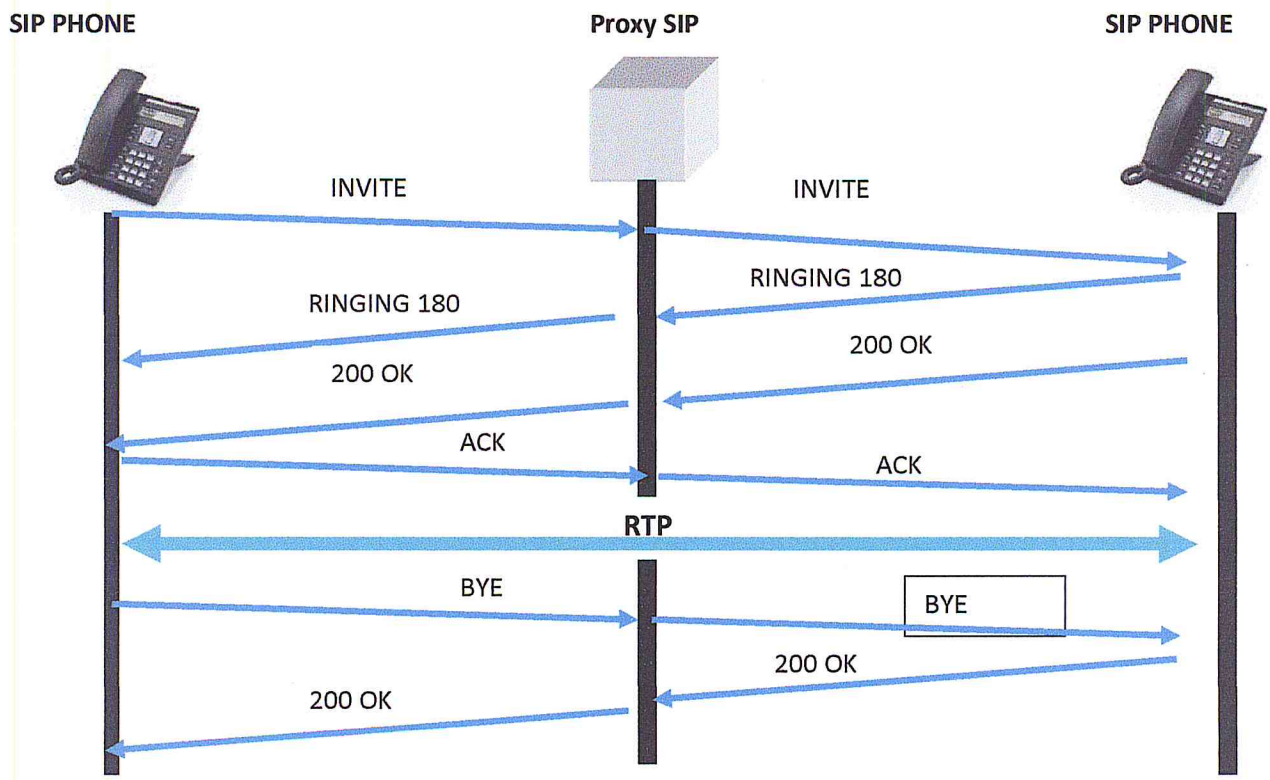


Figure I.7 Initialisation d'appel SIP

D'autres protocoles sont utilisés pour l'établissement de la session comme : SCCP, MGCP.

Dans ce projet, nous avons intéressé par le protocole SIP pour sa simplicité, sa rapidité et sa facilité d'utilisation.

C. Avantages de protocole SIP

- L'implémentation de la VoIP avec le protocole de signalisation SIP (Session Initiation Protocol) fournit un service efficace, rapide et simple d'utilisation. SIP est un protocole rapide et léger. La séparation entre ses champs d'en-tête et son corps du message facilite le traitement des messages et diminue leur temps de transition dans le réseau.[25]
- Les utilisateurs s'adressent à ces serveurs Proxy pour s'enregistrer ou demander l'établissement de communications. Toute la puissance et la simplicité du système viennent de là. On peut s'enregistrer sur le Proxy de son choix indépendamment de sa situation géographique. L'utilisateur n'est plus "attaché" à son autocommutateur. [25]
- Une entreprise avec plusieurs centaines d'implantation physique différente n'a besoin que d'un serveur Proxy quelque part sur l'Internet pour établir "son" réseau de téléphonique "gratuit" sur l'Internet un peu à la manière de l'émail [25]

D. Inconvénients de protocole SIP

L'une des conséquences de cette convergence est que le trafic de voix et ses systèmes associés sont devenus aussi vulnérables aux menaces de sécurité que n'importe quelle autre donnée véhiculée par le réseau.

En effet SIP est un protocole d'échange de messages basé sur HTTP. C'est pourquoi SIP est très vulnérable face à des attaques de types DoS (dénis de service), détournement d'appel, trafic de taxation etc... [4]

E. Protocole SDP (*Session Description Protocol*)

Le protocole de description de session (SDP) est utilisé par les protocoles de signalisation telle que SIP avant l'ouverture du flux média

Lors de l'initialisation d'une session, SDP fournit des informations sur le contenu multimédia qu'un agent utilisateur demande à utiliser, ainsi que d'autres informations nécessaires à la configuration du transfert de ces données.

I.6.1.3. MGCP

MGCP est un protocole de contrôler les passerelles multimédia de signalisation définie par RFC 3435 qui permet d'établir et assure la connectivité entre le réseau IP et le réseau téléphonique. Il fonctionne au niveau applicatif et permet d'offrir une couverture plus large en fédérant toutes les signalisations, qu'elles soient de type IP ou RTC entre autres. C'est le maître d'œuvre de l'interopérabilité entre tous les protocoles de signalisation et tous les réseaux, de quelque nature qu'ils soient, qu'il s'agisse de la signalisation, utilisée dans un réseau commuté, H.323 ou SIP. Le protocole MGCP est conçu pour relier et faire communiquer l'ensemble de ces réseaux. MGCP est aujourd'hui massivement utilisé par les fournisseurs d'accès Internet pour assurer le contrôle et l'administration à distance des boîtiers (box) mis à disposition de leurs abonnés. [26]

I.6.1.4. SCCP

Le SCCP, communément appelé "***Skinny***", a été initialement développé par SELSIUS Corporation, et actuellement, un protocole de contrôle de terminal propriétaire de Cisco utilisé pour l'établissement, la modification et la suppression d'appels dans des environnements VOIP (Voice over IP).C'est un protocole léger utilisé pour la signalisation de contrôle de session avec Cisco CallManager.

Le gestionnaire d'appel ou le commutateur logiciel contrôle le traitement d'établissement d'appel initié sur la plupart des autres protocoles courants tels que H.323, SIP, RNIS, MGCP, tandis que les points d'extrémité diffusent le média directement entre eux.

SCCP utilise le port TCP 2000 comme chemin de signalisation et utilise UDP comme chemin de média. Dans un réseau pris en charge par le sous-système SCCP où les points de terminaison sont des postes téléphoniques VoIP ou des dispositifs dotés de la fonction VoIP, exécutez un programme appelé le client maigre qui minimise le coût et la complexité des points de terminaison VoIP.[27]

I.6.2. Les protocoles de transport

Les protocoles de transport de la téléphonie sur IP servent à transmettre les données entre deux ou plusieurs points.

I.6.2.1. RTP

RTP est un protocole utilisé pour la transmission des paquets de voix est typiquement le *Real-time Transport Protocol*, RTP [RFC 3550]. Les paquets RTP ont des en-têtes spéciaux qui permettent de les réassembler correctement lors de la réception. Les paquets de voix seront transmis comme une « *payload* » du protocole UDP qui est également employé pour la transmission de données. En d'autres termes, les paquets RTP sont échangés comme des données par les datagrammes UDP, qui peuvent alors être traités par un réseau en mode paquet tel qu'Internet.Le but de RTP et de fournir un moyen uniforme de transmettre sur IP des données soumises à des contraintes de temps réel (audio, vidéo, etc.).[23]

Les fonctions fournies par RTP comprennent:

- Séquençage: le numéro de séquence dans le paquet RTP est utilisé pour détecter les paquets perdus.

- *Identification Payload*: sur Internet, il est souvent nécessaire de modifier l'encodage ajuster à la disponibilité de la bande passante. Pour fournir cette fonctionnalité, un identifiant de charge utile est inclus dans chaque paquet RTP pour décrire le codage du média.
- Indication *Frame* : La vidéo et l'audio sont envoyés dans des unités logiques appelées *frames*. Pour indiquer le début et la fin de *frame*, un bit marqueur de *frame* a été fourni.

- Identification de la source: dans une session de multidiffusion, nous avons beaucoup de participants. Un identifiant est donc nécessaire pour déterminer l'auteur du cadre. Pour cette source de synchronisation (SSRC), l'identifiant a été fourni.

- Synchronisation *Intramedia*: pour compenser la gigue différée pour les paquets dans le même flux, RTP fournit des horodatages nécessaires aux tampons de lecture.

Le protocole RTP permet de reconstituer la base de temps des différents flux multimédia (audio, vidéo, etc.), détecter les pertes de paquets, et d'identifier le contenu des paquets pour leur transmission sécurisée. Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'apporter une fiabilité dans le réseau. Ainsi il ne garanti pas le délai de livraison. [24]

I.6.2.2. RTCP

RTCP (Real-time Transport Control Protocol ou protocole de transport en temps réel) accompagne RTP. Il est basé sur la transmission périodique de paquets de contrôle par tous les participants dans la session. Ainsi RTCP est un protocole de contrôle du trafic RTP. Il permet de transmettre des informations sur la qualité de service et peut aussi fournir des informations basiques sur les participants de la session. [23].

Le protocole RTCP possède quatre fonctions, il permet de :

- Fournir des informations sur la qualité de la session (Ce feedback permet à la source de changer de politique de transmission et met en évidence des défauts de distribution individuels et/ou collectifs).
- Garder une trace de tous les participants à une session grâce au
- CNAME (Canonical Name). C'est un identifiant unique et permanent propre à un participant et au SSRC (Synchronisation Source Identifier).
- Contrôler le débit auquel les participants à une session RTP transmettent leurs paquets RTCP. Plus il y a de participants, moins la fréquence d'envoi de paquets RTCP par un participant est grande. Il faut faire en sorte que le trafic RTCP reste en dessous de 5% du trafic de la session. [23]

I.7. Codec

Le mot codec vient de « compression-décompression » (ou « codage-décodage » et désigne un procédé capable de numériser et compresser ou de décompresser un signal, analogique ou numérique. Le codec numérise et compresse la voix de l'émetteur, ainsi les données numériques sont encapsulées dans des paquets IP et acheminées vers le destinataire. A l'arrivée au destinataire, ce dernier, grâce au même codec décompresse et restitue le son. [4]

Le tableau suivant récapitule les principaux codecs utilisés dans la VoIP, le taux de compression ainsi que la consommation en la bande passante:

Codec	Débit du Codec par seconde (Kbps)	Largeur de bande Ethernet Nominale (Kbps)	Utilisation approx. par heure (Mbytes)
G.711	64	87.2	39.24
G.729	8	31.2	14.04
G.723.1	6.4	21.9	9.86
GSM	13.2	28.7 approx	12.92 approx
iLBC	15.2	30.83 approx	13.87 approx
G.723.1	5.3	20.8	9.36
G.726	32	55.2	24.84
G.726	24	47.2	21.24
G.728	16	31.5	14.18

Tableau I.5: Les différents codecs de la voix [4]

I.8.Qos (Quality Of Service)

La qualité de service (QoS) est un problème majeur dans les implémentations de la téléphonie sur IP.

Le problème est de savoir comment garantir que le trafic de paquets pour une connexion vocale ou autre ne sera pas retardé ou interrompu en raison des interférences provenant d'un trafic de moindre priorité.

Les choses à considérer sont :

- **Latence :** qui signifie le délai de livraison des paquets.
- **La gigue de phase :** qui est les variations du délai de livraison des paquets.
- **La Perte de paquets :** c'est à dire trop de trafic sur le réseau entraîne la perte de paquets sur le réseau.

I.9. Futur de la téléphonie sur IP (Everything over IP)

La téléphonie sur IP va pouvoir tirer partie des capacités et fonctionnalités presque illimitées, en termes de services ajoutés à la simple transmission de la voix, que propose les TIC.

Le futur de la téléphonie IP s'oriente clairement vers la mutualisation et la multiplication des services offerts, mais aussi vers la mobilité avec les systèmes 3G/Wi-Fi.

Les solutions IP Centrex commencent à être largement disponibles, au travers de multiples solutions. Il est donc théoriquement possible de faire passer n'importe quel type de flux temps-réel, la limitation se trouvant concrètement dans les fonctionnalités des terminaux et des plates-formes de services.
De plus, les nouveaux smartphones possédant une interface Wi-Fi permettent de mettre en place des solutions de communications « dual mode ». Si un hot-spot Wi-Fi est disponible, alors un client VoIP peut être utilisé. Sinon, le téléphone peut basculer automatiquement sur le réseau GSM [4].

Ce progrès technologique de la téléphonie sur IP, malgré la multiplicité de ses services, peut ouvrir d'autres méthodes de hack, c'est-à-dire augmenter le risques de sécurité de cette technologie par les hackers, et peut être créé de nouveaux types de piratage.

Conclusion

Nous avons vu dans ce chapitre que la téléphonie sur IP est une technologie qui utilise les protocoles de signalisation et de transmission pour réaliser une bonne transmission de voix, et fournir une communication facile.

Cela peut être dangereux, car avec les progrès de cette technologie la voix devient encore vulnérable sur le réseau que les applications classiques.

Les entreprises qui décident d'adopter la téléphonie sur IP doivent le faire prudemment, en mettant le facteur sécurité au premier plan.

Le chapitre suivant décrira les risques et les vulnérabilités les plus récentes et connue dans le monde de la téléphonie sur IP.

CHAPITRE II

Vulnérabilités et mesures de sécurité de la ToIP

Introduction

La téléphonie sur IP se divise en deux phases la première est celle de la signalisation, et la deuxième consiste à transporter la voix, ces dernières partagent les mêmes technologies que les réseaux de données IP. Ce qui fait que la téléphonie sur IP partage les mêmes vulnérabilités que les réseaux de données. À cela il faut rajouter les risques propres aux protocoles de signalisations et de transport de la voix.

L'objectif de ce chapitre sera de savoir comment les technologies ToIP, tout en étant très complexe eux-mêmes, sont toujours ouverts à de nombreuses attaques simples qui peuvent causer beaucoup de dommage.

On va définir les problèmes et vulnérabilités de la téléphonie sur IP, puis l'application de mesures de sécurité nécessaire contre les attaques possibles de la téléphonie sur IP.

II.1. propriétés de sécurité

- **Authentification**

  L'authentification est le processus d'identification de l'utilisateur.

  C'est un mécanisme de liaison de demande entrante avec un ensemble d'identifiants. Les informations d'identification fournies sont comparées aux fichiers d'une base de données contenant des informations utilisateur autorisées sur un système d'exploitation ou un serveur d'authentification local.

  Dans la ToIP c'est de garantir l'identité de l'usager qui fait l'appel ou envoie le message, cette propriété permet par exemple à un serveur de téléphonie de vérifier qu'il fournit le service à l'usager légitime.

- **Intégrité**

  L'intégrité aide à certifier que les données, les traitements ou les services n'ont pas été détruits tant de façon intentionnelle qu'accidentelle, manipulés ou modifiés.

  L'altération est principalement occasionnée par le média de transmission mais peut provenir du système d'informations.

  Il est également nécessaire de s'assurer que les données sont protégées d'une écoute active sur le réseau.

- **Confidentialité**

  La confidentialité indique que seules les personnes autorisées ont accès aux données sensibles. En d'autres termes, protéger les informations contre les accès non autorisés. Cette propriété dans la téléphonie IP est de rendre une conversation compréhensible aux personnes concernées uniquement, pour avoir ça il faut chiffrer le flux audio.

- **Non répudiation de l'appel**

Le non répudiation permet d'associer une communication à une personne de manière certaine. Cette dernière nécessite l'archivage des données échangées.

- **Non rejeu**

Dans la ToIP le non rejeu permet que les protocoles ne puissent pas être ré-échangés et de ne pas pouvoir rejeuer ces échanges protocolaires par un tiers souhaitant accéder au service.

- **L'anonymat de l'appel**

Capacité du système à masquer l'identité de l'utilisateur. La propriété "anonymat" peut entraîner le masquage de l'identité de l'appelant.

II.2.Sécurité de la téléphonie sur IP

Les vulnérabilités de la ToIP sont regroupées en trois points essentiels à savoir les attaques au niveau de système d'exploitation, au niveau de l'infrastructure et celle de protocoles.

II.2.1. Sécurité de système d'exploitation

Une classification indique que le système d'exploitation est le Software de L'infrastructure. Dans une autre classification, il y en a une qui indique que le système d'exploitation le composant qui contient l'infrastructure ToIP.

A. Vulnérabilités du système d'exploitation

Une des principales vulnérabilités du système d'exploitation est le « buffer overflow » qui permet à un attaquant de prendre le contrôle partiel ou complet de la machine.
Elle n'est pas la seule vulnérabilité et elle varie selon le fabricant et la version de l'OS.

Ces attaques visant l'OS sont pour la plupart relative au manque de sécurité de la phase initiale de développement du système d'exploitation et ne sont découvertes qu'après le lancement du produit.

Les dispositifs de la VoIP tels que les téléphones IP, Call Managers, et les serveurs proxy, héritent les mêmes vulnérabilités du système d'exploitation ou du firmware sur lequel ils tournent. On déduira qu'une application de la VoIP est vulnérable dès que le système d'exploitation sur lequel elle tourne est compromis. [7]

B. Sécurisation de système d'exploitation

Il y a plusieurs mesures de sécurités à prendre pour protéger le système d'exploitation :

- Les nouvelles versions contiennent toujours des défauts et des bogues qui doivent être corrigés et nettoyés avant. Il faut également utiliser un système d'exploitation stable.

- Installation de correctifs de sécurité recommandés pour la sécurité en mettant à jour le système d'exploitation.

- Utilisation des mots de passe rebuste. Ils sont fondamentaux contre les intrusions. Et ils ne doivent pas être des noms, des dates de naissance...etc. Un mot de passe doit être assez long pour former une combinaison de lettres et de ponctuations et chiffres.

- Exécution du serveur VoIP sans utilisateur privilège, car si un utilisateur malveillant peut accéder au système via une exploitation de vulnérabilité sur le serveur VoIP, il héritera de tous les privilèges de cet utilisateur.

- L'installation des composants nécessaires uniquement peut limiter les menaces sur le système d'exploitation. Il est préférable d'installer le système d'exploitation et le serveur sur la machine.

- Suppression de tout logiciel, programme ou objet sans importance et pouvant constituer une cible d'attaque pour accéder au système.

- Renforcer la sécurité du système d'exploitation en installant des patches qui permettent de renforcer la sécurité générale du noyau.
  On peut aussi utiliser les pare feu ou/et les ACL pour limiter l'accès à des personnes bien déterminé et fermer les ports inutiles et ne laisser que les ports Utilisés (5060, 5061, 4569...etc). [5]

II.2.2.Sécurité de l'infrastructure

Dans cette section, nous présentons les vulnérabilités de l'infrastructure et les mécanismes de sécurisation de cette dernière.

A. Vulnérabilité du l'infrastructure

Les réseaux de téléphonie sont vulnérables à de nombreuses formes d'attaques réseau courantes et les périphériques prenant en charge l'infrastructure ToIP sont également vulnérables à des problèmes similaires :

- **Téléphone IP**

  Généralement un attaquant obtient les privilèges qui lui permettent de commander complètement la fonctionnalité du dispositif, soit un téléphone IP, un Soft phone, ou d'autres programmes ou matériels client.

  Le pirate pourrait modifier les aspects opérationnels d'un tel dispositif : Il peut changer la pile du système d'exploitation pour masquer la présence de l'attaquant.
  Il peut modifier et configurer d'une manière malveillante des logiciels de téléphonie IP qui peuvent permettre :
  - Aux appels entrants d'être réorientés vers un autre point final sans que l'utilisateur soit au courant ou aux appels d'être surveillés.
  - A l'information de la signalisation et/ou les paquets contenant de la voix d'être routés vers un autre dispositif et également d'être enregistrés et/ou modifiés.

  Les soft phones sont plus susceptibles aux attaques, ils sont plus susceptibles aux vulnérabilités du system d'exploitation et vulnérabilité de l'application, et vulnérabilité du services, des virus.etc... [7]

- **Serveur VoIP**

Un pirate peut viser les serveurs qui fournissent le réseau de téléphonie sur IP. Compromettre une telle entité mettra généralement en péril tout le réseau de téléphonie dont le serveur fait partie.

Par exemple, si un serveur de signalisation est compromis, un attaquant peut contrôler totalement l'information de signalisation pour différents appels. Ces informations sont routées à travers le serveur compromis.Avoir le contrôle de l'information de signalisation permet à un attaquant de changer n'importe quel paramètre relatif à l'appel.

Si un serveur de téléphonie IP est installé sur un système d'exploitation, il peut être une cible pour les virus, les vers, ou n'importe quel code malveillant. [5]

B. Sécurisation de l'infrastructure

La sécurisation d'une architecture VoIP passe par trois étapes : l'exploration des dangers, le choix du niveau de protectorat, et la mise en place des solutions de sécurisation. Le tout accompagné des bonnes pratiques de l'utilisation de ses outils.
Dans cette section, nous rappellerons les mécanismes principaux de la sécurité appliquée au niveau de l'architecture.

- **Séparation au niveau IP (layer 3)**

Cette solution consiste à attribuer une plage d'adresses IP au réseau DATA. Et une autre plage d'adresses IP aux équipements VoIP.

Une fois cette séparation effectuée, il est possible de définir des ACL sur les équipements de couche 3 (switches L3/routeurs/firewalls) afin de n'autoriser les communications qu'entre les adresses IP autorisées.

- **Séparation grâce aux VLAN (layer 2)**

  La deuxième solution consiste à définir un VLAN VoIP dédié aux équipements VoIP et un VLAN DATA dédié aux équipements réseaux présents dans le réseau DATA

- **Filtrage des adresses MAC**

Pour éviter que n'importe qui se connecte sur les ports d'un switch, il est possible de faire un contrôle sur les adresses MAC des machines connectées sur chaque port. Une simple commande permet d'activer cette sécurité sur l'interface concernée.La définition des adresses MAC autorisées sur un port donné peut se faire de deux façons.

- Par adresse MAC fixée en spécifiant explicitement l'adresse MAC à qui l'on souhaite donner l'accès dans la commande au Switch.

- Par apprentissage de l'adresse MAC source de la première trame qui traversera le port via l'option « sticky mac ». [28]

Utilisation d'une carte réseau supportant le 802.1Q

Cette solution consiste à équiper les ordinateurs d'une carte Ethernet prenant en charge le protocole 802.1q et à les configurer pour utiliser ce protocole. Ces cartes Ethernet peuvent séparer le trafic DATA du trafic VoIP, en plaçant chaque type de trafic dans leur VLAN respectif. [9]

II.2.3.Sécurité des protocoles ToIP

Un appel téléphonique VoIP est constitué de deux parties : la signalisation, qui instaure l'appel, et les flux de media, qui transporte la voix.

La signalisation, en particulier SIP, transmet les entêtes et la charge utile (Payload) du paquet en texte clair, ce qui permet à un attaquant de lire et falsifier facilement les paquets. Elle est donc vulnérable aux attaques qui essaient de voler ou perturber le service téléphonique

Le protocole RTP, utilisé pour le transport des flux multimédia, présente également plusieurs vulnérabilités dues à l'absence d'authentification et de chiffrage.

Les protocoles de la VoIP utilisent TCP et UDP comme moyen de transport et par conséquent sont aussi vulnérables à toutes les attaques contre ces protocoles, telles le détournement de trafic (Hijacking) et la mystification (UDP) (Spoofing) ...etc. [6]

Les types d'attaques les plus fréquentes contre les protocoles VoIP seront détaillées dans les sections suivantes.

II.2.3.1.Sécurité des protocoles de signalisation

Dans la phase de signalisation on présente les attaques SIP et le contre mesure de chaque attaque.

A. DoS (*Denial of service*)

Il s'agit ici de la privation d'accès à un service réseau en inondant les serveurs, avec des paquets malveillants. Dans le cas de SIP, une attaque DoS peut être directement dirigée contre les utilisateurs finaux ou les autres dispositifs, l'attaque DoS peut prendre différentes formes :

DoS par BYE

L'attaque par la méthode du BYE est dirigée contre les usagers. L'attaquant génère un BYE et interrompt une conversation. Pour réaliser cette attaque, le pirate écoute le trafic et prend les informations nécessaires (comme par exemple le Call-Id, le From ou encore le To) pour générer un BYE frauduleux correspondant à la session qui est injecté sur le réseau. Le BYE n'étant pas authentifié, celui qui reçoit l'information l'exécute. [29]

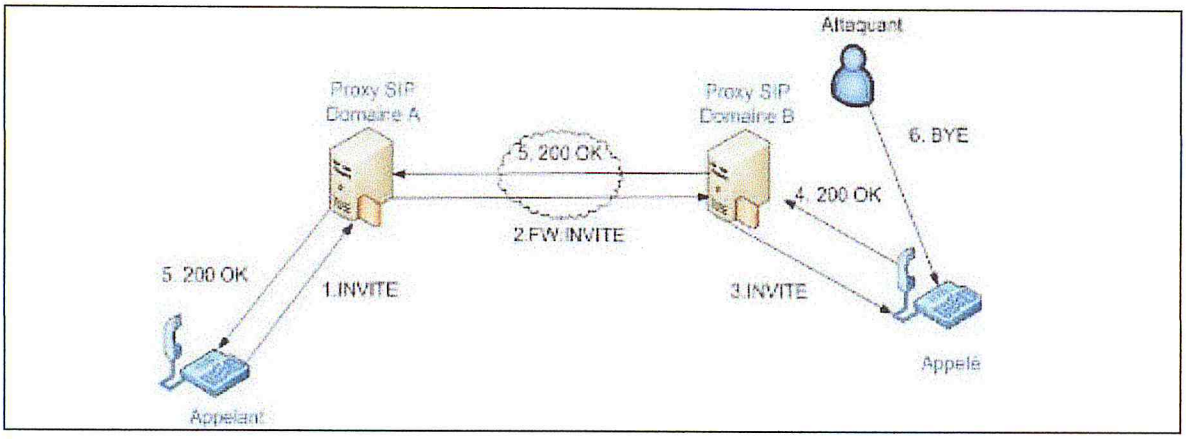


Figure II.1 Attaque DoS via une requête BYE. [29]

DoS par CANCEL

Dos par Cancel est un type de déni de service lancé contre l'utilisateur. L'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive pour un utilisateur spécifique. Une fois que le dispositif de l'utilisateur reçoit la requête INVITE, l'attaquant, envoie immédiatement une requête CANCEL. Cette requête produit une erreur sur le dispositif de l'appelé et termine l'appel. Ce type d'attaque est employé pour interrompre la communication. [29]

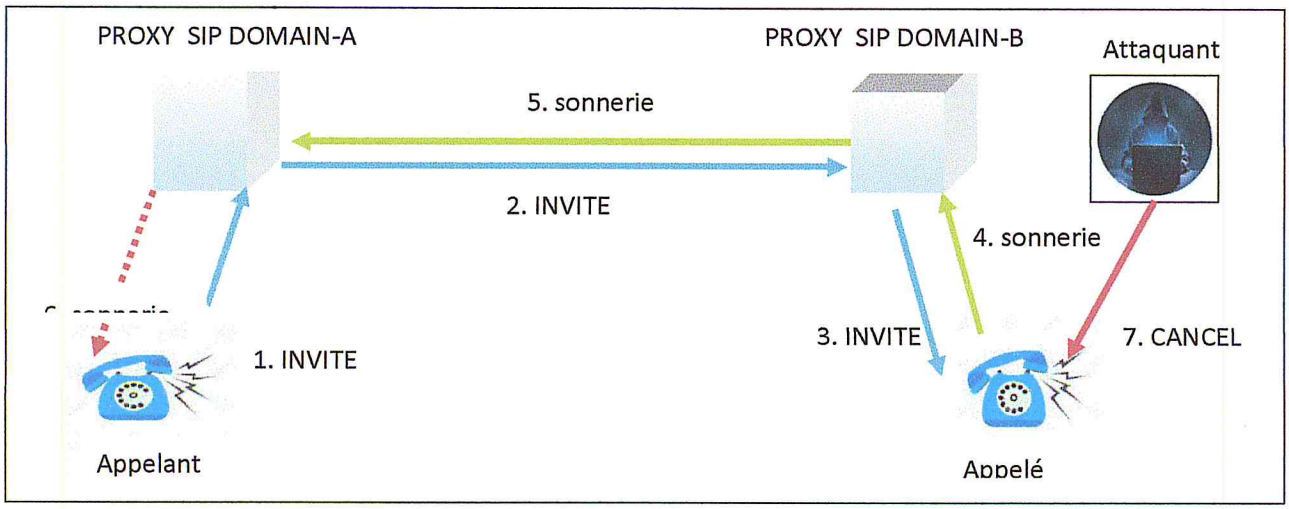


Figure II. 2 Attaque DoS via une requête CANCEL.

DoS en utilisant les messages INVITE ou REGISTER en masse

- Bulk REGISTER :

Cette attaque provoque un débordement de la table des enregistrements afin d'empêcher les utilisateurs légitimes de s'enregistrer sur le serveur Registrar, pour cela l'attaquant envoie un grand nombre de messages de requête REGISTER (avec des URIs différentes) au serveur des enregistrements.

- Bulk INVITE :

Le but ici est d'épuiser les ressources de sessions simultanées sur le proxy. Le nombre de connexions simultanées maximum dépend du serveur et du réseau. Il nous suffit donc d'initier plus de connexions pour que le proxy soit devenu non fonctionnel.

➢ Solution de sécurité contre l'attaque DoS

Pour atténuer les attaques DoS , l'authentification est la clé. Les composants VoIP doivent faire sûr qu'ils communiquent avec légitime homologues.

Le pare-feu VoIP devrait également être implémenté pour surveiller les flux et filtrer les signaux anormaux.

B. Détournement (Hijacking)

Le but ici est de détourner l'appel vers le pirate ou d'enregistrer les communications. Cela permet également de se joindre à un appel (conférence audio).

Ce type d'attaque peut se faire de plusieurs manières :

Attaque MITM (*Man In The Middle*) en utilisant les messages 3xx

Cette attaque redirige le trafic de signalisation vers un parti qui n'est pas l'appelé.

Quand un agent SIP envoie un message INVITE pour initier un appel, l'attaquant envoie un message de redirection 3xx indiquant que l'appelé s'est déplacé (par exemple la réponse 301 indique que L'utilisateur ne peut plus être joint à l'adresse indiquée (URI) et le demandeur devrait essayer à nouveau à l'adresse fournie dans le champ Contact de l'en- tête), en même temps il donne sa propre adresse de renvoie.

A partir de ce moment, tous les appels destinés à l'utilisateur sont transférés et c'est l'attaquant qui les reçoit.

La figure II.3 Illustre comment se passe cette attaque

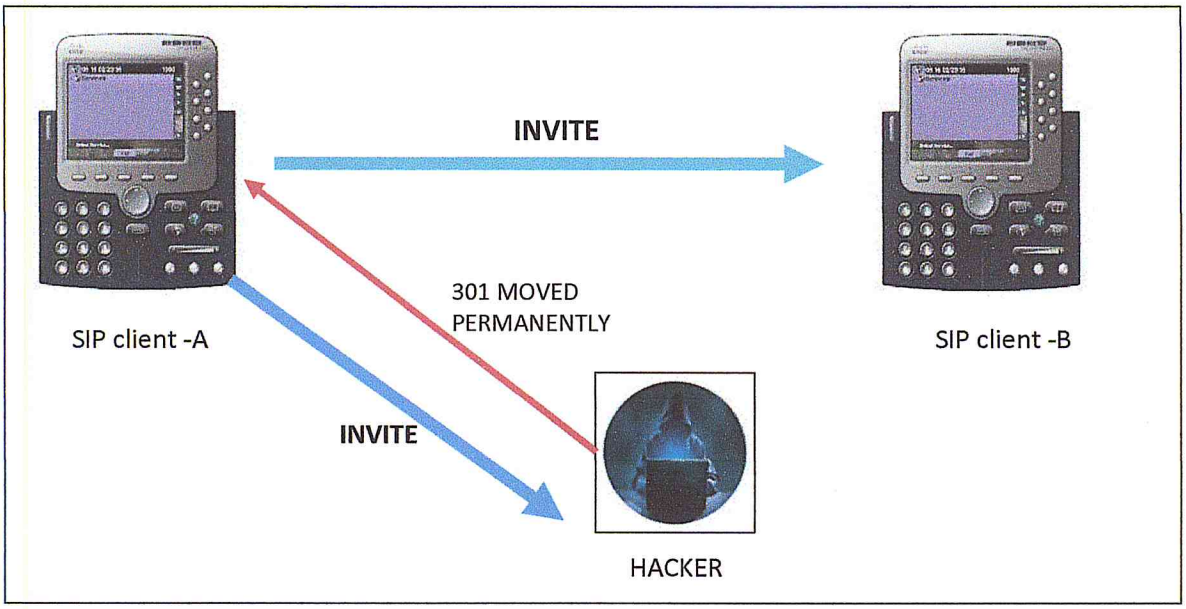


Figure II.3 Attaque MITM en utilisant le message 301

- **Attaque MITM en utilisant la requête REGISTER**

Cette attaque redirige les appels vers l'attaquant en sabotant le serveur Register. L'attaquant doit tout d'abord écouter le réseau afin de récupérer un message du type REGISTER. Ensuite, après avoir analysé ce message, il peut façonner un message REGISTER et se réenregistrer auprès du serveur Register avec une nouvelle URI pour la victime. Ceci ayant comme résultat de rediriger tous les appels entrants qui seront envoyés

Vers la nouvelle URI (celle de l'attaquant) permettant ainsi à l'attaquant de plagier la cible de l'attaque et ainsi mener à bien son plan.

➢ Solution de sécurité contre le MITM

Le cryptage des paquets de messages vocaux peut protéger contre les attaques MITM. IPSec peut être déployé pour chiffrer des paquets entiers.

- **SIP protégé par IPSec (IP Security Protocol)**

IPSec est un protocole pouvant être utilisé pour protéger les messages SIP au niveau IP. Avec SIP, chaque proxy sur le chemin doit avoir accès en lecture/écriture sur l'entête des messages SIP afin de pouvoir ajouter/retirer des entêtes VIA.

Pour permettre l'utilisation d'IPSec ESP (Encapsulating Security Payload) qui assure l'authentification, l'intégrité et la confidentialité grâce au chiffrement du paquet, ou AH (Authentification Header) pour garantit l'authentification de l'origine des données et le contrôle d'intégrité de l'ensemble du paquet (données et en-têtes IP), son fonctionnement doit être basé sur un mode Hop-By-Hop. AH et ESP peuvent fonctionner avec plusieurs algorithmes cryptographiques, toutefois l'IETF préconise l'utilisation de triple DES (128 bits) pour le chiffrement et HMAC-MD5 ou HMAC-SHA1 pour l'authenticité. [5]

C. Attaques SPAM

Les formes principales de spams jusqu'à maintenant identifiés dans SIP sont :

Call Spam

Ce type de spam est défini comme une masse de tentatives d'initialisation de session non sollicitées. Généralement c'est un UAC (*User Agent Client*) qui lance, en parallèle, un grand nombre d'appels. Si un appel est établi, l'application spammeuse génère un ACK, joue une annonce préenregistrée, et ensuite clôt l'appel. [6]

IM (*Instant Message*) Spam

Ce type de spam est semblable à celui de l'e-mail. Il est défini comme une masse de messages instantanés non sollicitées. Les IM spams sont pour la plupart envoyés sous forme de requête SIP. Ce pourraient être des requêtes INVITE avec un entête très grand, ou des requêtes INVITE avec un corps en format texte ou HTML. [9]

Présence Spam

Ce type de spam est semblable à l'IM spam. Il est défini comme une masse de requêtes de présence (des requêtes SUBSCRIBE) non sollicitées. L'attaquant fait ceci dans le but d'appartenir à la " white list " d'un utilisateur afin de lui envoyer des messages instantanés ou d'initier avec lui d'autres formes de communications. L'IM Spam est différent du Presence Spam dans le fait que ce dernier ne transmet pas réellement de contenu dans les messages. [6]

SPIT (Spam over Internet Telephony)

Tout comme un spam classique par courrier électronique, le SPIT peut être généré de manière similaire à partir de serveurs visant des millions d'utilisateurs de la ToIP.

Le SPIT peut ralentir notablement le fonctionnement des architectures de téléphonie sur IP (exemple en engorgeant les boîtes vocales des usagers) [2]

➢ Solution de sécurité contre les attaques SPAM

Protocole SIPS (SIP/TLS)

SIPS est basé sur TLS (Transport Layer Security). L'intégrité des données est garantie grâce aux MACs (Message Authentification Code) basé sur les fonctions de hachage MD5, ou SHA-1. Il fournit, en plus du chiffrement, selon la configuration :

- L'authentification simple (serveur authentifié auprès de l'IP Phone).
- L'authentification mutuelle entre les serveurs et les IP Phones.

L'authentification des entités est basée sur le protocole X.509, et elle a lieu durant la phase de négociation de TLS. C'est aussi durant cette phase que sont négociés les algorithmes utilisés ainsi que la génération de la clé symétrique de session pour le chiffrement des données. Le diagramme en flèche présenté dans la figure II.4 présente les principaux échanges lors d'une négociation TLS.

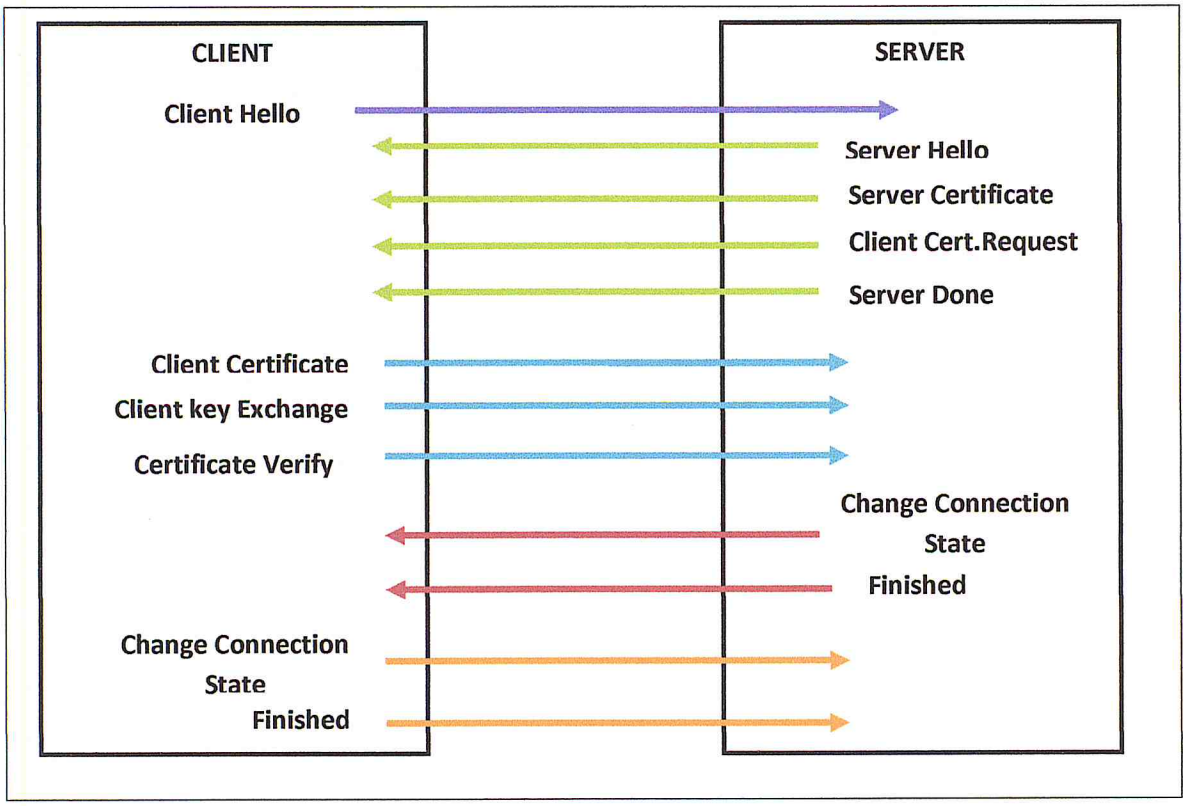


Figure II.4 : Echanges de messages TLS

D. Usurpation d'identité (*Call ID Spoofing)*

L'usurpation d'identité de l'appelant est la technologie qui vous permet de modifier les informations transmises à votre identifiant d'appelant afin de masquer le véritable identifiant d'origine de l'appel téléphonique.

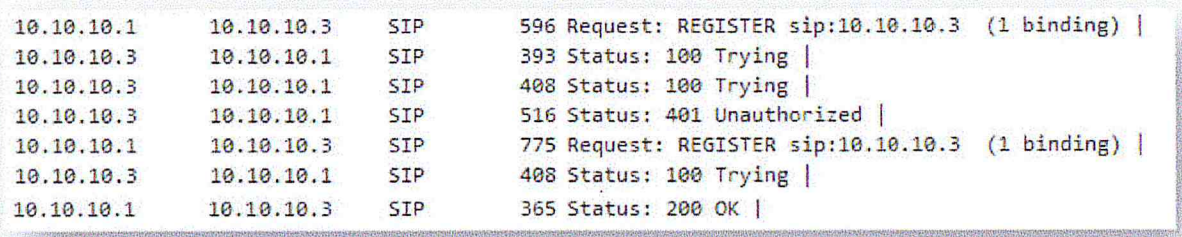
Dans la VoIP peut être effectuée en manipulant les messages du protocole de signalisation utilisé (par exemple, SIP INVITE).

➢ Solution de sécurité contre l'usurpation d'identité

L'authentification est un processus et une propriété de sécurité efficace permettant au système de s'assurer de la légitimité de la demande d'accès faite par une entité.

Authentification HTTP Digest des messages SIP

L'authentification par HTTP Digest permet au serveur d'authentifier les messages SIP REGISTER et INVITE envoyés par un IP Phone. Les attaques basées sur l'usurpation d'identité du client ne sont alors plus possibles. Le principe de l'authentification HTTP Digest est classique. Le serveur envoie un défi au client « nonce », ce dernier répond par une valeur (response) dérivée de ce challenge et d'un secret qu'il partage avec le serveur. Le serveur s'assure alors que le client possède certainement le secret en calculant à son tour la réponse et en vérifiant l'adhérence des deux. La figure II.5 montre un exemple d'authentification HTTP Digest.



10.10.10.1	10.10.10.3	SIP	596 Request: REGISTER sip:10.10.10.3 (1 binding) |
10.10.10.3	10.10.10.1	SIP	393 Status: 100 Trying |
10.10.10.3	10.10.10.1	SIP	408 Status: 100 Trying |
10.10.10.3	10.10.10.1	SIP	516 Status: 401 Unauthorized |
10.10.10.1	10.10.10.3	SIP	775 Request: REGISTER sip:10.10.10.3 (1 binding) |
10.10.10.3	10.10.10.1	SIP	408 Status: 100 Trying |
10.10.10.1	10.10.10.3	SIP	365 Status: 200 OK |

Figure II.5 : Authentification HTTP Digest SIP pour un message REGISTER

II.2.3.2. Sécurité des protocoles de transport

Dans la phase de transport on concentre sur les attaques RTP et on cite pour chaque attaque son solution possible de sécurité.

A. Ecoute passive (*passive eavesdropping*)

Les paquets de texte en clair de RTP peuvent être détectés sur le réseau comme avec telnet, FTP et HTTP. Cependant, contrairement à une telle attaque sur telnet, il suffit de capturer quelques paquets RTP sur le réseau ne fourniront pas à un attaquant tous les informations sensibles qu'il ou elle veut. C'est parce que RTP transfère des flux des paquets audio, ce qui signifie qu'un attaquant doit capturer un flux entier afin de capturer une conversation. Des outils tels que Cain & Abel et Wireshark permettent de capturer des flux RTP sur le réseau presque facile. Ces outils capturent une séquence de paquets RTP, les réassembler dans le bon ordre et sauvegarder le flux RTP en audio fichier (par exemple .wav) en utilisant le codec audio correct. Cela permet à tout attaquant passif pour simplement pointer, cliquer et écouter toutes les communications VoIP dans son propre sous-réseau.

B. Écoute Active (*Active eavesdropping*)

Outre les attaques d'écoute passive, RTP est également vulnérable aux attaques actives.Par exemple, un attaquant pourrait injecter un fichier audio indiquant «Vendre à 1004» entre deux courtiers en valeurs mobilières discutant d'informations sur les opérations d'initiés.

➢ Solution de sécurité contre l'écoute

- **Secure RTP (SRTP)**

Le protocole SRTP est utilisé pour chiffrer le flux RTP entre les utilisateurs. Au début de cette phase le protocole **ZRTP** est normalement utilisé pour réaliser les échanges des clés de session, en utilisant l'algorithme **Diffie-Hellman** .L'attaquant **(*man in the middle*)** peut intentionnellement provoquer la perte des paquets RTP utilisés pendant cette phase, occasionnant le non chiffrement du flux. Les utilisateurs ne s'en aperçoivent pas, car l'appel est toujours réalisé, mais leur communication n'est plus chiffrée. [10]

C. DoS

Les attaquants peuvent inonder la passerelle, le téléphone IP et les autres composants VoIP de traitement des médias avec un grand nombre de paquets RTP. Si la cible est obligée de supprimer des paquets RTP, la qualité de la voix se dégradera. En outre, l'attaquant pourrait faire tomber des composants clés tels que la passerelle hors ligne. Une panne dans l'un de ces appareils pourrait interrompre tout le réseau vocal.

DoS par injection des paquets RTP

Cette attaque perturbe une communication en cours. L'attaquant devra tout d'abord écouter un flux RTP de l'appelant vers l'appelé, analyser son contenu et générer un paquet RTP contenant un en-tête similaire mais avec un plus grand numéro de séquence et timestamp afin que ce paquet soit reproduit avant les autres paquets (s'ils sont vraiment reproduits). Ainsi la communication sera perturbée et l'appel ne pourra pas se dérouler correctement.

Pour réaliser cette attaque, l'attaquant doit être capable d'écouter le réseau afin de repérer une communication et ainsi repérer les timestamps des paquets RTP. Il doit aussi être capable d'insérer des messages RTP qu'il a généré ayant un timestamp modifié. [3]

Solution de sécurité contre l'injection RTP

Un pare-feu VoIP devrait être implémenté pour surveiller les flux et filtrer les paquets RTP. Les limites de débit des médias peuvent être définies par observer les modèles de trafic normaux.

Conclusion

La sécurité de la téléphonie doit pouvoir répondre à trois grandes exigences : la disponibilité, l'intégrité et la confidentialité. D'autres propriétés comme l'authentification, le non-rejeu et la non-répudiation peuvent être également nécessaires.

L'étude de vulnérabilités de la ToIP peut estimer les risques probables de l'utilisation de la ToIP, d'autre part nous avons vu dans ce chapitre les contres mesures qui sert à protéger l'utilisateur et entreprise qui utilise cette technologie.

Donc ce chapitre montre les attaques possibles que se soit les risques associés à l'infrastructure et protocoles de la ToIP, et nous avons parlé aussi sur les techniques pour atteindre un haut niveau de sécurité et mettre en œuvre une architecture sécurisée de téléphonie sur IP.

CHAPITRE III

Présentation de l'organisme d'accueil

Introduction

Dans ce chapitre, nous allons présenter l'entreprise d'accueil NAFTAL. Elle a pour mission principale, la distribution et la commercialisation des produits pétroliers et dérivés sur le marché national.

III.1. Historique du NAFTAL

Issue de SONATRACH, (société nationale pour la recherche, transport, production, transformation, la commercialisation des hydrocarbures), l'entreprise nationale de raffinage et de distribution de produits pétroliers (ERDP) a été crée par le décret N 80-101 du 06 avril 1980.

Entrée en activité le 01 janvier1982, elle est chargée de l'industrie de raffinage et de la distribution de produits pétroliers. Le 04 mars 1985, les anciens districts (Carburants, lubrifiants, pneumatique et bitume) ont été regroupés sous le nom UND (unité NAFTAL de distribution).

En 1987, l'activité raffinage est séparée de la distribution, conformément au Décret n 87-189 du 25 Aout 1987 modifiant le décret n 80-101 du 6 Avril 1980, modifié, portant création de l'Entreprise nationale de raffinage et de distribution de produits pétroliers, il est crée une Entreprise nationale dénommée : Entreprise nationale de commercialisation et de distribution de produits pétroliers, sous le sigle de NAFTAL.

A partir de 1998, elle change de statut et devient société par action filiale à 100% de SONATRACH, en intervenant dans les domaines suivants : l'enfutage GPL, la formulation des bitumes, la distribution, le stockage et commercialisation. [8]

NAFTAL a pour mission principal, la distribution et la commercialisation pétrolière sur le marché national.

L'appellation de l'entreprise NAFTAL provient de :

NAFT : terme arabe désignant le pétrole.

Al : en référence à AL-DJAZAIR.

III.2. Mission Et Objectifs De L'entreprise NAFTAL

Dans le cadre du plan national de développement économique et sociale de la commercialisation et de la distribution des produits pétroliers y compris ceux destinés à l'aviation à la marine, le GPL, les combustibles, les solvants, les aromatiques, paraffines, Bitumes et pneumatiques. [15]

Ses Mission Essentielles Sont :

- Organiser et développer l'activité de Commercialisation et de la distribution des produits pétroliers et dérivés.
- Stocker, transporter et /ou faire transporter tout produit pétrolier commercialisé sur le territoire national.
- Veiller à l'application et au respect des mesures relatives à la sécurité industrielle, la sauvegarde et la protection de l'environnement, en relation avec les organismes concernée.
- Procéder à toutes études de marché en matière d'utilisation et de consommation des produits pétroliers.
- Définir et développer une politique en matière d'audit, concevoir et mettre en œuvre des systèmes intégrés d'information.
- Développer et mettre en œuvre les actions visant à une utilisation optimale et relationnelle des infrastructures et moyens.
- Veiller à l'application et au respect des mesures liées à la sûreté interne de la société conformément à la réglementation.
- Développer une image de marque et qualité.

III.3. Présentation de l'architecture de téléphonie IP au sein de NAFTAL

Dans le cadre de la modernisation des infrastructures réseau et télécom de l'entreprise, la Direction Centrale des systèmes d'information DCSI à projeter d'intégrer tous les services de communication de l'entreprise sur un réseau unifié.

En 2015 la DCSI à déployé la première solution de téléphonie IP CISCO au profit de la Banche carburant, par la suite des projets de généralisation de la solution en suivie pour intégrer tous les sites de NAFTAL.

La DCSI et les services techniques télécom de NAFTAL travaille conjointement pour migrer la téléphonie classique vers la téléphonie IP, à cet effet une stratégie de migration et mis en place pour permettre une migration en douceur et assuré la disponibilité du service téléphonie.

La stratégie repose sur le passage de la téléphonie classique vers la voix sur IP (VOIP) puis de la voix sur IP vers téléphonie IP ou (Telephony Over IP en anglais).

Cette démarche implique de relier en premier lieu les équipements de la téléphonie classique (PABX) avec les équipements du réseau WAN (routeurs) et assuré un routage des appels classique et IP, par la suite tous les utilisateurs seront équipés d'un téléphone IP, et la téléphonie classique serra isolé du réseau WAN au fur à mesures.

La solution de la téléphonie IP de NAFTAL est full Cisco, elle déployé en mode « Cluster Over the WAN » comme suit : [18]

- Un serveur Call Manager
- Un serveur Publisher est installé au niveau de la Direction générale.
- Deux serveurs Subscriber installés au niveau des branches GPL et CBR, pour assurer la redondance en cas de coupure de liaison avec le site central.
- Un serveur Call Manager Express est installé au niveau de chaque site distant (District, Station de service, dépôt de stockage)

En cas de non disponibilité d'un système, l'autre système prendra en charge d'une manière automatique et totalement transparente les abonnés de son homologue.

- Les utilisateurs des districts de NAFTAL seront abonnés au système installé au niveau de la DG.
- Les utilisateurs du siège de la Branche seront abonnés au système installé au niveau de la branche.

Pour les districts la solution doit comporter des mécanismes de secours qui garantissent le maintien des services de téléphonie standard et classique dont les utilisateurs ont besoin en cas de dysfonctionnement des liaisons WAN (interruption de la signalisation avec le serveur d'appels auquel les postes IP sont rattachés).

III.4. Les composants de l'architecture

L'architecture globale de l'entreprise NAFTAL est composé de :

III.4.1. Serveurs de communication

Cisco Unified Communications est un système de communication basé sur IP intégrant des produits et des applications voix, vidéo, données et mobilité [12].

Le serveur ***Cisco Unified Communications*** fournit une plate-forme de serveur à haute disponibilité pour le traitement des appels, des services et des applications ***Cisco Unified Communications Manager.***

Le système CUCM étend les fonctionnalités et les fonctions de téléphonie d'entreprise aux périphériques réseau de téléphonie par paquets tels que les téléphones IP, les dispositifs de traitement multimédia, les passerelles VoIP (voix sur IP) et les applications multimédias.

CUCM fournit des services de signalisation et de contrôle des appels aux applications de téléphonie intégrée de Cisco, ainsi qu'aux applications tierces.

Il effectue les fonctions primaires suivantes :

- traitement des appels
- la signalisation et le contrôle des appareils

• Administration des fonctionnalités du téléphone

• services d'annuaire.

Concernant la sécurité de CUCM plusieurs faiblesses ont été identifiées. Ces vulnérabilités peuvent être exploitées par un utilisateur malveillant pour provoquer un déni de service ou une exécution de code arbitraire distance.

- **Injection SQL**

Une vulnérabilité dans l'interface de base de données SQL de Cisco Unified Communications Manager pourrait permettre à un attaquant distant authentifié d'avoir un impact sur la confidentialité du système en exécutant des requêtes SQL arbitraires. Un attaquant pourrait exploiter cette vulnérabilité en envoyant des URLs contenant des instructions SQL malveillantes au système affecté. Cisco n'a pas publié de mises à jour logicielles qui corrigent cette vulnérabilité [11]

La version 10.5 (2.13900.9) de ***Cisco Unified Communications Manager*** est un produit vulnérable à l'attaque injection sql.

- **DOS du sous-système de gestion des identités utilisée par les applications Web du CUCM**

Une vulnérabilité de déni de service du sous-système de gestion des identités utilisée par les applications Web Applications du logiciel ***Cisco Unified Communications Manager*** pourrait permettre à un attaquant distant non authentifié de provoquer un déni de service (DoS).

La vulnérabilité est due à des demandes de session non valides. Un attaquant pourrait exploiter cette vulnérabilité en envoyant des jetons de session non valides au sous-système d'un système affecté. Un exploit réussi pourrait permettre à l'attaquant de provoquer une condition DoS pour une application spécifique [11].

La version 10.5 (0.98000.88) de ***Cisco Unified Communications Manager*** est vulnérable à cette attaque.

III.4.2. L'outil de Collaboration

Jabber est un protocole de messagerie instantanée inventé en 1998 par Jeremi Miller et fondé sur XML.

Ultérieurement, une distinction s'est faite entre le protocole à proprement parler(XMPP) et le nom d'origine (Jabber) devenu une marque. On distingue ainsi :

- **Jabber**, appellation d'origine du réseau de messagerie instantanée construit sur le protocole Extensible Messaging and Presence Protocol (XMPP), lui-même désigné autrefois sous l'appellation "Jabber".

- **Jabber**, le nom commercial de l'entreprise Jabber Inc, fondée en 2000 et rachetée en 2008 par *Cisco systems.*[17]

Cisco Jabber offre des informations de présence, la messagerie instantanée, la communication vocale et vidéo, la conférence Web et le partage de bureau sur des appareils mobiles et fixes.

Cisco Djabber est disponible pour PC et Mac, ainsi que pour tablettes et *smartphones*. En un clic, l'utilisateur de ***Cisco Djabber*** peut immédiatement voir le bon interlocuteur et savoir quel périphérique est disponible.

Ce logiciel est proposé en tant que client *Unified*. Ce client permet à la fois d'utiliser des services en Cloud ainsi que des applications développées en interne. L'utilisateur peut travailler partout, au bureau ou en voyage à partir d'une fonction de messagerie instantanée, démarrer un appel vocal ou vidéo tout en traitant des documents. ***Cisco Jabber*** fonctionne sur Mac et Windows, *iPhone*, iPad, *Blackberry*,*Nokia* et *Android*. *Jabber* est compatible avec toutes les solutions vidéo Cisco. [13]

Jabber ne présente pas les problèmes des anciennes plateformes et améliore les communications de l'entreprise tout en accélérant les processus décisionnels. [13]

Cisco Djabber est vulnérable au Déni de service à distance, ces systèmes infectés sont :

- Versions antérieures à Cisco Unified Presence 8.6(3).
- Versions antérieures à Jabber XCP 5.3.

Une vulnérabilité a été corrigée dans Cisco Unified Presence et Jabber Extensible Communication Platform. Elle concerne un déni de service à distance pouvant être provoqué par un entête XMPP spécialement conçu. [14].

III.4.3. Cisco Unity Connection

Cisco Unity Connection est une plate-forme de messagerie vocale riche en fonctionnalités qui s'exécute sur le même système d'exploitation ***Cisco Unified Communications*** basé sur Linux.

Cisco Unity Connection est une solution de messagerie unifiée et de messagerie vocale qui offre aux utilisateurs des options d'accès aux messages flexibles et une solution informatique facile à gérer.

Cette solution permet aux utilisateurs d'accéder et de gérer les messages depuis une boîte de réception, un navigateur Web, **Cisco *Jabber***, un téléphone IP *Cisco Unified*,un *smartphone* ou une tablette.

Unity Connection fournit également des options flexibles d'accès aux messages et de format de livraison, y compris la prise en charge des commandes vocales, de la transcription voix-texte et même des messages d'accueil vidéo. [16]

Cisco Unity Connection est flexible, très sécurisé, évolutif et conforme ,ce dernier est la solution de messagerie unifiée systématiquement sélectionnée par les entreprises de taille moyenne et mondiales, les agences gouvernementales et les entreprises soucieuses de la sécurité depuis l'année 2005.

III.4.4. Cisco Unity Express

Cisco Call Manager Express (CME) est une solution de traitement des appels intégrée aux routeurs d'accès Cisco sous la forme d'un ensemble de fonctionnalités du logiciel Cisco IOS (C'est un plus petit produit que le Call Manager qui nécessite un ou plusieurs serveurs à l'encontre du CME qui ne nécessite qu'un routeur).

Cette solution offre des services locaux de traitement des appels, de messagerie vocale et d'accueil automatique via une unique plate-forme de routage intégrée. [18]

La solution CME à beaucoup d'avantage pour les entreprises parmi les :

- L'orientation rapide des Clients de l'entreprise vers le bon interlocuteur.
- La téléphonie et les données sont traitées sur la même plateforme.
- La centralisation de configuration et l'administration sur un équipement unique.
- la maintenance L'administration et peuvent se faire à distance.
- La possibilité de L'évolution vers une architecture de téléphonie centralisée sans aucune remise en cause des investissements.

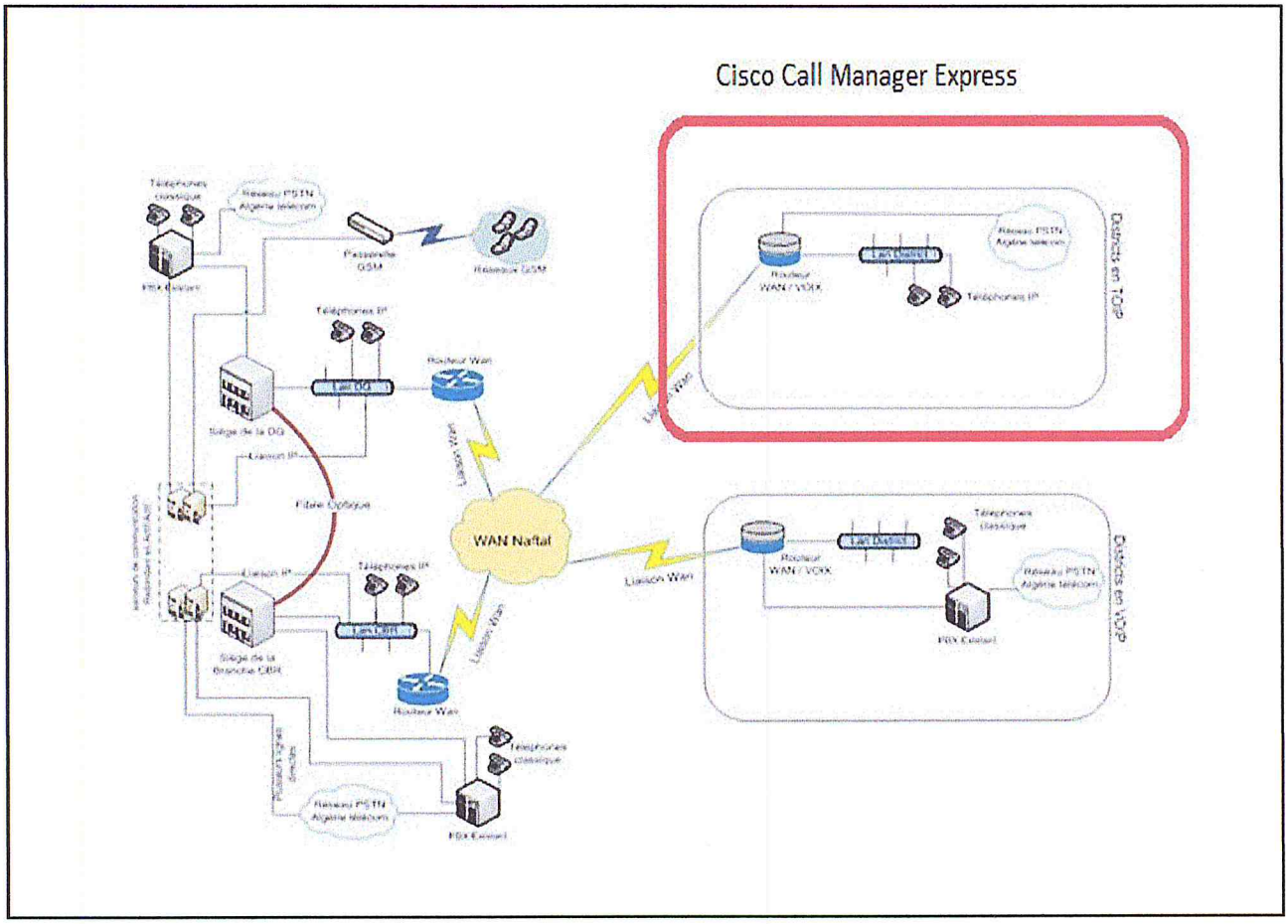


Figure III.2: Cisco Call Manager Express. [18]

Conclusion

Nous avons vu tout au long de ce chapitre les composants de l'architecture de ToIP de l'entreprise NAFTAL.

D'une autre part L''etude de l'existant nous a permis de connaitre Les problèmes de sécurité rencontré par l'entreprise NAFTAL concernant l'utilisation de cette technologie(Téléphonie sur IP), ce qui nous a permis de cerner la problématique de notre projet et de proposer des solutions.

CHAPITRE IV

Mise en œuvre d'une architecture ToIP sécurisée

Introduction

Après avoir étudié la théorie de la téléphonie sur IP et ses vulnérabilités. Nous passons maintenant à la partie pratique qui montre en détail la mise en œuvre de notre solution de sécurité.

Dans ce chapitre nous présenterons la simulation de notre architecture de téléphonie sur IP et nous parlerons des technologies que nous utiliserons pour la réalisation de notre architecture. Nous consacrons la première partie à la présentation des différents choix techniques, tandis que dans la deuxième, nous exposerons la réalisation de notre travail avec quelques interfaces.

IV.1.Outils de réalisation du projet

Nom de logiciel	Description
GNS3	GNS3 est un simulateur d'équipements Cisco. Cet outil permet donc de charger de véritable IOS Cisco et de les utiliser en simulation complète sur un simple ordinateur. [30]
VMWare Workstation11	VMware Workstation permet aux utilisateurs de configurer des machines virtuelles (VM) sur une seule machine physique, et les utiliser simultanément avec la machine réelle. Chaque machine virtuelle peut exécuter son propre système d'exploitation, y compris les versions de Microsoft Windows, Linux, BSDt MS-DOS.[31]
Cisco IP Communicator /softphone	Cisco IP Communicator est une application bureautique qui fournit à un ordinateur toutes les fonctions d'un téléphone IP Cisco permettant de passer, recevoir et traiter des appels. [3]
CUCM (*Cisco Unified Communications Manager* Version 10.5)	Serveur de téléphonie propriétaire Cisco, le « Cisco Unified Communications Manager v10.5» qui s'exécute sur une machine RedHat Entreprise Linux 3. [3]
Kali Linux OS	Kali Linux est une distribution GNU/Linux spécialisée dans l'audit et le pentest, basée sur la distribution GNU/Linux Debian.
MetaSpoit FrameWork	.
NMAP	Nmap est un scanneur des ports libre.
Ettercap	Ettercap est un logiciel libre d'analyse du réseau informatique, créé à l'origine par les programmeurs italiens de la Hacking Team.[]
Wireshark	Wireshark est un analyseur de paquets libre et gratuit.

Tableau IV.1 : Outils réalisation du projet

Nous avons commencé comme première étape par mettre en place le réseau de test SIP/ToIP dans l'état non sécurisé. Pour débuter, nous devons installer le serveur SIP/ToIP, nous choisissons le serveur de téléphonie propriétaire Cisco, le « Cisco Unified Communications Manager v10.5.La figure IV.1 montre l'interface Web du CUCM 10.5 :

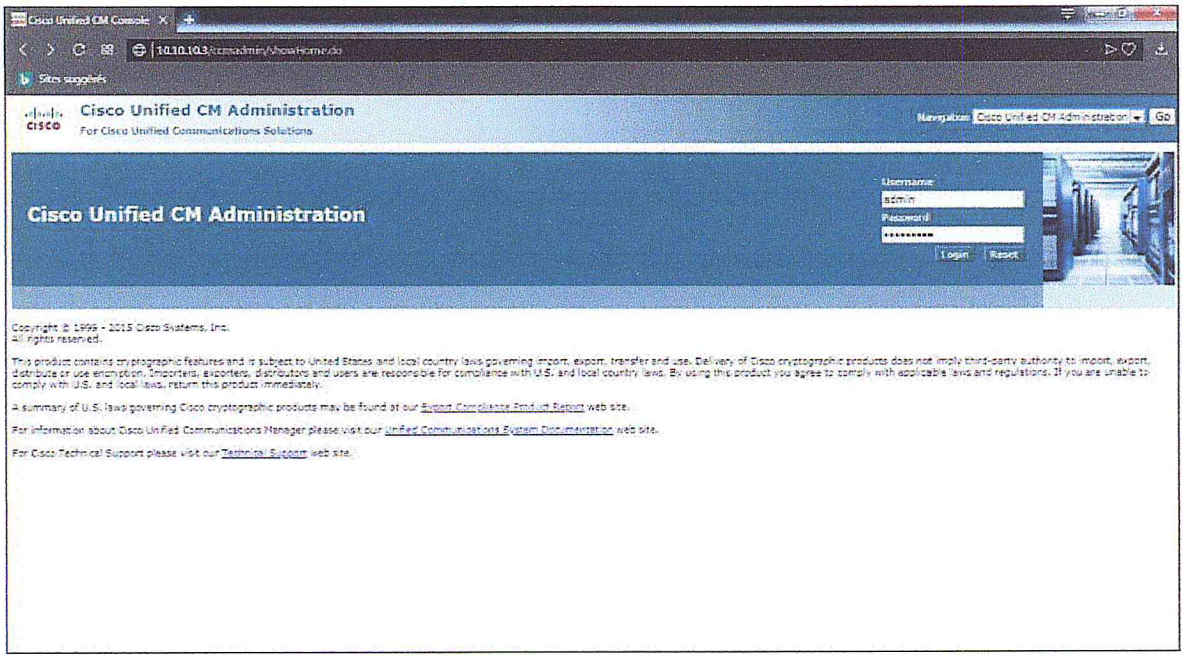


Figure IV.1 : Interface Web du CUCM 10.5

IV.2.Phase D'Audit

Lors de la réalisation de notre PFE, nous avons eu accès au service DCSI local de NAFTAL. Pour mener à bien une attaque, nous devons d'abord collecter les informations nécessaires sur les protocoles utilisés, les ports ouverts. Nous avons donc utilisé l'outil NMAP. Nous avons utilisé la commande « nmap 10.10.10.3 » pour Scanner les ports ouverts de serveur *CallManager*. Cette commande permet de vérifier la sécurité de base de serveur en identifiant les ports ouverts, donc susceptibles d'être attaqués.

```
root@kali:~# nmap  10.10.10.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-05 13:49 CEST
Nmap scan report for 10.10.10.3
Host is up (0.55s latency).
Not shown: 902 filtered ports, 82 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
1720/tcp open  h323q931
2000/tcp open  cisco-sccp
2001/tcp open  dc
2002/tcp open  globe
5001/tcp open  commplex-link
5004/tcp open  avt-profile-1
5060/tcp open  sip
5061/tcp open  sip-tls
8002/tcp open  teradataordbms
8080/tcp open  http-proxy
8090/tcp open  opsmessaging
8443/tcp open  https-alt
8500/tcp open  fmtp

Nmap done: 1 IP address (1 host up) scanned in 276.37 seconds
```

Figure IV.2 : Résultat de scan par NMAP

La commande nmap -p 5060 10.10.10.1-254 permet d'afficher les hôtes ouverts avec leur port et service, elle donne également l'adresse MAC de cet hôte.Ces informations sont sensibles et peuvent être exploitées par des pirates informatiques.

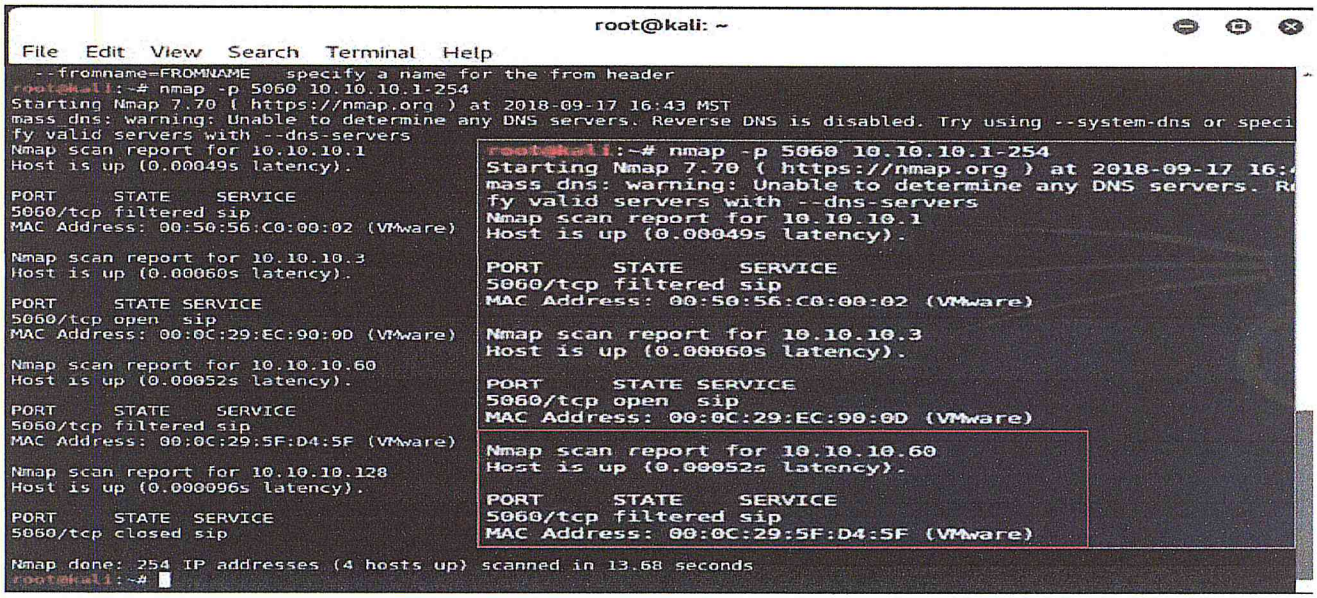


Figure IV.3 : Résultat de scan par NMAP

IV.3. Attaques simulées

IV.3.1. Écoute clandestine (eavesdropping)

En utilisant l'outil Ethercap pour faire un "poison ARP" qui vise à détourner le trafic vers le pc qui initié l'attaque (10.10.10.130)

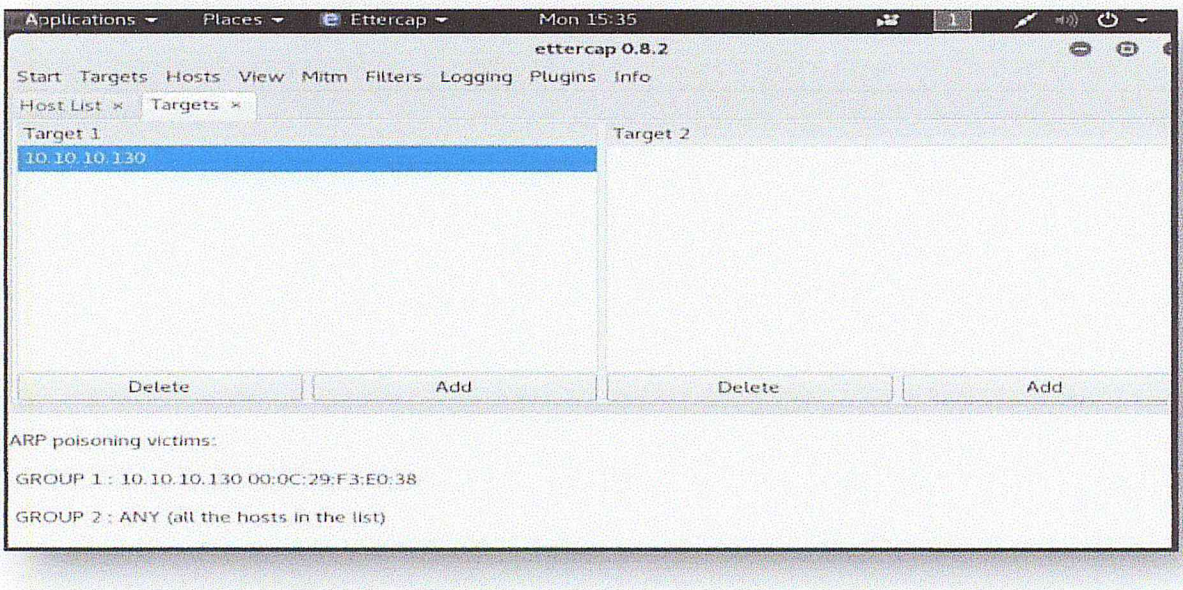


Figure IV.4 : Lancement de ARP poisoning en utilisant Ettercap

Puis, comme il n'y a pas de chiffrement et à l'aide de Wireshark, nous pouvons écouter le flux RTP.

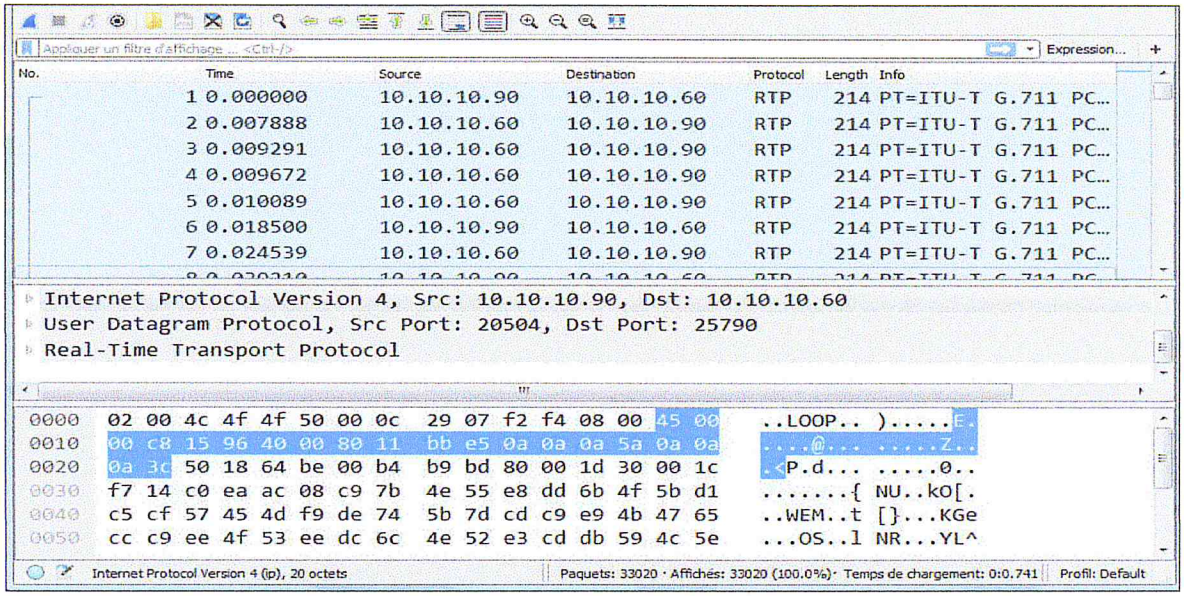


Figure IV.5 : Flux RTP capté par Wireshark

Pour l'écoute de la communication, nous avons utilisé la fonctionnalité player RTP intégrée dans Wireshark.La figure IV.4 montre le décodage de flux RTP par Wireshark.

Figure IV.6 : Le flux décodé par Wireshark

IV.3.2. DOS par Bulk INVITE

En falsifiant des requêtes "INVITE" (Figure IV.5) et en les envoyant en grand masse au serveur CUCM, nous avons provoqué un DoS.

Il ne sera plus possible de faire un appel du CIPC_1 vers CIPC_2 ou inversement.

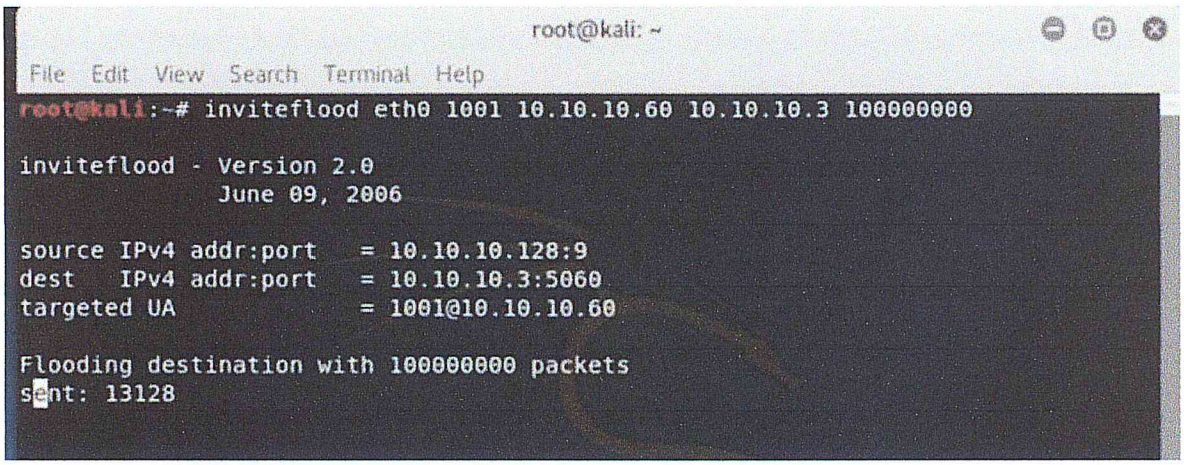


Figure IV.7 : La commande INVITEflood

En utilisant wireshark, nous pouvons capturer l'attaque INVITEFlood, en peut observer le grand nombre de packets envoyés

No.	Time	Source	Destination	Protocol	Length	Info
22506	2.536326	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22507	2.536327	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22508	2.536327	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22509	2.536329	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22510	2.536330	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22511	2.536331	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22512	2.536352	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22513	2.536353	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22514	2.536354	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22515	2.536355	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22516	2.536356	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |
22517	2.541405	10.10.10.128	10.10.10.3	SIP/SDP	1099	Request: INVITE sip:1001@10.10.10.60 |

Figure IV.8 : L'attaque INITEflood capté par wireshark

IV.3.3. DoS (RTPFlood)

Après avoir écouté un trafic RTP En générant des requêtes "RTPFLOOD" (Figure IV.8) avec un grand nombre de paquets RTP, nous avons provoqué un DoS qui a pour but de perturber une communication en cours

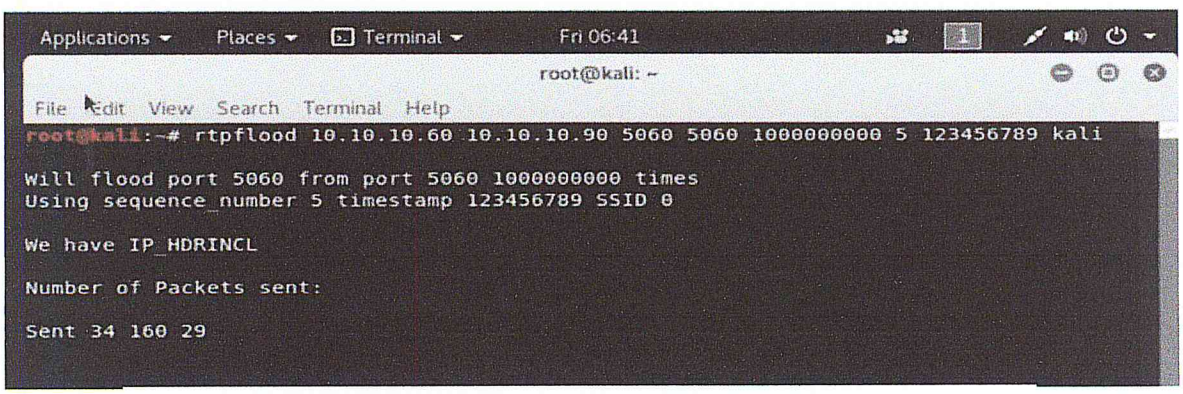


Figure IV.9 : La commande RTPflood

IV.3.4. Usurpation d'identité

L'outil MSFConsole (MetaSploit Framework Console) nous permet de générer une fausse requête INVITE et de l'envoyer à CUCM à l'aide d'un ID utilisateur légitime.

Dans cet exemple nous avons envoyé fake SIP Invite avec l'adresse IP 10.10.10.60 à CUCM qui a l'adresse 10.10.10.3

```
msf auxiliary(voip/sip_invite_spoof) > set domain 10.10.10.3
domain => 10.10.10.3
msf auxiliary(voip/sip_invite_spoof) > set RHOSTS 10.10.10.60
RHOSTS => 10.10.10.60
msf auxiliary(voip/sip_invite_spoof) > set SRCADDR 10.10.10.3
SRCADDR => 10.10.10.3
msf auxiliary(voip/sip_invite_spoof) > run

[*] Sending Fake SIP Invite to: 10.10.10.3
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(voip/sip_invite_spoof) >
msf auxiliary(voip/sip_invite_spoof) > show options

Module options (auxiliary/voip/sip_invite_spoof):

   Name       Current Setting          Required  Description
   ----       ---------------          --------  -----------
   DOMAIN     10.10.10.3               no        Use a specific SIP domain
   EXTENSION                           no        The specific extension or name t
o target
   MSG        The Metasploit has you   yes       The spoofed caller id to send
   RHOSTS     10.10.10.60              yes       The target address range or CIDR
 identifier
   RPORT      5060                     yes       The target port (UDP)
   SRCADDR    10.10.10.3               yes       The sip address the spoofed call
 is coming from
   THREADS    1                        yes       The number of concurrent threads
```

Figure IV.10: Attaque Usurpation d'identité

IV.4. Mise en œuvre d'une architecture sécurisée

La sécurité de l'architecture de ToIP du NAFTAL, illustré dans la figure IV.10, notre proposition de sécurité passe par deux phases : la première comprend la sécurité de la voix dans le LAN, le second consiste effectivement à sécuriser la voix dans les réseaux WAN.

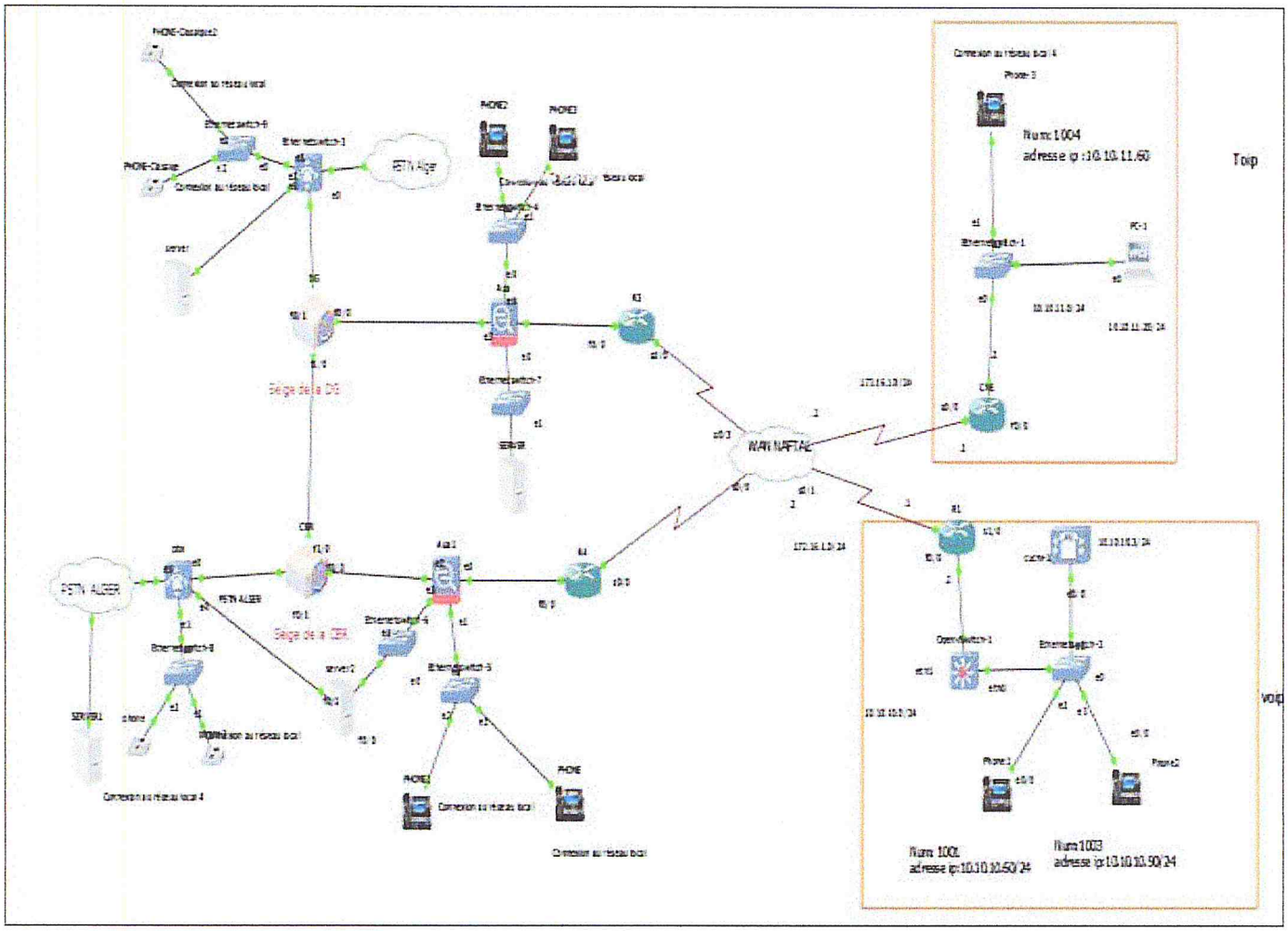


Figure IV.11 L'architecture simulé

IV.4.1. Sécurisation du LAN

La sécurisation du LAN passe par trois étapes essentielles :

- Activation le Mixed-mode.
- Configuration d'un profil sécurisé associé au téléphone.
- Configuration des utilisateurs finaux« end users »

IV.4.1.1. Activation du « mixed mode » sur le CUCM

Avec CLI du CUCM, on active le mode « mixed » pour que ce dernier puisse supporter le mode sécurisé. Un redémarrage du CUCM est nécessaire.

```
Cisco Unified Communications Manager 10.5.2.10000-5
cucum login:

Cisco Unified Communications Manager 10.5.2.10000-5
cucum login: meriem
Password:
Last login: Wed May 30 18:44:16 on tty1
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        2 vCPU: Intel(R) Core(TM) i3-4005U CPU @ 1.70GHz
        Disk 1: 80GB, Partitions aligned
        2048 Mbytes RAM

admin:utils ctl set-cluster mixed-mode
```

Figure IV.12 : Activation du mode « MIXED»

Pour s'assurer que le mixed Mode est activé on doit Vérifier, via (System > Entreprise parameters) , que le champ Cluster Security Mode est à 1.

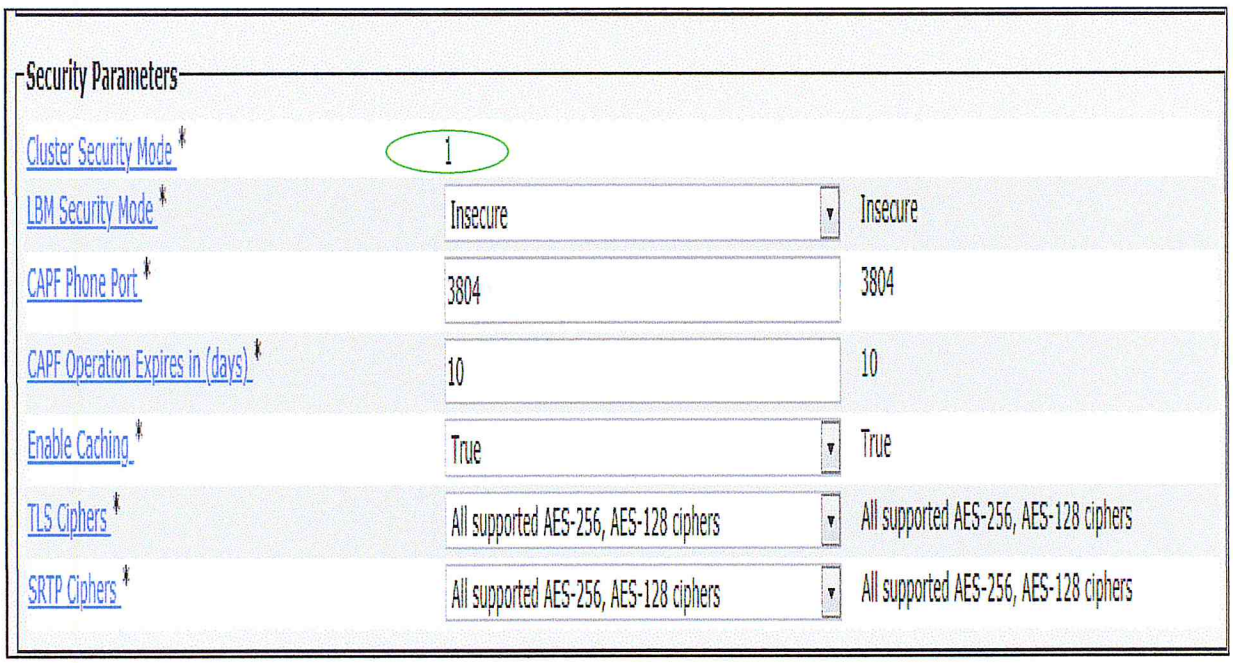


Figure IV.13 : Vérification du CUCM

IV.4.1.2. Configuration d'un profil sécurisé

La création d'un nouveau profil avec des paramètres de sécurités est nécessaire pour l'installer plus tard aux téléphones IP. Cela permet de mettre l'IP phone en mode sécurisé

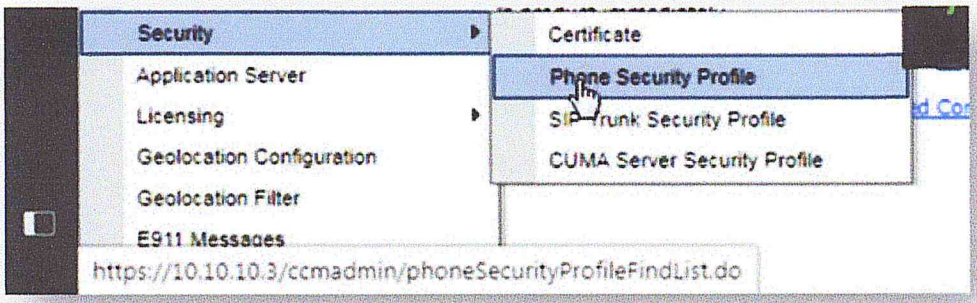


Figure IV.14 Ajout d'un nouveau profil

Le mode « Encrypted » dans le champ « Device Security Mode » active l'utilisation de TLS avec les clés AES 128/ SHA pour la signalisation et le SRTP pour le flux.

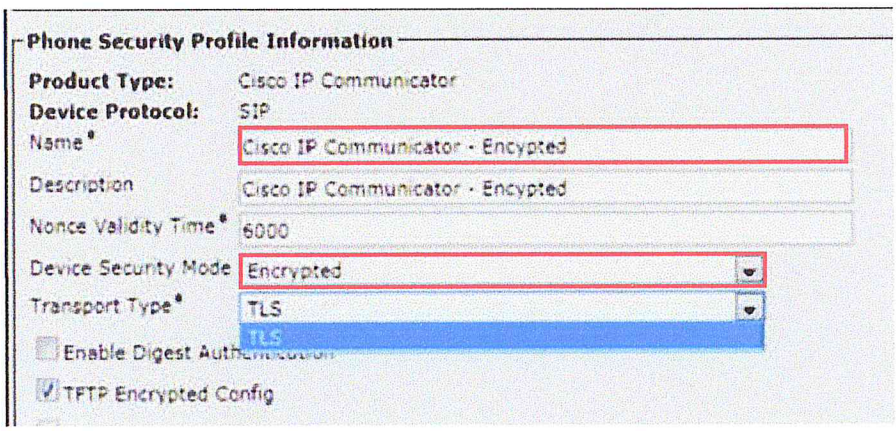


Figure IV.15 Configuration du profil sécurisé

IV.4.1.3. Configuration des Utilisateurs Finaux « end users »

Cette étape consiste à implémenter l'authentification HTTP Digest en créant un terminal usager pour chaque IP-phone en lui attribuant un mot de passe. Un utilisateur ne peut pas posséder deux téléphones en même temps.

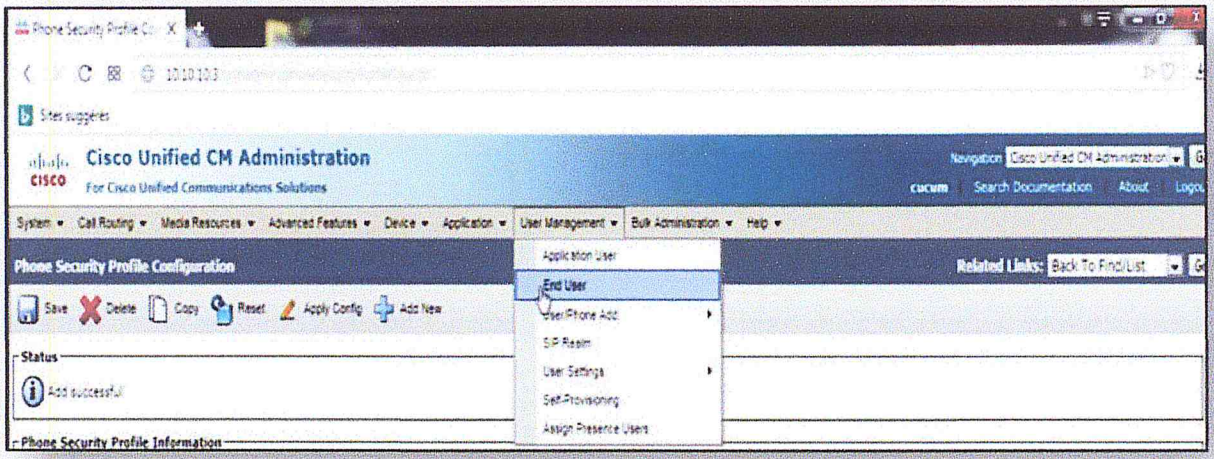


Figure IV.16 Ajout d'un nouveau terminal

Le champ Digest Credentials doit être une chaîne de caractères alphanumériques. Cette authentification applique une fonction de hachage au nom d'utilisateur et mot de passe avant de les envoyés sur le réseau.

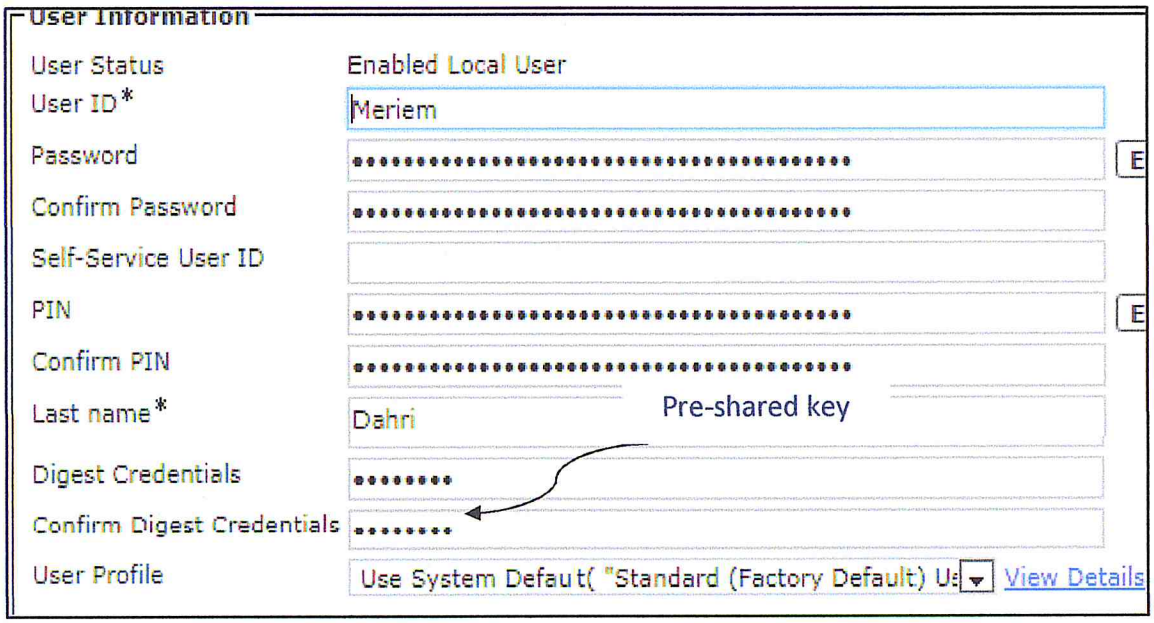


Figure IV.17 : L'authentification Http Digest

IV.4.1.4. Enregistrement du téléphone

La dernière étape consiste à l'enregistrement des IP Phone en mode sécurisé (Via : Device > phone > add new). Cette phase fait appel au « phone Security profile » et « end users » préalablement créés.

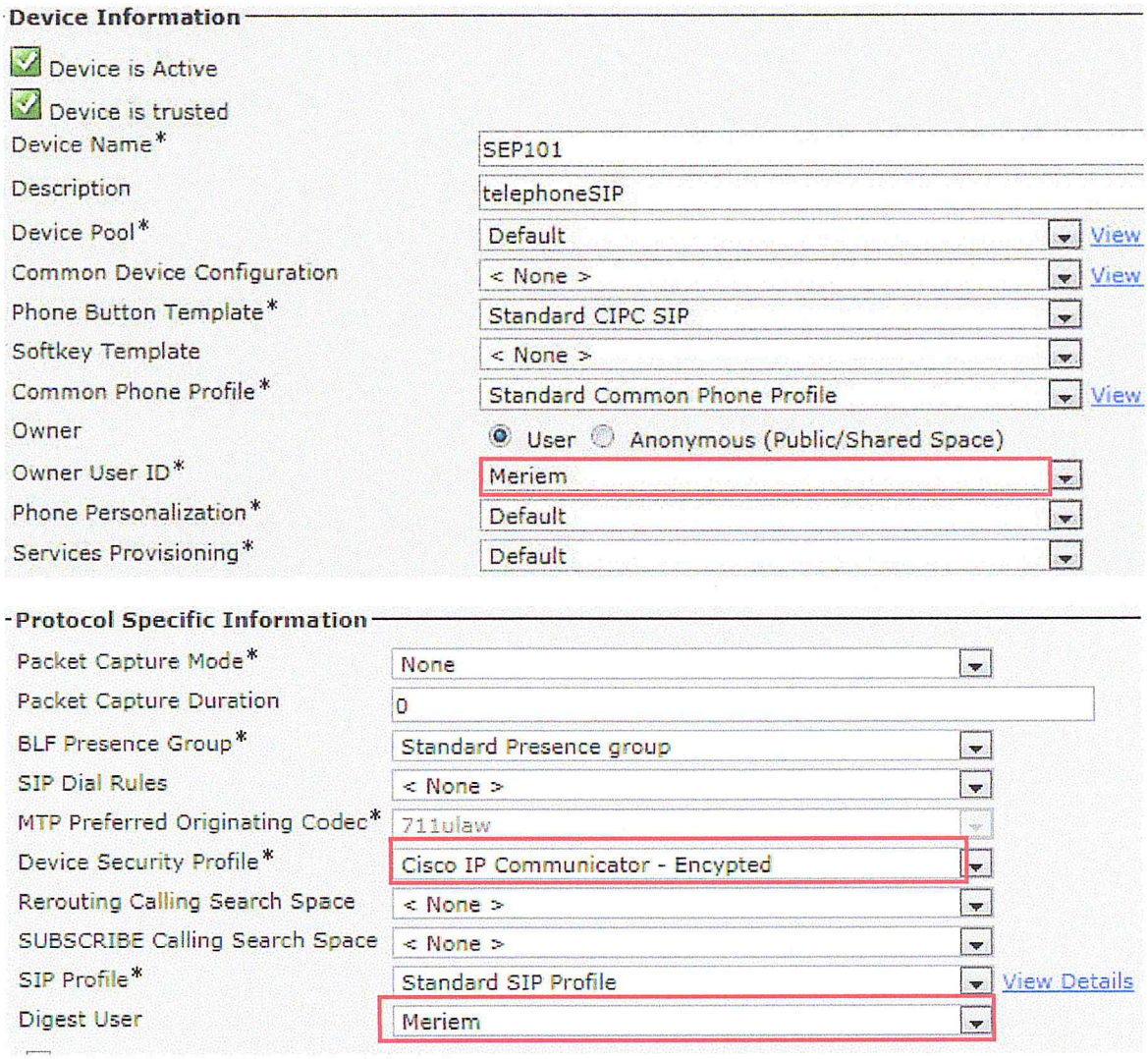


Figure IV.18 : Enregistrement du téléphone IP

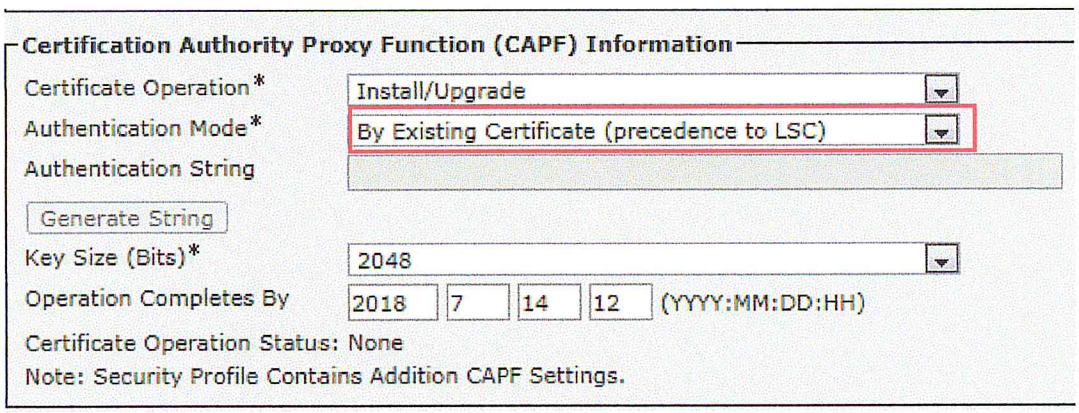


Figure IV.19 : Enregistrement du téléphone IP sécurisé par LSC

Nous avons rencontré un problème lors la sécurisation de IP phone, car pour mettre le ce dernier à l'état sécurisé il faut que LSC (Locally Significant Certificate) soit installé. L'installation du LSC nécessite l'utilisation d'au moins deux eTokens USB et du client CTL.

Le client CTL est utilisé pour générer les certificats nécessaires sur le CallManager. Une fois que le fournisseur CTL et les services CAPF sont activés sur le cluster, le client CTL peut être exécuté pour générer le fichier CTL sur le CallManager. Une fois ce processus terminé, il est alors possible de définir "Opération de certificat" sur le téléphone IP sur "Installer / mettre à niveau" via l'interface CCMAdmin.

Sans le USB eToken et le client CTL, il n'y a aucun moyen d'installer des LSC sur les téléphones IP Le numéro de pièce de l'eToken USB est: KEY-CCM-ADMIN-K9 =. [33]

Nous avons réussit de mettre le IP Phone a l'état Encrypted,mais faute de matériel(manque de USB eToken) le LSC n'a pas été installé.

Théoriquement, le LSC a été installé, notre téléphone IP sera sécurisé, la voix sera cryptée et c'est notre objectif de cette configuration.

Figure IV.20: Etat de téléphone avant et après la sécurisation

Le redémarrage de téléphone est nécessaire. Le mot de passe définit auparavant doit être saisie pour que le IP phone puisse s'enregistrer.

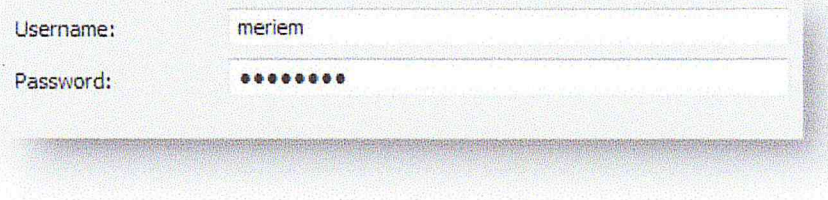


Figure IV. 21 Saisie de mot de passe sur l'IP-phone

L'authentification Digest applique une fonction du hachage cryptographique MD5 avec utilisation de valeurs nonce .la figure IV.22 Montre le défi http digest.

Figure IV.22 : défi http digest

IV.4.2. Sécurité WAN

Commençant par sécuriser la partie trunk entre le CUCM et le CUBE, puis nous allons passer au WAN où nous allons implémenté le VPN-IPsec.

IV.4.2.1.Configuration du CUBE

CUBE (Cisco Unified Border Element) est un élément de frontière de communications unifiées qui relie la connectivité voix et vidéo entre deux réseaux VoIP distincts. [32]

CUBE est utilisé par les entreprises pour interconnecter l'accès SIP PSTN aux réseaux de communications unifiées d'entreprise SIP et H.323.

Nous avons choisi le cube car il fournit des services d'interconnexion sécurisés entre les réseaux IP.

Etape 1 : Configuration du CUBE sur le routeur

1. Activation du mode CUBE sur le routeur.

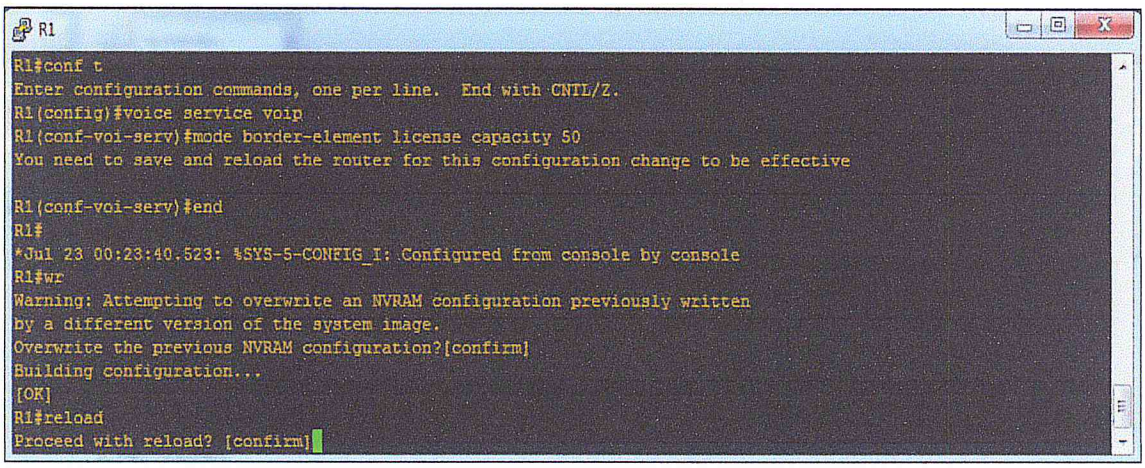


Figure IV.23 : Activation du mode CUBE

Tout d'abord, nous devant nous assurer que le serveur HTTP sur le routeur est activé car, par défaut, le port 80 (TCP) sera utilisé pour la concession des certificats et pour l'acceptation des demandes de signature des certificats par IOS CA (*certificate authority/Autorité de Certification*).

2. la génération des clés privées et publiques RSA.

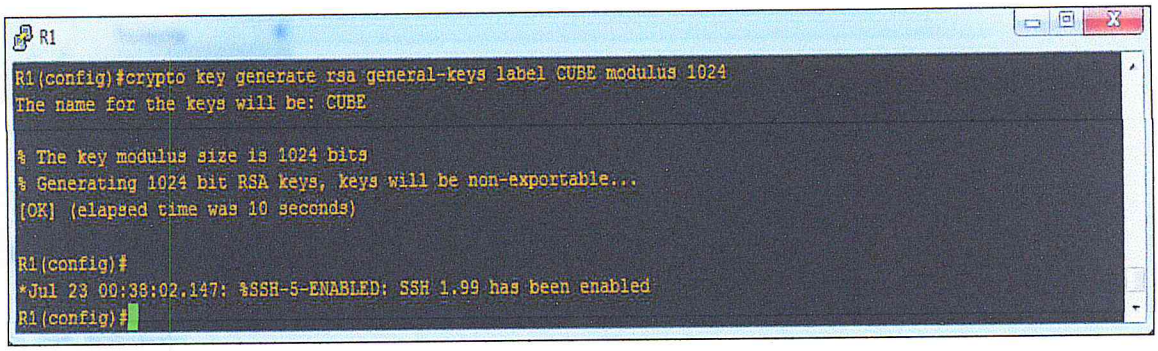


Figure IV.24 : Génération des clés RSA

3. Configuration et activation du CA.

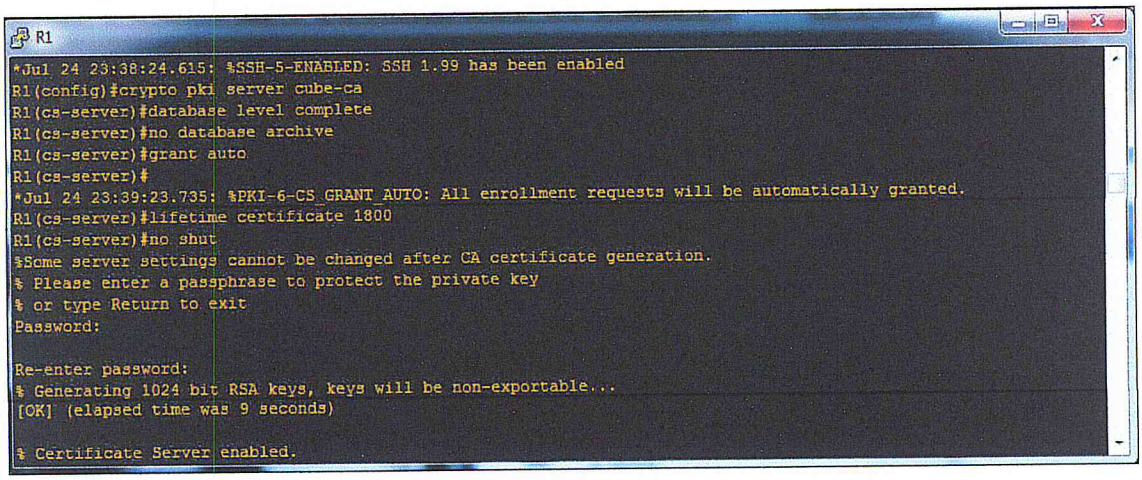


Figure IV.25 : Configuration du CA

4. Création du point de confiance pour cube « CUBE-TLS ».

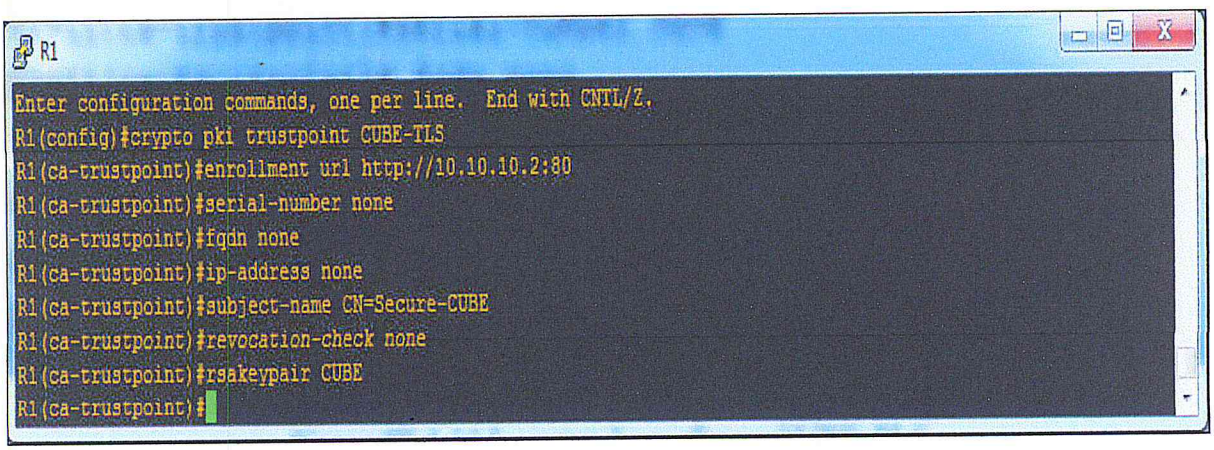


Figure IV.26 : Le point de confiance CUBE-TLS

5. Authentification du point de confiance « CUBE-TLS » avec le serveur CA.

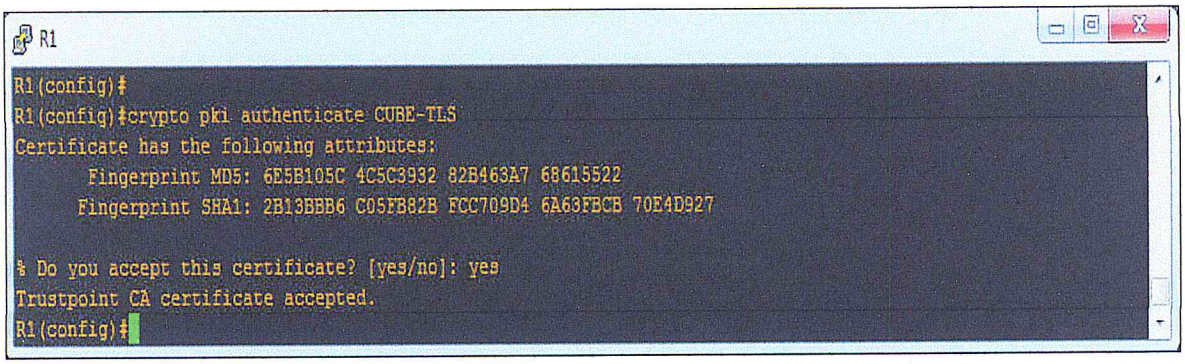


Figure IV.27 : Authentification de CUBE-TLS

6. Inscription du point de confiance avec le serveur CA.

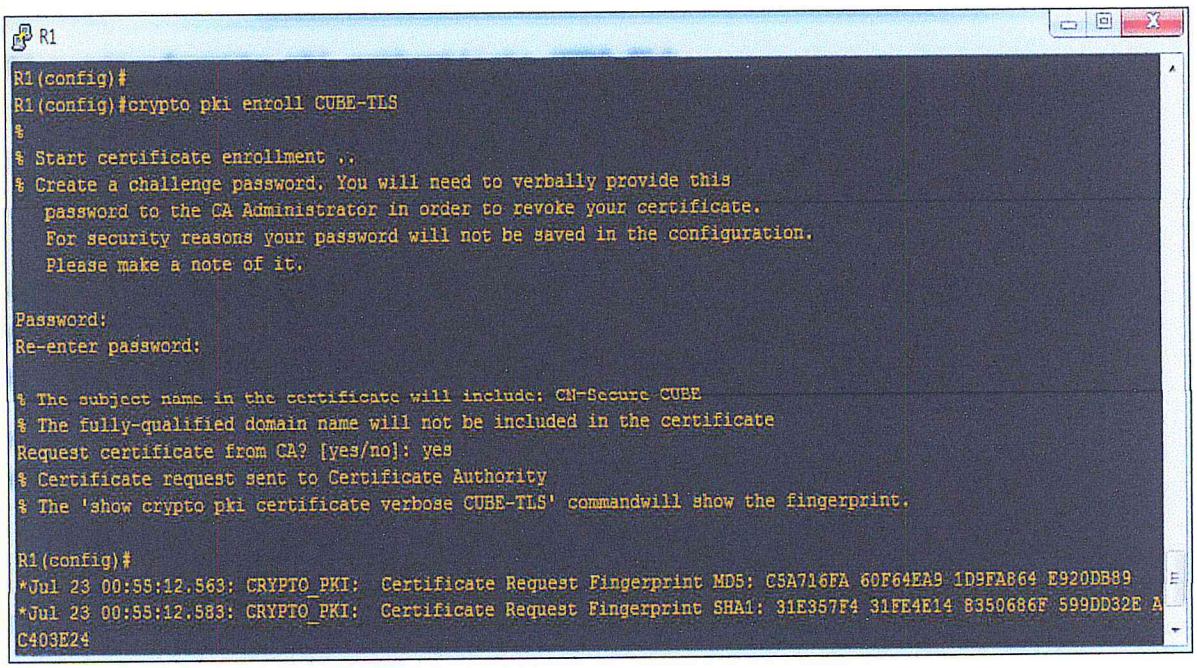


Figure IV.28 : Inscription de CUBE-TLS

7. Création d'un point de confiance pour le CUCM

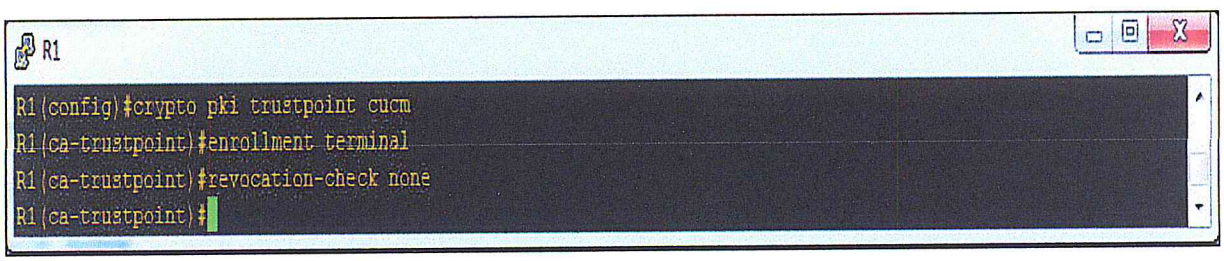


Figure IV.29: Création du point de confiance « cucm »

Sur le CUCM via (Security > Certificate Management > Find), nous allons telecharger le « CallManager certificat .PEM », l'ouvrir avec Notepad et copier/coller son contenu dans CUBE comme indiqué sur la figure IV.24

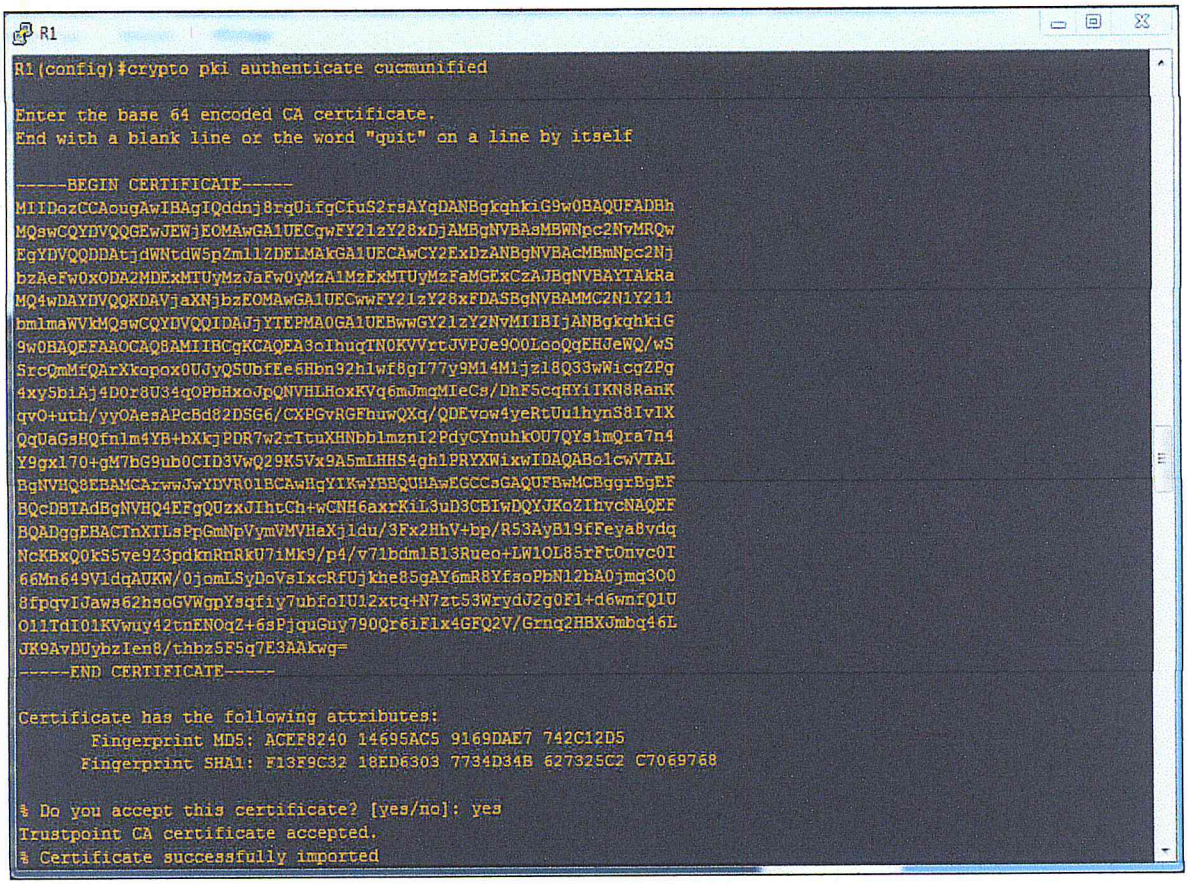


Figure IV.30 : Authentification du cucm.

8. Configuration de TCP TLS comme un protocole de transport sur le cube

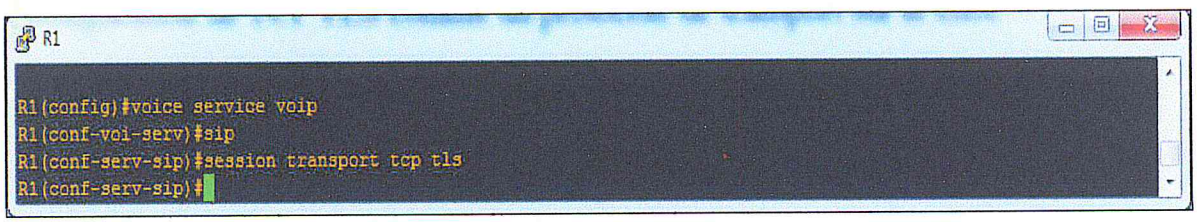


Figure IV.31 : Activation de TLS

9. Configuration de CUBE-TLS comme point de confiance par défaut pour toutes les signalisations SIP de CUBE

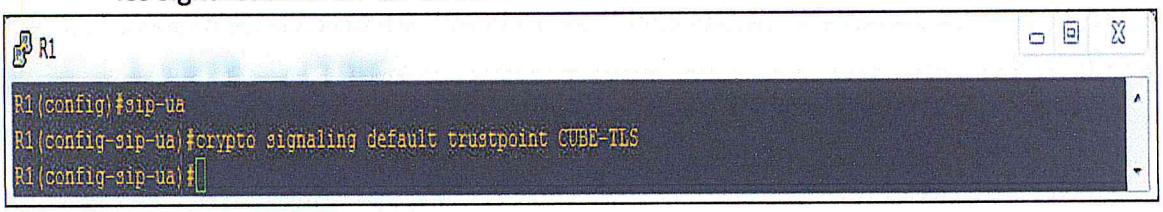


Figure IV.32: Configuration du CUBE-TLS comme point de confiance

10. Activation de SRTP sur CUBE :

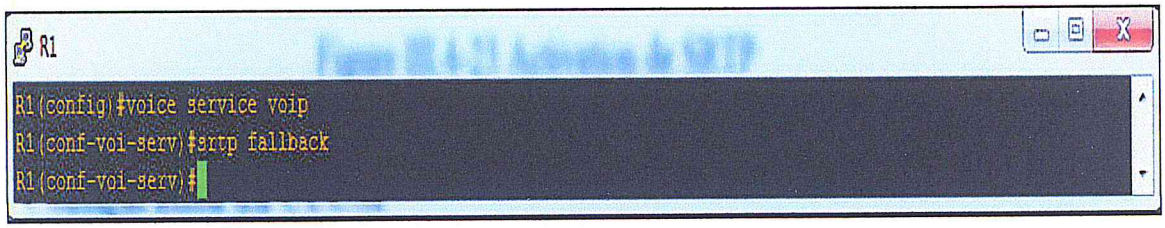


Figure IV.33 : Activation de SRTP

Etape 2: Configuration du CUCM

Maintenant nous allons exporter « CUBE-TLS certificate » au CUCM. (Copier le certificat auto-signé par CA et la coller sur Notepad et l'enregistrer sous forme .PEM)

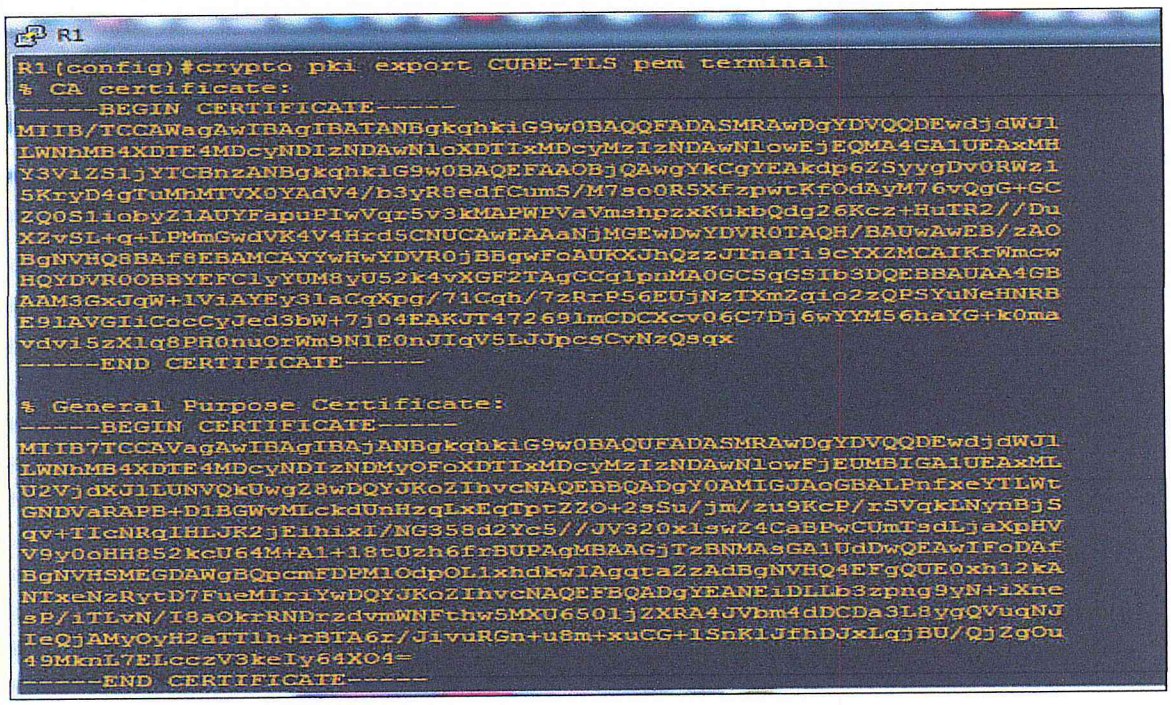


Figure IV.34 : le certificat de CUBE

11. Téléchargement du certificat sur le CUCM (en tant que CALLManager-trust via Security > Certificate Management > Upload Certificate/Certificate Chain)

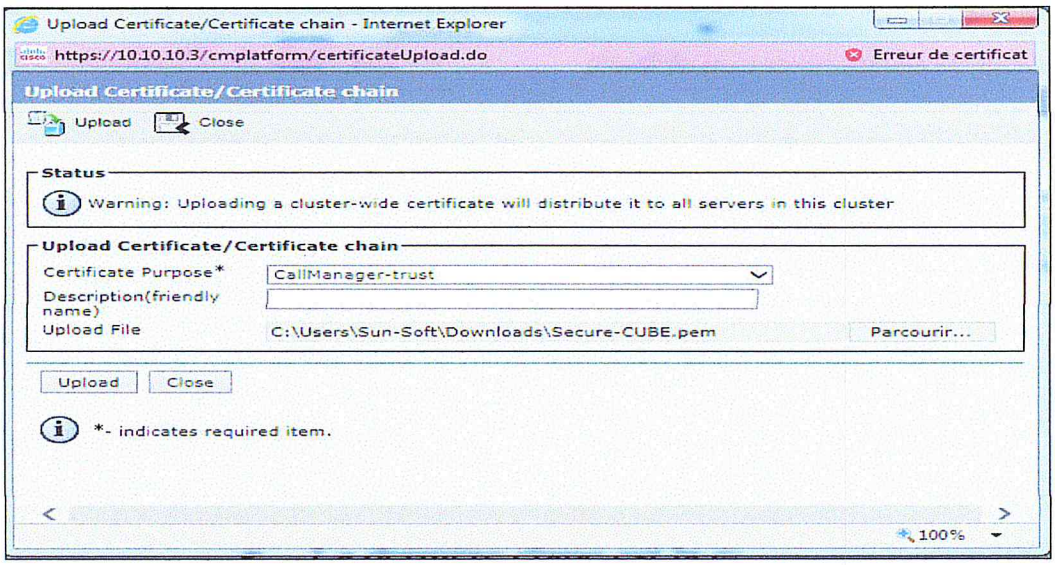


Figure IV.35 : Téléchargement du certificat sur le CUCM

12. La dernière étape est la création d'un nouveau SIP Trunk Security Profile (System > Security > SIP Trunk Security Profiles > add new)

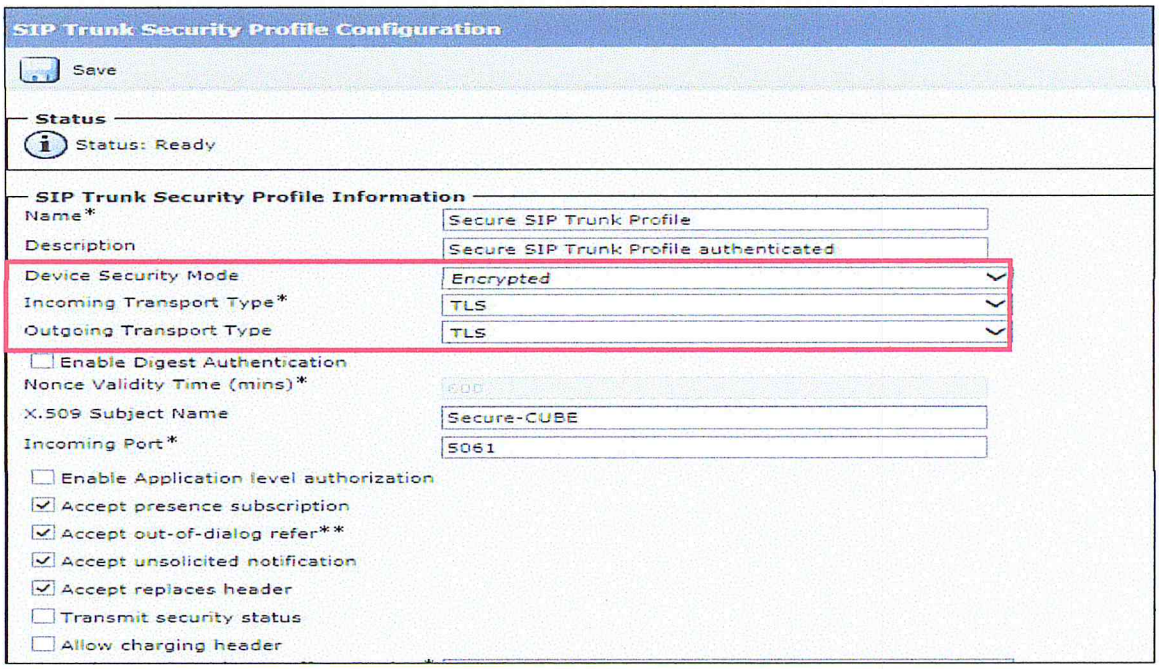


Figure IV.36 : Creation d'un nouveau SIP Trunk Security Profile

En conséquence de cette configuration on aura une signalisation authentifiée Mutuellement entre le CUCM et les téléphones IP en utilisant SIP/TLS et Http Digest, et un flux médias chiffrés lui aussi à l'aide de SRTP. Par le manque des ressources nous étions obligés de réaliser une partie de notre architecture dans un environnement GNS3, cette partie consiste à sécuriser le trafic VoIP dans le WAN via un tunnel VPN-IPSEC

IV.4.2.2. Configuration d'IPSec

Nous avons commence par la configuration de politique isakmp. On a défini ensuite les paramètres suivants:

- Encryptage AES
- Authentification par clé pré-partagées.
- Algorithme de hachage SHA (valeur par défaut).
- Méthode de distribution des clés partagées DH-2 (Algoritme de clé asymétriques Diffie-Hellman 1024bits)
- Durée de vie 3600 secondes (1h) (valeur par défaut).

```
R1#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#hash md5
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#EXIT
```

Figure IV.37 : création d'un numéro de séquence 10

On a crée ensuite une clé pré-partagée « voip » qu'on associe avec l'adresse de l'autre bout du tunnel (172.16.1.2)

La méthode de cryptage (transform-set) que l'on nomme siteA.

Esp-aes est la méthode de cryptage, esp-sha-hmac est la méthode d'authentification.

```
R1(config)#crypto isakmp key voip address 172.16.1.2
R1(config)#crypto ipsec transform-set  siteA esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)#mode transport
```

Figure IV.38 : cryptage de données

La création d'ACL etendue permet de filtrer les packet a travers VPN-IPsec et crypto map qui permet definir un lien entre isakmp et la configuration de IPsec

```
R1(config)#crypto ipsec security-association lifetime seconds 1800
R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255
R1(config)#crypto map mapsiteA 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#match add 101
R1(config-crypto-map)#set peer 172.16.1.2
R1(config-crypto-map)#set pfs group2
R1(config-crypto-map)#set security-association lifetime seconds 900
R1(config-crypto-map)#exit
```

Figure IV.39 : Configuration acl et crypto map.

Nous avons appliqué cette crypto-map à l'interface sortie de router S0/0 de mapA

```
R1(config)#int f0/1
R1(config-if)#crypto map mapsiteA
R1(config-if)#
*Aug  8 15:23:12.971: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#end
R1#
```

Figure IV.40 : Application de crypto-map à l'interface WAN

La figure ci-dessous montre que le trafic circulant entre les deux sites distants est crypté, Apres VPN -IPsec.

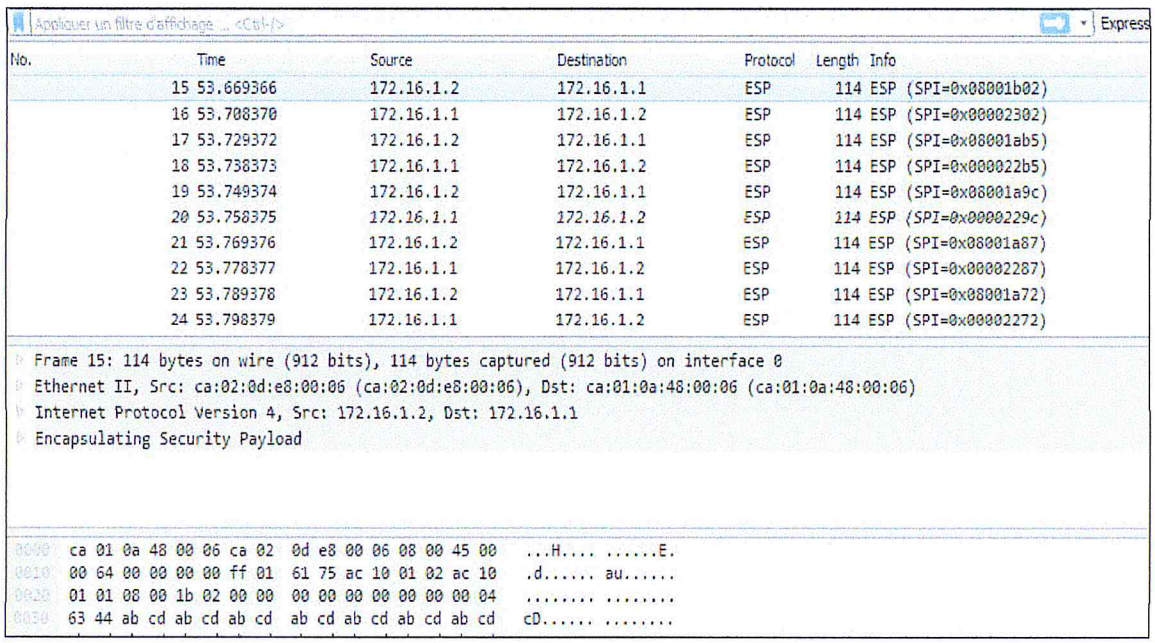


Figure IV.41 : Capture de trafic avec Wireshark

Conclusion

Dans ce chapitre, nous avons proposé des solutions et les avons mises en œuvre pour établir une architecture de téléphonie IP sécurisée.

Pour ce faire, nous avons d'abord étudié et analysé les vulnérabilités existantes en matière de sécurité, puis identifié les risques afin d'obtenir une solution de sécurité robuste prenant en compte le niveau de sécurité requis selon les besoins de l'entreprise et les équipements disponibles.

Ces solutions proposées nous permettent de répondre à trois exigences majeures : Authenticité, intégrité et confidentialité.

Conclusion Générale

À la fin de notre travail effectué, nous concluons que la téléphonie sur IP a connu une croissance significative ces dernières années.

Notre objectif principal est mettre en œuvre une architecture de téléphonie sur IP sécurisée. Nous sommes tous au départ intéressés à étudier cette technologie en détail, y compris ses différents protocoles et standard.

Nous avons ensuite étudié divers problèmes liés à la sécurité de la voix sur IP, aux attaques et aux Faiblesses sur différents niveaux et solutions possibles pour réduire ces attaques.

Enfin, nous avons effectué un audit de sécurité sur l'architecture actuelle afin de déceler les lacunes de cette dernière, certes la sécurité n'est pas absolue et les risques restent présents. Malgré la difficulté de la tâche, le manque d'équipement en temps voulu, ainsi que les licences CUBE, nous avons pu mis en place un ensemble de mécanismes de sécurité appropriés avec le niveau de sécurité requis par NAFTAL afin de renforcer cette structure et se protéger efficacement contre les différents risques impliqués.

Pour améliorer la sécurité de la téléphonie IP de l'entreprise NAFTAL on propose de mettre en place des systèmes redondants pour gérer les ressources local et distantes et mutualiser les ressources afin d'assurer une haute disponibilité. On propose aussi l'adaptateur Cisco SPA122, ce dernier prend en charge des méthodes hautement sécurisées basées sur le cryptage pour la communication, et la mise en service et la maintenance.

Le développement de ce travail nous a permis. D'une part, savoir sécuriser les réseaux VoIP et approfondir les connaissances acquises au cours de nos années d'étude à l'Université Saad Dahlab blida 1, et d'autre part, nous avons présenté une technologie à grande échelle par les grandes entreprises dans le domaine des TIC.

Bibliographie

[1] H. DWIVEDI, HACKING VOIP, SAN FRANCISCO: MEGAN DUNCHAK, 2009.

[2] G.THOMAS, SECURITE DE LA TELEPHONIE SUR IP. RESEAUX ET TELECOMMUNICATIONS [CS.NI]. TELECOM PARISTECH, 2010.

[3] M.LABIDI, ETUDE ET MISE EN PLACE D'UNE SOLUTION VOIX SUR IP SECURISEE, PROJET DE FIN D'ETUDE, 2013.

[4] Z.SIMON, D.JEAN-LOUIS, SIP_EFORT, R GELDWERTH, 2005.

[5] I.DEBBI, C.LAMICHE, ABBACHE, ETUDE ET ELABORATION D'UNE TECHNIQUE DE PROTECTION DE LA VOIX SUR IP, MEMOIRE DE FN D'ETUDE ,2015.

[6] M.BENISSE, TRANSMISSION MÉDIA SUR LES RÉSEAUX IP EN UTILISANT LES PROTOCOLES SIP ET IAX, MÉMOIRE PRÉSENTÉ À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE, MONTRÉAL, 2009.

[7] K.DOUBAL, K.SEDDI, SECURITE DES DONNEES DE LA VOIP BASEE SUR FIRWAL, MEMOIRE DE FIN CYCLE, BEJAIA, 2017.

[8] JUG.AIT AMMARA, L.AMEZZA, ORGANISATION DU RESEAU EN VLAN CAS D''ETUDE ENTREPRISE NAFTAL, BEJAIA, MEMOIRE DE FIN DE CYCLE, 2017.

[9] ALISTAIR DOSWALD (HEIG) ET ALL, BEST PRACTICES FOR VOIP-SIP SECURITY, 2006.

[10] F. CUPPENS, N. CUPPENS, Y.BOUZIDA, DETECTION D'INTRUSION ET REACTION DANS LES RESEAUX VOIP, PROJET BIBLIOGRAPHIQUE ENST BRETAGNE, 2008.

Webographie

[11] **https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-security-advisories-list.html 19:17 09/03/2018**

[12] **https://www.networkworld.com/article/2274082/lan-wan/chapter-1--cisco-unified-communications-manager-architecture.html 18:57** ***07/03/2018***

[13] **https://www.dekom.com/fr-fr/visioconference/produits/cisco-jabber/18:00** ***09/03/2018 18 :38***

[14] **https://www.cert.ssi.gouv.fr/avis/CERTA-2012-AVI-503/19:23** ***09/03/2018***

[15] **www.naftal.dz**

[16] **https://www.cisco.com/c/dam/global/fr_ch/assets/docs/Cisco_Unity_Connection.pdf19:40 09/03/2018**

[17] **https://fr.wikipedia.org/wiki/Jabber 12/09/2018**

[18] **https://fr.scribd.com/document/372122889/TheseV0 12/09/2018**

[19] **http://ipbx.pro/le-concept-de-t-voip/ 14/09/2018**

[20] **http://igm.univ-mlv.fr/~dr/XPOSE2009/Introduction au Cisco Call Manager/VOIPTOIP.html**

[21] **http://www.itresearch.fr/differences-entre-voip-et-toip/ 14/09/2018**

[22] **https://fr.slideshare.net/stepmike/etude-et-mise-en-oeuvre-dune-architecture-de-telephonie-sur-ip-securisee-au-sein-de-data-consulting-circlemonrapport 17/04/2018**

[23]https://wapiti.telecomlille.fr/commun/ens/peda/options/st/rio/pub/exposes/exposesrio2003ttnfa04/couraudschoehn/rtcp.htm

[24] https://www.memoireonline.com/10/13/7498/m_Mise-en-place-dune-solution-VoIP-au-sein-de-lautorite-aeronautique-camerounaise21.html

[25] https://www.memoireonline.com/09/14/8917/m_Gestion-dinterconnexion-et-deregulation-de-flux-dappel-dans-serveur-telephonique-elastix36.html 05/05/2018

[26]polodossantos.ch/Documentation/Reseaux/Shared%20Documents/Réseaux%20Telephonie%20sur%20ip.pdf

[27] https://www.differencebetween.com/difference-between-sip-and-vs-sccp/

[28] https://aitibourek.wordpress.com/port-security-securisation-des-interfaces-du-switch/

[29] https://www.memoireonline.com/09/13/7361/m_Etude-dimplementation-dune-solution-VOIP-securisee-dans-un-reseau-informatique-dentrepr44.html

[30] www.nemako.net/dc2/?post/GNS3

[31] https://www.vmware.com/fr/products/workstation-pro.html

[32] https://www.cisco.com/c/en/us/td/docs/iosxml/ios/voice/cube/configuration/cube-book/voi cubeoverview.pdf

[42] https://community.cisco.com/t5/collaboration-voice-and-video/cucm-generating-lsc-certificates-for-secure phones/ta-p/3119717 20/09/2018

Annexe A. Les protocoles ToIP

TCP est un protocole de contrôle de transmission de la couche de transport du modele OSI est défini dans la RFC 793 qui il permet d établir la connexion, c'est-à-dire il simule un circuit virtuel entre les deux points qui échangent de l'information et garantie une certaine fiabilité des transmissions des données. Le protocole TCP etablit un mécanisme pour assurer le bon acheminement des données, Il utilise pour cela les adresses IP uniques à chaque ordinateur, à la manière d'une adresse postale .TCP a la capacité de mémoriser des données

ICMP est un protocole de message de contrôle sur Internet de la couche de réseau définie par la RFC 792 c'est un protocole de la signialisation du protocole IP qui permet de contrôle des erreurs de transmission des données.

UDP est protocole de datagramme utilisateur de la couche de transport du modele TCP/IP permet de transmission des paquets des données sans aucune garantie sans contrôle des erreurs.

Annexe B. les outils de sécurité

Certificat : Une identité électronique qui est émise par une tierce partie de confiance pour une personne ou une entité réseau. Chaque certificat est signé avec la clé privée de signature d'une autorité de certification. Il garantit l'identité d'un individu, d'une entreprise ou d'une organisation. En particulier, il contient la clé publique de l'entité et des informations associées à cette entité.

Certificat Auto signé : un certificat auto signé contient comme tout certificat une clé publique. Sa particularité réside dans le fait que ce certificat est signé avec la clé secrète associée. Dans ce cas précis, l'autorité de certification est donc le détenteur du certificat.

Certificat X.509 : Il s'agit d'une norme sur les certificats largement acceptée et conçue pour supporter une gestion sécurisée et la distribution des certificats numériquement signés sur le réseau Internet sécurisé. Le certificat X.509 définit des structures de données en accord avec les procédures pour distribuer les clés publiques qui sont signées numériquement par des parties tierces.

Clé : Une quantité utilisée en cryptographie pour chiffrer/déchiffrer et signer/vérifier des données. Se compose en deux types :

- **Clé privé :** quantité numérique secrète attachée à une ressource ou à un individu, lui permettant de déchiffrer des données chiffrées avec la clé publique correspondante ou d'apposer une signature au bas de messages envoyés vers des destinataires.
- **Clé publique :** quantité numérique, attachée à une ressource ou un individu, qui la distribue aux autres afin qu'ils puissent lui envoyer des données chiffrées ou déchiffrer sa signature.

AES : *standard de chiffrement avancé est un algorithme symetrique de cryptage par bloc* utilisé pour protégé des données

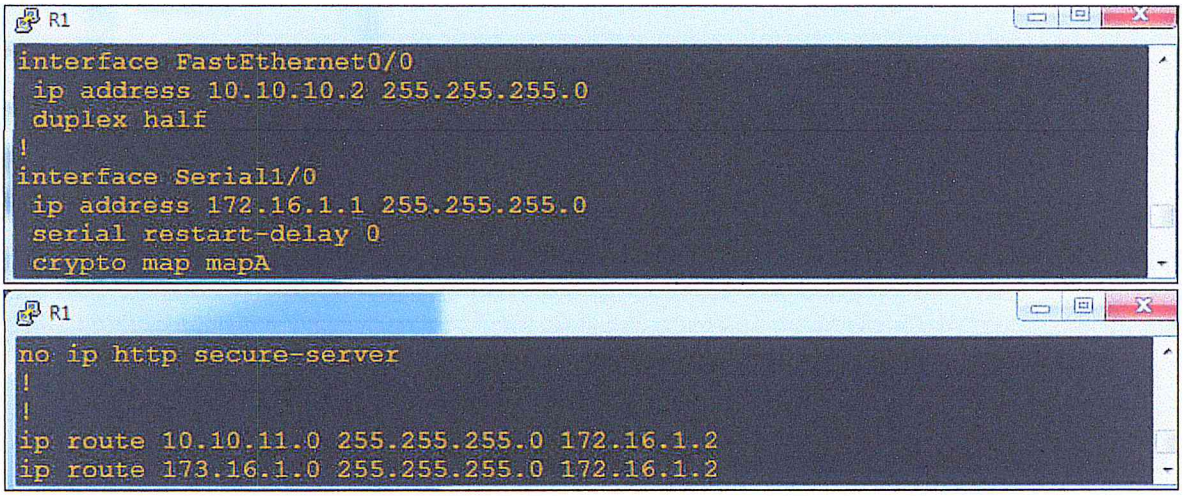
SHA1 : est une fonction de hachage cryptographique conçue par NSA

MD5 : Message Digest 5 c'est un algorithme de hachage utilisé en cryptographie dévloppé par « Ronald Rivest »

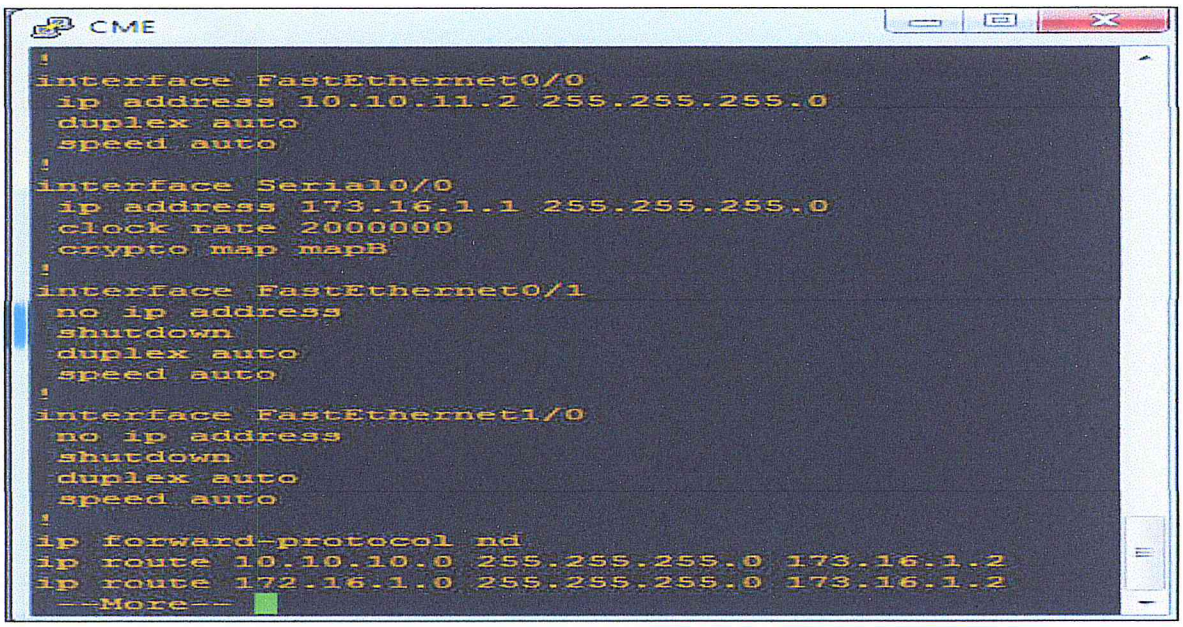
Annexe C. Configuration des Routeurs

Configuration des router

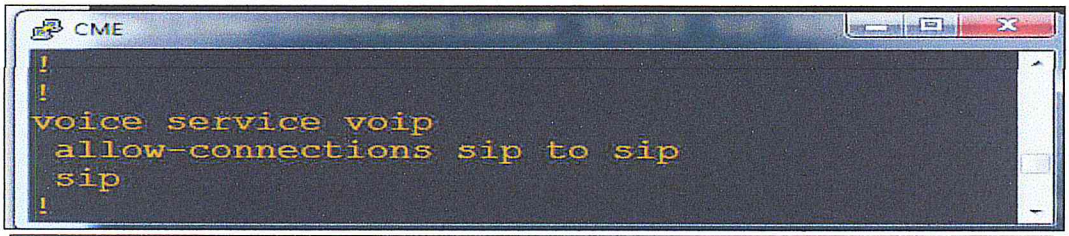
- **Router 1 (R1)**

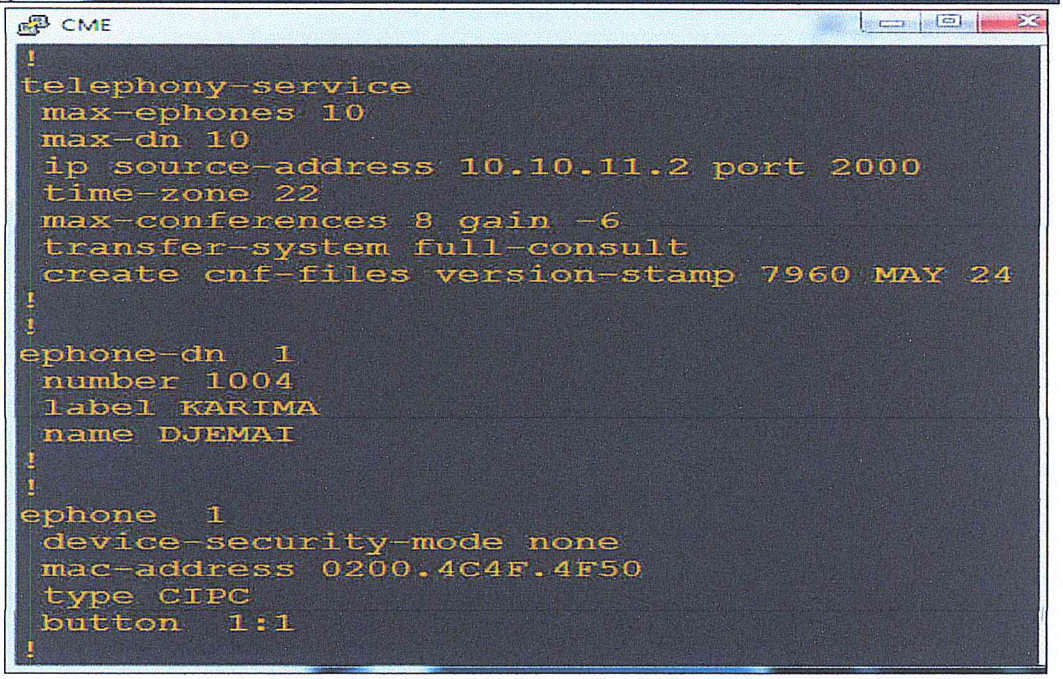


- **Router 2(CME)**



Les figures suivantes montrent les étapes de la configuration de callmanager express au niveau de routeur cme.





Le téléphone est configuré par cisco unified callmanager express (cme) avec numero d'utilisateur « 1004 » et un utilisateur « karima »