Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Fin de Cycle

En Vue de l'Obtention du Diplôme de Master en Informatique

Option : Administaration et Sécurité des Réseaux Informatiques

Thème

Configuration et Mise en œuvre d'un systeme de détection d'intrusion. "Cas d'étude : NAFTAL"

Réalisé par :

CHEURFA Zahra & DJAOUDENE Nadjet

Soutenu devant le jury composé de :

Président	M^r ***BAADACHE*** **Abederrahmane**
Promoteur	M^r ***AISSANI*** **Soufiane**
Examinatrice	M^{lle} ***BENKEROU*** **Hayet**
Examinatrice	M^{me} ***BATTAT*** **Nadia**

Promotion 2013/2014

Remerciements

N ous rendons grâce à notre Dieu, le tout puissant et miséricordieux, pour nous avoir donné le courage et la patience pour mener à bout ce travail.

Nos plus sincères remerciements s'adressent à notre encadreur M^r AISSANI Soufiane pour nous avoir proposé ce sujet intéressant et pour ses précieux conseils et encouragements, sans lesquels cette étude n'aurait pas vu le jour. Merci pour votre confiance, votre disponibilité et le temps que vous avez bien voulu consentir à l'aboutissement de ce mémoire.

Nos remerciements s'adressent également aux membres de jury, en l'occurrence M^r BADACHE Abderrahmane, M^{me} BATTAT Nadia et M^{me} BENKAROU Hayat d'avoir accepté d'évaluer notre travail et pour l'intérêt qu'ils y portent.

Nous tenons à remercier tous les enseignants, qui ont assuré notre formation durant notre cycle universitaire, particulièrement D^r OMAR Mawloud.

Nos remerciements vivement M^r HAROUNE Lamine et M^{me} BAALICHE Nabila pour leurs aide, leurs soutiens permanent et leurs conseils

Enfin un grand merci à nos familles, pour leur soutien permanent et indéfectible qui nous ont permis de chercher au plus profond fond de nous même la force, la volonté et la persévérance à même d'arriver à cet instant des plus important de notre vie et à nos amis et tous ceux qui ont contribué de près ou de loin à la concrétisation de cette œuvre.

Dédicaces

Je dédie ce modeste travail à :

A mes trés chèrs parents,

A mes frères et soeurs ,

A toute ma famille,

A mon homme d'avenir Soufiane ;

CHEURFA Zahra

Dédicaces

Je dédie ce modeste travail à :

A mes trés chèrs parents,

A mes frères et soeurs ,

A toute ma famille,

A tous mes amis et collègues, et tous ceux qui m'ont aidé,

A ma binôme Zahra et sa famille ;

DJAOUDENE Nadjet

Table des matières

Liste des Abréviations

CPU	Central Processing Unit.
DNS	Domain Name Serveur.
DHCP	Dynamic Host Configuration Protocol.
FTP	File Transfer Protocol.
HIDS	Host Intrusion Detection System.
HTTP	Hyper Text Transfer Protocol.
IDS	Intrusion Detection System .
IDM	IPS Device Manager.
IETF	Internet Engineering Task Force.
IP	Internet Protocol.
IPS	Intrusion Prevention System.
IPSec	Internet Protocol Security .
L2F	Layer Two Tuneling Protocol
L2TP	Goldwaser Micali.
NIDS	Network Intrusion Detection System.
PPP	Point to Point Protocol.
PPTP	Point to Point Tuneling Protocol.
TCP	Transmission Control Protocol.

Table des figures

Introduction Générale

Les réseaux informatiques sont devenus des outils indispensables aux fonctionnements et à l'évolution de toutes les activités des entreprises. Internet de sa part, relie des millions d'ordinateurs à travers le monde fonctionnant sur des plateformes multiples de matériels et de logiciels, avec des communications caractérisées par une offre multiservice. Cependant, Internet a créé de nouveaux problèmes dus à l'ampleur des réseaux pouvant comporter plusieurs centaines de machines et des dizaines de sous-réseaux, ceci permet aux utilisateurs malveillants de s'introduire dans le réseau d'une façon illégitime menaçant ainsi l'intégrité et le bon fonctionnement des ressources du réseau. C'est pour cette raison que les entreprises investissent, de plus en plus, dans le domaine de la sécurité informatique et intègrent des mécanismes de sécurité dans leurs architectures réseaux. De plus, la mise en place d'une politique de sécurité informatique autour de ces systèmes pour détecter d'éventuelles intrusions devient une nécessité.

La mise en place de pare-feux et des systèmes d'authentification sécurisés, les systèmes de détection d'intrusions (IDS) et les systèmes de prévention d'intrusions (IPS) interviennent pour assurer une protection éfficace face aux tentatives intrusives. Cependant cette protection révèle certaines limites dues à la multitude des techniques et des possibilités de contournement mais aussi la complexité des choix au niveau de la politique de sécurité à adopter et des obligations vis-à-vis des dispositions.

Les systèmes de détection d'intrusions sont parmi les outils de sécurité les plus récents. Nous pouvons les classer en différents types selon leurs caractéristiques, par exemple selon leurs techniques de détection ou leurs architectures. Malheureusement, malgré leur utilité, en pratique la plupart des IDS souffrent plus ou moins de deux problèmes : le nombre important de faux

positifs et de faux négatifs. Les faux positifs (c'est-à-dire les fausses alertes) sont générés lorsque l'IDS identifie des activités normales comme des intrusions, alors que les faux négatifs correspondent aux attaques ou intrusions qui ne sont pas détectées (aucune alerte n'est générée)[29].

Notre projet s'inscrit dans cet axe, en effet notre objectif principal est de definir une bonne politique de sécurité puis de configurer un IDS en respectant cet politique , L'organisation de notre mémoire reflète la démarche que nous avons adoptée lors de la réalisation de ce travail

Ce travail est composé de quatre parties :

La première partie sera consacrée à la définition de quelques notions de bases sur la sécurité informatique, ainsi que les attaques menaçant un réseau et outils utilisés pour sécuriser un réseau. Dans la seconde partie, nous allons effectuer une étude théorique des systèmes de détection d'intrusions et approfondir les notions relatives à ce dernier. Dans le troisième chapitre nous allons présenter l'organisme d'accueil où nous avons effectué notre stage. Et nous terminerons par la description de la partie pratique de notre travail, dans laquelle nous expliquerons quels sont les étapes que nous avons du suivre pour établir une politique de securité puis simuler une configuration d'un IDS Cisco.

Chapitre 1

Généralités sur la sécurité des réseaux

introduction

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprises ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. Les réseaux sont toujours devant des menaces. Il y a de plus en plus de techniques pour les protéger, mais il y a aussi de plus en plus de techniques pour les attaquer.

Au long de ce chapitre nous allons présenter d'abord les mesures et les techniques de sécurité, les étapes d'une mise en œuvre d'une politique de sécurité, ensuite les différents types d'attaque qui peuvent nuire à un système et enfin les différents mécanismes de sécurité pour permettre la protection des données et des ressources et d'assurer le bon fonctionnement du système.

1.1 Définition

Stéphane Natkin [1] a défini la sécurité informatique comme étant un ensemble de moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles (accident dus à l'environnement, les défauts du système) ou intentionnelles (actions malveillantes intentionnelles) pour éviter les erreurs, afin d'assurer le bon fonctionnement de tel système [1].

Géraldine Vache-Marconato [1] l'a définie comme étant un terme large qui réunit les moyens humains, techniques, organisationnels et juridiques qui tentent de garantir certaines propriétés

d'un système d'information [2] .

Donc, en informatique, le terme sécurité recouvre tout ce qui concerne la protection des informations. Trois grands concepts ont été définis [3] :

- Les fonctions de sécurité, qui sont déterminées par les actions pouvant compromettre la sécurité d'un établissement ;
- Les mécanismes de sécurité, qui définissent les algorithmes à mettre en œuvre ;
- Les services de sécurité, qui représentent les logiciels et les matériels mettant en œuvre des mécanismes dans le but de mettre à la disposition des utilisateurs les fonctions de sécurité dont ils ont besoin.

1.2 Objectifs de sécurité

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Puisqu'on ne voit pas son correspondant directement, il faut l'authentifier. Puisqu'on ne sait pas par où passent les données, il faut les chiffrer. Puisqu'on ne sait pas si quelqu'un ne va pas modifier les informations émises, il faut vérifier leur intégrité [3].

Assurer la sécurité revient alors à assurer les fonctions suivantes [3] :

- ***La Confidentialité :*** assurer que l'information ne sera lue que par les personnes autorisées.
- ***L'authentification :*** vérifier l'identité d'un utilisateur pour lui associer des droits d'accès.
- ***L'intégrité :*** assurer que les informations ne peuvent être modifié ou altéré que par les personnes autorisées.
- ***La non-répudiation :*** garantir qu'aucun des correspondants ne pourra nier la transaction (l'envoi ou la réception des données).
- ***La disponibilité :*** assurer que l'information est disponible pour les personnes autorisées.
- ***Contrôle d'accès :*** qui doit permettre de limiter et de contrôler l'accès à des systèmes et des applications via des maillons de communications.

1.3 Menaces sur les réseaux

1.3.1 Vulnérabilité

Une vulnérabilité ou une faille est une faiblesse de sécurité qui peut être de nature logique, physique, etc.

Une vulnérabilité peut découler, par exemple, d'une erreur d'implémentation dans le développement d'une application, erreur susceptible d'être exploitée pour nuire à l'application (pénétration, refus de service, etc.). Elle peut également provenir d'une mauvaise configuration. Elle peut enfin avoir pour origine une insuffisance de moyens de protection des biens critiques, comme l'utilisation de flux non chiffrés, l'absence de protection par filtrage de paquets, etc [2].

1.3.2 Attaque

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de pirates informatiques.

1.3.2.1 Définition

Une attaque est l'exploitation d'une vulnérabilité d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) par des actions que se soit accidentelles, malveillantes ou intentionnelles [1].

1.3.2.2 Les différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma [12] :

- **Identification de la cible :** cette étape est indispensable à toutes attaques organisées, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'interrogation des serveurs DNS (Domain Name Serveur).

- **Le scanning :** l'objectif est de compléter les informations réunies sur une cible visées. Il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée.
- **L'exploitation :** Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.
- **La progression :** Il est temps pour l'attaquant de réaliser son objectif. Le but ultime étant d'élever ses droits vers root (administrateur) sur un système afin de pouvoir y faire tout ce qu'il souhaite.

1.3.2.3 Les attaquants

Avant de présenter les attaques informatiques, nous allons définir les deux principales notions de l'attaquant [11] :

- ***les Hackers :*** ils sont moins dangereux, car ils sont considérés comme des personnes qui s'introduisent dans un système pour y poser des actes qui ne lui sont pas autorisées pour consulter ou modifier des données et des programmes communiques aux frais d'autres utilisations sans motivation réelle c'est surtout un " passe-temps ".
- ***les Crackers :*** les plus dangereux parmi les pirates informatiques. Leur rôle est " craquer " (forcer) les réseaux informatiques des entreprises ou des administrations.Ils ont des motivations criminelles par pur vandalisme ou part des intérêts financiers.

1.3.2.4 Les différents types d'attaques

Les attaques peuvent être regroupées en trois familles différentes [4] :

- **Les attaques directes**

  C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrable.et un grand nombre de ces logiciels envoient directement les paquets a la victime.

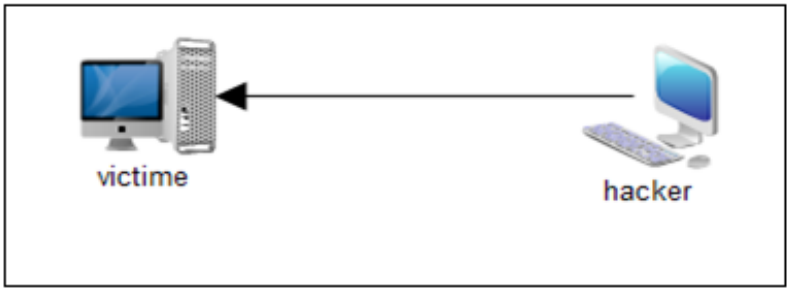


FIGURE 1.1 – Attaque directe

.

- **Les attaques indirectes par rebond**

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

– Masquer l'identité (l'adresse IP) du hacker.

– Utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante) pour réaliser son attaque.

Le principe en lui même, est simple : les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'ou le terme de rebond.

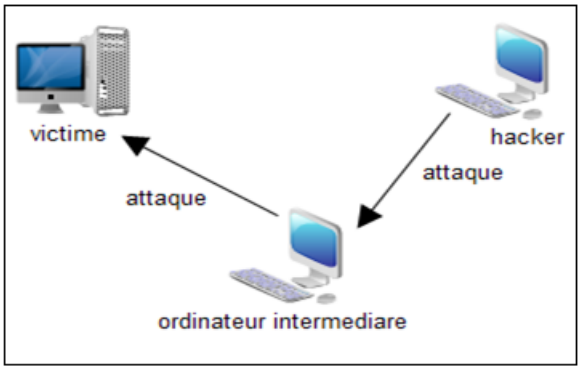


FIGURE 1.2 – Les attaques indirectes par rebond

.

- **Les attaques indirectes par réponse**

Cette attaque est un dérivé par rebond. Elle offre les mêmes avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour

qu'il la répercute, l'attaquant va lui envoyer une requête et c'est cette réponse à la requête qui va être envoyé à l'ordinateur victime.

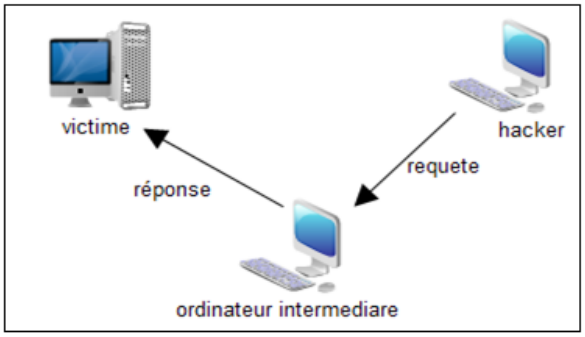


FIGURE 1.3 – Les attaques indirectes par réponse

1.3.2.5 Quelques techniques d'attaque

Il existe un grand nombre d'attaques qui peuvent intervenir à chaque composant du système informatique mais généralement elle touche la couche réseau, le système d'exploitation, et la couche application, pour vue qu'il existe une vulnérabilité exploitable. En voici quelques techniques les plus utilisées [11] :

1. **Le sniffing (Espionnage du réseau local) :** Cette attaque est utilisée pour obtenir des mots de passe en interceptant tous les paquets qui circulent sur un réseau et ceci en configurant l'interface réseau de la station dans un mode spécial, qui permet de recevoir toutes les trames qui circulent sans pour autant en être le destinataire. Il est alors possible de récupérer par exemple les comptes des utilisateurs utilisant FTP ou Telnet [1].
2. **Le craquage de mots de passe :** Le craquage consiste à faire de nombreux essais pour trouver le bon mot de passe. Il existe deux grandes méthodes :
   - ***L'utilisation de dictionnaires :*** le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci. Utilitaire permettant l'utilisation de programmes sur des machines distantes (par exemple via le réseau internet).

1. Utilitaire permettant l'utilisation de programmes sur des machines distantes (par exemple via le réseau internet)

- ***La méthode brute :*** toutes les possibilités sont faites dans l'ordre pour trouver la bonne solution.

3. **Les attaques par saturation (déni de service) :** Cette technique d'attaque consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs dont le but de paralyser un site pendant quelques heures, et d'en bloquer ainsi l'accès aux internautes. Il existe différentes attaques par saturation, parmi ces attaques :
   - ***Le flooding :*** Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.
   - ***Le smurf :*** Le smurf est une attaque qui s'appuie sur le ping (Packet INternet Groper) et les serveurs de broadcast. On falsifie d'abord son adresse IP pour se faire passer pour la machine cible. On envoie alors un ping sur un serveur de broadcast. Il le fera suivre à toutes les machines qui sont connectées qui renverront chacune une réponse au serveur qui fera suivre à la machine cible. Celle-ci sera alors inondée sous les paquets et finira par se déconnecter.
4. **Le débordement de tampon :** Cette attaque se base sur une faille du protocole IP. On envoie à la machine cible des données d'une taille supérieure à la capacité d'un paquet. Celui-ci sera alors fractionné pour l'envoi et rassemblé par la machine cible. A ce moment, il y aura débordement des variables internes. Suite à ce débordement, plusieurs cas se présentent : la machine se bloque, redémarre ou ce qui est plus grave, écrit sur le code en mémoire.
5. **L'IP spoofing :** Cette technique permet de s'infiltrer dans un ordinateur en falsifiant son adresse IP, en se faisant passer pour un autre en qu'il a confiance. Il existe des variantes car on peut faire spoofing aussi des adresses e-mail, des serveurs DNS.

1.3.3 Types de logiciels malveillants

1.3.3.1 Virus

Un virus est un logiciel capable de s'installer sur un ordinateur à l'insu de son utilisateur légitime. Le terme virus est réservé aux logiciels qui se comportent ainsi avec un but malveillant, parce qu'il existe des usages légitimes de cette technique dite de code mobile. En général, pour infecter un système, un virus agit de la façon suivante : il se présente

sous la forme de quelques lignes de code en langage machine binaire qui se greffent sur un programme utilisé sur le système cible, afin d'en modifier le comportement. Le virus peut être tout entier contenu dans ce greffon, ou il peut s'agir d'une simple amorce, dont le rôle va être de télécharger un programme plus important qui sera le vrai virus. Une fois implanté sur son programme-hôte, le greffon possède aussi en général la capacité de se recopier sur d'autres programmes, ce qui accroît la virulence de l'infection et peut contaminer tout le système ; la désinfection n'en sera que plus laborieuse [19].

1.3.3.2 Vers

Un ver (worm) est une variété de virus qui se propage par le réseau. Il se reproduit en s'envoyant à travers un réseau (e-mail, Bluetooth, chat..). Le ver contrairement aux virus, n'a pas besoin de l'interaction humaine pour pouvoir se proliférer [19].

1.3.3.3 Cheval de Troie

Un cheval de Troie (Trojan horse) est un logiciel qui se présente utile ou agréable, et qui une fois installé sur un ordinateur y effectue des actions cachées et pernicieuses. La différence essentielle entre un cheval de troie et un ver réside dans le fait que le ver tente de se multiplier. Ce que ne fait pas le cheval de troie [19].

1.3.3.4 Porte dérobée

Une porte dérobée (backdoor) est un logiciel de communication caché, installé par exemple par un virus ou par un cheval de Troie, qui donne à un agresseur extérieur accès à l'ordinateur victime, par le réseau [19].

1.3.3.5 Bombe logique

Une bombe logique est une fonction, cachée dans un programme en apparence honnête, utile ou agréable, qui se déclenchera à retardement, lorsque sera atteinte une certaine date, ou lorsque surviendra un certain événement. Cette fonction produira alors des actions non désirées, voir nuisibles [19].

1.3.3.6 Logiciel espion

Un logiciel espion, comme son nom l'indique, collecte à l'insu de l'utilisateur légitime des informations au sein du système où il est installé, et les communique à un agent extérieur, par exemple au moyen d'une porte dérobée. Une variété particulièrement toxique de logiciel espion est le keylogger (espion dactylographique), qui enregistre fidèlement tout ce que l'utilisateur tape sur son clavier et le transmet à son honorable correspondant ; il capte ainsi notamment identifiants, mots de passe et codes secrets [19].

1.4 Mécanisme de défense et de sécurité

La mise en œuvre des mesures de sécurité consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans la politique de sécurité. De nombreux mécanismes ont été développés pour assurer la sécurité, qu'il est souvent indispensable de combiner pour atteindre un niveau de sécurité suffisant. La sécurité est une question essentielle aussi bien pour les utilisateurs que pour les administrateurs de ces systèmes d'information. Un mécanisme donc est un moyen pour la mise en œuvre de la politique.

1.4.1 La cryptographie

Le mot 'cryptographie' vient de mot grec cryptos 'cacher' et le verbe graphien 'écrire' qui signifie étude des écritures secrètes [5]. Donc la cryptographie est une discipline du domaine de la sécurité de l'information et des communications qui permet à travers des primitives mathématiques de fournir un ensemble de services de sécurité telles que la confidentialité, l'intégrité, l'authenticité et le non répudiation. Pour ce faire, des primitives de chiffrement et déchiffrement sont utilisées. Le chiffrement consiste à transformer les données de telle sorte qu'il soit pratiquement impossible de les lire sans avoir la clé de déchiffrement [6].

Il existe quatre primitives cryptographiques de base qui sont largement répandues et souvent combinées pour sécuriser les communications à travers les réseaux [16] :

1.4.1.1 Cryptage symétrique (à clé secrète)

il est basé sur l'utilisation d'une clé privée (ou algorithme) partagée entre les deux parties communicantes. La même clé sert à crypter et décrypter les messages comme cela est indique sur la figure 1.4 . Cette primitive permet d'assurer la confidentialité dont le but est d'empêcher les entités non autorisées d'avoir accès à un message sensible. La principale difficulté est de trouver un moyen sécurisé pour communiquer la clé aux deux entités. Pour résoudre ces problèmes de transmission de clés, les mathématiciens ont inventé le cryptage asymétrique qui utilise une clé privée et une clé publique.

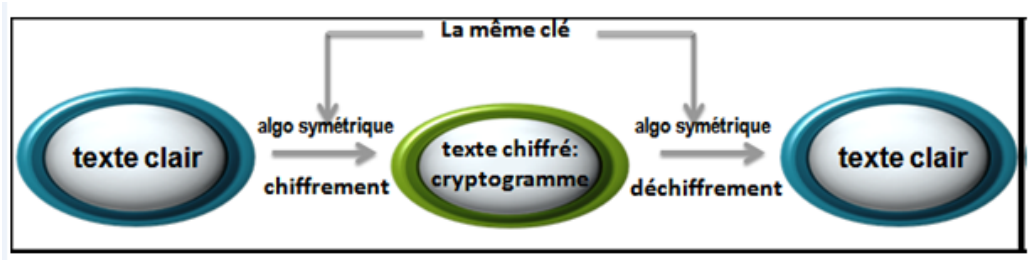


FIGURE 1.4 – Chiffrement symétrique

.

1.4.1.2 Cryptage asymétrique (à clé publique)

le cryptage asymétrique utilise deux clés différentes pour chaque utilisateur :
La première est privée et n'est connue que de l'utilisateur qui a générer les clés.
La deuxième est publique et peut être transmise sur Internet.
La clé publique et la clé privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante et qu'il est impossible de déduire la clé privée à partir de la clé publique. Une clé est donc utilisée pour le cryptage l'autre pour le décryptage comme cela est indique sur la figure 1.5. Son principal avantage est qu'il résout le problème du transfert de la clé mais en revanche, il est plus couteux en termes de temps de calcul et nécessite des tailles de clé plus importantes (couramment 1024 ou 2048 bits)[7].

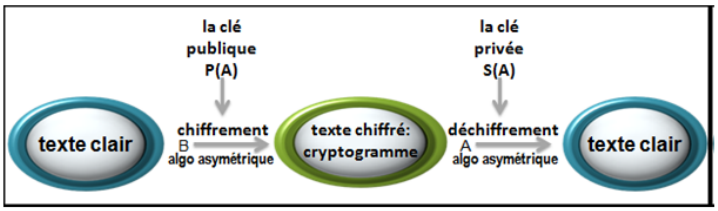


FIGURE 1.5 – Chiffrement asymétrique

.

1.4.1.3 Fonction de hachage

C'est une fonction mathématique à sens unique qui permet de chiffrer un message dont son déchiffrement est impossible, dont l'objectif est de fournir un résultat représentatif du contenu d'un message de taille restreinte (fonction de condensation) à la taille initiale et ainsi de garantir l'intégrité de ce dernier [5].

1.4.1.4 La signature numérique

Elle consiste à appliquer une fonction de hachage sur une portion du message. Un schéma de signature numérique (figure 1.6) est composé de [8] :

- La fonction de signature est paramétrée par une clé secrète propre au signataire, elle associe à tout message clair une signature.
- La fonction de vérification permet à partir du message clair et de la signature de vérifier l'authenticité de ce dernier.

Le schéma de chiffrement asymétrique en faisant appel à la signature numérique est illustré dans la figure Tels que :

1. Une entité A signe le message m avec sa clé privée,
2. Puis elle chiffre le résultat m1 avec la clé publique de l'entité B, et envoie m2 à B,
3. L'entité B à son niveau va déchiffrer le message (m2) avec sa clé secrète,
4. Puis elle va déchiffrer le résultat avec la clé publique de l'entité A, et trouve finalement le message m que l'entité A avait envoyé.

   Seulement avec la clé publique de l'entité A que l'entité B peux déchiffrer le message obtenu, cela garantie l'authentification. Et aussi le message ne peut pas être altéré, donc l'intégrité est assuré, et la non-répudiation.

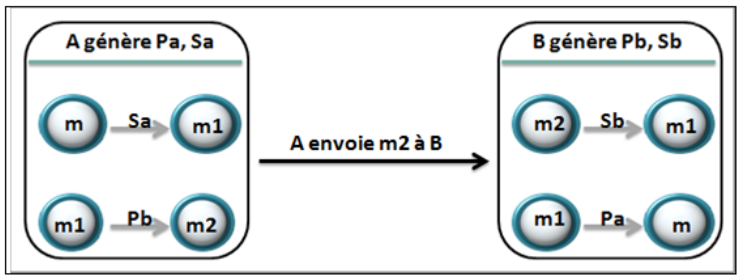


FIGURE 1.6 – Le schéma de signature numérique

.

Notamment ce processus de signature, alourdi encore plus le processus de chiffrement asymétrique qui est déjà un processus lent. Une solution qui permet de garantir ces services tous en évitant d'augmenter le temps de calcul et ainsi de réduire la taille des messages, consiste à utiliser une fonction de hachage.

la figure 1.7 illustre le fonctionnement de chiffrement asymétrique en utilisant la fonction de hachage. Soit m le message que l'entité A veut envoyer à l'entité B :

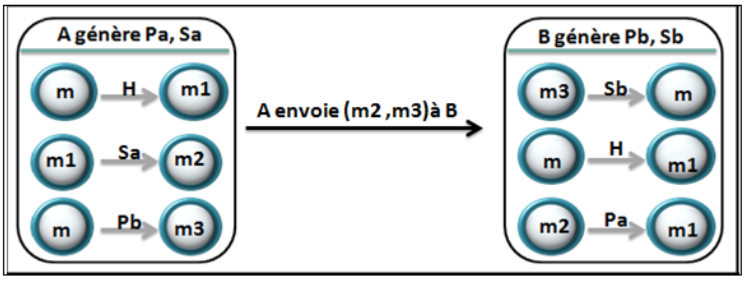


FIGURE 1.7 – Le chiffrement asymétrique avec la fonction de hachage

.

1. A calcule le haché de message m : H(m)=m1
2. A signe le haché avec sa clé privée : Sa(m1)=m2
3. A crypte le message m avec la clé publique de l'entité B : Pb(m)=m3
4. A envoie le message chiffré m3 ainsi sa signature m2
5. B déchiffre le message m3 avec sa clé privé : Sb(m3)=m
6. B calcule le haché de message obtenu a son niveau : H(m)=m4
7. B vérifie la signature de haché envoyé par A : Pa(m2)=m5

8. Il faut que m4=m5 (le haché calculé=le message signé après le décryptage).

1.4.2 Les antivirus

Sont des programmes qui permettent de détecter la présence de virus, vers ou chevaux de Troie sur un ordinateur et les supprimer. Éradiquer un virus est le terme utilisé pour nettoyer un ordinateur. Il existe plusieurs méthodes d'éradication : Nettoyer le fichier infecté en supprimant le code malveillant, la suppression du fichier infecté entièrement, et la mise en quarantaine du fichier infecté, qui consiste à le déplacer vers un endroit où il ne peut pas être exécuté. Outils antivirus appliquent souvent des techniques de détection à base de signatures et présentent de nombreuses similitudes avec les systèmes de détection d'intrusions [9].

1.4.3 Firewalls (pare-feux)

Le but de cette partie est de présenter une autre technique très efficace et plus utilisée avec les systèmes de détection d'intrusions dans le but de renforcer la sécurité des réseaux : il s'agit des pare-feux. Ces derniers sont utilisés pour contrôler, analyser, sécuriser et gérer le trafic dans les réseaux. Cela permet d'utiliser le réseau de la façon pour laquelle il a été prévu et d'empêcher les accès non-autorisés. Un pare-feu contient généralement un ensemble de règles prédéfinies permettant de rejeter ou d'autoriser des connexions et/ou des paquets. De ce fait, la protection d'un réseau local qui utilise des pare-feux (matériels ou logiciels) des accès non autorisés revient à configurer ces derniers d'une manière correcte par rapport aux contraintes de sécurité spécifiées [13].

1.4.3.1 Définition

Les pare-feux (firewalls) sont des dispositifs physiques (matériel) ou logiques (logiciels) conçus pour contrôler le trafic entre le réseau interne et le réseau externe en autorisant uniquement la circulation du trafic qui ne viole pas la politique de sécurité mise en place figure(1.8). Ils sont configurés via des règles de filtrages spécifiées par des experts en sécurité des réseaux. Quand un pare-feu reçoit un paquet, il commence par vérifier sa liste de règles de filtrages du début à la fin à la recherche d'une règle permettant d'accepter ou de rejeter le paquet [11].

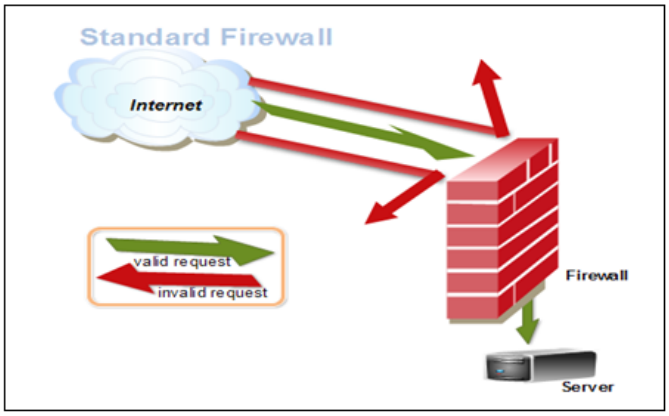


FIGURE 1.8 – pare-feux

.

Les règles du pare-feu permettent de mettre en œuvre un filtrage dépendant de la politique de sécurité adoptée. Les deux approches d'implantation de politiques de sécurité les plus répandues sont [13] :

– Le premier type autorise uniquement les connexions ayant été explicitement autorisées : tout ce qui n'est pas explicitement autorisé est interdit.
– Le deuxième type empêche les échanges qui ont été explicitement interdits : tout ce qui n'est pas explicitement interdit est autorisé.

1.4.3.2 Principe de fonctionnement

Essentiellement, il y a trois modes de fonctionnement de pare-feux [13] : le filtrage statique, le filtrage dynamique et le filtrage applicatif.

– **Filtrage statique (stateless packet filtering) :** C'est le filtrage de paquets le plus simple. Un pare-feu qui fonctionne selon ce mode de filtrage inspecte les entêtes de chaque paquet qui le traverse et décide selon la politique de sécurité de le laisser passer ou de le supprimer et ce sans tenir compte des autres paquets. Parmi les champs qui peuvent être analysées et pris en considération lors de la décision d'un pare-feu, nous trouvons :
– Adresse IP de la machine émettrice.
– Adresse IP de la machine réceptrice.
– Type de protocole (TCP, UDP, etc.).
– Numéro de port : le numéro associé à un service ou une application réseau.

- **Filtrage dynamique (Statcful Inspection) :** Cette technique a été proposée pour palier aux certaines limites de pare-feux utilisant le filtrage simple. L'idée est de conserver les traces de sessions et de connexions dans des tables d'états internes aux pare-feux. Ces traces seront également prises en considération par les pare-feux lors de prise de décisions. Ces informations augmentent considérablement les capacités des pare-feux à détecter des attaques sophistiquées. Il reste, cependant, que les failles applicatives (les failles liées aux logiciels), qui sont à l'origine de la plus grande majorité de problèmes de sécurité.
- **Filtrage applicatif :** Un firewall éffectuant un filtrage applicatif est appelé généralement passerelle applicative ou proxy. Le serveur Proxy permet de faire le relais au niveau des applications pour rendre les machines internes invisibles à l'extérieur. Il permet la destruction des en-têtes précédant le message applicatif ce qui fournit un niveau de sécurité supplémentaire. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit donc d'un proxy http (Hyper Text Transfer Protocol), toutefois il peut exister des serveurs proxy pour chaque protocole applicatif parmi eux FTP(File Transfert Protocol) [14].

1.4.4 La DMZ (DeMilitarized Zone)

Une DMZ (Zone Démilitarisée) est une interface située entre un segment de réseau connu (réseau interne) et un segment inconnu (réseau Internet). Une série de règles de connexion configurées sur le pare-feu font de cette interface une zone physiquement isolée entre les deux réseaux (figure 1.9). Cette séparation physique permet d'autoriser les accès Internet à destination des serveurs placés dans la DMZ et non à ceux destins au réseau privé.

Le principal avantage de cette configuration est le confinement de toutes les requêtes inconnues au niveau de la DMZ. Cela évite de les recevoir sur le réseau interne, avec tous les risques que cela comporte [7].

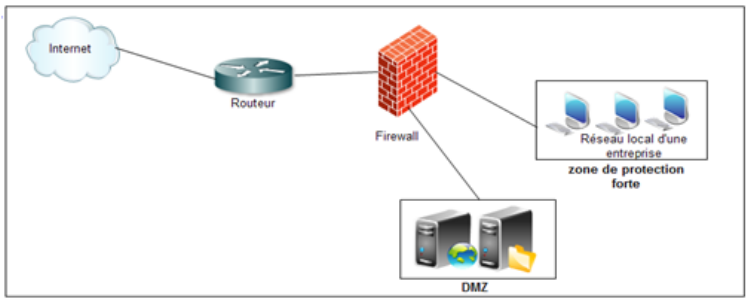


FIGURE 1.9 – DMZ simple

.

Un niveau supplémentaire de sécurité peut être introduit avec un deuxième firewall. Les règles d'accès sur le firewall du réseau local privé sont plus restrictives(figure 1.10). La DMZ est située entre les deux firewalls (DMZ en sandwich) avec des règles moins restrictives introduites par le premier firewall [7].

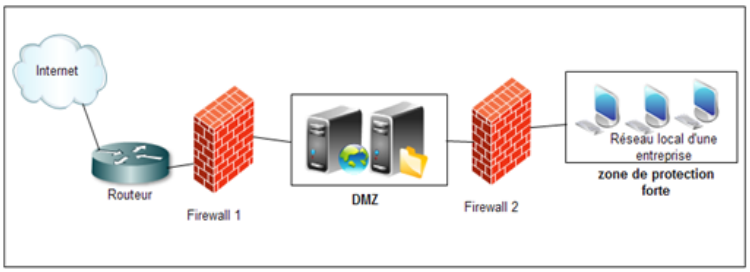


FIGURE 1.10 – DMZ en sandwich

.

1.4.5 Système de détection d'intrusion

Le système de détection des intrusions (IDS signifie Intrusion Detection System) est un logiciel ou un matériel de surveillance des événements se trouvant dans un système des ordinateurs ou du réseau et les analysant pour détecter les signes des intrusions, défini comme des tentatives pour compromettre la confidentialité, intégrité, disponibilité ou éviter des mécanismes de sécurité de l'ordinateur ou du réseau [15].(plus de détails dans le chapitre 2).

Aujourd'hui, les systèmes IDS évoluent vers ce que l'on appelle des systèmes de prévention d'intrusions (IPS) qui en complément de la détection apporte une protection

active. Un système IPS peut ainsi décider, suite à des remontées d'alertes, de fermer des ports et de rejeter des paquets en fonctions du paramétrage qui en a été fait.

1.4.6 VPN (Virtual Private Network)

Afin d'assurer la sécurité des connexions entre sites distants tout en utilisant le réseau public (internet), de plus en plus d'organisation déploient des réseaux privés virtuels (VPN).

1.4.6.1 Définition et fonctionnement d'un VPN

Un VPN fournit un canal sécurisé de transmission de données en les faisant passer dans un tunnel (tunnelling), dont les bouts sont tous les deux dans un réseau de confiance (réseau local)(figure 1.11). Un chiffrement des données est utilisé pour assurer qu'aucun ordinateur autre que ceux des extrémités ne puissent déchiffrer la communication. Pour cela les données à transmettre peuvent appartenir à un protocole différent d'IP. Dans ce cas, les protocoles de tunnelling sont utilisés pour encapsuler les données en rajoutant un entête permettant le routage des trames dans le tunnel. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de décapsulation [1, 7].

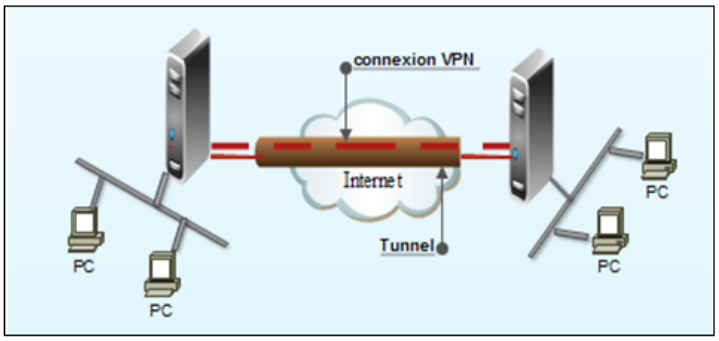


FIGURE 1.11 – Connexion VPN entre 2 cites.

1.4.6.2 Les protocoles de tunnelling

Pour qu'un tunnel soit établie entre deux sites distants, il faut que ces deux derniers utilisent le même protocole de tunnelling (ou protocoles d'encapsulation). Les protocoles

utilisés dans le cadre d'un VPN sont de 2 types, suivant le niveau de la couche OSI auquel ils travaillent [16] :

– Les protocoles de niveau 2 comme PPTP ou L2T.
– Les protocoles de niveau 3 comme IPsec.
– Les protocoles de niveau 4 comme SSL.

1. **Le protocole PPP (Point to Point Protocol) :** est un protocole qui permet le transférer des données sur un lien synchrone ou asynchrone. Il est employé généralement entre un client d'accès à distance et un serveur d'accès réseau. Ce protocole n'est pas un protocole sécurisé mais sert de support aux protocoles PPTP ou L2TP.
2. **Les protocoles PPTP (Point to Point Tuneling Protocol) :** est un protocole qui utilise une connexion PPP à travers un réseau Ip en créant un réseau VPN. Il permet l'encryptage des données ainsi que leur compression. Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP.
3. **Le protocole L2TP (Layer Two Tuneling Protocol) :** est issu de la convergence des protocoles PPTP et L2F (Layer Two Fowarding). Il permet l'encapsulation des paquets PPP au niveau des couches 2 et 3. L2TP n'intègre pas directement de protocole pour le chiffrement des données.
4. **Le protocole IPsec :** IPSec est le standard actuel défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau (niveau 3). Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP en encapsulant les paquets IP dans un en-tête additionnel avant de les transmettre à travers le réseau, afin de garantir la confidentialité, l'intégrité et l'authentification des échanges [w1].
5. **Le protocole SSL (Secure Socket Layer) :** est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application. Il a deux grandes fonctionnalités : l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion. L'inconvénient de ce type de protocole est qu'il se limite au protocole http, ce qui n'est pas le seul besoin de connexion des entreprises.

1.4.7 VLAN (Virtual Local Area Network)

Dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.) .

1.4.7.1 Définition

Les réseaux virtuels (VLAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs. La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusions restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN [17]. Un VLAN, est donc, un regroupement logique, et non physique, de plusieurs stations. Pour réaliser ce regroupement, on intervient directement, par voie logicielle, sur le ou les éléments actifs qui sont les commutateurs VLAN. Les VLAN offrent une solution pour regrouper les stations et les serveurs en ensembles indépendants, de sorte à assurer une bonne sécurité des communications [3].

1.4.7.2 Typologies des VLANs

Les VLANs différent selon les informations utilisées pour regrouper les stations. Il en existe trois modèles [18] :

1. **VLAN par port :** Dans ce modèle, chaque port d'un commutateur est attribué à un VLAN. Toutes les stations connectées à un port appartiennent au VLAN correspondant. Lorsqu'une station est déplacée sur un autre port, celui-ci est également attribué au VLAN de la station. De même, si une station change de VLAN, le port auquel elle est connectée est attribué à son nouveau VLAN (figure 1.12). Les VLAN par ports sont facile à mettre en place et offrent une bonne flexibilité en utilisant le protocole DHCP (Dynamic Host Configuration Protocol) cependant tout déplacement d'une station nécessite une reconfiguration des ports (Manque

de souplesse).

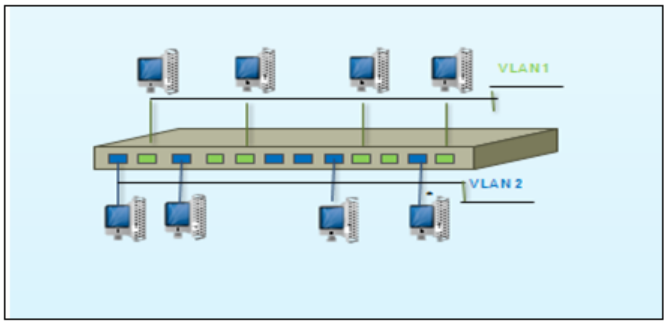


FIGURE 1.12 – VLAN par port

2. **VLAN par Adresse IEEE** [2] **:** Un VLAN par adresse IEEE, ou VLAN de niveau 2 est constitué en associant les adresses MAC (intégrée sur la carte réseau) des stations à chaque VLAN (Fig 1. 13). Les VLANs de niveau 2 Permettent une sécurité au niveau de l'adresse MAC, c'est à dire qu'un pirate souhaitant se connecter sur le VLAN devra au préalable récupérer une adresse MAC du VLAN pour pouvoir entrer mais l'inconvénient est la nécessité de maintenir à jour la base de données des adresses MAC ainsi que les performances sont ralenti du à l'échange des tables d'adresse MAC entre les commutateurs.

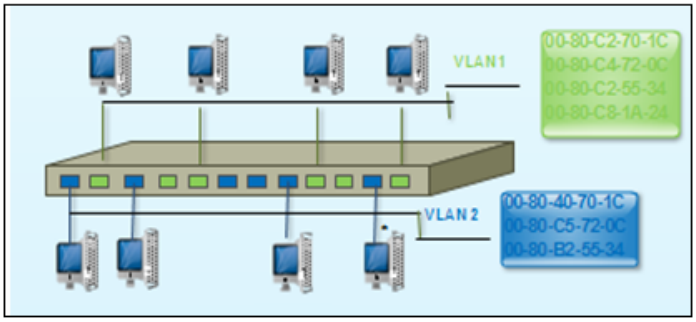


FIGURE 1.13 – VLAN par adresse IEEE.

3. **VLAN par protocole et par sous-réseau**

- ***VLAN par protocole :*** ou VLAN de niveau 3, est obtenu en associant un réseau virtuel par type de protocole du réseau. On peut ainsi constituer un réseau virtuel pour les stations communiquant avec le protocole TCP/IP, et un autre pour

2. l'organisme publiant des recommandations sur les réseaux LAN (technologie Ethernet) et RadioLAN (technologie WiFi).

les stations communiquant avec le protocole IPX [3]. Dans ce type de VLAN, les commutateurs apprennent la configuration. Par contre, elle est légèrement moins performante car les commutateurs doivent analyser des informations.

- ***VLAN par Sous-réseau :*** Un VLAN par sous réseau utilise les adresses IP. Un réseau virtuel est associé à chaque sous réseau IP. Dans ce cas, les commutateurs apprennent aussi la configuration et il est possible de changer une station de place sans reconfigurer le VLAN. Ce type de vlan est souffre de lenteur par rapport aux Vlan de niveau 1 et 2. En effet, le commutateur est obligé de décapsuler le paquet jusqu'à l'adresse IP pour pouvoir détecter à quel Vlan il appartient. Il faut donc des équipements plus couteux (car ils doivent pouvoir décapsuler le niveau 3) pour une performance faible.

1.5 Notion de politique de sécurité

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.

La sécurité informatique doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes [11] :

- analyser la valeur des informations à protéger et analyser des risques ;
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

3. protocole de communication utilisé par le NOS Netware(OS) de Novell.

Donc la politique de sécurité est l'ensemble de règles définies et destinées à contrôler les aspects de sécurité comme les droits d'accès et à appliquer des mesures de sécurité destinées à réduire les risques et les dommages, ainsi pour protéger le personnel, préserver la confidentialité, la disponibilité et l'intégrité des biens, des services et des informations et assurer la continuité de fonctionnement du système [11].

conclusion

Pour l'efficacité de l'utilisation des systèmes d'information et les réseaux informatiques, la sécurité doit être mise au premier plan. Afin de garantir une meilleure sécurisation, on doit d'abord identifier les vulnérabilités des systèmes pour pouvoir contrer aux différents types d'attaques. Pour cela des outils et des techniques de sécurisation sont mise en place.

Chapitre 2

Les systèmes de détection d'intrusions

introduction

Les méthodes de détection d'intrusions utilisées à l'heure actuelle reposent essentiellement sur l'observation d'événements et leur analyse. La collecte d'informations constitue donc la première étape dans tout système de détection d'intrusions. Il s'agit d'une part des informations fournies par le journal système, les journaux propres à certaines applications, mais aussi des données provenant de "sondes" installées par les outils de détection eux mêmes, comme des analyseurs réseau (sniffers [1]) ou des modules applicatifs spécifiques, permettant d'observer l'utilisation de l'application, des modules système permettant de signaler l'exécution de certaines opérations particulières. Le rôle des outils de détection d'intrusions consiste alors à exploiter cette masse d'informations, appelée audit, de manière à y détecter des événements signalant potentiellement une intrusion.

Dans ce chapitre nous présentons tout d'abord la notion de système de détection d'intrusions ainsi que ses différents éléments, ensuite nous présentons les systèmes de prévention d'intrusions, enfin nous terminons par une comparaison entre les deux.

1. Wireshark est un exemple d'un sniffer, est un analyseur de protocole qui examine les données à partir d'un réseau en direct ou à partir d'une capture de fichier sur disque. Il est disponible à cette adresse : http : //www.wireshark.org/.

2.1 IDS (Systèmes de Détection d'Intrusions)

2.1.1 Définition

Il s'agit d'un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion. Un IDS est un système informatique, composé généralement de logiciel et éventuellement de matériel, dont le rôle est la détection d'intrusions. Par définition, un IDS n'a pas de vocation préventive ou réactive dans la mesure ou il n'empêche pas une intrusion de ce produire. Il se contente plutôt d'analyser certaines informations en vue de détecter d'éventuelles activités malveillantes qu'il aura à notifier dans les plus brefs délais au responsable de la sécurité du système. C'est pour cette raison que la majorité des IDS opèrent en temps réel. Toutefois, il y'a des IDS qui réagissent suite à la détection d'une intrusion en mettant fin par exemple a une connexion suspecte [20].

2.1.2 Concepts de base relatifs aux IDS

Nous désirons, dans cette section éclairer quelques notions de base relatives aux IDS et qui seront utilisées dans le reste de ce travail[29].

- ***Administrateur :*** personne chargée de mettre en place la politique de sécurité, et par conséquent, de déployer et configurer les IDS.
- ***Alerte :*** message formaté émis par un analyseur s'il trouve des activités intrusives dans une source de données.
- ***Analyseur :*** c'est un outil logiciel qui met en uvre l'approche choisie pour la détection comportementale ou par scénarios (que nous détaillerons plus tard), il génère des alertes lorsqu'il détecte une intrusion.
- ***Capteur :*** logiciel générant des événements en filtrant et formatant les données brutes provenant d'une source de données.
- ***Sonde :*** un ou des capteurs couplés avec un analyseur.
- ***Evènement :*** message formaté et renvoyé par un capteur. C'est l'unité élémentaire utilisée pour représenter une étape d'un scénario d'attaques connu.
- ***Manager :*** composant d'un IDS permettant à l'opérateur de configurer les différents éléments d'une sonde et de gérer les alertes reçues et éventuellement la réaction.

- ***Notification*** la méthode par laquelle le manager d'IDS met au courant l'opérateur de l'occurrence d'alerte.
- ***Opérateur :*** personne chargée de l'utilisation du manager associé à l'IDS. Elle propose ou décide de la réaction à apporter en cas d'alerte. C'est, parfois, la même personne que l'administrateur.
- ***Réaction :*** mesures passives ou actives prises en réponse à la détection d'une attaque, pour la stopper ou pour corriger ses effets.
- ***Source de données :*** dispositif générant de l'information sur les activités des entités du système d'information.
- ***Détection d'intrusions :*** processus logiciel de recherche de traces laissées par une intrusion dans les données produites par une source.
- ***Faux positif :*** alerte en l'absence d'attaque (fausse alerte).
- ***Faux négatif :*** absence d'alerte en présence d'attaque.
- ***Scénario :*** suite constituée des étapes élémentaires d'une attaque.
- ***Signature :*** suite des étapes observables d'une attaque, utilisée par certains analyseurs pour rechercher dans les activités des entités, des traces de scénarios d'attaques connus.

2.1.3 Architecture d'un IDS

Nous décrivons dans cette section les trois composants qui constituent classiquement un système de détection d'intrusions [22].(figure 2.1) illustre les interactions entre ces trois composants.

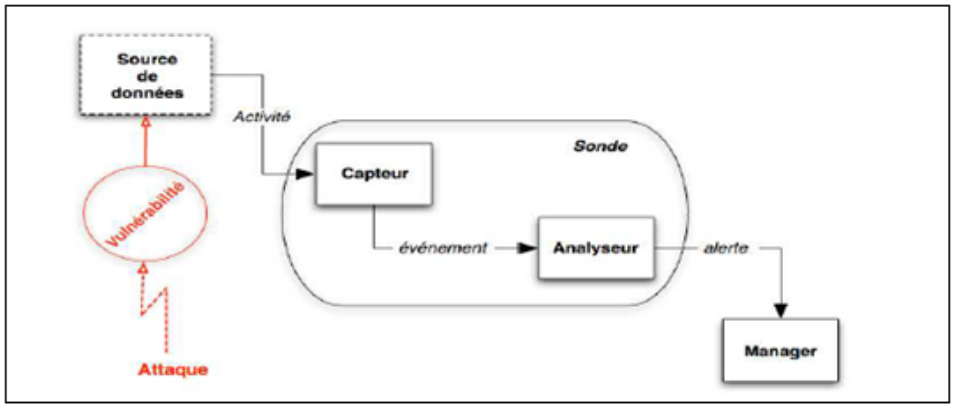


FIGURE 2.1 – Architecture classique d'un IDS

.

2.1.3.1 Capteur

Le capteur observe l'activité du système par le biais d'une source de données et fournit à l'analyseur une séquence d'événements qui renseignent de l'évolution de l'état du système. Le capteur peut se contenter de transmettre directement ces données brutes, mais en général un prétraitement est effectué. On distingue classiquement trois types de capteurs en fonction des sources de données utilisées pour observer l'activité du système : les capteurs système, les capteurs réseau et les capteurs applicatifs.

2.1.3.2 Analyseur

L'objectif de l'analyseur est de déterminer si le flux d'événements fourni par le capteur contient des éléments caractéristiques d'une activité malveillante.

2.1.3.3 Manager

Le manager collecte les alertes produites par le capteur, les met en forme et les présente à l'opérateur. Éventuellement, le manager est chargé de la réaction à adopter qui peut être :

- Confinement de l'attaque, qui a pour but de limiter les effets de l'attaque ;
- Eradication de l'attaque, qui tente d'arrêter l'attaque ;
- Recouvrement, qui est l'étape de restauration du système dans un état sain ;
- Diagnostic, qui est la phase d'identification du problème. Du fait du manque de fiabilité des systèmes de détection d'intrusions actuels, les réactions sont rarement automatisées, car elles peuvent se traduire par un déni de service en cas de faux positif.

2.1.4 Méthodes d'analyses

La technologie des systèmes de détection d'intrusions permet d'analyser les données recueillies de trois façons [23] :

2.1.4.1 Analyse centralisée

L'IDS possède plusieurs capteurs, il centralise les alertes pour les analyser sur une seule machine. Ce type d'analyse présente l'avantage d'avoir une vue globale sur toutes les machines protégées. Toutefois, il a l'inconvénient d'occupation très longue du réseau pour

acheminer l'information.

2.1.4.2 Analyse locale

Chaque machine dispose d'un capteur et analyse l'information à son niveau. Avec ce type d'analyse le trafic réseau est diminué mais les attaques distribuées peuvent échapper à la détection.

2.1.4.3 Analyse distribuée

Des petits programmes appelés agents sont déployés sur les nœuds du réseau. Pour les besoins d'analyse un agent est envoyé sur une machine pour traiter l'information.

2.1.5 Les différentes types d'IDS

Comme nous l'avons vu, les attaques utilisées par les pirates sont très variées. Certaines utilisent des failles réseaux et d'autres des failles de programmation. Nous pouvons donc facilement comprendre que la détection d'intrusions doit se faire à plusieurs niveaux. Ainsi, il existe différents types d'IDS dont nous détaillons ci-dessous les caractéristiques principales.

2.1.5.1 La Détection d'Intrusion Réseau (NIDS)

Ces outils analysent le trafic réseau, ils comportent généralement des dispositifs matériels ou logiciels (sniffers) qui permettent de capturer le trafic réseau sur le segment réseau à surveiller et un moteur qui réalise l'analyse du trafic afin de détecter les signatures d'attaques ou les divergences face au modèle de référence. Ils permettent de détecter les attaques en déni de service qui se passent au niveau réseau et les tentatives de pénétration à distance. Néanmoins il est difficile de savoir qui est à l'origine de l'attaque, car il est facile de masquer son identité en modifiant les paquets réseau[4].

- **Les avantages des NIDS [24]**

– L'IDS basé réseau est capable de contrôler un grand nombre d'hôte avec un petit coût de déploiement.
– Il n'influence pas sur les performances des entités surveillées.

- L'IDS basé réseau est capable d'identifier les attaques de /à multiples hôtes.
- L'IDS basé réseau assure une grande sécurité contre les attaques parce qu'il est invisible aux attaquants.
- Il peut capturer le contenu de tous les paquets envoyés à un système cible.
- Les NIDS sont des systèmes à temps réel.

- **Les inconvénients des NIDS [24]**

- L'IDS basé réseau ne peut pas fonctionner dans des environnements cryptés. Sauf si l'on dispose des clés de déchiffrement, ce qui reste peu probable.
- Ce type d'IDS ne permet pas d'assurer si une tentative d'attaque est couronnée de succès.
- Ils ne peuvent donner d'alertes que si le trafic correspond aux règles ou aux signatures pré configurées.
- Il ne peut pas déterminer si une attaque a réussi.
- Il faut des configurations spéciales sur les réseaux commutés pour que le NIDS puisse voir tout le trafic.

- **L'emplacement des capteurs NIDS [24]**

- Il est également possible de placer un capteur a 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.
- Les capteurs places a l'extérieur du pare-feu servent a détecter toutes les attaques en direction du réseau, leur tache 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 également possible de placer un capteur et un autre apres le firewall.
- Les capteurs IDS sont parfois situes a l'entrée de zones du réseau particulièrement sensibles (parcs de serveurs, données confidentielles), de façon a surveiller tout trafic en direction de cette zone.

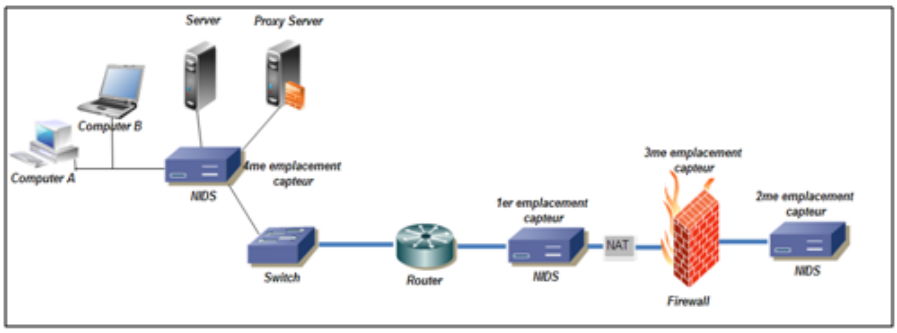


FIGURE 2.2 – Emplacement des capteurs NIDS

.

2.1.5.2 La détection d'intrusion basée sur l'hôte (HIDS)

Les systèmes de détection d'intrusion basés sur l'hôte ou HIDS (Host IDS) analysent le fonctionnement ou l'état des machines sur lesquelles ils sont installés afin de détecter les attaques. Ils sont très dépendants du système sur lequel ils sont installés. Ces IDS peuvent s'appuyer sur des fonctionnalités d'audit propres au système d'exploitation ou non, pour vérifier l'intégrité du système et générer des alertes [4].

- **Les avantages des HIDS [24]**

– La capacité de contrôler les activités locales des utilisateurs avec précision.
– Capable de déterminer si une tentative d'attaque est couronnée de succès.
– La capacité de fonctionnement dans des environnements cryptés.
– L'IDS basé hôte fonctionne sur les traces d'audit des systèmes d'exploitation ce qui lui permet de détecter certains types d'attaques (exemple : Cheval de Troie).
– ils génèrent peu de faux positifs, permettant d'avoir des alertes pertinentes.

- **Les inconvénients des HIDS [24]**

– La difficulté de déploiement et de gestion, surtout lorsque le nombre d'hôtes qui ont besoin de protection est large.
– Ces systèmes sont incapables de détecter des attaques contre de multiples cibles dans le réseau.
– Ils peuvent être identifiés et mis hors service par un attaquant.

– Sensibles aux attaques de type Déni de Service.

- **L'emplacement des capteurs HIDS [24]**

– Les HIDS sont en general places sur des machines sensibles, susceptibles de subir des attaques et possedant des donnees sensibles pour l'entreprise.les serveurs, web et applicatifs, peuvent notamment etre proteges par un HIDS.

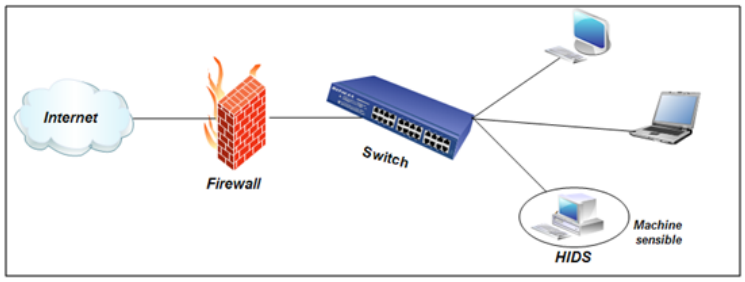


FIGURE 2.3 – Emplacement des capteurs HIDS

.

2.1.5.3 IDS Hybrides

Les IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, en un seul outil, de surveiller le réseau et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser le tout, et lier les informations d'origines multiples. Ainsi,Nous comprenons que les IDS hybrides sont basés sur une architecture distribuée, ou chaque composant unifie son format d'envoi d'alerte (typiquement IDMEF)(Intrusion Detection Message Exchange Format) voir (figure 2.4).Cela permet de communiquer et d'extraire des alertes plus pertinentes [4].

- **Les avantages des IDS hybrides [25]**

– Moins de faux positifs

– Meilleure corrélation (la corrélation permet de générer de nouvelles alertes à partir de celles existantes).

– Possibilité de réaction sur les analyseurs.

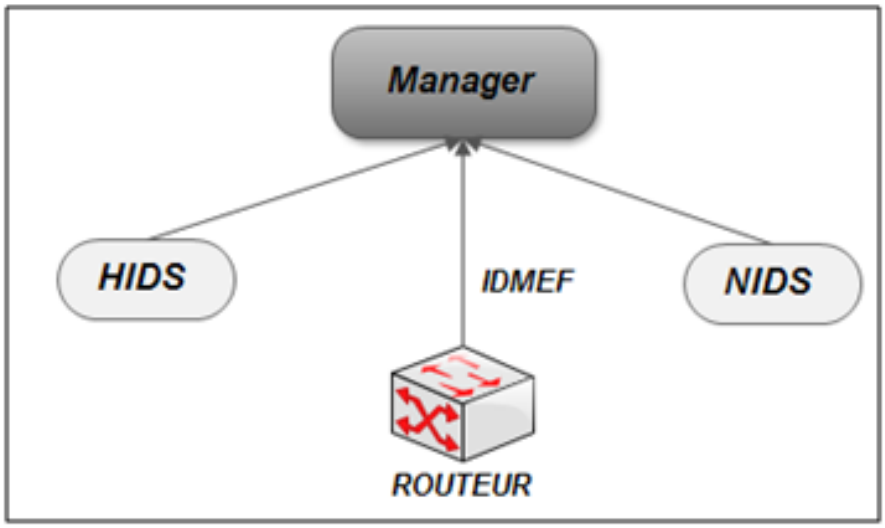


FIGURE 2.4 – le fonctionnement de l'IDS hybride

.

2.1.6 Méthodes de détection

En général, il existe deux types d'approches pour détecter les intrusions dans les systèmes informatiques : l'approche comportementale basée sur un modèle constitué des actions autorisées, l'approche par scénarios basée sur un modèle constitué des actions interdites dans le système d'informations.

2.1.6.1 Approche comportementale

Elle permet de détecter toute déviation par rapport à un comportement normal préalablement défini, ce comportement normal, appelé profil, peut être par apprentissage ou en spécifiant une politique de sécurité[29].

1. ***Profils construit par apprentissage***

   Parmi les méthodes proposées pour construire les profils par apprentissage, les plus marquantes sont les suivantes [29] :

   - ***Méthodes statistiques :*** propose une approche statistique permettant d'obtenir le profil, ce dernier est calculé à partir de variables considérées comme aléatoires et échantillonnées à intervalles réguliers. Ces variables peuvent être le temps processeur utilisé, la durée, les heures de connexions, le nombre de mails reçus par jour, etc. Un modèle statistique est utilisé pour construire la distribution de chaque variable et pour mesurer le taux de déviation entre un comportement courant et

un comportement passé. Si ce taux dépasse un certain seuil, le système déclare qu'il est attaqué.

- ***Système expert :*** la différence majeure entre un système expert et un modèle statistique est que ce dernier utilise des formules statistiques pour identifier un profil alors que le système expert utilise un ensemble de règles pour le représenter. Ainsi le comportement d'un utilisateur courant est comparé aux règles, à la recherche d'une anomalie.
- ***Réseaux de neurones :*** cette technique consiste à apprendre à un réseau de neurones le comportement normal d'un utilisateur. Le réseau enregistre les opérations de l'utilisateur durant une fenêtre temporelle donnée, puis tente de prédire la prochaine opération. Un échec de prédiction correspond, ainsi, à une déviation par rapport au profil et donne potentiellement lieu à une alerte.
- ***Immunologie :*** cette approche est inspirée du système immunitaire. Elle consiste à construire un modèle de comportement normal des services et non des utilisateurs au travers des courtes séquences d'appels systèmes. La phase d'apprentissage consiste à observer un service pendant un certain temps afin de construire une base de séquences d'appels normaux. En phase de détection, toute séquence étrangère a cet ensemble est considérée une potentielle exploitation d'une faille de sécurité du service.
- ***Les réseaux bayésiens :*** les réseaux bayésiens permettent de modéliser des situations dans lesquelles la causalité joue un rôle, mais où la connaissance de l'ensemble des relations entre les phénomènes est incomplète, de telle sorte qu'il est nécessaire de les décrire de manière probabiliste.

2. ***Profil spécifiant une politique de sécurité (policy-based)***
   Pour les IDS dits policy-based, il n'y a pas de phase d'apprentissage. Leur comportement de référence est spécifié par une politique de sécurité : la détection d'une intrusion intervient chaque fois que la politique est violée.

2.1.6.2 Approche par scénarios

Généralement, les IDS réseaux se basent sur un ensemble de signatures qui représentent chacune le profil d'une attaque. Cette approche consiste à rechercher dans l'activité de l'élément surveillé (un flux réseau) les empreintes d'attaques connues, à l'instar des antis

virus.

Une signature est habituellement définie comme une séquence d'événements et de conditions relatant une tentative d'intrusion. La reconnaissance est alors basée sur le concept de "pattern matching" (analyse de chaînes de caractères présente dans le paquet, à la recherche de correspondance au sein d'une base de connaissance). Si une attaque est détectée, une alarme peut être remontée (si l'IDS est en mode actif, sinon, il se contente d'archiver l'attaque)[25]. Trois familles de méthodes sont utilisées par les IDS à signature qui se basent tous sur la recherche d'un profil connu d'attaque [25] :

- ***Système expert :*** L'idée consiste à coder les attaques sous forme de règles condition-action. Les conditions portent sur l'état du système surveillé et la nature des événements analysés ; les actions permettent, soit de mémoriser le nouvel état du système, soit de conclure à la présence d'une attaque [21].
- ***"Pattern matching" (reconnaissance de formes) :*** Cette méthode consiste à identifier dans les paquets analysés une suite d'événements ou de caractères caractéristiques d'une attaque connue. En fait, Le trafic réseau peut être vu comme une chaîne de caractères principale et les scénarios d'attaque comme des sous-suites qu'on veut identifier.
- ***Algorithmes génétique :*** Les algorithmes génétiques utilisent la notion de sélection naturelle et l'appliquent à une population de solutions potentielles à un problème difficile (dont on ne sait pas trouver la solution optimale) pour trouver une solution approchée dans un temps raisonnable.

2.1.6.3 Avantages et inconvénients des deux approches

Chacune de ces deux approches présente des avantages et des inconvénients [25] :

– L'avantage de l'analyse comportementale est avant tout lié à sa capacité à détecter des attaques inconnues. Les inconvénients sont que ces outils ont tendance à générer un grand nombre de faux positifs si le modèle de référence n'est pas exhaustif, laissant ainsi la possibilité à un attaquant potentiel de modifier lentement son comportement afin d'habituer le système à un comportement intrusif. En outre, des attaques peuvent ne pas être détectées (faux négatifs) si le corpus utilisé pour l'apprentissage contient des activités intrusives. De plus, les alertes sont plus difficiles à appréhender qu'avec

une analyse par signature car l'alerte ne désigne pas une attaque connue.

– L'avantage des outils basés sur l'approche par scénarios est lié à leur capacité de prendre en compte les comportements exacts des attaquants potentiels, ce qui devrait présenter un taux de faux négatif très faible. Cependant, si la signature de l'attaquant n'est pas dans la base, l'attaque en question ne sera pas détecter (faux négatifs). En autre, si cette signature n'est pas assez précise, elle peut également conduire à de nombreux faux positifs. En revanche, de nouvelles attaques ne sont pas systématiquement reconnues à cause de la difficulté de mise à jour de la base d'attaque.

  Chacune de ces approches peut, donc, conduire a des faux positifs ou a des faux négatifs. Il semble, donc, indispensable d'utiliser simultanément une approche comportementale et une approche par scénarios de manière à profiter des avantages de l'une et de l'autre.

2.1.7 Comportement d'un IDS en cas d'attaque détectée

Le comportement d'un IDS après la détection d'une intrusion est l'ensemble des actions prises par le système lorsqu'il détecte une attaque. Ces réponses peuvent être actives ou bien passives.

2.1.7.1 Réponse active

Des systèmes de détection d'intrusions peuvent, en plus de la notification à l'opérateur, prendre automatiquement des mesures pour stopper l'attaque en cours. Par exemple, ils peuvent couper les connexions suspectes ou même, pour une attaque externe, reconfigurer le pare-feu pour qu'il refuse tout ce qui vient du site incriminé. Des outils tels que RealSecure propose ce type de réaction. Toutefois, il apparait que ce type de fonctionnalité automatique est potentiellement dangereux car il peut mener à des dénis de service provoqués par l'IDS. Un attaquant déterminé peut, par exemple, tromper l'IDS en usurpant des adresses du réseau local qui seront alors considérées comme la source de l'attaque par l'IDS. Il est préférable de proposer une réaction facultative à un opérateur humain (qui prend la décision finale) [28].

2.1.7.2 Réponse passive

Dans ce cas, quand une attaque est détectée, le système de détection d'intrusions ne prend aucune action. Il génère seulement une alarme pour notifier l'administrateur de

système qui va prendre des mesures en se basant sur les rapports générés par le système de détection d'intrusions [24].

2.1.8 Placement des IDS

Nous trouvons sur Internet plusieurs propositions et plusieurs solutions toutes faites pour positionner les sondes sur un réseau, quel que soit les besoins. Il serait faux de penser que tous les réseaux doivent être protégés de la même manière. Tout d'abord, il faut analyser la topologie du réseau pour comprendre les vulnérabilités qu'un attaquant peut utiliser pour accéder à ce dernier, et identifier les composants critiques qu'ils seront probablement visés par les attaquants, donc le placement des IDS va dépendre de la politique de sécurité menée(figure 2.5). Une fois l'analyse est faite il reste à déterminer où les positionner au sein de l'infrastructure pour avoir une vision globale du système et surveiller l'activité intrusive à toutes les frontières fonctionnelles courantes sur le réseau. Il est important pour cela de bien définir les zones sensibles du système d'information, il serait intéressant de placer des IDS [27, 30] :

- ***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 a surveiller.
- ***Localisation 3 :*** sur chaque segment reseau.il se concentre sur les attaques ayant passées le firewall et s'étant introduites sur ce segment réseau.
- ***Localisation 4 :*** sur un sous réseau, comme pour la location 3, vise à protéger un sous réseau particulier.

2.1.9 Les limites des IDS

La plupart des IDS souffrent actuellement de quelques problèmes [31] :

– malgré que les IDS utilisent des techniques de plus en plus sophistiquées pour les analyses statistiques des profils des utilisateurs, on ne peut pas affirmer qu'ils sont fiables complètement. Un IDS ne peut remplacer les systèmes d'authentification, et ne peut compenser les faiblesses d'identifications.

– Plusieurs solutions doivent être associées pour obtenir un niveau de sécurité accep-

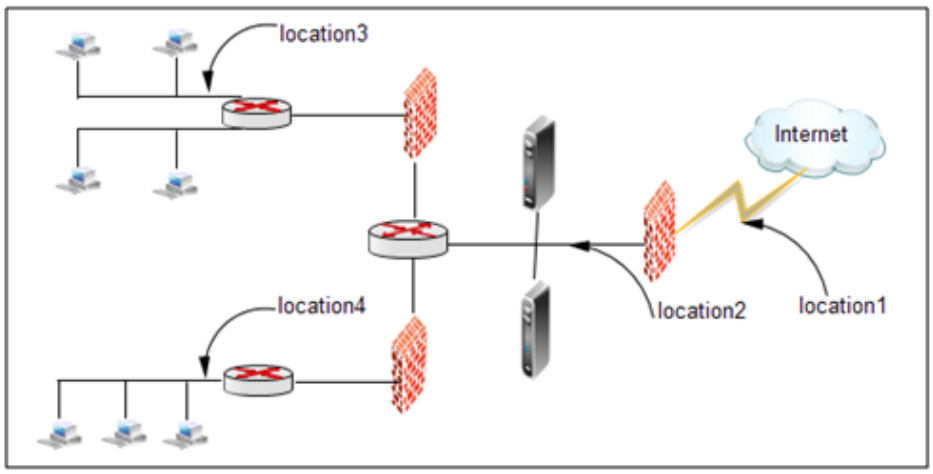


FIGURE 2.5 – Emplacement des IDS

.

table. Un IDS ne peut être considéré comme étant le produit miracle pour sécuriser un système.

– Un IDS ne peut conduire des recherches concernant les attaques sans l'intervention de l'être humain. Par exemple un IDS ne peut fournir que l'adresse IP de la machine a partir de laquelle l'attaque a été commise sans pour autant pouvoir identifier la personne responsable.
– Un IDS ne peut analyser tous les paquets dans un système à fort taux d'occupation. les différentes solutions commerciales existantes ne peuvent assurer l'analyse de tous les paquets si le débit dans le réseau dépasse un certain seuil.

2.2 IPS (Le système de prévention d'intrusions)

Les IPS (Intrusion Prevention System) sont, à la différence des IDS, un ensemble de matériel et de logiciel ayant pour but d'empêcher les intrusions ou autres activités suspectes détectées. Les IPS sont donc des outils actifs permettant de stopper toutes activités suspectes, contrairement aux IDS qui ne font que les détecter.

Un IPS possède de nombreux inconvénients. Le premier est qu'il bloque toute activité qui lui semble suspecte. Or, il est impossible d'assurer une fiabilité complète dans l'identification des attaques. Les faux positifs sont donc très dangereux pour les IPS. Le deuxième inconvénient est qu'un pirate peut utiliser sa fonctionnalité de blocage pour mettre hors

service un système. Et enfin, le troisième inconvénient et non le moindre, un IPS est peu discret. En effet, à chaque blocage d'attaque, il montre sa présence. Cela peut paraître anodin, mais si un pirate remarque la présence d'un IPS, il tentera de trouver une faille dans celui-ci afin de réintégrer son attaque, mais cette fois en passant inaperçu [29].

2.3 La comparaison entre IDS et IPS

Nous pouvons dire qu'un IPS est un IDS étendu qui a pour principale différence d'intercepter les paquets intrus, il agit et est donc actif au sein du réseau. Les systèmes IDS et IPS appliquent des méthodes similaires lorsqu'ils essaient de détecter des intrus ou des attaques sur le réseau. En fait le principe de détection de l'IPS correspond exactement à celui de l'IDS. Il possède donc généralement soit une base de données de signatures qui peut être régulièrement mise à jour a mesure que de nouvelles menaces sont identifiées, soit un système a approche comportementale qui analyse les différences avec le niveau de fonctionnement normal du réseau qui a été défini par l'administrateur (figure 2.6). Il y a donc une certaine symétrie entre IPS et IDS sauf que la définition d'un IDS n'inclut pas la prévention contre les intrusions, il se contente de les détecter et de les reporter à un opérateur [w3].

Un IPS est conçu pour identifier les attaques potentielles et exécuter de façon autonome une contre-mesure pour les empêcher, sans affecter le système d'exploitation normal.

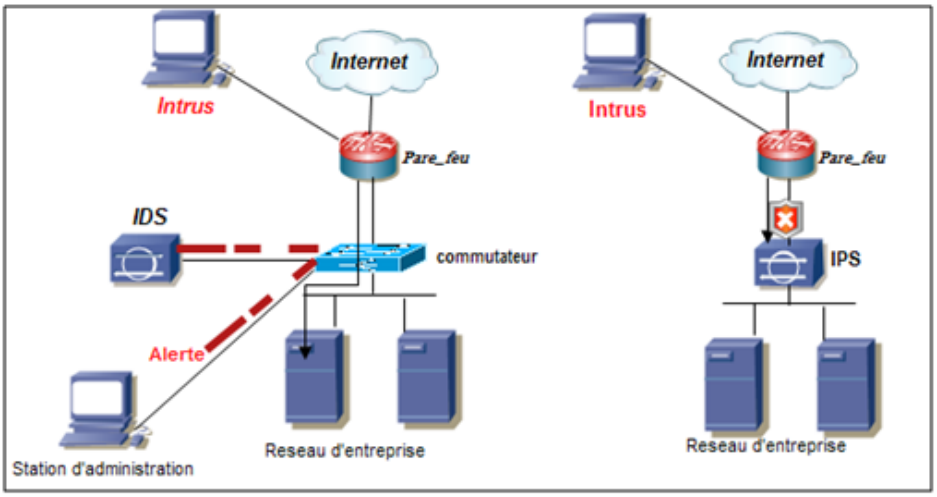


FIGURE 2.6 – La comparaison entre IDS et IPS

.

conclusion

La plupart des IDS sont plus aux moins fiables, ce qui explique qu'ils sont souvent intégrés dans les solutions de sécurité. Les avantages qu'ils présentent face aux autres outils de sécurités les favorisent, mais d'un autre côté cela n'empêche pas que les meilleurs IDS présentent aussi des lacunes et quelques inconvénients. Nous comprenons donc bien qu'ils sont nécessaires mais ne peuvent pas se passer de l'utilisation d'autres outils de sécurité visant à combler leurs défauts.

Ce chapitre nous a permis de découvrir les systèmes de détection d'intrusions leurs fonctionnements et leurs capacités et il nous est paru évident que ces systèmes sont à présent indispensables aux entreprises afin d'assurer leur sécurité informatique, compléter les tâches des autres équipements de sécurité. Nous allons voir dans le chapitre suivant comment réussir une bonne configuration de ces derniers afin de mieux sécuriser le réseau.

Chapitre 3

Organisme d'accueil et contexte du projet

introduction

Ce chapitre est une introduction au réseau et l'environnement de l'entreprise NAFTAL District GPL (Gaz de Pétrole Liquéfie) de Béjaïa, nous avons en premier lieu pris connaissance de celle-ci et des différents services qui la constituent, ainsi que les tâches associées à chaque service. En second lieu nous nous sommes intéressées au département informatique afin de comprendre l'architecture réseau requise par l'entreprise et illustrer les différents équipements qui la constituent.

3.1 Présentation générale de " NAFTAL "

L'entreprise publique NAFTAL est passée en Société Par Action (SPA) dès le 18 Avril 1998. Suivant les statuts déposés auprès de l'étude de Maître BRAHIMI Notaire à Alger. La raison sociale de la société change suite à cette séparation des activités NAFTAL SPA est désormais chargé de la commercialisation des produits pétroliers.

3.1.1 Historique et situation géographique

L'entreprise ERDP (entreprise de raffinage et de distribution des produits pétroliers) a été créée le 6 Avril 1980 par décret N°80/101, issue de " SONATRACH ". Entrée en activité le 01 Janvier 1982, elle est chargée de l'industrie de raffinage et de distribution des produits pétroliers sous le sigle de " NAFTAL ", dont le siège est transféré à CHERAGA (direction générale), Suite à la séparation de l'activité de raffinage de l'activité de distribution.

La création est l'évolution de NAFTAL peuvent être présentées sous forme de trois étapes essentielles 1984,1987et 1998.

- **En 1984 :** SONATRACH restructurée à donnée naissance à plusieurs entreprises nationales : NAFTEC, ENIP, ENPC et NAFTAL qui est l'unité de distribution des produits pétroliers et dérives.
- **En 1987 :** NAFTAL est désormais chargé de la commercialisation et la distribution des produits pétroliers et dérivés.
- **En 1998 :** Elle change de statut est devient SPA (société par action) 100% de SONATRACH avec un capital de 15 650 000 000 DA. Au début de l'année 2000, cette unité (NAFTAL) se répartie en deux zones biens distinctes ; zone GPL (gaz de pétrole liquéfié) et zone CPLB (carburant, lubrifiant, pneumatique et bitumes). La structure centrale de NAFTAL est située à CHERAGA, elle est subdivisée en dix neufs districts GPL dont le district de Béjaïa.

3.1.2 Missions et objectifs de NAFTAL

La mission principale de NAFTAL est la commercialisation et la distribution des produits pétroliers raffinés sur le marché national, notamment ; le GPL (gaz de pétrole liquéfié), Les carburants et lubrifiants y compris ceux destinés à l'aviation et la marine, solvant, aromatiques, paraffinés, bitumes et pneumatiques. Elle intervient aussi dans la formulation des bitumes, distribution, stockage et commercialisation des carburants, GPL, lubrifiants et GPL/carburants spéciaux, et le transport des produits pétroliers. A fin de mener à terme sa mission principale, NAFTAL s'est tracé les objectifs suivants :

– organiser et développer la commercialisation et la distribution de produits pétroliers ;
– stocker, transporter, et/ou faire transporter tous produits pétroliers commercialisés sur le territoire national ;
– développer les infrastructures de stockage et de distribution pour assurer une meilleure couverture du marché ;
– élaborer des plans en liaison avec l'organisme concerné visant la couverture du marché national en produits pétroliers ;
– promouvoir, participer et veiller à l'application de la normalisation et du contrôle de la qualité des produits relevant de son objet ;
– centraliser les informations relatives aux besoins en produits pétroliers en vue de pla-

nifier et d'assurer l'approvisionnement du marché ;
- procéder à tout étude du marché de consommation ;
- développer et mettre en uvre les actions visant l'utilisation optimale et rationnelle des infrastructures et moyens ;
- participer et veiller à la mise en œuvre des actions visant le renforcement de l'intégration économique ;
- concourir à la formation, au recyclage et au perfectionnement des travailleurs ;
- assurer la maintenance des équipements, matériels roulants relevant de son patrimoine.

3.2 Présentation du district GPL de BEJAÏA

La présentation du district GPL va se faire à travers trois points notamment la définition du produit de l'entreprise (le GPL), sa structure organisationnelle, ses missions et objectifs.

3.2.1 Définition du district et du GPL

La branche GPL de NAFTAL est subdivisée en plusieurs districts GPL (gaz de pétrole liquéfié) dont le district de Béjaïa qui se situe à l'arrière port BP123 cette position est stratégique, du fait que le district a une façade vers le port ce qui lui donne l'avantage de faciliter l'approvisionnement direct de la raffinerie vers le port par cabotage. Ce district comprend aussi géographiquement, Jijel et quelques communes de Bouira.

- ***GPL :(gaz de pétrole liquéfié)***

Le GPL est un produit pétrolier au même titre que le gasoil ou l'essence, nous le trouvons soit à l'état naturel dans les nappes du pétrole, soit il résulte du raffinage du pétrole, il est composé de 50{

Le GPL est incolore, il est extrêmement inflammable est volatile et il est plus lourd que l'air. Pour déceler d'éventuelle fuites nous lui donnons odeur particulière en moyens mercaptan à base de souffre.

Le GPL liquide dépend de la pression et de la température auquel il est stocké. Pour l'utilisateur automobile le GPL/C est constitué d'un mélange de butane et de propane, dans une proportion variant les saisons.

3.2.1.1 La structure organisationnelle du district GPL

Le district comprend plusieurs départements qui sont gérés par la direction générale avec des services qui assure le lien entre eux. Ces départements et services sont les suivants :

- ***Service de Sureté :*** ce service assure la sécurité au sien de l'entreprise.
- ***Service Sécurité Industrielle :*** il se charge d'assurer les tâches suivantes :
  - La protection et la préservation du personnel ;
  - La préservation et la conservation du patrimoine industriel ;
  - La protection de l'environnement.
- ***Service Juriste.***
- ***Département informatique :*** il comprend deux services, service ING (Information de Gestion) et service réseau et système.
- ***Département personnel et moyen communs :*** il comprend trois services, à savoir ; Le service personnel, le service moyens communs et le service ressources humaines.
- ***Département commercial :*** il comprend deux services, service des ventes et service marketing.
- ***Département technique et maintenance :*** Le département technique et maintenance comprend trois services, le service de maintenance, installation fixe, le service planning et méthode et le service maintenance matériel roulant.
- ***Département exploitation :*** Le département d'exploitation comprend trois services, le service approvisionnement et distribution, le service transport et le service production.
- ***Département finance et comptabilité :*** Le département finance et comptabilité est subdivisé selon la nouvelle structure en trois services : service comptabilité, service trésorerie et service budget et coût. L'ensemble de ces services et départements est schématisé par l'organigramme suivant du district GPL (Béjaïa).

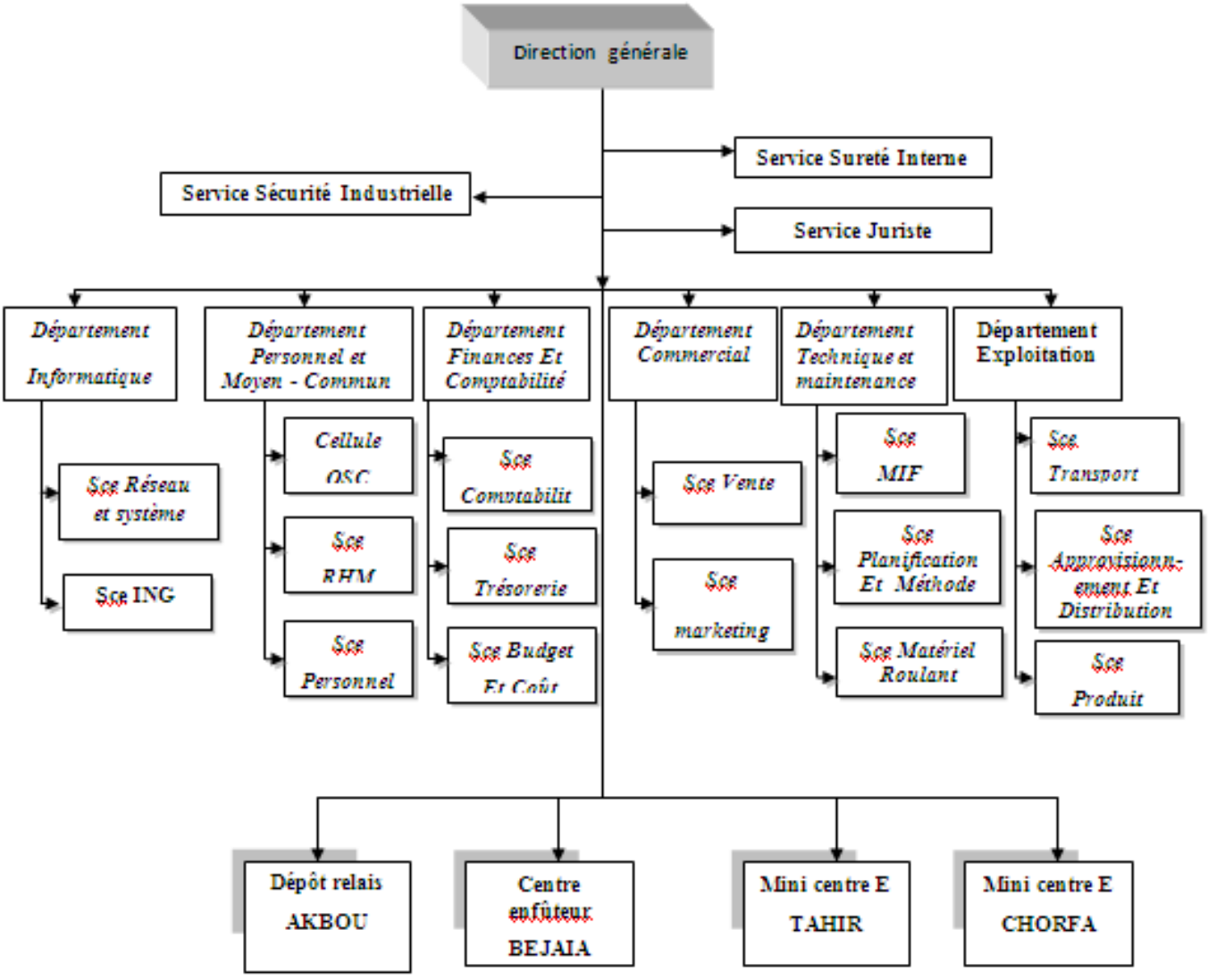


FIGURE 3.1 – Organigramme du district GPL (Béjaïa)

.

3.2.2 Présentation du département informatique

3.2.2.1 Le rôle du département informatique de GPL

La division informatique rassemble une quinzaine de personnes qui exercent différentes tâches, dans le but d'assurer le bon fonctionnement du réseau de l'entreprise "NAFTAL GPL".

3.2.2.2 Organigramme du département Informatique

Nous allons à présent illustrer l'organigramme associé à la section informatique, afin d'étudier de plus près les deux services qui y contribuent.

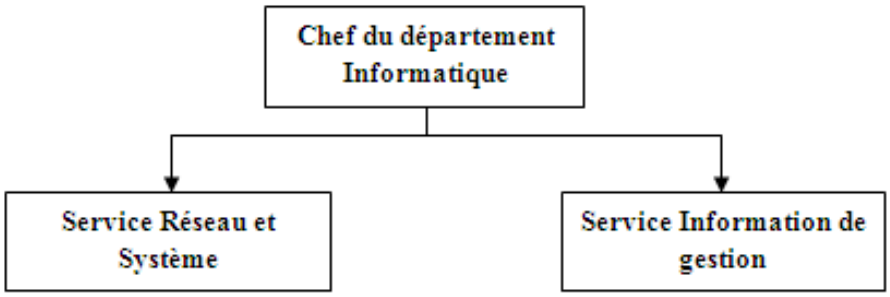


FIGURE 3.2 – Organigramme du département informatique

.

- ***Description et rôle de chaque service au sein du département Informatique :*** Les deux services associés au département Informatique jouent les tâches cités ci-dessous : Service Réseaux et Systèmes assure :

– Maintenance de matériels informatique ;
– Maintenance des logiciels, système et application ;
– Suivi des différentes activités administrateur réseau. Service Informatique de Gestion assure : ce service se charge à remplir certain tâches et responsabilités :
– Consolide sur la base des rapports des unités, les rapports périodiques des activités relevant des structures de la zone ;
– Veille au recueil de l'information à partir des CDS (Centre De Stock) et structure de la zone ;

- Analyse les états ;
- Participe à l'élaboration des plans de production de la zone, consolide les plans élaborés par les structures de la zone ;
- Exécute toute autre tâche, relevant de ses compétences, pouvant lui être confiée par la hiérarchie.

3.2.3 L'architecture réseau de district GPL de Bejaia

Une architecture réseau est un ensemble d'équipements matériels et logiciels interconnectés en réseau, afin de régir des activités informatiques collectives, en centralisant ou répartissant les ressources et les tâches à travers le système. C'est donc une façon d'interconnecter physiquement les différents éléments d'un réseau et de combiner son organisation logicielle, dans le but de communiquer et d'effectuer des opérations informatiques.

L'architecture de l'entreprise NAFTAL GPL, dispose d'un réseau LAN constitué d'un ensemble d'équipements matériels et logiciels. Le meuble de GPL de Bejaia se compose de 4 blocs séparés, dans chaque bloc se trouve un sous réseau composé d'une armoire où se trouve un commutateur de niveau 2, un onduleur, un panneau de brassage. L'armoire située au département informatique est reliée en cascade "câble RJ45" avec les autres armoires existantes (département ressource humaine, département archive) et celle située au département commerciale est liée en fibre optique, par contrainte de distance entre ces deux départements soit 150 m.

Le département informatique comprend un serveur qui offre certains services, nous citons parmi eux : FTP, DHCP, DNS et l'annuaire Active Directory. Pour qu'une machine interne puisse se connecter à internet, le LAN de NAFTAL est connecté à un fournisseur d'accès, en passant par le routeur qui se trouve dans l'armoire du département et pour qu'elle puisse accéder à un réseau étendu, il est impératif qu'elle passe en premier lieu par un mécanisme de filtrage, qui représente dans notre cas le " pare-feu " qui est intégrer dans le routeur.

La figure suivante illustre l'architecture décrite :

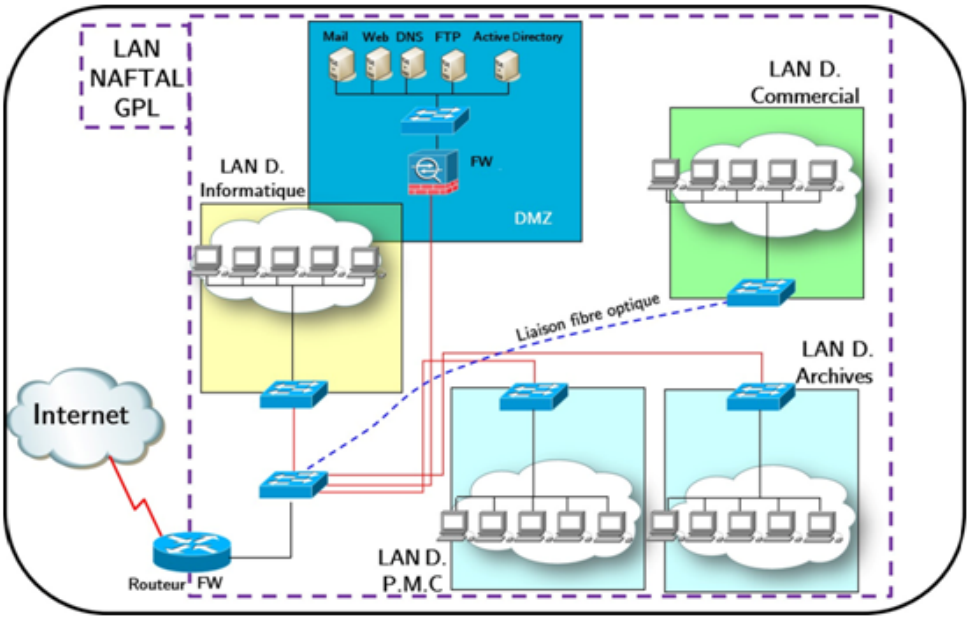


FIGURE 3.3 – L'architecture du réseau informatique de district GPL BEJAIA

.

3.2.3.1 Infrastructure matériel

L'entreprise NAFTAL dispose de plusieurs équipements réseau le serveur, les switch et les routeurs,...

Dans le but de faciliter la gestion du système d'information, il existe des services au sein de l'entreprise, on cite parmi eux :

– Le contrôleur de domaine " Active Directory " : est un service d'annuaire, qui fournit un certain nombre de différents services relatifs au stockage des ressources du réseau.
– Services DNS, DHCP, FTP.

3.2.3.2 Les supports de transmissions

Pour relier les différents équipements qui sont utilisé dans le réseau ; NAFTAL opte pour deux types de média :

– Le câble à paire torsadées : on distingue deux catégories, le câblage 'UTP', terminé par des connecteurs RJ45 (les catégories de câble UTP utilisées par le réseau de NAFTAL " GPL" sont 3, 4, 5, 5e, 6, 6a et 7) et le câble à pire torsadées blindées 'STP'.
– la fibre optique : le câblage en fibre optique utilise des fibres de verre ou de plas-

tique pour guider des impulsions lumineuses de la source à la destination. Le réseau de NAFTAL dispose aussi de point d'accès de gamme "Aironet Cisco", permettant d'assurer une connexion sans fil.

3.2.3.3 Gestion des utilisateurs et autorisations d'accès au réseau

Chaque employé possède un compte sur son ordinateur (dont les identifiants vous sont donnés à votre arrivée dans l'entreprise par le service informatique), sécurisé par un mot de passe. Lorsque l'ordinateur s'allume le nom d'utilisateur et le mot de passe sont demandés par le serveur. C'est lui qui s'occupe d'authentifier l'utilisateur et lui autoriser l'accès à son poste de travail.
Le serveur va également mettre à disposition des employés des dossiers partagés, accessibles à certains et pas à d'autre, selon le poste de l'employé.
Chaque service pourra avoir son propre dossier partagé. Le secrétariat pour avoir un dossier partagé avec tous les employés pour mettre à leur disposition des documents types, notes de frais...

3.2.3.4 La sécurité au niveau du réseau NAFTAL

L'entreprise NAFTAL utilise un firewall comme mécanismes de barrière, interdisant l'entrée à un certain type de trafic et en autorisant d'autres trafics (filtrer les paquets) suivant une politique de sécurité pour sécurisé son réseau, plus une application de sécurité (Kaspersky Security) pour surveiller l'état de ces machines.

3.2.4 Problématique

Utiliser un firewall pour sécuriser un réseau d'une entreprise n'est plus suffisant à l'avenir. Il n'est capable de filtrer que le trafic qui le traverse, donc il est impossible d'interdire les actions malveillantes des utilisateurs via des stations non protégée par celui-ci.

Les systèmes de pare-feu traditionnels manquent souvent cruellement de solutions intégrées pour détecter les intrusions et maîtriser les risques liés aux attaques. Les vers, troyens et les hackers sont beaucoup trop nombreux et intelligents pour être détectés et éliminés par une simple porte filtrant les entrées / sorties en fonctions des IP et des

ports. Il n'y a pas de système permettant de contrôler et d'analyser le trafic dans le but de détecter des actions suspectes.

3.2.5 La solution proposée

Pour repérer les activités anormales ou suspectes dans le réseau, il est préférable de disposer d'un système de détection d'intrusion (IDS) afin d'écouter le trafic circulant sur les principaux liens du réseau d'une manière furtive. IDS joue le rôle d'un complément aux firewalls en lui permettant une analyse plus intelligente du trafic. Il augmente le degré de sécurité.

Les IDS servent à contrôler les trafics qui sont autorisés par le firewall et prennent des décisions si le trafic observé est suspect. Les IDS peuvent découvrir les attaquants qui parviennent à pénétrer les firewalls et les annoncer aux administrateurs de système, qui peuvent prendre des mesures pour empêcher des dégâts.

Pour notre cas d'étude, nous avons choisi d'installer un IDS Cisco Appliance (non intégré) et configurer cet équipement d'une manière sécurisée.

conclusion

L'étude du réseau Naftal nous a permis de bien comprendre son architecture et les stratégies utilisées pour sa sécurisation et c'est se qui nous à permet de voir ses faiblesses, et conduit à proposé la solution pour palier à ces derniers.
Le chapitre suivant va être concrétisé à mettre en œuvre notre solution et pouvoir la simuler avec le simulateur GNS3.

Chapitre 4

Mise en œuvre de la solution

introduction

Après avoir étudié en terme de sécurité le réseau de Naftal et décrit notre solution dans le chapitre précédent, nous allons voir dans ce dernier chapitre la simulation de notre solution qui consiste à configurer un système de détection d'intrusion, qui est IPS Cisco série 4235.

Pour visualiser notre travail et mettre en évidence la configuration de notre application, nous avons utilisé un outil de simulation qui se nomme GNS3 version 0.8.3.1. Ainsi nous allons présenter les autres outils utilisés et la procédure de configuration pour mettre en œuvre notre solution.

4.1 Présentation de GNS3

4.1.1 Définition

GNS3 signifie Graphical Network Simulator, est un simulateur de réseau graphique qui permet l'émulation de réseaux complexes. Il est utilisé pour reproduire différents systèmes d'exploitation dans un environnement virtuel. Il permet l'émulation en exécutant un IOS Cisco (Internetwork Operating Systems) [w5].

4.1.2 Objectif de GNS3

L'objectif de GNS3 est d'apporter aux étudiants et professionnels des nouvelles technologies de communication travaillant dans le domaine de l'administration systèmes et réseaux une solution pour virtualiser et modéliser fidèlement des réseaux. Le principal avantage de GNS3 réside dans l'émulation matérielle, en lieu et place de l'utilisation de simulateurs qui souvent est une manière limitée de virtualiser du matériel. Grâce à GNS3, les utilisateurs peuvent tester et estimer, dans des conditions quasi réelles et sans avoir à financer le matériel, leurs configurations et réseaux avant de les mettre en place physiquement [w4].

4.1.3 Les fonctionnalités du logiciel

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à :

- ***Dynamips :*** est un émulateur de routeur Cisco écrit par Christophe Fillot. Il émule 1700, 2600, 3600, 3700 et 7200 plates-formes matérielles [w5].
  Dynamips est un émulateur de routeurs Cisco capable de faire fonctionner des images Cisco IOS non modifiées comme si elles s'exécutaient sur de véritables équipements. Le rôle de Dynamips n'est pas de remplacer de véritables routeurs, mais de permettre la réalisation de maquettes complexes avec de vraies versions d'IOS [31].
  Ce type d'émulateur serait utile de [w4] :
- Être utilisé comme une plate-forme de formation, avec les logiciels utilisés dans le monde réel. Il permettrait aux gens de se familiariser avec les équipements Cisco, Cisco est le leader mondial dans les technologies de mise en réseau ;
- Test et fonctionnalités expérimentales de Cisco IOS ;
- Vérifier rapidement les configurations qui seront déployés par la suite de véritables routeurs.
- ***Dynagen :*** est un produit complémentaire écrit en Python s'interfaçant avec Dynamips grâce au mode hyperviseur. Dynagen facilite la création et la gestion de maquettes grâce à un fichier de configuration simple décrivant la topologie du réseau à simuler et une interface texte interactive [31].
- ***Qemu :*** est un émulateur et une machine de virtualisation qui nous permet de courir à un système d'exploitation complet juste en tant que autre tâche sur votre ordinateur de bureau. Il peut être très utile pour essayer différents logiciels d'exploitation, logiciel

d'essai, et le fonctionnement des applications qui ne fonctionneront pas sur la plate-forme indigène de notre ordinateur de bureau [w5].

- ***VirtualBox :*** est un logiciel de virtualisation de systèmes d'exploitation. En utilisant les ressources matérielles de l'ordinateur (système hôte), VirtualBox permet la création d'un ou de plusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation (systèmes invités).

  Les systèmes invités fonctionnent en même temps que le système hôte, mais seul ce dernier a accès directement au véritable matériel de l'ordinateur. Les systèmes invités exploitent du matériel générique, simulé par un " faux ordinateur " (machine virtuelle) créé par VirtualBox.

  VirtualBox permet de faire fonctionner plus d'un système d'exploitation en même temps en toute sécurité. En effet, les systèmes invités n'interagissent pas directement avec le système hôte, et n'interagissent pas entre eux. Le champ d'action des systèmes invités est confiné, limité à leur propre machine virtuelle [w6].

  Grâce à ces applications, GNS3 nous permet [w4] :

- Le design de topologies réseaux de haute qualité et complexes.
- Emulation de plusieurs plate-forme de routeurs Cisco IOS, ou encore IPS, PIX et firewalls ASA.
- Simulation de switches Ethernet, ATM et Frame Relay.
- Connexion de réseaux simulés au monde réel.
- Capture de paquets grâce à Wireshark.

4.1.4 La configuration de GNS3

1. GNS3 est téléchargeable depuis le site officiel www.gns3.net.
   Cliquer dans la rubrique Windows sur GNS3 v0.8.3.1 all-in-one.exe et installer tous les composants.
2. Une fois le logiciel téléchargé et installé. Lors du lancement du logiciel une fenêtre apparait au milieu(figure 4.1), c'est pour la création d'un nouveau projet. Pour cela il faut spécifier dans l'onglet Nom de projet le chemin où sauvegarder le projet et son nom ensuit coché les deux cases.

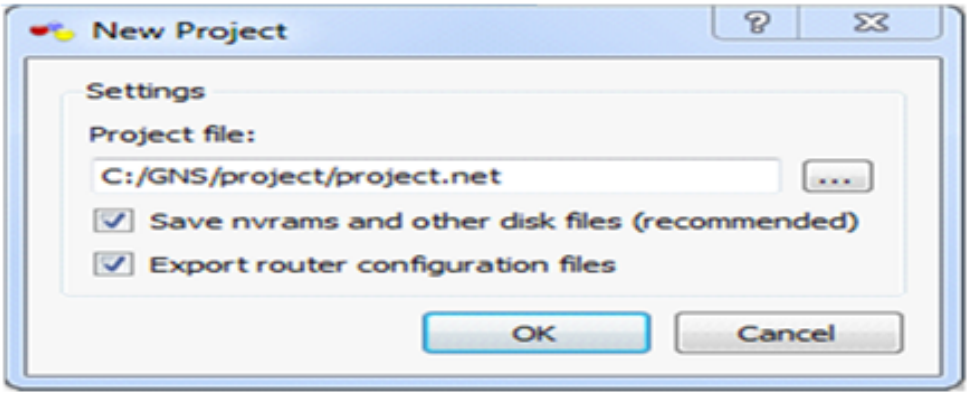


FIGURE 4.1 – Création d'un nouveau projet sous GNS3

Une fois enregistré, nous arrivons sur l'espace de travail de GNS3 qui est divisé en trois parties, la partie gauche affiche la liste des équipements matériels disponibles que nous pouvons ajouter dans notre topologie, la partie droite affiche la liste des éléments actifs et au milieu c'est l'espace de travail(figure 4.2).

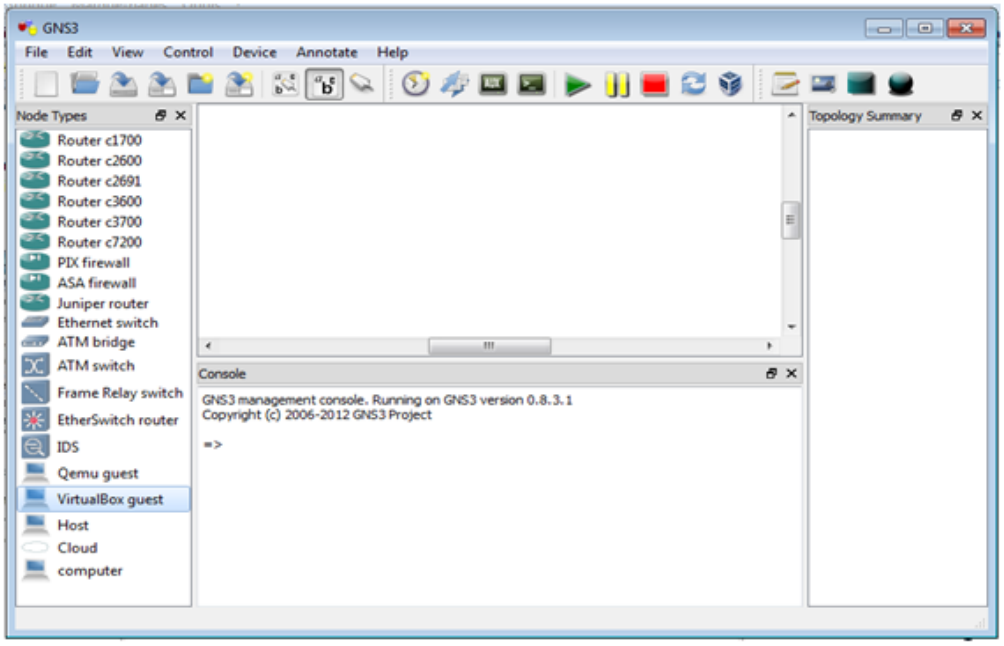


FIGURE 4.2 – Espace de travail de GNS3

3. Pour commencer à travailler avec GNS3, nous devons avoir l'IOS image de Cisco, il faut donc télécharger les IOS (est le système d'exploitation des routeurs Cisco) dont nous allons se servir. Une fois effectué, nous allons renseigner pour chaque

modèle de routeur que nous voulons utiliser, le chemin vers l'image IOS [1].

4. Pour ajouter l'IOS (OS Cisco) à la plate forme adéquate :
   Aller sur le menu Edit, IOS Images and Hypervisors. Cliquer sur image file, et sélectionner l'une des IOS précédemment télécharger, puis choisir la plate forme et le modèle du routeur adéquat puis cliquer sur Save (figure 4.3).

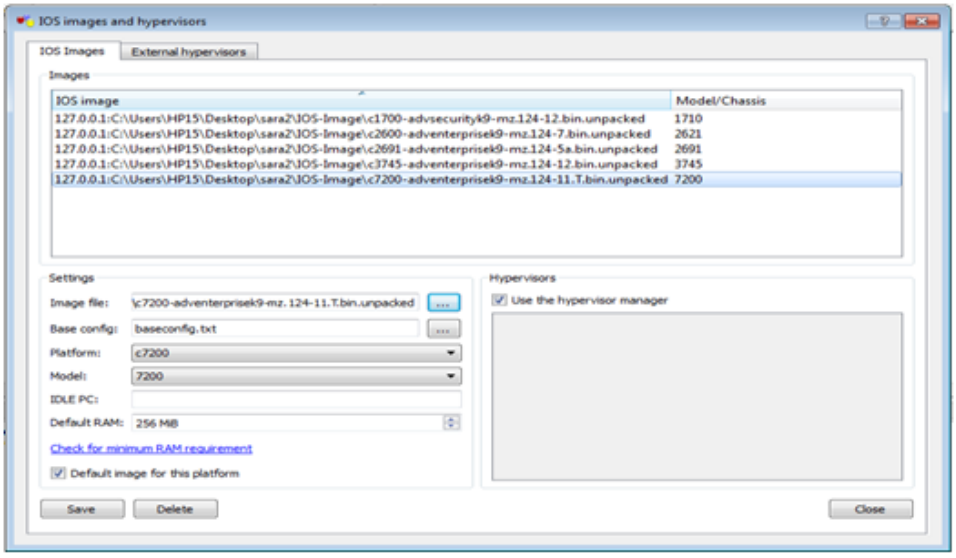


FIGURE 4.3 – Ajout des IOS

Après avoir ajouté l'IOS, nous pouvons utiliser un routeur, il suffit de faire un glisser-déposer à l'un des routeurs de la liste gauche et de le déposer dans la partie centrale de GNS3. Pour le démarrer clic droit sur le routeur et Start, et pour avoir accès a la console, clic droit et console.

5. Pour ajouter une machine virtuelle dans notre architecture, il nous faut d'abords préalablement installer Virtualbox et avoir déjà configuré au moins une machine virtuelle (voir plus de détail dans l'annexe B).

6. Pour intégrer la machine virtuelle dans GNS3, il faut d'abord l'importer comme suit : Aller dans Edit, Preferences, Virtualbox, VirtualboxGuest, RefreshVM List, puis donner un nom à la machine et dans le menu VM list sélectionner la machine à importer en suite sélectionner le numéro de la carte réseau laquelle elle va utiliser

1. Document officiel de l'IDWG : http ://www.ietf.org/html.charters/idwg-charter.html

(Number of NICs) pour se connecter. Coucher les deux cases Enable console support et Enable console server (for remote access), en fin Save, Apply, OK (figure 4.4).

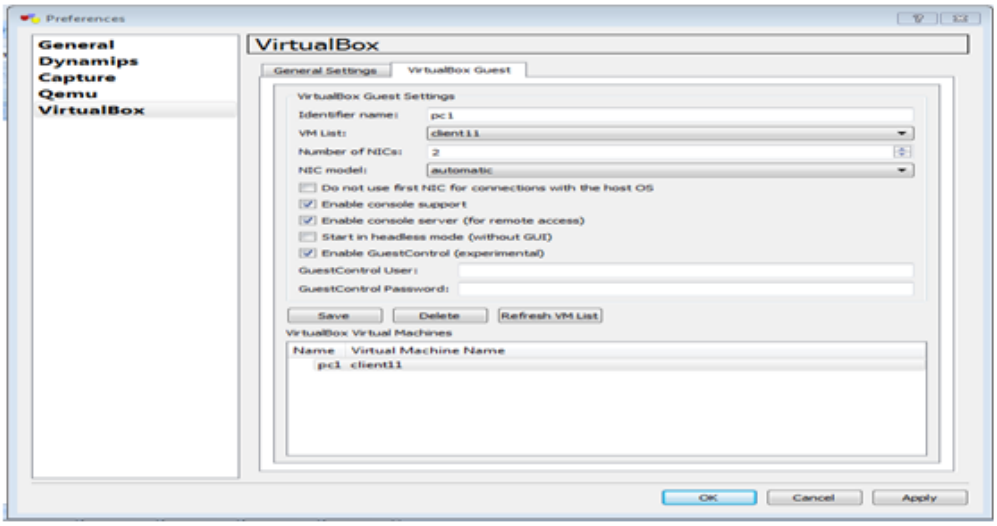


FIGURE 4.4 – L'ajout d'une machine virtuelle

Maintenant un glisser-déposer de la machine sur l'interface de travail nous permet de l'utiliser et pour la configurer un clic droit sur la machine permet d'afficher le menu contextuel de configuration.

4.2 Mise en œuvre

A l'issue de la mise en œuvre, nous serons en mesure d'effectuer trois tâches essentielles qui consistent en premier lieu à la configuration des routeurs, en deuxième lieu la configuration et l'initiation de l'IDS et en troisième lieu l'intégration de l'IDS dans GNS3, mais avant d'entamer la configuration nous devons installer notre réseau local de l'entreprise NAFTAL branche GPL de Béjaia sur GNS3.

Pour les besoins de la simulation et pour des raisons de manque de certains dispositifs, nous avons choisi de remplacer les switchs par des switchs de niveau trois avec un IOS routeur pour pouvoir les configurer en y créant des VLANs. Nous avons obtenus la topologie suivante :

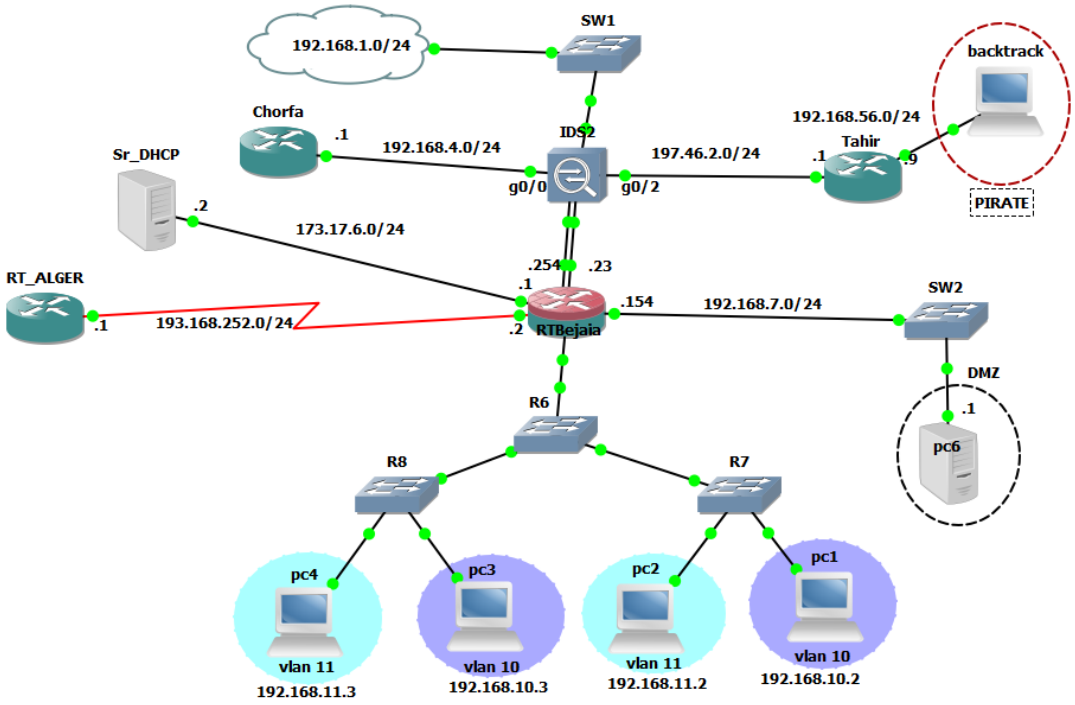


FIGURE 4.5 – la topologie du réseau local NAFTAL GPL-Béjaia sous GNS3

4.2.1 La politique de sécurité

Pour bien mener notre projet, il est nécessaire de déterminer une politique de sécurité qui est la suivante :

- Le serveur DHCP est autorisé à attribuer les adresses IP à tous les VLANs du réseau sauf celui des serveurs qui ont des adresses statiques.
- L'accès à tout les sous réseaux est réservé seulement aux administrateurs réseau.
- Aucun des utilisateurs autres que les administrateurs peuvent accéder au Switch.
- L'administrateur réseau peut accéder au routeur à n'importe quelle machine.
- L'IDS est configuré selon quelques règles définies pour le contrôle de la circulation du trafic provenant de l'Internet en générant des alertes selon le type du trafic détecté :

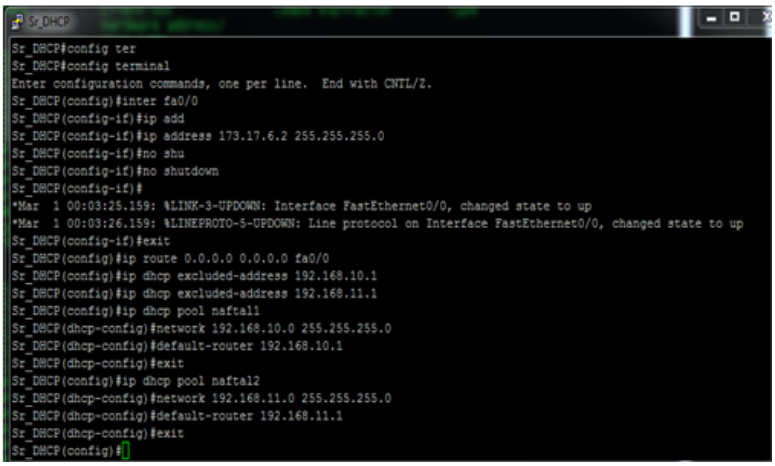
– La circulation d'un trafic ICMP-ECHO-Request.
– La circulation trafic ICMP-ECHO-Reply.

Pour réaliser cette politique, nous suivons ces étapes :

4.2.2 La configuration des routeurs

- ***La configuration du serveur DHCP***

Pour attribuer les adresses IP aux machines d'une manière dynamique, nous avons configuré serveur DHCP comme illustrer dans cette figure :



- ***La configuration de routeur RTBejaia***

Nous avons configuré les adresses IP des interfaces des routeurs pour la connectivité des réseaux, nous prenons comme exemple le RTBejaia :

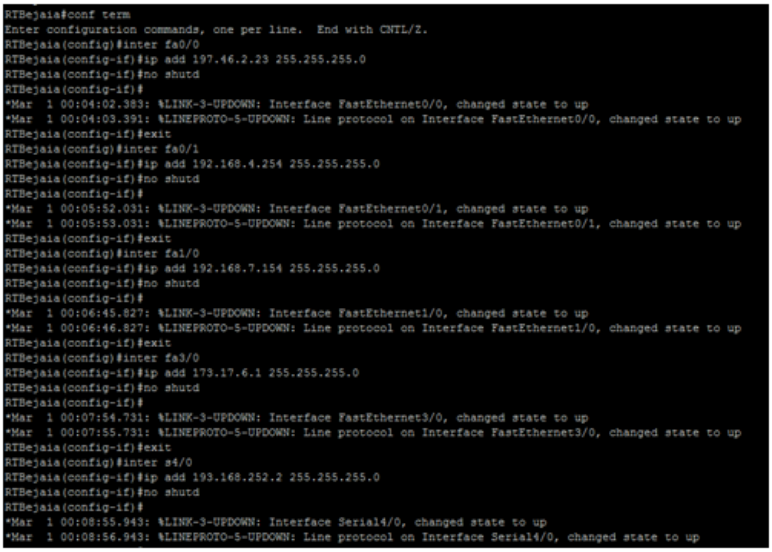


FIGURE 4.6 – Configuration des interfaces du routeur RTBejaia

Et nous avons activé le protocole rip sur ce routeur comme suit :

```
RTBejaia(config)#router rip
RTBejaia(config-router)#version 2
RTBejaia(config-router)#network 197.46.2.0
RTBejaia(config-router)#network 192.168.4.0
RTBejaia(config-router)#network 192.168.7.0
RTBejaia(config-router)#network 173.17.6.0
RTBejaia(config-router)#network 193.168.252.0
RTBejaia(config-router)#exit
RTBejaia(config)#do wr
Building configuration...
[OK]
```

FIGURE 4.7 – Activation du protocole rip

- ***Configuration du routage inter-vlan***

Au niveau de l'interface FastEthernet 2/0 du routeur RTBejaia, nous avons créé et configuré des sous interfaces pour effectuer le routage inter-vlan :

```
RTBejaia(config)#inter f2/0
RTBejaia(config-if)#no ip add
RTBejaia(config-if)#no shut
RTBejaia(config-if)#
*Mar  1 00:16:09.591: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
*Mar  1 00:16:10.591: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
RTBejaia(config-if)#exit
RTBejaia(config)#inter f2/0.10
RTBejaia(config-subif)#encapsulation dot1q 10
RTBejaia(config-subif)#ip add 192.168.10.1 255.255.255.0
RTBejaia(config-subif)#no shut
RTBejaia(config-subif)# exit
RTBejaia(config)#inter f2/0.11
RTBejaia(config-subif)#encapsulation dot1q 11
RTBejaia(config-subif)#ip add 192.168.11.1 255.255.255.0
RTBejaia(config-subif)#no shut
RTBejaia(config-subif)#exit
RTBejaia(config)#inter f2/0.10
RTBejaia(config-subif)#ip helper-address 173.17.6.2
RTBejaia(config-subif)#exit
RTBejaia(config)#inter f2/0.11
RTBejaia(config-subif)#ip helper-address 173.17.6.2
RTBejaia(config-subif)#exit
RTBejaia(config)#do wr
```

FIGURE 4.8 – Configuration des sous interfaces de f2/0

4.2.3 La configuration de l'IDS

À ce niveau nous allons montrer comment émuler un IDS avec Qemu et GNS3. D'abord il faut avoir l'image IOS de l'IPS "IPS-K9-cd-1.1-a-6.0-5-E3.iso" et la copie dans le fichier d'installation de GNS3 et suivre ces étapes :

- ***Étape 1 :*** Créer les deux images disque (hda et hdb) :

  Dans le menu démarrer, ouvrir une Invite de commandes (cmd) et accéder au fichier d'installation de GNS3 comme suit :

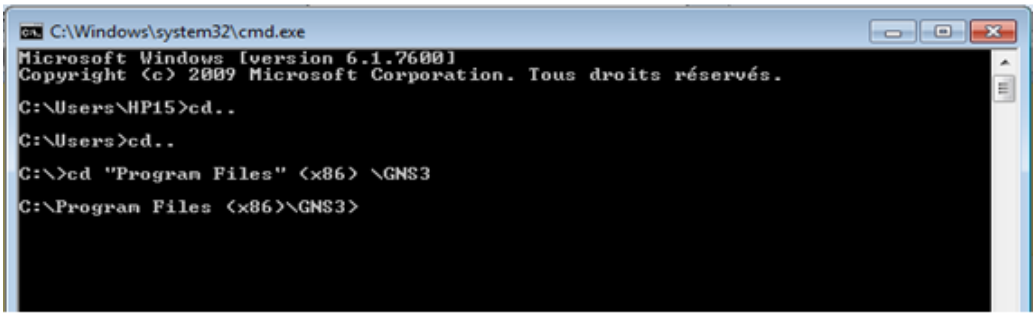


FIGURE 4.9 – Les commandes d'accès au fichier de GNS3

Puis saisir les commandes suivantes : qemu-img.exe create ipsdisk1.img 512M et qemu-img.exe create ipsdisk2.img 4000M.

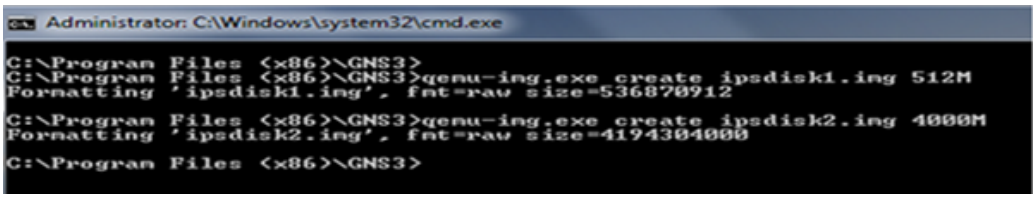


FIGURE 4.10 – Les commandes de création des deux disques de l'IDS

- ***Étape 2 :*** Charger une image IDS en utilisant qemu.

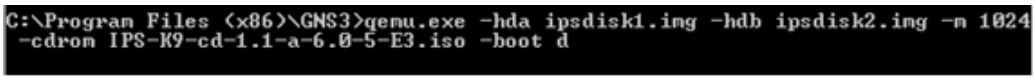


FIGURE 4.11 – Processus de récupération d'IDS image

Quand qemu bottes, appuyer sur k pour lancer le processus de ré-imagerie (récupération de l'image).
Quand le ré-imagerie est fait, qemu se plaindre dans l'écran du BIOS des problèmes de démarrage. Quitter le processus qemu (en utilisant Ctrl-C).

- ***Étape 3 :*** démarrage à partir des disques ré-imagé Cette étape consiste à démarrer à partir du disque.

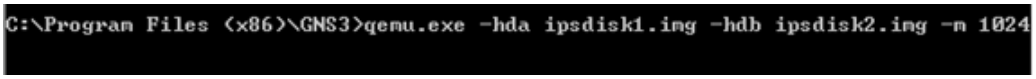


FIGURE 4.12 – Démarrage à partir du disque ré-imagé

Lorsque le système démarre, modifier l'entrée de démarrage GRUB (GRandUnified Bootloader) pour s'assurer que le système commence à niveau d'exécution en mode promiscuité [2].
Dans le menu GRUB, appuyez sur "e" pour éditer la première entrée de démarrage.
Dans le menu suivant, sélectionner la deuxième ligne (qui commence par "kernel") et appuyer sur "e" à nouveau.
Changez l'option init = / loadrc à init = 1, puis entrez suivi par "b" pour démarrer.

Le logiciel IDS démarre maintenant au niveau d'exécution 1. Lorsqu'on est invité, appuyer sur Enter et émettre les commandes suivantes :
/ loadrc

2. Promiscuous mode (traduit mode promiscuité), se réfère à une configuration de la carte réseau, qui permet à celle-ci daccepter tous les paquets quelle reçoit, même si ceux-ci ne lui sont pas adressés. Ce mode est une fonctionnalité généralement utilisée pour écouter le trafic réseau

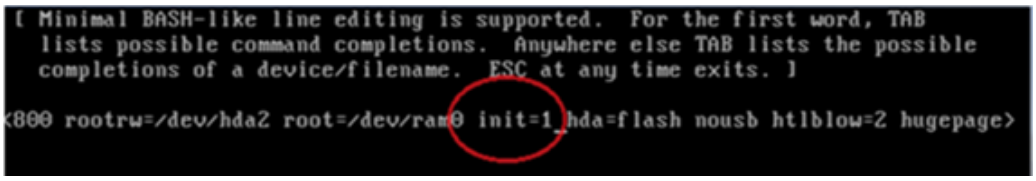


FIGURE 4.13 – Le menu GRUB d'initialisation de l'IDS

cd /etc/ init.d

./rc.init

Taper la commande ls -l pour visualiser la configuration.

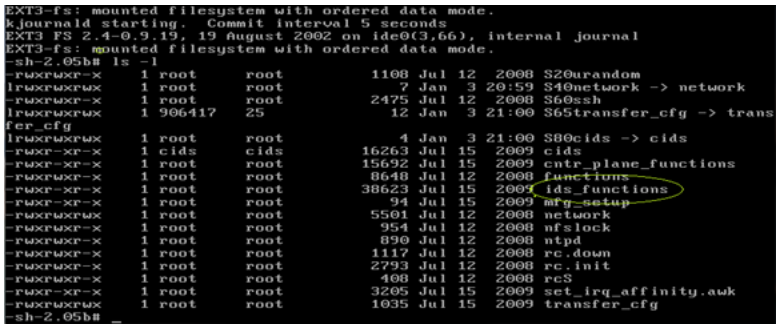


FIGURE 4.14 – La visualisation de la configuration

Taper les commandes de configuration des fonctionnalités d'IDS qui sont :

cp ids functions ids functions.orig

vi ids functions

Dans le fichier résultant, saisir / 845 et il va passer à la section qui ressemble à ceci :

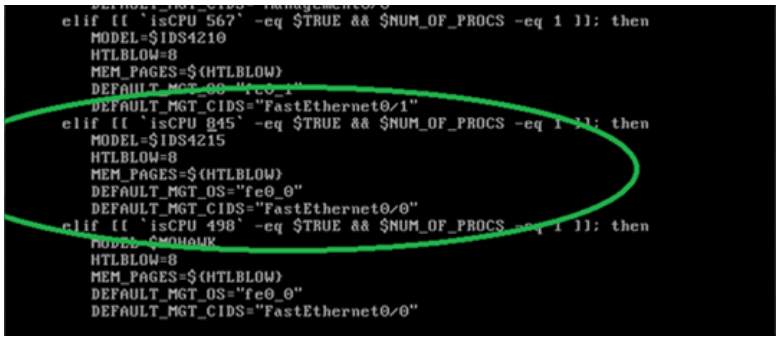


FIGURE 4.15 – La section du fichier 845

- ***Étape 4 :*** attribuer les cartes émulées de NIC aux interfaces d'IDS : Maintenant, régler le processus de cartographie des cartes réseau émulées pour les interfaces IDS. Exécuter les commandes suivantes : Avancer à la section qui traite de

FIGURE 4.16 – Les commandes de configuration d'interfaces IDS

la sonde 4235. Nous avons seulement besoin d'apporter des modifications à [models/IDS-4250/interfaces/X].

Nous allons configurer le capteur avec cinq interfaces, une interface Management 0/0 pour le commandement et le contrôle et quatre interfaces GigabitEthernet pour la détection.Le résultat devrait ressembler à ce qui suit :

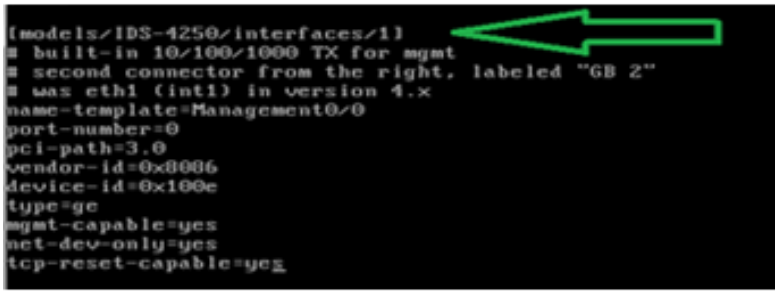


FIGURE 4.17 – La configuration de l'interface Management

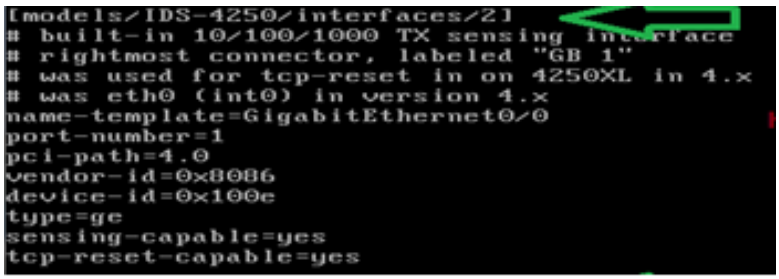


FIGURE 4.18 – La configuration de l'interface GigabitEthernet0/0

FIGURE 4.19 – La configuration de l'interface GigabitEthernet0/1

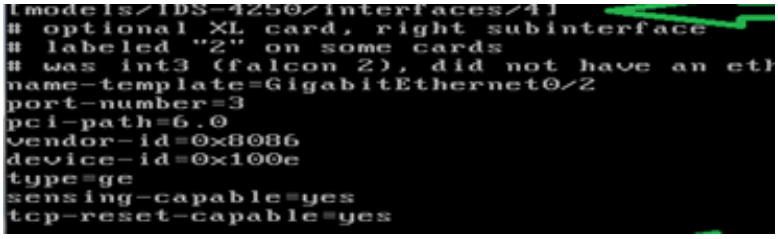


FIGURE 4.20 – La configuration de l'interface GigabitEthernet0/2

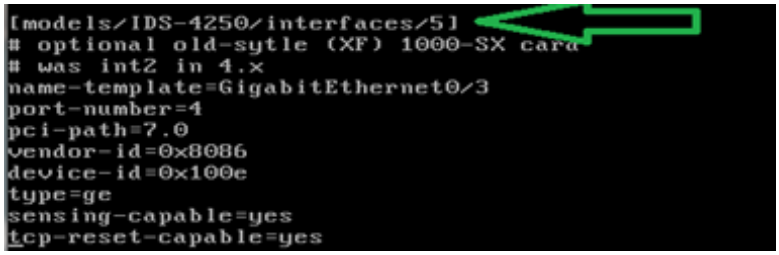


FIGURE 4.21 – La configuration de l'interface GigabitEthernet0/3

Enregistrez les modifications et sortir de vi. Les modifications du système sont faites, maintenant recharger l'appareil.

Appareil se recharge deux fois, puis le sensor IDS demande un login et un mot de passe, les deux sont par défaut cisco.

4.2.3.1 IDS dans GNS3

Maintenant l'IDS est prêt à être intégré dans GNS3. Nous allons le configurer comme suit : Aller dans Edit -Preferences -Qemu -IDS et apporter ces modifications :

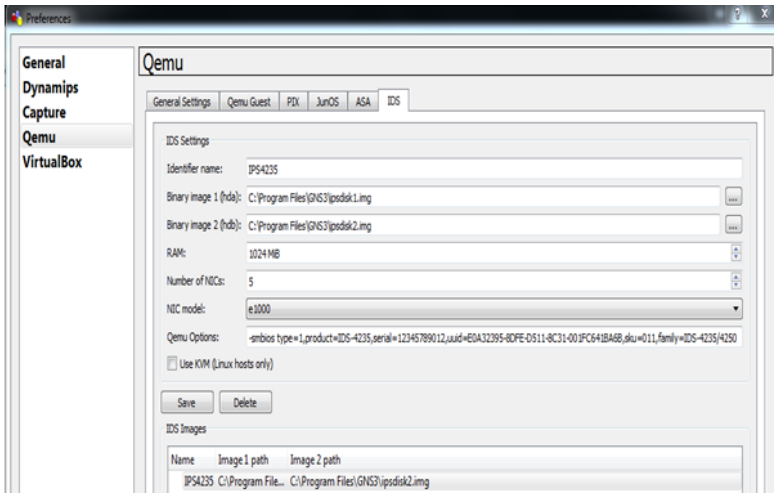


FIGURE 4.22 – Configuration de l'IDS sous GNS3

Démarrer l'IDS à partir de GNS3. Un accès CLI et aussi un accès via IDM (IPS Device Manager) est possible, comme indiqué.

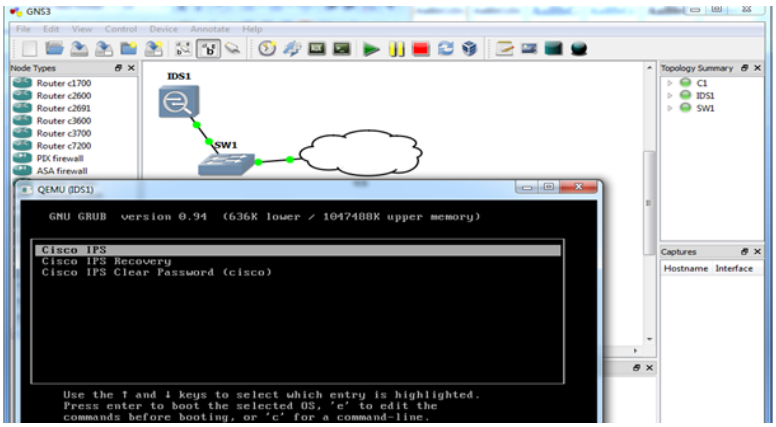


FIGURE 4.23 – Le démarrage de l'IDS sous GNS3

- ***Initialisation du capteur via CLI***

  1. Saisir le Sensor login et Password qui sont par défaut cisco.
  2. La CLI exige le changement de mot de passe par défaut.
  3. Saisir setup puis Enter pour afficher le dialogue de configuration par défaut du capteur,taper sur Enter jusqu'à arriver à la ligne où s'affiche la question suivante : Continue with configuration dialog ?[yes] : , taper Enter pour pouvoir effectuer les configurations souhaitées et changer la configuration par défaut.
  4. Spécifier le nom du capteur :
     Enter hostname [senssor] : IDS et taper sur Enter.
  5. Changer l'adresse IP et la passerelle par défaut :
     Enter IP interface[192.168.1.2/24,192.168.1.1] :192.168.1.23/24,192.168.1.99
  6. Continuer à taper sur Enter jusqu'au linge où s'affiche modifier la liste d'accès et saisir yes après une sous-ligne s'affiche permit pour permettre le réseau où appartient l'IDS afin de pouvoir y accéder via IDM.
     Modify current access list [no] : yes Permit : 192.168.1.0/24
     Permit : taper Enter
  7. Continuer à taper sur Enter jusqu'à ce que un message de demande de sauvegarde s'affiche, enregistrer et quitter.

  Nous pouvons continuer a utilisé la configuration avancée dans la CLI ou nous pouvons utiliser l'assistant de démarrage IDM.
  Pour notre projet nous avons choisi la configuration par l'interface graphique IDM.

- ***La configuration via l'interface graphique IDM***

  L'IDM (IPS Device Manager) Cisco est une interface web basé sur Java qui permet de configurer et de manipuler le fonctionnement des capteurs réseau. Chaque Appliance IPS fonctionnant sur le réseau possède son propre serveur Web qui permet d'accéder à la demande d'IDM sur le capteur. Le serveur Web utilise Transport Layer Security (TLS) pour crypter le trafic vers et à partir du capteur pour empêcher un attaquant d'afficher le trafic de gestion sensible.

Le serveur Web est également durci pour réduire la capacité d'un attaquant de perturber ou compromettre son fonctionnement [w6].

L'exigence majeure de l'IDM est un navigateur web et avoir suffisamment de mémoire (minimum 256Mo). Pour les besoins de configuration il est d'abords recommandé d'installer la version Java 1.5 et de désinstaller la version 1.7 si elle existe.

Afin de pouvoir faire la configuration via IDM, nous avons suivi ces étapes :

1. Ouvrir un navigateur web et saisir l'adresse IP de la sonde sous forme d'une URL : https ://sensor,ip address (https ://192.168.1.23).
2. Une page de certification s'affiche, cliquer sur 'Pour suivre avec ce site Web (non recommandé).
3. Pour lancer l'IDM et accéder à son interface graphique, cliquez sur Run IDM (Exécuter IDM). La boîte de message de chargement JAVA apparaît, puis un avertissement (boîte de dialogue de sécurité) s'affiche.

FIGURE 4.24 – Interface d'accueil de l'IDM

4. Une fenêtre d'authentification de l'IDM 'Cisco IDM Launcher' s'affiche, entrez le nom d'utilisateur et mot de passe, puis cliquez sur OK. L'IDM commence à se charger.

FIGURE 4.25 – Fenêtre d'authentification 'Cisco IDM Luncher'

5. La fenêtre principale de l'IDM apparaît. Elle affiche les informations essentiel de l'appareil telles que le nom d'hôte, l'adresse IP, la version et le modèle.

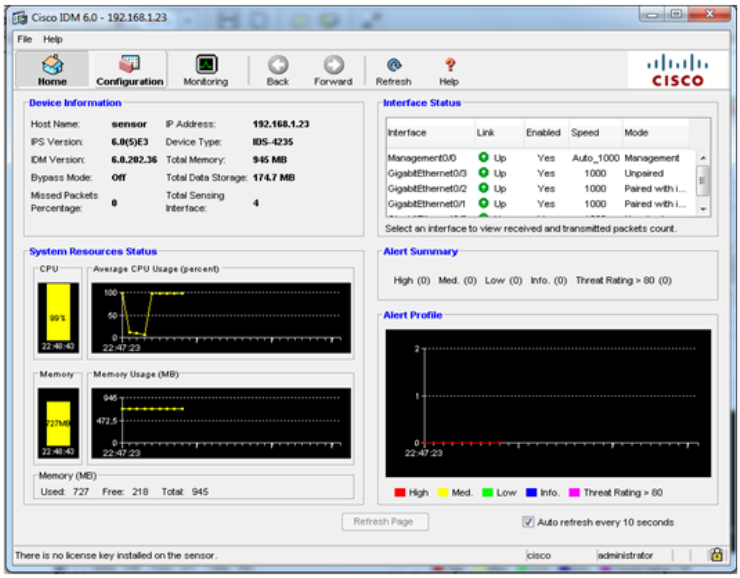


FIGURE 4.26 – Interface graphique IDM

Pour configurer le capteur, choisisser l'icône Configuration et passer par les menus dans le volet de gauche.

Ces menus sont répartis dans les catégories opérationnelles suivantes :

1. ***Configuration du capteur (Sensor Setup)***

Le capteur peut recevoir des données d'un ou plusieurs flux de données surveillées qui peuvent être soit des ports d'interface physique ou des ports d'interface virtuelle. Le capteur VS0 est le capteur par défaut à qui nous avons appliqué une politique de configuration pour tous les flux de données surveillées.

Nous trouvons dans la configuration du capteur les éléments suivant :

- **Réseau (Network) :** permet de spécifier le réseau et les paramètres de communication pour le capteur tel que le nom de l'hôte, l'adresse IP, le masque réseau et la route par défaut.
- **Hôtes permise (Allowed Hosts) :** permet de spécifier les hôtes ou les réseaux qui ont l'autorisation pour accéder au capteur via son interface management. Nous avons ajouté l'adresse IP de l'administrateur qui est 192.168.10.3 avec son masque réseau 255.255.255.0 comme montrer dans la figure suivante :

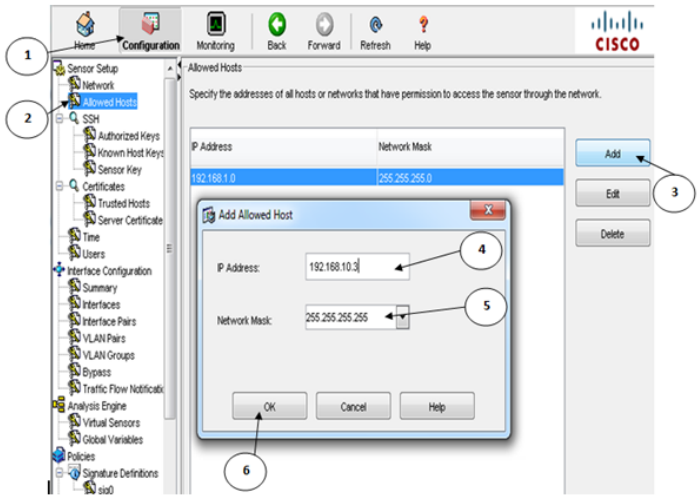


FIGURE 4.27 – adresse IP de l'administrateur

Cliquer sur Apply pour enregistrer.

- **Utilisateurs (Users) :** IDM autorise des utilisateurs multiples à se connecter à la fois. Nous pouvons modifier seulement un compte de l'utilisateur à la fois.

Chaque utilisateur est associé avec un rôle qui contrôle ce qui cet utilisateur peut et ne peut pas modifier.

Il y a quatre rôles de l'utilisateur : Viewers, Operators, Administrators et Service.

L'utilisateur par défaut est cisco avec des privilèges administrateur. Nous ajoutons un utilisateur avec un rôle d'administrateur comme montrer ci-dessus :

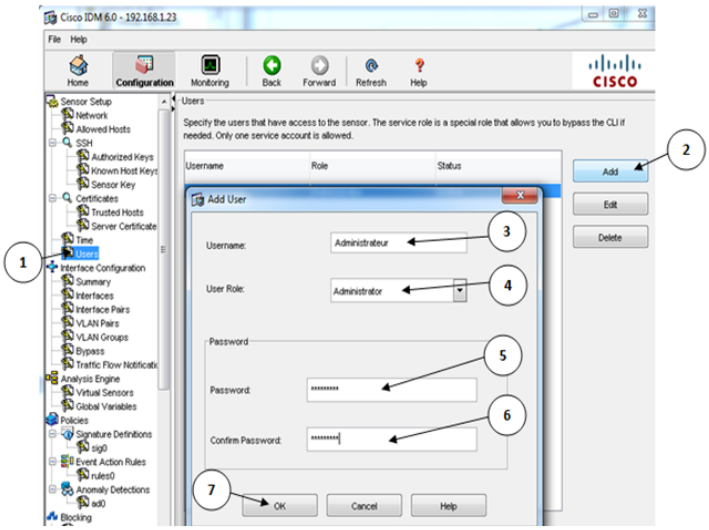


FIGURE 4.28 – Ajout d'un utilisateur

Cliquer sur Apply pour enregistrer.

2. ***Configuration des interfaces (Interface configuration) :*** Le capteur détecte automatiquement les modules d'interfaces qui sont installés à chaque fois qu'il est allumé et les interfaces doivent d'abord être activées pour la surveillance du trafic. Nous trouvons dans la configuration des interfaces les éléments suivants :

- **Interface (Interfaces) :** permet d'inscrire les interfaces existantes sur le capteur et leurs cadres associés.
- **Paires d'interface (Interface Pairs) :** permet de créer des paires d'interface qui autorisent le capteur de surveiller le trafic réseau en utilisant des modes de fonctionnement en ligne.

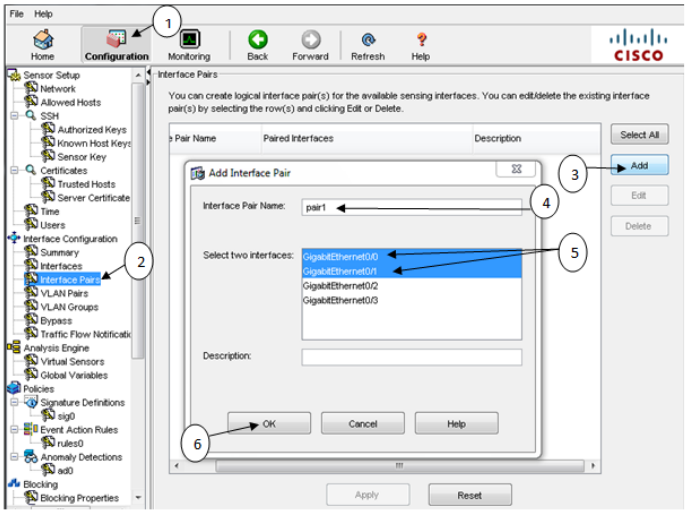


FIGURE 4.29 – Ajout de la première paire d'interface en ligne

Cliquer sur Apply pour enregistrer. Idem pour la deuxième paire d'interface en ligne.

- **Déviation (Bypass) :** permet d'assurer que les paquets continuent à circuler à travers la sonde quand les processus de contrôle de la sonde sont arrêtés temporairement. Il y a trois modes : sur (On), fermé (Off), et automatique (Auto), choisir le mode "off (Always inspect inline traffic)" et cliquer sur Apply pour enregistrer la configuration.

3. ***Le moteur d'analyse (Analysis Engine) :*** permet d'exécuter une analyse de paquet et de détection d'alerte. Il surveille la circulation du trafic qui traverse des interfaces spécifiées.

   Dans le moteur d'analyse, nous créons des capteurs virtuels.

- **Capteurs virtuels (Virtuel Sensors) :** dans la boite du dialogue de capteur virtuel, nous trouvons seulement les interfaces ou les paires d'interfaces qui sont disponible à être assignées à ce capteur.

  Pour éviter les conflits ou les chevauchements dans les affectations et pour que aucun paquet ne soit traité par plus d'un capteur virtuel, nous attribuons une interface à un capteur virtuel spécifique. Nous allons attribuer les deux paires d'interfaces crées au capteur virtuel Vs0 comme suit :

  Aller dans Configuration, Virtual Sensors et dans la fenêtre qui s'affiche cliquer sur Edit une autre fenêtre s'affiche cliquer sur Assign puis sur Ok.

Cliquer sur Apply pour enregistrer la configuration.

4. ***Définition de signature (Signature Definitions) :*** permet de définir l'ensemble de règles qui utilise le capteur pour détecter l'activité intrusive. Pour cela le capteur analyse le trafic réseau, il recherche les correspondances aux signatures qu'il a configurées.

   La politique de la définition de la signature par défaut est appelée sig0. Dans la définition de signature sig0, nous trouvons plusieurs options parmi eux l'option suivante :

- Configuration de signature (Signature Configuration) : permet de voir toutes Les signatures disponibles et leurs propriétés, de les activer ou désactiver, d'ajouter de nouvelles signatures et de modifier les propriétés des signatures existantes. Il est possible de définir les actions à prendre en cas de détection d'attaque. Nous allons activer les deux signatures 2000 et 2004 qui permettent la fonction de ping comme montrer ci-dessous :

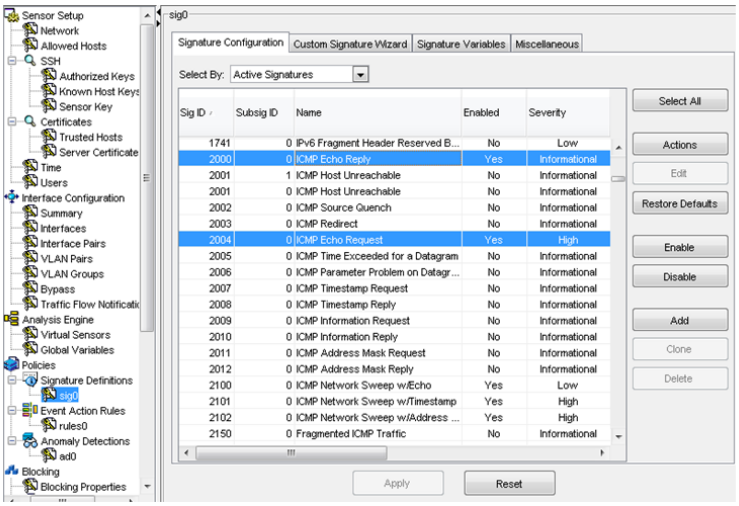


FIGURE 4.30 – activation de signatures 2000 et 2004

5. ***Règles d'action d'événement (Event Action Rules) :*** L'option du rules0 (par défaut) définit comment le capteur traite des événements spécifiques quand elles sont détectées sur le réseau. Il contient les fonctions suivantes :

- Estimation de la valeur de la cible (Target Value Rating) : est l'un des facteurs qui permet de calculer les risques d'estimation évaluent pour chaque

alerte. nous pouvons assigner une estimation atout pour un réseau spécifique. L'estimation de la valeur de la cible peut être une des valeurs suivantes : Aucune valeur, Faible, Medium, Elevé ou Mission critique.

Nous définissons les adresses IP cible de notre réseau en mettant l'estimation à élevé (High).

- Filtres d'action d'événement (Event Action Filters) : permet de définir des filtres d'action d'événement qui sont traités comme une liste rangée. Ces filtres empêchent le capteur d'exécuter certaines actions à des événements spécifiques.

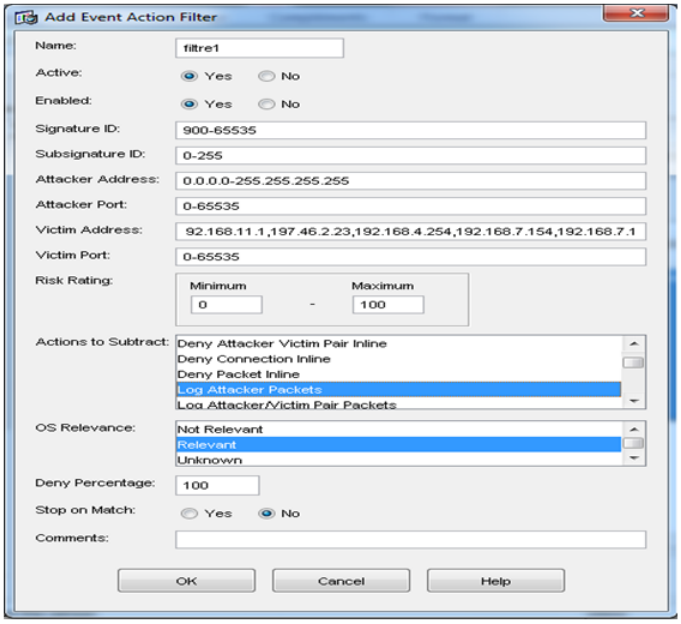


FIGURE 4.31 – Ajout d'un filtre d'actions d'événements

6. ***Blocage (Blocking) :*** permet de bloquer le trafic du système intrusif lors de déclenchement d'une signature. La catégorie de blocage présente les options de configuration suivantes :

- Propriétés de blocage : permet régler le capteur pour identifier les hôtes et les réseaux qui ne devraient jamais être bloqués. Régler correctement les signatures réglées correctement réduit le nombre de faux positifs.

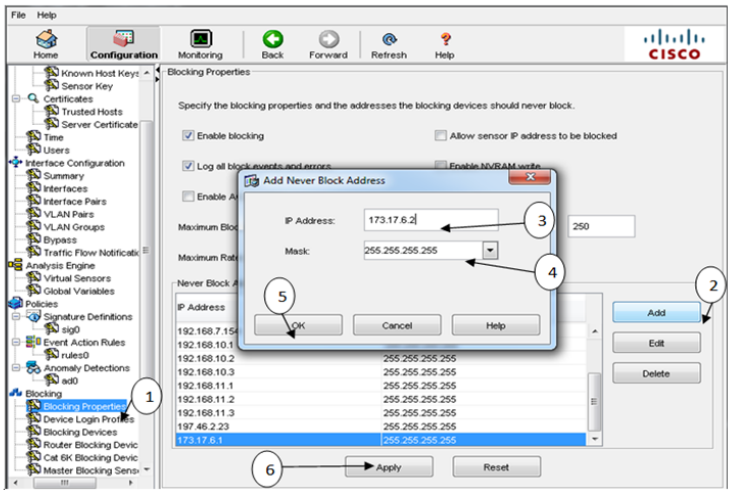


FIGURE 4.32 – Propriétés de blocage

En plus de la proprité de configuration, IDM offre la possibilité de surveiller l'état et le fonctionnement du capteur.

4.3 Tests

Nous avons traité deux tests :

4.3.1 Scénario 1

Dans le menu Configuration, aller sur Sig0, Actions, nous allons choisir l'option 'produce Alert' pour que l'IDS génère une alerte dans le cas de détection d'un trafic malveillant.

4.3.2 Scénario 2

Dans le menu Configuration, aller sur Sig0, Actions, nous allons choisir l'option 'Deny Attacker Inline' pour que l'IDS refuse un trafic dans le cas qu'il le détecte malveillant.

Nous allons effectuer des tests et voir le résultat pour chaque un de ces deux scénarios :

- **La fonction ping**

La fonction ping se base sur les deux requêtes ICMP Echo Reply et ICMP Echo Request que nous configurer avant.

- **Scénario 1 :** Faire un ping de la machine pirate vers la machine Pc1 du réseau local.

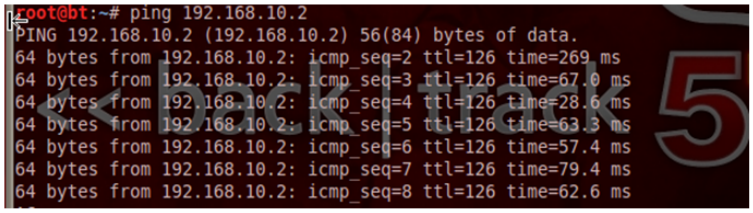
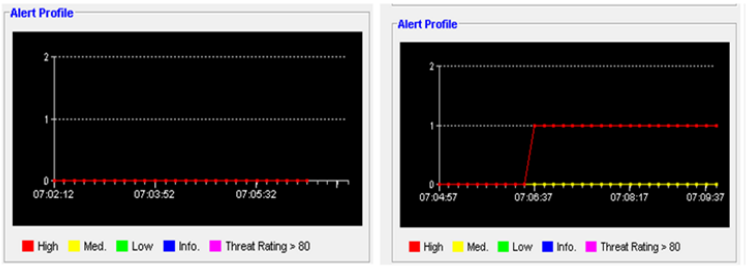


FIGURE 4.33 – Résultat de ping

Sur le profil d'alerte qui s'affiche sur la page d'accueil, nous observons le changement de son état :



L'état de la courbe avant l'attaque. L'état de la courbe après l'attaque.

FIGURE 4.34 – Changement de l'état de la courbe

L'axe des Y représente l'estampille de l'événement et l'axe des X le nombre d'attaquant.

Pour voir le journal d'événements de l'IDS, aller sur Monitoring, Events. Sur la fenêtre qui apparait modifier les paramètres d'affichage puis cliquer sur View.

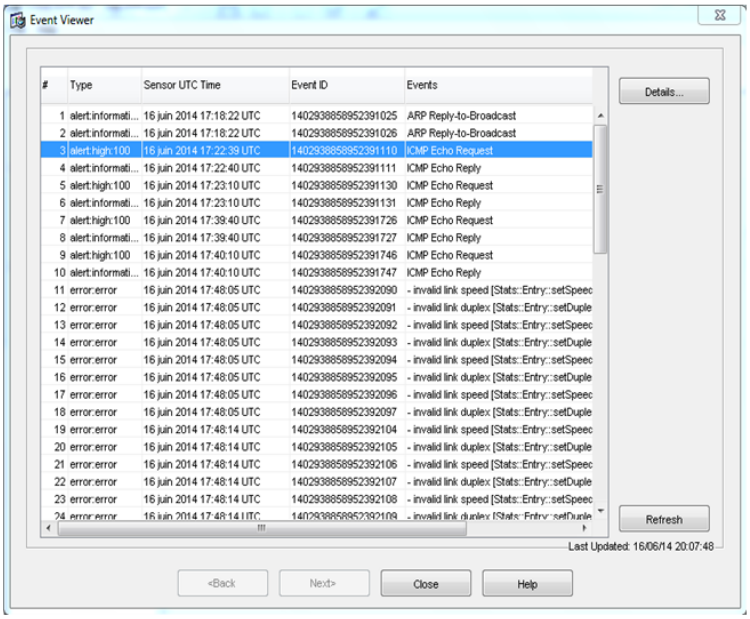


FIGURE 4.35 – Affichage d'une alerte

Pour voir les détailles de l'alert, cliqué sur Détails.

- **Scénario 2 :** faire un ping de la machine pirate vers la machine Pc1 du réseau local. L'IDS bloc ce pirate et le met dans la liste des attaquants bloqués, donc il interdit le passage du trafic dans les deux sens, comme montrer ci-dessous :

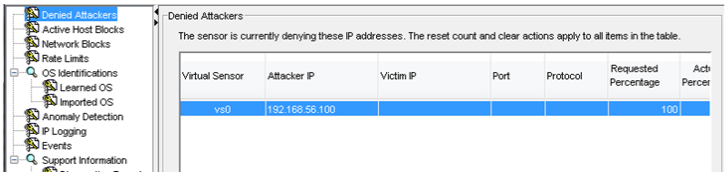


FIGURE 4.36 – Blocage du pirate par l'IDS.

Dans ce scénarios, pour toutes signatures interdites l'IDS ne laisse pas passer le trafic contenant un match interdit par cette signature et bloc l'´emetteur extérieure.

conclusion

Au long de ce chapitre nous avons opté à la configuration et la mise en uvre de notre solution qui est basée sur IDS et nous avons présenté l'environnement et les outils de travail que nous avons utilisé.

Le simulateur GNS3 nous a permis à partir de son interface graphique de concevoir et simuler notre topologie. Après la configuration nous avons montré quelques tests afin de vérifier le bon fonctionnement de l'IDS.

Conclusion Générale

La sécurisation d'un réseau est une étape délicate qui permet sa protection contre les risques les plus courants.
Sur Internet, les pirates emploient de plus en plus de stratégies pour dissimuler leurs caractères intrusifs.

Une gamme complète de solutions telles que les antivirus, scanneurs de failles et firewall permet d'obtenir une sécurité presque convenable face aux attaques les plus courantes. Ces dernières sont d'ailleurs en évolution quotidienne et de nombreuses failles sont découvertes et exploitées chaque jour.
Il faut alors prendre au sérieux les risques provenant du réseau et analyser régulièrement ses flux, afin d'y déceler les anomalies, pouvant prouver une intrusion. Cette tâche serait aussi rebutante que fastidieuse si les IDS n'avaient pas été développés.

Nous avons suivi dans le cadre de notre PFE plusieurs étapes afin de parvenir à notre but, celui de renforcer la sécurité au sein du réseau LAN de l'entreprise à l'aide de système de détection d'intrusions.

Dans notre mémoire nous avons opté à la simulation et la mise en œuvre d'un système de détection d'intrusions au niveau de l'architecture réseau de Naftal. Tout d'abords nous avons proposé une implémentation de cette architecture en s'appuyant sur le simulateur de réseau graphique GNS3 puis configurer les différents matériels nécessaires a la connectivité du réseau (les routeurs les machines les serveurs et la création des VLANs) puis placer l'IDS (c'est l'IDS Cisco Appliance, NIDS) dans le point stratégie dans le réseau et le configurer pour surveiller le tra-

fic sortant et/ou entrant a l'intérieur et/ou a l'extérieur du réseau local et en fin, présenter les tests que nous avons mené et les résultats obtenus par ce dernier et sa performance en termes de détection d'intrusions par une évaluation de sa fiabilité.

En perspective, il serait intéressant d'améliorer les performances de notre IDS à travers l'approche hybride qui consiste en la sérialisation d'un IDS comportementale suivi d'un IDS par signatures, l'IDS comportementale permet de filtrer les requetes normales et ainsi seules les requetes détectées comme anormales sont passées à l'IDS par signatures,de réduire le taux de faux positif en améliorant la qualité des tests. Plus ces taux sont bas, plus la solution est performante, coopérer les différents systèmes de détection d'intrusions pour une sécurité parfaite et complète. tester notre proposition et configurer sur des réels dans le réseau de Naftal.

Il faut bien signaler que ce projet est une excellente initiation a 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 une expérience enrichissante aussi bien sur le plan théorique que pratique.

Bibliographie

[1] Stéphane Natkin, les protocoles de sécurité d'internet, DUNOD science SUP,mai2002

[2] Géraldine Vache-Marconato, Evaluation quantitative de la sécurité informatique : approche par les vulnérabilitès, thèse doctorat,Université Toulouse, Mars 2010.

[3] Guy Pujjolle, Les réseaux, 6éme édition Eyrolles, 2008.

[4] Noudjoud KAHYA, Etude critique des méthodes d'optimisation pour la détection d'intrusion dans un système informatique, Mémoire de magistère en informatique, option : Réseau et Système de distribués, université ABDE RAHMANE MIRA de Bejaia, nouvembre 2005.

[5] K.DAHOUMANE, K.NAIT ATMANE, "Conception et Implémentation d'un système de Gestion de Certificats pour les Réseaux de Capteurs Sans Fil", Mémoire d'ingénieur à l'université de Bejaia 2011.

[6] Walid BAGGA, Policy-Based Cryptography : Theory and Applications, Ecole Nationale Supérieure des Télécommunications, 2006.

[7] Stéphane Lohier, Auréie Quidelleur, Le réseau Internet, des services aux infrastructures, Edition Dunod, Paris, 2010.

[8] Nicolas T. Courtois,"La sécurité des primitives cryptographiques basées sur des problèmes algèbriques multivariables :MQ, IP,Minrank, HFE",thèse de Doctorat de l'Université Paris 6, Soutenue le 25 Septembre 2001.

[9] Mohammed El-Sayed Gadelrab, Evaluation des systèmes de détection d'intrusion, Thèse doctorat, université Toulouse, délivré par l'université Toulouse

III-Paul Sabatier, 15 décembre 2008.

[10] Laurent Bloch Christophe Wolfhugel, Sécurité informatique, Principes et méthode à l'usage des DSI, RSSI et administrateurs, Eyrolles, 2 éme édition, 2009.

[11] Yves Deswarte, Ludovic Mé, Sécurité des réseaux et systèmes répartis, Eyrolles, 2002.

[12] Mohammed S. Gadelrab, Anas Abou El Kalam, and Yves Deswarte, Execution Patterns in Automatic Malware and Human-centric Attacks,NCA 2008 : Proceedings of the 2008 Seventh IEEE International Symposium on Network Computing and Applicaions vol. 29-36.

[13] TOUHAMI MECHRI, Approche algébrique pour la sécurité des réseaux informatique, Mémoire de Magister, Université Laval, Canada ,2007.

[14] Imad Bou Akl, Etude des protocoles et infrastructures de sécurité dans les réseaux, DEA d'Informatique, Université Paul Sabatier - I.R.I.T., 2006.

[15] M. Tran Van Tay, Le système de détection des intrusions et le système d'empêchement des intrusions (ZERO DAY), Rapport de stage de fin d'étude, institut de la francophonie pour l'informatique, université de Québec à Montréal, Février 2005.

[16] Eric BERTHOMIER, Formation Sécurité des Réseaux, Support Instructeur, 2005.

[17] Christophe WOLFHUGEL, Déploiement de VLAN 802.1Q/ISL dans un environnement hétérogène, France Telecom Oléane, 2000.

[18] Génaël VALET, Les LANs virtuels (VLANs), support de cours, Greta industriel des technologies avancées, Avril 2007.

[19] Laurent Bloch et Christophe Wolfhugel, " Sécurité Informatique : Principes et méthode ", Juin 2011.

[20] Gunadiz Safia, algorithme d'intellegence artificielle pour la classification d'attaques réseaux à partir de données TCP, Mémoire de magistère, université M'hamed BOUGARA de Boumerdes, 2011.

[21] HAMZA Lamia, Génération automatique de scénario d'attaques pour les systèmes de détection d'intrusions, Mémoire de magister, université Abderrahmane Mira de Béjaia, 2005.

[22] Hervé Debar, Marc Dacier et Andreas Wespi, " A Revised Taxonomy for Intrusion-Detection Systems - Annales des Télécommunications ", 55, n° 7-8, 2000.

[23] Madjid Ouharoun, " Modélisation de détection d'intrusion par des jeux probabilistes ", Mémoire de maitrise, Université du Québec Canada, 2010.

[24] LABED Ines, Proposition d'un système immunitaire artificiel pour la détection d'intrusion, Mémoire de magister en informatique option : information et computation, Université de MENTOURI de Constantine faculté des sciences de l'ingénieur, 2005-2006.

[25] Michaël AMAND, Mohamed NSIRI, Etude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire, Rapport de projet tutoyé, janvier 2011.

[26] Jonathan-Christofer Demay, Génération et évaluation de mécanismes de détection des intrusions au niveau applicatif, Thèse de doctorat, école doctorale Matisse, université de Rennes 1, Juillet 2011.

[27] Thierry Evangelista, Les IDS Les systèmes de détection d'intrusion informatiques édition DUNOD, Paris 2004.

[28] Cédric Michel, Langage de description d'attaques pour la détection d'intrusions par corrélation d'événements ou d'alertes en environnement réseau hétérogène, Thèse de doctorat, Université de Rennes 1, Décembre 2003.

[29] ADDA Mehdi, GUERROUT Farida, Contribution à la sécurité informatique, mise en uvre d'un IDS (intrusion detection system), Mémoire du projet de fin d'études, mémoire de Magister, université des sciences et de la technologie Houari BOUMEDIENNE, 2001.

[30] Mercier Denis, Mise En Place D'un Système De Détection D'intrusion sur le réseau de l'entreprise, Rapport de stage en licence QSSI, Université François-Rabelais Tours, 2008-2009.

[31] A. VAUCAMPS. Sécurité des routeurs et contrôle du trafic, édition Eni, 2010.

[w1] : Le grand livre de sécuritéinfo, http : //www.securiteinfo.com, 05/03/2014.

[w2] http ://dbprog.developpez.com,22/04/2014.

[w3] http :// IDS T/IPS.html, 25/02/2014.

[w4] http ://eip.epitech.eu/2013/gns3/fr/project.html,15/12/2013.

[w5] www.gns3.net,15/12/2013.

[w6] virtualBox-documentation Ubentu Francophone,http ://doc.ubuntu-fr.org/, 13/01/2014.

Annex A

Les couches TCP/IP

En Comparaison avec le modèle OSI, on peut ramener l'architecture de communication de données utilisant TCP/IP à un ensemble de quatre couches superposées :

Couche 1 : Accès réseau

Cette couche a pour fonction l'encapsulation des datagrammes provenant de la couche IP et la traduction des adresses IP en adresses physiques utilisées sur le réseau. Il y a donc autant de versions de la couche physique qu'il y a de type de moyen de transport des données.

- **IP (Internet Protocol),** est un ensemble de protocoles permettant de résoudre les problèmes d'interconnexion en milieu hétérogène. Le réseau IP assure un transfert de données non fiable (remise pour le mieux), dans ces conditions les programmes d'application doivent prendre en compte toutes les défaillances éventuelles du réseau et en particulier :
  1. la détection et la reprise sur erreur ;
  2. la perte de données dues à la saturation des mémoires tampons des éléments actifs du réseau,phénomène connu sous le nom de congestion ;

Couche 2 : Internet

Cette couche sert à gérer la circulation des paquets à travers le réseau en assurant leur routage. Elle comprend aussi les protocoles ARP (Adresse Resolution Protocol), ICMP (Internet Control Message Protocol) et d'autre.

- **Le protocole ARP :** gère les adresses des cartes réseaux. Chaque carte a sa propre adresse d'identification codée sur 48 bits.
- **Le protocole ICMP :** Le protocole ICMP (Internet Control Message Protocol, RFC 792) permet d'informer la source d'une erreur réseau (message d'erreur) ou de formuler une demande d'état à un système (message d'information). Les messages ICMP sont encapsulés dans un datagramme IP (Protocole = 1).

Couche 3 : Transport

Elle assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire. Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP (Transmission Control Protocol) ou non fiable dans le cas d'UDP (User Datagram Protocol).

- **Le protocole TCP**

  TCP (Transmission Control Protocol) est un protocole de niveau transport en mode connecté. S'appuyant sur un protocole réseau non fiable, TCP garantit la délivrance des données en séquence, il en contrôle la validité et organise les éventuelles reprises sur erreur ou sur temporisation, enfin, il effectue un contrôle de flux de bout en bout. Les paquets TCP sont envoyés sous forme de datagrammes Internet. L'en-tête IP transmet un certain nombre de paramètres, tels que les adresses Internet source et destinataires. L'en-tête TCP est placé à la suite, contenant les informations spécifiques au protocole TCP. Cette division permet l'utilisation de protocoles autres que TCP, au-dessus de la couche IP.

  1. **La structure du segment TCP**

     TCP ne définit qu'un seul format de segment contre dix pour les messages de transport du modèle de référence. De ce fait, l'en-tête de TCP est

prévu à la fois pour le transport des données, la gestion des acquittements et l'envoi de commandes .

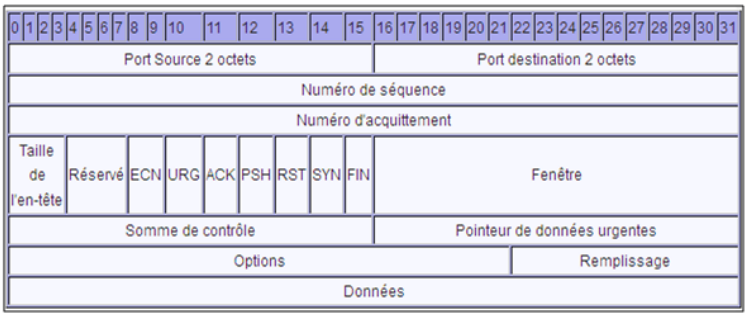


FIGURE 4.37 – La structure de segment TCP

.

- **Le protocole UDP(User Datagram Protocol)**

  Le protocole UDP est un protocole de transport d'acheminement au mieux, décrit dans le document RFC 768. Le protocole UDP est un protocole de transport léger qui offre les mêmes fonctions de segmentation et de réorganisation des données que le protocole TCP, mais sans la fiabilité et le contrôle de flux du protocole TCP. C'est un protocole simple, qui est généralement décrit en indiquant ce qu'il ne fait pas par rapport au protocole TCP.

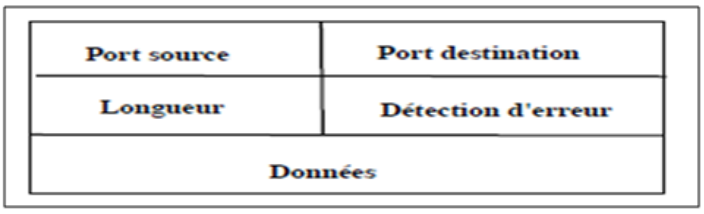


FIGURE 4.38 – Entête UDP.

Couche 4 : Application

Elle prend en charge les protocoles d'adressage et l'administration réseau. Elle comporte des protocoles assurant le transfert de fichiers, le courrier électronique et la connexion à distance.

- **Protocole DNS (Domain Name System)**

  DNS est une base de données distribuée basée sur le modèle relationnel client/serveur. La partie cliente, le solveur, est chargée de résoudre la correspondance entre le nom symbolique de l'objet et son adresse réseau. En introduisant un nommage hiérarchique et la notion de domaine (chaque nud de la hiérarchie peut être un domaine ou sous-domaine de nommage).

- **Protocole DHCP (Dynamic Host Configuration Protocol)**

  DHCP permet d'attribuer des adresses IP dynamiquement, c'est-à-dire que l'adresse IP affectée à la machine qui démarre peut changer d'un démarrage à l'autre.

- **FTP (File Transfert Protocol)** L'originalité de FTP est d'ouvrir pour chaque session FTP deux connexions simultanées. L'une sur le port 21 (FTP), l'autre sur le port 20 (FTP Data). La première connexion , connexion de contrôle ou de service, sert à l'échange des messages FTP (connexion de signalisation), l'autre au transfert de données . La demande de connexion FTP est établie sur le port 21 et reste active durant toute la session FTP (connexion permanente). La connexion de transfert sur le port 20 n'est active que durant le transfert effectif d'un fichier (connexion temporaire).

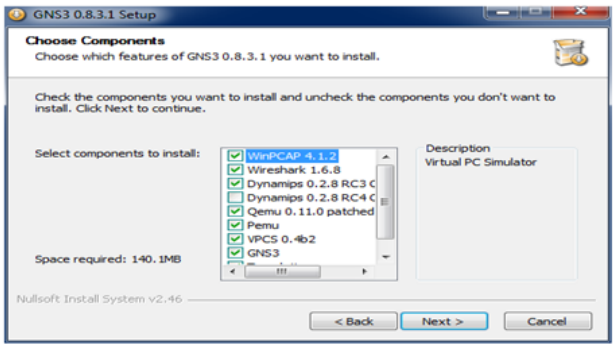
Annex B

Téléchargement de GNS3

- Site Internet pour le téléchargement de GNS3 : http ://www.gns3.net.
- Sélectionnez le menu ”Downloads” puis cliquez sur le lien ”GNS3 v0.8.3.1.all-in-one”.

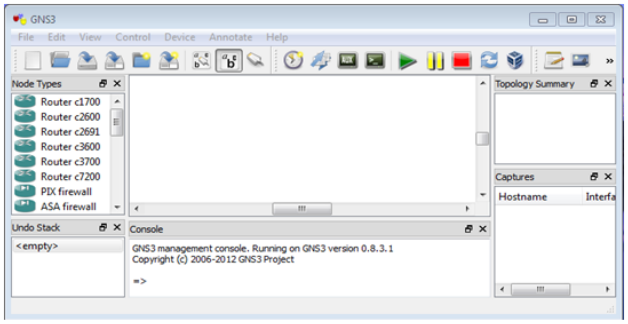
Installation

- ***Etape1 :*** Double-cliquez sur le fichier ”GNS3-0.8.3.1-all-in-one.exe”.
- ***Etape2 :*** Cliquez sur le bouton [Next >]. Acceptez les termes de la licence.
- ***Etape3 :*** Acceptez le nom proposé par défaut. Cliquez sur le bouton [Next >].



- ***Etape4 :*** Acceptez la sélection proposée par défaut puis cliquez sur le bouton [Next >].
- ***Etape5 :*** Acceptez le répertoire d'installation par défaut. Cliquez sur le bouton ”Install”.

- ***Etape6 :*** L'installation est terminée. Cliquez sur le bouton [Netxt >] puis sur [Finish].

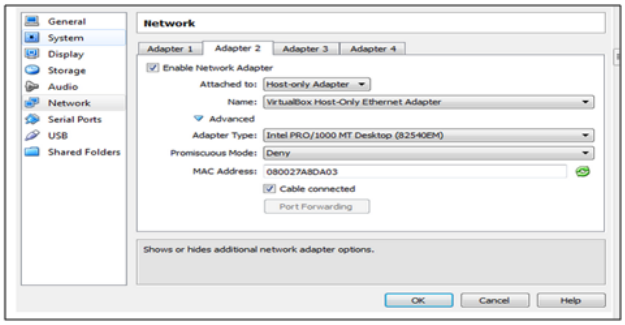


L'installation de Virtualbox

- pour télécharger virtualbox allez sur le site :http ://www.virtualbox.org/wiki/Downloads.
- Choisir la version adéquate au système et lancez l'installation.

Paramètres de la machine virtuelle

Sur notre machine (déjà installée), il nous faut aller modifier les paramètres réseaux. Une seule carte réseau suffit, nous allons faire en sorte que celle-ci soit donc dans notre réseau GNS3, on va par exemple utiliser la carte "Adaptater 2", cela permettera par exemple de garder une interface connectée à Internet en plus. Nous devons donc aller dans les "Settings" de la machine virtuelle puis dans "Network" :



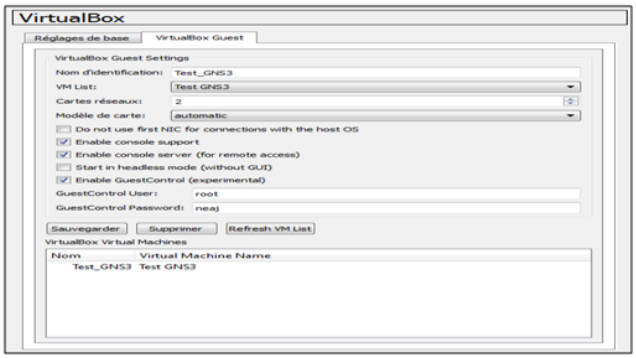
Ici, nous allons mettre notre carte réseaux numéro 2 en "Host-only Adapter" et

laisser le nom par défaut "VirtualBox Host-Only Ethernet Adapter". Les autres paramètres avancés sont aussi à laisser par défaut, il faut juste s'assurer que le câble est connecté pour que la liaison s'effectue correctement.

Importation de la machine virtuelle

Nous pouvons maintenant passer à l'onglet "VirtualBox Guest" où nous allons réellement importer la machine virtuelle dans GNS3. La première chose à faire dans cet onglet et de cliquer sur "Refresh VM List" pour que le module natif GNS3 aille chercher les machines virtuelles disponibles. Suite à cela, celles-ci seront disponibles dans la "VM List" :

Nous pourrons alors sélectionner la machine que nous voulons importer. Il faudra également entrer d'autres paramètres comme suivant :



On entre le nom de la machine aprés l'avoir sélectionnée, le numéro de la carte réseau de la machine virtuelle que nous voulons connecter à notre réseau GNS3 (ici c'est la carte numéro 2), puis le modèle de carte (laisser ce paramètre en "automatic" suffira).

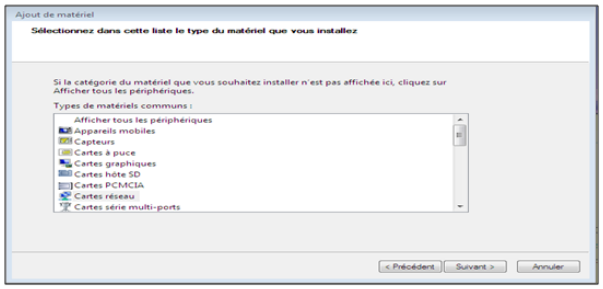
Enfin nous pouvons directement mettre l'user et le mot de passe de notre machine pour simplifier la connexion et la gestion de celle ci dans notre réseau. Ces paramètres sont facultatifs et accessoires. De plus, GNS3 nous indique que

les mots de passe transitent en texte sur le réseau (virtuel) lors de l'activation de ce paramètre.Pour finir, il faut cliquer sur "Appliquer" pour valider l'importation de la machine.

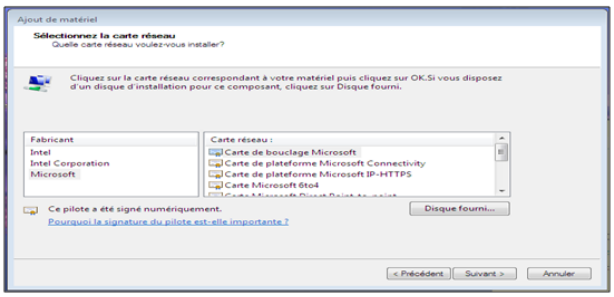
Ajout d'une carte de loopback Microsoft

Il est possible de connecter une topologie réseeau sous GNS3 à un réseau réel. Nous allons créer une interface de bouclage "loopback" que nous utiliserons avec l'interface réelle de l'hôte.

- ***Etape1 :*** Allez sur Démarrer et tapez "hdwwiz" et appuyez sur Entrée. L'assistant "Ajout de matériel" démarre .
- ***Etape2 :*** Après avoir cliqué sur "Suivant", sélectionnez "Installer le matériel que je sélectionne manuellement dans la liste (avancé)".
- ***Etape3 :*** Sélectionnez "Network Adapters".



- ***Etape4 :*** Dans la liste "fabricant" a choisi Microsoft et de "Network Adapter" pick "carte de bouclage Microsoft" :



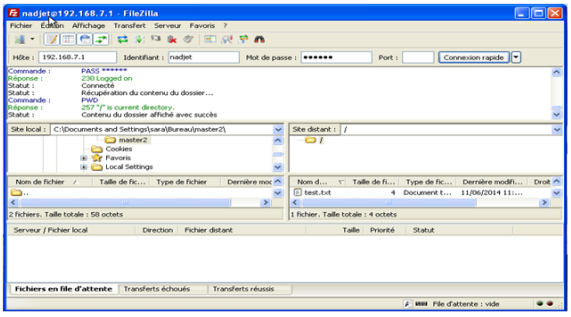
- ***Etape5 :*** Allez "Next-Next-Finish" et vous avez une carte de bouclage installé.

Le serveur FTP

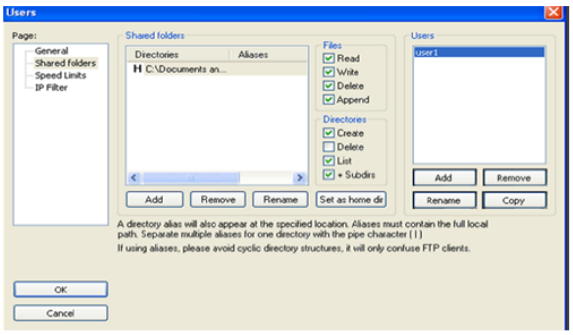
Nous avons installé l'application FileZila Server sur une machine qui va représenter le serveur ftp et FileZila client sur des machines du réseau local qui vont représenter les machines clientes.

- ***Le FileZila client***

[1] Une fois l'application est installée une fenêtre s'ouvre permet au client d'accéder au serveur ftp comme montrer dans la figure ci-dessous :



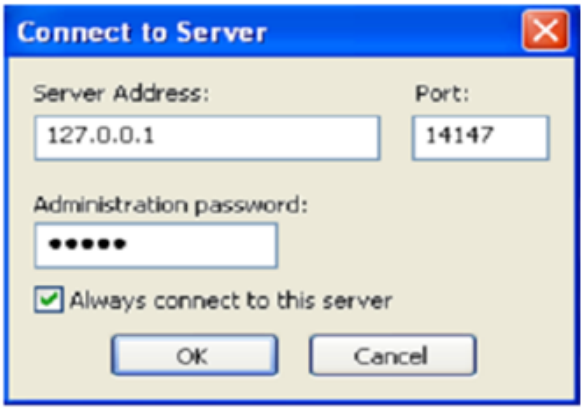
[2] Le client maintenant peut effectuer tous ces droits sur les fichiers partagés et apporter des modifications selon ces besoins.



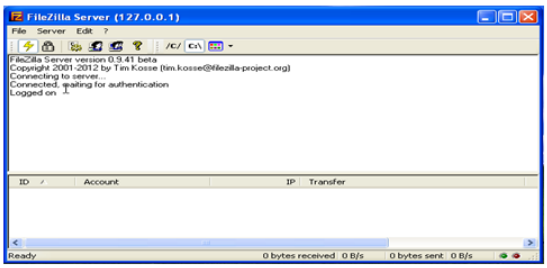
- ***Le FileZila Server***

[3] Une fois l'installation est terminée la fenêtre ci-dessous apparait :

[4] Clique sur le bouton OK pour effectuer la connexion 'a l'interface d'administration du serveur ftp.



[5] Pour configurer les paramètres de connexion et l'ajout des utilisateurs aller au menu Edit.



- ***Le menu Settings :*** affiche la fenêtre qui permet de définir les options du serveur ftp. En autres, nous pouvons définir les options de type message de bienvenue, port utilisé, etc.
- ***Le menu Users :*** affiche la fenêtre qui permet de définir les utilisateurs (ainsi les options ayant trait à leurs comptes) du serveur ftp.
- ***Le menu groups*** affiche la fenêtre qui permet de définir le ou les groupes qui seront disponibles sur le serveur ftp.

Résumé

Notre travail a consisté à configurer un système de détection d'intrusions (IDS) et sa mise en uvre au niveau de l'architecture réseau de NAFTAL. L'IDS protège un système contre les attaques, les mauvaises utilisations et les compromis. Il peut également surveiller l'activité du réseau, analyser les configurations du système et du réseau contre toute vulnérabilité, analyser l'intégrité de données et bien plus selon les méthodes de détection que nous avons choisie de déployé.

Nous avons étudié dans ce mémoire les différents aspects relatifs à notre projet à savoir : les généralités sur la sécurité informatique, les systèmes de détection d'intrusions et en fin, nous avons terminé avec une réalisation d'une solution basé sur IDS où nous avons utilisé un ensemble d'outils : GNS3 pour la simulation et la configuration de la topologie, IDM pour l'accès et la configuration de l'IDS et BackTrack pour les tests de fiabilité.
Mots clés **:** IDS, Attaque, Sécurité informatique, Test.

Abstract

Sensor networks are networks containing a large number of sensor nodes that can work together to provide a service specified property, whose their areas of application are numerous. However, such networks have limited resources, limitations of capacity ,storage and treatment.

Nevertheless, many obstacles inherent to their specific characteristics. Amongst these obstacles, the security problem is an increasing problem who must resolve in accordance with the special characteristics of RCSF, and among these security issues is the problem of key Management.

In this memoir, we present a study of security issues in RCSF and various attacks have been studied and to deal with, the cryptographic technique has proved a good choice of solution. In addition we also study and classify the different asymmetric cryptosystems proposed, through which the goals of security against potential attacks are made more or less satisfactory, thus we developed

a comparison between these cryptosystems following criteria clearly specify in order to summarize the applicability of such a cryptosystem in RCSF.

Keywords **:** Networks of wireless sensors, security, Asymmetric cryptography.