Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaïa
Faculté des sciences exactes
Département informatique

En vue d'obtention d'un Master Professionnel en Informatique

Option : Administration et sécurité des réseaux informatique (ASR)

Sécurisation des réseaux de télécommunication et services VOIP par un IDS/IPS open source *SNORT*.

Encadré par :
Pr. KHIREDDINE Abdelkrim

Présenter par :
TRABELSI Oussama

-Promotion 2013-

Remerciement:

Nous tiens à remercier en premier lieu, mon encadreur Monsieur ***KHIREDDINE Abdelkrim*** *pour son soutiens et son aide précieuse durant mes premier deux cycle universitaire, surtout sa disponibilité, ses précieux conseils et ainsi pour sa sympathie, mes surtout d'avoir crue en moi.*

je remercie Mr et Mme ALLOUI d'avoir acceptée de jugé mon travail.

je remercie Melle KHOULALLEN d'avoir acceptée d'être partie du membre du jury.

je remercie tous mes enseignant qui en donner tant d'efforts pour nous transmettre leurs savoirs.

…Merci

Aux personnes les plus chères a ma vie

mes parent, mes sœurs, mes frères.

Sommaire

Liste des figures

Liste des Tableaux

Glossaire

ADSL Adaptative Digital Subscriber Line

AES Advanced Encryption Standard

AH Authentication Header

AKA Authentication and Key Agreement

API Application Protocol Interface

BTS Base Transceiver Station

CA Certification Authority

CLNP ConnectionLess Network Protocol

CPU Central Processing Unit

CRC Cyclic Redundancy Check

cRTP compressed Real- time Transport Protocol

DCCP Datagram Congestion Control Protocol

DES Data Encryption Standard

DHCP Dynamic Host Configuration Protocol

DoS Denial of Service

DDOS Distributed Denial Of Service

DTLS Datagram Transport Layer Security

EAP Extensible Authentication Protocol

ESP Encapsulating Security Protocol

ETSI European Telecommunication Standardization Institute

FA Foreign Agent

FAI Fournisseur d'Accès Internet

GPRS General Packet Radio Service

GSM Global System for Mobile Communications

GTP **GPRS** Tunneling Protocol

HA Home Agent

HLR Home Location Register

HTTP HyperText Transfer Protocol

HTTPS HTTP with SSL

IDS Intrusion detection system

IEEE Institute of Electrical and Electronics Engineers

IMAP Internet Message Access Protocol

IMT-2000 International Mobile Telecommunications-2000

IP Internet Protocol

IPS intrusion prevention system

IPsec Internet Protocol Security

ISDN Integrated Services Digital Network

MCU Multipoint Control Unit

ME Mobile Equipment

MGCP Media Gateway Control Protocol

MitM Man in the middle

MP Multi-Processor

MS Mobile Station

MSC Mobile-services Switching Center

MTU Maximum Transport Unit

NAT Network Address Translation

NGN Next Generation Network

NNI Network to Network Interface

NSA National Security Agency

OSI Open Systems Interconnect

PABX Private Automatic Branch eXchange

PC Personal Computer

PEAP Protected Extensible Authentication Protocol

PKI Public Key Infrastructure

PLMN Public Land Mobile Network

PMK Pair Wise Master Key

PMTU Path Maximum Transport Unit

POP Post Office Protocol

PSTN Public Switched Telephone Network

QoS Quality of Service

RADIUS Remote Authentication Dial In User Service

RNC Radio Network Controller

RNIS Réseau Numérique à Intégration de Service

RNS Radio Network Subsystems

RSA Rivest-Shamir-Adleman algorithm

RSVP Resource Reservation Protocol

RTC Réseau téléphonique commuté

RTCP Real-time Transport Control Protocol

RTP Real-time Transport Protocol

RTPC Réseau Téléphonique Public Commuté

SA Security Association

SIM Subscriber Identity Module

SIP Session Initiation Protocol

SRTP Secure Real- time Transport Protocol

SSL Secure Socket Layer

SSRC Synchronization source

STP Signaling Transfer Point

SVSP Simple Voice Security Protocol

TCP Transport Control Protocol

TLS Transport Layer Security

ToIP Telephony over IP

UAC User Agent Client

UAS User Agent Server

UDB User DataBase

UDP User Datagram Protocol

UE User Equipment

UMTS Universal Mobile Telecommunications System

VLAN Virtual Local Area Network

VoIP Voice over IP

VPN Virtual Private Network

WEP Wired Equivalent Privacy

WLAN Wireless Local Area Network

Introduction Générale

La sécurité est un enjeu majeur des technologies numériques modernes. Infrastructures de télécommunication (GSM, GPRS, UMTS), réseaux sans fils (Bluetooth, Wifi, WiMax), Internet, systèmes d'information, téléphones, systèmes d'exploitation, applications informatiques, toutes ces entités présentent des vulnérabilités : faille de sécurité, défaut de conception ou de configuration. Ces systèmes tombent en panne, subissent des erreurs d'utilisation et sont attaqués de l'extérieur ou de l'intérieur par des pirates ludiques, des cybercriminels, ou sont la proie d'espionnage industriel. Une approche globale de la sécurité des systèmes est essentielle pour protéger la vie privée, pour défendre le patrimoine d'une entreprise ou pour réduire les vulnérabilités des grands systèmes d'information.

De nos jours, la voix sur IP occupe une place privilégiée dans le monde des télécommunications. L'avantage incontesté de cette technologie est sa possibilité d'intégrer la voix et les données sur une même infrastructure Internet déjà existante. Grâce à cette technologie, les coûts des communications interurbaines ont chuté de manière considérable ce qui laisse penser qu'el le a encore de beaux jours devant elle. Or, avec l'augmentation du nombre des clients et du niveau d'interconnexion entre opérateurs, il est prévisible que les réseaux VoIP soient soumis dans un futur proche à des actes ou tentatives de vandalisme tels que : accès gratuit ou usurpation d'identité, envoi de messages polluants, tentatives de mise hors service de terminaux tiers ou d'équipements réseaux. La mise en place d'une politique de sécurité autour de ces systèmes est donc primordiale.

Outre la mise en place de pare-feux et de systèmes d'authentification de plus en plus sécurisés, il est nécessaire , pour compléter cette politique de sécurité, d'avoir des outils de surveillance pour auditer le système d'information et détecter d'éventuelles intrusions : ce que nous appelons intrusion signifie pénétration des systèmes d'information mais aussi tentatives des utilisateurs d'accéder à de plus hauts privilèges que ce eux qui leur sont attribués, ou tentatives des administrateurs d'abuser de leurs privilèges.

Dans ce même contexte se situe le présent travail, dont le but est de mettre en place une solution détection/prévention d'intrusion open source évolué destiné à la VOIP, basé sur les vulnérabilités les protocoles de signalisation SIP et H323.

Ce travail comprend cinq chapitres :

- Dans le premier chapitre, nous présentons une petite aperçue sur les réseaux de télécommunication.
- Dans le deuxième chapitre nous donnant une introduction générale sur la VOIP.
- Dans la troisième chapitre nous présentons une la sécurité dans la VOIP. les risque et les défit.
- Dans le quatrième chapitre nous détaillant une des solutions pour sécuriser un réseau informatique est celle de la Détection et la prévention des intrusions IDS/IPS.
- et enfin, dans le cinquième chapitre, en propose la mise en place d'une solution Open source Snort qui est un IDS et Un IP au même temps. ou nous simulant des attaques réel sur une plateforme VOIP a fin de donner une aperçue sur le mode de fonctionnement des IDS/IPS.

Mots-clés : sécurité, sûreté, confiance, confidentialité, intégrité, disponibilité, menace, vulnérabilité, piratage, cybercriminalité, pare-feu, VOIP, IDS, IPS.

Chapitre I:

Les réseaux IP de Nouvelle Génération

Introduction:

Actuellement, l'ensemble des architectures de communication est en train d'évoluer vers une infrastructure globale fondée sur IP : les réseaux de nouvelle génération (**NGN** : Next Generation Networks). Le modèle IP est caractérisé par une structure modulaire composée de plusieurs couches distinctes qui communiquent à travers des interfaces bien définies. L'évolution vers les réseaux NGN s'explique par la capacité du modèle IP d'offrir un mode d'acheminement des données indépendant, d'une part, du type de technologies réseaux sous-jacentes (Ethernet, Fibre optique, Wi-Fi, WiMax, Satellite, 3G/2G, etc.) et, d'autre part, du type de données véhiculées (audio, vidéo, données). L'objectif est ainsi de réaliser, à travers les réseaux NGN, le support de multiples services (téléphonie, télévision, services Internet) au sein d'une unique infrastructure tirant parti de l'hétérogénéité des technologies d'accès.

Cette architecture a donc pour objectif de permettre à des utilisateurs utilisant différents terminaux d'accéder à plusieurs types de services via des réseaux d'accès variés. Dans ce contexte, l'un des défis majeurs est de gérer les besoins des différents utilisateurs en termes de qualité de service (QoS : Quality of Service), de sécurité des services fournis, mais aussi de mobilité des utilisateurs.

Dans ce chapitre, nous rappelons le contexte de l'évolution des architectures de télécommunications traditionnelles vers les réseaux de nouvelle génération, avant d'évoquer les principales caractéristiques de ces nouveaux réseaux. Tout en détaillant les différents mécanismes qui permettent de fournir des garanties en matière de QoS, de sécurité et de mobilité.

I.1. La typologie des réseaux et des systèmes :

Le monde numérique des réseaux et des systèmes comprend :

- les réseaux informatiques : les réseaux locaux d'entreprises, les réseaux de vidéosurveillance sur IP, Internet, les réseaux sans fil (WiMax, WiFi, Bluetooth), les réseaux passifs d'étiquettes intelligentes (RFId) ;
- les réseaux de télécoms : les réseaux satellites, les réseaux de localisation GPS ou Galiléo, les réseaux téléphoniques, les réseaux d'opérateurs de téléphonie mobile (GSM, GPRS, EDGE, UMTS) ;
- les réseaux de diffusion de télévision (TNT, câble) et de radio mais aussi les réseaux résultant de la numérisation de la totalité du processus de production audiovisuelle, et ceux qui émergeront du déploiement des salles de cinéma numérique ;
- Les SI de l'État, des institutions, des entreprises, des banques, des organisations, des réseaux à domicile (réseau domestique), de gestion des infrastructures critiques et du patrimoine numérique naissant des familles et des individus.

I.2. Évolution des réseaux:

I.2.1 Des réseaux dédiés:

Jusqu'au milieu des années 80, les services de télécommunications traditionnels possèdent chacun leur réseau dédié optimisé pour le transport d'un type d'information pour lequel il a été conçu, et l'interconnexion entre ces réseaux a été très limitée ou inexistante. Ainsi, le monde des réseaux était constitué de trois sous-réseaux distincts et indépendants, à savoir les réseaux de diffusion, les réseaux de télécommunications et les réseaux de données. En effet, la voix est transportée sur les réseaux téléphoniques commutés (RTC) qui répondent alors parfaitement aux impératifs de QoS, de fiabilité et d'interactivité en se basant sur un plan de contrôle rigide. La télévision est diffusée par satellite ou par voie hertzienne qui apparaît comme le mode de transmission le plus adapté vue leur nature diffusive intrinsèque caractérisée par une communication unidirectionnelle qui permet la scalabilité en supportant un grand nombre d'utilisateurs. Enfin, les réseaux de données, basés sur X.25, représentent un intermédiaire entre la fiabilité du réseau de

télécommunications et la mise à l'échelle du réseau de diffusion tout en permettant une certaine interactivité.

Cette vision des réseaux de communication se révèle progressivement étroite puisqu'elle entraîne des situations de « monopole naturel » caractérisées par la mise en œuvre systématique de solutions propriétaires et d'infrastructures qu'il est difficile de faire évoluer ou d'interconnecter. Par conséquent, l'infrastructure dédiée au transfert de données va proposer une nouvelle vision des architectures de communication ; il s'agit de l'architecture Internet qui se fonde sur le modèle TCP/IP.

I.2.2 L'Internet:

Au cours des années 90, l'explosion du volume du trafic véhiculé sur Internet et l'accroissement de son hétérogénéité en termes de services (données, voix, vidéo), ont favorisé l'adoption de l'architecture d'Internet.

Basé sur le modèle TCP/IP et la commutation de paquets, le développement de protocoles et de services sur Internet est largement simplifié puisque ce modèle est ouvert, indépendant d'une architecture particulière et propose une hiérarchie protocolaire qui permet à chaque couche de s'abstraire des difficultés soulevées et résolues par la couche inférieure. En effet, le protocole IP, offre une connectivité en mode paquet indépendante du réseau sous-jacent permettant d'interconnecter tout type de réseau.

Avec les protocoles de niveau « Transport » (UDP et TCP), les applications disposent alors d'une interface standard pour transmettre sur un réseau IP. Graduellement, des protocoles de niveau applicatif (FTP, SMTP, HTTP) ont été standardisés ; ce qui a permis le développement des services « classiques » d'Internet (mail, Web, FTP). Finalement, l'augmentation en puissance des terminaux utilisateurs, conjointement avec l'accroissement des débits et portées des réseaux d'accès, a permis d'envisager non seulement la réplication, sur Internet, des services RTC ou télévisuels mais aussi le développement de nouveaux services large bande multimédia.

I.3. La convergence des réseaux:

Durant ces dernières années, les trois réseaux ont connu des évolutions conséquentes. Le réseau de télécommunications est devenu numérique, sans fil et mobile grâce à l'émergence des réseaux mobiles de 2ème et 3ème générations qui ont augmenté le débit de transmission, et par la même, le nombre de services.

Le même constat peut être fait pour le réseau de diffusion qui migre actuellement vers la télévision et la radio numérique. Ainsi, les frontières entre les trois réseaux tendent à disparaître et les services se généralisent sur tous les réseaux. Par exemple, l'Internet et la TV sont disponibles sur les réseaux de télécommunications, les communications téléphoniques peuvent être effectuées sur Internet, etc.

Cette nouvelle mouvance a fait émerger la notion de convergence des réseaux qui a pour objectif de définir un cadre global pour le regroupement des trois types de réseaux sous une seule architecture.

Les nouveaux défis techniques des réseaux de nouvelle génération sont alors la convergence des services (voix, vidéo et données), la convergence des réseaux autour du mode paquet, l'offre de service sans couture d'un réseau à un autre (handovers horizontal et vertical), l'ubiquité, le support de terminaux multimédias, le déploiement de services disponibles de bout en bout accessibles depuis n'importe quel réseau d'accès, etc.

I.4. Les réseaux de nouvelle génération:

I.4.1 Définition et principes fondamentaux:

Les réseaux NGN représentent la prochaine génération de réseaux censée réaliser la convergence totale des services en une seule architecture. Cependant, il n'existe pas encore une définition unique de la notion de NGN. L'ITUJT a publié deux recommandations concernant les réseaux NGN. La première recommandation, Y.2001 [ITU 04a], définit les principales caractéristiques d'un réseau NGN, tandis que la deuxième, Y.2011 [ITU 04b], propose une architecture fonctionnelle. Le comité technique **TISPAN** de l'**ETSI** (**E**uropean **T**elecommunications **S**tandards **I**nstitute) a aussi défini une architecture fonctionnelle pour les réseaux NGN largement inspirée de celle proposée par l'ITUJT. Les définitions des organismes de normalisation tels que l'ETSI et l'ITUJT

restent assez vagues et dressent une liste générale des principales caractéristiques des réseaux NGN qui se veulent multi-réseaux, multiservices, multi-protocoles et multi-terminaux. Ces caractéristiques communes sont : la convergence ou intégration des réseaux, le « tout IP », le découplage des fonctions applicatives du réseau de transport sous-jacent, la distribution de l'intelligence dans le réseau, l'ubiquité.

I.4.2 Architectures des réseaux NGN:

Afin de répondre aux différentes exigences citées précédemment et d'intégrer ainsi les infrastructures de télécommunication existantes avec celles à venir au sein d'une seule et unique infrastructure commune, flexible et évolutive, des impératifs ont été clairement identifiés par les organismes œuvrant pour les réseaux NGN (3GPP, ITUJT, ETSI, ATIS, etc.) :

- Un cœur de réseau unique et mutualisé pour tous les types de réseaux d'accès et de services,
- Une architecture de cœur de réseau en 2 couches : « Transport » / « Services »,
- Une évolution du transfert des données vers le mode paquet,
- Des interfaces ouvertes et standardisées entre chaque couche afin de réaliser l'indépendance des services vis-à-vis du réseau,
- Un découplage entre la fourniture de service et la fourniture de réseau.
- Le support de technologies d'accès multiples,
- Le support de la convergence des réseaux voix/données et fixe/mobile,
- Le support de terminaux multiples (modulaires, multi-mode, multimédia et adaptatifs).

Ainsi, la principale caractéristique d'un réseau de nouvelle génération est son fondement sur IP qui offre un mode de transfert homogène de bout en bout indépendant, d'une part, des réseaux sous-jacents et, d'autre part, du type de données applicatives véhiculées. Après l'évolution du cœur de réseau vers le « tout-IP », la notion la plus importante reste la décomposition en plans fonctionnels séparés par des interfaces ouvertes qui assure à la fois le passage à l'échelle et la flexibilité d'une telle architecture en offrant une facilité d'interconnexion et d'intégration de nouveaux services.

La ***Figure 1-1*** offre une représentation communément admise de l'architecture des réseaux NGN.

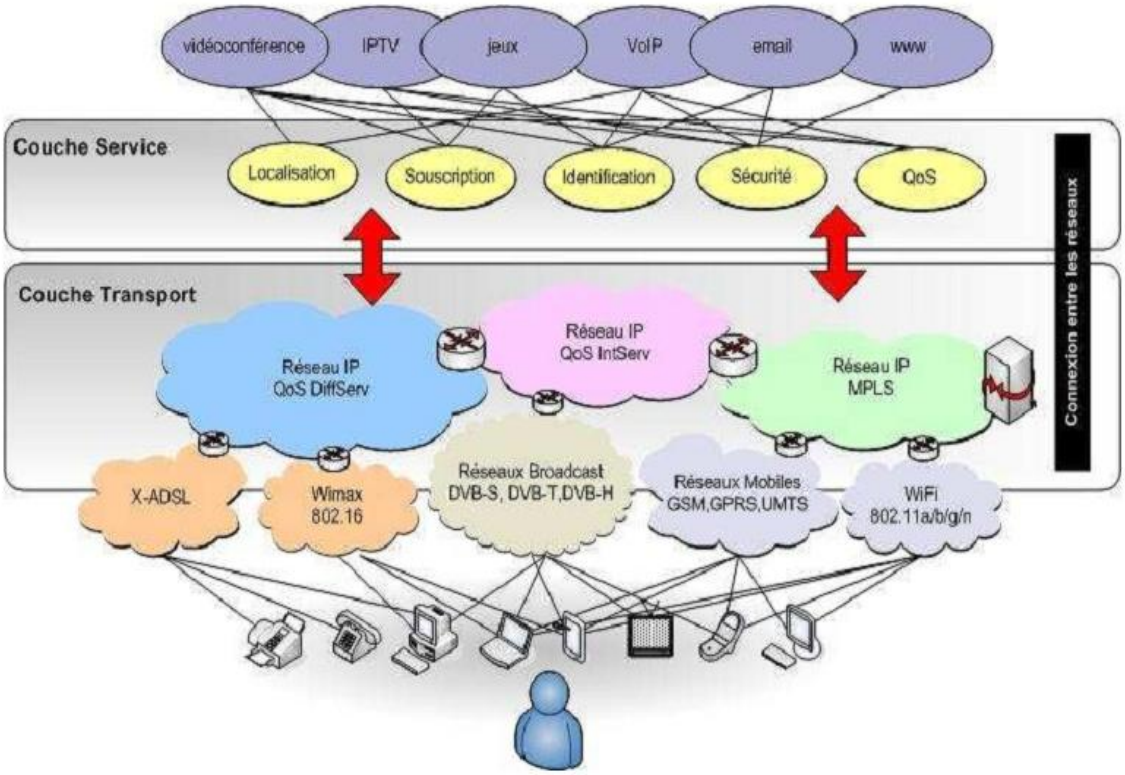


Figure 1-1 : Architecture générique des réseaux NGN

Le plan de « Transport » regroupe l'ensemble des ressources mises en place pour assurer le transfert de données. Ainsi, il gère l'acheminement du trafic vers sa destination en fournissant une connectivité IP aux différents composants d'un réseau NGN tout en garantissant une QoS de bout en bout. Ce plan dépend directement de la technologie du réseau de transport utilisé pour acheminer les paquets.

Le plan de « Service » fournit les fonctionnalités de base pour l'exécution des services avec ou sans session. En effet, il regroupe les plateformes d'exécution de service et de diffusion de contenu tout en masquant la diversité technologique aux clients et aux fournisseurs de services.

Après ces plans horizontaux, on peut différencier les réseaux d'accès des réseaux de transit. En effet, les premiers ont pour but de concentrer le trafic des différents utilisateurs vers des équipements centraux.

Alors que, les deuxièmes ont pour vocation d'acheminer des volumes de trafic importants entre quelques entités limitées. Dans la ***Figure 1-1***, nous pouvons noter la diversité des technologies permettant à l'utilisateur d'accéder aux services ; ce qui peut former ce qu'on appelle parfois le plan d'accès. Il est important de noter que l'interaction entre les réseaux de nouvelle génération est les réseaux traditionnels est prise en charge par différentes passerelles d'interconnexion afin d'assurer une compatibilité avec les technologies déployées actuellement.

I.4.3 Caractéristiques des réseaux NGN:

Un réseau NGN doit pouvoir supporter n'importe quel réseau d'accès, filaire ou sans fil, et n'importe quel équipement terminal, fixe ou mobile. Par ailleurs, dans un tel environnement, la définition d'un service est indépendante des technologies des réseaux sous-jacents ainsi que des différents terminaux utilisés afin d'accéder à ces services.

I.4.3.1 Des terminaux de plus en plus sophistiqués :

Un terminal peut être défini comme est un équipement situé en extrémité d'un réseau de Télécommunication, permettant à un utilisateur de communiquer sur ce réseau en assurant l'interface avec cet utilisateur. Aujourd'hui, les terminaux sont de plus en plus nombreux et sophistiqués tels que les téléphones (fixe, GSM, Wi-Fi, etc.) les PDA, les ordinateurs (fixe et portable) ; et supportent des applications de types très variés comme le texte, la parole, l'image et la vidéo. En s'équipant de divers types d'interfaces de connexion (Ethernet, Wi-Fi, WiMax, Bluetooth, etc.), ces terminaux permettent d'utiliser différents types de réseaux d'accès pour qu'un utilisateur puisse se connecter aux réseaux NGN.

I.4.3.2 Des réseaux d'accès supportant des débits de plus en plus élevés :

Les réseaux d'accès multiplient les technologies d'accès (fixe, mobile, sans fil, etc.), évoluant constamment pour supporter de plus hauts débits (technologies ADSL, 802.11b, a, g) indispensables au support de services large bande et offrant des services adaptés à IP. En effet, le RTC, initialement conçu pour le service de téléphonie (voix), a permis une ouverture à des services haut débit de type voix et données grâce aux technologies xDSL (ADSL, HDSL, VDSL, etc.). Les réseaux ADSL ou câblés ont constitué, par ailleurs, un des premiers exemples opérationnels de la convergence des services Voix/Vidéo/Donnée. D'un autre coté, les réseaux d'accès sans fil ont connu des évolutions importantes leur permettant d'offrir des débits de plus en plus élevés tout en gérant la mobilité des utilisateurs.

Par ailleurs, les réseaux mobiles 2G (GSM) et 2.5G (GPRS) ont largement contribué à habituer l'utilisateur à un usage mobile du service voix. La migration vers les technologies 3G (UMTS : Universal Mobile Telecommunication System), qui fournit des débits plus élevés en utilisant de nouvelles bandes de fréquence, a impliqué l'implémentation d'un cœur de réseau unifié pour les services voix et données. Ainsi, cette technologie (UMTS) représente le premier système global entièrement normalisé avec une architecture de réseau et de services NGN. Par ailleurs, il existe d'autres technologies d'accès telles que le WiMax (Worldwide Interoperability for Microwave Access) et le LTE (Long Term Evolution) qui émergent.

I.4.3.3 Des services de types variés:

L'évolution vers les réseaux NGN, fondés sur des technologies de transmission haut débit avec des garanties en matière de QoS, a permis de supporter des types variés de services tels que la voix, la vidéo et les données.

La variété des services envisageables dans les réseaux de nouvelle génération est due aux multiples possibilités qu'ils offrent en termes de média, de mode de communication, de mobilité, de réseaux d'accès et de terminaux. Ces services incluent les services IP traditionnels comme le mail et le web, mais aussi des services émergents comme : la voix sur IP (VoIP : Voice over IP), la diffusion de la télé sur IP (IPTV), et les applications fondées sur la présence tels que la

messagerie instantanée (Instant Messaging) et les services de localisation (Location-Based Services).

I.5. Sécurité dans les NGN:

Ces nouvelles infrastructures et les services qu'elles offrent aux usagers doivent être absolument sûrs, robustes, fiables et présenter une totale disponibilité. Les exigences de sécurité posées par ces nouveaux réseaux sont bien supérieures à celles des infrastructures classiques de télécommunications, en raison des risques inhérents à la technologie IP et à la créativité quasi illimitée d'usagers malveillants et d'organisations criminelles, ou encore à des erreurs humaines ou des défauts de jeunesse des équipements.

I.5.1 Différentes zones de sécurité:

Comme le montre la ***Figure 1-2***, la sécurité est divisée en trois zones distinctes. La zone de confiance est celle dans laquelle les systèmes et ressources du NGN sont hébergés et sous le contrôle de l'opérateur. Aucun contact n'est possible avec les équipements de l'usager ou ceux d'un autre réseau. Cette zone est protégée par diverses mesures, par exemple : sécurisation physique des éléments du réseau, durcissement des systèmes visant à réduire les vulnérabilités et à diminuer les risques opérationnels, mise en œuvre d'une signalisation et d'une gestion sûres, séparation des réseaux virtuels privés entre zone de confiance et zone vulnérable.

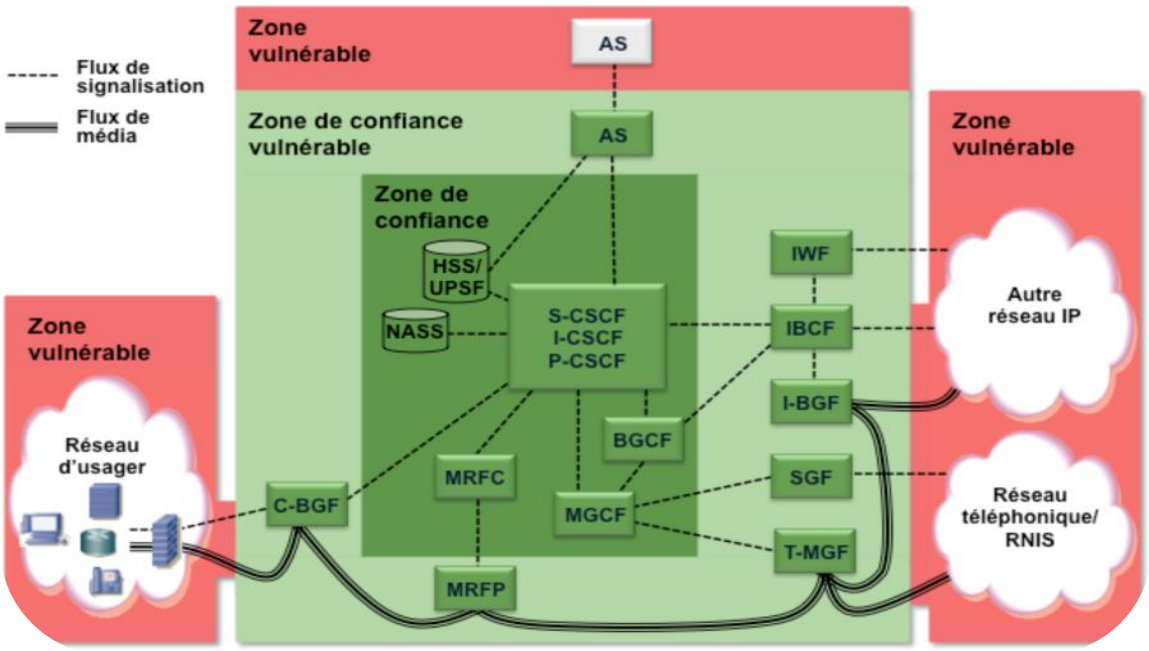


figure 1-2 : les trois zones différentes de sécurité

Dans la zone de confiance vulnérable, les équipements sont exploités par l'opérateur du NGN et sont contrôlés soit par l'opérateur lui-même, soit par l'usager. Leur rôle principal est de protéger les systèmes et ressources du NGN situés dans la zone de confiance. En plus des mesures de protection appliquées à la zone de confiance, l'utilisation de *firewalls* et de passerelles de filtrage ainsi que la mise en place de fonctionnalités de type *fusible* sont prévues. La zone vulnérable regroupe les systèmes et les ressources situées chez les usagers et chez les opérateurs partenaires, qui sont aussi des concurrents. Il s'agit d'infrastructures qui ne sont ni exploitées, ni hébergées par l'opérateur en propre.

I.5.2 Protection de l'accès:

L'accès au NGN et à ses ressources (***Figure 1-3***) n'est possible que pour les usagers authentifiés. L'authentification est faite par le serveur S-CSCF du réseau dans lequel l'usager a souscrit aux services, et non par un serveur du réseau visité. Elle se réfère au profil de l'usager mémorisé dans la base de données HSS. L'accès aux ressources du NGN requiert une autorisation de la part de ce même serveur S-CSCF, en fonction des informations contenues dans la base de données HSS et des éventuels contrats de fourniture de services passés avec les serveurs

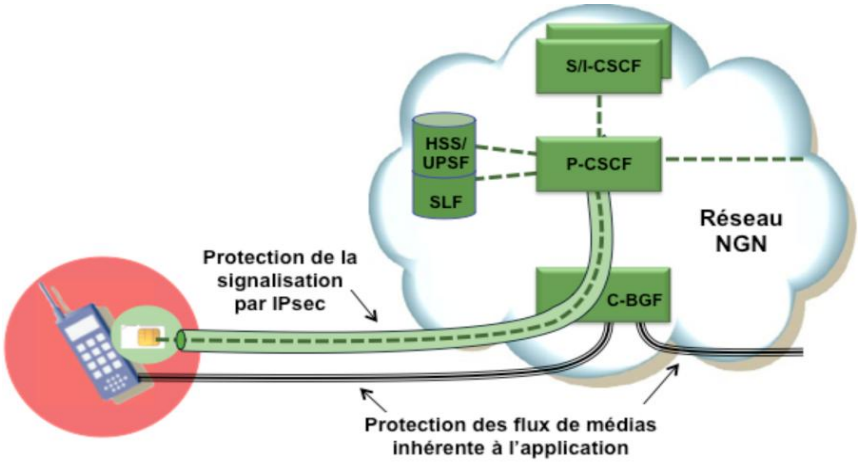


Figure 1-3: protection de l'accès au réseau NGN

d'applications. En plus, pour les équipements mobiles (téléphones cellulaires, équipements terminaux mobiles embarqués), le système de transmission est protégé par cryptage. La protection des flux de médias est inhérente à l'application.

I.5.3 Sécurisation des interconnexions:

En raison des exigences juridiques d'interception des communications (écoute légale), les échanges de messages de signalisation et contrôle ne peuvent pas être encapsulés dans un tunnel sécurisé allant de l'équipement terminal en itinérance jusqu'au serveur SIP de son propre réseau (***Figure 1-4***). La communication entre réseaux NGN est sécurisée au moyen de tunnels IPsec ESP(*Encapsulating Security Payload))*. Le système de signalisation et de contrôle, de terminal d'usager à terminal d'usager, peut être considéré comme sûr, car les segments critiques sont sécurisés et ils aboutissent dans le cœur IMS de chaque NGN.

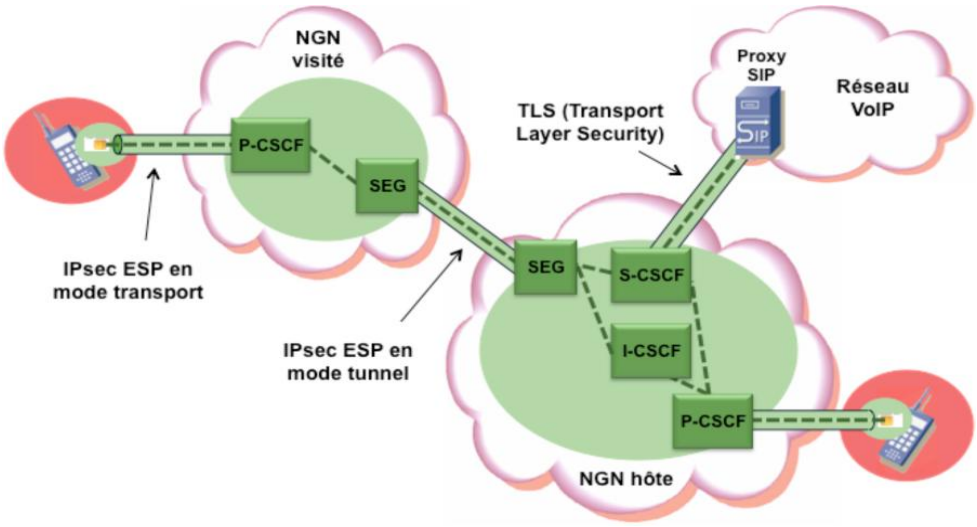


figure 1-4 : confidentialité et intégrité des données assurées aussi bien au niveau de l'accès d'usager que de l'interconnexion entre réseaux

Pour l'interconnexion avec des réseaux VoIP *(Voice over IP)* traditionnels, la sécurisation se sert de TLS *(Transport Layer Security).* Dans ce cas, le serveur S-CSCF tient à jour la liste des usagers VoIP habilités à établir des connexions vers le NGN. Pour des raisons de sécurité, ils n'auront pas accès à l'ensemble des services offerts aux usagers du NGN.

Conclusion:

L'apparition des réseaux de nouvelle génération a été principalement motivée par l'évolution des réseaux d'accès et des équipements terminaux, mais surtout par le besoin des clients de pouvoir accéder aux plateformes des différents services quel que soit le type de terminal et la technologie du réseau d'accès. L'architecture NGN décrite ci-dessus est loin d'être achevée. Héritée en grande partie d'Internet, cette architecture va se heurter aux mêmes problèmes, notamment ceux de la QoS et de la sécurité. En effet, les services supportés par les réseaux NGN ne pourront se déployer sans fournir aux clients des garanties en matière de QoS et de sécurité. Pour ce faire, les fournisseurs de services doivent pouvoir disposer d'outils permettant de gérer ces services (facturation, authentification, profil des utilisateurs, garantie de la qualité de service et de sécurité de bout en bout, etc.).

Chapitre II:

Étude Générale De La Voix Sur IP

Introduction

La voix sur IP constitue actuellement l'évolution la plus importante du domaine des Télécommunications. Avant 1970, la transmission de la voix s'effectuait de façon analogique sur des réseaux dédiés à la téléphonie. La technologie utilisée était la technologie électromécanique **(Crossbar)**. Dans les années 80, une première évolution majeure a été le passage à la transmission numérique ***Time-division multiplexing*** **(TDM)**. La transmission de la voix sur les réseaux informatiques à commutation de paquets IP constitue aujourd'hui une nouvelle évolution majeure comparable aux précédentes.

L'objectif de ce chapitre est l'étude de cette technologie et de ses différents aspects. On parlera en détail de l'architecture de la VoIP, ses éléments et son principe de fonctionnement. On détaillera aussi des protocoles VoIP de signalisation et de transport ainsi que leurs principes de fonctionnement et de leurs principaux avantages et inconvénients.

II.1. Présentation de la voix sur IP:

II.1.1. Définition:

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.

Figure 2.1: principe de la voix sur IP

II.1.2. Architecture:

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 trois principaux protocoles sont H.323, SIP et MGCP/MEGACO. Il existe donc plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP.
Certaines placent l'intelligence dans le réseau alors que d'autres préfèrent une approche égale à égale avec l'intelligence répartie à la périphérie. Chacune ayant ses avantages et ses inconvénients.
La **Figure-2.2** décrit, de façon générale, la topologie d'un réseau de téléphonie IP.

Elle comprend toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux. Chaque norme a ensuite ses propres caractéristiques pour garantir une plus ou moins grande qualité de service. L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur les passerelles/ contrôleur de commutation, appelées Gatekeeper. On retrouve les éléments communs suivants :

- **Le routeur :** permet d'aiguiller les données et le routage des paquets entre deux réseaux. Certains routeurs permettent de simuler un Gatekeeper grâce à l'ajout de cartes spécialisées supportant les protocoles VOIP.

- **La passerelle :** permet d'interfacer le réseau commuté et le réseau IP.
- **Le PABX :** est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur, et le réseau téléphonique commuté (RTC). Toutefois, si tout le réseau devient IP, ce matériel devient obsolète.
- **Les Terminaux :** sont généralement de type logiciel (software phone) ou matériel (hardphone), le softphone est installé dans le PC de l'utilisateur. L'interface audio peut être un microphone et des haut-parleurs branchés sur la carte son, même si un casque est recommandé. Pour une meilleure clarté, un téléphone USB ou Bluetooth peut être utilisé.

Le hardphone est un téléphone IP qui utilise la technologie de la Voix sur IP pour permettre des appels téléphoniques sur un réseau IP tel que l'Internet au lieu de l'ordinaire système **PSTN (Public switched telephone network - les réseaux téléphonique public commutés)** . Les appels peuvent parcourir par le réseau internet comme par un réseau privé.
Un terminal utilise des protocoles comme le SIP (Session Initiation Protocol) ou l'un des protocoles propriétaire tel que celui utilisée par Skype.

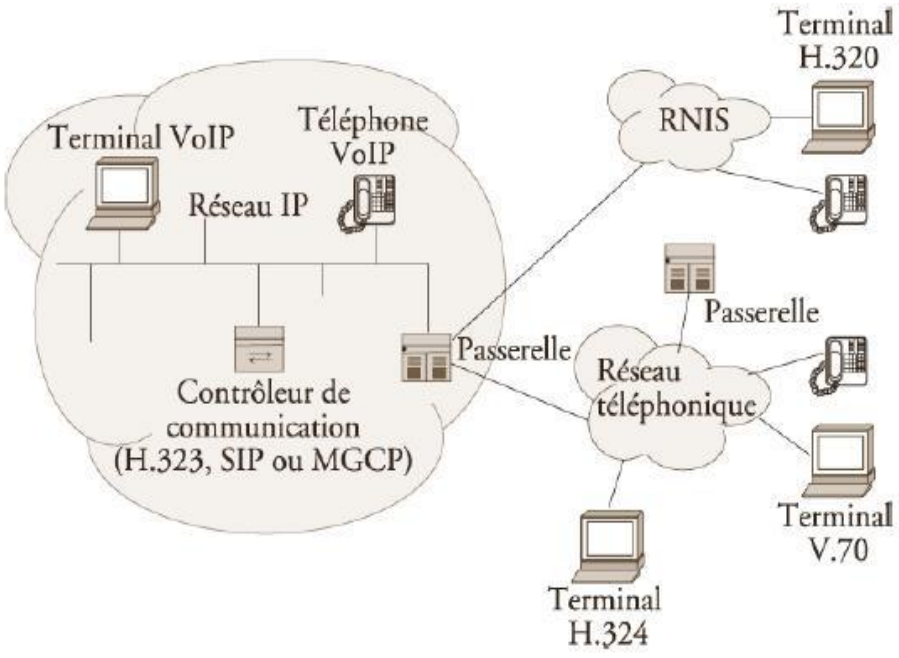


Figure-2.2 : schéma générale de l'utilisation de la VOIP en entreprise

II.1.3. Principe de fonctionnement:

Depuis nombreuses années, il est possible de transmettre un signal à une destination éloignée sous forme de données numériques. Avant la transmission, il faut numériser le signal à l'aide d'un CAN (convertisseur analogique-numérique). Le signal est ensuite transmis, pour être utilisable, il doit être transformé de nouveau en un signal analogique, à l'aide d'un CNA (convertisseur numérique-analogique).

La VOIP fonctionne par numérisation de la voix, puis par reconversion des paquets numériques en voix à l'arrivée. Le format numérique est plus facile à contrôler, il peut être compressé, routé et converti en un nouveau format meilleur. Le signal numérique est plus tolérant au bruit que l'analogique.

Les réseaux TCP/IP sont des supports de circulation de paquets IP contenant un en-tête (pour contrôler la communication) et une charge utile pour transporter les données.

Il existe plusieurs protocoles qui peuvent supporter la voix sur IP tel que le H.323, SIP et MGCP.
Les deux protocoles les plus utilisées actuellement dans les solutions VoIP présentes sur le marché sont le H.323 et le SIP.

II.2. Protocole H.323:

II.2.1 Description générale du protocole H.323 :

Le standard H.323 fournit, depuis son approbation en 1996, un cadre pour les communications audio, vidéo et de données sur les réseaux IP. Il a été développé par l'ITU (International Telecommunications Union) pour les réseaux qui ne garantissent pas une qualité de service (QoS), tels qu'IP IPX sur Ethernet, Fast Ethernet et Token Ring. Il est présent dans plus de 30 produits et il concerne le contrôle des appels, la gestion multimédia, la gestion de la bande passante pour les conférences point-à-point et multipoints. H.323 traite également de l'interfaçage entre le LAN et les autres réseaux.

Le transport de l'information s'appuie sur le protocole RTP qui transporte la voix, la vidéo ou les données numérisées par les codecs. Les messages RTCP

peuvent être utilisés pour le contrôle de la qualité, ou la renégociation des codecs si, par exemple, la bande passante diminue.

Une communication H.323 se déroule en cinq phases : l'établissement d'appel, l'échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource reservation Protocol), l'établissement de la communication audio-visuelle, l'invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.) et enfin la libération de l'appel.

II.2.2 Rôle des composants:

L'infrastructure H.323 repose sur quatre composants principaux : les terminaux, les Gateways, les Gatekeepers, et les MCU (Multipoint Control Units).

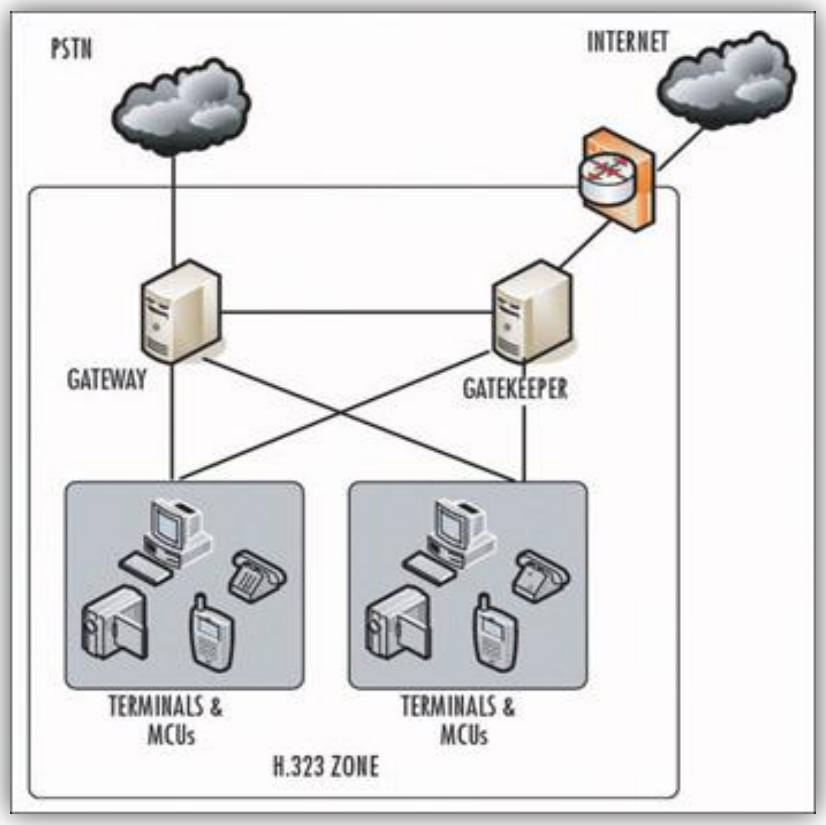


Figure 2.3: Les composants de l'architecture H.323

II.2.2.1 Les terminaux H.323:

Le terminal peut être un ordinateur, un combiné téléphonique, un terminal spécialisé pour la vidéoconférence ou encore un télécopieur sur Internet. Le minimum imposé par H.323 est qu'il mette en œuvre la norme de compression de la parole G.711, qu'il utilise le protocole H.245 pour la négociation de l'ouverture d'un canal et l'établissement des paramètres de la communication, ainsi que le protocole de signalisation Q.931 pour l'établissement et l'arrêt des communications.

Le terminal possède également des fonctions optionnelles, notamment, pour le travail en groupe et le partage des documents. Il existe deux types de terminaux H.323, l'un de haute qualité (pour une utilisation sur LAN), l'autre optimisé pour de petites largeurs de bandes (28,8/33,6 kbit/s – G.723.1 et H.263).

II.2.2.2 Gateway ou les passerelles vers des réseaux classiques (RTC, RNIS, GSM etc.):

Les passerelles H.323 assurent l'interconnexion avec les autres réseaux, ex: (H.320/RNIS), les modems H.324, téléphones classiques, etc. Elles assurent la correspondance de signalisation de Q.931, la correspondance des signaux de contrôle et la cohésion entre les médias (multiplexage, correspondance des débits, transcodage audio).

II.2.2.3 Gatekeeper ou les portiers:

Dans la norme H323, Le Gatekeeper est le point d'entrée au réseau pour un client H.323. Il définit une zone sur le réseau, appelée zone H.323 (voir **Figure 2.4** ci-dessous), regroupant plusieurs terminaux, Gateways et MCU dont il gère le trafic, le routage LAN, et l'allocation de la bande passante. Les clients ou les Gateway s'enregistrent auprès du Gatekeeper dès l'activation de celui-ci, ce qui leur permet de retrouver n'importe quel autre utilisateur à travers son identifiant fixe obtenu auprès de son Gatekeeper de rattachement**.**

- Le Gatekeeper a pour fonction :
  - La translation des alias H.323 vers des adresses IP, selon les spécifications RAS (Registration/Admission/Status) ;
  - Le contrôle d'accès, en interdisant les utilisateurs et les sessions non autorisés ;
  - Et la gestion de la bande passante, permettant à l'administrateur du réseau de limiter le nombre de visioconférences simultanées.

Concrètement une fraction de la bande passante est allouée à la visioconférence pour ne pas gêner les applications critiques sur le LAN et le support des conférences multipoint adhoc.

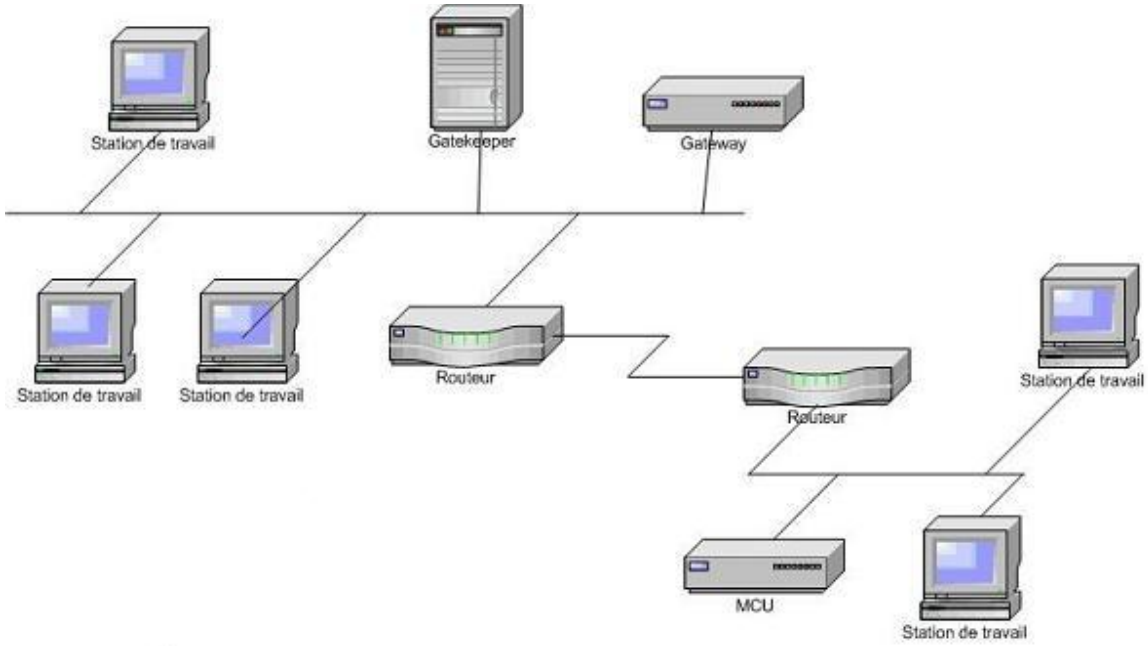


Figure 2.4: La zone H.323

II.2.2.4 Les MCU:

Les contrôleurs multipoint appelés MCU (Multipoint Control Unit) offrent aux utilisateurs la possibilité de faire des visioconférences à trois terminaux et plus en « présence continue » ou en « activation à la voix ». Une MCU consiste en un Contrôleur Multipoint (MC), auquel est rajouté un ou plusieurs Processeurs Multipoints (MP) (**voir Figure 2.5**). Le MC prend en charge les négociations H.245 entre tous les terminaux pour harmoniser les paramètres audio et vidéo de chacun. Il contrôle également les ressources utilisées. Mais le MC ne traite pas directement avec les flux audio, vidéo ou données, c'est le MP qui se charge de récupérer les flux et de leurs faire subir les traitements nécessaires. Un MC peut contrôler plusieurs MP distribués sur le réseau et faisant partie d'autres MCU.

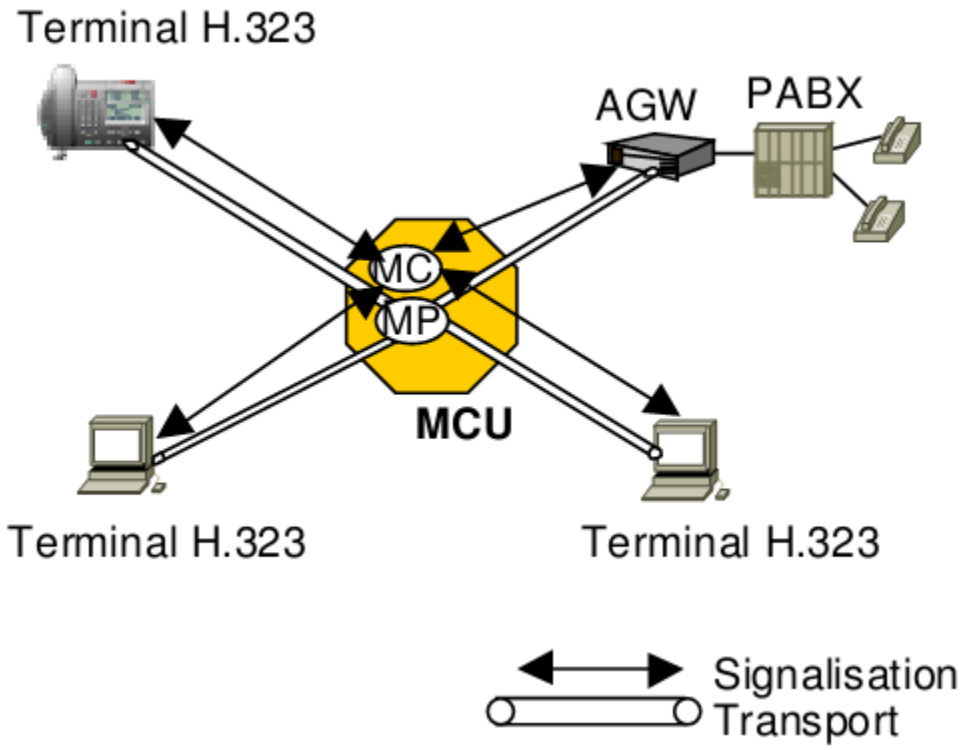


Figure 2.5 - MCU centralisé

II.2.3. Avantages et inconvénients de la technologie H323 :

La technologie H.323 possède des avantages et des inconvénients. Parmi les avantages, nous citons :

- **Gestion de la bande passante :** H.323 permet une bonne gestion de la bande passante en posant des limites au flux audio/vidéo afin d'assurer le bon fonctionnement des applications critiques sur le LAN. Chaque terminal H.323 peut procéder à l'ajustement de la bande passante et la modification du débit en fonction du comportement du réseau en temps réel (latence, perte de paquets et gigue).
- **Support Multipoint :** H.323 permet de faire des conférences multipoint via une structure centralisée de type MCU (Multipoint Control Unit) ou en mode ad-hoc.
- **Support Multicast :** H.323 permet également de faire des transmissions en multicast.

- **Interopérabilité :** H.323 permet aux utilisateurs de ne pas se préoccuper de la manière dont se font les communications, les paramètres (les codecs, le débit…) sont négociés de manière transparente.
- **Flexibilité :** une conférence H.323 peut inclure des terminaux hétérogènes (studio de visioconférence, PC, téléphones…) qui peuvent partager selon le cas, de la voix de la vidéo et même des données grâce aux spécifications T.120.

Les inconvénients de la technologie H.323 sont :

- La complexité de mise en œuvre et les problèmes d'architecture en ce qui concerne la convergence des services de téléphonie et d'Internet, ainsi qu'un manque de modularité et de souplesse.
- Comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité.

II.3. Protocole SIP:

II.3.1 Description générale du protocole SIP:

Le protocole SIP (Session Initiation Protocol) est un protocole normalisé et standardisé par l'IETF (décrit par le RFC 3261 qui rend obsolète le RFC 2543, et complété par le RFC 3265) qui a été conçu pour établir, modifier et terminer des sessions multimédia. Il se charge de l'authentification et de la localisation des multiples participants. Il se charge également de la négociation sur les types de média utilisables par les différents participants en encapsulant des messages SDP (Session Description Protocol). SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo. SIP étant indépendant de la transmission des données, tout type de données et de protocoles peut être utilisé pour cet échange. Cependant le protocole RTP (Real-time Transport Protocol) assure le plus souvent les sessions audio et vidéo. SIP remplace progressivement H323.

SIP est le standard ouvert de VOIP, interopérable, le plus étendu et vise à devenir le standard des télécommunications multimédia (son, image, etc.). Skype par exemple, qui utilise un format propriétaire, ne permet pas l'interopérabilité avec un autre réseau de voix sur IP et ne fournit que des passerelles payantes vers la téléphonie standard. SIP n'est donc pas

seulement destiné à la VOIP mais pour de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo.

II.3.2 Principe de fonctionnement:

On s'approfondira à expliquer les différents aspects, caractéristiques qui font du protocole SIP un bon choix pour l'établissement de la session, les principales caractéristiques du protocole SIP sont :

- **Fixation d'un compte SIP:** Il est important de s'assurer que la personne appelée soit toujours joignable. Pour cela, un compte SIP sera associé à un nom unique.
- **Changement des caractéristiques durant une session:**
  Un utilisateur doit pouvoir modifier les caractéristiques d'un appel en cours. Par exemple, un appel initialement configuré en (voix uniquement) peut être modifié en (voix + vidéo).
- **Différents modes de communication:**
  Avec SIP, les utilisateurs qui ouvrent une session peuvent communiquer en mode point à point, en mode diffusif ou dans un mode combinant ceux-ci.:
  - ✓ **Mode Point à point :** on parle dans ce cas là d'«unicast » qui correspond à la communication entre deux machines.
  - ✓ **Mode diffusif :** on parle dans ce cas là de « multicast » (plusieurs utilisateurs via une unité de contrôle MCU – Multipoint Control Unit).
  - ✓ **Combinatoire :** combine les deux modes précédents. Plusieurs utilisateurs interconnectés en multicast via un réseau à maillage complet de connexion.
- **Gestion des participants:**
  Durant une session d'appel, de nouveaux participants peuvent joindre les participants d'une session déjà ouverte en participant directement, en étant transférés ou en étant mis en attente.

- **Négociation des médias supportés:**

Cela permet à un groupe durant un appel de négocier sur les types de médias supportés. Par exemple, la vidéo peut être ou ne pas être supportée lors d'une session.

- **Adressage:**
  Les utilisateurs disposant d'un numéro (compte) SIP disposent d'une adresse ressemblant à une adresse mail (**sip:**numéro@serveursip.com). Le numéro SIP est unique pour chaque utilisateur.

- **Modèle d'échange:**
  Le protocole SIP repose sur un modèle Requête/Réponse. Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes. La liste des requêtes échangées est la suivante :
  - ✓ **Invite :** cette requête indique que l'application (ou utilisateur) correspondante à l'url SIP spécifié est invité à participer à une session. Le corps du message décrit cette session (par ex : média supportés par l'appelant). En cas de réponse favorable, l'invité doit spécifier les médias qu'il supporte.
  - ✓ **Ack :** cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête Invite.
  - ✓ **Options :** un proxy server en mesure de contacter l'UAS (terminal) appelé, doit répondre à une requête Options en précisant ses capacités à contacter le même terminal.
  - ✓ **Bye :** cette requête est utilisée par le terminal de l'appelé à fin de signaler qu'il souhaite mettre un terme à la session.
  - ✓ **Cancel :** cette requête est envoyée par un terminal ou un proxy server à fin d'annuler une requête non validée par une réponse finale comme, par exemple, si une machine ayant été invitée à participer à une session, et ayant accepté l'invitation ne reçoit pas de requête Ack, alors elle émet une requête Cancel.
  - ✓ **Register :** cette méthode est utilisée par le client pour enregistrer l'adresse listée dans l'URL TO par le serveur auquel il est relié.

- **Codes d'erreurs:**

Une réponse à une requête est caractérisée, par un code et un motif, appelés respectivement code d'état et raison phrase. Un code d'état est un entier codé sur 3 digits indiquant un résultat à l'issue de la réception d'une requête. Ce résultat est précisé par une phrase, textbased (UTF-8), expliquant le motif du refus ou de l'acceptation de la requête. Le code d'état est donc destiné à l'automate gérant l'établissement des sessions SIP et les motifs aux programmeurs. Il existe 6 classes de réponses et donc de codes d'état, représentées par le premier digit :

- ✓ **1xx** = Information - La requête a été reçue et continue à être traitée.
- ✓ **2xx** = Succès - L'action a été reçue avec succès, comprise et acceptée.
- ✓ **3xx** = Redirection - Une autre action doit être menée afin de valider la requête.
- ✓ **4xx** = Erreur du client - La requête contient une syntaxe erronée ou ne peut pas être traitée par ce serveur.
- ✓ **5xx** = Erreur du serveur - Le serveur n'a pas réussi à traiter une requête apparemment correcte.
- ✓ **6xx** = Echec général - La requête ne peut être traitée par aucun serveur.

II. 3.3 Rôle des composants:

Dans un système SIP on trouve deux types de composantes, les agents utilisateurs (UAS, UAC) et un réseau de serveurs (Registrar, Proxy).

1. **L'UAS (User Agent Server)** représente l'agent de la partie appelée. C'est une application de type serveur qui contacte l'utilisateur lorsqu'une requête SIP est reçue. Et elle renvoie une réponse au nom de l'utilisateur.

2. **L'U.A.C (User Agent Client)** représente l'agent de la partie appelante. C'est une application de type client qui initie les requêtes.

3. **Le Registrar** est un serveur qui gère les requêtes REGISTER envoyées par les Users Agents pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données (**Figure 2.6**).

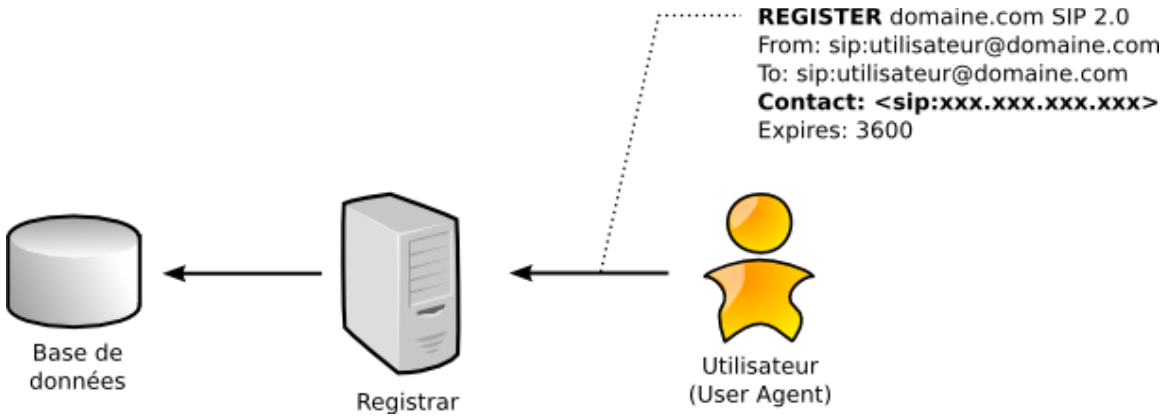
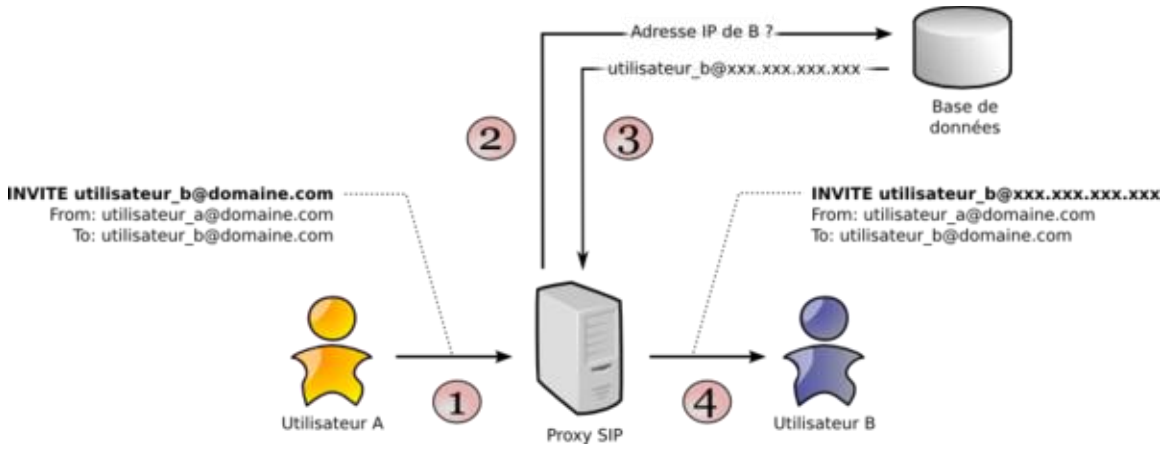


Figure 2.6: Enregistrement d'un utilisateur

4. Les URI SIP sont très similaires dans leur forme à des adresses email sip:utilisateur@domaine.com. Généralement, des mécanismes d'authentification permettent d'éviter que quiconque puisse s'enregistrer avec n'importe quelle URI.

5. Proxy SIP: Il sert d'être l'intermédiaire entre deux User Agents qui ne connaissent pas leurs emplacements respectifs (adresse IP). En effet, l'association URI-Adresse IP a été stockée préalablement dans une base de données par un Registrar. Le Proxy peut donc interroger cette base de données pour diriger les messages vers le destinataire. La **Figure 2.7** montre les étapes de l'interrogation du proxy la base de données.



1- envoie d'une requête INVITE au proxy.

2- Le Proxy interroge la base de donnée.

3- la base de donnée renvoie l'adresse IP du destinataire.

4- le proxy relaie le message au destinataire

Figure 2.7: Principe du protocole SIP

Le Proxy se contente de relayer uniquement les messages SIP pour établir, contrôler et terminer la session (voir **Figure 2.7**). Une fois la session établie, les données, par exemple un flux RTP pour la VOIP, ne transitent pas par le serveur Proxy. Elles sont échangées directement entre les User Agents.

II. 3.4 Avantages et inconvénients:

Ouvert, standard, simple et flexible sont les principales atouts du protocole SIP, voilà en détails ces différents avantages :

- ✓ Ouvert : les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement.
- ✓ Standard : l'IETF a normalisé le protocole et son évolution continue par la création ou l'évolution d'autres protocoles qui fonctionnent avec SIP.
- ✓ Simple : SIP est simple et très similaire à http.
- ✓ Flexible : SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, mais aussi musique, réalité virtuelle, etc.).
- ✓ Téléphonie sur réseaux publics : il existe de nombreuses passerelles (services payants) vers le réseau public de téléphonie (RTC, GSM, etc.) permettant d'émettre ou de recevoir des appels vocaux.

- ✓ Points communs avec H323 : l'utilisation du protocole RTP et quelques codecs son et vidéo sont en commun.

Par contre une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les User Agents peut perturber le fonctionnement ou générer du trafic superflu sur le réseau. Un autre inconvénient est le faible nombre d'utilisateurs : SIP est encore peu connu et utilisé par le grand public, n'ayant pas atteint une masse critique, il ne bénéficie pas de l'effet réseau.

II.4. Protocoles de transport:

Nous décrivons deux autres protocoles de transport utilisés dans la voix sur IP à savoir l'RTP et le RTCP.

II.4.1 Le protocole RTP :

Le protocole RTP a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie. Ceci de façon à reformer les flux avec ses caractéristiques de départ. RTP est un protocole de bout en bout, volontairement incomplet et malléable pour s'adapter aux besoins des applications. Il sera intégré dans le noyau de l'application. Il laisse la responsabilité du contrôle aux équipements d'extrémité. Il est aussi un protocole adapté aux applications présentant des propriétés temps réel. Il permet ainsi de Transporter les applications audio et vidéo dans des trames (avec des dimensions qui sont dépendantes des codecs qui effectuent la numérisation) ***(Voir Figure 2-8)***. Ces trames sont incluses dans des paquets afin d'être transportées et doivent, de ce fait, être récupérées facilement au moment de la phase de segmentation des paquets afin que l'application soit décodée correctement.

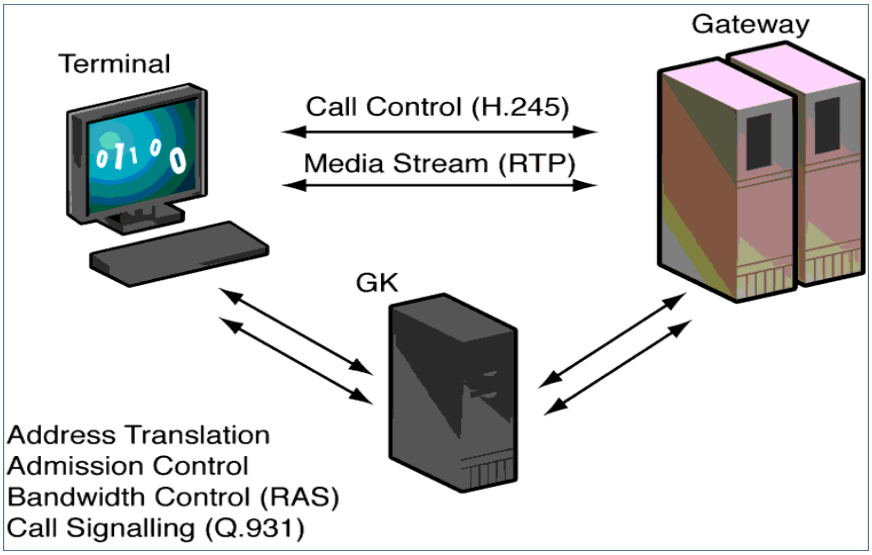


Figure 2-8: La transmission des flux média avec RTP

II.4.1.1 Avantages et inconvénients:

Le protocole RTP permet de reconstituer la base de temps des différents flux multimédia (audio, vidéo, etc.); de 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.

II.4.2 Le protocole RTCP:

Parmi les principales fonctions qu'offre le protocole RTCP sont les suivants :

- Une synchronisation supplémentaire entre les médias : Par exemple, la voix, l'image ou même des applications numérisées sur plusieurs niveaux hiérarchiques peuvent voir les flots gérées et suivre des chemins différents.
- L'identification des participants à une session.
- Le contrôle de la session : en effet le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement de fournir une indication sur leur comportement.

II.4.2.1 Point fort et limite du protocole RTCP :

Le protocole de RTCP est adapté pour la transmission de données temps réel. Il permet d'effectuer un contrôle permanant sur une session et ces participants. Par contre il fonctionne en stratégie bout à bout. Et il ne peut pas contrôler l'élément principal de la communication "le réseau".

II.5. Points forts et limites de la voix sur IP :

Différentes sont les raisons qui peuvent pousser les entreprises à s'orienter vers la VOIP comme solution pour la téléphonie.

Les avantages les plus marqués sont :

- **Réduction des coûts :** En effet le trafic véhiculé à travers le réseau RTC est plus couteux que sur un réseau IP.
- **Standards ouverts :** La VOIP n'est plus uniquement H323, mais un usage multi-protocoles selon les besoins de services nécessaires. Par exemple, H323 fonctionne en mode égale à égale alors que MGCP fonctionne en mode centralisé. Ces différences de conception offrent immédiatement une différence dans l'exploitation des terminaisons considérées.
- **Un réseau voix, vidéo et données (à la fois) :** Grace à l'intégration de la voix comme une application supplémentaire dans un réseau IP, ce dernier va simplifier la gestion des trois applications (voix, réseau et vidéo) par un seul transport IP.
- **Un service PABX distribué ou centralisé :** Les PABX en réseau bénéficient de services centralisés tel que la messagerie vocale et la taxation. Cette même centralisation continue à être assurée sur un réseau VoIP sans limitation du nombre de canaux.

Les points faibles de la voix sur IP sont :

- **Fiabilité et qualité sonore :** un des problèmes les plus importants de la téléphonie sur IP est la qualité de la retransmission qui n'est pas encore optimale, surtout dans le cas de perte de paquet.
- **Dépendance de l'infrastructure technologique et support administratif exigeant :** les centres de relations IP peuvent être particulièrement vulnérables en cas d'improductivité de l'infrastructure. Par exemple, si la base de données n'est pas disponible, les centres ne peuvent tout simplement pas recevoir d'appels.

La convergence de la voix et des données dans un seul système signifie que la stabilité du système devient plus importante que jamais et l'organisation doit être préparée à travailler avec efficience ou à encourir les conséquences.

- **Vol :** les attaquants qui parviennent à accéder à un serveur VOIP peuvent également accéder aux messages vocaux stockés et au même au service téléphonique pour écouter des conversations ou effectuer des appels gratuits aux noms d'autres comptes.
- **Attaque de virus :** si un serveur VOIP est infecté par un virus, les utilisateurs risquent de ne plus pouvoir accéder au réseau téléphonique. Le virus peut également infecter d'autres ordinateurs connectés au système.

Conclusion

Comme on a pu le voir tout au long de ce chapitre, la VOIP est la solution la plus rentable pour effectuer des conversations. Actuellement il est évident que la VOIP va continuer à évoluer.

La téléphonie IP est une bonne solution en matière d'intégration, fiabilité et de coût. On a vu que la voix sur IP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. Chaque standard possède ses propres caractéristiques pour garantir une bonne qualité de service. En effet, le respect des contraintes temporelles est le facteur le plus important lors de transport de la voix.

Malgré que la normalisation n'ait pas atteint la maturité suffisante pour sa généralisation au niveau des réseaux IP, il n'est pas dangereux de miser sur ces standards vu qu'ils ont été acceptés par l'ensemble de la communauté de la téléphonie.

Pour finir lors de la mise en œuvre de cette technologie, il faut poser la question suivante : le développement de cette technologie représente t'il un risque ou une opportunité pour les utilisateurs et les opérateurs téléphoniques ?

Chapitre III:

La sécurité dans la VOIP

Introduction:

L'opportunité de migrer de la téléphonie classique vers la téléphonie IP, a offert plusieurs avantages pour les entreprises, et les a permirent de bénéficier de nouveaux services tel que la vidéoconférence et la transmission des données. L'intégration de ces services dans une seule plateforme nécessite plus de sécurité.

Dans ce chapitre, nous dériverons des attaques qui menacent la VoIP, et nous détaillerons quelques uns. Nous finirons par une description des bonnes pratiques pour sécuriser les communications de type voix sur IP.

Le système VoIP utilise l'Internet, et particulièrement le protocole IP. De ce fait les vulnérabilités de celui-ci.

Les attaques sur les réseaux VoIP peuvent être classées en deux types : les attaques internes et les attaques externes. Les attaques externes sont lancées par des personnes autres que celle qui participe à l'appel, et ils se produisent généralement quand les paquets VoIP traversent un réseau peu fiable et/ou l'appel passe par un réseau tiers durant le transfert des paquets. Les attaques internes s'effectuent directement du réseau local dans lequel se trouve l'attaquant.

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

III.1- Notions de sécurité:

Nous allons tout d'abord rappeler quelques notions sur la mise en œuvre d'une politique de sécurité et sur les attaques existantes.

III.1.1 Mise en place d'une politique de sécurité:

La mise en œuvre d'une politique de sécurité globale est assez difficile, essentiellement par la diversité des aspects à considérer. Une politique de sécurité peut se définir par un certain nombre de caractéristiques : les niveaux où elle intervient, les objectifs de cette politique et enfin les outils utilisés pour assurer cette sécurité.

Chaque aspect différent doit être pris en compte, de façon à atteindre les objectifs de sécurité désirés, en utilisant de façon coordonnée les différents outils à disposition.

Nous allons tout d'abord parler des différents aspects d'une politique de sécurité, Avant de définir les objectifs visés, puis de voir les outils disponibles pour appliquer cette politique.

III.1.1.1 Différents aspects de la sécurité:

Une politique de sécurité s'élabore à plusieurs niveaux.

- On va tout d'abord sécuriser l'accès aux données de façon logicielle (authentification, contrôle d'intégrité).
- On va également sécuriser l'accès physique aux données : serveurs placés dans des salles blindées (qui empêchent les ondes électromagnétiques d'être captées) avec badge d'accès…
- Un aspect très important pour assurer la sécurité des données d'une entreprise est de sensibiliser les utilisateurs aux notions de sécurité, de façon à limiter les comportements à risque : si tout le monde peut accéder aux salles de serveurs, peut imposte qu'elles soient sécurisées !

  De même, si les utilisateurs laissent leur mot de passe écrit à côté de leur PC, son utilité est limitée…
- Enfin, il est essentiel pour un responsable de sécurité de s'informer continuellement, des nouvelles attaques existantes, des outils disponibles…de façon à pouvoir maintenir à jour son système de sécurité et à combler les brèches de sécurité qui pourraient exister.

III.1.1.2 Objectifs:

Les objectifs d'une politique de sécurité sont de garantir la sécurité des informations et du réseau de l'entreprise.

Ces impératifs peuvent être définis à plusieurs niveaux :

Disponibilité : les données doivent rester accessibles aux utilisateurs (une attaque de type Dos, par exemple, vise à empêcher les utilisateurs normaux d'un service d'y accéder).

- **Confidentialité :** les données ne doivent être visibles que des personnes habilitées pour.
- **Intégrité :** il faut pouvoir garantir que les données protégées n'ont pas été modifiées par une personne non autorisée.
- **Non répudiation :** on doit pouvoir certifier, quand un fichier a subi des modifications, la personne qui l'a modifié

III.1.1.3 Outils:

Pour assurer une bonne protection des données d'une entreprise, différents outils sont disponibles. Ils ont en général utilisés ensemble, de façon à sécuriser les différentes failles existantes dans un système.

On va tout d'abord utiliser un firewall, qui permet de filtrer le trafic réseau entrant sur le réseau de l'entreprise.

Les antivirus seront plutôt utilisés sur les différentes machines branchées sur le réseau afin de vérifier si des virus ont pu se propager.

On dispose également d'agents d'authentification afin de contrôler l'accès aux données et aux ressources.

Enfin, ces dernières années, de plus en plus d'entreprises ont mis en place des systèmes de détection d'intrusion afin de limiter les attaques sur leurs réseaux.

De plus pour transporter les données entre différentes agences d'une même entreprise, les VPN (Virtual Private Network) ***(voir Figure 3-1)*** sont de plus en plus utilisés, car ils permettent un cryptage des données qui transitent sur un réseau public.

Tous ces outils sont complémentaires et surveillent un aspect précis du réseau qui peut être sensible aux attaques. Nous allons maintenant présenter rapidement les types d'attaques existants.

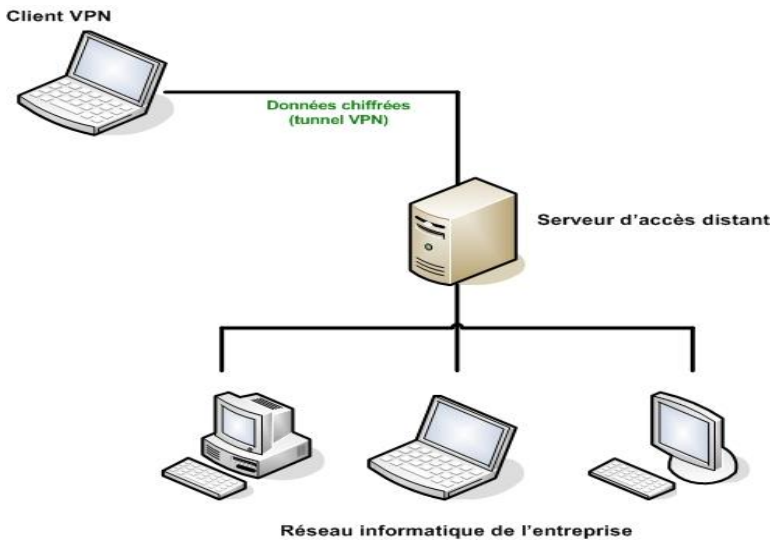


Figure 3-1 : Sécurisation des donnés avec le VPN

III.1.2. Les différents types d'attaque:

III.1.2.1. Attaques sur le protocole:

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, 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 ouvre 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.

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.

Les types d'attaques les plus fréquentes contre un system VoIP sont :

III.1.2.1.1 Sniffing:

Un reniflage (Sniffing) peut avoir comme conséquence un vol d'identité et la révélation d'informations confidentielles. Il permet également aux utilisateurs malveillants perfectionnés de rassembler des informations sur les systèmes VoIP. Ces informations peuvent par exemple être employées pour mettre en place une attaque contre d'autres systèmes ou données ***(voir Figure 3-2)***.

Plusieurs outils requis pour le sniffing, y compris pour le protocole H.323 et des plugins SIP, sont disponibles en open source.

Figure 3-2: exemple de sniffing d'une communication client serveur

III.1.2.1.2 Suivie des appels:

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

Pour réaliser cette attaque, L'attaquant doit être capable d'écouter le réseau et récupérer les messages INVITE et BYE (**voir Figure 3-3**).

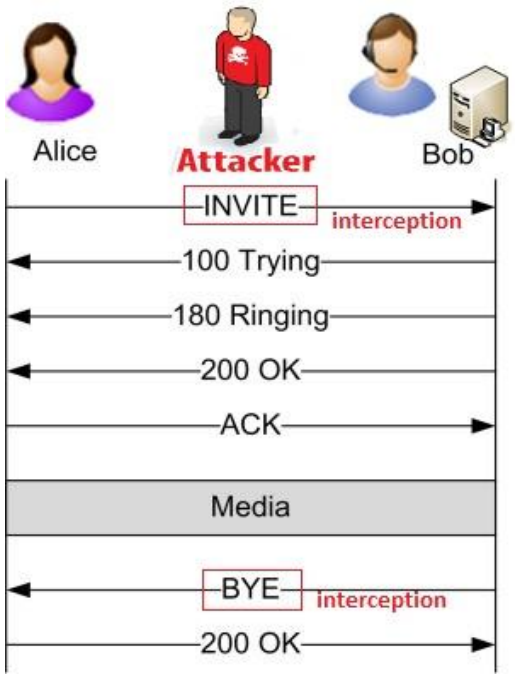


Figure 3-3: INVITE ET BEY ATTACK - interception de message INVITE et BYE

III.1.2.1.3 Injection de paquet RTP:

Cette attaque se fait au niveau du réseau LAN/VPN. Elle cible le serveur registrar, et a pour but de perturber 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 ***time stamp*** 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 times stamps des paquets RTP ***(voir Figure 3-4).***

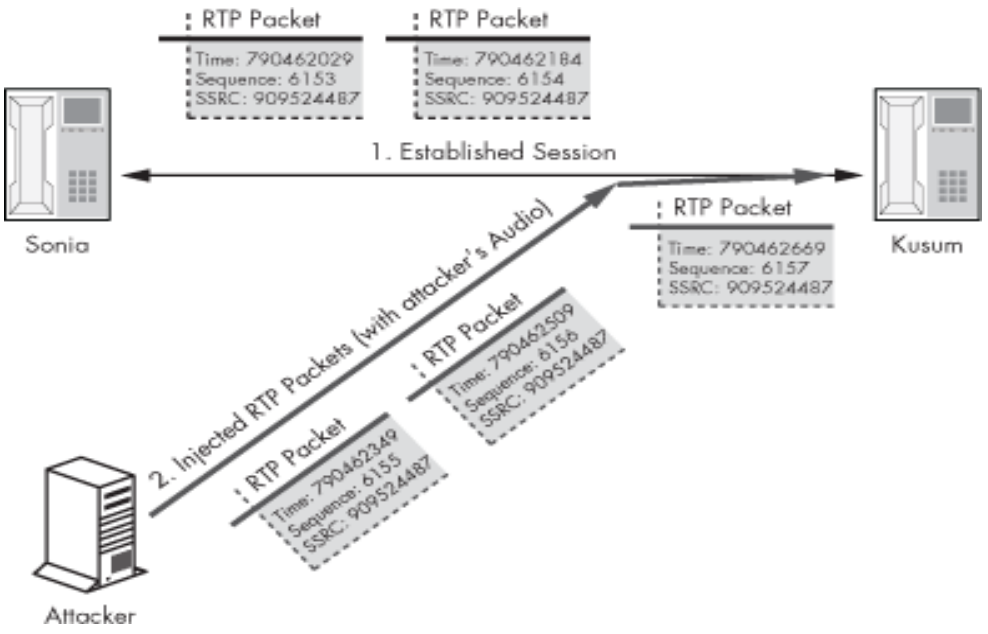


Figure 3-4: Injection RTP.

Il doit aussi être capable d'insérer des messages RTP qu'il a généré ayant un time stamp modifié.

III.1.2.1.4 Les Spam:

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

III.1.2.1.4.1 Call Spam : Ce type de spam est défini comme une masse de tentatives d'initiation de session (des requêtes INVITE) non sollicitées.

Généralement c'est un UAC (User Agent Client) qui lance, en parallèle, un grand nombre d'appels. Si l'appel est établi, l'application génère un ACK, rejoue une annonce préenregistrée, et ensuite termine l'appel.

III.1.2.1.4.2 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 « Subject » très grand, ou des requêtes INVITE avec un corps en format texte ou HTML ***(****voir l'exemple dans la* ***Figure 3-5)***.

```
Code View: Scroll / Show All

INVITE sip:Bob1@192.168.10.10:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.10.10:5060;branch=z9hG4bK00002000005
From: Spammer <sip:spammer1@10.10.10.10:5060>;tag=2345
To: Bob <sip:Bob1@192.168.10.10>
Call-Id: 9252226543-0001
CSeq: 1 INVITE
Subject: Hi there, buy a cool stuff in our website www.spam-example.com
Contact: <sip:spammer1@10.10.10.10>
Expires: 1200
Max-Forwards: 70
Content-Type: application/sdp
Content-Length: 143

======================================================================
MESSAGE sip:Bob1@192.168.10.10:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.10.10:5060;branch=z9hG4bK00002000005
From: Spammer <sip:spammer1@10.10.10.10:5060>;tag=2345
To: Bob <sip:Bob1@192.168.10.10>
Call-Id: 9252226543-0001
CSeq: 1 MESSAGE
Max-Forwards: 70
Content-Type: test/plain
Content-Length: 25

Hi there, buy a cool stuff in our website www.spam-example.com
```

Figure 3-5: Exemple de IM SPAM ATTACK

Bien-sûr, l'IM spam est beaucoup plus intrusif que le spam email, car dans les systèmes actuels, les IMs apparaissent automatiquement sous forme de pop-up à l'utilisateur.

III.1.2.1.4 .3 Presence Spam (SPPP) :

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 (voir l'exemple sur la ***Figure 3-6***). L'IM Spam est différent du Presence Spam dans le fait que ce dernier ne transmet pas réellement de contenu dans les messages.

```
SUBSCRIBE sip:bob@example.com SIP/2.0
Event: presence
To: sip:bob@example.com
From: sip:buy-cool-dvds-and-games@spam-example.com
Contact: sip:buy-cool-dvds-and-games@spam-example.com
Call-ID: knsd08alas9dy@3.4.5.6
CSeq: 1 SUBSCRIBE
Expires: 3600
Content-Length: 0
```

Figure 3-6: Exemple PRESENCE SPAM ATTACK

Dans cette exemple le spammer génère une requête d'enregistrement avec le ID: `(sip:buy-cool-dvds-and-games@spam-example.com`, et ce bref message peut être transmis à l'utilisateur, même si le spammeur na pas la permission d'accéder presence. En tant que tel, le spam de présence peut être considéré comme une forme de messages instantanés non sollicités.

III.1.2.1.5 Le déni de service (DOS : Denial of service):

C'est, d'une manière générale, l'attaque qui vise à rendre une application informatique ou un équipement informatique incapable de répondre aux requêtes de ses utilisateurs et donc hors d'usage.

Dans une attaque de type DoS flood attack, les ressources d'un serveur ou d'un réseau sont épuisées par un flot de paquets. Un seul attaquant visant à envoyer un flot de paquets peut être identifié et isolé assez facilement. Cependant l'approche de choix pour les attaquants a évolué vers un déni de service distribué (DDoS). Une attaque DDoS repose sur une distribution d'attaques DoS voir la ***Figure 3-7***.

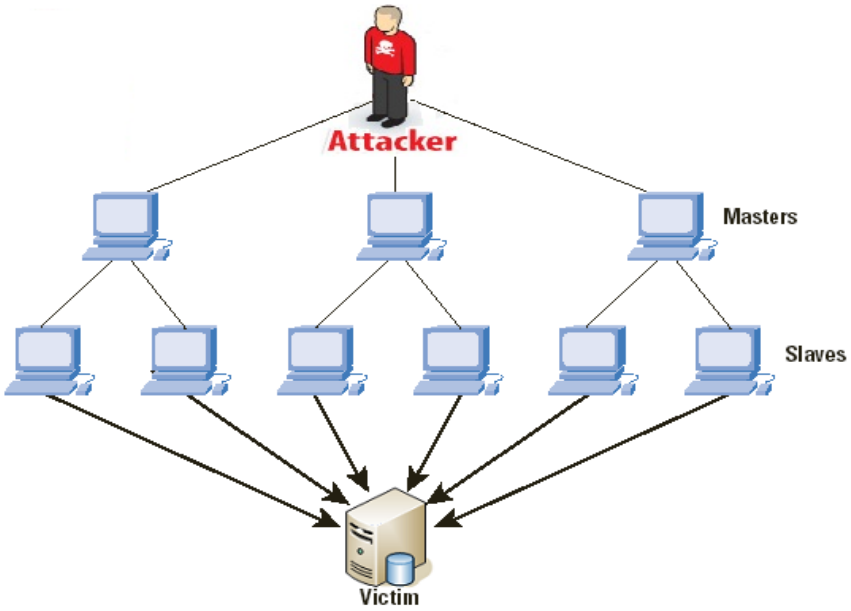


Figure 3-7 : ATTACK DDOS

Une attaque de type DoS peut s'effectuer à plusieurs niveaux soit :

III.1.2.1.5.1 Couche réseau :

- **IP Flooding :** Le but de l'IP Flooding est d'envoyer une multitude de paquets IP vers une même destination de telle sorte que le traitement de ces paquets empêche une entité du réseau (un routeur ou la station destinatrice) de traiter les paquets IP légitimes.
- **Fragmentation des paquets IP :** Par la fragmentation des paquets, il est possible de rendre hors service de nombreux systèmes d'exploitation et dispositif VoIP par le biais de la consommation des ressources. Il existe de nombreuses variantes d'attaques par fragmentation, parmi les plus populaires teardrop, opentear, nestea, jolt, boink, et Ping of death.

III.1.2.1.5.2 Couche transport :

- **L'UDP Flooding Attacks :** Le principe de cette attaque est qu'un attaquant envoie un grand nombre de requêtes UDP vers une machine. Presque touts les dispositifs utilisant le protocole SIP fonctionnent au dessus du protocole UDP, ce qui en fait d'elles des cibles. De nombreux dispositifs de VoIP et de systèmes d'exploitation peuvent être paralysés grâce à des paquets UDP

Flooding visant l'écoute du port SIP (5060) ou d'autres ports ***(voir Figure 3-8).***

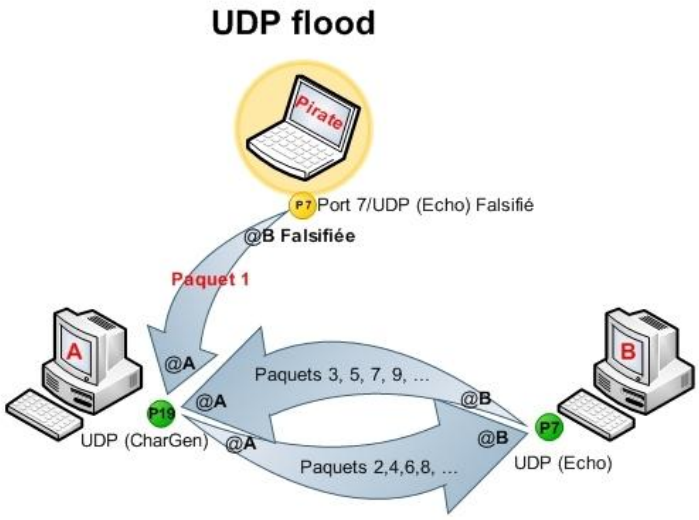


Figure 3-8: UDP FLOOD ATTACK

- **TCP SYN floods:** est une attaque visant le protocole TCP et plus exactement la phase d'établissement de connexion. Celle ci consiste en trois sous étapes :
  1. Le client envoie un paquet SYN au serveur.
  2. Le serveur répond avec un paquet SYN-ACK.
  3. Le client envoie un paquet ACK au serveur.

L'attaque consiste en l'envoie d'un grand nombre de paquets SYN. La victime va alors répondre par un message SYN-ACK d'acquittement. Pour terminer la connexion TCP, la victime ensuite va attendre pendant une période de temps la réponse par le biais d'un paquet ACK. C'est là le cœur de l'attaque parce que les ACK final ne sont jamais envoyés, et par la suite, la mémoire système se remplit rapidement et consomme toutes les ressources disponibles à ces demandes non valides. Le résultat final est que le serveur, le téléphone, ou le routeur ne sera pas en mesure de faire la distinction entre les faux SYN et les SYN légitimes d'une réelle connexion VoIP ***(Voir la Figure 3-9)***.

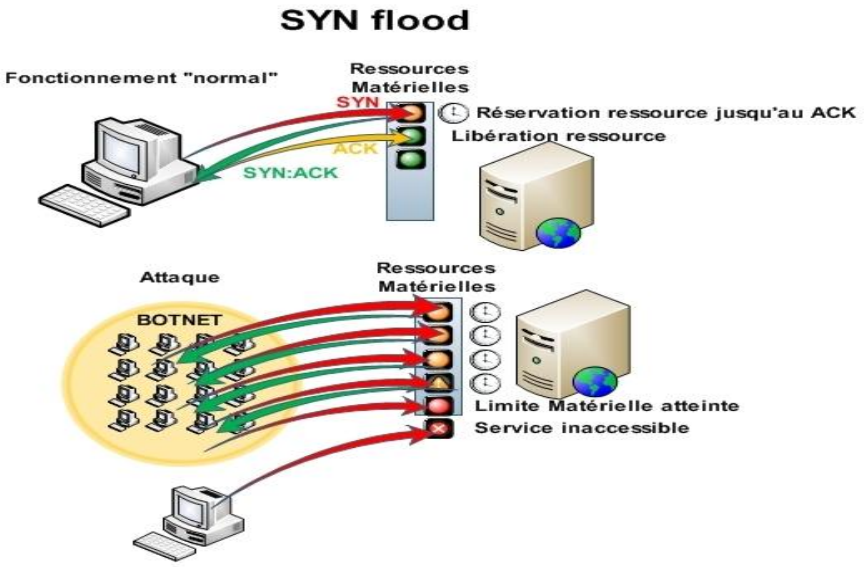


Figure 3-9: SYN flood ATTACK

III.1.2.1.5.3 Couche applications :

- ✓ **SIP Flooding :** Dans le cas de SIP, une attaque DoS peut être directement dirigée contre les utilisateurs finaux ou les dispositifs tels que téléphones IP, routeurs et proxy SIP, ou contre les serveurs concernés par le processus, en utilisant le mécanisme du protocole SIP ou d'autres techniques traditionnelles de DoS.

Voyons maintenant en détail les différentes formes d'attaque DoS :

- **CANCEL:**

  C'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.

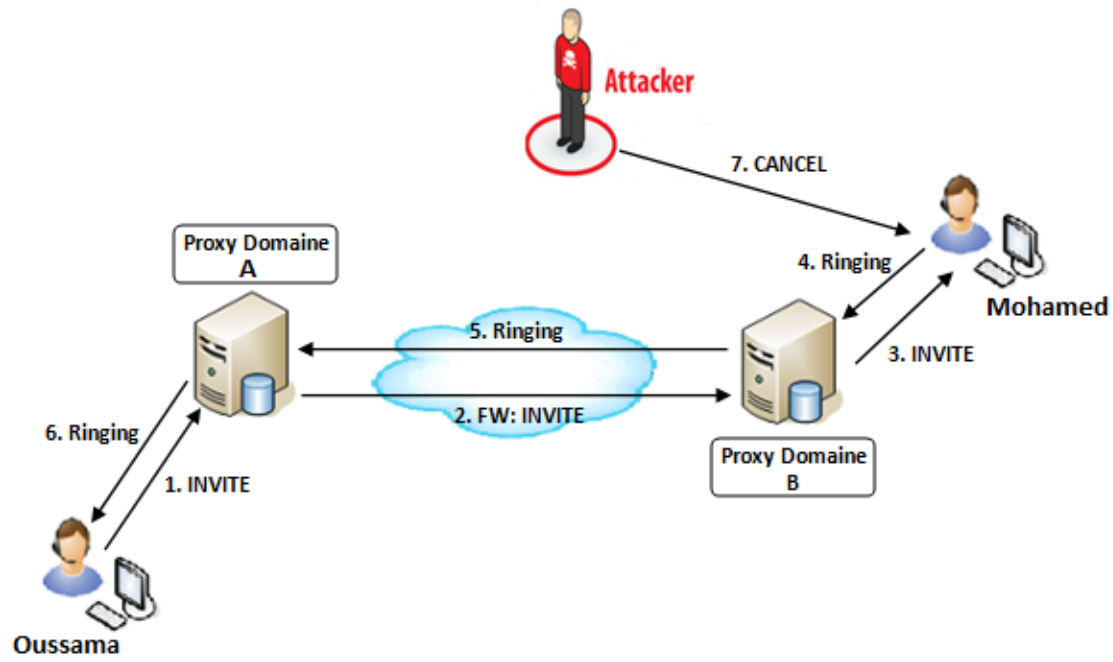


Figure 3.10: Attaque DoS via une requête CANCEL

La ***Figure 3.10*** suivante montre un scénario d'attaque DoS CANCEL, l'utilisateur Oussama initie l'appel, envoie une invitation **(1)** au proxy auquel il est rattaché. Le proxy du domaine A achemine la requête **(2)** au proxy qui est responsable de l'utilisateur Mohamed. Ensuite c'est le proxy du domaine B qui prend le relais et achemine la requête INVITE **(3)** qui arrive enfin à destination. Le dispositif de titi, quand il reçoit l'invitation, sonne **(4)**. Cette information est réacheminée jusqu'au dispositif de toto. L'attaquant qui surveille l'activité du proxy SIP du domaine B envoie une requête CANCEL **(7)** avant que titi n'ait pu envoyer la réponse OK qui accepte l'appel. Cette requête annulera la requête en attente (l'INVITE), l'appel n'a pas lieu.

- **REGISTER:**

  Le serveur d'enregistrement lui-même est une source potentielle de déni de service pour les utilisateurs. En effet ce serveur peut accepter des enregistrements de tous les dispositifs. Un nouvel enregistrement avec une «*» dans l'entête remplacera tous les précédents enregistrements pour ce dispositif. Les attaquants, de cette façon, peuvent supprimer l'enregistrement de quelques-uns des utilisateurs, ou tous, dans un

domaine, empêchant ainsi ces utilisateurs d'être invités à de nouvelles sessions.

Notez que cette fonction de suppression d'enregistrement d'un dispositif au profit d'un autre est un comportement voulu en SIP afin de permettre le transfert d'appel. Le dispositif de l'utilisateur doit pouvoir devenir le dispositif principal quand il vient en ligne. C'est un mécanisme très pratique pour les utilisateurs mais également pour les pirates.

III.1.2.1.6 Détournement d'appel (Call Hijacking):

Le Call Hijacking consiste à détourner un appel. Plusieurs fournisseurs de service VoIP utilisent le web comme interface permettant à l'utilisateur d'accéder à leur système téléphonique.

Un utilisateur authentifié peut changer les paramètres de ses transferts d'appel à travers cette interface web. C'est peut être pratique, mais un utilisateur malveillant peut utiliser le même moyen pour mener une attaque.

dans l'exemple de la ***Figure 3-11***, quand un agent SIP envoie un message INVITE pour initier un appel, l'attaquant envoie un message de redirection 3xx indiquant que l'appelé s'est déplacé et par la même occasion donne sa propre adresse comme adresse de renvoi. A partir de ce moment, tous les appels destinés à l'utilisateur sont transférés et c'est l'attaquant qui les reçoit.

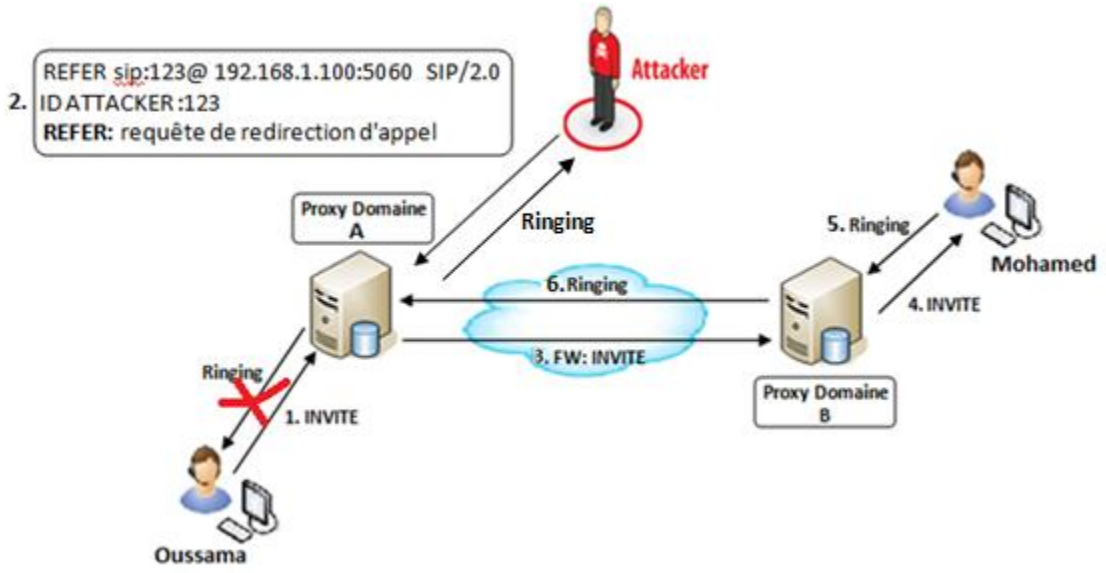


Figure 3-11: Détournement d'appel

III.1.2.1.7 L'écoute clandestine:

L'eaves dropping est l'écoute clandestine d'une conversation téléphonique. Un attaquant avec un accès au réseau VoIP peut sniffer le trafic et décoder la conversation vocale. Des outils tels que VOMIT (Voice Over MisconFigured Internet Telephones) permettent de réaliser cette attaque. VOMIT convertit les paquets sniffés en fichier .wav qui peut être réécouté avec n'importe quel lecteur de fichiers son.

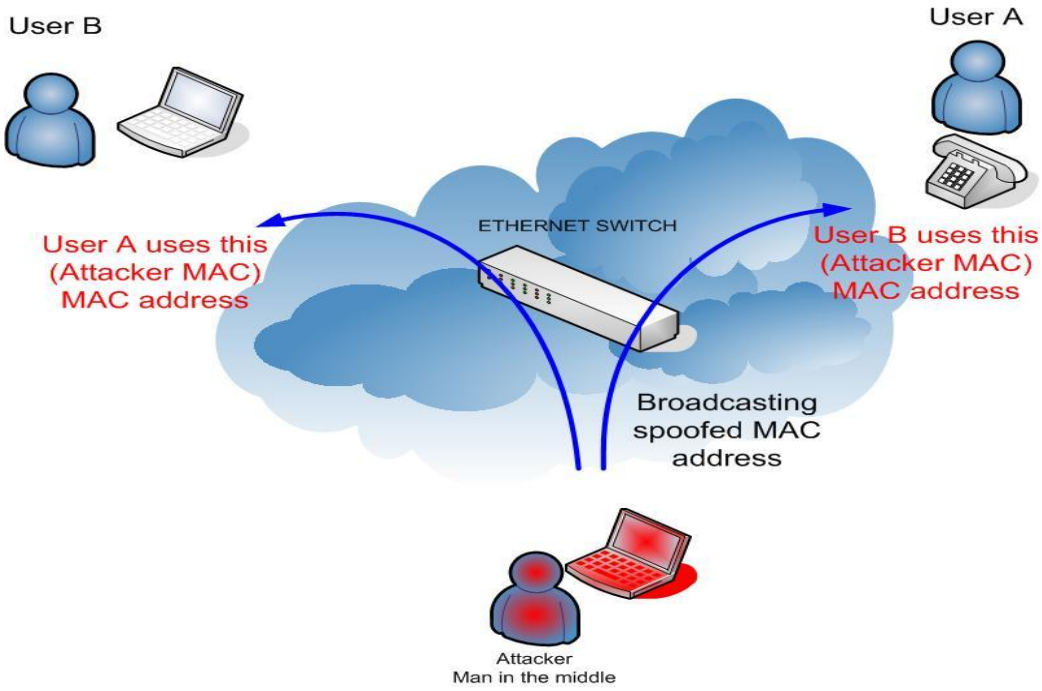


Figure 3.12: Exemple de détournement d'appel " Man in the middle"

Le principe de l'écoute clandestine est montré dans la ***Figure 3.12*** comme suit :

1. déterminer les adresses MAC des victimes (client serveur) par l'attaquant
2. Envoi d'une requête ARP non sollicités au client, pour l'informer du changement de l'adresse MAC du serveur VoIP à l'adresse MAC.
3. Envoi d'une requête ARP non sollicités au serveur, pour l'informer du changement de l'adresse MAC du client à l'adresse MAC.
4. Désactiver la vérification des adresses MAC sur la machine d'attaque afin que le trafic puisse circuler entre les 2 victimes.

III.2. Les vulnérabilités de 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.

III.2.1 Faiblesses dans la configuration des dispositifs de la VoIP:

Plusieurs dispositifs de la VoIP, dans leur configuration par défaut, peuvent avoir une variété de ports TCP et UDP ouverts. Les services fonctionnant sur ces ports peuvent être vulnérables aux attaques DoS ou buffer overflow.

Plusieurs dispositifs de la VoIP exécutent également un serveur WEB pour la gestion à distance qui peut être vulnérable aux attaques buffer overflow et à la divulgation d'informations.

Si les services accessibles ne sont pas configurés avec un mot de passe, un attaquant peut acquérir un accès non autorisé à ce dispositif.

Les services SNMP (Simple Network Management Protocol) offerts par ces dispositifs peuvent être vulnérables aux attaques de reconnaissance ou attaques d'overflow.

Plusieurs dispositifs de la VoIP sont configurés pour télécharger périodiquement un fichier de configuration depuis un serveur par TFTP ou d'autres mécanismes. Un attaquant peut potentiellement détourner ou mystifier cette connexion et tromper le dispositif qui va télécharger un fichier de configuration malveillant à la place du véritable fichier.

III.2.2 Les téléphone IP:

Un pirate peut compromettre un dispositif de téléphonie sur IP, par exemple un téléphone IP ***(voir Figure 3.13)***, un softphone ***(voir Figure 3.14)*** et autres programmes ou matériels clients. Généralement, il obtient les privilèges qui lui permettent de commander complètement la fonctionnalité du dispositif.

Figure 3.13: téléphone IP Cisco-7975G

Figure 3.14: Softphone eyeBeam

Les modifications faites à la configuration des logiciels de téléphonie IP peuvent permettre:

- ✓ Aux appels entrants d'être réorientés vers un autre point final sans que l'utilisateur soit au courant.
- ✓ 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.
- ✓ De compromettre la disponibilité du point final. Par exemple, ce dernier peut rejeter automatiquement toutes les requêtes d'appel, ou encore, éliminer tout déclenchement de notification tel qu'un son, une notification visuelle à l'arrivée d'un appel. Les appels peuvent également être interrompus à l'improviste (quelques téléphones IP permettent ceci via une interface web).

III.2.3 Les serveurs:

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.

III.2.4 Les vulnérabilités du système d'exploitation:

Ces vulnérabilités sont pour la plupart relatives au manque de sécurité lors de la phase initiale de développement du système d'exploitation et ne sont découvertes qu'après le lancement du produit.

Une des principales vulnérabilités des systèmes d'exploitation est le buffer overflow. Il permet à un attaquant de prendre le contrôle partiel ou complet de la machine.

Les dispositifs de la VoIP tels que les téléphones IP, Call Managers, Gateway et les serveurs proxy, héritent les mêmes vulnérabilités du système d'exploitation ou du firmware sur lequel ils tournent.

Il existe une centaine de vulnérabilités exploitables à distance sur Windows et même sur Linux. Un grand nombre de ces exploits sont disponibles librement et prêts à être téléchargés sur l'Internet.

Peu importe comment, une application de la VoIP s'avère être sûre, celle ci devient menacé si le système d'exploitation sur lequel elle tourne est compromis.

III.3. Sécurisation et bonne pratiques:

On déjà vu que les vulnérabilités existe au niveau protocolaire, application et systèmes d'exploitation. Pour cela, on a découpé la sécurisation aussi en trois niveaux : Sécurisation protocolaire, sécurisation de l'application et sécurisation du système de l'exploitation.

III.3.1 Sécurisation protocolaire:

La prévalence et la facilité de sniffer des paquets et d'autres techniques pour la capture des paquets IP sur un réseau pour la voix sur IP fait que le cryptage soit une nécessité. La sécurisation de la VoIP est à la protection des personnes qui sont interconnecté.

IPsec peut être utilisé pour réaliser deux objectifs. Garantir l'identité des deux points terminaux et protéger la voix une fois que les paquets quittent l'Intranet de l'entreprise. VOIPsec (VoIP utilisant IPsec) contribue à réduire les menaces (voir **Figure 3.15**), les sniffeurs de paquets, et de nombreux types de trafic « vocal analyze ». Combiné avec un pare-feu, IPsec fait que la VOIP soit plus sûr qu'une ligne téléphonique classique. Il est important de noter, toutefois, que IPsec n'est pas toujours un bon moyen pour certaines applications, et que certains protocoles doivent continuer à compter sur leurs propres dispositifs de sécurité.

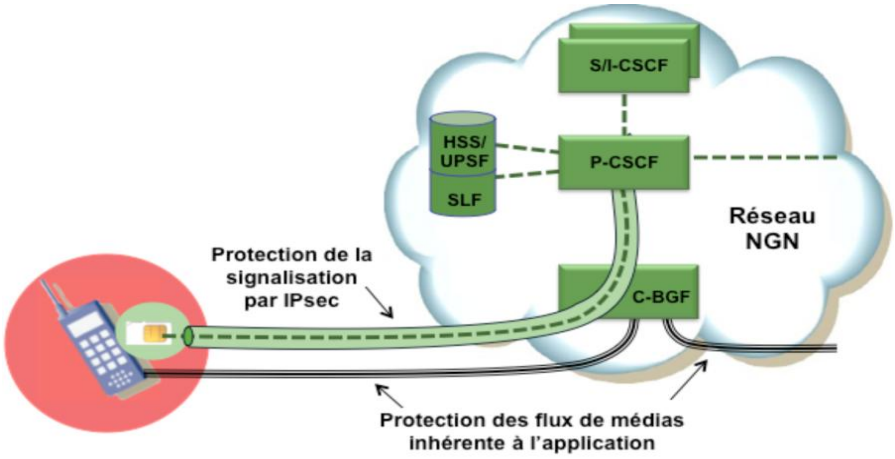


Figure 3.15: La Protection IPSec dans les réseaux IP

III.3.1.1 VoIP VPN:

Un VPN VoIP combine la voix sur IP et la technologie des réseaux virtuels privés pour offrir une méthode assurant la préservation de la prestation vocale. Puisque la VoIP transmet la voix numérisée en un flux de données, la solution VPN VoIP semble celle la plus approprié vu qu'elle offre le cryptage des données grâces a des mécanismes de cryptages, puisqu'elle permet d'offrir l'intégrité des paquets VoIP.

- **Cryptage aux points terminaux:**
  Vu que notre objectif est d'assurer la confidentialité et l'intégrité des clients, le mode choisie est donc le mode tunnel. Puisqu'il sécurise le paquet comme un tout (contrairement en mode transport qui ne sécurise que le payload IP). Le mode tunnel se base sur l'encapsulation de tout le paquet IP et ajoute un nouvel entête pour l'acheminement de ce dernier. Ce mode est généralement utilisé pour les routeur-to-routeur. En plus du mode tunnel, on choisi le protocole ESP qui lui a son tour va assurer le cryptage des données et donc la confidentialité contrairement au protocole AH qui lui ne permet que l'authentification des paquets et non le cryptage.

Dans ce cas, la solution qu'on propose est ESP mode tunnel qui sera appliqué uniquement sur les points de terminaison à la voix IP, c'est-a-dire le routeur. Ceci nous permettra donc de minimiser le nombre de machines qui seront impliquées dans le traitement engendré par la sécurité. De plus le nombre des clés nécessaires sera réduit.

III.3.1.2 Secure RTP ou SRTP:

SRTP est conçu pour sécuriser la multiplication à venir des échanges multimédias sur les réseaux. Il couvre les lacunes de protocoles de sécurité existants comme IPsec (IP Security), dont le mécanisme d'échanges de clés est trop lourd. Il aussi est bâti sur le protocole temps réel RTP (Real Time Transport Protocol). Il associe aussi une demi-douzaine de protocoles complémentaires. Il est donc compatible à la fois avec des protocoles d'initiation de session de voix sur IP tel que SIP (Session Initiation Protocol), ainsi que le protocole de diffusion de contenu multimédia en temps réel RTSP (Real Time Streaming Protocol). Mais, surtout, il s'adjoint les services du protocole de gestion de clé MIKEY (Multimedia Internet KEYing).

III.3.1.2.1 Service de sécurités offertes par SRTP:

Les principaux services offerts par SRTP sont :

- Rendre confidentielles les données RTP, que ce soit l'en-tête et la charge utile ou seulement la charge utile.
- Authentifier et vérifier l'intégrité des paquets RTP. L'émetteur calcule une empreinte du message à envoyer, puis l'envoie avec le message même.

- La protection contre le rejeu des paquets. Chaque récepteur tient à jour une liste de tous les indices des paquets reçus et bien authentifiés.

III.3.1.2.2 Principe de fonctionnement de SRTP:

Avec une gestion de clé appropriée, SRTP est sécurisé pour les applications unicast et multicast de RTP. En théorie, SRTP est une extension du protocole RTP dans lequel a été rajoutée des options de sécurité. En effet, il a pour but d'offrir plusieurs implémentations de cryptographie tout en limitant l'overhead lié à l'utilisation des chiffrements. Il propose des algorithmes qui monopoliseront au minimum les ressources et l'utilisation de la mémoire.
Surtout, il permet de rendre RTP indépendant des autres couches en ce qui concerne l'application de mécanismes de sécurité.

Pour implémenter les différents services de sécurité précités, SRTP utilise les composants principaux suivants :

- Une clé maîtresse utilisée pour générer des clés de session; Ces dernières seront utilisées pour chiffrer ou pour authentifier les paquets.
- Une fonction utilisée pour calculer les clés de session à partir de la clé maîtresse.
- Des clés aléatoires utilisées pour introduire une composante aléatoire afin de contrer les éventuels rejeu ou effets de mémoire.

SRTP utilise deux types de clés : clef de session et clef maîtresse. Par « clef de session » nous entendons une clef utilisée directement dans les transformations cryptographiques; et par « clef maîtresse », nous entendons une chaîne de bit aléatoire à partir desquelles les clefs de sessions sont dérivées par une voie sécurisé avec des mécanismes cryptographiques.

III.3.1.2.3 Format du paquet SRTP:

Un paquet SRTP ***(voir la Figure 3.16)*** est généré par transformation d'un paquet RTP grâce à des mécanismes de sécurité. Donc le protocole SRTP effectue une certaine mise en forme des paquets RTP avant qu'ils ne soient sur le réseau. La Figure suivante présente le format d'un paquet SRTP

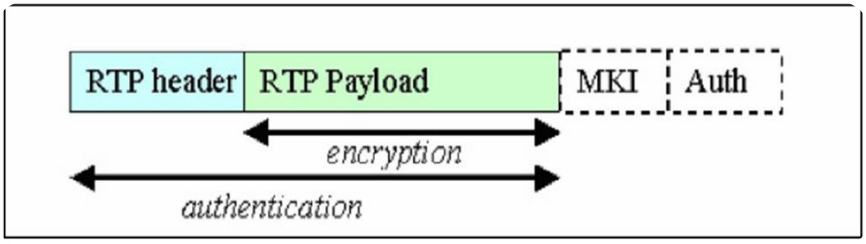


figure 3.16: Format d'un paquet SRTP

On remarque que le paquet SRTP est réalisé en rajoutant deux champs au paquet RTP :

- **SRTP MKI (SRTP Master Key identifier) :** sert à re-identifier une clef maîtresse particulière dans le contexte cryptographique. Le MKI peut être utilisé par le récepteur pour retrouver la clef primaire correcte quand le besoin d'un renouvellement de clefs survient.
- **Authentication tag :** est un champ inséré lorsque le message a été authentifié. Il est recommandé d'en faire usage. Il fournit l'authentification des en-têtes et données RTP et indirectement fournit une protection contre le rejeu de paquets en authentifiant le numéro de séquence.

III.3.2 Sécurisation de l'application:

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

- L'utilisation d'une version stable, Il est bien connu que toute application non stable contient surement des erreurs et des vulnérabilités. Pour minimiser les risques, il est impératif d'utiliser une version stable.

- Tester les mises à jour des softwares dans un laboratoire de test. Il est très important de tester toute mise à jour de l'application dans un laboratoire de test avant de les appliquer sur le système en production.
- Ne pas tester les correctifs sur le serveur lui-même.
- Ne pas utiliser la configuration par défaut qui sert juste à établir des appels. Elle ne contient aucune protection contre les attaques.
- Ne pas installer une application client dans le serveur.

Il est conseiller d'utiliser les paramètres qui utilise le hachage des mots de passe, et cela assure la confidentialité.

III.3.3 Sécurisation du système d'exploitation:

Il est très important de sécuriser le système sur lequel est implémenté le serveur de VoIP.

En effet, si le système est compromis, l'attaque peut se propager sur l'application serveur. Celle-ci risque d'affecter les fichiers de configuration contenant des informations sur les clients enregistrés.

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

- utiliser un système d'exploitation stable. Les nouvelles versions toujours contiennent des bugs et des failles qui doivent être corrigés et maîtrisés avant.
- mettre à jour le système d'exploitation en installant les correctifs de sécurité recommandé pour la sécurité.
- Ne pas mettre des mots de passe simple et robuste. Ils sont fondamentaux contre les intrusions. Et ils ne doivent pas être des dates de naissances, des noms, ou des numéros de téléphones. Un mot de passe doit être assez long et former d'une combinaison de lettre, de chiffres et ponctuations.
- Ne pas exécuter le serveur VoIP avec un utilisateur privilège. Si un utilisateur malveillant arrive à accéder au système via une exploitation de vulnérabilité sur le serveur VoIP, il héritera tous les privilèges de cet utilisateur.
- Asterisk in CHROOT : empêcher le serveur VoIP d'avoir une visibilité complète de l'arborescence du disque, en l'exécutant dans un environnement sécurisé qui l'empêche d'interagir librement avec le système.

- Sauvegarde des fichiers log à distance : les fichiers log sont très importants, il est conseillé de les enregistrer sur un serveur distant.
- Installer seulement les composants nécessaires : pour limiter les menaces sur le système d'exploitation. Il vaut mieux installer sur la machine le système d'exploitation et le serveur.
- Supprimer tous programmes, logiciels ou des choses qui n'ont pas d'importance et qui peuvent être 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.

Le firewall peut être implémenté avec un ACL qui est une liste d'Access Control Entry (ACE) ou entrée de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe. On aura besoin d'ACL pour donner des droits à des personnes bien déterminés selon leurs besoins et leurs autorités.

Pour un serveur VoIP, il est important d'implémenter les ACL pour sécuriser le serveur en limitant l'accès à des personnes indésirables. Par exemple, seuls les agents enregistrés peuvent envoyer des requêtes au serveur. Il existe trois catégories d'ACL :

La liste de contrôle d'accès peut être installée en réseau sur les pare feu ou les routeurs, mais aussi ils existent dans les systèmes d'exploitation.

III.4. Les dispositifs de sécurité:

III.4.1. Les pare-feu:

Un pare-feu (firewall) est un dispositif matériel et/ou logiciel qui implémente la fonction de sécurité de contrôle d'accès.

Un pare-feu est donc un dispositif pour filtrer les accès, les paquets IP, les flux entrant et sortant d'un système68. Un pare-feu est installé en coupure sur un réseau lorsqu'il sert de passerelle filtrante pour un domaine à la frontière d'un périmètre fermé.

Dans le cas d'un pare-feu personnel, sur une machine cliente, il est installé en son cœur pour y contrôler et filtrer les accès au réseau.

Un pare-feu met en vigueur une politique de sécurité qui laisse passer, ou arrête les trames ou les paquets d'information selon cette politique. Il peut donc autoriser ou empêcher des communications selon leur origine, leur destination ou leur contenu. Dans la pratique, un pare-feu lit et analyse chacun des paquets

qui arrivent. Après analyse, il décide du passage ou de l'arrêt selon l'adresse IP de l'émetteur, du récepteur, selon le type de transport (TCP ou UDP) et le numéro de port, en relation avec le type d'application réseau.

Les pare-feu ont des limitations : ils doivent être très puissants en termes de ressources pour ne pas ralentir le trafic dans un sens ou dans un autre, puisqu'ils sont en coupure sur le réseau. Ils ne doivent pas être court-circuités par d'autres passerelles ou des modems connectés directement à l'extérieur. Ils sont des « bastions », c'est-à-dire des cibles pour les attaquants qui peuvent les assaillir pour saturer leur ressource.

Un pare-feu doit posséder un système de journalisation (.log) sophistiqué de manière à analyser a posteriori tous les faits importants qui jalonnent la vie de cette passerelle filtrante : tentatives d'intrusion, événements anormaux, attaques par saturation, par balayage.

Un pare-feu est en général architecturé de telle manière que l'on puisse distinguer physiquement les communications avec l'extérieur, celles avec le réseau à protéger et enfin celles qui sont déviées vers une zone tampon de parking, souvent appelée zone démilitarisée **(D**e**M**ilitarized **Z**one, **DMZ).** C'est dans cette zone qu'on place le site Web, ouvert sur Internet, à l'abri d'un pare-feu, mais nettement séparé du réseau interne à protéger.

III.4.2 Les systèmes de détection et de prévention d'intrusion (IDS/IPS):

Un système de détection d'intrusion (Intrusion Detection System, IDS) est un dispositif matériel et/ou logiciel de surveillance qui permet de détecter en temps réel et de façon continue des tentatives d'intrusion dans un réseau, 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.

Un IDS réagit en cas d'anomalies, à condition que le système puisse bien identifier les intrus externes ou internes qui ont un comportement anormal, en déclenchant un avertissement, une alerte, en analysant éventuellement cette intrusion pour empêcher qu'elle ne se reproduise, ou en paralysant même l'intrusion.

Un IDS est donc un capteur informatique qui écoute de manière furtive le trafic sur un système, vérifie, filtre et repère les activités anormales ou suspectes,

ce qui permet ultérieurement de décider d'actions de prévention. Sur un réseau, l'IDS est souvent réparti dans tous les emplacements stratégiques du réseau.
Les techniques sont différentes selon que l'IDS inspecte un réseau ou que l'IDS contrôle l'activité d'une machine (hôte, serveur) :

- Sur un réseau, il existe en général plusieurs sondes qui analysent de concert, les attaques en amont d'un pare-feu ou d'un serveur ;
- Sur un système hôte, les IDS sont incarnés par des démons ou des applications standards furtives qui analysent des fichiers de journalisation et examinent certains paquets issus du réseau.

Pour vaincre les tentatives d'intrusion, il faut définir un schéma d'identification, d'authentification et d'autorisation destiné à des utilisateurs légitimes et aux matériels et logiciels qui se situent à l'intérieur du système. On soulage fortement l'IDS en filtrant au préalable le trafic forcément régulier et légitime. On définit alors une sonde intelligente qui observe, enregistre et analyse le comportement des sujets, des objets et des événements. À partir d'un modèle de normalité et conformément à certains seuils, on décrète que le comportement du système et des personnes est normal ou suspect. On en déduit des actions à mettre en œuvre, immédiatement ou non.

III.4.3. Les pots de miel:

Les pots de miel **(honey pots)** sont des dispositifs de leurre, à la frontière des SI, destinés à piéger les attaques des pirates.
Les attaques par balayage, en particulier, ont tendance à tomber dans le panneau de ces attrape-nigauds.

Un pot de miel est un mécanisme qui permet d'augmenter la sécurité d'un réseau ou d'un système, pourvu qu'on soit capable d'analyser les profils des attaques tombées dans l'embuscade. Un pot de miel peut venir en complément d'un pare-feu. Mais les mises en œuvre concrètes sont plutôt rares.

Les pots de miel sont répertoriés selon deux catégories, à faible ou à forte interaction. L'interaction représente l'intensité de l'activité que peut avoir un attaquant avec le pot de miel.

Les pots de miel à faible interaction offrent peu de prérogatives à l'intrus qui aura un champ d'action limité, car ils ne font que proposer des services factices et ne renvoient jamais de réponse. L'avantage des pots de miel à faible interaction est leur simplicité. Ils sont faciles à implémenter, à gérer et présentent peu de danger avec des attaquants très cantonnés.

En pratique, on installe un logiciel, on sélectionne les OS et les services qu'on veut émuler et on surveille l'activité en laissant le pot de miel fonctionner. Les inconvénients sont que ces pots de miel examinent une information limitée et ne peuvent épier que des activités connues. Enfin ces pots de miel à faible interaction sont aisément détectables par un attaquant.

Les pots de miel à forte interaction n'émulent rien mais engagent des OS véritables et des applications réelles. L'avantage de cette solution est qu'il est possible de recueillir des informations nombreuses. Comme les attaquants ont accès à de vrais systèmes, on peut observer l'intégralité de leur comportement et on peut analyser ainsi les méthodes et les outils qu'ils utilisent.

Ces pots de miels permettent donc de révéler des modes d'attaques encore insoupçonnées. Néanmoins, leur utilisation comprend des risques élevés puisque la machine, désignée comme pot de miel, est destinée à être compromise. Il existe donc un risque que l'attaquant puisse utiliser les vrais services du pot de miel comme rebond pour affronter d'autres systèmes voisins. Enfin, ces pots de miel sont plus compliqués à mettre en place et à gérer.

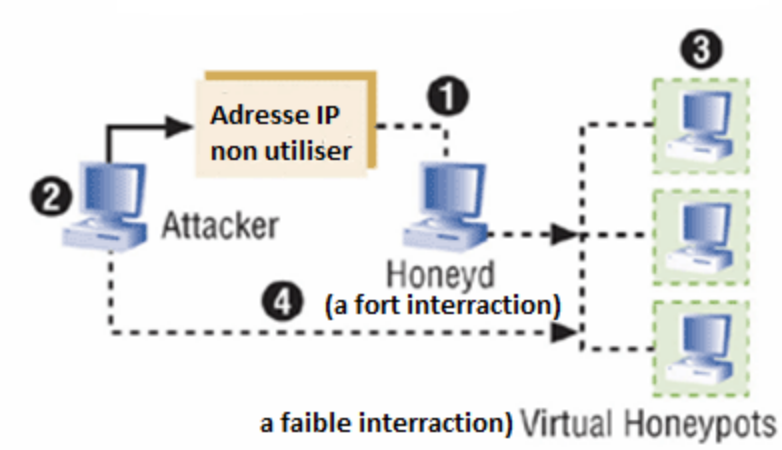


figure 3.17: fonctionnement de Honey Pot

La ***Figure 3.17*** donne le mode de fonctionnement de pot de miel:

1. A averti qu'une attaque viendrait.
2. Surveiller les activités des pirates / pirates.
3. Peut apprendre des méthodes d'attaques de pirates.
4. Création d'un environnement virtuelle » pour piéger l'attaquant.

Cette méthode de protection est Utile pour l'analyse des logiciels malveillants.

Conclusion :

Aucun système d'information n'est sûr à 100% ! Parmi les préceptes connus sur la sécurité informatique se trouve celui énonçant que, pour une entreprise connectée à l'Internet, le problème aujourd'hui n'est plus de savoir si elle va se faire attaquer, mais quand cela va arriver ; une solution possible est alors d'essayer de repousser les risques dans le temps par la mise en œuvre de divers moyens destinés à augmenter le niveau de sécurité. Pour contrer les menaces d'intrusion, les entreprises se tournent de plus en plus vers les solutions de détection d'intrusion, dont les possibilités faramineuses sont vantées par les sociétés éditrices de ces logiciels. Mais le décalage entre le discours commercial et les possibilités techniques réelles de ces produits peut être important, et les conséquences fâcheuses lorsqu'il s'agit de sécurité de l'information.

La voix sur IP devient jour après jour plus ciblé. Il existe plusieurs autres attaques qui menace la sécurité du VoIP, les attaques cité dans ce chapitre sont les plus fameux et courant dans les réseaux VoIP. Mais en suivant certaines bonnes pratiques parmi les cités, on peut créer un réseau bien sécurisé.

Dans le chapitre suivant en va étudier une solution qui permet de détecté et de prévenir les intrusions dans les systèmes (IDS/IPS).

Chapitre IV:

Les Détecteurs/Préventeurs d'intrusion IDS/IPS.

Introduction:

Afin de détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel spécialisé dont le rôle serait de surveiller les données qui transitent sur ce système, et qui serait capable de réagir si des données semblent suspectes. Plus communément appelé IDS/IPS, les systèmes de détection/prévention d'intrusions conviennent parfaitement pour réaliser cette tâche, celle de repousser les risques dans le temps par la mise en œuvre de divers moyens destinés à augmenter le niveau de sécurité. Les entreprises se tournent de plus en plus vers ces solutions de détection d'intrusion et pour contrer les menaces d'intrusion.

C'est pourquoi, avant de présenter les concepts d'IDS et d'IPS, nous allons tout d'abord rappeler quelques notions de sécurité concernant la mise en place d'une politique de sécurité et les attaques qu'un réseau d'entreprise peut subir.

Nous présenterons ensuite le concept d'IDS, les différents types d'IDS, leur mode de fonctionnement.

Nous verrons alors que ces outils ont certaines limitations en présentant quelques méthodes de contournement d'un IDS.

Ceci nous mène aux IPS, censés pallier à ces faiblesses, qui seront présentés dans la dernière partie du chapitre.

IV.1. Système de détection d'intrusions (IDS):

IV.1.1. Définition:

Pour améliorer la sécurité des réseaux, les administrateurs disposent de nombreux outils, dont les systèmes de détection d'intrusions (IDS pour Intrusion/Detection Systems en anglais). Ces outils ont connu un essor particulier au cours des dernières années, notamment en raison du nombre grandissant d'attaques.

Un IDS est un mécanisme écoutant le trafic sur le réseau, de manière furtive. Cela a pour but de repérer les activités et évènements anormaux, suspects,. . .

Cela permet ainsi d'avoir une action de prévention sur les différents risques d'intrusion.

Un IDS a quatre fonctions : l'analyse, la journalisation, la gestion et l'action :

- **Analyse :** analyse des journaux pour identifier des motifs dans la masse de données recueillie par l'IDS. Il y a deux méthodes d'analyse : une basée sur les signatures d'attaques, et l'autre sur la détection d'anomalies.
- **Journalisation :** Enregistrement des évènements dans un fichier (un fichier log). Exemples d'évènements : arrivée d'un paquet, tentative de connexion.
- **Gestion :** les IDS doivent êtres gérés de manière continue. Ils doivent êtres configurés, vérifiés. . .

On peut assimiler un IDS à une caméra de sécurité : ça détecte les intrusions, mais est inutile s'il n'y a personne derrière cette caméra.

- **Action :** alerter le personnel, ou transmettre une commande, quand une situation dangereuse est détectée.

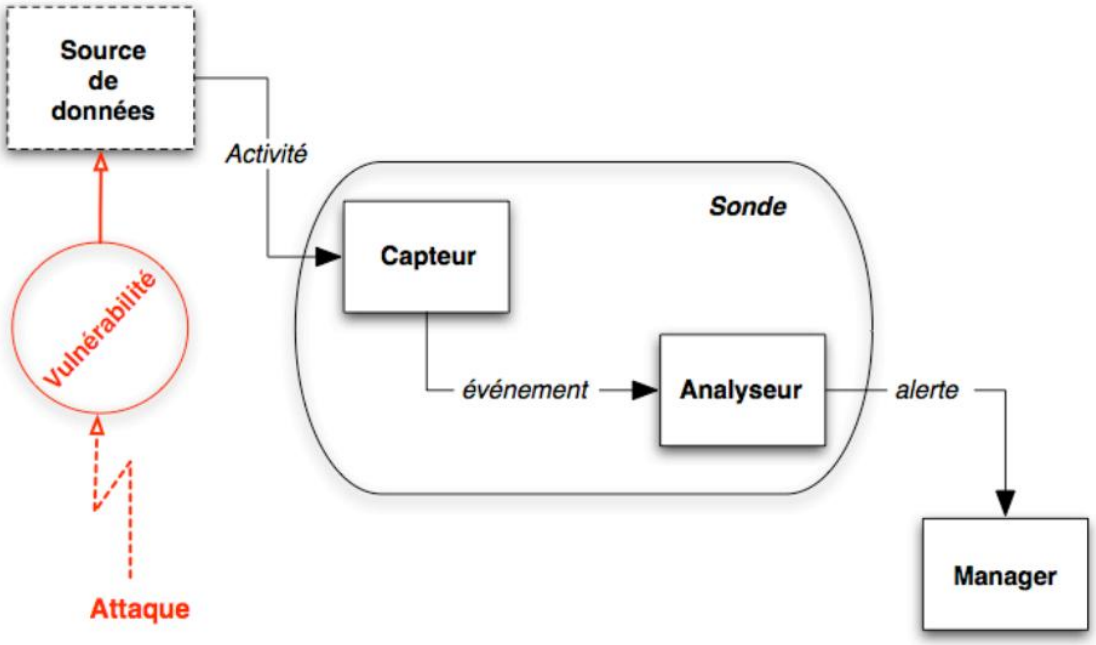


Figure 4-1: Architecture d'un IDS

IV.1.2 Pourquoi a-t-on besoin de l'IDS?:

Pourquoi vous avez besoin d'installer un système IDS dans votre système de réseau? Pour surveiller la circulation des paquets sur le réseau. Vous pouvez considérez le IDS comme une caméra installé devant votre port. Ça pour savoir qui essaye à attaquer à votre réseau.

Quand une tentative est réussie en passant votre par feu, il va peut être provoqué des menaces. Alors, vous pouvez diminuer des fautes positives en connaissant ces tentatives. Dans l'environnement de NAT est aussi un profit parce qu'il nous permet de tenir l'adresse réelle de la source par mettre en corrélation avec des événements entre le système IDS qui situe avant de après le par feu.

Cette topologie vous permettra de vérifier que votre ligne de base du par feu est suivi, ou que quelqu'un a fait une erreur en changeant une règle de par feu. Si vous savez que votre ligne de base du par feu proscrivent l'utilisation de ftp et votre système IDS montre des alertes de ftp, alors vous savez que le par feu ne bloque pas de trafic de ftp. C'est juste un effet secondaire et ne devrait pas être la seule manière que vous vérifiez la conformité à votre ligne de base.

IV.1.3 Les différents types d'IDS:

Les différents IDS se caractérisent par leur domaine de surveillance. Celui-ci peut se situer au niveau d'un réseau d'entreprise, d'une machine hôte, d'une application…

Nous allons tout d'abord étudier la détection d'intrusion basée sur l'hôte, puis basée sur une application, avant de nous intéresser aux IDS réseaux, NIDS et NNIDS (Network IDS et Node Network IDS) ou IDS Hybride.

IV.1.3.1. La détection d'intrusion basée sur l'hôte (HIDS):

Le HIDS réside sur un hôte spécifique, et est utilisé en tant qu'agent. Il analyse les informations particulières dans les fichiers de log pour détecter toute activité d'intrusion. Il capture les paquets réseaux entrant/sortant de l'hôte sur lequel il se trouve, et alerte lorsque nécessaire.

- **Points forts :**
  - ✓ Pouvoir surveiller des événements local jusqu'au host, détecter des attaques qui ne sont pas vues par NIDS.
  - ✓ Marcher dans un environnement dans lequel le trafic de réseau est encrypté, lorsque les sources des informations de host-based sont générées avant l'encrypte des données ou après le décrypte des données au host de la destination.
  - ✓ HIDS n'est pas atteint par le réseau commuté.
  - ✓ Lors que HIDS marche sur la traîné de l'audit de SE, ils peuvent détecter le Cheval de Troie ou les autres attaques concernant à la brèche intégrité de logiciel.

- **Points faibles :**
  - ✓ HIDS est difficile à gérer, et des informations doivent configurées et gérées pour chaque host surveillé.
  - ✓ Puisque au moins des sources de l'information pour HIDS se résident sur l'host de la destination par les attaques, le HIDS peut être attaqué et neutralisé comme une partie de l'attaque.
  - ✓ HIDS n'est pas bon pour le balayage de réseau de la détection ou les autres tels que la surveillance qui s'adresse au réseau entier parce que le HIDS ne voit que les paquets du réseau reçus par ses hosts.

- ✓ HIDS peut être neutralisé par certaine attaque de DoS; Les HIDS peuvent être victimes d'attaques (modification et effacement de fichiers) empêchant leur fonctionnement..
- ✓ Lorsque HIDS emploie la traîné de l'audit du SE comme des sources des informations, la somme de l'information est immense, alors il demande le stockage supplémentaire local dans le système.

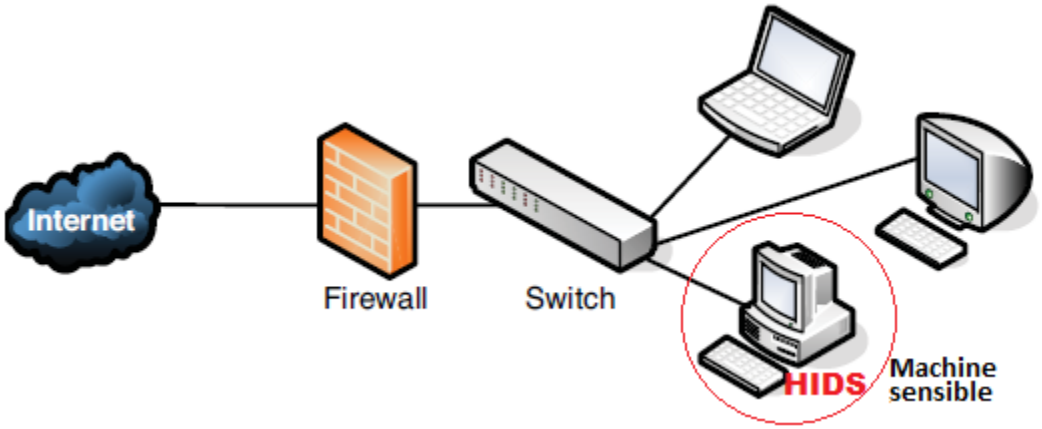


Figure 4.2: Emplacement d'un HIDS

Les HIDS sont en général placés sur des machines sensibles ***(voir la Figure 4.2)***, susceptibles de subir des attaques et possédant des données sensibles pour l'entreprise. Les serveurs, web et applicatifs, peuvent notamment être protégés par un HIDS.

Pour finir, voici quelques HIDS connus: Tripwire, WATCH, DragonSquire, Tiger, Security Manager, RealSecure Server Sensor …

IV.1.3.2 Détection d'Intrusion basée sur une application (ABIDS):

Les IDS basés sur les applications sont un sous-groupe des IDS hôtes.
Ils contrôlent l'interaction entre un utilisateur et un programme en ajoutant des fichiers de log afin de fournir de plus amples informations sur les activités d'une application particulière. Puisque vous opérez entre un utilisateur et un programme, il est facile de filtrer tout comportement notable. Un ABIDS se situe au niveau de la communication entre un utilisateur et l'application surveillée.

- **Points forts:**
  - ✓ il lui est possible de détecter et d'empêcher des commandes particulières dont l'utilisateur pourrait se servir avec le programme et de surveiller chaque transaction entre l'utilisateur et l'application. De plus, les données sont décodées dans un contexte connu, leur analyse est donc plus fine et précise.
- **Points faible:**
  - ✓ Le fait que cet IDS n'agit pas au niveau du noyau, la sécurité assurée est plus faible, notamment en ce qui concerne les attaques de type "Cheval de Troie".
  - ✓ Les fichiers de log générés par ce type d'IDS sont des cibles faciles pour les attaquants et ne sont pas aussi sûrs, par exemple, que les traces d'audit du système.

Ce type d'IDS est utile pour surveiller l'activité d'une application très sensible, mais son utilisation s'effectue en général en association avec un HIDS. Il faudra dans ce cas contrôler le taux d'utilisation CPU des IDS afin de ne pas compromettre les performances de la machine.

IV.1.3.3 La Détection d'Intrusion Réseau (NIDS):

Un NIDS est effectif sur un matériel précis, et est capable de contrôler tous les paquets qui circulent à un endroit précis du réseau. Il utilise des cartes réseau en mode espion, ceci garantit un fonctionnement furtif qui lui permet d'analyser tout les paquets passant par le lien en question.

L'implantation d'un NIDS sur un réseau se fait de la façon suivante ***(voir Figure 4.3)*** : des capteurs sont placés aux endroits stratégiques du réseau et génèrent des alertes s'ils détectent une attaque. Ces alertes sont envoyées à une console sécurisée, qui les analyse et les traites éventuellement. Cette console est généralement située sur un réseau isolé, qui relie uniquement les capteurs et la console.

❖ **Les capteurs:**

Les capteurs placés sur le réseau sont placés en mode furtif (ou stealth mode), de façon à être invisibles aux autres machines. Pour cela, leur carte réseau est configurée en mode "promiscuous", c'est à dire le mode dans lequel la carte réseau lit l'ensemble du trafic, de plus aucune adresse IP n'est configurée.

Un capteur possède en général deux cartes réseaux, une placée en mode furtif sur le réseau, l'autre permettant de le connecter à la console de sécurité. Du fait de leur invisibilité sur le réseau, il est beaucoup plus difficile de les attaquer et de savoir qu'un IDS est utilisé sur ce réseau.

❖ **Placer les capteurs:**

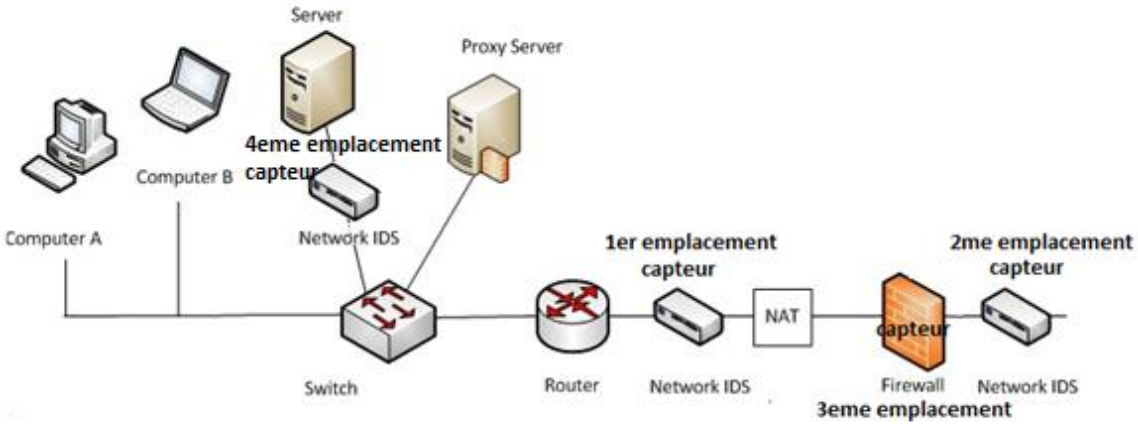


Figure 4.3: emplacement des capteurs NIDS

Il est également possible de placer un capteur à l'extérieur du pare-feu (avant le firewall). L'intérêt de cette position est que le capteur peut ainsi recevoir et analyser l'ensemble du trafic d'Internet. Si vous placez le capteur ici, il n'est pas certain que toutes les attaques soient filtrées et détectées. Pourtant, cet emplacement est le préféré de nombreux experts parce qu'il offre l'avantage d'écrire dans les logs et d'analyser les attaques (vers le pare-feu...), ainsi l'administrateur voit ce qu'il doit modifier dans la configuration du pare-feu.

Les capteurs placés à l'extérieur du pare-feu servent à détecter toutes les attaques en direction du réseau, leur tâche ici est donc plus de contrôler le fonctionnement et la configuration du firewall que d'assurer une protection contre toutes les intrusions détectées (certaines étant traitées par le firewall).

Il est également possible de placer un capteur et un autre après le firewall. En fait, cette variante réunit les deux cas mentionnés ci-dessus. Mais elle est très dangereuse si on conFigure mal les capteurs et/ou le pare-feu, en effet on ne peut simplement ajouter les avantages des deux cas précédents à cette variante.

Les capteurs IDS sont parfois situés à l'entrée de zones du réseau particulièrement sensibles (parcs de serveurs, données confidentielles…), de façon à surveiller tout trafic en direction de cette zone.

- **Points forts :**
  - ✓ Le NIDS peut surveiller un grand réseau.
  - ✓ L'déploiement de NIDS a peu d'impact sur un réseau existant. L'NIDS sont habituellement des dispositifs passifs qui écoutent sur un fil de réseau sans interférer l'opération normale d'un réseau. Ainsi, il est habituellement facile de monter en rattrapage un réseau pour inclure IDS avec l'effort minimal.
  - ✓ NIDS peut être très sûr contre l'attaque et être même se cache à beaucoup d'attaquants.

- **Points faibles :**
  - ✓ Il est difficile à traiter tous les paquets circulant sur un grand réseau. De plus il ne peut pas reconnaître des attaques pendant le temps de haut trafic.
  - ✓ Quelques fournisseurs essayent à implémenter le IDS dur le matériel pour qu'il marche plus rapidement.
  - ✓ Plusieurs des avantages de NIDS ne peut pas être appliqué pour les commutateurs modernes. La plupart des commutateurs ne fournissent pas des surveillances universelles des ports et limitent la gamme de surveillance de NIDS .Même lorsque les commutateurs fournissent de tels ports de surveillance, souvent le port simple ne peut pas refléter tout le trafic traversant le commutateur.
  - ✓ Les NIDS ne peuvent pas lire les données chiffrées. Il peuvent uniquement scanner les parties non chiffrées d'un paquet ; cela fournit donc des informations limitées. Ce problème a lieu dans les organisations utilisant le VPN.

- ✓ La plupart de NIDS ne peuvent pas indiquer si un attaque réussi ou non. Il reconnaît seulement que un attaque est initialisé. C'est-à-dire qu'après le NIDS détecte une attaque, l'administrateur doit examiner manuellement chaque host s'il a été en effet pénétré.
- ✓ Quelques NIDS provoque des paquets en fragments. Ces paquets mal formés font que l'IDS devient instable.

Pour finir, voici quelques NIDS connus RealSecure Network Sensor, Snort....

IV.1.3.4 Système de Détection d'Intrusion de Nœud Réseau (NNIDS):

Ce nouveau type d'IDS (NNIDS) fonctionne comme les NIDS classiques, c'est-à-dire vous analysez les paquets du trafic réseau. Mais ceci ne concerne que les paquets destinés à un nœud du réseau (d'où le nom) ***(voir Figure 4.4)***.;

Une autre différence entre NNIDS et NIDS vient de ce que le NIDS fonctionne en mode "promiscuous", ce qui n'est pas le cas du NNIDS. Celui-ci n'étudie que les paquets à destination d'une adresse ou d'une plage d'adresse. Puisque tous les paquets ne sont pas analysés, les performances de l'ensemble sont améliorées.

Exemple: L'exemple le plus connu dans le monde Open-Source est Prelude. Ce framework permet de stocker dans une base de données des alertes provenant de différents systèmes relativement variés.

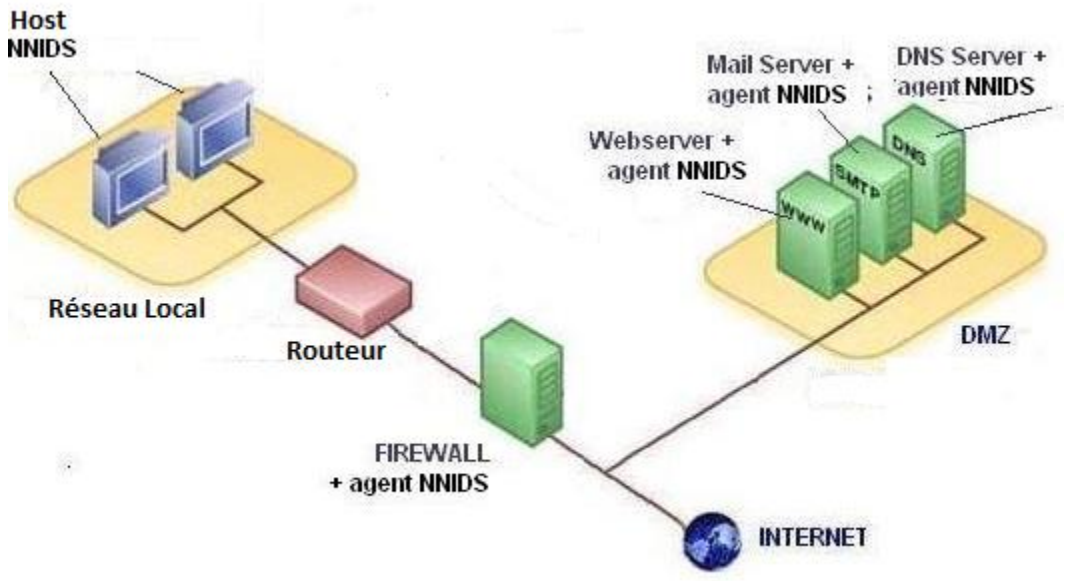


Figure 4-4: Emplacement des NNIDS.

Ce type d'IDS n'est pas encore très répandu, mais il est de plus en plus utilisé pour étudier le comportement de nœuds sensibles d'un réseau.

De nouveaux types d'IDS sont conçus actuellement, comme les IDS basés sur la pile, qui étudie la pile d'un système. Le secteur des IDS est en plein développement, le besoin des entreprises en sécurité réseaux étant de plus en plus pressant, du fait de la multiplication des attaques.

Actuellement, les IDS les plus employés sont les NIDS et HIDS, de plus en plus souvent en association. Les ABIDS restent limités à une utilisation pour des applications extrêmement sensibles.

Les recherches en cours visent également à améliorer les performances des IDS, notamment dans ce qui concerne les faux positifs et faux négatifs et la complexité d'administration (actuellement il faut souvent une personne dédiée à la gestion de l'IDS).

Nous allons à présent nous pencher sur le mode de fonctionnement d'un IDS.

1.3.5 IDS hybride :

Les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi d'alerte (typiquement IDMEF) (Voir **Figure 4.5)** permettant des composants divers de communiquer et d'extraire des alertes plus pertinentes.

Les avantages des IDS hybrides sont multiples :

- Moins de faux positifs.
- Meilleure corrélation.
- Possibilité de réaction sur les analyseurs.

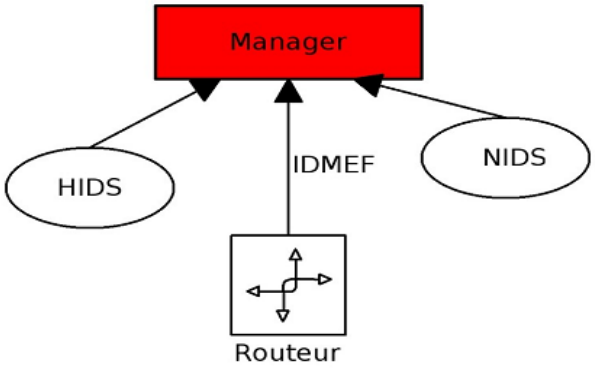


Figure 4.5: Le fonctionnement de l'IDS HYBRIDE

1.3.5.1 La corrélation :

La corrélation est une connexion entre deux ou plusieurs éléments, dont un de ces éléments crée ou influence un autre. Elle se traduit plus généralement par la transformation d'une ou plusieurs alertes en attaque. Ceci permet de faciliter la compréhension sur les attaques au lieu de s'éparpiller parmi les alertes.

Idéalement, elle nécessite un IDS Hybride car plus s'il y aura plus d'informations hétérogènes sur un évènement, la corrélation se fait d'une façon plus pertinente. Les formats ayant été normalisés (IDMEF), il ne reste plus qu'à faire des associations afin de détecter des alertes qui n'auraient jamais eu lieu sur un analyseur seul.

La corrélation permet de générer de nouvelles alertes à partir des unes auparavant existantes. C'est une étape préalable à une contre mesure efficace. Il y a diverses façons de faire de la corrélation. Cependant on peut définir deux catégories:

- **La corrélation passive**, correspondant à une génération d'alerte basée sur celles existantes. Nous pouvons prendre par exemple les scans de force brute ssh.
- **La corrélation active**, qui va chercher les informations correspondant à des alertes émises. Par exemple, lorsqu'une personne se connecte en dehors des heures de travail, ceci a un impact élevé qui n'aurait pas été en temps normal d'activité.

1.3.5.2 L'harmonisation des formats :

- Le format IDMEF (Intrusion Detection Message Exchange Format) décrit une alerte de façon objet et exhaustive. Une alerte correspond au message émis depuis un analyseur, qui est une sonde en langage IDMEF, vers un collecteur. Le but d'IDMEF est de proposer un standard permettant d'avoir une communication hétérogène quelque soit l'environnement ou les capacités d'un analyseur donné.

- ces alertes sont définies au format XML, offrant une possibilité de validation de chaque message. En général, les implémentations restent binaires, afin d'éviter les problèmes connus d'ajout d'information inutiles en dehors d'XML lorsqu'on envoie un message sur le réseau.

• IDMEF offre aussi un vocabulaire précis, qu'il est courant d'utiliser dans le domaine de la détection d'intrusions. Par exemple, une classification correspond au nom d'une alerte; un impact celui d'un niveau d'attaque.

1.3.6 Exemples d'IDS :

- **IDS réseau (NIDS) :**
  - Snort.
  - Bro.
- **IDS system (HIDS):**
  - Chkroottkit. - FChek - OSSEC
  - DarkSpy. - Integrit - Osiris
- **IDS hybrid :**
  - Prelude
  - OSSIM

A partir de la liste des IDS précédents, on a choisi d'installer et de configurer le NIDS Open Source SNORT, car c'est un IDS gratuit disponible dans sa version 2.9.4 (www.snort.org). A l'origine, ce fut un sniffer qui connu une telle évolution qu'il fut vite adopter et utiliser dans le monde de la détection d'intrusion en s'appuyant sur une base de signature régulièrement enrichie par le "monde du libre".

IV.1.4 Fonctionnement des IDS:

IV.1.4.1 Les méthodes de détection des IDS:

Les systèmes de détection d'intrusions se divisent en deux catégories :

IV.1.4.1.1 Par Signatures :

Les intrus possèdent des signatures, tout comme les virus, qui peuvent êtres détectés par certains logiciels. La procédure consiste à trouver les paquets de données contenant des signatures connues comme anormales et dangereuses. Basé sur un ensemble de signatures et de règles, le système de détection peut trouver et loguer les activités suspecte se produire des alertes. Cependant les IDS nécessitent des mises à jour de leur base de signatures pour pouvoir détecter les nouveaux types d'attaques.

Une signature permet de définir les caractéristiques d'une attaque, au niveau des paquets (jusqu'à TCP ou UDP) ou au niveau protocole (HTTP, FTP…).

Au niveau paquet, l'IDS va analyser les différents paramètres de tous les paquets transitant et les comparer avec les signatures d'attaques connues.

Au niveau protocole, l'IDS va vérifier si les commandes envoyées sont correctes ou ne contiennent pas d'attaque. Cette fonctionnalité a surtout été développée pour HTTP actuellement.

Cependant, une signature mal élaborée peut ignorer des attaques réelles ou identifier du trafic normal comme étant une attaque. Il convient donc de manier l'élaboration de signatures avec précaution, et en ayant de bonnes connaissances sur le réseau surveillé et les attaques existantes.

IV.1.4.1.2.Par Anomalies :

Les IDS basés sur la détection d'anomalies consistent à comparer les schémas d'évènements en cours pris dans leur ensemble aux schémas d'évènements habituels pris dans leur ensemble. Cela permet d'analyser beaucoup de choses comme par exemple des utilisateurs accédant à des fichiers systèmes, des modifications de fichiers inhabituelles, de nombreux échecs de connexion,. . .

Cette méthode permet d'identifier des attaques inhabituelles. Mais il est difficile de distinguer ce qui est normal de ce qui ne l'est pas, car les schémas d'activités varient très largement.

IV.1.4.1.3 Par intégrité:

Les IDS basés sur la vérification d'intégrité consistent à:

- ✓ Génération d'une somme de contrôle sur des fichiers d'un système
- ✓ Une comparaison est alors effectuée avec une somme de contrôle de référence
  - – Exemple : une page web
- ✓ Méthode couramment employée par les HIDS

Le diagramme dans la **Figure 4.6** illustre le fonctionnement d'un IDS.

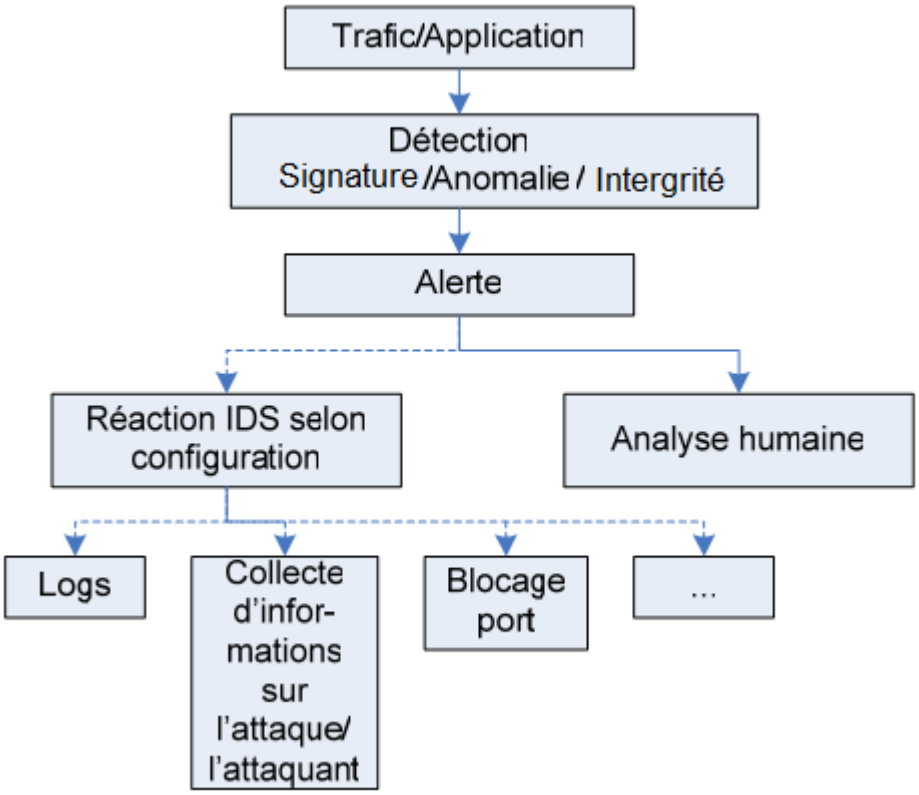


Figure 4.6 : le fonctionnement d'un IDS

Dans le cas d'HIDS, ce type de détection peut être basé sur des informations telles que le taux d'utilisation CPU, l'activité sur le disque, les horaires de connexion ou d'utilisation de certains fichiers (horaires de bureau…).

IV.1.5 Emplacement d'un IDS dans le réseau:

La **Figure 4.7** indique les emplacements possibles d'un IDS dans le réseau :

- **Localisation 1** : à l'entrée du firewall externe, relié à internet. C'est le meilleur endroit pour analyser les attaques externes contre le réseau.
- **Localisation 2 :** dans la zone des serveurs, une zone sensible pour le réseau et donc à surveiller.
- **Localisation 3 :** sur chaque segment réseau. Il se concentre sur les attaques ayant passé le firewall et s'étant intro duites sur ce segment réseau.

- **Localisation 4 :** sur un sous réseau, comme pour la location 3, vise à protéger un sous réseau particulier.

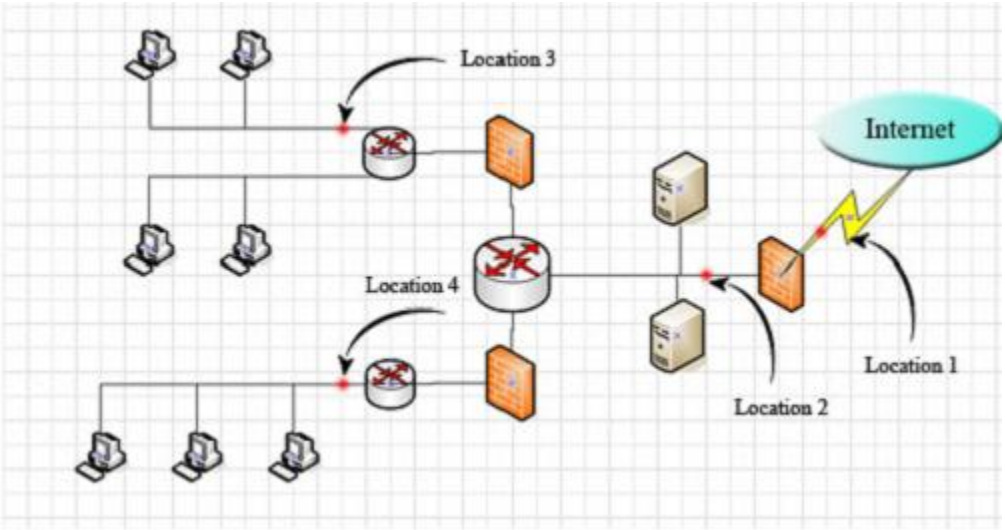


Figure 4.7: Emplacement des IDS.

IV.1.6 Les différentes actions des IDS:

Les IDS peuvent déclencher différents types d'alarmes et proposent des dispositifs d'analyse interactifs pour aider l'administrateur à identifier des motifs dans les journaux. Il existe plusieurs méthodes pour signaler les intrusions. Les principales sont les suivantes :

- ✓ Envoi d'un email aux utilisateurs concernés.
- ✓ Journalisation (log) de l'attaque. En quelque sorte une sauvegarde des circonstances et détail s de l'attaque, comme les adresse IP et le protocole utilisé.
- ✓ Alerte visuelle de l'attaque, un message s'ache signalant à l'utilisateur l'attaque.
- ✓ Sauvegarde des paquets suspects ; les paquets jugés suspects sont capturés et stockés.

Bon nombre d'IDS exécutent des actions limitées suivant certains types d'évènements, sans intervention humaine. Cependant, les actions automatisées sont à limiter car la plupart des schémas indiquent seulement des activités suspectes, et non des actions très certainement malveillantes.

En effet, cette classification fournit des informations essentielles pour la génération des attaques et l'analyse des cas de test. Par exemple, la dimension "source" donne une idée sur l'endroit d'où l'attaque doit être générée pour le test ; de même, la dimension "vulnérabilité" donne une information sur la configuration à avoir (ou l'inverse) pour le test. Dans le même sens, la sévérité des attaques est implicitement décrite à partir de la dimension "privilège".

IV.2. Système de prévention d'intrusions:

IV.2.1 Définition: Qu'es se qu'un IPS?

Un IPS est un dispositif aussi bien matériel que logiciel, qui permet de détecter des attaques, connues et inconnues, et de les empêcher d'être réussies.

Le système d'empêchement d'intrusion construit sa part à résoudre le problème Zero-Day. Le moment le plus important a lieu quand les attaques reconnaissent la vulnérabilité de votre système et vous devez trouver rapidement une solution. À ce moment là, les produits d'IPS deviennent très utiles.

Un système IPS est placé en ligne et examine en théorie tous les paquets entrants ou sortants. Il réalise un ensemble d'analyses de détection, non seulement sur chaque paquet individuel, mais également sur les conversations et motifs du réseau, en visualisant chaque transaction dans le contexte de celles qui précèdent ou qui suivent.

Si le système IPS considère le paquet inoffensif, il le transmet sous forme d'un élément traditionnel de couche 2 ou 3 du réseau. Les utilisateurs finaux ne doivent en ressentir aucun effet. Cependant, lorsque le système IPS détecte un trafic douteux il doit pouvoir activer un mécanisme de réponse adéquat en un temps record.

L'IPS doit aussi, offrir un moyen de diminuer considérablement l'utilisation des ressources humaines nécessaires au bon fonctionnement des IDS. Cela doit aboutir, notamment, à une automatisation des fonctions d'analyse des logs, même si ce point demeure encore une tâche difficile. La prise de décision doit ainsi pouvoir être automatisée non seulement grâce à la reconnaissance de signatures mais aussi, et de plus en plus, grâce à l'utilisation d'analyses heuristiques provenant du monde des anti-virus.

L'IPS est une réponse industrielle aux clients qui demandent la question « Pourquoi nous n'empêchons pas des attaques quand nous les détectons? »

IV.2.2 Compétences requises d'un IPS:

Afin de pouvoir prétendre à l'appellation IPS, il faut que le produit mis en œuvre s'articule autour de fonctionnalités essentielles :

- La compréhension des réseaux IP (les architectures existantes, les protocoles utilisés…) et des couches applicatives de niveau 7 doit permettre de détecter les anomalies protocolaires qui sont synonymes d'attaques.
- La connaissance des serveurs dédiés et de leur architecture logicielle afin de les enrichir de nouvelles fonctions et de les sécuriser encore plus.
- La maîtrise des sondes réseau et l'analyse des logs dans le but de déceler les attaques et d'écrire les scripts de commande qui piloteront les firewalls.
- Comprendre les besoins du client afin de consacrer en priorité la politique de défense aux fonctions vitales des réseaux de l'entreprise.
- Fonctionner à vitesse de ligne afin d'éviter tout effet néfaste sur la performance ou la disponibilité du réseau.
- Fonctionner en mode "statefull Inspection" dans le but de connaître à chaque instant le contexte de l'analyse en cours.

IV.2.3 Les différents types d'IPS:

Il existe deux types d'IPS :

- **Les NIPS** (Network Intrusion Prevention System): un logiciel ou un matériel dédié qui est connecté directement à un segment du réseau et qui protège les systèmes de ce segment.
- **les HIPS**: un programme système installé directement sur l'ordinateur à surveiller.

IV.2.3.1 NIPS:

Le NIPS combine le s caractéristiques d'un IDS standard avec celles d'un firewall. On le qualifie parfois de firewall à inspection en profondeur (deep inspection).

Comme avec un firewall, le NIPS a au minimum deux interfaces réseau, une interne et une externe. Les paquets arrivent par une des interfaces et sont passés au moteur de détection. L'IPS fonctionne pour le moment comme un IDS, c'est-à-dire qu'il détermine si oui ou non le paquet est malveillant. Cependant, en plus de déclencher une alerte dans le cas ou il détecte un paquet suspect, il rejettera le paquet et marquera cette session "suspecte". Quand les paquets suivants de cette session arriveront à l'IPS, ils seront jetés.

Les NIPS sont déployés en ligne avec le segment du réseau à protéger ***(voir Figure 4-8)***. Du coup, toutes les donné es qui circulent entre le segment surveillé et le reste du réseau sont forcées de passer par le NIPS.

Un NIPS déclenche des alarmes du type "tel ou tel trafic a été détecté en train d'essayer d'attaquer ce système et a été bloqué".

Un NIPS ne nécessite pas d'intervention humaine si la sécurité n'est pas primordiale pour l'entreprise. Dans le cas contraire une intervention humaine est préférable pour surveiller les interventions automatisées du NIPS. Les avantages d'un NIPS :

- ✓ Un seul point de contrôle pour le trafic peut protéger tout les systèmes situés en aval du dispositif.
- ✓ Le déploiement est facile car un seul dispositif IPS suffit pour des dizaines de systèmes.
- ✓ Il protège des autres dispositifs du réseau car toutes les attaques peuvent aussi être dirigées contre des routeurs, des firewalls.
- ✓ Il protège des attaques réseaux : Dos (deny of services), SYN flood (Synchronisation flood) etc... Travailler au niveau du réseau permet à un NIPS de protéger contre ces attaques.

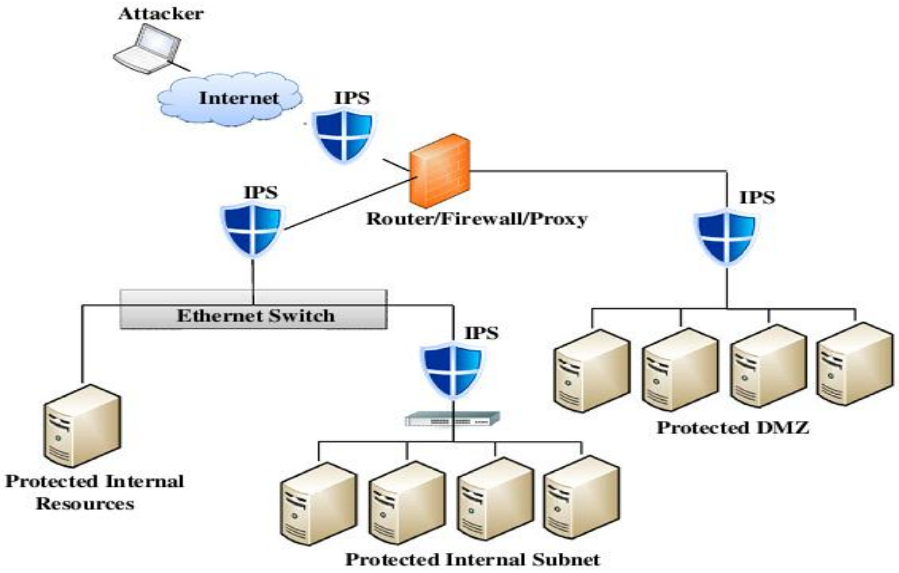


Figure 4-8: Emplacement de NIPS sur un réseau

IV.2.3.2 HIPS:

Le HIPS est un programme résidant sur un système tel que les serveurs ou les postes de travail ***(voir Figure 4-9)***.

Le trafic qui entre et sort de ce système est inspecté et les activités au niveau des applications et du système d'exploitation peuvent être surveillées afin d'y trouver des signes d'une attaque. Un HIPS peut détecter les attaques visant la machine, et arrêter le processus malveillant avant qu'il ne s'exécute.

Le HIPS ne nécessite plus de service de journalisation des évènements (log).

Quand une attaque e st détectée, le logiciel bloque l'attaque soit au niveau de l'interface réseau, soit en envoya nt des commandes à l'application ou au système d'exploitation, leur disant d'arrêter l'action lancée par l'attaque.

Un HIPS possède une liste prédéfinie de règles, définie par le fabriquant et livrée avec le produit. Ces règles savent comment un système d'exploitation ou une application doit se "comporter normalement". Si l'application entame une action suspecte, une des règles est activée et le processus est tué avant de nuire au système.

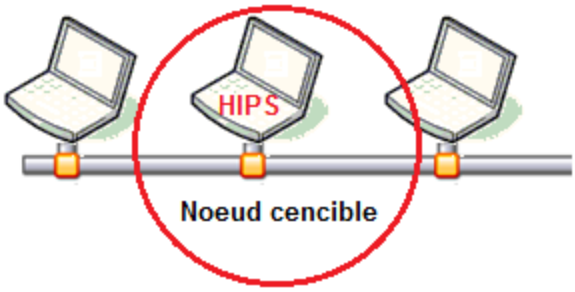


Figure 4-9: Emplacement de HIPS sur un réseau

D'autres systèmes HIPS emploient la méthode "surveillance". Un agent HIPS tourne sur l'ordinateur et se concentre sur les événements d'un système d'exploitation en observant tous les appels système, les entré es de la base de registre.

Les avantages d'un Host IPS :

- ✓Protège les systèmes mobiles contre une attaque quand il s sont hors du réseau protégé.
- ✓ Protège des attaques locales, le personnel ayant un accès physique et voulant corrompre certains systèmes à l'aide de disquette ou CD. . .
- ✓ Garantie une dernière défense contre les attaques ayant passé les autres systèmes de sécurité.
- ✓ Les attaques lancées entre les systèmes du même segment réseau ne peuvent être contrées qu'avec le HIPS.
- ✓ Indépendant de l'architecture réseau.

Le HIPS doit respecter certaines conditions : il doit être able, ne doit pas ralentir les performances des systèmes, et ne doit pas bloquer le trafic légitime.

IV.2.4 Fonctionnement des IPS:

IV.2.4.1 Les techniques de détection:

Plusieurs méthodes de détection existent :

- **L'analyse de protocole** : l'IPS contrôle la norme du protocole donné et vérifie si elle est conforme. De ce fait, la recherche d'une activité d'intrusion est plus précise et donc plus efficace.

- **Correspondance de motifs :** le trafic est surveillé pour déterminer les signatures des motifs d'attaque connus. Le système analyse tous les paquets. L'IPS conserve l a trace de l'état de connexion avec l'élément extérieur et évalue le contexte plus large de toutes les transactions établies au cours de la connexion. Cette méthode détecte uniquement les attaques connues, et ce ci uniquement si la liste des signatures d'attaques est régulièrement actualisée.
- **Comportementale :** basée sur le comportement. L'IPS tente de cerner les activités anormales en observant le comportement du système et des utilisateurs. Si l'IPS constate que l'activité courante s'éloigne trop du comportement habituel, il prend certaines mesures. Cette méthode a l'avantage de pouvoir détecter des tentatives malveillantes jusqu'alors inconnues.

IV.2.5 Où placer un IPS dans le réseau:

La ***Figure 4.10*** indique les emplacements possibles d'un IPS dans le réseau :

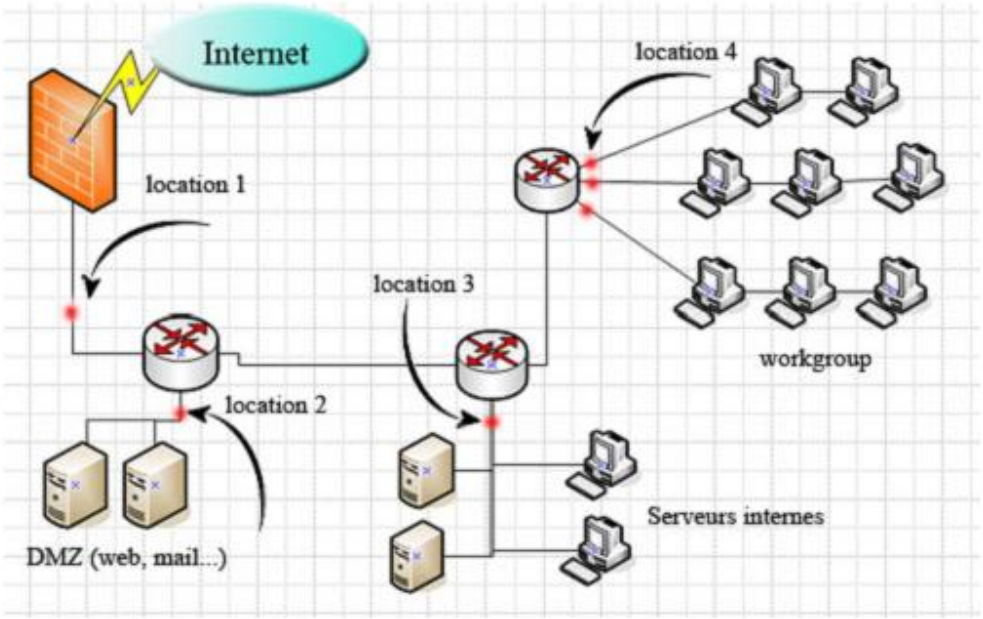


Figure 4.10 : Emplacement des IPS

- **Localisation 1 :** Derrière le firewall de périmètre réseau, assure une sécurité face aux attaques externes.
- **Localisation 2 :** entre le firewall et les serveurs placé en DMZ (DeMilitarized Zone) comme les serveurs web, email..
- **Localisation 3 :** devant les serveurs internes importants, et donc à risques.
- **Localisation 4 :** devant les principaux workgroups d'un service.

Une fois une attaque détectée, un IDS a le choix entre plusieurs types de réponses, que nous allons maintenant détailler.

IV.3 Type de réponses aux attaques:

Il existe deux types de réponses, suivant les IDS/IPS utilisés. La réponse passive est disponible pour tous les IDS/IPS, la réponse active est plus ou moins implémentée.

A/ Réponse passive:

La réponse passive d'un IDS/IPS consiste à enregistrer les intrusions détectées dans un fichier de log qui sera analysé par le responsable sécurité ***(voir Figure 4-11)***.

Certains IDS permettent de loger l'ensemble d'une connexion identifiée comme malveillante.

Ceci permet de remédier aux failles de sécurité pour empêcher les attaques enregistrées de se reproduire, mais elle n'empêche pas directement une attaque de se produire.

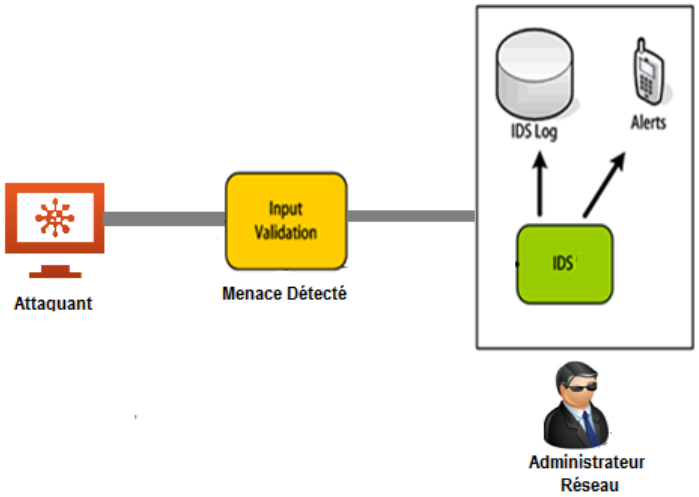


Figure 4-11: La réponse Passive des IDS/IPS

B/ Réponse active :

La réponse active au contraire a pour but de stopper une attaque au moment de sa détection ***(voir Figure 4-12)***. Pour cela on dispose de deux techniques : la reconfiguration du firewall et l'interruption d'une connexion TCP.
La reconfiguration du firewall permet de bloquer le trafic malveillant au niveau du firewall, en fermant le port utilisé ou en interdisant l'adresse de l'attaquant. Cette fonctionnalité dépend du modèle de firewall utilisé, tous les modèles ne permettant pas la reconfiguration par un IDS/IPS. De plus, cette reconfiguration ne peut se faire qu'en fonction des capacités du firewall.

L'IDS/IPS peut également interrompre une session établie entre un attaquant et sa machine cible, de façon à empêcher le transfert de données ou la modification du système attaqué.
Pour cela l'IDS/IPS envoie un paquet TCP reset aux deux extrémités de la connexion (cible et attaquant). Un paquet TCP reset a le flag RST de positionné, ce qui indique une déconnexion de la part de l'autre extrémité de la connexion. Chaque extrémité en étant destinataire, la cible et l'attaquant pensent que l'autre extrémité s'est déconnectée et l'attaque est interrompue.

Dans le cas d'une réponse active, il faut être sûr que le trafic détecté comme malveillant l'est réellement, sous peine de déconnecter des utilisateurs normaux. En général, les IDS/IPS ne réagissent pas activement à toutes les alertes. Ils ne répondent à des alertes que quand celles-ci sont positivement certifiées comme étant des attaques. L'analyse des fichiers d'alertes générés est donc une obligation pour analyser l'ensemble des attaques détectées.

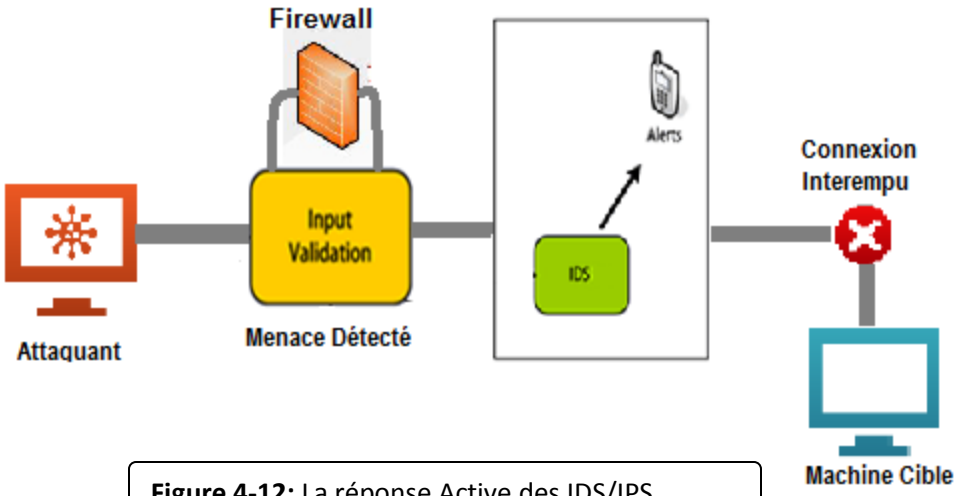


Figure 4-12: La réponse Active des IDS/IPS

IV.3.1 la Différence entre la réponse active et passive:

Type de Réponse	Avantages	Inconvénients
Réponse Active	- Permet de couper rapidement et simplement une connexion suspecte.	- N'est envisageable qu'en environnement TCP. - Permet a l'IPS d'être découvert. - Aucun garantie quant a l'authenticité de la source. - Risque de se voir exposer de la part du pirate.
Réponse Passive	- L'IPS demeure furtif - Fonctionne avec tout type de protocole	-Nécessite un firewall externe. - Aucune garantie quant a l'authenticité de la source .

Tableau 4-1: Les avantages et inconvénients entre la réponse active et passif

IV.4 Classification des Attaques pour l'évaluation des IDS/IPS:

Comme indiqué dans la ***Figure 4-13***, notre classification repose sur cinq dimensions. Ces dimensions sont sélectionnées de manière à couvrir les sources, les cibles et les manifestations des attaques, informations nécessaires et suffisantes pour le test des IDS. Ces dimensions sont les suivants :

- **Source :** indique l'endroit d'où l'attaque a été lancée. Elle possède deux classes : locale et distante.
- **Privilège obtenu :** nous distinguons quatre classes, les classes "root" et "utilisateur" signifient respectivement que l'attaquant a réussi à obtenir l'accès "root/administrateur", resp. "utilisateur" ; la classe "système" qui permet l'exécution de processus avec les privilèges "système" ; la quatrième classe "aucun" couvre les attaques qui n'ont besoin d'aucun privilège d'accès au système, ex. attaques de reconnaissance (scans).
- **Vulnérabilité :** d'un point de vue de l'évaluateur, il est intéressant d'exprimer la relation entre les attaques et les vulnérabilités exploitées; ceci va en particulier aider à choisir (lors de la phase de test) les attaques qui exploitent ces vulnérabilités, et qui sont d'ailleurs répertoriées et disponibles dans des bases de données standardisées de vulnérabilités.
- **Moyen par lequel l'attaque est lancée :** trafic réseau, action exécutée directement sur la machine et qui n'apparaît pas dans l'interface réseau.
- **Cible :** qui peut être la mémoire, le système d'exploitation, la pile réseau, le système de fichier ou un processus.

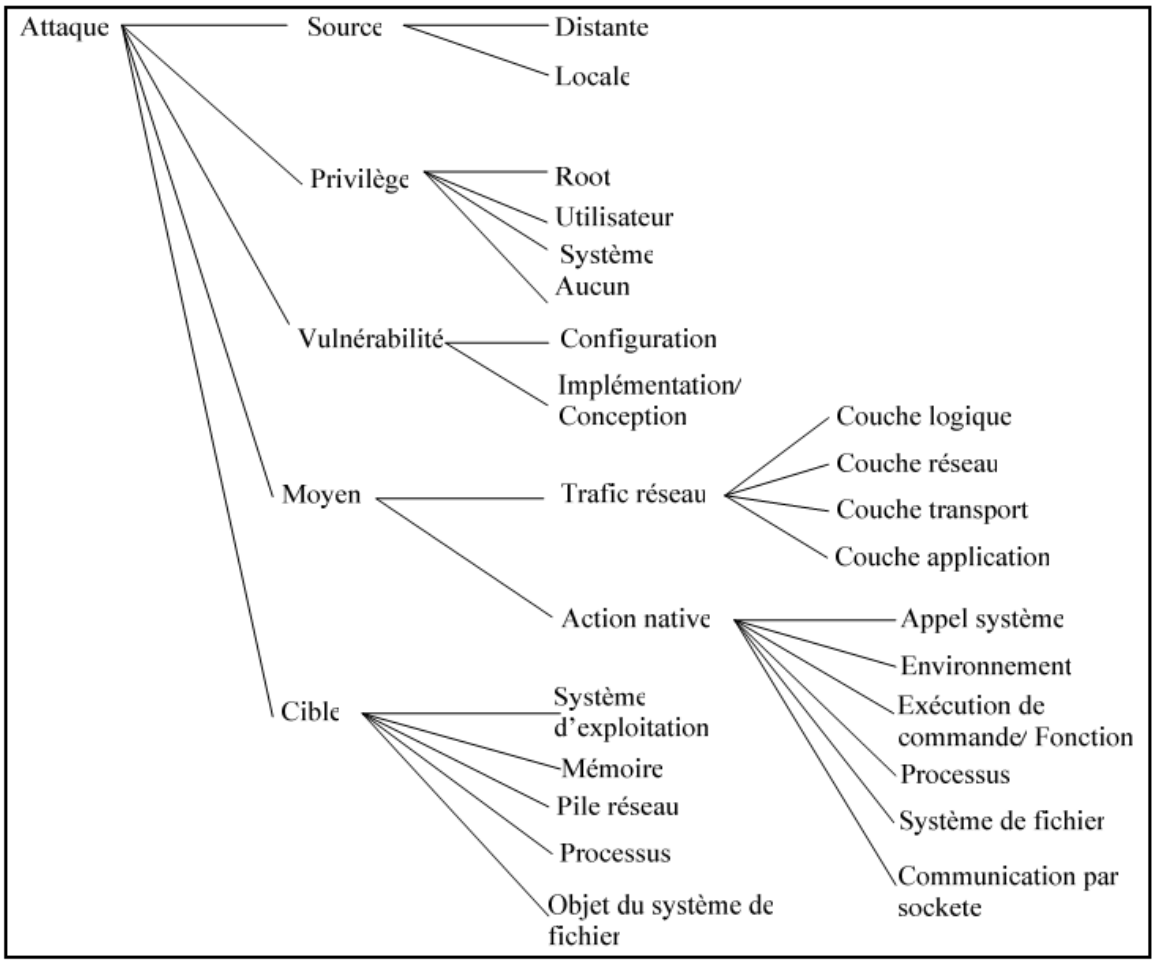


Figure 4-13: Nouvelle Classifications: Classe et attribue

IV.5 Comparaison entre Les IDS et Les IPS:

Détection d'intrusion	Prévention d'intrusion
HIDS **Le Pour:** - Peut détecter l'utilisation d'un système qui viole la politique de sécurité de l'entreprise. - Peut alerter sur des changements au niveau du système tels qu'une importante modification de fichier. **Le Contre:** - Le coût du déploiement et de la gestion est élevée puisque chaque hôte doit être équipé et une politique doit être développée. - La plupart des fabricants de HIDS ne construisent pas un produit destiné aux postes de travail, ainsi seuls les serveurs sont protégés. - La détection est généralement "a posteriori" dans la courbe de réponse. Une détection réussie vient d'une tentative réussie d'attaque. **NIDS** **Le Pour:** - Les systèmes basés sur la détection d'anomalie peuvent détecter une attaque même sur les systèmes qui emploient le cryptage (ils ne voient pas les exploits, ils voient la circulation anormale résultant d'une attaque réussie) - L'observation du trafic avec un système basé sur des règles peut aider à imposer une utilisation du réseau en respectant la politique de l'entreprise.	**HIPS** **Le Pour:** - Assure une protection contre les attaques inconnues. - Exige peu ou aucune mise à jour de sécurité dans une période annuelle. - Empêche les attaques de s'exécuter sur une machine au niveau noyau plutôt que de détecter les résultats d'une attaque réussie. **Le Contre:** - Le coût de tout le système peut être élevé puisqu'un agent est nécessaire pour chaque serveur et/ou poste de travail critique. - Le temps de déploiement afin d'équiper chaque serveur/poste de travail peut être long. - Le produit nécessite un ajustement après l'installation initiale pour être un outil de sécurité parfaitement fonctionnel. - Peut arrêter des applications légitimes en cas de mauvais ajustement. De nouvelles applications ont peut-être besoin d'être examinées par les HIPS avant qu'elles soient déployées. **NIPS** **Le Pour:** - Peut arrêter la propagation des vers si déployé correctement sans arrêter le trafic. - Protège contre de nouvelles attaques avant que le code d'exploit soit sorti (dans la plupart des cas). - Réduira le coût de la réponse aux incidents (puisque la plupart des réponses aux incidents sont automatiques).

Le Contre: - Le coût du facteur "humain" est élevé pour surveiller les événements et pour répondre aux incidents. - À moins qu'un plan de réponse ne soit conçu et mis en place, l'IDS fournit peu ou aucune sécurité. - Un déploiement réussi demande un important ajustement de l'IDS pour réduire au minimum les faux positifs.	**Le Contre:** - Le coût du déploiement NIPS au sein d'un réseau peut être important. - Puisque les NIPS sont un dispositif intégré au réseau, ils créent un point de défaillance bien qu'il y ait des méthodes pour traiter ce problème. L'approche la plus commune est d'ajouter des éléments redondants, sachant que tout le trafic de réseau traverse le NIPS. - Un NIPS nécessite toujours des mises à jour de sécurité pour être vraiment efficace.

Tableau 4-2: La comparaison entre les IDS et Les IPS.

Conclusion:

Les équipements IDS/IPS sont actuellement des produits mûrs et aboutis. Ils continuent d'évoluer pour répondre aux exigences technologiques du moment mais offrent d'ores et déjà un éventail de fonctionnalités capables de satisfaire les besoins de tous les types d'utilisateurs.

Néanmoins, comme tous les outils techniques ils ont des limites que seule une analyse humaine peut compenser. Un peu comme les Firewalls, les IDS/IPS deviennent chaque jour meilleurs grâce à l'expérience acquise avec le temps mais ils deviennent aussi de plus en plus sensibles aux problèmes de configuration et de paramétrage.

L'IPS utilise la technique de détection d'anomalie de protocole ainsi que la détection par correspondances de motifs en mode stateful (avec état). Il ne serait toutefois pas capable de détecter toutes les attaques contre un système de la VOIP sans compléter ces techniques par la méthode comportementale.

Dans le chapitre suivant en passe a la mise en place d'une solution Open source du NIPS Snort. En montrant par la suite le rôle important qui joue se dernier dans la prévention contre les attaque qui cible les infrastructures VOIP.

Chapitre V:

Audite et Mise en place d'une Solution Open source du NIDS Snort dans un système basé sur un PABX Asterisk.

Introduction:

Dans ce chapitre en décrit la mise en place d'une solution de détection d'intrusion réseau en utilisant les outils open source suivants :
SNORT (système de détection d'intrusion réseaux (NIDS)), Barnyard qui est une couche applicative qui exploite les événements générés par Snort au format « unifié », oinkmaster qui est un script simple de gestion et de mise à jour de règles Snort et enfin l'outil Base est une interface web permettant la gestion des alertes générées par snort. Cette partie descriptive de la solution sera guidée par les besoins fonctionnels de cette solution.

V.2 les Besoins:

La capture des besoins fonctionnels est une étape primordiale, sur son exhaustivité et sa qualité repose une grande partie de la réussite ou l'échec de la solution à mettre en place. Les besoins sont comme suit :

- ✓ Installation & configuration du Snort.
- ✓ Installation & Configuration de la Base de données MYSQL avec SNORT.
- ✓ Installation du Serveur web APACHE.
- ✓ Installation & Configuration de l'Interface WEB BASE avec MYSQL.
- ✓ Installation un serveur SSH pour sécuriser la communication entre interlocuteurs.

V.3 Plateforme De Test:

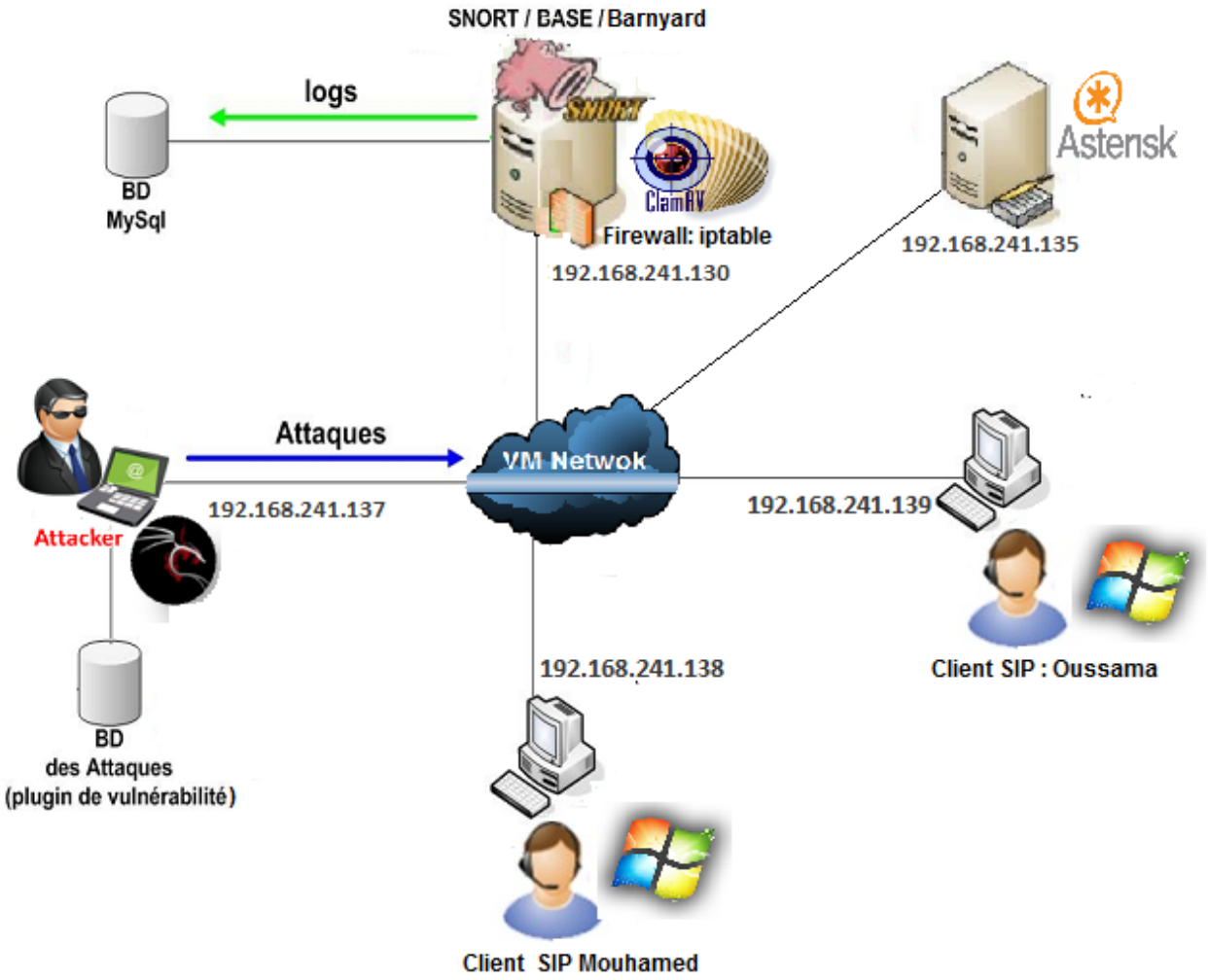


Figure 5.1 : Architecture sécurisé avec SNORT

V.4 Description Des Stations:

TYPE	FONCTION	SERVICE	ADRESSE IP
Asterisk IPBX	Serveur a audité	TelIP	192.168.241.135
Windows XP SP3	EyeBeam	Client SIP	192.168.241.139 192.168.241.138
Ubuntu 10.0.4.2 LTS	Snort	Apache, MySQL, PHP, BASE, SSH, SSL	192.168.241.130
Backtrack 5 R3	Outil d'audite	Metasploit, Nmap, SIPCrack...	192.168.241.137

Tableau 5-1: Description des stations.

V.5 Préparation Des Stations:

V.5.1. Installation du serveur Asterisk sous Linux Ubuntu 10.0.4 LTS:

V.5.1.1 Présentation d'Asterisk:

Asterisk est un PBX-IP, ou IP PBX ou encore IPBX. Complet et performant, il offre une plate-forme personnalisable et modulable pour la mise en œuvre de services de téléphonie. Il garantit une très large interconnexion avec plusieurs serveurs PBX, mais aussi avec des réseaux de téléphonie non-IP.

Asterisk étant un logiciel libre d'utilisation, ses sources sont téléchargeables sous licence GNU GPL (General Public License). Cela permet à une importante communauté de contribuer à son développement.

Il est aujourd'hui multiplateforme et s'installe aussi bien sur Linux, OpenBSD, Sun Solaris, MacOS X ou Windows.

V.5.1.2 Fonctionnalités:

Asterisk propose toutes les fonctionnalités d'un standard téléphonique de niveau professionnel, des plus élémentaires aux plus complexes. Non seulement, il permet de gérer le routage des appels au sein du réseau, mais en plus il supporte une large gamme de services, notamment les suivants (pour la liste exhaustive, voir le site de l'éditeur, à l'adressehttp://www.asterisk.org) :

• Authentification des utilisateurs appelants.
• Serveur vocal, ou standard d'accueil téléphonique automatisé, aussi appelé IVR (Interactive Voice Response). Cette fonction permet de demander à l'appelant le service qu'il souhaite utiliser et d'effectuer le routage correspondant.
• Numérotation abrégée pour définir des raccourcis.
• Transfert d'appel.
• Filtrage des appels.
• Messagerie vocale (répondeur automatique).
• Notification et écoute par e-mail des messages laissés sur son répondeur (voice mail).
• Gestion des conférences.
• Double appel.
• Mise en attente.
• Journalisation des appels.

• Facturation détaillée.
• Enregistrement des appels.

Le logiciel peut être utilisé comme une passerelle ToIP hétérogène. Par exemple, des utilisateurs utilisant différents protocoles de signalisation, comme H.323 ou SIP, peuvent être mis en relation. C'est le logiciel qui se charge d'effectuer les conversions de signalisation. De la même manière, il peut servir de passerelle pour joindre des correspondants dans le réseau téléphonique RTC.

V.5.1.3 Configuration d'asterisk:

Dans se qui suit en suppose que le serveur Asterisk est préalablement installer, pour le cette architecture, nous avons besoin de crée deux comptes SIP. Pour cela nous avons besoin d'éditer deux fichiers de base; ***sip.conf*** et ***extensions.conf***.

V.5.1.3 .1 Configuration des comptes sip:

» sip.conf: On ajoute les deux compte client comme suite au début ou la fin du fichier.

```
[oussama]
type=friend
host=dynamic
username=oussama
secret=pc
context=test
callerid="oussama" <111>
mailbox=oussama@192.168.244.146

[mohamed]
type=friend
host=dynamic
username=mohamed
secret=pc
context=test
callerid="mohamed" <222>
mailbox=mouhamed@192.168.244.146
```

» extensions.conf : on doit crée le contexte "test" et ajouté les lignes suivante dans le contexte default.

```
exten => 111,1,Dial(SIP/oussama,60)

exten => 222,1,Dial(SIP/mohamed,60)
```

V.5.1.3 .2 lancement du serveur Asterisk et l'établissement de la liaison entre les interlocuteurs:

Le lancement du serveur Asterisk a l'aide de la commende suivant:

 # asterisk -vvvvc

Une fois sur la console en recharge le fichier sip:

CLI> sip reload

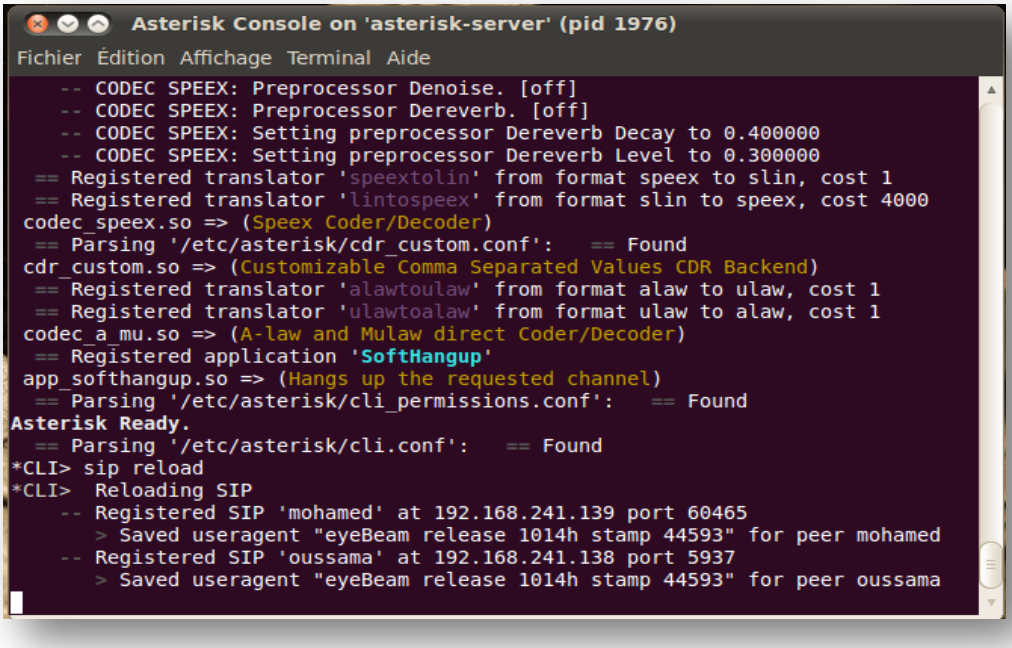


Figure 5.2 : activation du serveur Asterisk

V.5.2 Préparation du softphone EyeBeam:

Pour crée un compte SIP sur eyeBeam, en suit la démarche suivante:

» cliquer sur sip Account Setting.

» cliquer sur add et remplisser les informations nécessaire, comme c'est mentionner sur la Figure suivante **(voir Figure 5.3)**

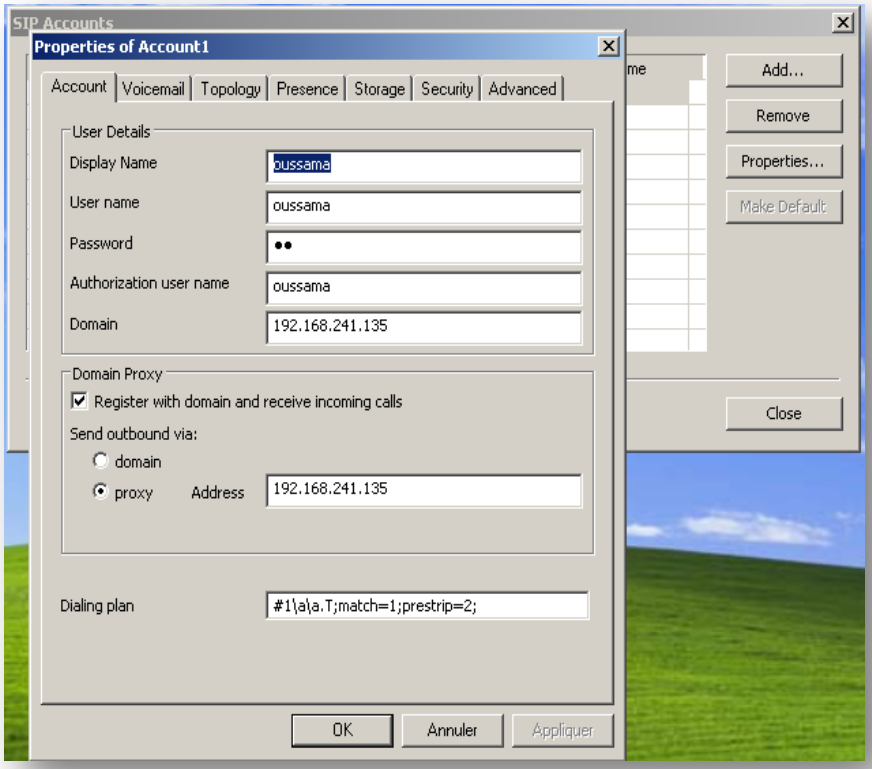


Figure 5.3: création du compte SIP sous eyeBeam

Établissement de la connexion avec le serveur Astersik comme nous montre la Figure suivante.

Figure 5.4: Établissement de la liaison Serveur-client

V.5.3 Présentation de l'outil d'audite (BACKTRACK V5 R3):

V.5.3.1: Présentation de BACKTRACK:

Backtrack 5 est une distribution Linux gratuite basée sur Ubuntu Lucid LTS. Cette distribution est destinée à tous ceux qui souhaitent faire du pentesting et plus généralement de la sécurité informatique.

La téléphonie sur IP (Voice Over IP) est une technologie de plus en plus utilisée offrant de nombreux avantages (conversation a plusieurs, enregistrement de conversations, mobilité) a cout réduit. De plus en plus d'entreprises remplacent leur ancienne architecture téléphonique au profit de la VOIP. Cependant, la principale faiblesse de cette technologie est la capture d'écoute téléphonique. En effet, vu que la conversation s'établit par le biais du réseau, il n'est pas difficile pour un hacker d'intercepter cette conversation. Wireshark, logiciel d'écoute réseau, dispose d'un outil permettant la capture de trafic VOIP. Backtrack met également a notre portée une panel de logiciels nous permettant d'auditer un réseau VOIP, allant du simple diagnostic (grâce a SIPsak) à la tentative d'intrusion de ce réseau (grâce a SIPcrack)

Figure 5.5. : Environnement BACKLTRACK V5

V.5.3.2 Les Outils:

Backtrack inclut ces nombreux logiciels: Metasploit, RFMON, pilote sans-fil, Aircrack-NG, Gerix Wifi, Cracker, Kismet, Nmap, Ophcrack, Ettercap, Wireshark (Aussi connu en tant qu'Ethereal) et de dizaine d'autres.

Pour notre audit en s'intéressera que aux outils dédié a la VOIP, tel-que:

- Metasploit test des Vulnérabilités des systèmes et des applications.
- Nmap (analyseur de réseaux).
- Sipviscious et SIPcrack (cracker des comptes SIP).

V.5.4 Mise en place d'IDS/IPS Open source Snort:

V.5.4.1Présentation de SNORT:

Snort est un système de détection d'intrusion réseau (NIDS) open source, disponible sous licence GPL, fonctionnant sur les systèmes Windows et linux.

Dans cette partie on va installer la dernière version de Snort « Snort 2.8.5» qui est disponible depuis son site official http://www.snort.org/ sous un système d'exploitation linux Ubuntu 10.0.4 LTS.

Snort est capable d'effectuer en temps réel des analyses de trafic et de logger les paquets sur un réseau IP. Il peut effectuer des analyses de protocole, recherche/correspondance de contenu et peut être utilisé pour détecter une grande variété d'attaques et de sondes comme des dépassements de buffers, scans, attaques sur des CGI, sondes SMB, essai d'OS finger printings et bien plus.

Pour effectuer ces analyses snort se base sur des règles. Celles-ci sont écrites par Sourcefire ou bien contribuées par la communauté. On l'utilise en général pour détecter une variété d'attaques et de scans tels que des débordements de mémoire, des scans de ports, des attaques CGI, des tentatives de déni de service (DOS). Dans cette partie en va expliquer les différentes étapes pour mettre en place un NIDS avec une base de données MySQL pour les logs.

Snort peut également être utilisé avec d'autres projets open sources tels que Barnyard et BASE (qui utilise ACID) afin de fournir une représentation visuelle des données concernant les éventuelles intrusions.

V .5.4.2 Architecture de Snort :

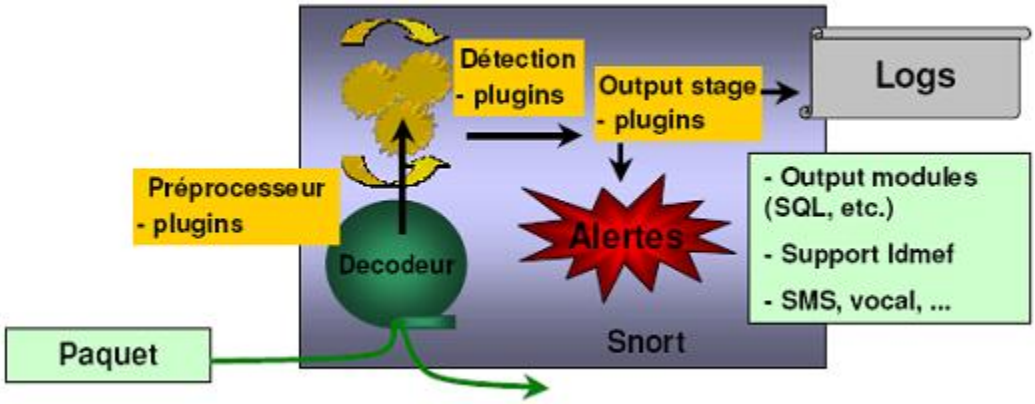


Figure 5.6 : Architecture Snort

Un noyau de base : (Packet Decoder) au démarrage, ce noyau charge un ensemble de règles, les compile, les optimise et les classe. Durant l'exécution, le rôle principal du noyau est la capture des paquets.

Une série de pré–processeurs: (Detection Engine) ces derniers améliorent les possibilités de SNORT en matière d'analyse et de recomposition du trafic capturé. Ils reçoivent les paquets directement capturés et décodés, les retravaillent éventuellement puis les fournissent au moteur de recherche des signatures pour les comparer avec a base des signatures.

Une série de « Detection plugins »: Les analyses se composent principalement de comparaison entre les différents champs des headers des protocoles (IP, ICMP, TCP et UDP) par rapport à des valeurs précises.

Une série de « output plugins »: permet de traiter cette intrusion de plusieurs manières : envoie vers un fichier log, envoie d'un message d'alerte vers un serveur syslog, stocker cette intrusion dans une base de données SQL.

V .5.4.3 Fonctionnalités du Snort:

V .5.4.3.1 Mode Sniffer :

C'est le mode basic, il permet de lire et afficher à l'écran les paquets TCP/IP circulant dans le réseau :

snort–v : Cette commande permet d'exécuter et d'afficher les entêtes des paquets TCP/IP.

snort–vd : Cette commande permet d'exécuter SNORT et d'afficher tout le paquet TCP/IP (entête et données).

snort –vde : Cette commande permet d'exécuter SNORT et d'afficher tout le paquet TCP/IP (entête et données) ainsi que de l'entête de la couche liaison de données.

V .5.4.3.2 Mode journalisation « packet logger » :

L'option '-l répertoire ': Active le mode journalisation des paquets et spécifie le répertoire où sont stockés les alertes et les paquets capturés. Par défaut, le répertoire est /var/log/snort.

V .5.4.3.3 Mode Detection d'intrusion :

L'option'-c fichier': Active Snort en mode `Détection d'intrusion` On donne en paramètre le fichier de configuration des règles de détection. Par défaut, les alertes sont mémorisées dans le fichier alert.

V .5.4.3.4 Mode Prévention des intrusions réseau (IPS): SNORT_inline :

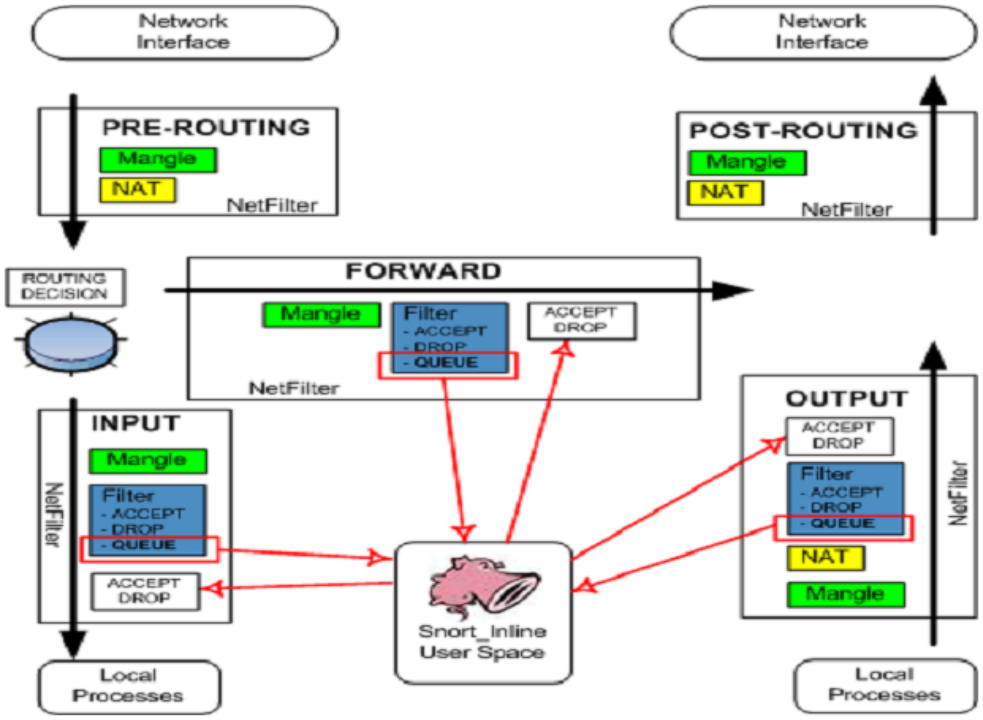


Figure 5.7: Fonctionnement du snort_inline

Avant d'exécuter snort_inline il faut lancer le module d'IPTABLES «ip_queue» :

#modprobe ip_queue

On peut vérifier l'exécution de ce module avec la commande :

#lsmod | grep ip_queue

Ce qui va activer la file d'attente d'iptable dans laquelle snort_inline va effectuer ces traitement sur les paquets.

Maintenant il reste à rediriger le trafic d'IPTABLES vers la file d'attente QUEUE:

#iptables -A INPUT -j QUEUE

On peut vérifier la redirection du trafic avec la commande :

#iptables -L

Dans notre cas, snort_inline et netfilter vont jouer le rôle d'IPS qui protégera la machine sur laquelle ils sont installés.

« INPUT » veut dire qu'on va contrôler le trafic qui arrive sur cette même machine,

mais dans le cas réel snort_inline est généralement installée sur une machine en amont d'un réseau (une machine par laquelle passe tout le trafic entrant au réseau) dans ce cas, on filtrera le trafic «FORWARD».

Exécution du Snort_inline:

#snort -Q -v -c /etc/snort/snort.conf -l /var/log/snort

-Q -> process the queued traffic

-v -> verbose

-l -> log path

-c -> config path

V.5.4.4 les règles de SNORT:

Les règles de SNORT sont composées de deux parties distinctes : le header et les options.

Le header permet de spécifier le type d'alerte à générer (alert, log et pass) et d'indiquer les champs de base nécessaires au filtrage : le protocole ainsi que les adresses IP et ports sources et destination.

Les options, spécifiées entre parenthèses, permettent d'affiner l'analyse, en décomposant la signature en différentes valeurs à observer parmi certains champs du header ou parmi les données.

Exemple de règle :

Alert tcp any any -> 192.168.1.0/24 80 (flags :A ;\content : "passwd"; msg: "detection de `passwd' " ;)

Cette règle permet de générer un message d'alerte "détection de passwd" lorsque le trafic à destination d'une machine du réseau local 192.168.0.0/16 vers le port 80, contient la chaîne « passwd » (spécifié par l'utilisation du mot-clé « content »), et que le flag ACK du header TCP est activé (flags : A).

V.5.4.2Installation & configuration:

V.5.4.2.1 Installation des dépendances Snort:

- ✓ **apache2 pour le serveur web:**

  #sudo apt-get install apache2

- ✓ **bison:**

  #sudo apt-get install bison

- ✓ **flex:**

  #sudo apt-get install flex

- ✓ **MySQL-server pour la base de données:**

  #sudo apt-get install mysql-server

  mot de passe de la base MySQL=test12345

Le processus d'installation consiste a l'installation de gestionnaire de base de données MySQL.

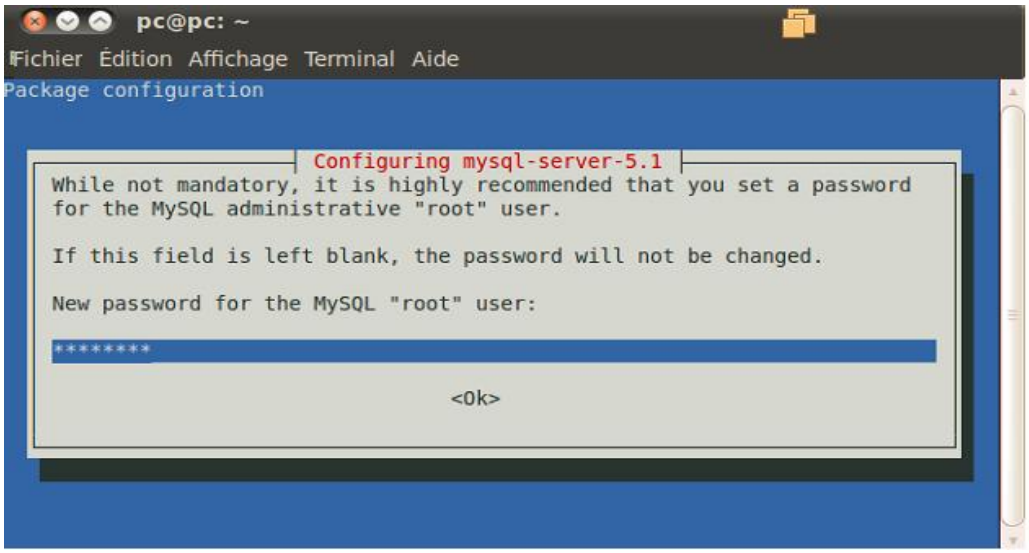


figure 5.8. : installation MySQL-server

- ✓ **php5 pour le script orienté serveur:**

  #sudo apt-get install php5

- ✓ **php5-MySQL pour la configuration du php avec mysql:**

  #sudo apt-get install php5-mysql

- ✓ **php5-gd pour la librairie graphique:**

  #sudo apt-get install php5-gd

- ✓ **libtool:**

  #sudo apt-get install libtool

- ✓ **PEAR pours 'PHP Extension' et 'Application Repository':**
  #sudo apt-get install php-pear
- ✓ **Iptables est un pare-feu sous linux:** pour rendre SNORT un IPS (SNORTinline).
  #sudo apt-get install iptables-dev
- ✓ **Clamav Anti-virus:**
  #sudo apt-get install clamav

V.5.4.2.2 Installation de Snort:

L'installation automatique du snort-mysql est très simple avec la commande :

#sudo apt-get install snort-mysql

Dans cette phase en devra donner l'adresse du réseau ou snort doit écouté, dans notre cas c'est le 192.168.0.0/16 masque du réseau : 255.255.0.0.

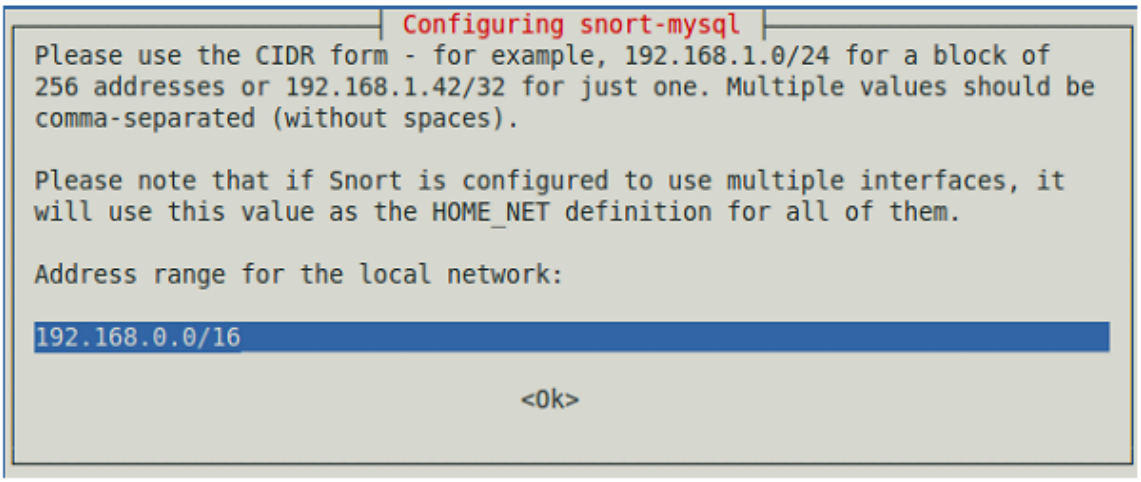


Figure 5.9: l'interface réseau de snort

- ➢ **Creation de la base de donné MySQL:**

```
mysql -u root -p
```

étape01: création de la table snort.

```
mysql> create database snort;
Query OK, 1 row affected (0.13 sec)

mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort@localhos
t;
Query OK, 0 rows affected (0.12 sec)

mysql> SET PASSWORD FOR snort@localhost=PASSWORD('Test12345 ');
Query OK, 0 rows affected (0.01 sec)

mysql> exit
Bye
snort@snort-desktop:~$
```

étape02: construction du schéma de la base crée.

```
mysql> exit
Bye
snortroot@snortroot-desktop:~$ cd /usr/share/doc/snort-mysql/
snortroot@snortroot-desktop:/usr/share/doc/snort-mysql$ zcat create_mysql.gz | m
ysql -u root -p snort
Enter password:
```

étape03: visualiser la base snort crée.

```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| snort              |
+--------------------+
3 rows in set (0.08 sec)

mysql>
```

étape04: afficher la table de la base snort sur la console MySQL en utilise la commande use snort pour sélectionner la base, et utiliser la commande show tables pour afficher la table.

En quitte la console MySQL a l'aide de la commende ***exit***.

- **Configuration du fichier snort.conf:** A fin d'ajouter ou de modifier des paramètres de configuration de snort, telle que définir le chemin vers le répertoire des règles.

```
sudo vim /etc/snort/snort.conf
```

En doit ajouter les lignes suivantes:

```
#var HOME_NET any
var HOME_NET $eth0_ADDRESS
```

Et ajouter la ligne:

```
output unified2: filename snort.log, limit 128
```

Cette linge donne l'information que la taille maximal du log ne dépassera pas 128MO.

V.5.4.2.3 Exécution de snort: la commende suivante permet de lancer snort avec nos paramètres de configuration

```
sudo snort -c /etc/snort/snort.conf -i eth0
```

Figure 5.10: Le Moniteur de SNORT

V.5.4.3 Installation Oinkmaster: cet outil permet à Snort de mettre à jours ces règles. Pour télécharger et mettre en place l'outil de Oinkmaster en utilisent les commandes ci-dessous:

• Télécharger et déballer la distribution Oinkmaster 2.0 est la dernière version. L'URL utilisée suppose que la source de Oinkmaster est disponible dans le miroir de téléchargement "easynews".

• Copiez le fichier de script oinkmaster.pl dans le répertoire / usr / local / bin sorte qu'il sera trouvé dans le chemin de l'exécutable.

• Copiez le fichier de configuration oinkmaster.conf dans / etc qui est où le oinkmaster.pl script chercher par défaut.

```
cd /usr/src
wget http://easynews.dl.sourceforge.net/sourceforge/oinkmaster/oinkmaster-
2.0.tar.gz
tar xzvf oinkmaster-2.0.tar.gz
cd oinkmaster-2.0
cp oinkmaster.pl /usr/local/bin
cp oinkmaster.conf /etc
```

en suite en va conFigurer Oinkmaster:

```
vi /etc/oinkmaster.conf
```

ou en va déffinir le chemin d'ou Oinkmaster va télécharger les rules (règles)

```
# URL examples follows. Replace <oinkcode> with the code you get on the
# Snort site in your registered user profile.

# Example for Snort 2.4
url = http://www.snort.org/pub-
bin/oinkmaster.cgi/234ef981dab34964db36f1f209fed1f5b7891a3/snortrules-
snapshot-2.4.tar.gz

# Example for Snort-current ("current" means cvs snapshots).
# url = http://www.snort.org/pub-bin/oinkmaster.cgi/<oinkcode>/snortrules-
snapshot-CURRENT.tar.gz
```

a la fin en doit ajouter le script suivant afin que Oinkmaster peut envoyer la mise a jours vers le répertoire snort/rules.

```
oinkmaster.pl -o /etc/snort/rules
```

V.5.4.4 Installation de la Console Base :

Base va jouer le rôle d'un Moniteur pour Snort. Ces étapes sont nécessaires pour faire fonctionner ADOdb avec BASE.

Ainsi, ADOdb est une couche qui se trouve entre PHP et les bases de données. Qui permet de communiquer de la même manière que toutes les bases de données en PHP. PHP est utilisé afin que toute base de données soit abstraite.

Les étapes sont comme suites:

A - a fin que BASE prend en considération les message SMTP:

```
sudo pear install --alldeps Mail
sudo pear install --alldeps Mail_Mime
```

```
sudo aptitude install php-mail
sudo aptitude install php-mail-mime
```

```
) packages upgraded, 2 newly installed, 0 to remove and 62 not upgraded.
Need to get 34.3kB of archives. After unpacking 242kB will be used.
Do you want to continue? [Y/n/?] y
Writing extended state information... Done
Get:1 http://tr.archive.ubuntu.com/ubuntu/ lucid/universe php-mail-mimedecode 1.
5.0-3 [14.0kB]
Get:2 http://tr.archive.ubuntu.com/ubuntu/ lucid/universe php-mail-mime 1.5.3-0.
1 [20.3kB]
Fetched 34.3kB in 0s (46.3kB/s)
Selecting previously deselected package php-mail-mimedecode.
(Reading database ... 126314 files and directories currently installed.)
Unpacking php-mail-mimedecode (from .../php-mail-mimedecode_1.5.0-3_all.deb) ...
Selecting previously deselected package php-mail-mime.
Unpacking php-mail-mime (from .../php-mail-mime_1.5.3-0.1_all.deb) ...
Setting up php-mail-mimedecode (1.5.0-3) ...
Setting up php-mail-mime (1.5.3-0.1) ...
Reading package lists... Done
Building dependency tree
Reading state information... Done
Reading extended state information
Initializing package states... Done
Writing extended state information... Done
```

figure 5.11 : "Php-mail" et "php-mail-mime"

B- Installation de BASE et ODODB:

Création d'un répertoire temporaire qui va contenir les installable des deux applications

```
cd
mkdir snortinstall
cd snortinstall
```

installation des deux composants:

```
cd ~/snortinstall
tar -xzvf adodb4991.tgz
tar -xzvf base-1.4.5.tar.gz
sudo mv adodb /var/www
sudo mv base-1.4.5 /var/www
```

C- configuration du fichier php.ini:

```
sudo vim /etc/php5/apache2/php.ini
```

et ajouter les lignes suivantes:

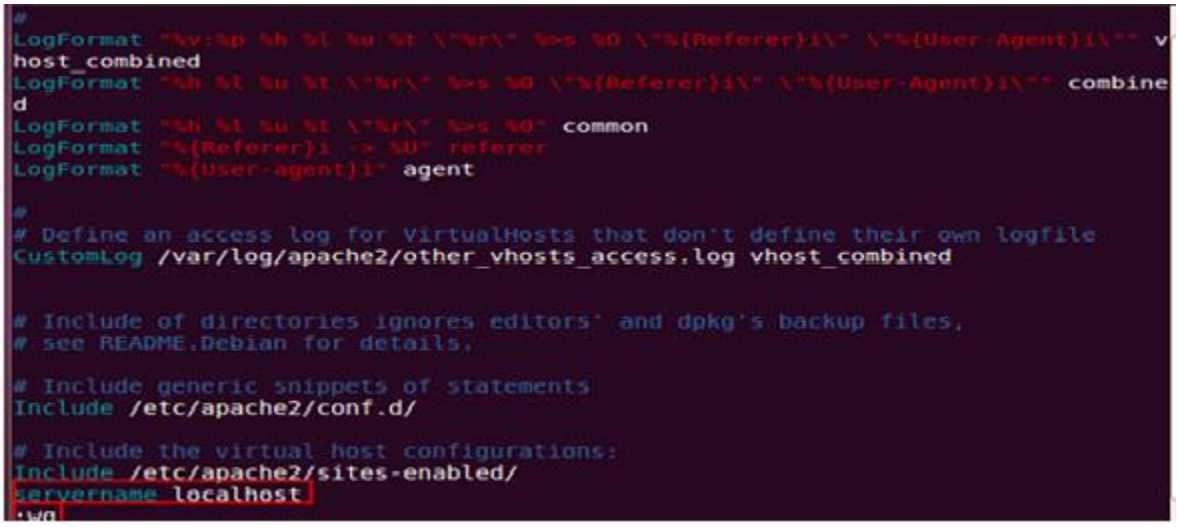
```
extension=mysql.so
extension=gd.so
```

D- configuration du fichier Apache2.conf:

```
sudo vim /etc/apache2/apache2.conf
```

et ajouter la ligne suivante:

```
servername localhost
```



une fois terminer, en redémarre le server web apache

```
sudo /etc/init.d/apache2 restart
```

E- configuration de Base:

Afin d'éviter toute faille de sécurité, en remet le dossier base en lecture seule.

```
cd /var/www
sudo ln -s base-1.4.5 ./base
chmod a+w base
```

F- lancement de BASE:

en ouvre le navigateur web, et dans la barre d'adresse en introduit le lien suivant:

http://localhost/base

G- configuration de BASE:

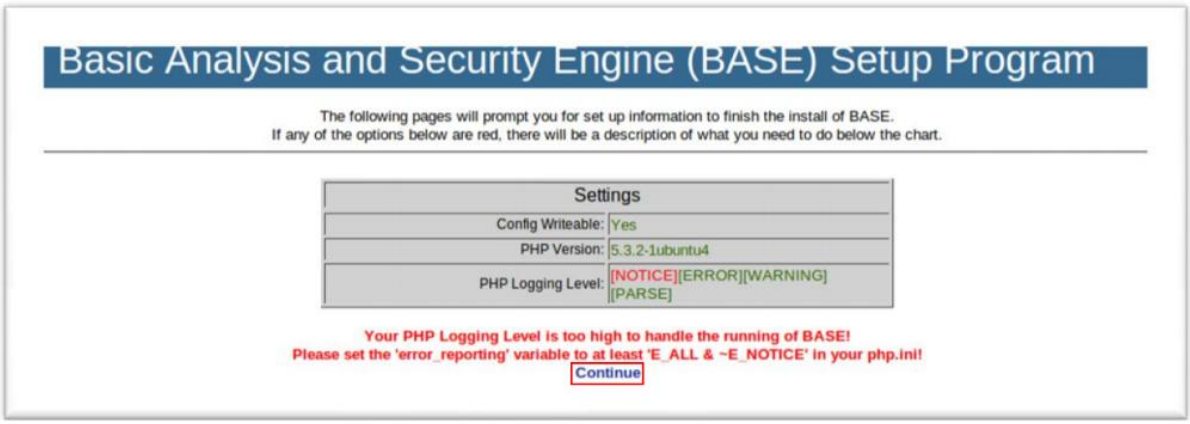
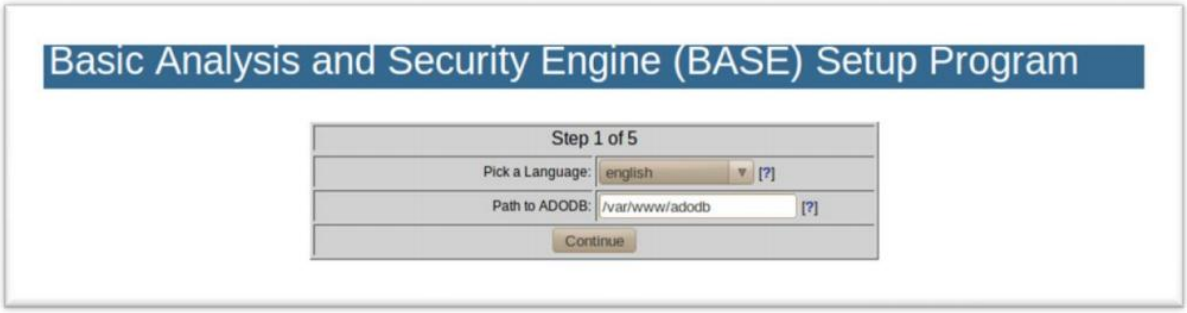


figure 5.12: configuration de base

Etape 1: Donner le chemin de ADOdb "/ var / www / adodb "



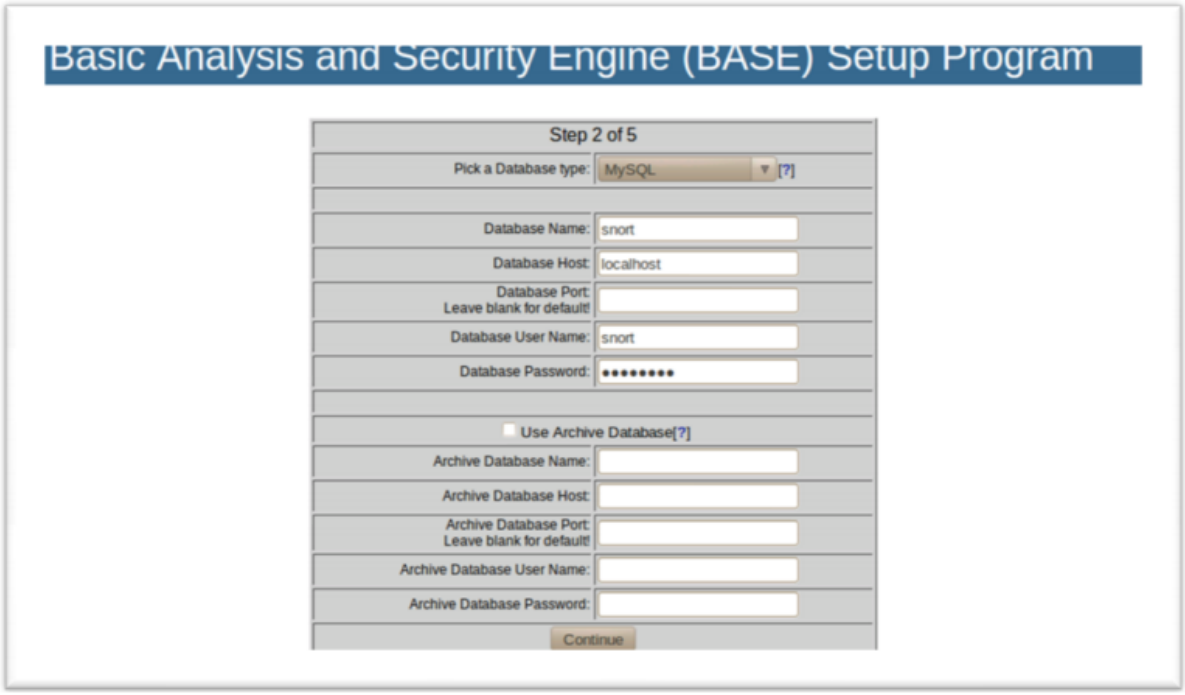
Etape 2: Entrez les valeurs appropriées dans les champs.

Database Name = snort

Database Host = localhost

Database User = snort

Database Password = “test12345”



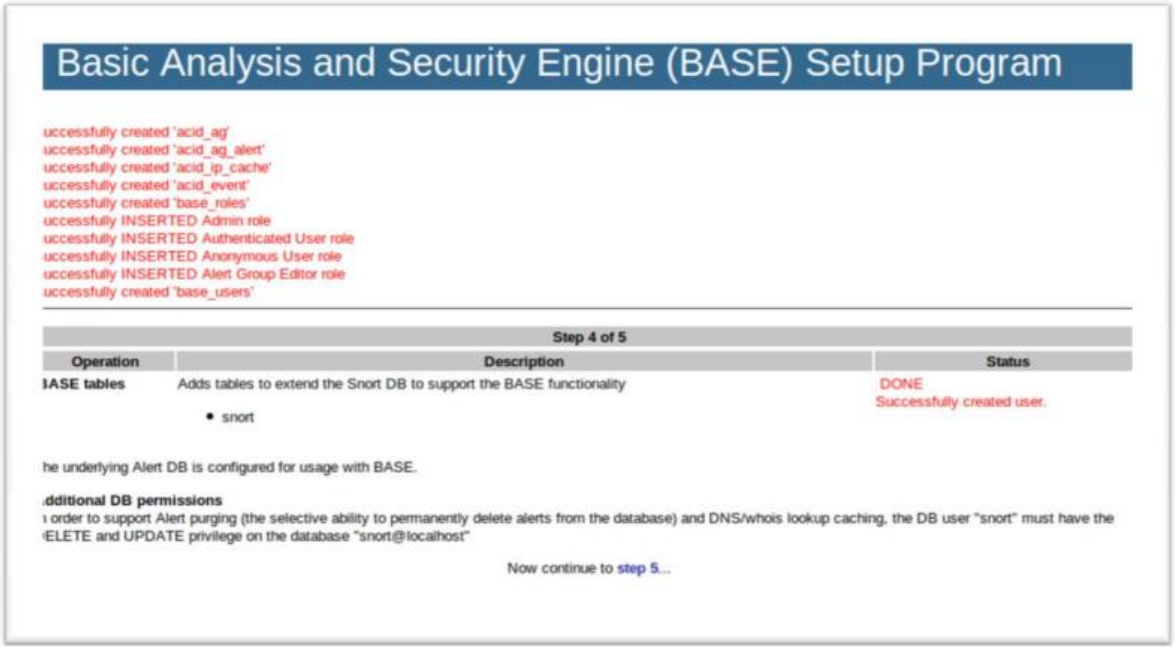
Etape 3: Crée le compte administrateur qui va gérée BASE.

Admin User Name: snort

Password: admin

Full Name: snort

Etape 4: Création de BASE Agent.



Etape 5: écran de connexion BASE.

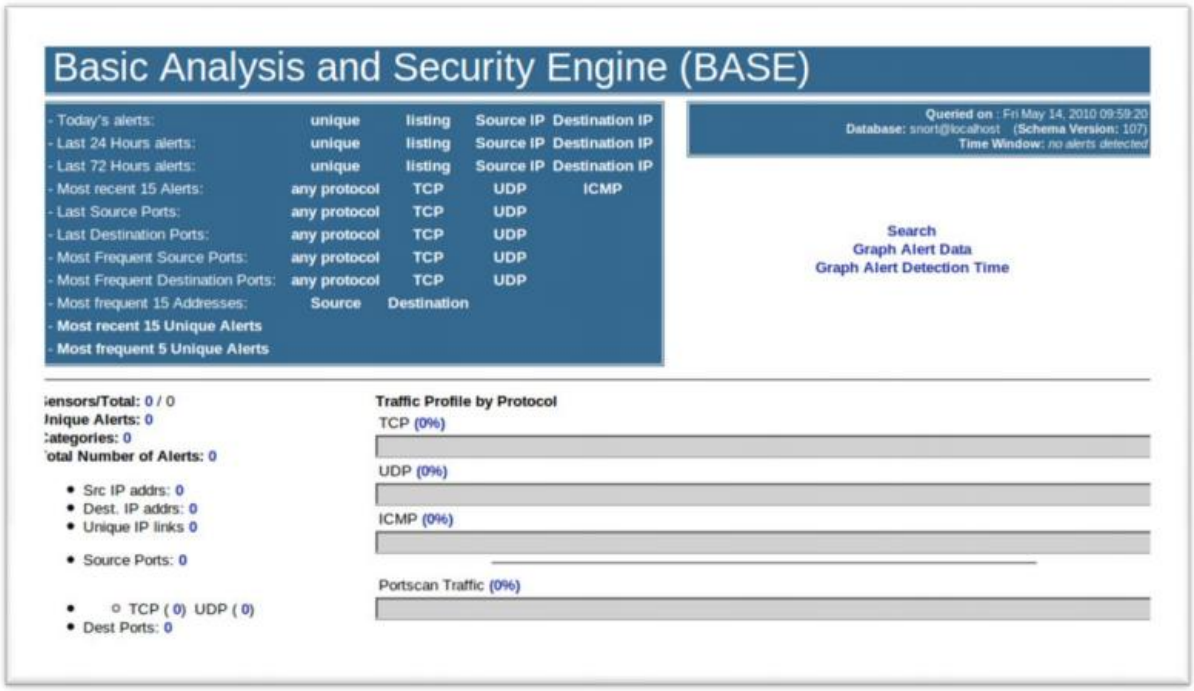


Figure 5.13: Le Moniteur BASE.

Enfin, la commande "BASE" pour lire et écrire les droits de la série sont donnés.

```
chmod og-w base
```

V.5.4.5 Installation de BARNYARD:

Snort prend beaucoup de temps durant la détection d'intrusion. ainsi BARYARD a pour rôle de générer le flux par snort (les logs) vers BASE. pour le mettre en œuvre, en suit les étapes suivante:

```
cd ~/snortinstall
wget -O barnyard2-1.7.tar.gz \
http://www.securixlive.com/download/barnyard2/barnyard2-1.7.tar.gz
tar zxvf barnyard2-1.7.tar.gz
cd barnyard2-1.7
./configure --with-mysql
make
sudo make install
sudo cp etc/barnyard2.conf /etc/snort
sudo mkdir /var/log/barnyard2
```

Modifier les paramètres de configuration sur "barnyard2.conf"

```
sudo vim /etc/snort/barnyard2.conf
```

Ajouter les lignes suivantes:

```
config hostname: localhost
```

```
config interface: eth0
```

```
# to ensure that any plugins requiring some level of uniqueness in their output
# the alert with interface name, interface and hostname directives are provided.
# An example of usage would be to configure them to the values of the associated
# snort process whose unified files you are reading.
#
# Example:
#   For a snort process as follows:
#     snort -i eth0 -c /etc/snort.conf
#
#   Typical options would be:
#     config hostname:  thor
#     config interface: eth0
#     config alert_with_interface_name
#
config hostname: localhost
config interface: eth0
# enable printing of the interface name when alerting.
#
```

figure 5.14: configuration de BARNYARD

a la fin du fichier en ajoute la lignes suivante:

```
output database: alert, mysql, user=snort password=Test12345 dbname=snort
host=localhost
```

V.5.4.6 Exécution de Snort avec Barnyard :

```
sudo snort -c /etc/snort/snort.conf -i eth0
```

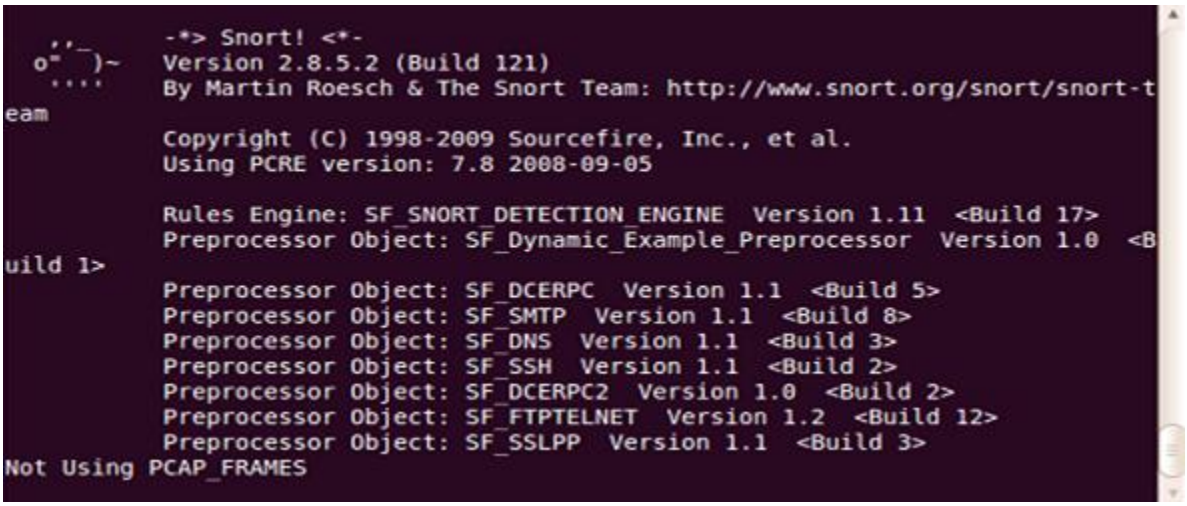
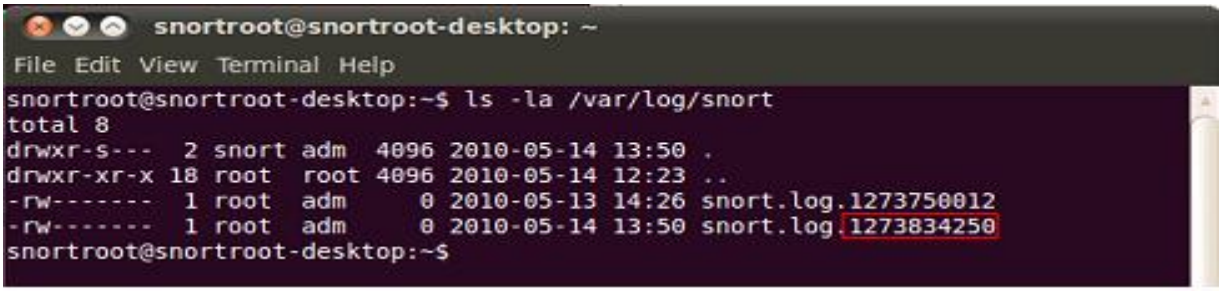


figure 5.15: le Moniteur de snort sur le shell Linux

Récupération du numéro de log : ouvrir un 2eme terminal

```
ls -la /var/log/snort
```




```
sudo vim /var/log/snort/barnyard.waldo
```

```
snortroot@snortroot-desktop: ~
File Edit View Terminal Help
/var/log/snort
snort.log
<1273834250>
0
```

Démarrage Barnyard:

```
sudo /usr/local/bin/barnyard2 -c /etc/snort/barnyard2.conf \
-G /etc/snort/gen-msg.map -S /etc/snort/sid-msg.map \
-d /var/log/snort -f snort.log -w /var/log/snort/barnyard.waldo
```

V.6 TEST D'AUDITE:

Scénario d'attaque n°1: Détection des périphériques SIP Sur le réseau:

Machine Cible	@ Machine Cible	Service Ciblé	Port ciblé	@Machine source
Serveur Asterisk	192.168.241.134	TELIP	5060	192.168.241.137

Étape 1: Récolte d'information sur les périphérique existant sur le réseau: Backtrack fourni un utilitaire puisant qui permet de balayer un réseau donner et de récolter des informations concernant les machine existante sur se réseaux

```
nmap -PN -v -O 192.168.241.0/24
```

```
Nmap scan report for 192.168.241.138
Host is up (0.0012s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:70:8B:B7 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
```

figure 5.16: Une partie du résultat du scan de Nmap.

Étape 2: Détection des périphériques SIP:

Sa consiste a identifier sur le réseau les périphérique SIP tel que les BAPX et les clients SIP qui utilise comme protocole de session SIP avec le port UDP 5060. Backtrack fourni un kit complet dédié a la pentest des plateformes VOIP. La commande ***smap*** permet de balayé un réseau donner et d'identifier tous le composant SIP.

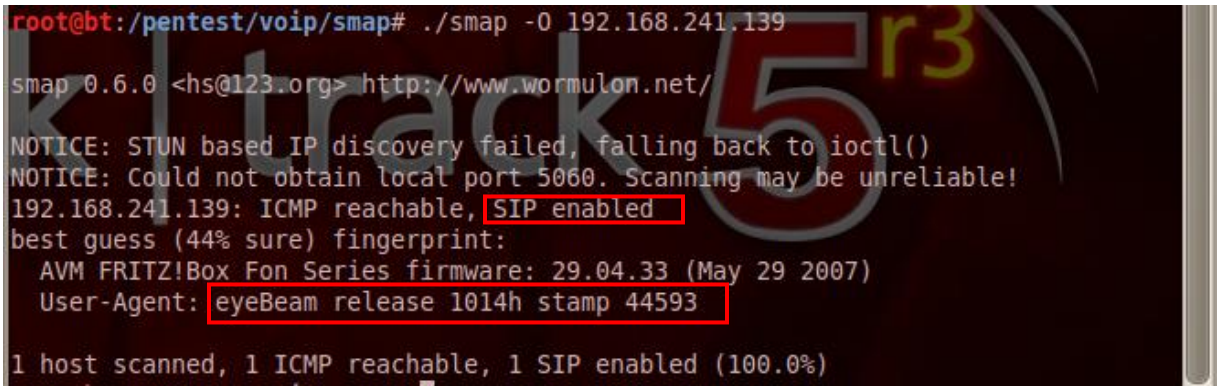


figure 5.17: indentification du client eyeBeay avec smap

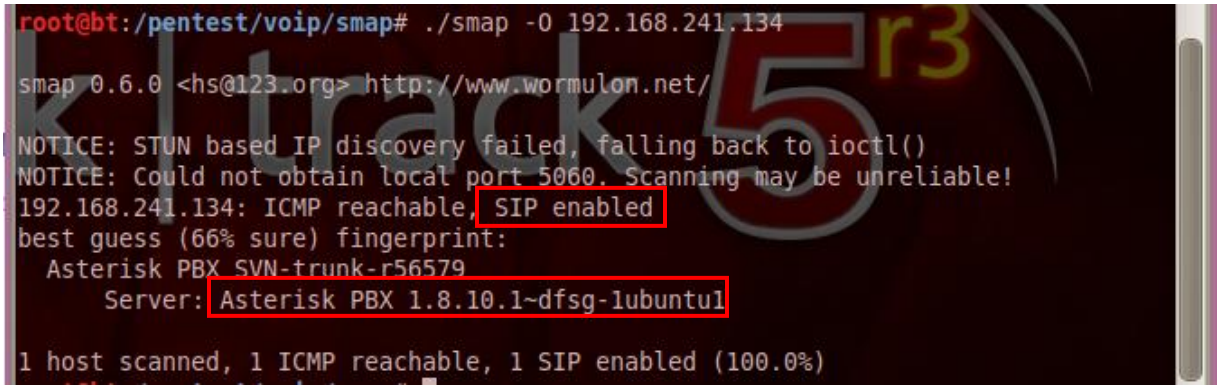


figure 5.18: indentification du serveur Asterisk avec smap

smap permet comme d'après la ***Figure 5.18*** *et la* ***Figure 5.19*** d'identifier les périphérique SIP ainsi que leur type et leur nom (client ou serveur).

Étape 3 : Détection d'attaque par Snort:

A- détection du scan smap par snort:

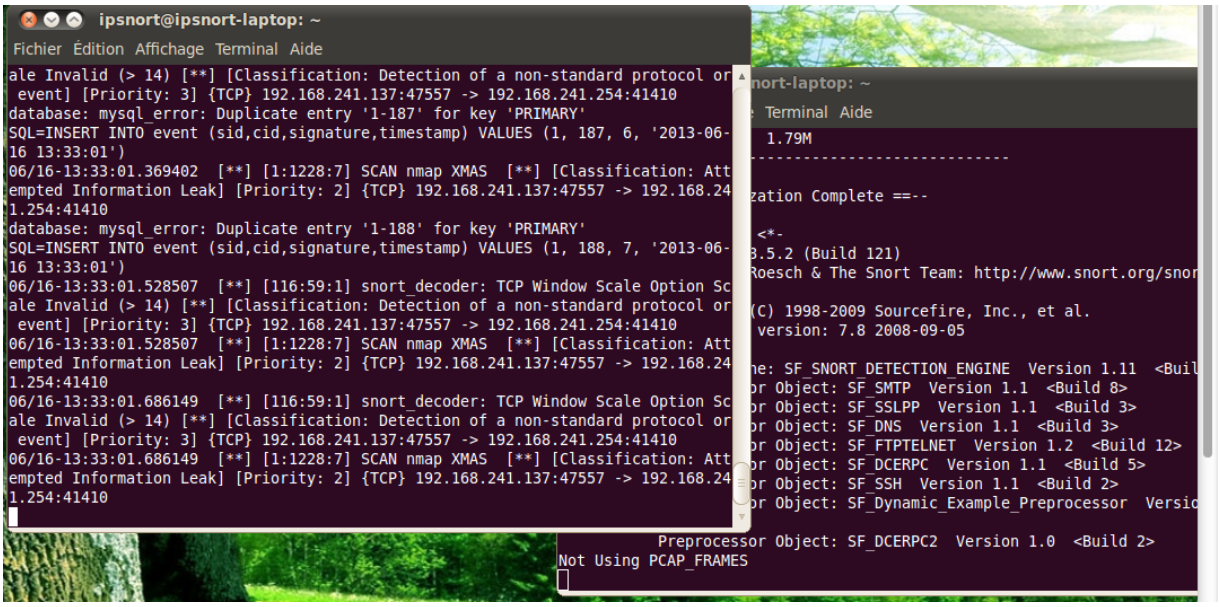


Figure 5.19: Détection d'attaque avec Snort et Barnyard

Détaille d'attaque sur BASE: ou il nous donne l'information que qu'il y a un utilisateur sur le réseau, qui est entrain de faire un scan de port, pour détecté les informations sur les machine sur le réseau.

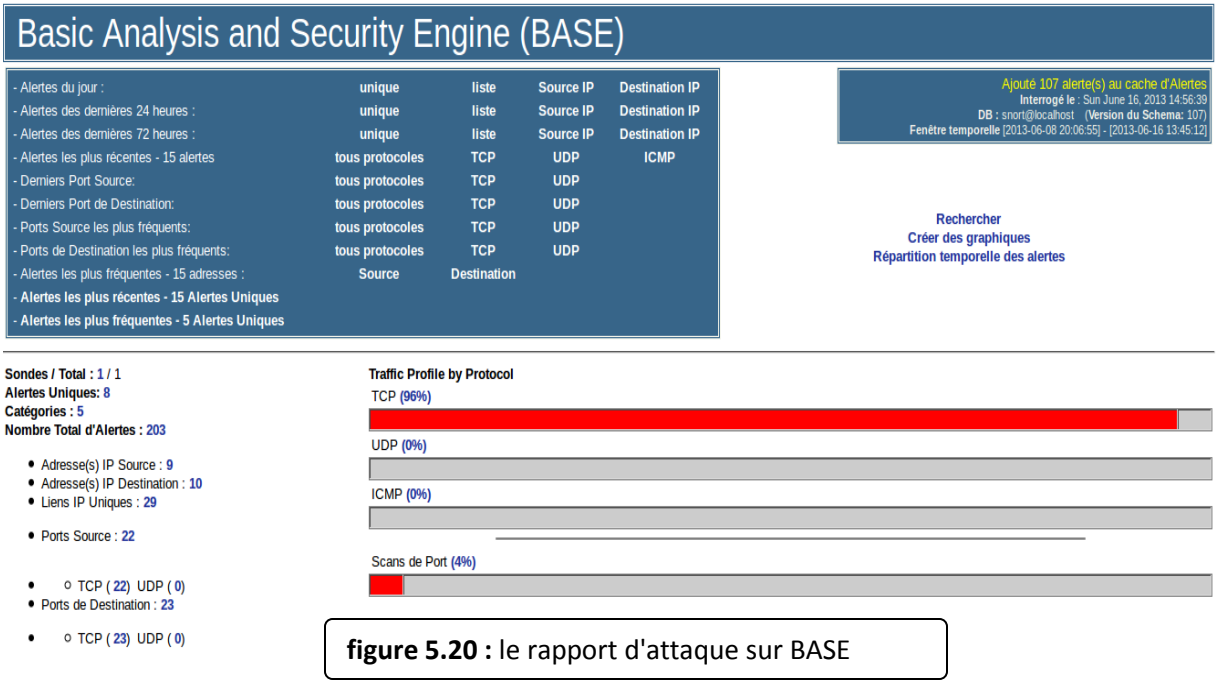


figure 5.20 : le rapport d'attaque sur BASE

ID	< Signature >	< Horodatage >	< Adresse Source >	< Adresse Dest. >	< Protocole de niveau 4 >
#0-(1-168)	[snort] portscan: TCP Portscan	2013-06-16 13:32:56	192.168.241.137	192.168.241.139	Raw IP
#1-(1-169)	[snort] portscan: TCP Portscan	2013-06-16 13:32:56	192.168.241.137	192.168.241.138	Raw IP
#2-(1-126)	[snort] portscan: TCP Portsweep	2013-06-16 13:32:22	192.168.241.137	192.168.241.2	Raw IP
#3-(1-127)	[snort] portscan: TCP Portscan	2013-06-16 13:32:22	192.168.241.137	192.168.241.134	Raw IP
#4-(1-128)	[snort] portscan: TCP Portscan	2013-06-16 13:32:22	192.168.241.137	192.168.241.2	Raw IP
#5-(1-129)	[snort] portscan: TCP Portscan	2013-06-16 13:32:22	192.168.241.137	192.168.241.130	Raw IP
#6-(1-97)	[snort] portscan: TCP Portscan	2013-06-16 13:25:24	192.168.241.130	192.168.241.137	Raw IP
#7-(1-75)	[snort] portscan: TCP Portscan	2013-06-16 13:24:50	192.168.241.130	192.168.241.2	Raw IP
#8-(1-76)	[snort] portscan: TCP Portsweep	2013-06-16 13:24:50	192.168.241.130	192.168.241.2	Raw IP

figure 5.21 : rapport détaillé sur le scan avec BASE

Scénario d'attaque n°2: Attaque DOS de type inviteflood:

Cet outil peut être utilisé pour inonder une cible avec des requêtes INVITE, qu'elle peut être employée pour viser des Gateways/proxy. Dans cette exemple la cible est le serveur Asterisk. Le bute de l'attaque est d'émerger le serveur est le mettre hors service, et d'un autre coter le client reçois de million de requête INVITE.

Étape 01: récupérer les extensions des clients sip sur le serveur:

La commande suivante permet de interroger le serveur Asterisk a fin de récupéré tous le extension probable.

```
# ./svwar.py -e100-400 192.168.241.134 -m INVITE
INFO:root:we have 7 extensions
| Extension | Authentication |
-------------------------------
| 333       | weird          |
| 111       | weird          |
| 102       | noauth         |
| 103       | noauth         |
| 100       | noauth         |
| 101       | noauth         |
| 222       | weird          |
```

figure 5.22 : tableau des extensions sur Asterisk

Étapes 2: lancement de l'attaque sur le serveur:

```
# ./inviteflood eth1 111 192.168.241.0 192.168.241.134 10000000
```

```
inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port    = 192.168.241.13:9
dest   IPv4 addr:port    = 192.168.241.134:5060
targeted UA              = 111@192.168.241.0
```

Résultat obtenue l'hors de l'attaque:

Figure 5.23 : invite flood attaque sur le client SIP

Le client SIP portons l'extension 111 a été inonder par des requêtes INVITE, d'après la ***figure 5.23*** le client ne pourra plus recevoir des appelles par des clients légitime.

Et comme deuxième résultat de l'attaque le serveur ASTERISK ne repend plus aux requêtes à cause de dépassement de temps de traitement et de la surcharge de sont mémoire du Buffer.

Étape 3: Détection de l'attaque DOS par snort:

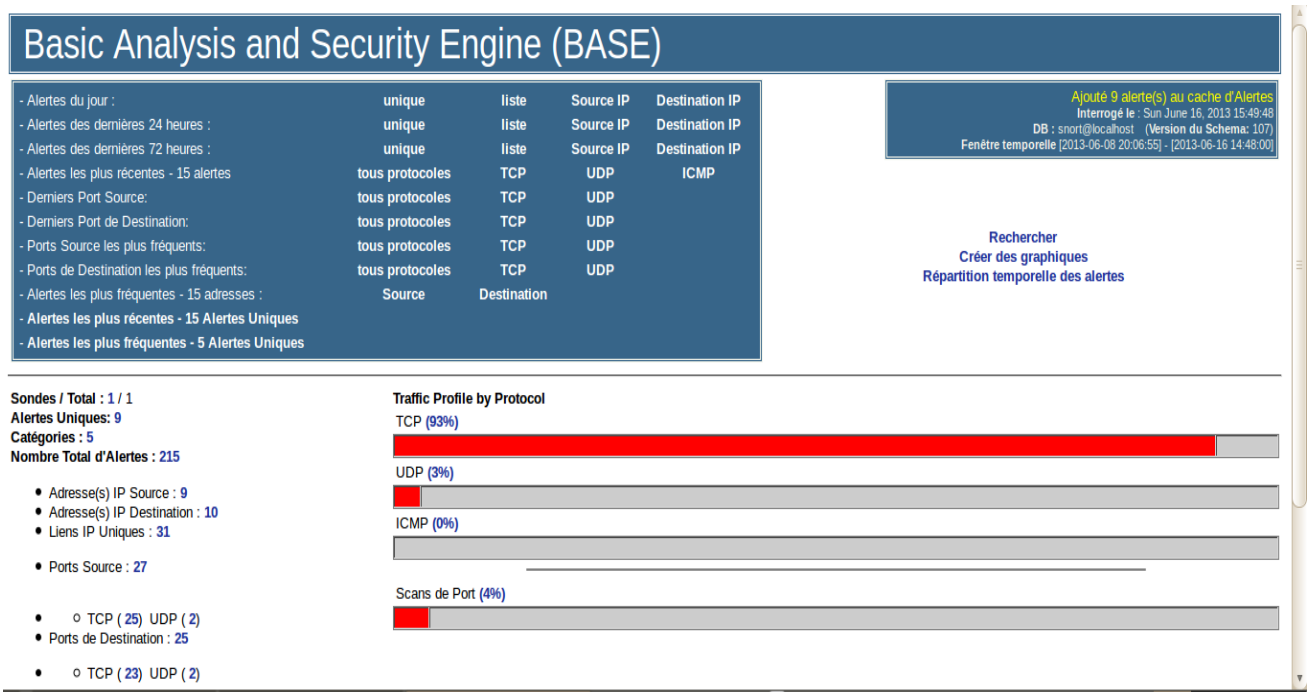


Figure 5.24 : affichage d'alertes d'attaque sur BASE

ID	< Signature >	< Horodatage >	< Adresse Source >	< Adresse Dest. >	< Protocole de niveau 4 >
#0-(1-215)	[snort] Snort Alert [1:100000160:0]	2013-06-16 14:48:00	192.168.241.134:5060	192.168.241.137:9	UDP
#1-(1-214)	[snort] Snort Alert [1:100000160:0]	2013-06-16 14:47:34	192.168.241.134:5060	192.168.241.137:9	UDP
#2-(1-212)	[snort] Snort Alert [1:100000158:0]	2013-06-16 14:47:33	192.168.241.137:9	192.168.241.134:5060	UDP
#3-(1-213)	[snort] Snort Alert [1:100000160:0]	2013-06-16 14:47:33	192.168.241.137:9	192.168.241.134:5060	UDP
#4-(1-211)	[snort] Snort Alert [1:100000160:0]	2013-06-16 14:30:51	192.168.241.137:5060	192.168.241.134:5060	UDP
#5-(1-210)	[snort] Snort Alert [1:100000160:0]	2013-06-16 14:30:50	192.168.241.134:5060	192.168.241.137:5060	UDP
#6-(1-209)	[snort] Snort Alert [1:100000158:0]	2013-06-16 14:30:49	192.168.241.137:5060	192.168.241.134:5060	UDP

Figure 5.24: rapport détaillé sur l'attaque DOS avec BASE

Base nous informe qu'au 16/06/2013 a 14:48 à détecter une alerte, qui s'agit d'une attaque dos de type flood UDP (voir la ***figure 5.24.***)

Conclusion :

Snort est un outil très intéressant dans la mise en place d'une sécurité réseau. Grâce aux communautés très actives qui créent les librairies d'attaques. Snort permet de voir avec une bonne acuité de quoi il faut se protéger. Il est à souligner l'importance d'une bonne mise à jour de ces librairies. De plus Snort placé dans l'enceinte d'un réseau permet de détecter les failles les plus répandues qui proviennent généralement de l'intérieur de l'entreprise, et non de l'extérieur. Ce système de détection multiplateforme est en perpétuelle évolution et semble un des meilleurs outils dans la connaissance des vulnérabilités auxquelles on est exposé.

Cependant, nous avons rencontré de nombreux problèmes au cours de la mise en place de cette solution. Ces derniers consistent principalement en des difficultés rencontrées lors de l'installation du snort ainsi qu'au nombre important des p aquets complémentaires qu'il faut installer et bien conFigurer.

A un niveau plus personnel, j'ai énormément apprécié ce projet. Il m'a déjà permis de me familiariser un peu plus avec le monde Linux. Il m'a également permit d'enrichir mes connaissances sur la sécurité informatique. Cela m'a réellement enthousiasmé et m'a conforté dans mon envie de poursuivre dans cette direction.

Conclusion Générale et perspectives:

Ce projet nous a permis d'avoir une idée plus claire sur les applications du Domaine de la sécurité informatique. Nous avons également découvert les IDS et les IPS et amélioré notre aptitude à utiliser LINUX. Il nous est paru évident que ces systèmes sont à présent indispensables aux entreprises afin d'assurer leur sécurité informatique.

Néanmoins, ces technologies sont amenées à se développer dans les prochaines années, du fait des besoins de sécurité croissants des entreprises et de l'évolution des technologies qui permet un fonctionnement plus efficace des systèmes de détection et de prévention d'intrusion.

De plus, les constructeurs de systèmes de sécurité ont tendance à intégrer les IDS et IPS directement dans les firewalls, de façon à renforcer la coopération entre ces équipements de sécurité complémentaires.

L'avenir des technologies de sécurité réseau est peut-être dans une intégration plus poussée des différents outils disponibles pour assurer la sécurité d'un réseau, car l'administration de la sécurité d'une entreprise est une tâche de plus en plus complexe et étendue, alors que les besoins en sécurité ne font que croître.

En perspective, nous proposons d'améliorer les performances de notre IDS à travers l'exploitation des fichiers logs générés par SNORT en alertant l'administrateur réseau à chaque tentative d'intrusion de haut niveau par un mail ou un SMS.
Il faut bien signaler que ce projet est une excellente initiation à la vie professionnelle car il offre un aperçu de ce que sera le travail au sein d'une équipe de sécurité informatique.
Il a donc été une expérience enrichissante aussi bien sur le plan théorique que pratique.

Bibliographie

[1] **Article : La sécurité des réseaux et des systèmes**
Michel Riguidel
ENST PARIS
2007

[2] **Article : Vers une détection d'intrusions à fiabilité et pertinence prouvables**
Christophe Bidan, Guillaume Hiet, Ludovic Mé, Benjamin Morin
Supélec, Campus de Rennes
16 janv. 2012

[3] **Article : VOIP INTRUSION DETECTION SYSTEM WITH SNORT**
Pavol Číž, Ondrej Lábaj, Pavol Podhradský, Juraj Londák
Slovak University of Technology
2012

[4] **Article : NT Réseaux**
IDS et IPS
Etienne Duris
2004

[5] **Asterisk™: The Future of Telephony, Second Edition**
Jim Van Meggelen, Leif Madsen, and Jared Smith
Copyright © 2007, 2005 O'Reilly Media, Inc.
ISBN-13: 978-0-596-51048-0
August 2007: Second Edition

[6] **Article : SECURITY ANALYSIS SYSTEM TO DETECT THREATS ON A SIP VOIP INFRASCTRUCTURE ELEMENTS**
Filip REZAC, Miroslav VOZNAK, Karel TOMALA, Jan ROZHON, Jiri VYCHODIL
ADVANCES IN ELECTRICAL AND ELECTRONIC ENGINEERING
2011.

[7] **Article : Evaluation of Security and Countermeasures for a SIP-based VoIP Architecture**
Marius HERCULEA, Tudor Mihai BLAGA, Virgil DOBROTA
Technical University of Cluj-Napoca.
2008

[8] **Article : Secure Voice2Web servers from misuse**
Jan Stanek, Jan Rudínský
Czech Technical University in Prague
Décembre 2008

[9] **ASTERISK Security Hardening Guide v1.0**
Nethemba s.r.o.
Boris Pisarcík
2012

[10] **DoS Attacks Targeting SIP Server and Improvements of Robustness**
M.Voznak and J. Safarik
Issue 1, Volume 6, 2012
[11] **HACKING VOIP.**
Himanshu Dwivedi.
ISBN-13: 978-1-59327-163-3
No Starch Presss
October 2008
[12] **Metasploit.Penetration.Testing.Cookbook**
Abhinav Singh
Packt Publishing Ltd.
ISBN 978-1-84951-742-3
June 2012
[13] **Article : LE SYSTÈME DE DÉTECTION DES INTRUSIONS ET LE SYSTÈME D'EMPÊCHEMENT DES INTRUSIONS (ZERO DAY)**
Tran Van Tay
Institut de la Francophonie pour l'Informatique
Montréal, Février 2005
[13] **Intrusion Prevention Systems For Dummies**
Steve Piper, CISSP, SFCP
Wiley Publishing, Inc.
2008
[14] **Article : Intrusion Detection using Open Source Tools**
Jack TIMOFTE
Revista Informatica Economică nr.2(46)/2008
[15] **Article : Denial-of-Service Detection and Mitigationfor SIP Communication Networks.**
vorgelegt von
Berlin 2009
[16] **thèse : Mise en place d'une sonde snort**
Fathi BEN NASR
Alia KHESSAIRI ABBASSI
Université de la Manouba
Ecole Nationale des Sciences de l'Informatique
2005
[17] **Snort 2.0Intrusion Detection**
Jay Beale
James C. Foster
EDITION Syngress Publishing, Inc
ISBN: 1-931836-74-4

[18] thèse : Installation et Configuration d'un système de détection d'intrusion (IDS) Ibrahim Mohamed Amine
Tebourbi Hamdi
UNIVERSITE 7 NOVEMBRE CARTHAGE
2009

[19] Article : Audit de la sécurité de réseaux VoIP
J. Ehrensberger, X. Hahn, A. Doswald
29 novembre 2006

[20] thèse : VoIP & Security: IPS/IDS
Lalaina KUHN
École D'ingénieures Du Caton De Vaud
2003

[21] SNORT Users Manual 2.8.5
The Snort Project
September 21, 2009

Webographie

[22] -IDS

wikipédia.com : “ Système de détection d'intrusion ”

http://fr.wikipedia.org/wiki/Systeme_de_detection_d%27intrusion

[23] -Snort

wikipédia.com: “Snort”

http://fr.wikipedia.org/wiki/Snort

[24] -Tutorial d'installation

http://openmaniak.com : “ tutorial --> snort & Base”

http://openmaniak.com/fr/snort.php

[25] -Téléchargement des paquets nécessaires

http://sourceforge.net/

http://www.snort.org

[26] -Tutorial des mises à jour des règles

http://openmaniak.com

http://openmaniak.com/fr/snort_tutorial_update.php

[27] -Téléchargement des mises à jour

http://www.bleedingsnort.com

http://www.snort.org

[28] - Asterisk:

http://www. asterisk.org