République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa

Faculté des Sciences Exactes

Département D'Informatique

Mémoire de fin de cycle
En vue de l'obtention du diplôme master professionnel en informatique
Spécialité : Administration et Sécurité des Réseaux

Thème

Sécurité des données de la VOIP basée sur Firewall

Membres du jury :

Président : Mr. ALOUI Abdelouhab

Examinateur : Mr. AMROUN Kamal

Encadreur : Mr. KHIREDDINE Abdekrim

Présenté par :

DOUBAL Kahina

SEDDI Kahina

Promotion 2016/2017

TABLE DES MATIÈRES

Table des matières **I**

Liste des abréviation **VI**

Introduction Générale **1**

1 Généralités sur les réseaux **3**
Introduction 3
1.1 Réseau informatique 3
1.1.1 Définition 3
1.1.2 Topologie des réseaux informatique 4
1.2 Réseau filaire 4
1.2.1 Définition 4
1.2.2 Les architectures des réseaux filaires 5
1.2.3 Les topologies des réseaux filaires 6
1.3 Réseau sans fils 8
1.3.1 Définition 8
1.3.2 Architecture des réseaux sans fil 9
1.3.2.1 Le réseau cellulaire 9
1.3.2.2 Le réseau mesh 10
1.3.2.3 Le réseau Ad-hoc 10
1.4 Réseau mobile 11
1.4.1 Présentation 11
1.4.2 Architecture de réseau de mobile 11
1.5 Générations des réseaux de mobiles 12
1.5.1 Première génération (1G) 12
1.5.2 Deuxième génération (2G) 13

1.5.3 Troisième génération (3G) 14
1.5.4 Quatrième génération (4G) 14
Conclusion 14

2 La téléphonie par paquet **15**
Introduction 15
2.1 Quelques définitions 15
2.1.1 la voix sur IP 15
2.1.2 La téléphonie sur IP 15
2.2 La téléphonie par circuit et par paquets 16
2.3 Comparaison entre la téléphonie par paquet et par circuit . . . 17
2.4 Les étapes de déroulement d'une communication téléphonique sur IP 18
2.4.1 Mise en place la communication 18
2.4.2 Établissement de la communication 18
2.4.3 Transport de l'information téléphonique 19
2.4.4 Changement de réseau 19
2.4.5 Arrivée au destinataire 19
2.5 Avantages de la ToIP 19
2.6 La problématique de base de la téléphonie 20
2.7 La dernière solution ToIP 20
Conclusion 21

3 Vulnérabilité des systèmes sur un environnement VoIP et les techniques de sécurité **22**
Introduction 22
3.1 Protocole de signalisation H.323 22
3.2 Protocole de signalisation SIP 23
3.3 Vulnérabilité des protocoles 24
3.4 Vulnérabilité sur l'infrastructure 25
3.4.1 Infrastructure Hardware 25
3.4.2 Infrastructure Software 26
3.5 Qualité de service 26
3.5.1 Protocole TCP et le transport de données multimédias temps réel 27
3.5.2 Protocole UDP et le transport de données multimédias temps réel 27
3.5.3 Les protocoles RTP et RTCP 27
3.6 Les attaques dans le réseau 30
3.6.1 Interruption 30
3.6.2 Interception 30

3.6.3 Modification 31
3.6.4 Fabrication 31
3.6.5 Les attaques dans les réseaux local 31
3.6.5.1 Usurpation IP spoofing 32
3.6.5.2 Vol de session (Connection Hijacking) 33
3.7 Mise en place d'une politique de sécurité 33
3.8 Les dispositifs de sécurité 34
3.8.1 Les firewall 34
3.8.1.1 Définition 34
3.8.1.2 Les différents types de firewall 34
3.8.2 Les systèmes de détection et de prévention de l'intrusion 35
3.8.3 VPN 35
Conclusion 35

4 Simulation d'un Réseau VoIP **37**
Introduction 37
4.1 Choix technique 37
4.1.1 GNS3(Graphical Network Simulator) 37
4.1.2 VMware Workstation 38
4.1.3 Cisco IP Communicator 38
4.1.4 Serveur TFTP (Trivial File Transfer Protocol) 39
4.1.5 Les plates-formes utilises 39
4.1.5.1 Routeur Cisco 3600 39
4.1.5.2 Firewall ASA 39
4.1.5.3 Switch 40
4.2 Présentation du prototype réalisé 41
4.2.1 Topologie 41
4.2.2 La configuration des équipements du réseau de la topologie 41
4.2.3 Installation de Cisco ASDM 45
4.2.4 Configuration ASDM du tunnel VPN 47
4.2.5 Configuration SDM du routeur 50
4.2.6 Configuration de la VoIP passant par le firewall ASA . 51
Conclusion 52

Conclusion Générale **53**

Bibliographie **54**

LISTE DES FIGURES

1.1 Arechetecture client/serveur. 5
1.2 Architecture d'égal à égal ou poste à poste. 6
1.3 Représentation d'une topologie en bus. [6] 7
1.4 Représentation d'une topologie en étoile. 7
1.5 Représentation d'une topologie en anneau. 8
1.6 Réseau cellulaire [7] 9
1.7 Réseau mesh [7] 10
1.8 Réseau Ad-hoc [7] 10
1.9 Architecture de réseau de mobile [11] 12

2.1 La technique de transfert de paquets [10] 16
2.2 La technique de transfert de paquets [10] 16
2.3 Un flot de paquets téléphoniques [10] 17
2.4 La commutation de circuits [4] 17
2.5 La technique de transfert de paquets 18
2.6 La téléphonie IP de bout en bout [3] 21

3.1 Communication entre deux terminaux H.323 [3] 23
3.2 Exemple d'établissement d'une session SIP entre deux User Agents. [15] 23
3.3 La transmission des flux média avec RTP.[18] 28
3.4 La transmission des flux média avec RTP.[18] 29
3.5 L'interruption 30
3.6 L'interception 30
3.7 La modification 31
3.8 La fabrication 31
3.9 IP Spoofing[18] 32

3.10 Les étapes du hacking[18] 33
3.11 Un pare-feu[18] 34
3.12 Le tunnel VPN[18] 35

4.1 La topologie du réseau réalises. 41
4.2 Appel entre deux softphone Cisco IP Communicator. 44
4.3 Le réseau interne(inside). 45
4.4 Les commandes a exécuté pour avoir l'interface Cisco ASDM. 45
4.5 Le serveur TFTP 45
4.6 L'interface de téléchargement Cisco ASDM. 46
4.7 Cisco ASDM. 46
4.8 Cisco ASDM pour ASA. 47
4.9 Site-to-site VPN Wizards. 47
4.10 Identification d'interface homologue. 48
4.11 Trafic a sécurise. 48
4.12 Les algorithme de chiffrement. 49
4.13 Translation NAT. 49
4.14 VPN Wizards final. 50
4.15 La topologie de réseau VoIP avec firewall 51
4.16 Les messages sur l'interface Cisco ASDM. 52
4.17 Le protocole h323 sur l'interface Cisco ASDM. 52

LISTE DES ABRÉVIATION

ADSL Asymmetric Digital Subscriber Line

AP Access Point

ASA Adaptive Security Appliance

ASAv Adaptive Security Appliance Vertuel

ASDM Adaptive Security Device Manager

AMPS Advanced Mobile Phone System

BSC Base Station Controller

DHCP Dynamic Host Configuration Protocol

EDGE Enhanced Data rates for Global Evolution

FAI Fournisseur d'accès à Internet

FDMA Frequency Division Multiple Access

GNS3 Graphical Network Simulator

GPRS General Packet Radio Service

GSM uses Gaussian Minimum

H-IDS Host Based Intrusion Detection system

HLR Home Location Register

IEEE Institute of Electronic and Electronics Engineers

IETF Internet Engineering Task Force

IMT Integrated Media Technologies

IP Internet Protocol

IPX Internetwork Packet Exchange

ISDN Integrated Services Digital Network

ITU International Télécommunication Union

IDS système de détection d'intrusion

LAN Local Area Network

MGCP Media Gateway Control Protocol

MAC Media Access Control

MAN Metropolitan Area Network

NMT Nordic Mobile Telephone

N-IDS Network Based Intrusion Detection system

PAN Personal Area Network

QoS Qualité de service

RNIS Réseau Numérique à Intégration de Services

RR Receiver Report

RTCP Real-time Control Transport Protocol

RTP Real-time Transport Protocol

SDES Source Description

SDM Security Device Manager

SIP Session Initiation Protocol

SR Sender Report

TACS Total Access Communications System

TCP transport de données multim édias temps réel

ToIP Telephony over Internet Protocol

UAC User Agent Client

UAS User Agent Server

UDP User Datagram Protoco

UMTS Universal Mobile Telecommunications System

VLR Visitor Location Register

VoIP Voice over Internet Protocol

VPN Virtual Private Network

WAN World Area Network

WIFI Wireless Fidelity

WIMAX Worldwide Interoperability for Microwave Access

WLAN Wireless Local Area Network

1G Première Génération

2G Deuxième Génération

3G Troisième Génération

4G Quatrième Génération

5G Cinquième Génération

INTRODUCTION GÉNÉRALE

Pour faire fonctionner un téléphone,il doit être relier par un fil jusqu'aux centraux téléphonique.Aujourd'hui le téléphone fait partie intégrante de notre vie quotidienne de tout les jours.
La ToIP ou la téléphonie IP n'utilise plus cet indispensable fil mais plutôt une connexion internet et les réseaux informatiques pour remplacer les centraux et connecter les téléphones entre eux.Depuis quelques années, la technologie VoIP commence à intéresser les entreprises, La migration des entreprises vers ce genre de technologie n'est pas pour rien. Le but est principalement de minimiser le coût des communications , utiliser le même réseau pour offrir des services de données, de voix, et d'images , et simplifier les coûts de configuration et d'assistance.

Plusieurs fournisseurs offrent certaines solutions qui permettent une migration vers le monde IP,tels que Cisco et Asterisk qui ont développé des PABXs software.

L'entreprise a toutes les chances de se retrouver avec un réseau de VoIP qui fonctionne correctement, mais est ouvert à tous et à tout Les risques,Cette solution, qui est totalement basée sur la technologie IP, est donc affectée par les vulnérabilités qui menacent la sécurité de ce protocole et l'infrastructure réseau sur laquelle elle est déployée. Cette dernière est le majeur problème pour les entreprises et un grand défi pour les développeurs. Certaines attaques sur les réseaux VoIP, comme les attaques de déni de service, et les vols d'identité, peuvent causer des pertes catastrophiques et énormes pour les entreprises. Pour cela la sécurité du réseau VoIP est une obligation, avec laquelle on peut minimiser, le risque d'attaques sur les réseaux VoIP.

Cisco propose d'ajouter des équipements de type ASA (« Adaptive Security Appliance »). En ce qui concerne la fonction de pare-feu hébergée par l'ASA , elle supporte l'inspection des protocoles de signalisation tels que SIP, H.323 et MGCP, l'écoulement du trafic inspecté sans ralentissement,et la qualité de service (QoS).

Ce travail a pour objectif : l'étude des protocoles de VoIP et des architectures proposées , l'étude des vulnérabilités et des attaques de sécurités des divers composants d'une infrastructure VoIP dans des réseaux , et la mise en place une solution de VoIP sécurisée basée sur des outils Cisco , précisément le firewall ASAv, les routeur Cisco,et le client Cisco IP Communicator.

Ce mémoire se compose de quatre chapitres :
Le premier chapitre "Généralité sur les réseaux",définit quelque généralité et notions de base essentielles sur les réseaux informatiques, et les générations du réseau .
Le deuxième chapitre s'intéresse au théorie de la ToIP. Il détaille les différents étapes de déroulement d'une communication téléphonique,et la problématique de base de la téléphonie internet.
Le troisième chapitre, s'intéresse aux vulnérabilités des systèmes sur un environnement VoIP et les techniques de sécurité .
Le dernier chapitre du rapport s'intéresse au réalisation du réseau VoIP sur GNS3 et l'implémentation d'un firewall ASAv pour filtrer le trafic de ce réseau. Nous terminons par une conclusion et une bibliographie.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX

Introduction

L'informatique est un domaine très vaste on constate une évolution de plus en plus présente au fils des années, chez les particuliers comme chez les entreprises. Pour qu'une entreprise soit plus coordonnée elle a essentiellement besoin d'un réseau locale. Dans ce chapitre nous allons définir quelques notions de base telle que les réseaux informatique, et les générations de réseau .

1.1 Réseau informatique

1.1.1 Définition

Un réseau informatique ou un réseau de télécommunication est l'ensemble des machines inter-connectés qui délivrent des information comme les serveur ou bien qui reçoivent ou émettent des informations , telles que les ordinateurs ,les terminaux bureautiques et les terminaux téléphoniques...etc.
«Un réseau peut également être constitué d'un ensemble de réseaux interconnecté, comme c'est le cas d'Internet.» [8]

Selon Guy Pujolle , un réseau informatique : « désigne tout ensemble d'éléments capables de véhiculer l'information d'une source vers une destination. Le téléphone en est la meilleure illustration » [3]

1.1.2 Topologie des réseaux informatique

Les réseaux informatiques sont classés suivant leur portée :
• **Réseaux personnel PAN (Personal Area Network) :**
Relie des appareils personnels, il couvre une zone de quelque mètres.
• **Réseau local LAN (Local Area Network) :**
Relie les ordinateurs ou postes téléphoniques situés dans la même pièce ou dans le même bâtiment, il couvre de quelques dizaines de mètres, à centaines de mètres.
• **Réseau métropolitain MAN (Metropolitan Area Network) :**
Est un réseau à échelle d'une ville
• **Réseau étendu WAN (World Area Network) :**
Réseau à grand échelle qui relie plusieurs sites ou des noeuds du monde entier.

Les réseaux informatiques peuvent être classé selon le type de lien en : réseaux filaires et réseaux sans fil[1].

1.2 Réseau filaire

1.2.1 Définition

Le réseau filaire est un réseau qui comme son nom l'indique est un réseau que l'on utilise grâce à une connexion avec fil. Ce réseau utilise des câbles Ethernet pour relier des ordinateurs et des périphériques grâce à un routeur ou à un commutateur.[18]

1.2.2 Les architectures des réseaux filaires

On distingue généralement deux grands types bien différents, ayant tout de même des similitudes :

L'architecture client / serveur : De nombreuses applications fonctionnent selon un environnent client / serveur, cela signifie que les machines clientes (des machines faisant parties du réseau) contactent un serveur, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion. la figure suivante présente un exemple d'architecture client-serveur : deux clients font leurs requêtes à un serveur via Internet. (Figure 1).

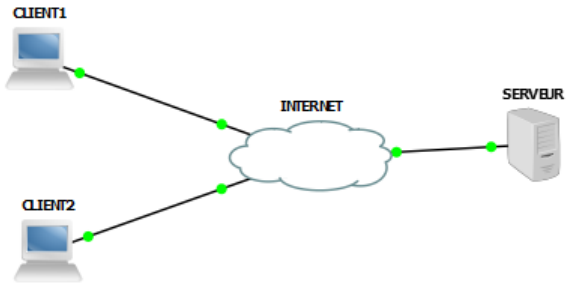

FIGURE 1.1 – Arechetecture client/serveur.

L'architecture d'égal à égal ou poste à poste : Dans une architecture poste à poste, contrairement à une architecture de réseau de type client / serveur, il n'y a pas de serveur dédié. Chaque ordinateur est à la fois, client et serveur (Figure 2).

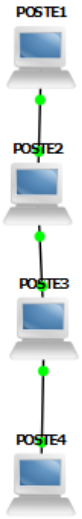

FIGURE 1.2 – Architecture d'égal à égal ou poste à poste.

1.2.3 Les topologies des réseaux filaires

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à du matériel (câblage, cartes réseau), ainsi que d'autres équipements permettant d'assurer la bonne circulation des données. L'arrangement physique de ces éléments est appelé topologie physique.
Il en existe trois principales topologie physique :

La topologie en BUS : Dans une topologie en Bus, tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau. La figure 3 indique ce type de topologie.

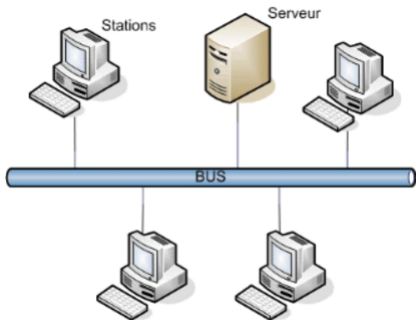

FIGURE 1.3 – Représentation d'une topologie en bus. [6]

La topologie en ETOILE : Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel appelé hub ou concentrateur. Il s'agit d'une boite comprenant un certain nombre de jonctions auxquelles on peut connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions (figure 4).

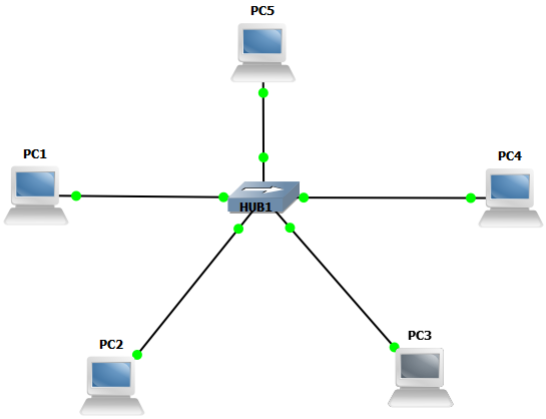

FIGURE 1.4 – Représentation d'une topologie en étoile.

La topologie en ANNEAU : Dans une topologie en anneau, les ordinateurs communiquent, chacun à son tour c'est à dire de manière sporadique.

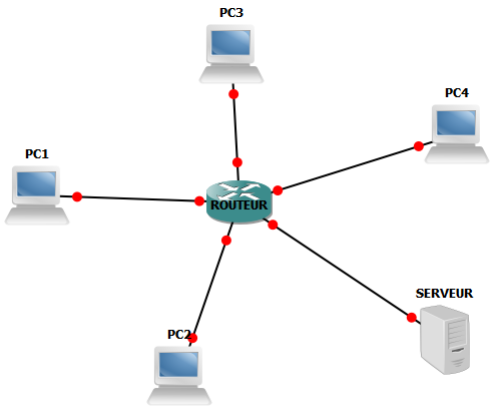

FIGURE 1.5 – Représentation d'une topologie en anneau.

1.3 Réseau sans fils

1.3.1 Définition

Un réseau sans fil est un réseau informatique , composé d'un ensemble d'appareils connectés entre eux et qui peuvent s'envoyer et recevoir des données sans qu'aucune connexion « filaire » physique reliant ces différents composants entre eux ne soit nécessaire. C'est les ondes radio qui reliées les différents nœuds entre eux. Le rayonnement géographique des ondes est relativement limité et de faible puissance d'émission. Pour cette raison, les réseaux sans fil se sont avant tout développés comme réseaux internes, propre à un bâtiment, soit comme réseau d'entreprise, soit comme réseau domestique. Néanmoins, des projets de réalisation de réseaux à grande échelle ont vu le jour, notamment le WiMAX. La norme la plus utilisé actuellement pour les réseaux sans fil est la norme IEEE802.11, mieux connue sous le nom de Wi-Fi.[8]

1.3.2 Architecture des réseaux sans fil

1.3.2.1 Le réseau cellulaire

Un tel réseau, dit aussi réseau d'infrastructure, s'appuie sur une infrastructure filaire à laquelle sont raccordés des points d'accès (ou Access Point AP) qui rayonnent chacun sur une zone tridimensionnelle donnée nommée cellule. Les équipements terminaux du réseau (ordinateurs, téléphones...) se raccordent par radio à un point d'accès à portée.
Un terminal peut être à portée de radio de plusieurs points d'accès. Il choisit alors celui pour lequel il reçoit le niveau de signal radio le plus élevé.
Cette architecture est typique du WLAN, seul ou en complément d'un LAN dont les points d'accès radio utilisent l'infrastructure.

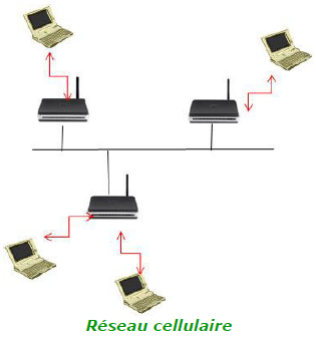

FIGURE 1.6 – Réseau cellulaire [7]

1.3.2.2 Le réseau mesh

Il ressemble beaucoup au réseau précédent, mais ici, les points d'accès sont reliés par radio entre eux au lieu d'être raccordés sur une infrastructure filaire.

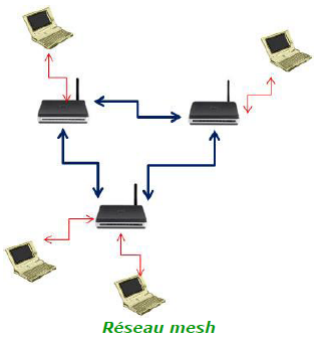

FIGURE 1.7 – Réseau mesh [7]

1.3.2.3 Le réseau Ad-hoc

Il s'agit d'un réseau entièrement radio et sans infrastructure. Toutes les machines du réseau sont reliées à toutes les autres qui sont à portée radio. Chaque machine est donc à la fois point d'accès et terminal.

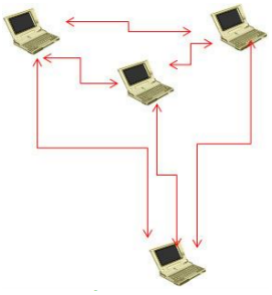

FIGURE 1.8 – Réseau Ad-hoc [7]

1.4 Réseau mobile

1.4.1 Présentation

Le réseau de mobile est un réseau qui offre à des utilisateurs munis d'une unité mobile (téléphone mobile, PDA,...), la possibilité d'accéder à des services et à des applications évoluées, à travers une infrastructure sans fil, indépendamment de la localisation physique ou du mouvement de ces utilisateurs.[11] Le réseau de mobiles est basé sur la technologie du réseau cellulaire (mode infrastructure) dont le principe est fondé sur la division d'une région sur le terrain en plusieurs cellules.[14] Les réseaux cellulaires sont des systèmes de communication sans fil qui reposent sur une infrastructure fixe. Les terminaux qui évoluent au sein de ces réseaux doivent obligatoirement s'adresser à cette infrastructure (point d'accès) pour pouvoir accéder aux services qu'ils demandent.

1.4.2 Architecture de réseau de mobile

Puisque le réseau de mobile est basé sur la technologie de réseau cellulaire, dans un réseau de mobile, le territoire couvert, ou la zone de couverture, est généralement découpé en petites surfaces géographiquement limitées et communément appelées cellules. Elles sont représentées par des hexagones dont le rayon varie de quelques centaines de mètre à quelques kilomètres. Les cellules se chevauchent partiellement entre elles de manière à assurer une couverture plus complète du territoire.[14] Une infrastructure de réseau de mobile typique consiste en un certain nombre de composants : les cartes à puces, les unités mobiles, les stations de bases, les centres de commutation des services mobiles (Mobile Switching Centre), satellite, les enregistreurs de localisation nominal et les enregistreurs de localisation des visiteurs.[11]

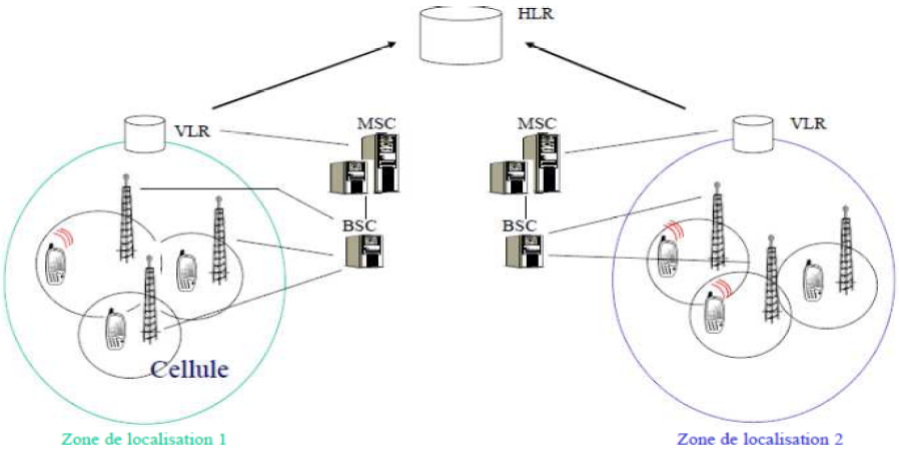

FIGURE 1.9 – Architecture de réseau de mobile [11]

1.5 Générations des réseaux de mobiles

Le terme génération sert à désigner les améliorations incrémentales survenues au cours de l'évolution des réseaux de mobiles.

1.5.1 Première génération (1G)

La première génération de systèmes cellulaires (1G) reposait sur un système de communications mobiles analogiques. Cette génération a bénéficié de deux inventions techniques majeures des années 1970 : le microprocesseur et le transport numérique des données entre les téléphones mobiles et la station de base. Les appareils utilisés étaient particulièrement volumineux. La première génération de systèmes cellulaires (1G) utilisait essentiellement les standards suivants :

AMPS (Advanced Mobile Phone System) : Lancé aux Etats-Unis, est un réseau analogique reposant sur la technologie FDMA (Frequency Division Multiple Access).

NMT (Nordic Mobile Telephone) : A été essentiellement conçu dans les pays nordiques et utilisés dans d'autres parties de la planète.

TACS (Total Access Communications System) : Qui repose sur la technologie AMPS, a été fortement utilisé en Grande Bretagne.[20]

Les systèmes 1G présentent beaucoup de point faibles, leur plus grande faiblesse demeure leur capacité limitée, qui a rendu opportune l'introduction d'une technologie de deuxième génération. On observe aussi des limitations de mobilité, particulièrement entre réseaux de fournisseurs différents, l'absence de mécanismes de sécurité contre la fraude et la perte potentielle d'utilisateurs mobiles que le réseau n'est pas capable de retracer.[13]

1.5.2 Deuxième génération (2G)

La deuxième génération (2G) de systèmes cellulaires repose sur une technologie numérique a été développée à la fin des années 1980. Ces systèmes cellulaires utilisent une technologie numérique pour la liaison ainsi que pour le signal vocal. Ce système apporte une meilleure qualité ainsi qu'une plus grande capacité à moindre coût pour l'utilisateur. La deuxième génération de systèmes cellulaires (2G) utilise essentiellement les standards suivants :

GSM (2G) : Système cellulaire numérique de communication avec des mobiles ou entre mobiles, destiné principalement aux communications téléphoniques.

GPRS : Service de communication de données par paquets fourni sur un réseau GSM.

EDGE : est un standard de mobiles de 3ème génération. EDGE est une évolution des normes de téléphonie mobile GPRS pour GSM qui permet à un accès à l'Internet à partir d'un téléphone mobile ou d'un microordinateur. EDGE permet des transferts de données avec un débit maximal de 384 kbit/s.

1.5.3 Troisième génération (3G)

La troisième génération (3G) de systèmes cellulaires est une génération de systèmes mobiles labellisé IMT 2000 par l'UIT. Ce système permet des services de communications plus rapides notamment pour la voix, la télécopie, l'Internet de n'importe quel endroit et à tout moment. L'UIT IMT-2000 est la norme internationale de la 3G a ouvert la voie à de nouvelles applications et services comme par exemple le divertissement multimédia, la localisation des services, La troisième génération de systèmes cellulaires (3G) utilise notamment les standards suivants :

UMTS (Universal Mobile Telecommunications System) : Système cellulaire numérique de communication avec des mobiles ou entre mobiles, destiné à offrir une large gamme de services de voix, de données et d'images, ainsi que l'accès à l'Internet.

1.5.4 Quatrième génération (4G)

La quatrième génération de systèmes cellulaires (4G) utilise notamment les standards suivants :

WIMAX (Worldwide Interoperability for Microwave Access) : Est une technologie permettant des connexions sans-fil à haut-débit sur des zones de couverture de plusieurs kilomètres. Le WIMAX est une des alternatives de couverture pour l'Internet haut-débit de zones difficiles à couvrir par l'ADSL.

Conclusion

Pour conclure ce chapitre, nous avons parlée sur les généralité des réseaux informatique, tells que les réseaux filaires,les réseaux sans fils et les réseaux mobils, où on a parlée sur les génération des réseaux ,et dans le chapitre qui suit nous parlerons sur la théorie de la ToIP.

CHAPITRE 2

LA TÉLÉPHONIE PAR PAQUET

Introduction

Déférents termes pour la ToIP ou la téléphonie sur internet .Aujourd'hui les utilisateurs comme les professionnelles disent que la ToIP par rapport à la téléphonie classique c'est une révolution.Certaine la comparent a la révolution au moment que on a passé de télégraphe à la téléphonie classique. Nous donnerons au cours des sections qui suivent quelques notions du téléphonie sur IP.

2.1 Quelques définitions

2.1.1 la voix sur IP

VoIP signifie Voice over Internet Protocol ou Voix sur IP. Comme son nom l'indique, la VoIP permet de transmettre des sons (en particulier la voix) dans des paquets IP circulant sur Internet. La VoIP peut utiliser du matériel d'accélération pour réaliser ce but et peut aussi être utilisée en environnement de PC.[12]

2.1.2 La téléphonie sur IP

En anglais, Telephony over IP, est un service de téléphonie offert sur un réseau de télécommunications, public ou privé, utilisant principalement le protocole de réseau IP, ainsi que toutes les technologies liées à la voix sur IP.

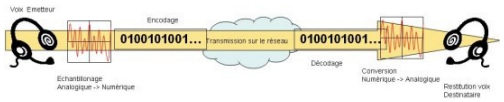

FIGURE 2.1 – La technique de transfert de paquets [10]

2.2 La téléphonie par circuit et par paquets

Dans la communication à transfert de paquets,chaque message est découpé en morceaux (fragmentation), a chaque morceau on ajoute un entête qui comporte les informations de contrôle utilisées d'une extrémité du réseau à une autre . Cette technique est illustrée à la figure 2.1.

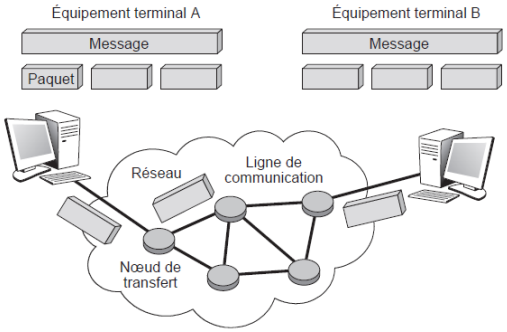

FIGURE 2.2 – La technique de transfert de paquets [10]

• La téléphonie par paquet :
Dans la parole téléphonique, l'information est regroupée pour être placée dans un paquet, comme illustré à la figure 2.2. Le combiné téléphonique produit des octets, provenant de la numérisation de la parole, c'est-à-dire le passage d'un signal analogique à un signal sous forme de 0 et de 1, qui remplissent petit à petit le paquet. Dès que celui-ci est plein, il est émis vers le destinataire. Une fois le paquet arrivé à la station terminale, le processus inverse s'effectue, restituant les éléments binaires régulièrement à partir du paquet pour reconstituer la parole téléphonique.[10]

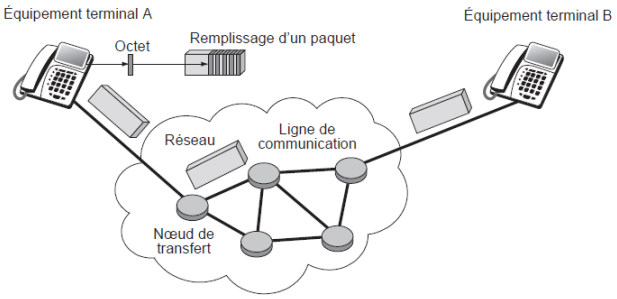

FIGURE 2.3 – Un flot de paquets téléphoniques [10]

• **La commutation de circuits :**
Pour chaque communication téléphonique un (ou plusieurs) circuit est établi entre les extrémités .[4]

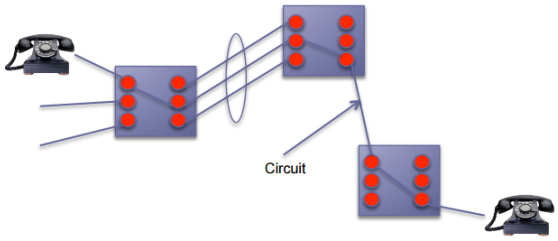

FIGURE 2.4 – La commutation de circuits [4]

2.3 Comparaison entre la téléphonie par paquet et par circuit

Elles présentent toutes les deux les mêmes contraintes temporelles (le temps de transit doit être limité pour offrir une interactivité entre les individus). Dans une communication par circuit (RNIS, ISDN), les ressources physiques étant réservées, la voix est toujours dégagée sur le circuit et les ressources servent aux signaux transmis entre l'émetteur et le récepteur. Dans un transfert de paquets, aucune ressource n'étant réservée, il sera donc impossible de connaître précisément le temps d'attente des paquets dans les noeuds de transfert. (Analogique, Numérique, SIP, IP).[19]

2.4 Les étapes de déroulement d'une communication téléphonique sur IP

Le déroulement d'une communication téléphonique sur IP parcourt les cinq grandes étapes suivantes :

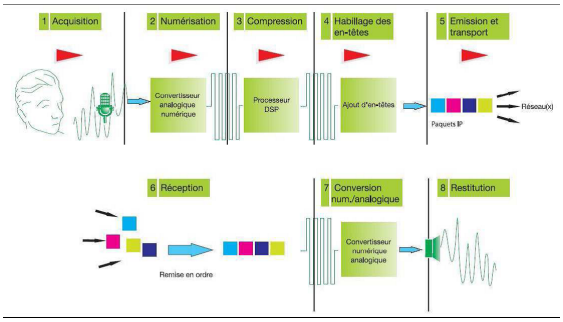

FIGURE 2.5 – La technique de transfert de paquets

2.4.1 Mise en place la communication

La session Une signalisation qui se démarre la première,qui s'effectue par une conversion de l'adresse IP du destinataire en une adresse IP d'une machine qui puisse joindre le destinataire . Le récepteur peut être un combiné téléphonique classique sur un réseau d'opérateur télécoms ou une station de travail . Le protocole DHCP et les passerelles spécialisées (gatekeeper) sont employés à cette fin.[10]

2.4.2 Établissement de la communication

Cela passe par une acceptation du terminal destinataire, que ce dernier soit un téléphone, une boîte vocale ou un serveur Web. Plusieurs protocoles de signalisation sont utilisés pour cela, en particulier le protocole SIP (Session Initiation Protocol) qui sera présenté dans le chapitre suivant. Comme son nom l'indique, SIP est utilisé pour initialiser la session. Le serveur gère la demande et fournit une réponse au client. Trois types de serveurs gèrent différents éléments : un serveur d'enregistrement, un serveur Proxy et un serveur de redirection. Ces serveurs travaillent à trouver la route : le serveur proxy détermine le prochain serveur , qui à son tour, trouve le suivant, et ainsi de suite.

2.4.3 Transport de l'information téléphonique

Le protocole RTP (Real-time Transport Protocol) prend le relais pour transporter l'information téléphonique proprement dite. Son rôle est d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie de façon à reformer le flot avec ses caractéristiques de départ (vérification du synchronisme, des pertes, etc.). C'est un protocole de niveau transport, qui essaye de corriger les défauts apportés par le réseau.[10]

2.4.4 Changement de réseau

Un autre lieu de transit important de la ToIP est constitué par les passerelles, qui permettent de passer d'un réseau à transfert de paquets à un réseau à commutation de circuits, en prenant en charge les problèmes d'adressage, de signalisation et de transcodage que cela pose. Ces passerelles ne cessent de se multiplier entre FAI et opérateurs télécoms.[10]

2.4.5 Arrivée au destinataire

De nouveau, le protocole SIP envoie une requête à la passerelle pour déterminer si elle est capable de réaliser la liaison circuit de façon à atteindre le destinataire. En théorie, chaque passerelle peut appeler n'importe quel numéro de téléphone. Cependant, pour réduire les coûts, mieux vaut choisir une passerelle locale, qui garantit que la partie du transport sur le réseau téléphonique classique est le moins cher possible.[10]

2.5 Avantages de la ToIP

Plusieurs raisons expliquent le succès de la téléphonie par paquet, et plus spécifiquement de la téléphonie sur IP :
Convergence de support de communication : Un seul réseau à maintenir
Flexibilité dans le dimensionnement : Plus besoin de la loi d'Erlang ou presque
Intégration dans le système d'information : Annuaires,Messagerie,Web, Réseaux sociaux
Réduction des coûts : Grâce à l'intégration de la téléphonie parmi de nombreuses autres applications, le coût du transport devient pratiquement nul.

2.6 La problématique de base de la téléphonie

La voix sur IP adresse deux types d'applications : celles qui, comme la téléphonie, mettent en jeu une interaction humaine, laquelle implique un temps de transit très court, et celles qui transportent des paroles unidirectionnelles, qui n'exigent pas de temps réel. La difficulté de la Téléphonie par paquet réside dans la très forte contrainte temporelle due à l'interaction entre individus. Si on veut garder une bonne qualité de la conversation, la latence ne doit pas dépasser 150ms. Une autre difficulté est l'écho qui est un signal qui rencontre des obstacles tel que le combiné téléphonique. L'écho qui repart en sens inverse est numérisé par un codec et traverse sans problème un réseau numérique. Une caractéristique de la téléphonie provient du besoin d'avertir par une sonnerie la personne appelée. La communication téléphonique est décomposée en trois phases :

- une première permettant d'avertir le destinataire.
- une seconde correspondant au transport de la parole proprement dite.
- et une troisième qui consiste à la finalisation de la communication lorsque l'un des deux terminaux raccroche.

La première et la dernière utilise un protocole de Signalisation.[5]

2.7 La dernière solution ToIP

La dernière solution proposé est la cinquième génération du processus aboutit à de la téléphonie IP de bout en bout. La paquétisation est repoussée dans l'équipement terminal de l'utilisateur. Le téléphone devient un téléphone IP. La figure 2.5 illustre cette solution. Le téléphone IP n'est pas connecté directement sur la boucle locale de l'opérateur mais sur le réseau d'entreprise, lui-même connecté à l'opérateur. Le téléphone IP fait en réalité office de routeur. Il intègre en outre un codec et assure la paquétisation IP et l'encapsulation des paquets IP dans une trame Ethernet. La trame Ethernet est ensuite transmise sur le réseau d'entreprise.

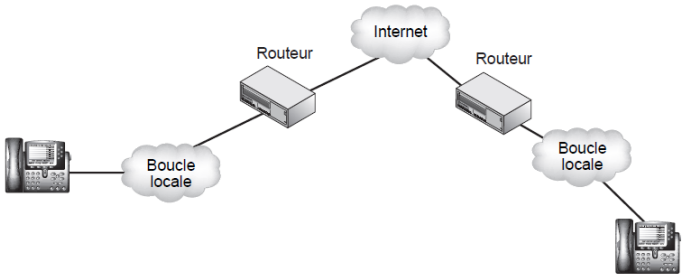

FIGURE 2.6 – La téléphonie IP de bout en bout [3]

Conclusion

Dans ce chapitre, nous avons présenté les notions de base du ToIP, tells que le type de commutation dans la ToIP,et nous avons parlé aussi sur les problématique de base de la ToIP,et sur la dernière solution proposer.Dans le chapitre suivant nous parlerons sur les vulnérabilité d'environnement VoIP.

CHAPITRE 3

VULNÉRABILITÉ DES SYSTÈMES SUR UN ENVIRONNEMENT VOIP ET LES TECHNIQUES DE SÉCURITÉ

Introduction

La technologie VoIP est une technologie très importante dans les entreprises,elle est facile à installer et à configurer ,et elle n'est pas très couteuse.Mais l'inconvénient de cette technologie est la facilité d'écouter l'appel par n'importe qui.

3.1 Protocole de signalisation H.323

Le protocole H.323 est un protocole dérivé du protocole H.320 utilise RNIS,c'est un standard fournissant une base pour la communication,utilisant de l'audio, de la vidéo et des données à travers les réseaux IP. H.323 est un protocole de signalisation développé par l'ITU(International Télécommunication Union), qui permet de garantir un contrôle sur l'utilisation des ressources réseaux et des contriantes de qualité de service tels qu'IP IPX sur Ethernet,Fastethernet et Token Ring. le transport des flux audio et video s'appuie sur le protocole RTCP,RTP.
La figure 3.1 illustre des terminaux peuvent parfaitement communiquer entre eux en utilisant le protocole H.323 et sans l'intervention d'autres éléments architecturaux.

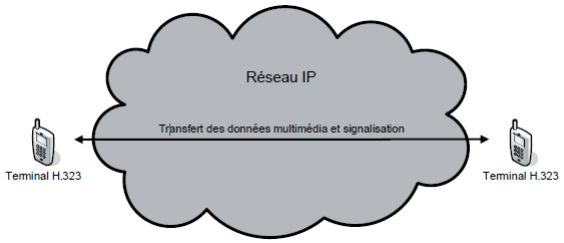

FIGURE 3.1 – Communication entre deux terminaux H.323 [3]

3.2 Protocole de signalisation SIP

Session Initiation Protocol (dont le sigle est SIP) est un protocole récent (1999), normalisé et standardisé par l'IETF qui a été conçu pour établir, modifier et terminer des sessions multimédia,Son rôle est d'ouvrir, modifier et libérer les sessions ou appels ouverts entre un ou plusieurs utilisateurs. L'ouverture de ces sessions permet de réaliser de l'audio ou vidéo-conférence, de l'enseignement à distance, de la voix (téléphonie) et de la diffusion multimédia sur IP essentiellement,comme il se charge de l'authentification. SIP n'est pas un protocole de réservation de ressource, il ne peut donc pas assurer la QoS. Il s'agit d'un protocole de contrôle d'appel et non de contrôle du média.

La figure suivante présente l'envoie des requêtes SIP par les User Agent Client,et les User Agent Server (UAS) les reçoit. Le principal objectif de SIP est de permettre l'établissement de sessions entre User Agents.

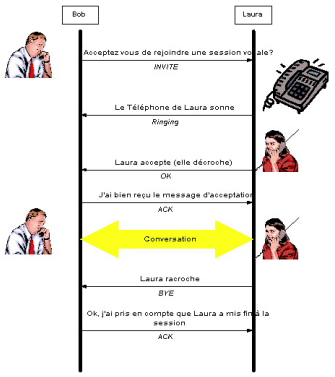

FIGURE 3.2 – Exemple d'établissement d'une session SIP entre deux User Agents. [15]

Il existe deux principales classes des vulnérabilités sur un environnement VoIP. La première dépend des protocoles utilisés (SIP, H.323...) et la deuxième est liée aux systèmes sur lesquels les éléments VoIP sont implémentés. Chaque protocole ou service a ses propres attaques.

3.3 Vulnérabilité des protocoles

Un appel téléphonique VoIP est constitué de deux parties : la signalisation, et le transporte du voix.

La signalisation, en particulier SIP, transmet les entêtes et la charge utile 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, et à l'écoute clandestine qui recherche des informations sur un compte utilisateur valide, pour passer des appels gratuits par exemple.

La signalisation utilise, en général, le port par défaut UDP/TCP 5060. Le firewall doit être capable d'inspecter les paquets de signalisation et d'ouvrir ce port afin de leurs autoriser l'accès au réseau. Un firewall qui n'est pas compatible aux protocoles de la VoIP doit être configuré manuellement pour laisser le port 5060 ouvert, créant un trou pour des attaques contre les éléments qui écoutent l'activité sur ce port.

Le protocole RTP utilisé pour le transport des flux multimédia, présente également plusieurs vulnérabilités dues à l'absence d'authentification et de chiffrement. Chaque entête d'un paquet RTP contient un numéro de séquence qui permet au destinataire de reconstituer les paquets de la voix dans l'ordre approprié. Cependant, un attaquant peut facilement injecter des paquets artificiels avec un numéro de séquence plus élevé. En conséquence, ces paquets seront diffusés à la place des vrais paquets.

Généralement, les flux multimédias contournent les serveurs proxy et circulent directement entre les points finaux. Les menaces habituelles conte le flux de la voix sont l'interruption de transport et l'écoute clandestine.

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 session (TCP) (session Hijacking) et la mystification (UDP) (Spoofing), etc.

3.4 Vulnérabilité sur l'infrastructure

Une infrastructure VoIP est composée de téléphones IP, Gateway, serveurs (proxy, register, etc.). Chaque élément, que ce soit un système embarqué ou un serveur standard tournant sur un système d'exploitation, est accessible via le réseau comme n'importe quel ordinateur.
Chacun comporte un processeur qui exécute des logiciels qui peuvent être attaqués ou employés en tant que points de lancement d'une attaque plus profonde.

3.4.1 Infrastructure Hardware

Téléphone IP

Généralement un attaquant obtient les privilèges qui lui permettent de commander complètement la fonctionnalité du dispositif,soit un téléphone IP, un Softphone, 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 softphones sont plus susceptibles aux attaques, ils sont plus susceptibles aux vulnérabilité du system d'exploitation et vulnérabilité de l'application, et vulnérabilité du services, des virus.etc.

Le serveur VoIP

Un autre élément du réseau vulnérable est le serveur fournisseur du réseau de téléphonie sur IP, qui est peut être la cible d'attaques pour mettre en péril tout le réseau.
Si un serveur de signalisation est compromis un attaquant peut contrôler totalement l'information de signalisation pour différents appels ce qui permettra à un attaquant de changer n'importe quel paramètre relatif à l'appel.
Pour finir, il faut préciser qu'un serveur de téléphonie IP est installé sur un système d'exploitation, il peut donc être une cible pour les virus, les vers, ou n'importe quel code malveillant.[2]

3.4.2 Infrastructure Software

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 téléphonies IP, Call Managers, Gateway 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.[2]

3.5 Qualité de service

Pour le transport de la parole téléphonique, il faut que le temps de transport de bout en bout soit limité puisque nous avons affaire à une application avec interaction humaine. Cette limitation est d'une centaine de millisecondes pour obtenir une très bonne qualité et jusqu'à 300 ms pour une conversation passant par un satellite géostationnaire.
Dans cette section nous expliquerons pourquoi les protocoles de transport TCP et UDP sont peu qualifiés pour assurer la qualité de service demandée dans la ToIP ,et nous nous parlerons sur RTP/RTCP.

3.5.1 Protocole TCP et le transport de données multimédias temps réel

Le protocole TCP exige de nombreuses procédures de contrôle, Contrôle de séquence,Contrôle de flux,Contrôle d'erreur, Contrôle de congestion. Toutes ces fonctionnalités assurent un service de transport fiable,mais ce n'est pas la fiabilité qui est l'élément le plus important dans les communications temps réel, mais le temps,ce qui rendent le protocole TCP peu adapté au transport de flux de ToIP avec de fortes contraintes de délai.

3.5.2 Protocole UDP et le transport de données multimédias temps réel

Le protocole UDP ne comporte que des fonctionnalités de transport pur, sans aucun mécanisme de contrôle. L'adressage des données avec les ports de communication utilisés est sa seule fonction fondamentale. UDP est ainsi notablement plus rapide que ne l'est TCP.
Mais la simplicité de ce modèle devient rapidement limitative. En particulier, UDP ne dispose d'aucun mécanisme lui permettant de reconstituer l'ordre des flux auprès du récepteur. Les datagrammes UDP sont totalement épurés, et aucune estampille d'horodatage,ni de numérotation n'y est insérée. Or, dans un réseau IP, les paquets peuvent emprunter des chemins différents. Avec le seul protocole UDP, la séquence temporelle originale ne peut être reconstituée au récepteur.[3]

3.5.3 Les protocoles RTP et RTCP

le couple de protocoles RTP/RTCP a été conçu dans le but d'enrichir les fonctions d'UDP et de fournir à ce dernier ce dont il a besoin pour gérer efficacement les données multimédias temps réel.

RTP (Real-time Transport Protocol) :
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.). RTP permet :
• d'identifier le type de l'information transportée.
• d'ajouter des marqueurs temporels permettant d'indiquer l'instant d'émission du paquet. L'application destinataire peut alors synchroniser les flux et mesurer les délais et la gigue.

• d'inclure des numéros de séquence à l'information transportée afin de détecter l'occurrence de paquets perdus et de délivrer les paquets en séquence à l'application destinataire. De plus, RTP peut être véhiculé par des paquets multicast afin d'acheminer des conversations vers des destinataires multiples. Mais, RTP n'a pas été conçu pour effectuer des réservations de ressources ou contrôler la qualité de service et ne garantit pas la livraison du paquet à l'arrivée.la figure 3.3 illustre la transmission des flux média avec RTP.

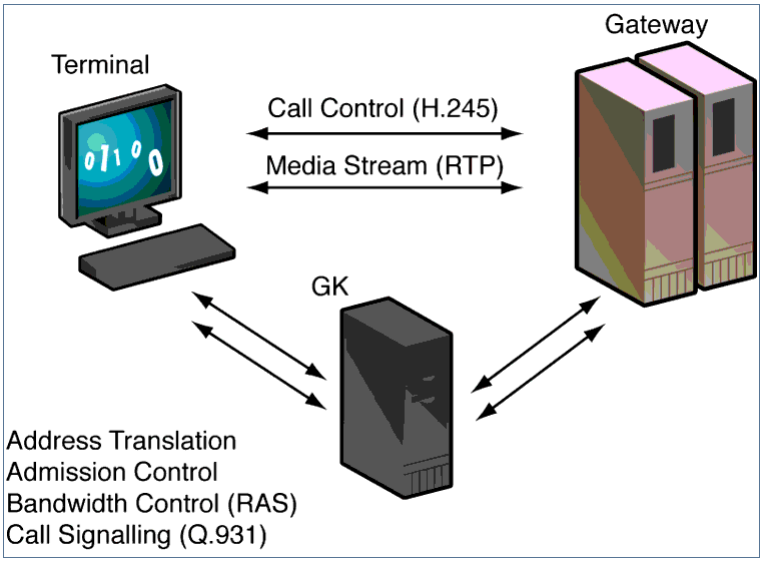

FIGURE 3.3 – La transmission des flux média avec RTP.[18]

RTCP(Real-time Control Transport Protocol) :
Le protocole RTCP est basé sur des transmissions périodiques de paquets de contrôle par tous les participants dans la session. C'est un protocole de contrôle des flux RTP, permettant de véhiculer des informations basiques sur les participants d'une session, et sur la qualité de service. Il existe cinq types différents de paquets RTCP pour chaque type d'information :

- SR (Sender Report) contient des statistiques de transmission et de réception pour les participants qui sont des émetteurs actifs.
- RR (Receiver Report) contient des statistiques de réception pour les participants qui ne sont pas des émetteurs actifs mais récepteurs d'une session.
- SDES (Source Description) décrit la source : nom, email, tél, etc.
- BYE permet à une station d'indiquer la fin de sa participation à une session.
- APP est un paquet de signalisation spécifique à une application.[17]

Les protocoles RTP et RTCP sont adaptés pour la transmission de données temps réel,et principalement utilisés en visioconférence, où les participants sont tour à tour, émetteurs ou récepteurs. Pour le transport de la voix, ils permettent une transmission correcte sur des réseaux bien ciblés. C'est-à-dire, des réseaux qui implémentent une qualité de service adaptée (ATM). Il est aussi possible de s'appuyer sur des réseaux bien dimensionnés (bande passante, déterminisme des couches sousjacentes, etc.), de type LAN d'entreprise.

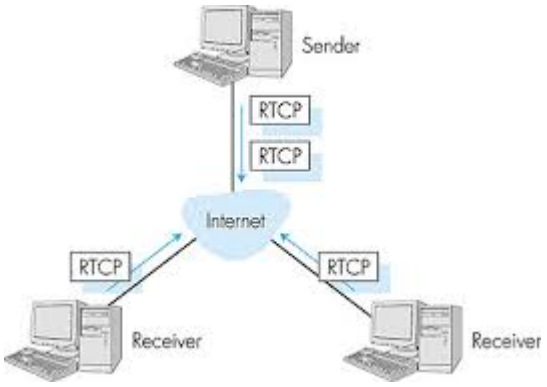

FIGURE 3.4 – La transmission des flux média avec RTP.[18]

3.6 Les attaques dans le réseau

Une attaque est l'exploitation d'une faille d'un système informatique.Les principales buts des attaques sont les suivant :

3.6.1 Interruption

Vise la disponibilité des informations.

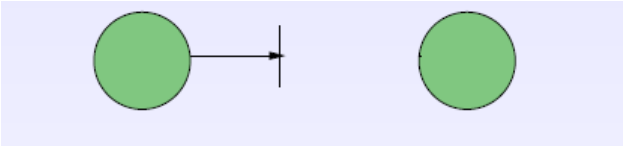

FIGURE 3.5 – L'interruption

3.6.2 Interception

Vise la confidentialité des informations (capture de contenu, analyse de traffic, . . .)

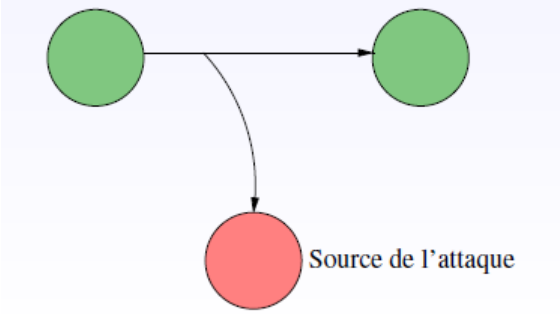

FIGURE 3.6 – L'interception

3.6.3 Modification

Vise l'intégrité des informations (modification, rejeu, . . .)

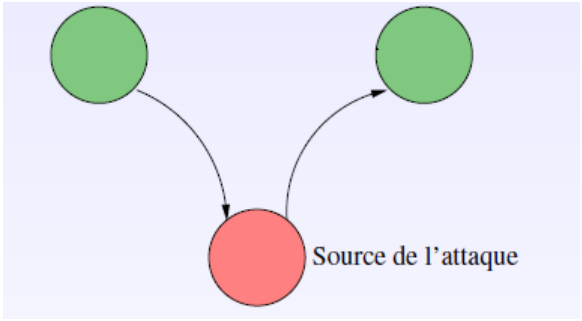

FIGURE 3.7 – La modification

3.6.4 Fabrication

Vise l'authenticité des informations (mascarade, . . .)

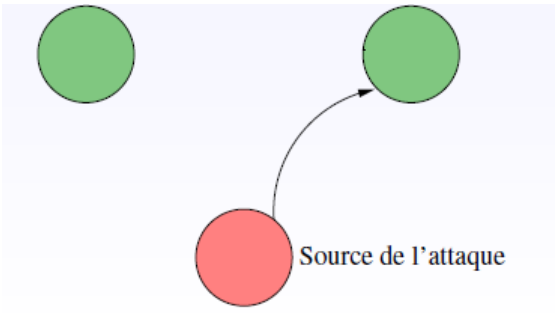

FIGURE 3.8 – La fabrication

3.6.5 Les attaques dans les réseaux local

Les principales buts des attaques dans les reseaux locale sont l'écoute du réseau,usurpation d'adresses (IP et MAC),Vol de session.

3.6.5.1 Usurpation IP spoofing

Technique utilisée afin de tenter d'obtenir un accès non autorisé sur une machine,la figure 3.9 illustre cette technique. L'intrus envoit des messages à un ordinateur cible en utilisant une Adresse IP semblant indiquer que le message provient d'une machine de confiance.
L'IP spoofing est plutôt utilisé contre des services dont le mécanisme d'authentification repose sur l'adresse IP. La difficulté principale - outre de trouver une Adresse IP cliente à simuler, et de mettre en place l'envoi de paquets réseaux dont l'adresse IP est falsifiée vers la cible - consiste à récupérer les paquets renvoyés par la cible à destination de la machine ayant l'adresse spoofée lorsque cela est nécessaire...
Une autre utilisation de l'IP Spoofing consiste à simplement falsifier la source d'une autre attaque. Lors d'une attaque de type déni de service par exemple, si l'adresse IP source des paquets envoyés est falsifiée, il sera plus difficile de localiser la provenance réelle de l'attaque.Dans la figure suivante présente une technique utilisée afin de tenter d'obtenir un accès non autorisé sur une machine.

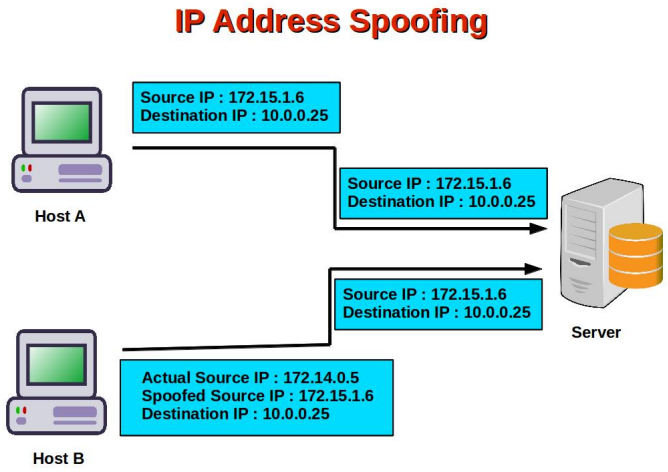

FIGURE 3.9 – IP Spoofing[18]

3.6.5.2 Vol de session (Connection Hijacking)

Hacking consiste à découvrir des informations sensibles et des sites internet vulnérables à l'aide des requêtes spécifiques et judicieusement construites.Sons objectif est de prendre la main sur une connexion déjà établie.sons principe est comme le suivant :
• Attendre l'établissement d'une connexion.
• Désynchroniser la connexion entre le client et le serveur (en forgeant un paquet avec un numéro de séquence particulier).
• Profiter de la désynchronisation pour faire au serveur ce qu'on veut.
La figure suivante illustre les étapes du hacking :

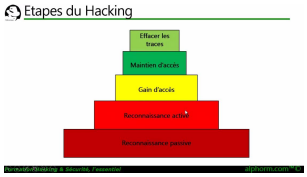

FIGURE 3.10 – Les étapes du hacking[18]

3.7 Mise en place d'une politique de sécurité

La sécurité informatique vise généralement cinq principaux objectifs l'intégrité,la confidentialité,la disponibilité, la non répudiation et l'authentification.

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.Et pour définir une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes :
• Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.
• Élaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés.
• Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés.
• Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

3.8 Les dispositifs de sécurité

3.8.1 Les firewall

3.8.1.1 Définition

Un pare-feu (firewall, en anglais) est un dispositif matériel et/ou logiciel qui implémente la fonction de sécurité de contrôle d'accès. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données.

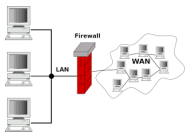

FIGURE 3.11 – Un pare-feu[18]

3.8.1.2 Les différents types de firewall

Packet filter : Le packet filter, comme son nom l'indique, filtre les paquets dans les deux sens. Pour ce faire, il utilise des fonctions de routage interne classiques. Ce sont des protections efficaces, mais pas toujours suffisantes. Certaines attaques complexes peuvent déjouer les règles.

Screening router : Evite le IP spooffing en vérifiant que les adresses d'origine des paquets qui arrivent sur chaque interface sont cohérentes et il n'y a pas de mascarade. Exemple : un paquet qui a une adresse de votre réseau interne et qui vient de l'extérieur est un Spoofed Packet. Il faut le jeter et prévenir le plus vite l'administrateur qu'il y a eu tentative d'attaque.

3.8.2 Les systèmes de détection et de prévention de l'intrusion

Un système de détection d'intrusion (IDS en anglais), est un dispositif matériel et/ou logiciel de surveillance qui permet de détecter en temps réel et de façon continue des tentatives d'intrusion en temps réel, dans un SI ou dans un ordinateur seul, de présenter des alertes à l'administrateur, voire pour certains IDS plus sophistiqué, de neutraliser ces pénétrations éventuelles et de prendre en compte ces intrusions afin de sécuriser davantage le système agressé. Il existe deux grandes familles distinctes d'IDS :

- Les N-IDS (Network Based Intrusion Detection system), ils assurent la sécurité au niveau du réseau.
- Les H-IDS (Host Based Intrusion Detection system), ils assurent la sécurité au niveau des hôtes.

3.8.3 VPN

Un réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de tunnel.La figure suivant présente un tunnel VPN :

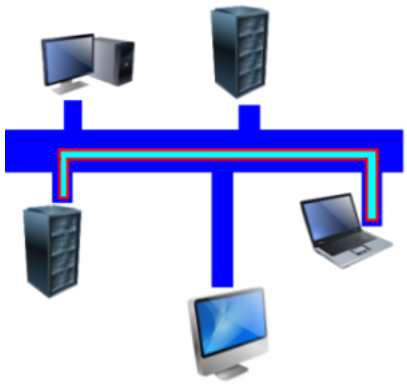

FIGURE 3.12 – Le tunnel VPN[18]

Conclusion

Dans ce chapitre nous avons parlé sur les vulnérabilités que se soit des vulnérabilités des systèmes d'exploitations dont un environnement VoIP est implémenté,ou les vulnérabilité des protocole utilisé par cette technologie,et nous avons parlé aussi sur les techniques de sécurité.Le prochaine chapitre concerne la simulation d'un réseau basé sur la VoIP en utilisant un firewall.

CHAPITRE 4

SIMULATION D'UN RÉSEAU VOIP

Introduction

Dans ce chapitre nous entamons la partie pratique .Nous présenterons la simulation de notre réseau VoIP et nous parlerons des technologies que nous utiliserons pour la réalisation de notre réseau.Nous consacrons la première partie à la présentation des différents choix techniques,tandis que dans la deuxième,nous exposerons quelques interface.

4.1 Choix technique

4.1.1 GNS3(Graphical Network Simulator)

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.GNS3 permet d'avoir un routeur Cisco virtuel sur son ordinateur. A noter simplement que GNS3 ne fournit pas d'IOS,il faut se les procurer à l'aide d'un compte Cisco CCO par exemple.Ou grâce à Google.
GNS3 est un logiciel libre qui fonctionne sur de multiples plateformes,incluant Windows,Linux,et MacOS X.[21]

4.1.2 VMware Workstation

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,BSD et MS-DOS.

VMware Workstation est développé et vendu par VMware, Inc., une division de Dell Technologies. Il existe une version gratuite, VMware Workstation Player, à des fins non commerciales. Une licence de système d'exploitation est nécessaire pour utiliser des droits tels que Windows.

VMware Workstation prend en charge le raccordement des cartes réseau existantes et le partage des disques physiques et des périphériques USB avec une machine virtuelle. Il peut simuler les lecteurs de disque, Un fichier image ISO peut être monté en tant que lecteur de disque optique virtuel, et les disques durs virtuels sont implémentés sous forme de fichiers .vmdk.

VMware Workstation Pro peut sauvegarder l'état d'une machine virtuelle (un "instantané") à tout instant. Ces instantanés peuvent ensuite être restaurés, renvoyant efficacement la machine virtuelle à l'état enregistré,tel qu'il était et libres de tout dommage postérieur à l'instantané de la machine virtuelle.

4.1.3 Cisco IP Communicator

Cisco IP Communicator est une application Windows Softphone Windows qui vous permet d'utiliser votre ordinateur personnel pour effectuer des appels vocaux et vidéo haut de gamme. En offrant les dernières technologies de communication IP, il est facile d'acquérir, de déployer et d'utiliser.

Avec un casque d'écoute USB ou un haut-parleur USB et Cisco IP Communicator, vous pouvez accéder facilement au numéro de téléphone de votre entreprise et à votre messagerie vocale. Tout ce dont vous avez besoin est une connexion Internet et un accès à distance à votre réseau d'entreprise, que vous travailliez à domicile, que vous preniez en charge un centre de contact ou que vous voyagiez en entreprise.

4.1.4 Serveur TFTP (Trivial File Transfer Protocol)

TFTP Server est un client TFTP gratuit qui permet d'envoyer et de recevoir plusieurs fichiers simultanément vers différents périphériques de réseau. Ainsi,TFTP Server est dédié aux administrateurs réseau souhaitant utiliser le protocole TFTP pour transférer de nouveaux firmwares vers leurs routeurs et leurs switchs réseau.
est un protocole simplifié de transfert de fichiers. Il fonctionne en UDP sur le port 69, au contraire du FTP qui utilise lui TCP.

4.1.5 Les plates-formes utilises

4.1.5.1 Routeur Cisco 3600

La série Cisco 3600 comprend les routeurs Cisco 3620, Cisco 3631, Cisco 3640 et Cisco 3660. En tant que solutions modulaires, les routeurs de la série Cisco 3600 permettent aux entreprises d'accroître la densité d'accès à distance et de profiter des technologies WAN actuelles et émergentes et des capacités réseau. Les routeurs de la série Cisco 3600 sont entièrement pris en charge par le logiciel Cisco IOS, qui comprend la connectivité à distance, le routage LAN-LAN, la sécurité des données et des accès, l'optimisation WAN et les fonctions multimédia.

4.1.5.2 Firewall ASA

Cisco ASA est l'abréviation de Adaptive Security Appliance,c'est une gamme de pare-feu réseau produite par Cisco.Un pare-feu ASA (matérielle) est situé généralement entre le réseau interne et internet pour contrôler le réseau entier.
En plus de la fonction principale du pare-feu ASA,d'autre extra fonctionnalités sont offerts selon la version de pare-feu ASA utiliser. parmi les fonctionnalités supplémentaire :
- Des services IPS système de prévention d'intrusion
- Un service VPN
- Des services IPsec
- 100-200 interfaces VLAN

Dans notre cas nous avons utilisé ASAv (Adaptive Security Virtual Appliance) est une solution de sécurité de réseau virtualisée basée sur les pare-feu Cisco ASA 5500-X leaders du marché. Il prend en charge les environnements réseau (SDN) et les environnements Cisco ICC (Application Centric

Infrastructure) définis par les logiciels traditionnels et de prochaine génération afin d'assurer l'application des politiques et l'inspection des menaces dans des environnements multisitiques hétérogènes.

4.1.5.3 Switch

Un switch désigne un commutateur réseau, équipement ou appareil qui permet l'interconnexion d'appareils communicants, terminaux, ordinateurs, serveurs, périphériques reliés à un même réseau physique. Contrairement au concentrateur (ou hub), il fractionne le réseau en domaines de collision indépendants.

4.2 Présentation du prototype réalisé

4.2.1 Topologie

Pour la création de la topologie nous avons connecté GNS3 avec VMware Configurer la liaison entre VMware et GNS3 en utilisant des cartes réseau virtuel (NIC), configurer les options TCP/IP de la carte réseau virtuel et la carte réseau loopack dans le même segment.La figure suivante présente la topologie réalises.

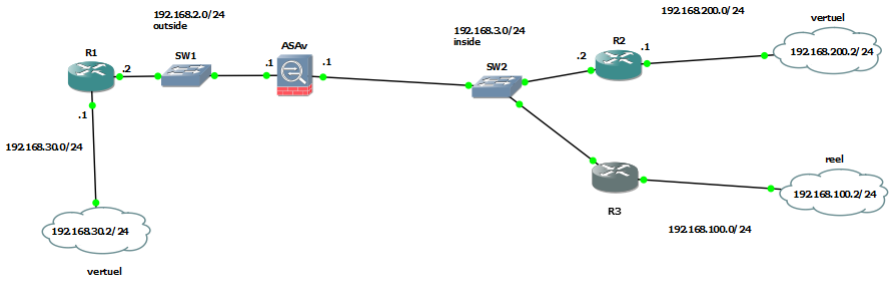

FIGURE 4.1 – La topologie du réseau réalises.

4.2.2 La configuration des équipements du réseau de la topologie

La configuration des équipements de réseau de la topologie sur GNS3 est représenté comme suit :

R3-configuration

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
```

```
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
!
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ip tcp synwait-time 5
!
!
!
!
!
interface FastEthernet0/0
ip address 192.168.3.3 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.100.1 255.255.255.0
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
network 192.168.3.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
!
no ip http server
no ip http secure-server
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.3.1
!
!
!
no cdp log mismatch duplex
```

```
!
!
!
control-plane
!
!
!
!
!
!
!
dial-peer voice 1 voip
destination-pattern 1..
session target ipv4 :192.168.3.2
!
!
!
telephony-service
max-ephones 1
max-dn 2
ip source-address 192.168.30.1 port 2000
system message SITE2
max-conferences 8 gain -6
!
!
ephone-dn 1 dual-line
number 200
label Administrateur
description Administrateur
name Administrateur
!
!
ephone-dn 2
number 201
label User
description User
name User
!
!
line con 0
exec-timeout 0 0
```

```
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
end
```

Après la configuration des deux routeurs R3 et R2 nous avons réussi à réaliser des appels VoIP avec des softphone Cisco IP Communicator sur le réseau local (inside),qui est sécurisé avec un firewall ASAv qui ne permettra pas à un trafic extérieur d'entrer à ce réseau local.
La figure suivante présente un appel entre deux softphone Cisco IP Communicator.

FIGURE 4.2 – Appel entre deux softphone Cisco IP Communicator.

La figure suivante présente la topologie de l'appel qui s'effectue entre deux utilisateur de réseau inside :

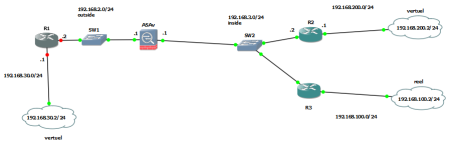

FIGURE 4.3 – Le réseau interne(inside).

4.2.3 Installation de Cisco ASDM

Après une configuration du base de firewall ASAv nous avons configuré les commandes suivantes pour avoir l'interface Cisco ASDM en utilisant un serveur tftpd32 qui doit être configuré avec une adresse IP adéquate et une image asdm-722.bin :

```
# copy tftp: flash:
Address or name of remote host [192.168.3.3]? 192.168.100.2
Source filename [192.168.200.2]? asdm.bin
Destination filename [asdm.bin]? _
```

FIGURE 4.4 – Les commandes a exécuté pour avoir l'interface Cisco ASDM.

La figure suivante présente le serveur TFTP après l'exécution des commandes au-dessus.

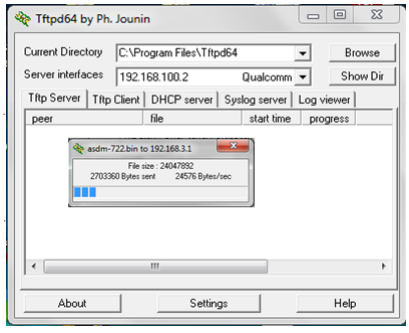

FIGURE 4.5 – Le serveur TFTP .

Nous avons connecté au firewall en utilisant un navigateur avec une adresse IP de firewall adéquate pour accéder à l'ASDM sur l'ASA. L'ASA présente cette fenêtre pour permettre le téléchargement de l'application ASDM.nous avons cliqué sur Install ASDM Luancher pour télécharger le programme d'installation de l'application ASDM.[16]

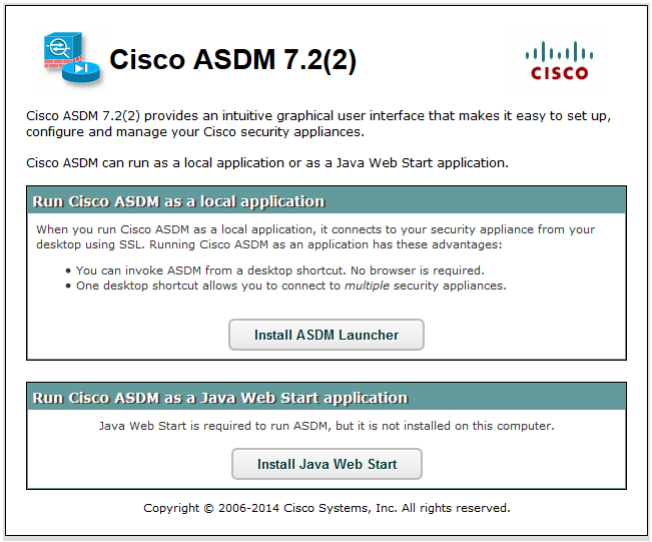

FIGURE 4.6 – L'interface de téléchargement Cisco ASDM.

Une fois le lanceur d'ASDM téléchargé,nous avons exécutés les étapes stipulées par les invites afin d'installer le logiciel et d'exécuter le lanceur de Cisco ASDM. Nous avons entré l'adresse IP pour l'interface que nous avons configuré avec la commande https, ainsi qu'un nom d'utilisateur et un mot de passe vide,et nous avons installé java version 8 pour que l'interface Cisco ASDM s'ouvre .

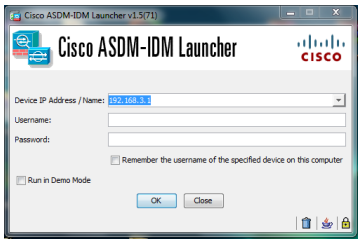

FIGURE 4.7 – Cisco ASDM.

La figure suivante présente l'interface une fois que l'application ASDM se connecte à l'ASA :

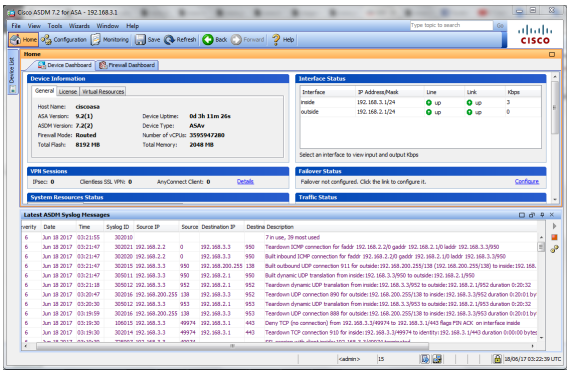

FIGURE 4.8 – Cisco ASDM pour ASA.

4.2.4 Configuration ASDM du tunnel VPN

Nous avons exécuté l'assistant VPN Wizards -> Site-to-site VPN Wizards.

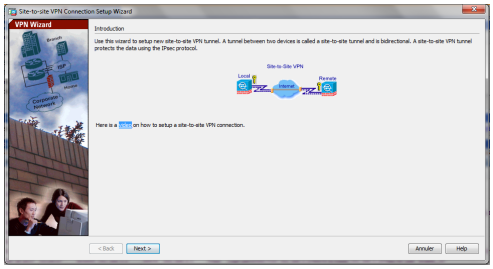

FIGURE 4.9 – Site-to-site VPN Wizards.

Nous avons spécifié l'adresse IP externe du partenaire distant.

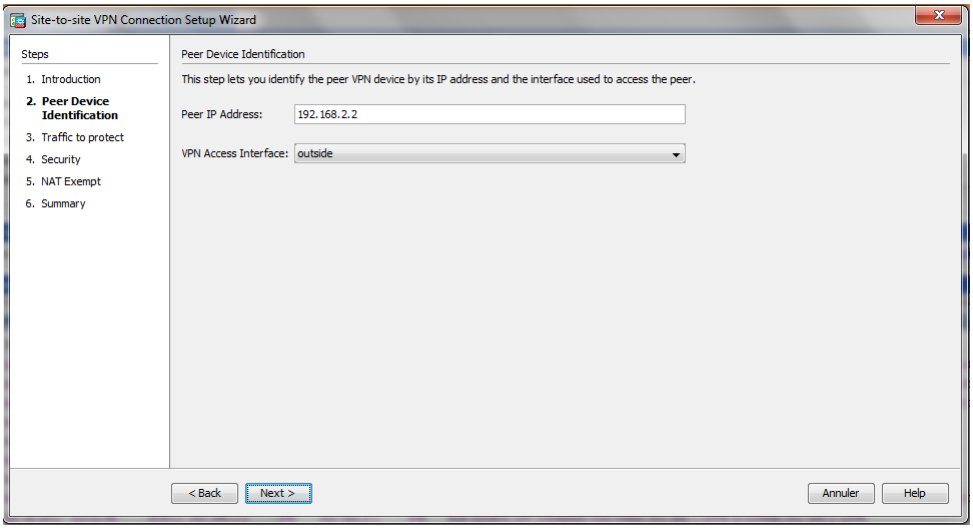

FIGURE 4.10 – Identification d'interface homologue.

Spécifiez les hôtes dont le trafic devra être autorisé à passer par le tunnel VPN.

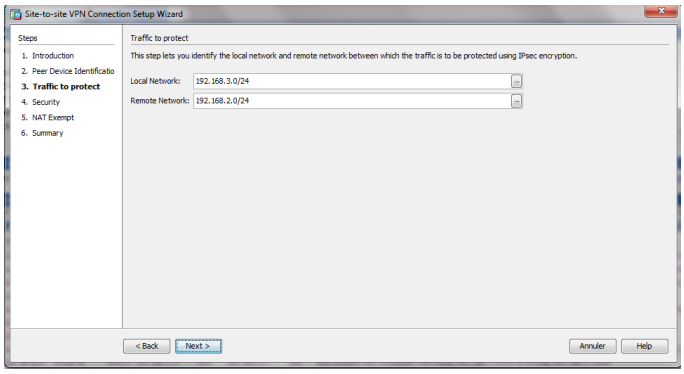

FIGURE 4.11 – Trafic a sécurise.

Nous avons configuré les informations d'authentification à utiliser et le trafic à sécuriser entre deux interfaces interne et externe en spécifiant les attributs à utiliser pour IPsec. Ces attributs doivent correspondre sur l'ASA et sur le routeur IOS.
Nous voyions dans la figure qui suit les algorithmes de chiffrement :

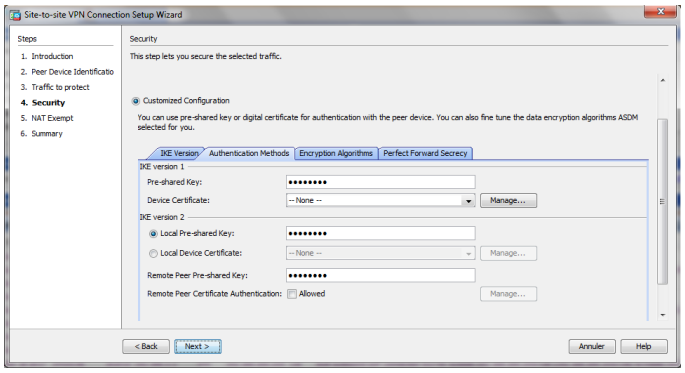

FIGURE 4.12 – Les algorithme de chiffrement.

La configuration de NAT des adresses privés inside vers une adresse publique outside .

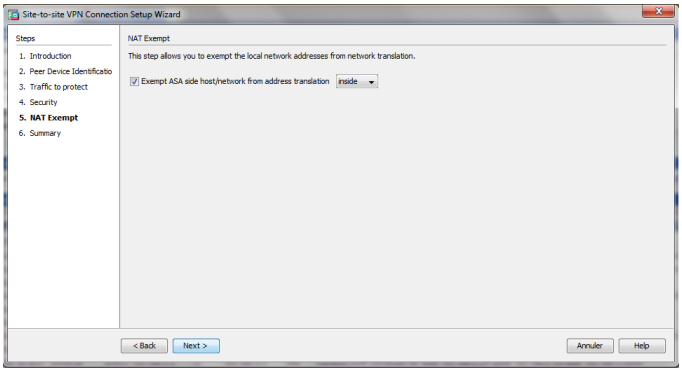

FIGURE 4.13 – Translation NAT.

Les attributs définis par l'assistant VPN sont affichés dans ce récapitulatif qui nous permettrons de vérifier une deuxième fois la configuration .

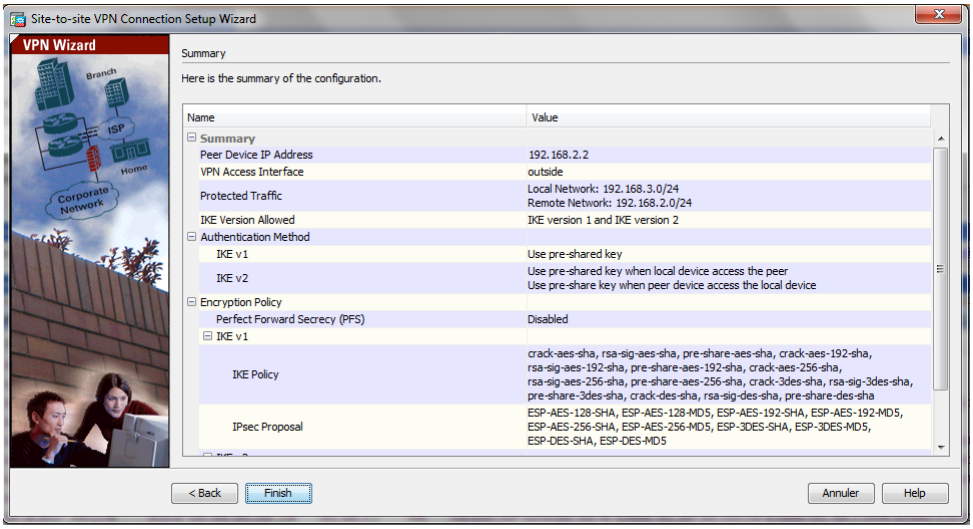

FIGURE 4.14 – VPN Wizards final.

4.2.5 Configuration SDM du routeur

Nous avons exécuté les mêmes étapes de configuration du tunnel VPN site à site sur le routeur Cisco IOS en utilisant la configuration sur Cisco SDM.

4.2.6 Configuration de la VoIP passant par le firewall ASA

La figure suivante illustre la topologie utilises :

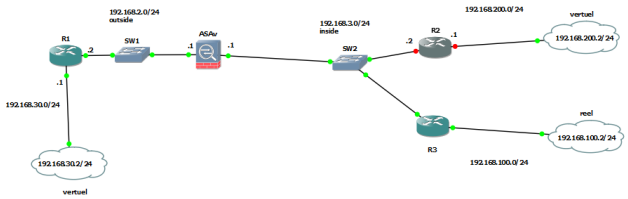

FIGURE 4.15 – La topologie de réseau VoIP avec firewall .

Pour permettre au trafic tcp du passerelle interne de sortir vers une interface extérieur nous avons configuré ces commandes sur le firewall ASAv :
#conf t
#object network 192.168.3.3
#host 192.168.3.3
#nat(inside,outside) dynamic interface
#exit
#access-list 100 extended permit tcp 192.168.3.0 255.255.255.0 eq sip host 192.168.2.2 eq sip
#access-group 100 in interface outside
Pour permettre aux utilisateurs de se connecter aux interfaces extérieur nous devons configurer les commandes suivant sur les passerelles interne :
#conf t
#access-list 100 permit ip any any
#ip inside source list 100 interface fa0/0 overload
#int fa0/0 outside
#ip nat outside
#int fa0/1
#ip nat inside

Après cette configuration et la configuration de la VoIP sur les routeurs nous avons réalisé un appel de l'interface inside vers une interface outside.Et les figure suivante présente le trafic sur le firewall.

FIGURE 4.16 – Les messages sur l'interface Cisco ASDM.

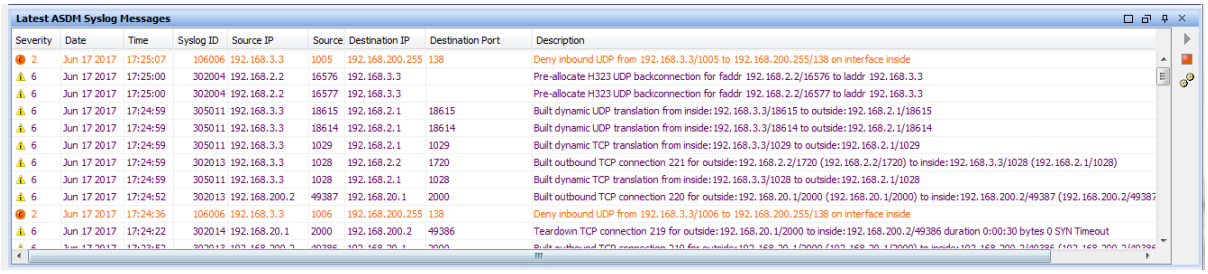

FIGURE 4.17 – Le protocole h323 sur l'interface Cisco ASDM.

Conclusion

Dans ce chapitre nous avons présenté une topologie d'un réseau qui supporte la téléphonie sur IP,ce réseau est sécurisé par un firewall ASAv et avant ça nous avons présenté les choix technique utilisés. puis nous avons présenté quelques commandes du configuration et quelques interfaces du configuration d'un tunnel VPN site à site entre le firewall ASAv et le routeur Cisco OUTSIDE.

CONCLUSION GÉNÉRALE

Durant ce travail, on a présenté les différentes générations de la téléphonie mobile, ainsi que les architectures des réseaux dont les opérateurs de télécommunication et les experts de l'industrie se sont déjà engagés dans la recherche pour son développement.

Pour améliorer la sécurité des réseaux, les administrateurs disposent de nombreux outils, dont les systèmes de détection d'intrusions et de pare-feu. Ces outils ont connu un essor particulier au cours des dernières années, notamment en raison du nombre grandissant d'attaques.

Un protocole de communication est une spécification de plusieurs règles pour un type de communication particulier. On a consacré ce mémoire à la mise en place d'un système de parefeu ASA sur l'utilisation de plusieurs protocoles comme le protocole VPN et H323...etc dont le but est d'améliorer la solution de sécurité VoIP.

La VoIP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités à ses solutions. Les principaux protocoles sont H.323, SIP . Nous avons donc présenté, dans ce mémoire plusieurs approches pour offrir des services de téléphonie sur des réseaux IP.

En perspectives nous souhaitons que ce modeste travail soit amélioré pour que l'appel VoIP s'effectue dans les deux sens d'une interface interne vers une interface externe et vice versa.

BIBLIOGRAPHIE

[1] BENSARI Mouchira,Sécurité des échanges dans un réseau de nœuds mobiles,mémoire de magistère,Université BATNA,2012.

[2] Denis TSHIMANGA,Etude d'implémentation d'une solution VOIP sécurisée dans un réseau informatique d'entreprise.Cas de l'ISTA de Kinshasa,Mémoire de magistère,INSTITUT SUPERIEUR DE TECHNIQUES APPLIQUEES CONGO,2013.

[3] Guy Pujolle,Les réseaux,livre,2011.

[4] H. HASSAN,De la téléphonie classique à la ToIP,Article,P :6,2010.

[5] Innocent Gerard Kouadi MANDIOUBA,PROBLEMATIQUE DE LA TELEPHONIE SUR IP,2017.

[6] Jamil,Caboré,Interconnexion d'un réseau filaire à un réseau wifi sécurisé,mémoire Online ,2009.

[7] Michèle , Germain , Introduction aux réseau , Forum Atena 2012.

[8] Michèle Germain ,Introduction aux réseaux,livre, 2012.

[9] Nicolas SIMON , Sécurité Dans Les Smartphones , mémoire Licence en Informatique , Université Libre De Bruxelles , P : 11-37; 2007.

[10] Ouakil, Pujolle , Téléphonie sur IP , 2^e édition , livre , P : 4-11,2007.

[11] Pujolle, Vivier, Al agha , Réseaux De Mobiles Et Réseaux Sans Fils , livre , 2001.

[12] Rebha Bouzaida , Étude et Mise en place d'une Solution VOIP Sécurisée , mémoire , P : 10 ;2011 .

[13] Samuel Pierre , Réseaux et systèmes informatiques mobiles , livre , P : 3-35 , 2002.

[14] Sidi-Mohammed SENOUCI , Application De Techniques D'apprentissage Dans Les Réseaux Mobiles , thèse de doctorat , université de pierre et marie curie – paris 6 , 2003.

Webographie

[15] igm.univ-mlv.frdrXPOSE2002DEBOURDEAU/

[16] www.cisco.com

[17] www.efort.com

[18] www.google.comsearchclient

[19] www.infonitec.com/definition-informatique-telecom/definition-informatique-telecom.php ?id=1043

[20] www.marche-public.fr/Terminologie/Entrees/1G.htm

[21] www.nemako.net/dc2/index.php

REMERCIEMENTS

Nous remercions Dieu,le tout puissant pour nous avoir donné la foi qui nous a guidé jusqu'à la réalisation et l'aboutissement de ce mémoire.

C'est avec une profonde reconnaissance et considération qu'on remercie particulièrement notre encadreur Mr A.khireddine pour son soutien, ses conseils judicieux et sa grande bienveillance durant l'élaboration de ce projet.

Nous aimerions aussi remercier tous nos amis,et nos familles de leur soutien et aide et qui nous ont donnés la force pour continuer.

Nous tenons à remrcier vivement les membres de jury,et à exprimer toute notre reconnaissance pour l'honneur qu'ils nous accordent en acceptant d'évaluer ce modeste travail.

DÉDICACES

Nous dédions ce modeste
travail à nos parents pour

leur soutient et leur présence
a nos cotés et leurs encouragement,

A toutes nos familles et
A toutes nos amis(e).

Résumé

Notre travail a consisté à concevoir une architecture du réseau de technologie VoIP qui utilise les protocoles du signalisation SIP et H323 sécurisé par un firewall ASA,qui permet de filtrer et de chiffrer le trafic échanger entre les utilisateur de ce réseau basant sur un tunnel VPN site à site.

Nous avons construit cette architecture avec un logiciel du simulation Cisco GNS3,en utilisant plusieurs plates-formes comme les routeur Cisco et un firewall ASAv qu'est installé sur une machine virtuelle Vmware Workstation.

Mots clés : VoIP,SIP,H323,firewall ASA,GNS3,ASAv,tunnel VPN

Abstract

Our work consisted in designing a network architecture of VoIP technology which uses the protocols of the signaling SIP and H323 secured by an ASA firewall Which allows filtering and encrypting traffic between users of that network based on a site-to-site VPN tunnel.

We built this architecture with Cisco GNS3 simulation software, using multiple platforms such as the Cisco router and an ASAv firewall that is installed on a VMware Workstation virtual machine.

Keywords : VoIP, SIP, H323, ASA firewall, GNS3, ASAv, VPN tunnel