République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

Mémoire de fin de cycle
En vue d'obtention du diplome
de Master en Informatique
Spécilité: Administaration et Sécurité des Réseaux Informatiques
Thème

Mise en oeuvre d'une solution de sécurité basé sur les IDS
Cas d'étude: entreprise Cevital

Réalisé par:

Mlle AGGOUN Sarra

Mlle BELKACEM Sabrina

Soutenu devant le jury composé de :

Président	M^{r} BADACHE Abderrahmane	U. A/Mira Béjaïa.
Examinateur	M^{me} BRAHIMI Samira	U. A/Mira Béjaïa.
Examinateur	M^{me} BATTAT Nadia	U. A/Mira Béjaïa.
Encadreur	M^{r} AISSANI Sofiane	U. A/Mira Béjaïa.
Co-Encadreur	M^{me} HAMZA Lamia	U. A/Mira Béjaïa.
Invité	M^{r} BOUKHARCHA Amar	Entreprise Cevital

Université de Béjaia 2013

Table des matières

Table des figures

Introduction Générale

Introduction Générale

La sécurité des systèmes informatiques est un problème sensible et préoccupant. Le progrès spectaculaire des technologies de l'information et de communication offre actuellement des facilités incontournables en matière de transfert de fichiers, messageries et bien d'autres formes d'échange d'informations. Le développement de l'informatisation des échanges s'est accompagné malheureusement du développement d'activités malveillantes dont les motivations sont aussi nombreuses que dangereuses et évoluent dans le temps.

Profitant de la connectivité croissante des systèmes d'informations, à l'Internet notamment, les possibilités d'attaques à distance sont plus grandes et plus menaçantes. Les vulnérabilités et les failles continuellement découvertes des systèmes informatiques (systèmes d'exploitation, applications, protocoles de communication, etc.), augmentent les risques d'attaques à distance. Actuellement, les pare-feu permettent de réduire partiellement ce risque, cependant un réseau protégé par un pare-feu demeure tout de même pénétrable. En plus un attaquant interne peut abuser de ses privilèges et attaquer des systèmes au sein du même réseau local.

Afin de détecter toute tentative de violation des mécanismes de sécurité, une surveillance permanente et régulière des systèmes peut être mise en place, ce sont les Systèmes de Détection d'Intrusions (en anglais Intrusion Detection System, IDS).

La détection d'intrusion consiste à scruter le trafic réseau, collecter tous les événements, les analyser, et générer des alarmes en cas d'identification de tentatives malveillantes.

Ces systèmes sont devenus très largement déployés dans les systèmes informatiques et ils ont gagné une place importante dans la conception de la stratégie de sécurité. Ils sont généralement utilisés pour surveiller l'accès et le flux d'information, dans le but de déterminer tout comportement malicieux, que ce soit de l'intérieur ou de l'extérieur de système d'informations, et rendre cette information disponible aux administrateurs de la sécurité. En option, les systèmes de détection d'intrusions peuvent réagir contre ces comportements malicieux et prendre des contre-mesures.

Pour détecter des intrusions, deux approches principales ont été proposées. La première, dite approche comportementale, consiste à modéliser dans une phase initiale le comportement normal d'entités du système pour rechercher ensuite des attitudes déviantes dans le comportement courant de ces entités. La seconde, dite approche par scénarios, consiste à rechercher dans les activités des entités des traces de scénarios d'attaque connus, exploitant les nombreuses vulnérabilités présentes dans les systèmes utilisés aujourd'hui.

Mettre en place des mécanismes préventifs est une condition nécessaire mais pas suffisante. En effet, compromettre un système est essentiellement une question de temps et de moyens mis en œuvre. Malgré tous les efforts déployés pour renforcer la sécurité d'un système ou d'un réseau, tout mécanisme de sécurité a ses limites et peut être contourné.

Notre projet a pour objectif la simulation et la configuration d'un système de détection d'intrusions et sa mise en œuvre au niveau de l'architecture réseau de Cevital.

Organisation du mémoire

L'organisation de ce mémoire reflète la démarche que nous avons adoptée lors de la réalisation de ce travail. Ce travail est composé de cinq chapitres :

Après l'introduction générale, le premier chapitre qui sera consacré à la définition de quelques notions de bases sur la sécurité informatique, ainsi que les attaques menaçant un réseau. Dans le second chapitre nous allons présenter les différents outils utilisés pour sécuriser un réseau. Dans le troisième chapitre, nous allons effectuer une étude théorique des systèmes de détection d'intrusions et approfondir les notions relatives à ce dernier. Dans le quatrième chapitre nous allons présenter l'organisme d'accueil où nous avons effectué notre stage. Enfin, le cinquième chapitre, décrit la partie pratique de notre travail, dans lequel nous allons présenter l'environnement de travail ainsi que le cas d'étude qui consiste à faire une simulation d'un système de détection d'intrusions IDS Cisco sur le réseau du groupe Cevital et définir les différentes configurations réalisées.

Chapitre I

Généralités sur la sécurité informatique

Introduction

Les systèmes informatiques et les réseaux sont devenus des outils indispensables pour la société actuelle. Ils sont aujourd'hui déployés dans tous les secteurs professionnels. Ce développement phénoménal est accompagné également par la croissance du nombre d'utilisateurs, qui ne sont pas forcément pleins de bonnes intentions vis-à-vis de ces systèmes informatiques, en exploitant ses vulnérabilités.

Des attaques réalisées par ces utilisateurs malveillants sont de plus en plus fréquentes, de telles attaques peuvent par exemple nuire à l'image du propriétaire du système d'information ou causer d'importants dommages financiers. La problématique de la sécurité devient donc une question essentielle aussi bien pour les utilisateurs que pour les administrateurs de ces systèmes d'information.

Au long de ce chapitre nous allons donner dans un premier temps des notions de base de la sécurité et par la suite nous décrivons les différentes attaques menaçant le système informatique.

I La sécurité informatique

I.1 Définition

La sécurité informatique est un terme large qui réunit les moyens humains, techniques, organisationnels et juridiques qui tentent de garantir certaines propriétés d'un système d'information[**1**].

I.2 Les objectifs de la sécurité informatique

La sécurité informatique consiste à garantir que les ressources matérielles ou/et logicielles d'une organisation sont uniquement utilisées dans le cadre prévu [**6**].

. **Disponibilité :** les données doivent rester accessibles aux utilisateurs. C'est la capacité à délivrer un service permanent à l'entreprise.

. **Confidentialité :** les données ne doivent être visibles que par les personnes autorisées. C'est le fait de ne pas divulguer des informations sensibles propres à l'entre-

prise.

. **Intégrité :** il faut pouvoir garantir que les données protégées n'ont pas été modifiées par une personne non autorisée. Le but étant de ne pas altérer les informations sensibles de l'entreprise.

. **Non répudiation :**on doit pouvoir certifier avec certitude quand un fichier a subi des modifications par la personne qui l'a modifié.

I.3 La politique de sécurité informatique

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

I.3.1 Définition

Avant de mettre en place des mécanismes de protection, il faut préparer une politique à l'égard de la sécurité. C'est elle qui fixe les principaux paramètres, notamment les niveaux de tolérance et les coûts acceptables. Donc une politique de sécurité informatique est un plan d'actions définies pour maintenir un certain niveau de sécurité [**2**].

I.3.2 Les étapes de mise en oeuvre d'une politique de sécurité

La mise en œuvre se fait selon les quatre étapes suivantes [**11**] :

. Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.

. Elaborer des règles et des procédures à mettre en oeuvre 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.

Cette politique est formalisée dans l'entreprise sous forme d'un document. Il doit comporter un recueil de pratiques qui régissent la manière de gérer, de protéger et de transmettre les informations critiques ou sensibles appartenant à l'organisation.

I.3.3 Les normes associées

La mise en œuvre de solutions de protection et de sécurité requiert de prendre des références par rapport à des normes ou des préconisations [**11**]. Nous citons ISO (International Organization for Standardization) qui décrit ces politiques dans l'ISO 27000 [1] **W2**.

I.4 Terminologie de la sécurité informatique

Le domaine de la sécurité possède un vocabulaire bien défini. Nous allons définir certains termes.

I.4.1 Vulnérabilités

Il s'agit d'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**].

I.4.2 Menace

La menace désigne l'exploitation d'une faiblesse de sécurité par un attaquant, qu'il soit interne ou externe à l'entreprise.

La probabilité qu'un événement exploite une faiblesse de sécurité est généralement évaluée par des études statistiques, même si ces dernières sont difficiles à réaliser [**2**].

I.4.3 Risque

Les menaces engendrent des risques et des coûts humains et financiers : perte de confidentialité de données sensibles, indisponibilité des infrastructures et des données,

[1] Série de normes dédiées à la sécurité de l'information.

dommages pour le patrimoine intellectuel et la notoriété. Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités [**4**].

I.4.4 Attaque

Une attaque est définie comme faute d'interaction malveillante visant à violer une ou plusieurs propriétés de sécurité. C'est une faute externe créée avec l'intention de nuire, y compris les attaques lancées par des outils automatiques : vers, virus,etc. La notion d'attaque ne doit pas être confondue avec la notion d'intrusion [**3**].

I.4.5 Intrusion

Une intrusion est définie comme une faute malveillante interne d'origine externe, résultant d'une attaque qui a réussi à exploiter une vulnérabilité. Elle est susceptible de produire des erreurs pouvant provoquer une défaillance vis-à-vis de la sécurité, c'est-à-dire une violation de la politique de sécurité du système.

Le terme d'intrusion sera employé dans le cas où l'attaque est menée avec succès et où l'attaquant a réussi à introduire et/ou compromettre le système [**3**].

I.4.6 Traçabilité

Ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise. Cela suppose que tout événement applicatif soit archivé pour investigation ultérieure [**2**].

I.4.7 Journalisation

- **Un journal**,ou **log** en anglais, est une zone de stockage contenant l'enregistrement des événements de l'activité d'un système. Ce journal peut être interne au système, en local ou sur un système externe (ex : la journalisation des requêtes sur le serveur proxy).
- La définition informatique de la **journalisation**, ou **logging** en anglais, est le fait de noter dans un journal ce qui se passe dans un système au fur et à mesure de son fonctionnement. Ces évènements sont donc enregistrés dans l'ordre historique, et selon un niveau de détail ou d'importance **W1** .

I.4.8 Les audits de sécurité

Le mécanisme d'audit de sécurité, consistant en l'enregistrement de tout ou partie des actions effectuées sur le système pour en faire une analyse a posteriori, permet de détecter des intrusions et de démasquer les auteurs de ces dernières.

Toute opération entreprise sur un système informatique se traduit par une séquence d'actions effectuées par le système. Ces actions sont appelées activités système. Une activité système intervenant à un certain moment est appelée événement. Les enregistrements du journal d'audit sont aussi appelés traces d'audit.

Le journal d'audit doit permettre, à partir de l'étude des séquences d'événements que l'on y trouve, de reconstituer les opérations entreprises par certains utilisateurs spécifiques du système, dits utilisateurs audités [**7**].

I.4.9 Les contre mesures

Les contre mesures donnent au système la capacité à réagir aux tentatives d'intrusions [**8**].

I.4.10 La Cryptographie et la Cryptanalyse

La Cryptographie est la science de l'invention des codes secrets pour assurer la confidentialité et l'intégrité d'une information transmise entre deux entités. La science adverse du déchiffrement de ces codes est la cryptanalyse [**4**].

Dans ce qui suit nous allons donner quelques définitions de base relatives à la cryptographie.

- **Cryptage**(chiffrement) : consiste à faire subir à un texte clair une transformation plus ou moins complexe pour en déduire un texte incompréhensible, dit chiffré La transformation repose sur deux éléments : une fonction mathématique et une clé secrète [**4**].
- **Décryptage**(déchiffrement) : c'est une transformation inverse du cryptage qui consiste à trouver le texte en clair à partir de son chiffré [**4**].

. **Clé** : il s'agit d'un paramètre impliqué dans les opérations de chiffrement et de déchiffrement qui est partagé entre l'émetteur et le récepteur [**6**].

II Les attaques informatiques

En informatique, il existe de nombreuses attaques possibles : certaines sont basées sur des failles des logiciels, d'autres sur l'accès à certaines ressources insuffisamment protégées ou encore sur l'ignorance ou la curiosité des utilisateurs (les attaquants).

II.1 Les attaquants et leurs objectifs

De nombreux internautes et entreprises sont connectés chaque jour à Internet et sont alors des cibles potentielles pour des personnes malfaisante.

II.1.1 Le piratage

Le piratage (haking en anglais) est un ensemble de technique, visant à attaquer un réseau, un site... [**9**], par la recherche et l'exploitation des failles de sécurité.

II.1.2 Les pirates informatiques

Le terme pirate (hacker ou encore cracker) fait référence à la personne qui s'introduit dans les systèmes d'information sans autorisation pour, dans le pire des cas, provoquer des dégradations dans les données ou les applications.

Ses actions peuvent s'effectuer à partir de l'intérieur (dans le cas où il a pu obtenir un accès sur le réseau) ou de l'extérieur de l'entreprise. Toutefois, il n'est pas toujours facile de détecter sa présence sur le système ni de connaître ce qu'il a provoqué comme dégâts [**11**].

Nous distinguons deux catégories de pirates :

. **Les White hat hackers :** Ils sont des experts des systèmes d'exploitation qui cherchent des failles de sécurité pour mettre en évidence les vulnérabilités des systèmes mais s'interdisent leur exploitation malveillante. Ils se contentent d'avertir les autorités du problème [**9**].

. **Les Blacks hat hackers :** Appelé aussi crackers les méchants, beaucoup moins scrupuleux, ils cherchent des failles eux aussi mais à des fins nuisibles, souvent pour en tirer un bénéfice personnel. Parmi eux nous distinguons [**9**] :

a. Les Scripts Kiddies : On qualifie un individu de script kiddie lorsque l'on considère qu'il est incapable de créer ses propres outils ou programmer pour exploiter les failles de sécurité et qu'il ne comprend pas très bien le fonctionnement des outils qu'il emploie.

b. Les phreakers : Sont des pirates s'intéressant au réseau téléphonique commuté RTC afin de téléphoner gratuitement grâce à des circuits électroniques connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement. On appelle ainsi "phreaking" le piratage de ligne téléphonique.

c. Les carders : S'attaquent principalement aux systèmes de cartes à puces (en particulier les cartes bancaires) pour en comprendre le fonctionnement et en exploiter les failles. Le terme "carding" désigne le piratage de cartes à puce.

II.2 Classification des attaques

Les hackers utilisent plusieurs techniques d'attaques. Ces attaques peuvent être regroupées en trois classes différentes :

II.2.1 La première classification

Cette première classification consiste à classer les attaques en deux types :

. **Les attaques passives :** ce type d'attaque vise à l'obtention d'accès pour pénétrer dans le système sans compromettre ces ressources.

. **Les attaques actives :** dont le résultat de cette attaque est un changement non autorisé d'état des ressources de système [**10**].

II.2.2 La deuxième classification

Cette classification consiste aussi à distinguer deux types d'attaques [**10**] :

. **Les attaques internes :** ce type d'attaque est causé :

1. Soit par les utilisateurs autorisés du système qui essayent d'utiliser des privilèges complémentaires dont ils n'ont pas le droit.

2. Soit par les utilisateurs autorisés qui emploient improprement les privilèges dont ils ont le droit.

. **Les attaques externes :** ce type d'attaque est causé par des utilisateurs externes qui essayent d'accéder à des informations ou des ressources d'une manière illégitime et non autorisée.

II.2.3 La troisième classification

Dans cette dernière classification nous distinguons [**9**] :

. **Les attaques directes :** C'est la plus simple des attaques. Le hacker attaque directement sa victime à partir de son ordinateur. La plupart des "script kiddies" utilisent cette technique. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrables, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

FIG. I.1 – Attaque directe

Par ce type d'attaque, il y a de grandes chances pour que la victime puisse remonter à l'origine de l'attaque, pour identifier l'identité de l'attaquant.

. **Les attaques indirectes par rebond :** Dans ce type d'attaque les paquets d'attaque son envoyés à l'ordinateur intermédiaire qui répercute l'attaque vers 1a victime. On utilise ces types d'attaque pour masquer l'identité ,l'adresse IP (Internet Protocol)du pirate ou pour utiliser des ressources de l'ordinateur intermédiaire car il est plus puissant (CPU (Central Processing Unit), bande passante,...).

Dans ce genre d'attaque, il n'est pas facile de remonter à la source. Au plus simple, vous remontrez à l'ordinateur intermédiaire.

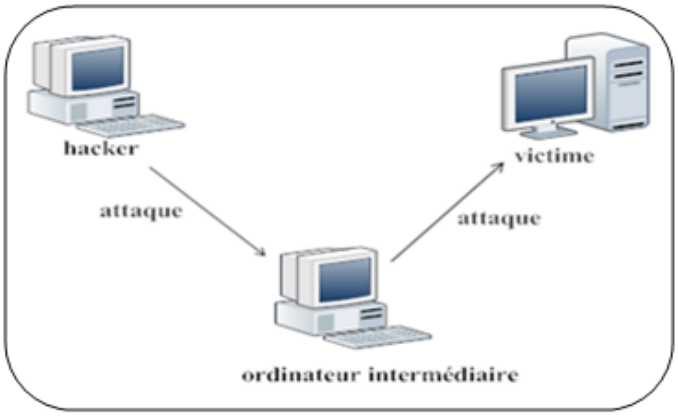


FIG. I.2 – Les attaques indirectes par rebond

. **Les attaques indirectes par réponse :** Cette attaque est un dérivé de l'attaque 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 envoyée à l'ordinatrice victime.

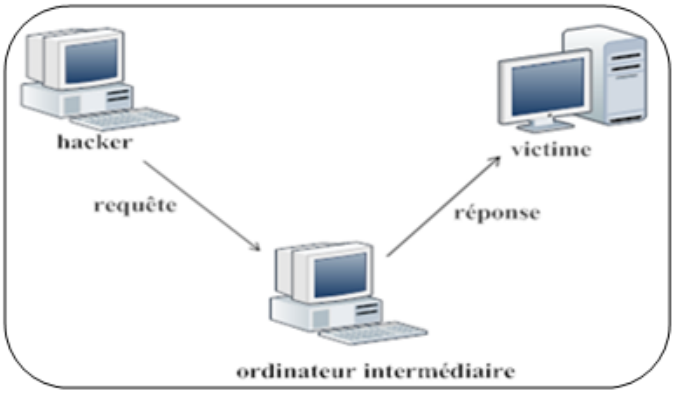


FIG. I.3 – Les attaques indirectes par réponse

Dans ce genre d'attaque, il n'est pas aisé de remonter à la source.

II.3 Les différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma. Observons le détail de chacune de ces étapes **W6** :

. **Identification de la cible :** cette étape est indispensable à toute attaques organisée, 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 System),....
. **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 (versions des services, règles de firewall...). Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entraîner la défaillance de certains systèmes.
. **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 ce pourquoi il a franchi les précédentes étapes. Le but ultime étant d'élever ses droits vers root [2] sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine,récupération d'informations, installation de backdoors, nettoyage des traces ,...).

II.4 Quelques attaques

Cette partie décrit les différentes attaques susceptibles d'affecter un réseau et les systèmes qui le composent

Nous allons caractériser quelques attaques.

II.4.1 Les attaque réseaux

Le but des attaques réseau est de cartographier le réseau afin d'en repérer les faiblesses et les cibles les plus intéressantes. Mais il peut être aussi de récupérer des informations circulant sur le réseau telles que les données d'authentification ou les caractéristiques d'un contrôle d'accès afin de les exploiter pour passer outre un autre mécanisme de sécurité.

[2]Est un mot anglais, signifiant racine,qui peut désigner : un super-utilisateur ou administrateur principal un répertoire racine d'un système de fichiers (exemple C : pour le premier disque dur sous Windows).

Nous allons présenter les techniques et méthodes qu'utilisent les pirates afin d'atteindre ces buts.

1. Le balayage de ports

Les scans ou balayage de ports ne sont pas des attaques à proprement parler. Le but des scans est de déterminer quels sont les ports ouverts, et donc en déduire les services qui sont exécutés sur la machine cible (ex : port 80/TCP (Transmission Control Protocol) pour un service HTTP (Hyper Text Transfer Protocol)) [**2**].

. **Attaque par balayage ICMP :** La méthode de balayage la plus simple consiste à utiliser le protocole ICMP (Internet Control Message Protocol) et sa fonction request, plus connue sous le nom de ping [3]. Elle consiste à ce que le pirate envoie vers le serveur un paquet ICMP echo-request, le serveur répondant (normalement) par un paquet ICMP echo-reply, comme l'illustre la figure 4.

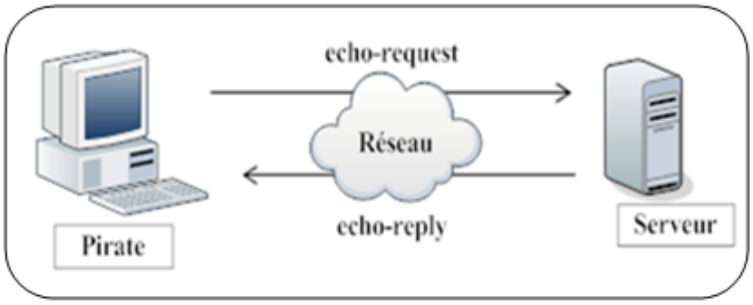


Fig. I.4 – Attaque par balayage ICMP

Il existe deux méthodes pour cartographier le réseau par cette technique :

– En balayant (scanning) le réseau et en interrogeant chaque adresse IP possible, ce qui n'est pas très discret.

– En visant une seule fois l'adresse de broadcast [4] La commande Ping permettant d'envoyer une requête ICMP Echo d'un ordinateur à un autre pour tester si cet ordinateur hôte est accessible par le réseau. du réseau, ce qui fait répondre

[3]La commande Ping permettant d'envoyer une requête ICMP Echo d'un ordinateur à un autre pour tester si cet ordinateur hôte est accessible par le réseau.

[4]Broadcast est un verbe anglais composé par broad (autour) et cast (distribuer), signifiant "diffuser", en informatique le terme broadcast désigne une méthode de transmission de données à l'ensemble des machines d'un réseau.

toutes les machines présentes. Une seule demande permet ainsi d'engendrer l'envoi de toutes les réponses.

Cependant, du fait de l'accroissement constant de l'insécurité, les administrateurs de pare-feu ont pris l'initiative de ne pas laisser passer les réponses à de telles demandes [**2**].

. **Attaque par balayage TCP :** Similaire au balayage ICMP, sa spécificité est de s'appuyer sur le protocole TCP. Le pirate envoie un paquet SYN vers un port réseau particulier de l'adresse IP du serveur. Si le port est en écoute, un paquet SYN/ACK est reçu en retour. Sinon, la réception d'un paquet RST signifie qu'il n'y a pas de service en écoute sur le port.

Si aucune réponse n'est reçue en retour, c'est qu'il existe un équipement filtrant entre le serveur et le pirate ou qu'il n'y a aucune machine derrière l'adresse IP visée. Le client envoie en réponse un paquet RST pour terminer la connexion, comme l'illustre la figure ci-dessous [**2**].

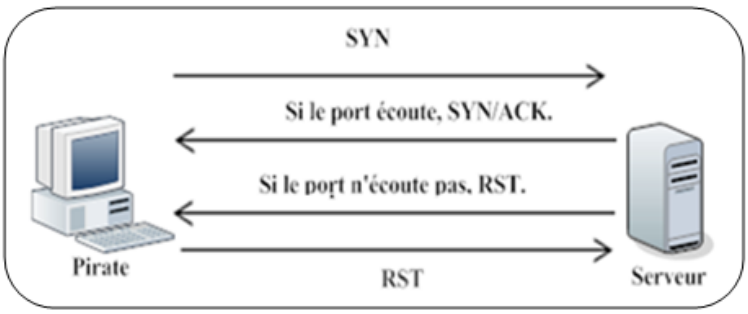


Fig. I.5 – Le balayage TCP

. **Attaque par balayage semi-ouvert TCP :** Le balayage semi-ouvert consiste en un balayage TCP normal dans le quel le pirate envoie son paquet SYN et reçoit les paquets prévus en retour, tel qu'il n'envoie pas de paquet RST pour rompre la session. Il note simplement la réponse et passe au port suivant. Par ce procédé, la session TCP n'est pas ouverte, puisque le handshake[5] ne s'est pas terminé, et le serveur ne trace pas cet échange de données [**2**].

[5]Handshake est une séquence d'étapes pour l'établissement d'une session TCP.

2. Attaques par sniffing

Un analyseur réseau (en anglais sniffer[6]) est un dispositif permettant d'écouter le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent.

Grâce à ce dispositif, il est possible d'intercepter les trames reçues par la carte réseau d'un système pirate et qui ne lui sont pas destinées. Le système pirate se situe sur le réseau local et capture tous les paquets réseau transitant sur ce réseau [**2**].

Fig. I.6 – Ecoute sur un réseau local

3. Attaques par Spoofing

La plupart des protocoles réseau n'ayant prévu aucun mécanisme d'authentification véritable, ils subissent des attaques qui s'appuient sur ces faiblesses d'authentification [**2**].

. **Attaque ARP spoofing :** Comme son nom l'indique, l'attaque ARP spoofing s'appuie sur le protocole ARP(Address Resolution Protocol), qui implémente le mécanisme de résolution d'une adresse IP en une adresse MAC (Media Access Control) pour rediriger le trafic réseau de un ou plusieurs systèmes vers le système pirate.

[6]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/.

La faiblesse d'authentification du protocole ARP permet à un système pirate d'envoyer des paquets ARP réponse au système cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne.

Le système du pirate reçoit donc tout le trafic à destination de la passerelle. Il lui suffit d'écouter ou de modifier passivement le trafic et de router ensuite les paquets vers leur véritable destination [**2**].

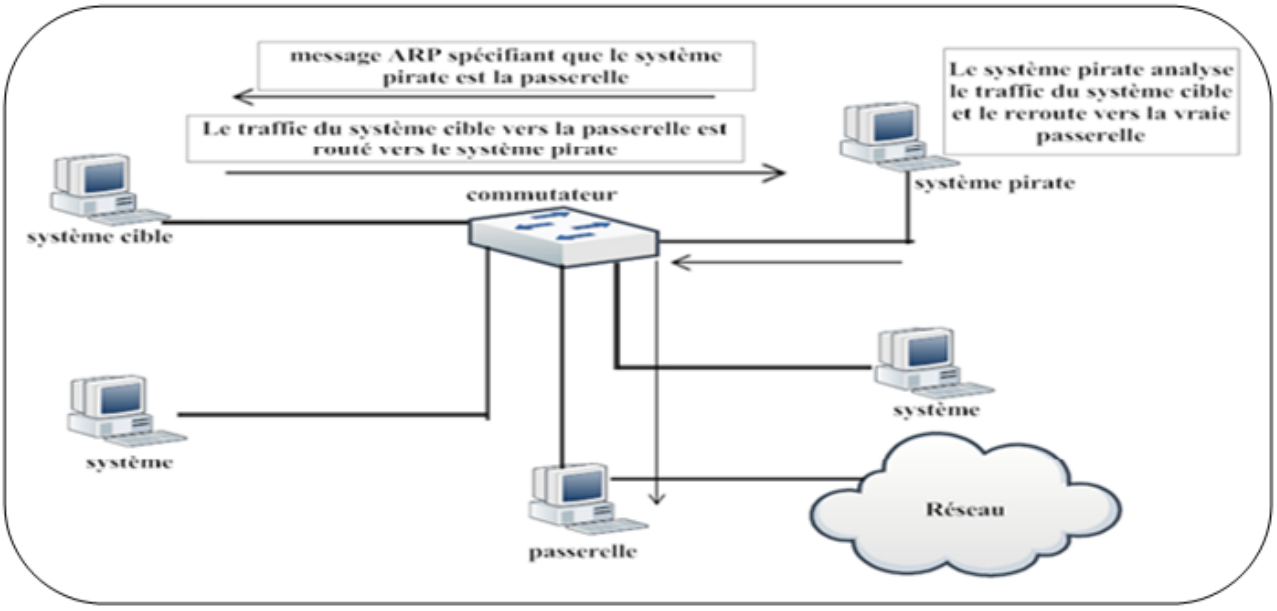


Fig. I.7 – L'attaque ARP Spoofing

. **Attaque IP spoofing :** L'attaque IP spoofing consiste à se faire passer pour un autre système en falsifiant son adresse IP. Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au système cible. Le pirate ensuite attaque le serveur cible en utilisant l'adresse IP falsifier [**2**].

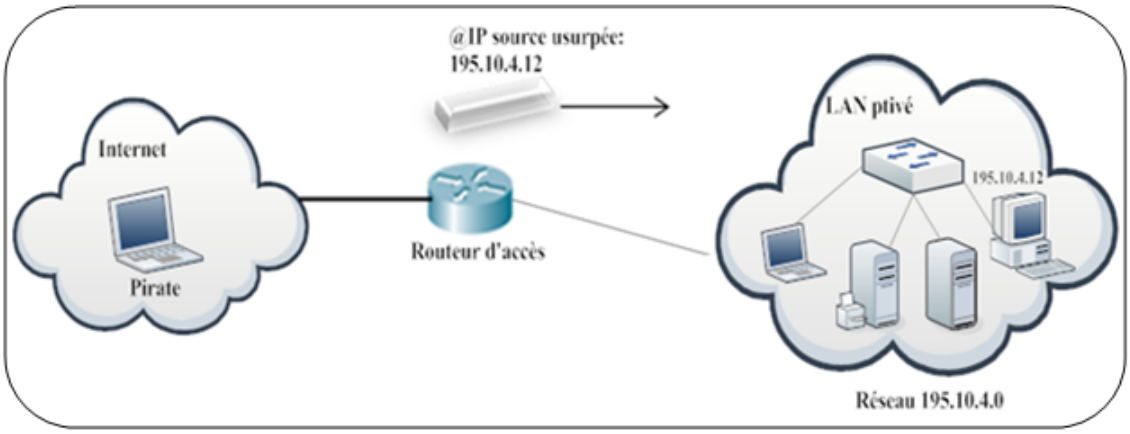


FIG. I.8 – attaque IP Spoofing

. **Attaque DNS Spoofing :** Le pirate utilise les faiblesses du protocole DNS et de son implémentation sur les serveurs de noms de domaine pour rediriger des internautes vers des sites falsifiés. Le but du pirate est donc de faire correspondre l'adresse IP d'une machine qu'il contrôle à l'URL (Uniform Resource Locator) réel d'une machine publique [**2**].

4. Attaques par fragmentation IP

Le but de cette attaque est de passer outre les protections des équipements de filtrage IP. En passant outre les protections, un pirate peut par exemple s'infiltrer dans un réseau pour effectuer des attaques ou récupérer des informations confidentielles. Deux types d'attaque sur les fragments IP peuvent être distingués :

. **Attaque par Tiny Fragments :** L'attaque par Tiny Fragments consiste à fragmenter (voir l'annexe A) sur deux paquets IP une demande de connexion TCP ou d'autres demandes sur une machine cible tout en traversant et en déjouant (par le mécanisme de fragmentation [7]) un filtrage IP.

Le premier paquet IP contient des données telles que les huit premiers octets de l'en-tête TCP, c'est-à-dire les ports source et destination et le numéro de séquence. Le second paquet contient la demande de connexion TCP effective (flag SYN à 1 et flag ACK à 0).

[7] Le mécanisme de fragmentation permet de découper un paquet IP en plusieurs fragments (paquets de plus petite taille).

Lors de la défragmentation au niveau IP de la machine cible, le paquet de demande de connexion était reconstitué et passé à la couche TCP. La connexion s'établissait alors malgré le filtre IP [**2**].

. **Attaque par Fragment Overlapping :** Quand un message est émis sur un réseau, il est fragmenté en plusieurs paquets IP. Afin de pouvoir reconstruire le message, chaque paquet possède un offset. Le but de l'attaque est de réaliser une demande de connexion et de faire chevaucher des paquets en spécifiant des offsets incorrects. La plupart des filtres analysant les paquets indépendamment, ils ne détectent pas l'attaque. Cependant, lors de la défragmentation, la demande de connexion est bien valide et l'attaque a lieu **W4**.

5. TCP session Hijacking

Le but de cette attaque est de rediriger un flux TCP afin de pouvoir outre passer une protection par mot de passe. Dans cette attaque la machine du pirate utilise la session engagée entre deux machines A et B afin que ce soit elle (la machine du pirate) qui soit en session avec la machine B [**2**].

Dans un premier temps, le pirate doit écouter le réseau, puis lorsqu'il estime que l'authentification a pu se produire (délai de n secondes par exemple), il désynchronise la session entre l'utilisateur et le serveur. Pour ce faire, il construit un paquet avec, comme adresse IP source, celle de la machine de l'utilisateur et le numéro d'acquittement TCP attendu par le serveur. En plus de désynchroniser la connexion TCP, ce paquet permet au pirate d'injecter une commande via la session préalablement établie **W4**.

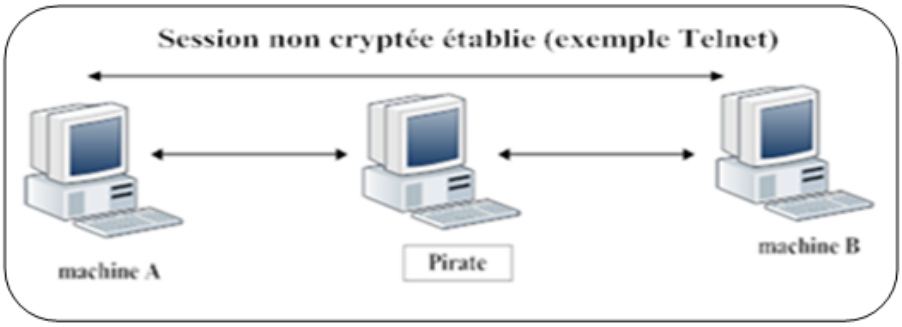


FIG. I.9 – Machine du pirate en tant que hijacker

6. Attaques de déni de service :

Le déni de service, ou DoS (Denial of Service), est une attaque qui vise à rendre indisponible un service, un système ou un réseau. Ces attaques s'appuient généralement sur une faiblesse d'implémentation, ou sur une faiblesse d'un protocole [**2**].

. **L'attaque par inondation :** Une ou plusieurs machines inondent le réseau avec des paquets réseau afin de saturer la bande passante de celui-ci.

a. Les attaques smurf : Le pirate fait des requêtes ICMP ECHO à des adresses de broadcast en spoofant l'adresse source (en indiquant l'adresse de la machine cible). Cette machine cible va recevoir un nombre énorme de réponses, car toutes les machines vont lui répondre, et ainsi utiliser toute sa bande passante **W4**.

b. Inondation par SYN : La technique d'inondation SYN(en anglais SYN Flooding) est identique à celle du balayage SYN, à la différence près qu'elle est utilisée à des fins de déni de service. Elle exploite la connexion en trois phases de TCP (Handshake : SYN / SYN-ACK / ACK).

Le principe est de laisser un grand nombre de connexions TCP en attente. Le pirate envoie de nombreuses demandes de connexion (SYN), reçoit les SYN-ACK mais ne répond jamais avec ACK. Les connexions en cours occupent des ressources mémoire, ce qui va entraîner une saturation et l'effondrement du système **W4**.

c. Ping of death : Un ping of death est un ping qui a une longueur de données supérieure à la taille maximale (65535 octets incluant un en-tête de 20 octets). Lors de son envoi, le ping of death est fragmenté en paquets plus petits. L'Ordinateur victime qui reçoit ces paquets doit alors les reconstruire. Certains système ne gèrent pas cette fragmentation, est ce bloquent ou crashent complétement [**9**].

d. Déni de service distribué (DDoS) : Une attaque Distibuted Denial of Service ou déni de service distribué est une attaque contre un ordinateur, situé en réseau par un ensemble de machines de façon simultané. A la différence des attaques de type DoS où l'attaquant est constitué d'une unique machine, plusieurs machines sont utilisées (Daemon [8]) pour l'attaque et donc celle-ci est plus dévastatrice et la saturation de la machine serveur est plus rapide [**9**].

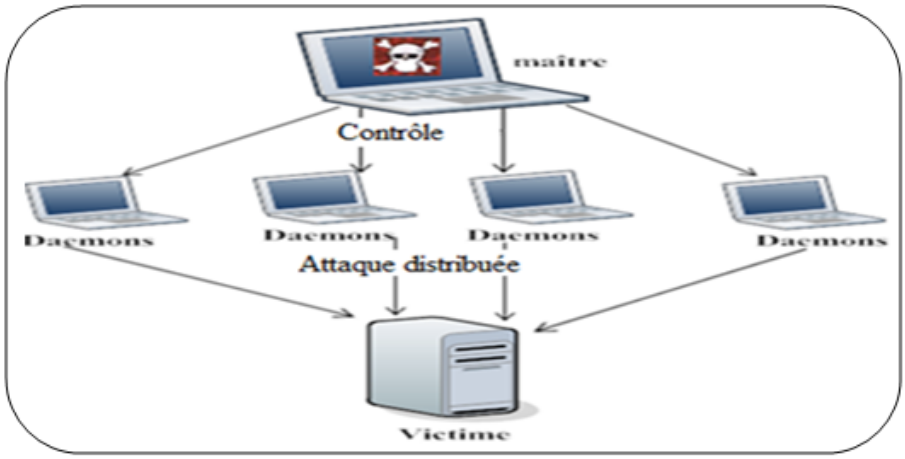


FIG. I.10 – Principe du DDOS

7. Attaque de l'homme du milieu (man-in-the-middle)

L'attaque man-in-the-middle consiste à faire passer les échanges réseau entre deux systèmes par le biais d'un troisième, sous le contrôle du pirate. Ce dernier peut transformer à sa guise les données à la volée, tout en masquant à chaque acteur de l'échange la réalité de son interlocuteur.

[8] Un Daemon est un type particulier de programme informatique, un processus qui s'exécute en arrière-plan plutôt que sous le contrôle direct d'un utilisateur.Les démons sont souvent démarrés lors du chargement du système d'exploitation, et servent en général à répondre à des requêtes du réseau, à l'activité du matériel ou à d'autres programmes en exécutant certaines tâches.

Pour mettre en œuvre l'échange réseau approprié, il faut soit que la machine du pirate se trouve physiquement sur le chemin réseau emprunté par les flux de données, soit que le pirate réussisse à modifier le chemin réseau afin que sa machine devienne un des points de passage [**2**].

8. Les attaques réseaux sans fil [14]

Les réseaux sans fil sont sensibles aux attaques comme les autres réseaux mais ils ouvrent également la voie à de nouvelles attaques : parce que les ondes hertziennes ne sont pas facilement contrôlables. La principale conséquence de cette "propagation sauvage" des ondes radio est la facilité que peut avoir une personne non autorisée d'écouter le réseau éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fil est déployé.

. **War-driving :** Le war-driving est une technique simple qui consiste à circuler dans les rues et les lieux publics à la recherche d'émetteurs. Un PC portable équipé d'une carte réseau sans fil écoute les différentes fréquences et détecte les caractéristiques des informations reçues.

Remarque : Si vous ne faites que définir un SSID (Service Set IDentifier) on peut se connecter sur votre réseau sans vraiment le chercher. Windows XP par exemple détecte les réseaux présents et peut se connecter automatiquement et si vous avez mis un DHCP en œuvre, on récupère une adresse IP légale.

. **War-chalking :** Le war-chalking est une extension du war-driving. Cette méthode consiste simplement à noter près de l'émetteur (du moins dans sa zone d'émission) ses caractéristiques : est-ce un réseau ouvert, fermé, protégé ? Pour cela, trois symboles sont couramment utilisés. Deux demi-cercles opposés désignent ainsi un réseau ouvert offrant un accès à Internet, un rond signale la présence d'un réseau sans fil ouvert sans accès à un réseau filaire et enfin un W encerclé met en évidence la présence d'un réseau sans fil correctement sécurisé comme le montre la figure suivante.

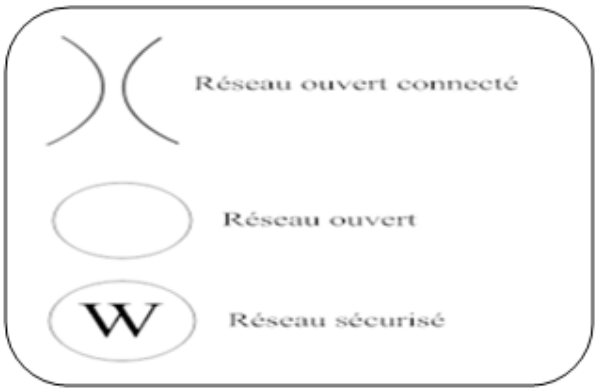


FIG. I.11 – Les symboles des réseaux sans fil

Ceux qui n'en connaissent pas la signification n'y voient qu'un graffiti alors que les hackers y voient une occasion de se connecter au réseau. De plus, l'attribution d'adresses IP de manière dynamique facilite la mise en œuvre d'un équipement sur ce réseau.

. **Brouillage :**Les fréquences employées par les réseaux sans fil peuvent être brouillées afin qu'aucune communication ne puisse passer.

Les ondes radio sont très sensibles aux interférences[9], c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisée dans le réseau sans fil ou par l'installation d'un point d'accès malicieux pour détourner le trafic comme montrer sur la figure ci-dessous, ou encore par un simple four à micro-ondes qui peut rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

Cette attaque utilisée de manière ponctuelle et irrégulière perturbe un réseau sans permettre de trouver facilement l'origine.

[9]On parle d'interférences lorsque deux ondes de même type se rencontrent et interagissent l'une avec l'autre. Ce phénomène apparaît souvent en optique avec les ondes lumineuses, mais il s'obtient également avec des ondes d'autres longueurs d'onde, ou avec d'autres types d'ondes comme les ondes sources.

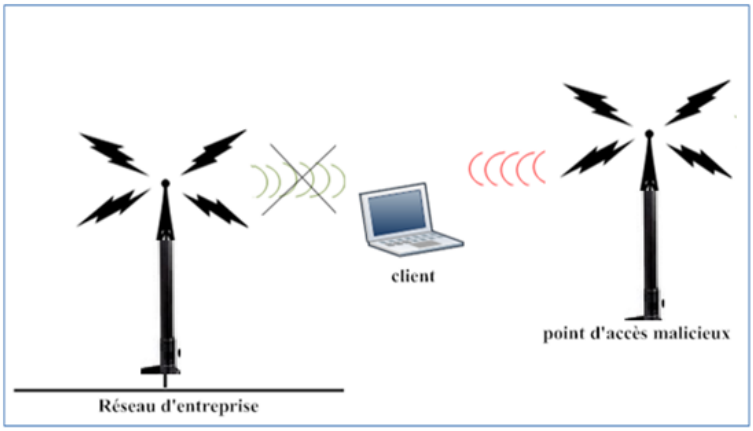


FIG. I.12 – point d'accès malicieux

. **Arp-poisoning :**Ce type d'attaque consiste à répondre plus rapidement que les autres postes à la demande de corrélation entre adresse IP et adresse MAC mais en fournissant une fausse adresse MAC. Une méthode dérivée de cette attaque est de remplir les tables ARP des équipements du réseau pour les saturer.

Le résultat rend possible l'usurpation d'une machine par une autre machine hors des locaux de l'entreprise.

II.4.2 Les attaques applicatives

Les attaques applicatives se basent sur des failles dans les programmes utilisés, ou encore des erreurs de configuration. Il est possible de classifier ces attaques comme suit :

1. Les problèmes de configuration

Il est très rare que les administrateurs réseaux configurent correctement un programme. En général, ils se contentent d'utiliser les configurations par défaut. Celles-ci sont souvent non sécurisées afin de faciliter l'exploitation du logiciel. De plus, des erreurs peuvent apparaître lors de la configuration d'un logiciel. Une mauvaise configuration d'un serveur peut entraîner l'accès à des fichiers importants, ou mettant en jeu l'intégrité du système d'exploitation. C'est pourquoi il est important de bien lire les documentations fournies par les développeurs afin de ne pas créer de failles **W4**.

2. Attaque par débordement de tampon

Les données d'entrée sont stockées dans des variables. Si le programmeur qui a conçu le programme source a fixé une limite pour l'espace de stockage de la variable (allocation statique au lieu de dynamique), le fait de fournir une donnée d'entrée qui excède la taille prévue provoque un débordement.

La pile[10] contient une information très précieuse : l'adresse de la prochaine instruction à exécuter. L'art du débordement de tampon consiste en fait à remplir la zone de stockage des variables afin que le programme vulnérable lance un code programme injecté par l'intrus en lieu et place du code original ou que l'adresse de la prochaine exécution soit modifiée pour lancer directement une fonction utile au pirate [**2**].

3. Attaque par shellcode

Le terme " shellcode " désigne un programme qui s'appuie sur un débordement de tampon. Il s'agit d'un programme en langage machine qui est exécuté à la place du programme normal, et donc avec ses privilèges [**2**].

Shellcode capable de lancer un shell(comme command.com sous DOS et Microsoft Windows par exemple). Il permettra aussi à une personne mal intentionnée d'exécuter des commandes sur le système distant, pouvant aller jusqu'à sa destruction.

4. Attaque sur les faiblesses des langages

De manière générale, le langage utilisé pour écrire un programme doit tenir compte de nombreux paramètres, tant au niveau de l'efficacité que de la sécurité. De plus, la gestion de la mémoire, la gestion des exceptions ainsi que la gestion des pointeurs sont des sources importantes de programmation si elles ne sont pas masquées et gérées par le langage [**2**].

[10]En informatique, une pile (en anglais stack) est une structure de données fondée sur le principe " dernier arrivé, premier sorti ", ce qui veut dire que les derniers éléments ajoutés à la pile seront les premiers à être récupérés.

. **Erreurs arithmétiques :** elles se produisent lorsque les limitations d'une variable sont dépassées. Ces erreurs génèrent des problèmes d'exécution importants (dépassement de capacité, valeur trop grande pour le type de données, etc.).

. **Scripts intersites (cross-site scripting) :** permettent aux pirates d'exécuter un script [11] malveillant dans un navigateur Web client, d'insérer des balises [12] ¡script¿, ¡object¿, ¡applet¿, etc. mais aussi de voler des informations de session (cookies [13],authentification, etc.) ou encore permettent d'accéder à l'ordinateur client [**2**].

. **Injections SQL** [14] **:** permettent d'ajouter des instructions SQL à une entrée utilisateur afin de tester les bases de données, contourner les autorisations, exécuter plusieurs instructions SQL ou appeler des procédures stockées intégrées [**2**].

. **Faiblesses cryptographiques :** concerne l'utilisation erronée des algorithmes soit en créant ses propres algorithmes, soit par une mauvaise utilisation d'algorithmes existants. Cela touche aussi la sécurisation des clés en termes de stockage non sécurisé, de durée d'utilisation trop longue, etc [**2**].

5. Attaques sur les faiblesses de conception

L'informatique évolue, les applications sont de plus en plus complexes et les délais laissés aux programmeurs et administrateurs sont souvent trop courts. Les risques de failles applicatives sont, de ce fait, très grands et peuvent s'avérer dangereux pour des applications largement répandues, ce qui crée des problèmes dans le code source appelé Bugs, ces derniers peuvent amener à l'exploitation de failles. Il n'est pas rare de voir l'exploitation d'une machine suite à une simple erreur de programmation. On ne peut toutefois rien faire contre ce type de problèmes, si ce n'est attendre un correctif de la part du développeur **W4**.

[11] Un Script est un programme informatique qui ne nécessite pas de compilation avant d'être exécuté (tels que JavaScript, PHP, Python, etc.). Pour fonctionner, les scripts doivent être interprétés par un programme ou un serveur dédié au langage dans lequel ils ont été écrits.

[12] Les balises sont des codes qui englobe un texte ou une image et qui lui donne des caractéristiques à elle. Ces caractéristiques peuvent être la couleur, la grosseur du texte, sous ligné, gras etc. exemple d'une balise ¡b¿ un texte ¡/b¿.

[13] Cookie fichier écrit sur l'ordinateur de l'internaute par le serveur web distant, permettant de sauvegarder un contexte de connexion (produits commandés, préférences, etc.

[14] SQL est un langage informatique ayant pour objet le dialogue avec une base de données relationnelle.

II.4.3 Les programmes malveillants

Un programme ou logiciel malveillant (malware en anglais) est un logiciel développé et utilisé par les pirates dans le but de nuire à un système informatique. Voici les principaux types de programmes malveillants :

1. Les virus

Un virus est une séquence d'instructions qui se fixent aux programmes. Lorsqu'un programme infecté est exécuté, le virus est exécuté et tente de se répliquer en créant (éventuellement modifiées) des copies de lui-même dans d'autres programmes.

Le principal critère de classification d'un morceau de code exécutable comme un virus, c'est qu'il se propage par Contaminer un programme hôte par analogie avec les virus biologiques. Les infections virales se produisent généralement par l'envoi des fichiers infectés, des programmes sur un réseau ou les transporter sur des supports de stockage amovibles [**13**].

Il existe différents types de virus, dont le comportement, la mise en place ou la capacité d'être détectés sont extrêmement variables. Nous détaillons les virus les plus importants, à savoir :

. **Les virus de secteur d'amorçage :** Ces virus ont pour principe de se placer sur le secteur 0 [15] du disque dur. Ce secteur étant lancé par l'ordinateur au démarrage pour initialiser le système d'exploitation, c'est évidemment un emplacement privilégié. Du fait qu'il se lance avant le système d'exploitation, le virus dispose de possibilités supplémentaires pour empêcher sa détection. Il peut, par exemple, détourner des interruptions pour rester invisible d'un antivirus mais également se doter de facilités de reproduction. En règle générale, le contenu par défaut du secteur 0 est copié dans un autre secteur, et le virus s'installe sur le secteur 0 pour être lancé. Par la suite, il charge lui-même le contenu précédent du secteur 0 [**2**].

[15] le secteur 0 ou Master Boot Record est le nom donné au premier secteur adressable d'un disque dur(cylindre 0, tête 0 et secteur 1, ou secteur 0 en adressage logique) dans le cadre d'un partitionnement Intel.Sa taille est de 512 octets.

. **Les virus à infection de fichiers (parasites) :** Les virus parasites ont pour méthode de se placer au sein de programmes exécutables sur le système d'exploitation, par exemple avec un suffixe en .com, .exe ou .sys sous Windows. Ils sont exécutés chaque fois qu'un des fichiers programme infecté est lancé par l'utilisateur. Ces fichiers infectés sont habituellement modifiés pour privilégier le fonctionnement du virus par rapport à celui du programme avant son infection. Ils s'installent au début ou à la fin du programme. Pendant son exécution, le virus se duplique sur d'autres programmes sans que l'utilisateur en ait conscience, voire commence son action nuisible sur le système (altération ou destruction de données, etc.) [**R2**].
. **Les virus furtifs :** Les virus furtifs sont également appelés intercepteurs d'interruptions, car ils prennent le contrôle des interruptions logicielles du système d'exploitation afin de lui faire croire que le système est sain. Lorsqu'un programme émet une requête d'interruption, celle-ci est habituellement redirigée vers la table d'interruptions qui gère les commandes et permet au programme de faire son travail. En cas d'infection par un virus furtif, celui-ci intercepte les requêtes et peut les rediriger où il le désire et effectuer toute opération possible selon son bon plaisir. Cette capacité des virus furtifs à contrôler la table d'interruptions leur permet de se cacher de manière extrêmement efficace, rendant leur détection particulièrement ardue [**2**].
. **Les virus polymorphes (mutants) :** Ces virus ont la capacité de chiffrer ou de modifier leur code de programmation à chaque nouveau clone, ce qui rend chaque copie unique et différente des autres. Les systèmes de détection se trouvent mis en échec par ce type de virus, car il n'existe pas de méthode pour les détecter [**2**].
. **Les virus cryptés :** Ces virus forment une famille très délicate à repérer puisqu'ils sont chiffrés et que les antivirus n'ont pas la possibilité de les déchiffrer pour les détecter. Ces virus doivent pouvoir être déchiffrés pour être mis en œuvre. Ils nécessitent donc un environnement qui leur est adapté. Ils utilisent généralement les techniques de chiffrement utilisées classiquement dans les systèmes d'exploitation qu'ils attaquent [**12**].

. **Les virus Macro :** Les virus Macros sont la plus grande menace à ce jour, ils se propagent lorsqu'un document Microsoft Word, Excel ou PowerPoint contaminé est exécuté. Le but du langage de macro est de pouvoir créer des raccourcis pour effectuer des fonctions courantes, par exemple en une touche enregistrer un document et ensuite l'imprimer.

Louverture d'un document infecté va contaminer le document par défaut de l'application, et ensuite tous les documents qui seront ouverts par cette application. Les documents Word, Excel et PowerPoint étant les documents les plus souvent partagés au sein même d'une entreprise par exemple, ou envoyés par Internet, ceci explique la diffusion exponentielle de ces virus **W3**.

2. Chevaux de Troie (trojan horses)

Ces virus bien connus sont des programmes qui s'introduisent à l'intérieur de l'ordinateur et donnent des renseignements à l'attaquant externe. Le code du cheval de Troie est généralement encapsulé dans un programme système nécessaire au fonctionnement de l'ordinateur [**12**].

Une nouvelle forme de cheval de Troie est apparue depuis quelques années par laquelle le virus prend l'initiative de se connecter à un serveur. L'objectif est de permettre à son concepteur d'atteindre la machine infectée malgré la présence d'un pare-feu, en remontant le flux sortant initié par le cheval de Troie [**2**].

3. Les vers (worms)

Les vers sont le type de virus que l'on rencontre aujourd'hui le plus fréquemment. Ces virus sont de nature différente. Ce sont eux-mêmes des programmes qui transportent des virus. Beaucoup d'attaques sur les messageries s'effectuent en attachant un vers au message. L'utilisateur à qui l'on a fait croire à l'utilité de ce programme l'ouvre et l'exécute. Le virus attaché peut alors commencer à infecter la machine [**12**].

4. 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 indésirées, voire nuisibles [**4**].

5. Portes dérobées

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 [**4**].

6. Attaques par messagerie

En dehors des nombreux programmes malveillants qui se propagent par la messagerie électronique, il existe des attaques spécifiques à celle-ci :

. **Courier électronique non sollicité pourriel :** Le courrier électronique non sollicité pourriel (spam en anglais) consiste en communications électronique massives, notamment de courrier électronique, sans sollicitation des destinataires, à des fins publicitaires ou malhonnêtes. Ce n'est pas à proprement parler du logiciel, mais les moyens de le combattre sont voisins de ceux qui permettent de lutter contre les virus et autres malfaisances, parce que dans tous les cas il s'agit finalement d'analyser un flux de données en provenance du réseau pour rejeter des éléments indésirables [**4**].

Il ne faut jamais répondre à ce type de message car cela indique à l'expéditeur que l'adresse électronique est valide.

. **Le Mail Bombing :** Il consiste à envoyer un nombre faramineux d'emails à un ou plusieurs destinataire, dont l'objectifs est de saturer le serveur de mails, saturer la bande passante du serveur et des destinataires, et comme résultat il est impossible aux destinataires de continuer à utiliser l'adresse électronique.

L'attaque avec mail bombing doit respecter les points suivants : l'attaquant doit spécifier l'adresse qu'il veut faire apparaître en tant qu'émetteur du message, le sujet du message, le nombre de messages à envoyer, le corps du message, l'adresse email de la victime.

L'attaque mail bombing devient plus dangereuse s'il permet d'attacher une pièce jointe qui permet à l'expéditeur d'insérer un virus dans les messages [**9**].

. **L'ingénierie sociale :** Social engineering en anglais, le vol de secret. Par exemple, l'agresseur entre en contact avec la personne qu'il veut usurper en se faisant passer pour un technicien en intervention bloqué dans son travail par une demande d'authentification ou une permission trop forte. Pour peu qu'il soit convaincant, l'agresseur peut obtenir les couples compte/mot de passe ou permissions qu'il désire, voire directement ceux de l'administrateur système [**2**].

. **L'hameçonnage (phishing) :** Le phishing est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes. Le mail usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et invite les internautes à se connecter en ligne par le biais d'un lien hypertexte. Il leurs est demandé de mettre à jour des informations les concernant sur un site Web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.

Dans la mesure où les adresses électroniques sont collectées au hasard sur Internet, le message à généralement peu de chance d'aboutir puisque l'internaute n'est peut-être pas client de la banque dont semble provenir le courriel. Mais sur la quantité des messages envoyés, il arrive que le destinataire soit effectivement client de cet organisme. Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes, leurs données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.). Grâce à ces données les pirates sont capables de transférer directement l'argent sur un autre compte **W5**.

FIG. I.13 – Le phishing.

Conclusion

Nous avons présenté dans ce chapitre une vue générale sur la sécurité informatique et les attaques menaçant cette dernière, ce chapitre n'a pas la prétention de faire une liste exhaustive des attaques mais de couvrir largement les avenues possible.

La sécurité des systèmes informatique est vitale à son bon fonctionnement. Il est donc nécessaire d'assurer sa protection, nous allons décrire dans le chapitre suivant les mécanismes de défiance et de sécurité mise en oeuvre pour assurer cette dernière.

Chapitre II

Les mécanismes de défense et de sécurité

Introduction

Dans un contexte de connectivité croissante des réseaux informatiques, la sécurisation des systèmes d'informations est devenue un enjeu majeur. De nombreux mécanismes ont été développés pour assurer la sécurité de ces derniers, 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.

Dans ce chapitre nous allons présenter les mécanismes de contrôle mettant en place pour permettre la protection des données et des ressources et d'assurer le bon fonctionnement du système.

I Les mécanismes de défense et de sécurité

Un mécanisme est un moyen pour la mise en oeuvre de la politique. La sécurité ne doit jamais reposer sur un seul mécanisme de sécurité. Une imbrication de mécanismes offre une garantie de sécurité bien supérieure.

I.1 Les défenses logicielles

Tous les systèmes de défense utilisent des programmes ou des algorithmes pour gérer essentiellement l'authentification, le cryptage des données et la détection de malwares. Ces défenses logicielles sont mises en place sur des architectures matérielles comme par exemple l'authentification sur une liaison point à point pour se connecter à son FAI (Fournisseur d'Accès Internet), le cryptage sur un tunnel VPN (Virtual Private Network) ou l'antivirus sur les postes de travail.

Dans ce qui suit nous allons décrire les principes de base utilisés dans le cryptage et l'authentification.

I.1.1 Le cryptage

Le but de la cryptographie est de garantir la confidentialité, l'authenticité et l'intégrité des échanges. Il existe à l'heure actuelle deux grands principes de chiffrement (cryptage) : le cryptage symétrique et le cryptage asymétrique.

a. Cryptage symétrique : 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. Ce type de chiffrement est efficace, rapide et peu gourmand en puissance de calcul. La principale difficulté est de trouver un moyen sécurisé pour communiquer la clé aux deux entités. 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[**5**].

FIG. II.1 – Principe du chiffrement symétrique

b. Cryptage asymétrique : 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. 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) [**5**].

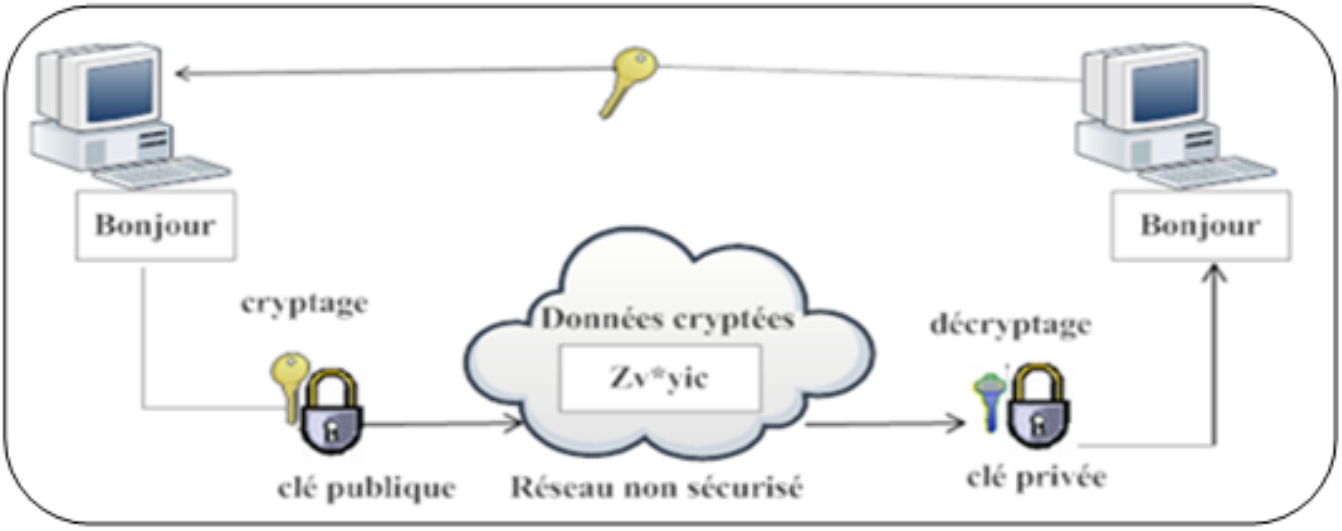


Fig. II.2 – Principe du chiffrement asymétrique.

c. Cryptage hybride : La cryptographie à clé mixte fait appel aux deux techniques précédentes, à clé symétrique et à clé asymétrique. Elle combine de la sorte les avantages des deux.

Lors d'un envoi de données, l'expéditeur chiffre le message avec une clé secrète grâce à un algorithme à clé symétrique. Dans le même temps, il chiffre cette clé secrète avec la clé publique générée par le destinataire. La transmission de la clé secrète peut ainsi se faire de manière fiable et sécurisée.

Le chiffrement d'une clé secrète sur 128 bits avec un algorithme à clé publique est très rapide, compte tenu de la taille de cette clé. Le tout est ensuite transmis au destinataire. Ce dernier déchiffre la clé secrète de l'expéditeur à l'aide de sa clé privée. Le destinataire possède maintenant la clé secrète en clair et peut l'utiliser pour déchiffrer le message [**15**].

I.1.2 La signature numérique

La signature électronique permet d'identifier et d'authentifier l'expéditeur des données.

Elle permet en outre de vérifier que les données transmises sur le réseau n'ont pas subi de modification.

Différentes techniques permettent de signer un message à envoyer. L'une d'elles fait appel aux algorithmes à clé publique, mais les plus utilisées sont les fonctions de hachage [**15**].

. **Le hash :** Un algorithme de hachage est une fonction mathématique qui converti une chaine de caractères d'une longueur quelconque en une chaine de caractères de taille fixe appelée empreinte ou hash ou encore digest. Cette fonction possède deux propriétés essentielles :

1. Elle est irréversible : il est impossible de retrouver le message lorsqu'on connait le hash.
2. Elle est résistante aux collisions : deux messages différents ne produiront jamais le même hash.

Ce type de fonction cryptographique est donc conçu de façon qu'une modification même infime du message initial entraîne une modification du hash. Si un message est transmis avec son hash, le destinataire peut vérifier son intégrité en recalculant son hash et en le comparant avec le hash reçu [**5**].

I.1.3 L'authentification

Une autre méthode pour s'assurer de l'identité de l'expéditeur et d'utiliser un chiffrement symétrique pour chiffrer le hash. Dans ce cas il s'agit d'une authentification et non d'une signature. La clé symétrique utilisée pour vérifier le hash permet aussi de le créer. Si cette clé n'est connue que par les deux partenaires, alors elle permet d'authentifier l'expéditeur du message.

Pratiquement, la clé n'est pas utilisée directement pour chiffrer le hash mais elle intervient lors du calcul du hash. Un hash ainsi généré est appelé un MAC (Message Authentication Code) [**5**].

I.1.4 Les certificats

Une difficulté qui s'impose à la station d'un réseau qui communique avec beaucoup d'interlocuteurs consiste à se rappeler de toutes les clés publiques dont elle a besoin pour récupérer les clés secrètes de session. Pour cela, il faut utiliser un service sécurisé et fiable, qui délivre des certificats. Un organisme offrant un service de gestion de clés publiques est une autorité de certification, appelée tiers de confiance. Cet organisme émet des certificats au sujet de clés permettant à une entreprise de les utiliser avec confiance.

Un certificat est constitué d'une suite de symboles et d'une signature [**16**].

I.1.5 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 [**13**].

Les antivirus peuvent s'installer principalement en deux sortes d'endroits :

- Soit à l'entrée d'un réseau local, là où arrivent les flux en provenance de l'Internet ; certains de ces flux seront filtrés pour y détecter des virus, essentiellement les flux relatifs aux protocoles SMTP (courrier électronique) et HTTP (Web) ;
- Soit sur le poste de travail de l'utilisateur, et là l'antivirus servira généralement à inspecter et désinfecter le disque dur [**4**].

I.2 Les défenses Matérielles

Les défenses Matérielles interviennent au niveau de l'architecture du réseau, directement sur le support sur lequel est stockée l'information à protéger (protection d'une base de donnée centralisée sur le disque dur d'un serveur par exemple), sur les médias servant à transporter cette information (sécurisation du réseau WIFI) et sur les équipements intermédiaires traversées lors du transport (utilisation d'un firewall installer sur le retour d'accès).

I.2.1 Les firewall

Un pare-feu, ou firewall, est, comme son nom l'indique, un équipement dont l'objectif est de séparer le monde extérieur du monde intérieur à protéger. Son rôle est de ne laisser entrer que les paquets dont l'entreprise est sûre qu'ils ne posent pas de problème.

Les pare-feu offrent de nombreuses fonctions, dont la principale est de trier ce qui entre ou ce qui sort et de décider d'une action lorsque la reconnaissance a été effectuée. Les actions peuvent aller du rejet du paquet, à sa compression-décompression, en passant par son examen par un antivirus, son ralentissement, son accélération, etc [**16**].

Ainsi, les machines d'extrémité possèdent également un firewall mais celui-ci est un logiciel (pare-feu Windows ou iptables sous Linux par exemple) et sert à protéger les machines du trafic entrant si le firewall à l'entrée du LAN n'a pas été suffisamment sélectif [**5**].

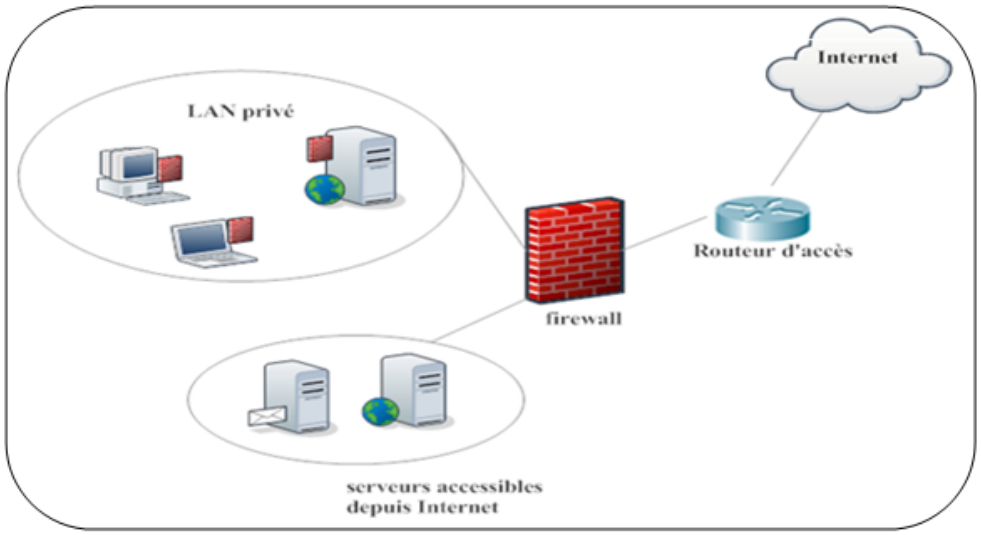


FIG. II.3 – Rôle et situation du firewall

I.2.2 Les systèmes 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.[**R19**]

I.2.3 Le NAT (Network Address Translation)

Ce mécanisme se rencontre fréquemment à la fois en entreprise et chez les particuliers. Il distingue deux catégories d'adresses : les adresses dites publiques, c'est-à-dire visibles et accessibles de n'importe où (on dit aussi routables sur Internet), et les adresses dites privées, c'est-à- dire non routables sur Internet et adressables uniquement dans un réseau local, à l'exclusion du réseau Internet.

Le NAT consiste à établir des relations entre l'adressage privé dans un réseau et l'adressage public pour se connecter à Internet [**17**].

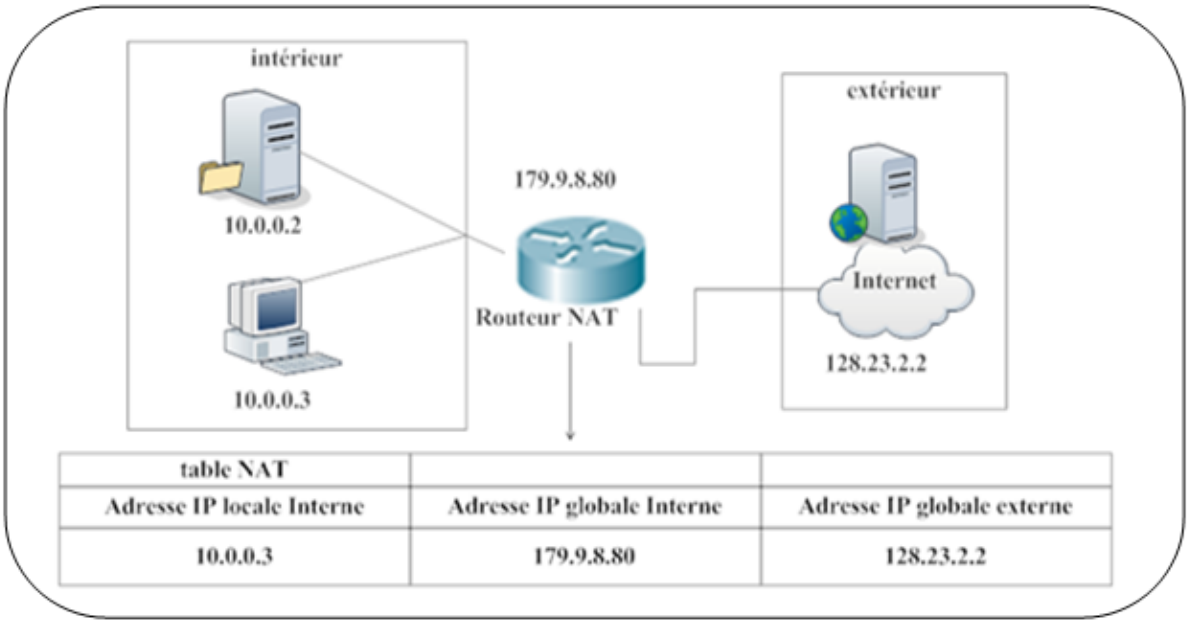


FIG. II.4 – La fonction NAT

Le NAT est aussi un dispositif de sécurité complémentaire au filtrage dans la mesure où elle masque les adresses privée qui ne sont par conséquent plus visibles de l'extérieure. Les firewalls étant généralement intégrés aux routeurs qui possèdent de plus des fonctionnalités de translation [**5**].

I.2.4 La DMZ

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. Cette séparation physique permet d'autoriser les accès Internet à destination des serveurs placés dans la DMZ et non à ceux destinés 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.

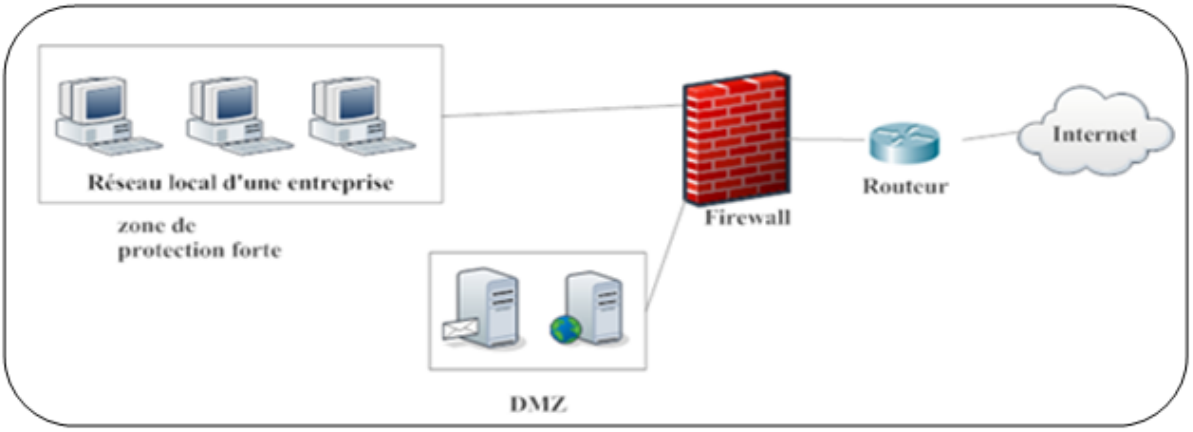


FIG. II.5 – DMZ simple

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.

La DMZ est située entre les deux firewalls (DMZ en sandwich) avec des règles moins restrictives introduites par le premier firewall [**5**].

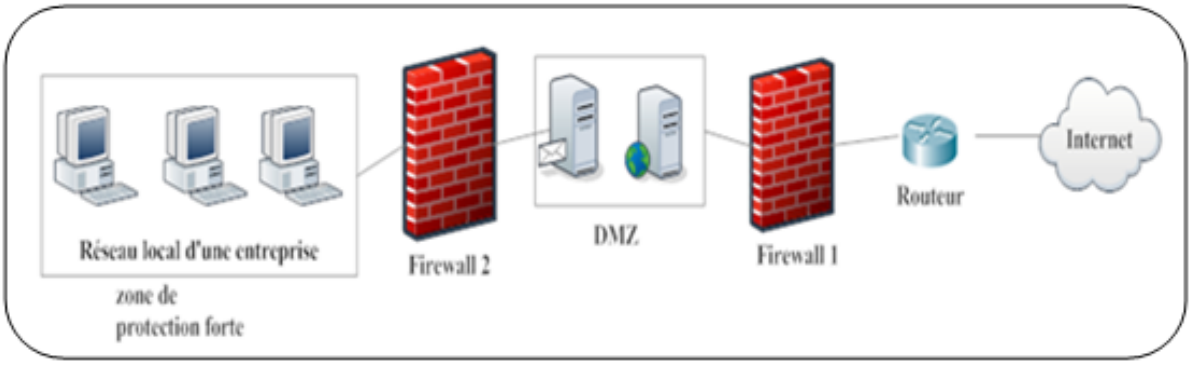


FIG. II.6 – DMZ en sandwich

I.2.5 Les Proxys

Un système mandataire (Proxy) repose sur accès à l'Internet par une machine dédié : le serveur mandataire ou proxy server, qui joue le rôle de mandataire pour les autres machines locales et exécute les requêtes pour les comptes de ces dernières. Un serveur

mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (HTTP, FTP (File Transfer Protocol), SMTP...) et permet de centraliser, donc de sécuriser les accès extérieurs (filtrage[1] applicatif, enregistrement des connexions, masquage des adresses des clients...).

Les serveurs mandataires configurés pour http permettent également le stockage de pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés (Proxy cache) **[5]**.

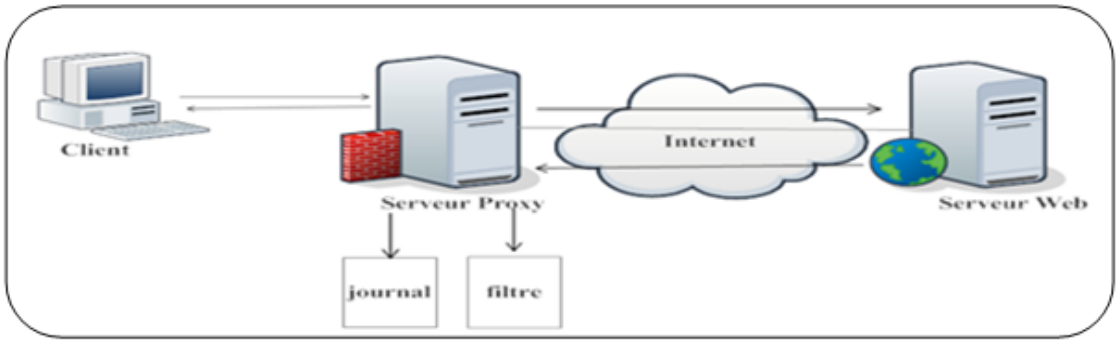


FIG. II.7 – Serveur Proxy

I.2.6 Les VPN

Le réseau privé virtuel (VPN, Virtual Private Network) est un élément essentiel dans les architectures modernes de sécurité. Un VPN est constitué d'un ensemble de LAN privés reliés à travers Internet par un « tunnel » sécurisé dans lequel les données sont cryptées. Les postes distants faisant partie du même VPN communiquent de manière sécurisée comme s'ils étaient dans le même espace privé, mais celui-ci est virtuel car il ne correspond pas à une réalité physique.

Cette solution permet d'utiliser les ressources de connexion Internet plutôt que de mettre en place, comme par le passé, une liaison spécialisée privée entre deux sites qui peut être très coûteuse si les sites sont fortement éloignés. La principale contrainte du

[1]La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur : L'adresse IP Source/Destination, le numéro de port Source/Destination, et bien sur le protocole de niveau 3 ou 4.

VPN est de sécuriser les transmissions, par nature exposées sur le réseau public Internet [5].

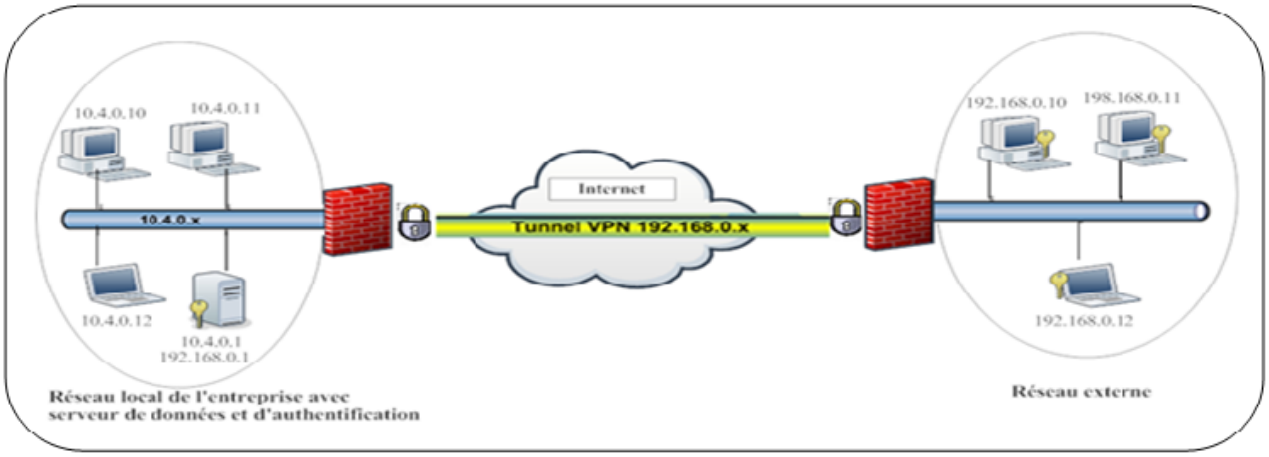


FIG. II.8 – Principe du VPN

I.2.7 La sécurité physique des équipements [11]

La sécurité physique vise à définir des périmètres de sécurité associés à des mesures de sécurité de plus en plus strictes suivant la nature des équipements à protéger. D'une manière générale, tout équipement réseau ou lié au réseau doit être situé dans des locaux dédiés, réservés au personnel habilité (badge, clé, etc.). De plus, tous les accès doivent être archivés à des fins d'investigation en cas d'incident de sécurité.

Tout local contenant des équipements de télécommunications doit être protégé des menaces telles que l'humidité, le feu, les inondations, la température, le survoltage, les coupures de courant, etc. La localisation d'un tel local doit suivre des règles de sécurité précises. Il est préférable qu'il ne soit ni au rez-de-chaussée ni au dernier étage d'un immeuble et qu'il ne se situe pas dans une zone géographique réputée à risque (inondations, orages, etc.).

D'autres règles peuvent être définies selon les critères de sécurité de l'entreprise, telles que le marquage des matériels, un plan de maintenance pour les pièces de rechange, des normes de sécurité centrales, etc. La sécurité physique mérite que chaque entreprise s'y

attarde, afin de définir une politique de sécurité adaptée pour protéger ses équipements les plus critiques.

I.2.8 la sécurisation des réseaux sans fil

Nous intéressons dans cette section à la sécurisation des réseaux sans fil d'entreprise Wi-Fi.

La sécurité d'un réseau local sans fil de type Wi-Fi est plus complexe. Elle intègre l'ensemble des préconisations de sécurité valables pour un réseau filaire avec en plus des préconisations spécifiques au réseau sans fil.

En plus de la sensibilisation des utilisateurs, des bonnes pratiques de protection comprennent impérativement :

a. L'isolement de cette partie de réseau par rapport au réseau d'entreprise grâce à des passerelles sécurisées.

b. La gestion rigoureuse des accès.

c. Les mises à jour logicielles des points d'accès du réseau sans fil, des équipements réseaux et des postes de travail.

d. L'audit périodique et la surveillance active du réseau. Et les recommandations suivantes pour l'installation et l'administration :

- Positionner les points d'accès pour couvrir des zones restreintes, faire attention aux débordements de couverture vers l'extérieur de locaux ou de bâtiments. Réduire la puissance de la borne d'accès si nécessaire.
- Sécuriser les points d'accès, les clients du réseau sans fil et utiliser une liste d'accès contrôlée d'équipements autorisés.
- Changer impérativement la configuration par défaut des équipements Wi-Fi (mot de passe d'administration, SSID (Service Set Identifier)...). C'est la cause principale de vulnérabilité. Désactiver la diffusion du nom de réseau.
- Utiliser, de préférence, des routeurs à la norme 802.11i (ce protocole utilise l'algorithme de chiffrement AES (Advanced Encryption Standard)). Ils authentifient les utilisateurs par un certificat présent sur leur machine (PC ou PDA (Personal

Digital Assistant)) et par un mot de passe.

- S'assurer que les mécanismes de sécurité intégrés et normalisés sont bien activés (authentification, chiffrement WPA (Wi-Fi Protected Access) ou WPA2, liste d'équipements autorisés).
- Augmenter l'authentification : pour mieux gérer ces authentifications, les autorisations et la gestion des comptes utilisateurs, il est recommandé de recourir à un serveur RADIUS (Remote Authentication DialIn User Service).
- Filtrer les adresses MAC (Media Access Control). Les appareils nomades (ordinateur portable, PDA disposent d'une carte réseau associée à une adresse spécifique. Dans la configuration du routeur, souvent associé au point d'Accès, il est recommandé d'activer l'option de filtrage et saisir les adresses MAC de chacun de ces périphériques. Ce qui limitera l'accès au réseau à ces seuls appareils.
- Pour éviter des attaques par déni de service, allouer automatiquement des canaux de diffusion en fonction de leur disponibilité.
- Mettre à jour le logiciel des équipements réseaux, Wi-Fi en particulier.
- Compléter les services de sécurité déjà déployés sur le réseau filaire.
- Mettre en oeuvre les outils et règles d'authentification en fonction de la politique de sécurité de l'entreprise.
- Informer les utilisateurs sur les risques associés à ces matériels et les former aux bonnes pratiques de sécurité.
- Auditer périodiquement le réseau : audit physique (vérification des zones de réception), audit de sécurité (vérification des protections).
- Auditer périodiquement les appareils en service utilisant le Wi-Fi. Ceci pour vérifier quels sont les appareils autorisés.
- Surveiller fréquemment le réseau : surveillance au niveau IP avec un outil de détection d'intrusions.

II Limitations et défauts de sécurité

Les défauts de sécurité d'un système d'information les plus souvent constatés sont [**18**] :

. Installation des logiciels et matériels par défaut.

. Mises à jour non effectuées.

. Mots de passe inexistants ou par défaut.

. Services inutiles conservés (Netbios...).

. Traces inexploitées.

. Pas de séparation des flux opérationnels des flux d'administration des systèmes.

. Procédures de sécurité obsolètes (périmés).

. Authentification faible.

II.1 l'état actif d'insécurité :

c'est-à-dire la non connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple le fait de ne pas désactiver des services réseaux non nécessaires à l'utilisateur).

II.2 l'état passif d'insécurité :

c'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur d'un système ne connaît pas les dispositifs de sécurité dont il dispose [**18**].

Conclusion

Il existe de nombreux mécanismes et outils pour améliorer la sécurité informatique, dans ce chapitre nous avons présenté que quelques briques de base traitant des éléments les plus couramment rencontrés et donner les principaux défauts de cette dernière.

Dans le chapitre suivant nous allons étudier en détaille l'un de ces mécanisme qui est le système de détection d'intrusions.

Chapitre III

Les systèmes de détection d'intrusions

Introduction

Aujourd'hui les systèmes d'information des entreprises connaissent une grande évolution sur les plans d'échange d'informations et l'ouverture sur le monde extérieur, et la mise en place des mesures sécuritaires devient une condition nécessaire, mais pas suffisante pour se protéger des risques présents sur la toile internet.

Ainsi les entreprises commencent à prendre conscience de l'importance de la sécurité informatique et intègrent des mécanismes de sécurité dans leurs architectures réseaux.

En effet, dans ce chapitre nous allons présenter un outil de protection face aux tentatives intrusives des systèmes informatique, les systèmes de détection d'intrusions.

I Définitions

Les systèmes de détection sont conçus pour informer, et dans certains cas pour empêcher, des accès non autorisés ou des intrusions dans les réseaux.

Nous allons définir les systèmes de détection d'intrusions (IDS (Intrusion Detection System)) et les systèmes de prévention d'intrusions (IPS (Intrusion Prevention System)).

I.1 Le système de détection d'intrusions (IDS)

Le concept de système de détection d'intrusions a été introduit en 1980 par James Anderson. Mais le sujet n'a pas eu beaucoup de succès. Il a fallu attendre la publication d'un modèle de détection d'intrusions par Denning en 1987 pour marquer réellement le départ du domaine.

La recherche dans le domaine s'est ensuite développée, le nombre de prototypes s'est énormément accru. La détection d'intrusion est devenue une industrie mature et une technologie éprouvée : à peu près tous les problèmes simples ont été résolus, et aucune grande avancée n'a été effectuée dans ce domaine ces dernières années, les éditeurs de logiciels se concentrant plus perfectionner les techniques de détection existantes.

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 où 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 à une connexion suspecte [**20**].

I.2 Le système de prévention d'intrusions (IPS)

IPS est un autre acronyme à la mode qui a fait son apparition au début des années 2000. L'idée sous-jacente de ce concept est qu'un système de détection des intrusions peut certes détecter des attaques contre un réseau mais sa fonction de détection, par nature passive, ne peut empêcher l'intrusion. Cela a mené certaines entreprises utilisatrices à se poser la question : pourquoi investir dans une solution de détection des intrusions si on ne peut pas empêcher l'intrusion ? La réaction des fournisseurs a été prompte et c'est ainsi que l'acronyme IPS a vu le jour.

Un système de prévention des intrusions est un ensemble de composants logiciels et/ou matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système.

Le qualificatif " détectée " de la définition est important car la notion de prévention des intrusions développée ici implique que la détection a été faite au préalable. En absence de ce qualificatif, la notion d'IPS est trop vague et des systèmes tels que les firewalls ou les logiciels de filtrage pourraient être qualifiés d'IPS. Les IPS est un sur ensemble des IDS dans la mesure où la notion de détection est un pré requis nécessaire à tout système de prévention.

Les premiers produits IPS apparus sur le marché sont en fait des IDS auxquels l'éditeur a adjoint des fonctionnalités de réaction automatique à des attaques (tels que Snort, RealSecure ou Dragon). A partir de 2002, certaines start-ups [1] comme Okena, Entercept ou Intruvert ont commencé à proposer sur le marché des solutions qui ont été conçues pour bloquer nativement les intrusions. Bien que les technologies soient encore jeunes, le rachat de ces jeunes pousses montre l'intérêt des éditeurs pour ces nouvelles tendances en matière de gestion des intrusions [**21**].

I.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 à mesure que de nouvelles menaces sont identifiées, soit un système à approche comportementale qui analyse les différences avec le niveau de fonctionnement normal du réseau qui a été défini par l'administrateur. 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.

Un Intrusion Prevention System (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 **W15**.

II Nécessité d'un système de détection d'intrusion

Un système de détection d'intrusion consiste à identifier des attaques ou des violations de sécurité issues du réseau de surveillance et des activités hébergées. Il peut être comparé

[1] La startup ou jeune pousse est une jeune entreprise à fort potentiel de croissance et qui fait la plupart du temps l'objet de levée de fonds. On parle également de startup pour des entreprises en construction qui ne se sont pas encore lancées sur le marché commercial (ou seulement à titre expérimental).

à une alarme domestique contre les cambrioleurs [**36**].

Les systèmes de détection d'intrusions (IDS) sont des compléments indispensables aux mécanismes de sécurité préventifs présents dans les systèmes informatiques et les réseaux [**19**].

III Présentation d'un système de détection d'intrusions

Dans cette section nous allons décrire les systèmes de détection d'intrusions.

III.1 Description d'un IDS

Plusieurs schémas ont été proposés pour décrire les composants d'un système de détection d'intrusions. Parmi eux, nous avons retenu celui issu des travaux d'Intrusion Detection exchange format Working Group (IDWG [2]) de l'Internet Engineering Task Force (IETF), car il résulte d'un large consensus parmi les intervenants du domaine [**24**]. L'objectif des travaux du groupe IDWG est la définition d'un standard de communication entre certains composants d'un système de détection d'intrusions. La figure suivante reproduit ce modèle et permet d'introduire un certain nombre de concepts :

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

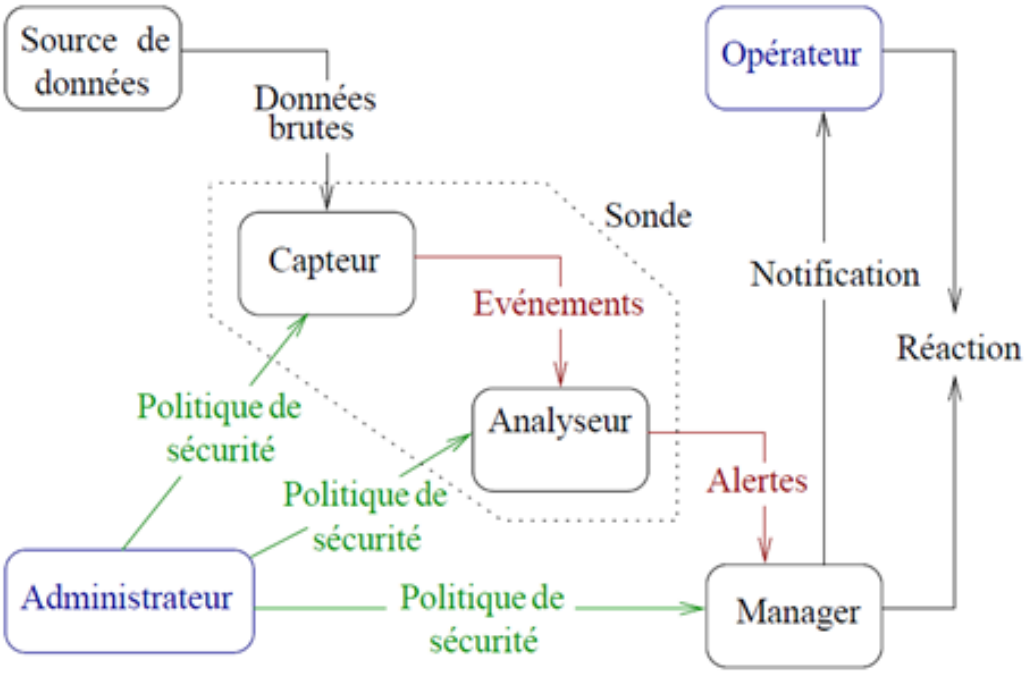


FIG. III.1 – Architecture IDWG d'un système de détection d'intrusions.

L'architecture IDWG d'un système de détection d'intrusions contient des capteurs qui envoient des événements à un analyseur. Un ou des capteurs couplés avec un analyseur forment une sonde. Une sonde envoie des alertes vers un manager qui la notifie à un opérateur humain [**24**].

III.1.1 Les différents éléments de ce modèle

différents éléments de ce modèle sont [**22**] :

- **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 œuvre l'approche choisie pour la détection (comportementale ou par scénarios), 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.

. **Evénement :** 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.
. **Sonde :** un ou des capteurs couplés avec un analyseur.
. **Source de données :** dispositif générant de l'information sur les activités des entités du système d'information.

Dans ce modèle, on peut voir le processus complet de la détection ainsi que le cheminement des données au sein d'un IDS. L'administrateur configure les différents composants (capteur(s),analyseur(s), manager(s)) selon une politique de sécurité bien définie. Les capteurs accèdent aux données brutes, les filtrent et les formatent pour ne renvoyer que les événements intéressants à un analyseur. Les analyseurs utilisent ces événements pour décider de la présence ou non d'une intrusion et envoient dans le cas échéant une alerte au manager, qui notifie l'opérateur humain, une réaction éventuelle peut être menée automatiquement par le manager ou manuellement par l'opérateur [**22**].

Donc un IDS a quatre fonctions principales [**6**] : l'analyse, la journalisation, la gestion et l'action.

a. Analyse : analyse des journaux du système pour identifier des intrusions dans la masse de données recueillie par l'IDS. Il y a deux méthodes d'analyse : une basée sur les signatures d'attaques et l'autre sur la détection d'anomalies (comportementale).
b. Journalisation : enregistrement des événements dans un fichier de log. Exemple d'événement : arrivée d'un paquet, tentative de connexion.

c. Gestion : les IDS doivent être administrés de manière permanente. On peut assimiler un IDS à une caméra de sécurité.

d. Action : alerter l'administrateur quand une attaque dangereuse est détectée. La détection d'intrusions utilise un vocabulaire bien défini (n'apparaissant pas directement sur le modèle de la figure précédente) que nous utiliserons tout au long de ce chapitre [**22**] :

. **Corrélation :** c'est l'interprétation conceptuelle de plusieurs événements (alertes) visant à leur assigner une meilleure sémantique et à réduire la quantité globale d'événements (d'alertes).

. **Détection d'intrusions :** processus logiciel de recherche de traces laissées par une intrusion dans les données produite par une source.

. **Exploit :** terme utilisé pour désigner un programme d'attaque.

. **Faux positif :** alerteen l'absence d'attaque (fausse alerte).

. **Faux négatif :** absence d'alerteen 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.

III.2 Type des 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.

III.2.1 IDS Réseaux (ou NIDS : Network IDS)

Les IDS réseaux analysent en temps réel le trafic qu'ils aspirent à l'aide d'une sonde (carte réseau en mode promiscuous[3]. Ensuite, les paquets sont décortiqués puis analysés.

[3]Promiscuous mode (traduit mode promiscuité), se réfère à une configuration de la carte réseau, qui permet à celle-ci d'accepter tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés. Ce

Il est fréquent de trouver plusieurs IDS sur les différentes parties du réseau. On trouve souvent une architecture composée d'une sonde placée à l'extérieur du réseau afin d'étudier les tentatives d'attaques et d'une sonde en interne pour analyser les requêtes ayant traversé le pare-feu [**32**].

a. Points forts

- 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 [**10**].

b. Points faibles

- L'IDS basé réseau ne peut pas fonctionner dans des environnements cryptés.
- Ce type d'IDS ne permet pas d'assurer si une tentative d'attaque est couronnée de succès [**10**].

III.2.2 IDS Systèmes (ou HIDS Host IDS)

Les IDS systèmes analysent le fonctionnement et l'état des machines sur les quelles ils sont installés afin de détecter les attaques en se basant sur des démons (tels que syslogd [4] par exemple). L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levées [**32**].

a. Points forts

- 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 (ex : Cheval de Troie) [**10**].

b. Points faibles

mode est une fonctionnalité généralement utilisée pour écouter le trafic réseau.

[4]Le démon syslogd permet d'enregistrer diverses activités du système, comme les messages de déboguage ou les avertissements affichés par le noyau. Son fichier de configuration, /etc/syslog.conf, permet de spécifier l'endroit où les informations doivent apparaître.

- La vulnérabilité aux attaques du type déni de service puisque l'IDS peut résider dans l'hôte cible par les attaques.
- 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 [**10**].

III.2.3 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, on comprend que les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi. Cela permet de communiquer et d'extraire des alertes plus pertinentes.

Les avantages des IDS hybrides sont multiples :

- 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 [**32**].

III.3 Architecture d'un système de détection d'intrusions

Un IDS est constitué d'un ou plusieurs capteurs, un ou plusieurs analyseurs et un ou plusieurs managers.

Le nombre et l'emplacement de ces composants définissent l'architecture de l'IDS. Selon l'architecture, la collection, d'une part, l'analyse des données, d'une autre part, l'IDS peut être centralisé ou distribué.

III.3.1 L'architecture centralisée (monolithique)

Les premières mises en œuvre des systèmes de détection d'intrusions ont employé une architecture monolithique sous laquelle les données rassemblées seront analysées à un point central. Puisque le contrôle de l'activité des utilisateurs d'un seul hôte ne révèle pas les attaques impliquant des hôtes multiples. L'IDS basé réseau a été développé, qui analyse le trafic de réseau pour déduire les anomalies venant du réseau.

Bien qu'un IDS basé réseau avec un serveur central a montré des résultats prometteurs pour des réseaux à petite échelle. Cependant, cette approche ne peut pas supporter un grand réseau à cause de la quantité énorme des données des différents hôtes qui doivent être analysée par le serveur central, ce qui engendre une dégradation sévère des performances de réseau [**10**].

III.3.2 L'architecture hiérarchique

Cette approche a été proposée pour surmonter les problèmes de l'approche monolithique. Elle est caractérisée par l'existence des secteurs de contrôle hiérarchiques. Chaque IDS contrôle un secteur avec l'élimination du transfert des données d'audit rassemblées par les hôtes locaux à un point central. Chaque IDS à n'importe quel niveau de contrôle exécute une analyse locale et envoie ses résultats d'analyse au niveau suivant dans la hiérarchie.

L'approche hiérarchique montre la meilleure incrémentabilité scalability [5] en permettant des analyses locales aux secteurs de contrôle distribués. Cependant, les problèmes vus précédemment demeurent toujours. En plus, le changement de la topologie du réseau cause un changement aussi bien dans la hiérarchie de réseau et dans les mécanismes de rassemblement des rapports d'analyse locaux. Ainsi, la difficulté de détecter les attaques qui visent le niveau le plus haut de la hiérarchie [**10**].

[5] scalability désigne la capacité d'un produit à s'adapter à un changement d'ordre de grandeur de la demande (montée en charge). En particulier sa capacité à maintenir ses fonctionnalités et ses performances en cas de forte demande.

III.3.3 l'architecture distribuée (coopérative)

Cette approche a été suggérée pour résoudre les problèmes de l'approche précédente. Elle essaye de distribuer les responsabilités d'un serveur central à un nombre de systèmes de détection d'intrusions coopératifs. La différence de cette approche avec l'approche hiérarchique est qu'il n'y a aucune hiérarchie entre les IDS distribués ce qui signifie que l'échec de n'importe quel IDS n'empêche pas la détection d'attaques coordonnées [**10**].

III.4 Méthodes de détection

Deux approches ont été proposées : l'approche comportementale et l'approche par scénario. La première se base sur l'hypothèse que l'on peut définir un comportement "normal" de l'utilisateur et que toute déviation par rapport à celui-ci est potentiellement suspecte. La seconde s'appuie sur la connaissance des techniques employées par les attaquants : on en tire des scénarios d'attaque et on recherche dans les traces d'audit leur éventuelle survenue.

III.4.1 Les IDS à signatures (ou à scénarios)

Les détecteurs d'intrusion par signature reposent sur la création a priori d'une base de motifs représentant des scénarios d'attaque connus au préalable. Cette base de signature est ensuite utilisée, le plus souvent en temps réel, sur les informations fournies par les sondes de détection. C'est un système de reconnaissance de motifs qui permet de mettre en évidence dans ces informations la présence d'une intrusion connue de la base de signature [**33**].

Il peut s'agir d'une chaîne alphanumérique, d'une taille de paquet inhabituelle, d'une trame formatée de manière suspecte, etc [**21**].

a. Recherche de motif (Pattern matching)

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.

Un exemple de chaînes de caractères malicieuses est la chaîne "/scripts/iisadmin/default.htm" qui vise à accéder à la page d'administration d'un serveur Web IIS (Internet Information Services) [**32**].

Le principal inconvénient de cette méthode est que seules les attaques reconnues par les signatures seront détectées. Il est donc nécessaire de mettre à jour régulièrement la base de signatures.

Un autre inconvénient est que les motifs sont en général fixes. Or une attaque n'est pas toujours identique à 100

b. Analyse de protocoles

C'est une méthode complémentaire à la précédente, elle analyse les flux selon deux axes :

. Vérification de la conformité du trafic avec les RFC (Requests For Comments)liées aux différents protocoles utilisés.
. Observation des champs et paramètres suspects liés à certains protocoles de façon à s'assurer que ceux-ci ne sont pas utilisés à des fins malicieuses par un attaquant. Ceci est à distinguer de la vérification de conformité car il est bien rare que les éditeurs et constructeurs respectent à la lettre les RFC et autres normes. Les nombreuses améliorations apportées par ces éditeurs découlent souvent d'une interprétation des RFC.

La détection peut être faite en utilisant des techniques à base de pattern matching ou de règles d'analyse implémentées dans un préprocesseur spécifique à chaque protocole. Avantages de cette méthode :

. L'analyse protocolaire permet de détecter des attaques inconnues.
. De plus, elle ne nécessite pas de développer de signatures spécifiques.

Inconvénients de cette méthode :

. Cette méthode nécessite l'écriture de décodeurs spécifiques à chaque protocole.

. Cette technique a tendance à générer plus de faux positifs. Cela est d'autant plus vrai que l'implémentation se contente de vérifier la conformité aux RFC, en effet, de nombreux constructeurs et éditeurs ont souvent tendance à améliorer les fonctionnalités des RFC afin de mieux les adapter à leur offre [**34**].

c. Analyse heuristique et détection d'anomalies Les méthodes dites de détection d'anomalies sont encore plus difficiles à catégoriser que les deux précédentes. Ces méthodes relèvent à la fois de l'analyse protocolaire et de l'approche comportementale (détailler ci-dessous). La détection d'anomalies s'appuie grandement sur l'analyse heuristique.

Les méthodes d'analyse heuristique sont issues des technologies utilisées par l'antivirus. Le principe est de détecter les virus d'origine inconnue par leur mode de fonctionnement et non pas au moyen d'une signature alphanumérique.

L'approche par signature possède un certain nombre d'avantages et d'inconvénients :

– **Les avantages**
  . L'analyse basée connaissance est très efficace pour la détection d'attaque avec un taux très bas des alarmes de type faux positif.
  . Les alarmes générées sont significatives [**10**].
– **Les inconvénients**
  . Cette analyse basée connaissance permet seulement la détection des attaques qui sont connues au préalable. Donc, la base de connaissances doit être constamment mise à jour avec les signatures de nouvelles attaques.
  . Le risque que l'attaquant peut influencer sur la détection après la reconnaissance des signatures [**10**].

III.4.2 Les IDS comportementaux

Les détecteurs d'intrusion comportementaux reposent sur la création d'un modèlede référence représentant le comportement de l'entité surveillée en situation de fonctionnement normal. Ce modèle est ensuite utilisé durant la phase de détection afin de pouvoir mettre en évidence d'éventuelles déviations comportementales. Pour cela, le comporte-

ment de l'entité surveillée est comparé à son modèle de référence.

Une alerte est levée lorsqu'une déviation trop importante vis-à-vis de ce modèle de comportement normal est détectée. Le principe de cette approche est de considérer tout comportement n'appartenant pas au modèle de comportement normal comme une anomalie symptomatique d'une intrusion ou d'une tentative d'intrusion [**33**].

a. Approche probabiliste

Des probabilités sont établies permettant de représenter une utilisation courante d'une application ou d'un protocole. Toute activité ne respectant pas le modèle probabiliste provoquera la génération d'une alerte.

Exemple : Avec le protocole HTTP, il y a une probabilité de 0.9 qu'une commande GET soitfaite après une connexion sur le port 80. Il y a ensuite une probabilité de 0.8 que la réponse àcette commande GET soit " HTTP/1.1 200 OK " **W4**.

Une alerte pourra être générée quand le nombre d'événements ne correspondant pas aux probabilités définies aura dépassé un certain seuil sur une période donnée. Il est capital pour l'administrateur d'un système utilisant cette méthode de suivre l'évolution du gabarit dans le temps et de s'assurer que celui-ci se conforme aux habitudes de travail des utilisateurs, sans quoi le taux de faux positifs risque d'être très élevé [**21**].

b. Approche statistique

Cette méthode consiste en un calcul de la variation (en fonction du temps) de l'utilisation d'un certain nombre de ressources, à l'aide d'outils statistiques [**34**].

- Le taux d'occupation de la mémoire
- L'utilisation des processeurs
- La valeur de la charge réseau
- Le nombre d'accès à l'Intranet par jour [**32**].

La constatation d'un changement dans la variation conduit au déclenchement d'une alerte. Par exemple, "un trafic réseau anormalement faible en matinée signale très probablement une panne ou une attaque de type déni de service" [**34**].

c. Immunologie

Cette analogie avec l'immunologie biologique consiste à construire un modèle de comportement normal des services (et non des utilisateurs) au travers des courtes séquences d'appels systèmes qui sont considérées comme représentatives de l'exécution normale des services considérés. L'objet de la méthode consiste donc à observer les services pendant un temps suffisamment représentatif de manière à établir une base des séquences d'appels normales [**21**].

L'approche comportementale possède un certain nombre d'avantages et d'inconvénients :

- **Les avantages**
  - L'analyse comportementale n'exige pas des connaissances préalables sur les attaques.
  - Elle permet la détection de la mauvaise utilisation des privilèges.
  - Elle permet de produire des informations qui peuvent être employées pour définir des signatures pour l'analyse basée connaissance [**10**].
- **Les inconvénients**
  - Les approches comportementales produisent un taux élevé des alarmes de type faux positif en raison des comportements imprévisibles d'utilisateurs et des réseaux.
  - Ces approches nécessitent des phases d'apprentissage pour caractériser les profils de comportement normaux.
  - Les alarmes générées par cette approche ne sont pas significatives [**10**].

III.5 Comportement 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.

III.5.1 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) [**25**].

III.5.2 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 [**10**].

III.6 Les outils disponibles

III.6.1 Critères de choix

Aujourd'hui les systèmes de détection d'intrusion sont réellement devenus indispensables lors de la mise en place d'une infrastructure de sécurité opérationnelle. Ils s'intègrent donc toujours dans un contexte et une architecture qui imposent des contraintes pouvant être très diverses. C'est pourquoi il n'existe pas de grille d'évaluation unique pour ce type d'outil. Pourtant un certain nombre de critères peuvent être dégagés, ceux-ci devront nécessairement être pondérés en fonction du contexte de l'étude.

Les systèmes de détection d'intrusions actuels tendent à garantir les cinq propriétés suivantes [**20**] :

. **Exactitude de détection :** elle se traduit par une détection parfaite des attaques avec un risque minimal de faux positifs.
. **Performance :** une détection rapide des intrusions avec une analyse approfondie des événements est indispensable pour mener une détection efficace en temps réel.
. **Complétude :** une détection exhaustive des attaques connues et inconnues.
. **Tolérance aux fautes :** les systèmes de détection d'intrusions doivent résister aux attaques ainsi qu'à leurs conséquences.
. **Rapidité :** une analyse rapide des données permet d'entreprendre instantanément les contre-mesures nécessaires pour stopper l'attaque et protéger les ressources du réseau et du système de détection d'intrusion.

L'efficacité d'un système de détection d'intrusions est déterminée par les mesures ci-dessus [**10**].

III.6.2 Quelques outils

Voici quelques exemples de systèmes IDS disponible sur le marché. Tous sont appelés " IDS " mais l'on trouve des disparités assez importantes entre les fonctionnalités des produits. Selon les entreprises, il faut également tenir compte de leurs capacités de traitement de ces produits en termes de bande passante.

a. ISS RealSecure

La société ISS (Internet Security Systems) [6], est l'un des précurseurs à l'origine des premiers systèmes IDS. Elle possède donc une grande expérience de ces produits et une certaine légitimité historique [**26**].

RealSecure est la solution d'ISS qui délivre en temps réel une détectionet une protection contre les intrusions à toutes les stations de travail connectées à votre réseau, y compris aux postes distants.

RealSecure combine en un seul agent trois fonctionnalités essentielles :
. un moteur de détection d'intrusion,

[6] Http ://www.iss.net/

. un firewall personnel,
. un module de contrôle d'applications et de communications [**27**].

Une version d'IDS hybride est possible et désormais supportée par différentes offres commerciales. Même si la distinction entre HIDS et NIDS est encore courante, certains HIDS possèdent maintenant les fonctionnalités de base des NIDS. Les IDS ISS RealSecure se nomment aujourd'hui "IDS hôte et réseau" [**28**].

b. Cisco IDS

Cisco IDS fournit une solution de sécurité complète, omniprésente pour lutter contre les intrusions, les vers Internet malveillants, ainsi que la bande passante et les attaques applicatives. Cisco IDS est un composant de sécurité dynamique de bout-en-bout.Cisco IDS a été conçu à partir du sol en place pour soutenir la plus large gamme de déploiements de réseaux, des petites entreprises aux plus grands environnements d'entreprise et les fournisseurs de service réclament des solutions rapides, souples. Cisco IDS utilise des techniques de détections hautement innovantes et sophistiqués, le protocole d'analyse, la détection heuristique et de détection d'anomalie, qui fournissent une protection complète contre une variété de menaces informatiques connus et inconnus. Offrir le meilleur coût de possession avec le réseau intégrée et des solutions basées sur le matériel, Cisco réduit le coût de la protection d'intrusion avancé.

La gamme complète des leaders du marché IDS appareils de la gamme Cisco 4200 offrent une protection d'intrusion performances optimisées au sein d'une solution intégrée, clé en main, nous citons :

. **Cisco IDS 4235 :** est conçu pour les déploiements de fournir une protection dans les environnements commutés. (C'est l'IDS simulé dans notre mémoire).
. **Cisco IDS 4250 :** prend en charge des performances inégalées à 500 Mbps et peut être utilisé pour protéger les sous-réseaux Gigabit et de déplacement de la circulation qui sont utilisées pour agréger le trafic de nombreux sous-réseaux.

. **IDS Host Sensor Cisco :** garanties l'ensemble du serveur en empêchant les attaques, comme les vers et les débordements de tampon. En bloquant ces attaques, le capteur de Host IDS Cisco diminue de manière significative les temps d'arrêt, réduit les coûts liés à la sécurité et protège les actifs critiques.
. **Pare-feu PIX de Cisco 500 :** en lui intégrant des fonctionnalités IDS pour fournit une protection contre une variété d'attaques basées sur le réseau commun.

Cisco offre une vaste gamme de gestion de la sécurité de classe entreprise globale et les options de suivi pour Cisco IDS répondre à toute échelle de déploiement et des exigences **W16**.

c. Enterasys DRAGON

Édité par Enterasys Networks, est un système de détection des intrusions considéré comme des leaders du marché du fait de ses performances, ses facultés d'adaptation à tout type d'environnement et ses capacité d'analyse.

Les solutions Dragon sont constituées de sondes NIDS (Network Sensor), d'agents HIDS (Host Sensor) et d'un système de management qui assure les fonctions d'exploitation des événements de la suite Dragon.

Le Network Sensor est un NIDS disponible en version logicielle ou en boîtier dédié. Depuis la version 6, Enterasys décline les appliances et les logiciels en trois versions selon la bande passante à analyser. Les versions matérielles sont adossées à leur équivalent logiciel.

Le Host Sensor est un agent HIDS qui détecte les attaques contre le système sur lequel il est installé en contrôlant les journaux systèmes et d'audit ainsi qu'en utilisant des mécanismes d'analyse de signatures.

L'Enterprise Management System (EMS) est le composant qui permet d'exploiter de d'administrer la solution globale.

Dragon détecte les intrusions sur l'ensemble de l'infrastructure informatique où qu'elles se produisent et permet d'avoir ainsi une visibilité globale sur le système d'informations. Cela permet notamment d'optimiser les ressources humaines nécessaires à l'analyse des journaux issus des différents firewalls ou serveurs Web en fédérant tous ces journaux au niveau d'une console Dragon unique qui analysera automatiquement les données afférentes [**21**].

d. SNORT

SNORT est un IDS particulièrement répondu car fourni en open source sous licence GNU [7] GPL (General Public Licence). Il est donc gratuit et facile à se procurer. Outre sa gratuité, son avantage est qu'il dispose d'une très grosse base de signatures réalisée par la communauté des utilisateurs (plus de 2000 signatures).

C'est également le gage d'obtenir rapidement des mises à jour de la base dès qu'une nouvelle menace est signalée. Il a été conçu à l'origine pour le système Linux mais il a également été porté sous Windows. On trouve dans le commerce plusieurs livres dédiés à l'installation et à l'utilisation de SNORT.

SNORT est généralement utilisé en conjonction avec un autre logiciel open source nommé ACID (Analysis Console for Intrusion Databases) qui est la console de gestion et d'analyse.

Pour ce qui est des points négatifs, on peut néanmoins considérer que SNORT est moins puissant en termes de moteur d'analyse que des solutions commerciales telles que celles d'ISS ou de Cisco.

Par ailleurs, bien que la base de signatures soit étendue, elle nécessite un travail constant de la part de l'administrateur qui doit les télécharger manuellement. Il n'y a pas de procédure de mise à jour automatique [**26**].

[7] GNU est un système d'exploitation libre lancé en 1984. Son nom signifie en anglais GNU's Not UNIX, (littéralement, GNU n'est pas UNIX). Il reprend les concepts et le fonctionnement d'UNIX.Le système GNU permet l'utilisation de tous les logiciels libres, pas seulement ceux réalisés dans le cadre du projet GNU.

III.7 Les caractéristiques d'un IDS

Les caractéristiques souhaitées d'un système de détection d'intrusion sont :

. Capacité de fonctionner continuellement avec un minimum d'invention humaine.

. Difficulté pour un attaquant de le désactiver ou modifier sa configuration.

. Capacité de se contrôler lui-même et de détecter s'il vient de faire l'objet de manipulation de la part d'un attaquant.

. Utilisation minimale de ressources (de calcul, de stockage, etc.) sur le système sur lequel il est installé.

. Capacité d'accepter des mises à jour et des modifications de configuration pour rendre compte des nouvelles dispositions de la politique de sécurité et les changements susceptibles de s'opérer dans l'organisation (nouvelles acquisitions, restructuration, etc.).

. Facilité et simplicité de déploiement : facilité d'installation et de configuration portabilité, etc.

. Interopérabilité avec d'autres systèmes et outils de la sécurité informatique [**20**].

. Il doit être tolérant aux fautes c'est-à-dire qu'il doit être capable de retrouver son état initial de fonctionnement après un crash causé soit par une manipulation accidentelle soit par des activités émanant de personnes malintentionnées [**36**].

. Lorsque le nombre de systèmes à superviser augmente et donc que les attaques potentielles augmentent également, nous pouvons alors attendre de l'IDS les caractéristiques suivantes :

  - Il doit être capable de superviser un nombre important de stations tout en fournissant des résultats de manière rapide et précise.
  - Il doit fournir "un service minimum de crise" c'est-à-dire que si certains composants de l'IDS cessent de fonctionner, les autres composants doivent être affectés le moins possible par cet état de dégradation.
  - Il doit autoriser des reconfigurations dynamiques. Si un grand nombre de stations est supervisé, il devient pratiquement impossible de redémarrer l'IDS sur tous les hôtes lorsque l'on doit effectuer un changement [**36**].

. La possibilité de générer des rapports simples ou exhaustifs, sous divers formats [**9**].

III.8 Les principales tâches d'un IDS

Un IDS permet de repérer des anomalies dans le trafic réseau comme suit :

. Dans le cas d'une attaque ciblée, l'IDS peut :
  - Détecter les tentatives de découvertes du réseau, qui sont la phase préparatoire à une attaque proprement dite (vu dans le chapitre I).
  - Détecter dans certains cas, si l'attaque a réussi ou non (par exemple réponse login acceptée).
  - Détecter le Déni de Service (DoS).

. Dans le cas d'une attaque d'ampleur de type " ver ", ce dernier génère un trafic réseau qui peut être reconnu par un IDS. Dans ce cas l'IDS peut :
  - Détecter le niveau d'infection du système informatique et les zones réseaux touchées.
  - Repérer rapidement les machines infectées.

. Dans le cas d'un réseau mal configuré l'IDS Analyse l'ensemble des messages de type maintenance du réseau (protocole ICMP) et détecte les problèmes de configuration, qui autrement finiraient par rendre le réseau peu performent, voir instable.

. Des systèmes utilisant de vieux protocoles peu sécurisés et non autorisés comme Telnet, ftp dans ce cas les buts de l'IDS sont nombreux :
  - Collecter les traces d'intrusion pour servir de preuves s'il y a un processus légal de lance.
  - Alerter de façon centrale pour toutes les attaques.
  - Réagir aux attaques et corriger les problèmes éventuels [**6**].

Les HIDS présente un avantage considérable par rapport à un NIDS dans le cas où le trafic est crypté. En effet, un NIDS n'a pas connaissance des clés de cryptage et ne peut appliquer ses algorithmes de détection au niveau des données chiffrées. La détection est effectuée à l'extrémité de la chaine de communication, une fois le flux est décrypté. Ceci est réalisé en mettant en œuvre un agent HIDS directement sur le serveur cible. Les flux chiffrés sont ainsi décodés par la cible et transmis ensuite au monteur d'analyse de l'HIDS [**21**].

IV 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 identifiez les composants critiques qu'ils seront probablement visés par les attaquant, donc le placement des IDS va dépendre de la politique de sécurité menée. 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, la meilleure possible 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 :

- dans la zone démilitarisée (attaques contre les systèmes publics),
- dans le (ou les) réseau privé (intrusions vers ou depuis le réseau interne),
- sur la patte extérieure du firewall (détection de signes d'attaques parmi tout le trafic entrant et sortant, avant que n'importe quelle protection intervienne).

Il y a plusieurs solutions pour le positionnement de sondes réseaux. Nous allons déterminer les plus connues et les plus importantes.

Il peut être intéressant de positionner les sondes pour étudier l'efficacité des protections mises en place. Par exemple dans un réseau se cachant derrière un firewall, nous mettrons une sonde côté extérieur du firewall, et une autre côté intérieur du firewall. La première sonde permet de détecter les tentatives d'attaques dirigées contre le réseau surveillé. La seconde sonde va remonter les attaques (préalablement détectées par la première sonde) qui ont réussi à passer le firewall. On peut ainsi suivre une attaque sur un réseau, voir si elle arrive jusqu'à sa victime, en suivant quel parcours.

Il est aussi intéressant de définir des périmètres de surveillance d'une sonde. Ce sera en général suivant un domaine de collision, ou sur des entrées uniques vers plusieurs domaines de collision (par exemple à l'entrée d'un commutateur). Par cette méthode, nous réduisons

le nombre de sondes, car il n'y a pas de doublons dans la surveillance d'une partie du réseau. Une alerte n'est remontée qu'une seule fois ce qui allège d'autant l'administration des IDS.

En ce qui concerne les sondes HIDS, l'idéal serait d'en déployer sur toutes les machines du parc informatique ainsi que sur tous les composants d'infrastructure. Ceci n'est pas toujours possible pour des raisons de coûts et d'exploitation, un compromis courant consiste donc à installer des agents HIDS sur toutes les machines de la DMZ ainsi que sur les serveurs névralgiques et les composants d'infrastructures quand c'est possible.

En fin, à chacun de créer ses propres architectures suivant ses besoins et son imagination [**21**] [**37**].

V Les limites d'un IDS

- Les IDS ne sont pas évolutifs, et sont difficilement dé-ployable sur un réseau d'entreprise.
- La gestion des fausses n'est pas toujours maîtriser, et reste un problème sur les IDS.
- Les IDS des différents opérateurs commerciaux dialoguent rarement (en attendant les travaux du groupe IDWG). Ce qui rend difficile le déploiement d'un IDS composé d'un détecteur et d'une console d'analyse de deux constructeurs différents.
- Les IDS commerciaux sont difficilement associables avec d'autres outils de la sécurité et de gestion de paquets sur un réseau.
- Ils ne peuvent pas compenser des manques significatifs dans votre stratégie de sécurité, votre politique de sécurité ou votre architecture de sécurité.
- Ils ne peuvent pas compenser les trous de sécurité dans les protocoles réseaux.
- Ils ne peuvent pas se substitué à d'autre type de mécanisme de sécurité à savoir l'identification, l'authentification, le chiffrement, les firewalls, et les ACL (Access Control List).
- Ils ne peuvent pas non plus protéger eux seuls contre tous les menaces de sécurité dont votre système d'information fait l'objet **W14**.

- Un IDS ne peut pas 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 [**9**].
- Un IDS ne peut pas conduire des recherches concernant les attaques sans l'intervention de l'être humain [**9**].

Conclusion

L'avenir des technologies de sécurité réseau est dans une intégration plus poussée des différents outils disponibles pour assurer la sécurité d'un réseau, car l'administration de la sécurité d'une entreprise est une tâche de plus en plus complexe et étendue, alors que les besoins en sécurité ne font que croître. Une gamme complète de solutions telles que l'anti-virus, 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 quotidiennes et de nombreuses failles sont découvertes et exploitées chaque jour.

Les produits existants ne sont pas encore suffisamment fiables. L'arrivée des IDS, tentent de pallier en partie à ces problèmes et continuent d'évoluer pour répondre aux exigences technologiques du moment et actuellement offrent un éventail de fonctionnalités capables de satisfaire les besoins de tous les types d'utilisateurs.

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 et aide 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 sécurisé le réseau.

Chapitre IV

Organisme d'accueil

Introduction

Le Groupe Cevital s'est constitué au fil des investissements, autour de l'idée forte de bâtir un ensemble économique. Porté par plus de 10 200 collaborateurs, elle représente le fleuron de l'économie algérienne. Le fondateur du Groupe Cevital résume les clefs du succès en sept points : le réinvestissement systématique des gains dans des secteurs porteurs à forte valeur ajoutée, la recherche et la mise en œuvre des savoir-faire technologiques les plus évolués, l'attention accordée au choix des hommes et des femmes, à leur formation et au transfert des compétences, l'esprit d'entreprise, le sens de l'innovation, la recherche de l'excellence et la fierté et la passion de servir l'économie nationale.

I Historique

Créer par des fonds privés l'entrepreneur " IssadRebrab " en mai 1998. Le Groupe Cevital a traversé d'importantes étapes historiques pour atteindre la taille et la notoriété d'aujourd'hui en continuant à œuvrer dans la création d'emplois et de richesse.

. **2000** Création de NOLIS : Transport maritime.

. **2005**

- Acquisition de LallaKhedidja : Unité d'eau minérale plate et gazeuse et de sodas.
- Création de CEVICO : Fabrication de bâtiment préfabriqué en béton.

. **2006**

- Acquisition de COJEK, filiale de ENAJUC : Jus et conserves.
- Création de Numidis : Grande distribution (UNO) et (Unocity).

. **2007**

- Création de MFG : Industrie du verre.
- Acquisition de BATICOMPOS : Industrie de fabrication d'éléments de construction préfabriqués.
- Création de SAMHA : Assemblage et distribution de produits électroniques et électroménagers de marque SAMSUNG Electronics en Algérie.

. **2007** Création du Groupe Cevital

. **2008**

- Création de MFG Europe : Commercialisation de verre plat en Europe.
- Création de COGETP : Engins de travaux publics VOLVO.
- Création de CEVIAGRO : Agriculture.

. **2010** Création de SodiAutomotive.

. **2011** Création de PCA - Création de Sierra Cevital.

II Présentation du complexe Cevital

Cevital est un groupe familial de vingt-cinq sociétés, réparties dans cinq secteurs d'activités : L'Industrie Métallurgique, l'Information et la Communication, la Distribution Automobile, le Transport Terrestre et Maritime, l'Industrie Agroalimentaire. CEVITAL est parmi les entreprises algériennes qui ont vu le jour dès l'entrée du pays dans l'économie de marché. Disposant de technologies de pointe.

Cevital possède deux raffineries une d'huile et l'autre de sucre.

La raffinerie d'huile alimentaire a été mise en chantier en Mai 1998 et en Aout 1999 elle est rentré en production, plus tard en 2000 la raffinerie du sucre est mise en chantier, elle n'est devenue fonctionnel que en 2002.

Un autre produit est mis en chantier en 2000 et en production en 2001 c'est la margarine.

Une deuxième raffinerie du sucre de 3000T de plus le silo sucre blanc 80000T et le silo sucre roux 150000T, et une unité d'eau minéral L'alla Khadîdja et une autre unité de

Cojek a El Kseur. Enfin, une station de cogénération.

II.1 Situation géographique

Le complexe de production agroalimentaire se situe dans le port de BEJAIA et s'étend sur une superficie de 45 000m, à 280Km d'Alger et à proximité de l'aéroport ainsi que la zone industrielle d'Akbou. Cevital est entouré de plusieurs entreprises comme " Sonatrach " (à droite), et " Naftal " (enface), son oublier " le Port" (à gauche). Cette situation a permet à Cevital d'être bien placer et d'avoir l'avantage de profite beaucoup de proximité économique.

II.2 Organigramme du groupe Cevital

Voici le schéma général du groupe Cevital, dont chaque direction a pour but d'assurer le bon fonctionnement de chaque partie du groupe comme le montre cette figure :

Le groupe Cevital garantit ces missionset ces activités :

II.2.1 Les Missions

L'entreprise a pour missions principales de développer la production et d'assurer la qualité du conditionnement des huiles, des margarines et du sucre à des prix nettement plus compétitifs et cela dans le but de satisfaire le client et de le fidéliser.

II.2.2 Les Activités

Lancé en Mai 1998, le complexe Cevital a débuté son activité par le conditionnement en Décembre 1998. En février 1999, les travaux de génie civil de la raffinerie ont débuté. Cette dernière est devenue fonctionnelle en Août 1999. L'ensemble des activités de Cevital est concentré sur la production et la commercialisation des huiles végétales, de margarine et de sucre se présente comme suit :

- Raffinage d'huile 1600 T/j pouvant passer après extension à 1800 T/J.
- Production de margarine de capacité 600 T/J.

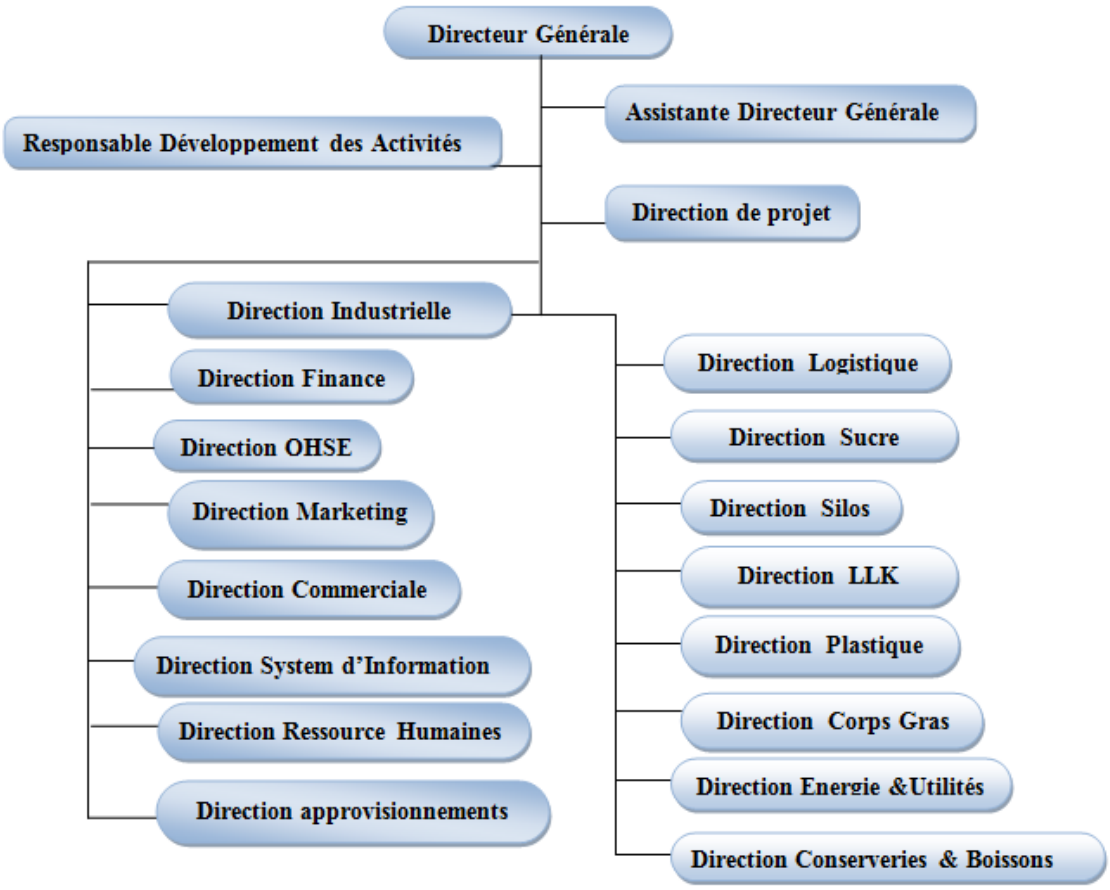


FIG. IV.1 – Organigramme du groupe Cévital

. Fabrication d'emballage en PET (9600 unités/h).

. Stockage céréales.

. Electrolyseur (par mesure de sécurité doit être déplacé hors Cevital).

. Extension de la sucrerie.

. Savonnerie.

. Minoterie (en cours d'étude).

. Hydroélectrique d'huile.

Cevital visent à réaliser ces objectifs :

II.2.3 Les objectifs

Les objectifs visés par Cevital peuvent se présenter comme suit :

. Encouragements des agricultures par des aides financières pour la production locale de graines oléagineuses.
. Importation de graines oléagineuses pour l'extraction directe des huiles brutes.
. Diversification de ses produits et sa diffusion sur tout le territoire national.
. Modernisation de ses installations et adoption de nouvelles démarches de gestion technique afin d'augmenter le volume de sa production.
. Positionner ses produits sur le marché étranger par leurs exportations.
. Optimisation de ses offres d'emploi sur le marché du travail.

Les produits de Cevital disponibles sur le marché présentés dans le titre suivant.

II.3 Les produits

Les produits du complexe sont de deux catégories :

II.3.1 Complexe agroalimentaire de Bejaia

Le complexe agroalimentaire fabrique que les produits huile alimentaire et végétales et sucre.

. **L'huile** Chez Cévital il existe plusieurs types de l'huile, ils sont commercialisés depuis 1999.
  - **Fleurial :** Aout 1999, l'huile 100
  - **Fridor :** huile végétale 100% équilibrée 10 cuisson et toujours bon.
  - **Elio :** huile végétal 100% équilibrée Le mélange entre le tournesol et le Soja.
  - **Soya :** Décembre 1999, 100% soya.
  - **Canola :** Septembre1999, 100% colza.
. **Margarine :** Le complexe Cevital n'est pas spécialisé que dans la margarine mais en trouve aussi du Berre, SMEN ....
  - **La Parisienne :** margarine de feuilletage pour les professionnels, Existe en format 500g.
  - **Elio :** C'est un nouveau produit 100% végétale.
  - **Matina :** Le mélange parfait entre la margarine et le berre .Matina existe en format 400g.

- **Medina :** 100% végétale, SMEN gastronomique Medina existe en formats 500g, 900g et 1.8Kg.
- **Rania :** est le beurre gourmant.
- **Fleurial :** margarine 100% végétale.

. **Sucre :** Il existe deux types :

- **SKOR :** est un sucre blanc cristallisé de qualité supérieure, C'est un produit grand public disponible en formats 1Kg et 5Kg.
- **Dolce :** est le sucre blanc morceaux

II.3.2 Le groupe Cevital

Le groupe Cévital a d'autre produit sur la marche dans d'autre secteur de commerce.

. **Boisson** Le just d'orange " Tchina" présent dans tout le territoire algérienGammeproduit : Orange, Mandarine, Cocktail, exotique, Orange pêche, Citron.

. **Automobile**

- **Fiat :** Représentant de la marque avec SODI auto motive.
- **Hyundai :** Représentant de la marque avec Hyundai Motors.
- **Cévicar :** Entreprise de location de véhicule.
- **ActCamions :** La commercialisation et la maintenance de véhicules.

. **L'Eau** L'eau minérale " LallaKhedidja " des monte neiges du Djurdjura (gazéifiée et non gazéifiée). Elle existe en formats 0.5L, 1Let 1.5L.

. **Journal et Panneaux :**

- **Press :** quotidien Liberté.
- **Futur Media :** Panneaux publicitaire.

. **Electronique**

- **Jbm :** Représentant IBM Algérie.
- **Samha :** Samsung Samha Algérie.

. **Autre produit**

- **Grande Distribution :** Créée en janvier 2007, Numidis est une filiale de Cevital spécialisée dans la grande distribution.

- **Cevico :** Construction est spécialisée dans la préfabrication des éléments en béton armé et en béton armé précontraint.
- **Ceviagro :** Agriculture.
- **MFG :** Float Glass Manufacture Une filiale spécialisé dans l'industrie du verre en Algérie.
- **Nolis :** Une compagnie maritime de transport de marchandise agroalimentaire, Cevital l'a doté d'un nombre important de silos portuaires ainsi qu'un terminal de déchargement portuaire.

II.4 Capacité du groupe Cévital

- Force de vente qualifiée.
- Une équipe marketing est toujours présente.
- Une large flotte de transport.
- Toujours en quête de protection.
- Le groupe possède des grands chercheurs.
- Disponible partout et aller toujours plus lion.
- Technologie de pointe.
- Une main d'œuvre qualifiée.
- Grande capacité de stockage.
- Département application Meilleur sélection de matières premières

III L'informatique dans Cevital

Cevital est parmi les entreprises possédant une direction informatique et donne une grande importance au domaine de l'informatique.

III.1 Présentation de l'organisme d'accueil

Notre étude se focalise au niveau du groupe Cevital de Bejaia dont nous avons effectué notre stage, dans la direction de l'informatique réseau et télécom.

III.1.1 Organigramme de La direction système d'information

La direction système d'information de Cevital est composée de deux départements :

. Métiers.

. Département système réseaux télécom : il assure le bon fonctionnement de réseaux (Internet) et même la télécommunication (Téléphonie).

Chaque département a pour objet d'amélioré le niveau de l'informatique et ces services pour garantir le développement et la progression des services de groupe Cévital.

L'organigramme de la direction système d'information est montré dans la figure suivante :

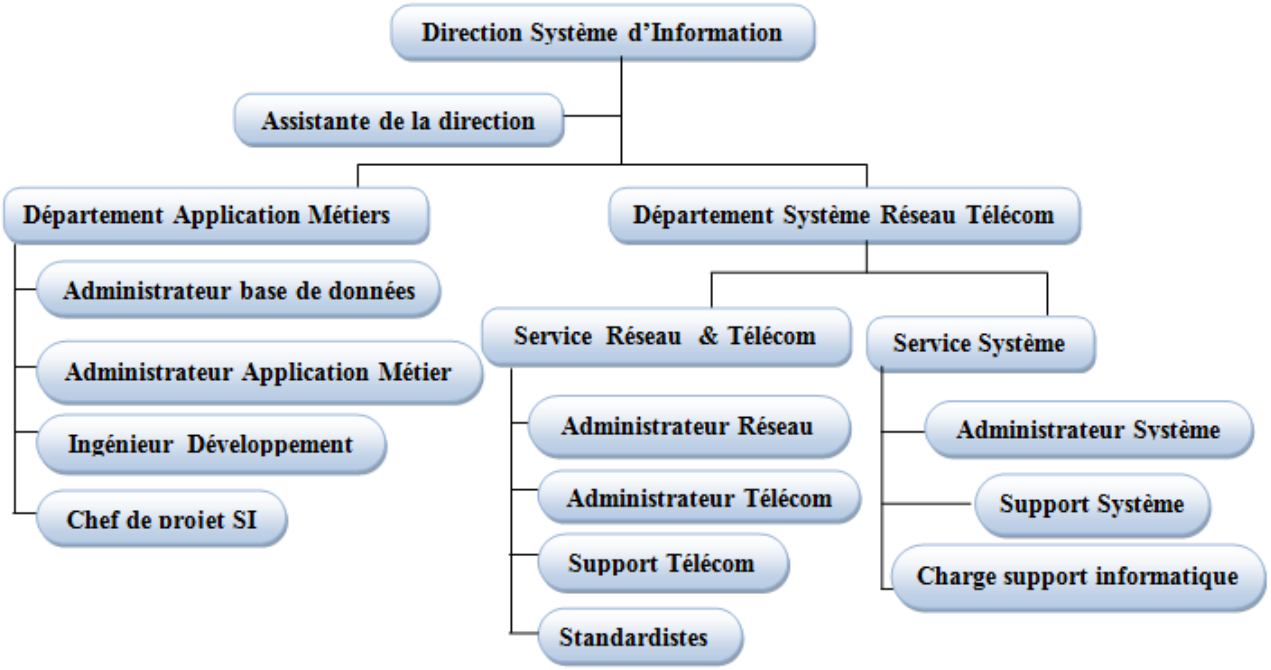


FIG. IV.2 – Organigramme de la direction système d'information.

III.1.2 Infrastructure matériel

Centre d'Information (Data Center) est le cœur de Cevital, il contient tous les équipements physiques et tous les serveurs que Cevital a besoin, mises dans des armoires.

Le Data Center est une pièce très importante pour cela le droit d'accès est limité que pour l'équipe de système d'information.

a) Les équipements physiques de Data Center

. **Onduleur :** Assure le bon fonctionnement et la continuité et la stabilité du courant électrique, il existe plusieurs.
. **Climatiseur :** Il y a deux grands climatiseurs pour éviter l'échauffement des équipements physiques.
. **Un Routeur :** Assure le fonctionnement et la liaison avec le réseau de groupe qui se trouve à Alger.
. **Un Anti-Spam :** Il assure le filtrage des messages.
. **Switch :** Il existe un Switch Corre série 4570R qui relie un ensemble de switch d'accès série 2950 48E 2F distribués sur les différent bureaux du l'entreprise et aussi des points d'accès Wi-Fi AP 1100 pour assure l'interconnexion des équipements réseau et des VLAN intégrés dans ces derniers.
. **Un Firewall :** pour la gestion de protection internet et pour l'autorisation d'accès à un nombre de site internet le Juniper modèle SSG 550.

Le service informatique a attribué un system pour la gestion téléphonique, soit d'une manière numérique ou analogique même pour l'application GSM, et un autre system de surveillance par vidéos pour assure l'enregistrement des vidéos, et pour l'écrasement de cette dernière il se fait automatique.

b) Parc serveurs de Data Center Armoire de brassages contenant des serveurs qui assure le bon fonctionnement du système informatique de Cevital.

. **CEVSRV1010/GRH :** Le serveur qui assure la gestion des ressources humaines.
. **CEVSRV 1004 / File :** Le serveur qui assure la gestion des imprimantes de tous le complexe.
. **CEVSRV 1045 :** Le Bodet c'est le serveur de la gestion du temps.
. **CEVSRV 1005/wsus :** Le but de ce serveur est d'évite l'encombrement, c'est le serveur de mise à jour.
. **CEVSRV 1034/sage paie :** Le serveur qui assure le filtre web.
. **CEVSRV 1009 :** Publication Exchange pour l'utilisateur externe.
. **CEVSRV 1001 et 1002 :** Les contrôleurs de domaine, c'est des serveurs a pour objet de stocker les données de l'annuaire et gère les interactions entre l'utilisateur et le domaine.

. **CEVSRV 1011 et 1013 :** Les serveurs de base de données :
  - 1011 : Coswin BD.
  - 1013 : Sage BD.

. **CEVSRV 1006, 1021, 1022 :** Les serveurs de messagerie de groupe :
  - 1006 : MBX Accès client, HUB.
  - 1021 : Nœud Exchange Active.
  - 1022 : Nœud Exchange Passive.

. **NAS :** Network Storage le serveur de sauvegarde partage les utilisateurs. Dans le Data center on trouve trois types de fils : Fils blanc pour les liaisons entre les différents serveurs, Fils orange pour les liaisons entre les différents bâtiments et des fils jaune.

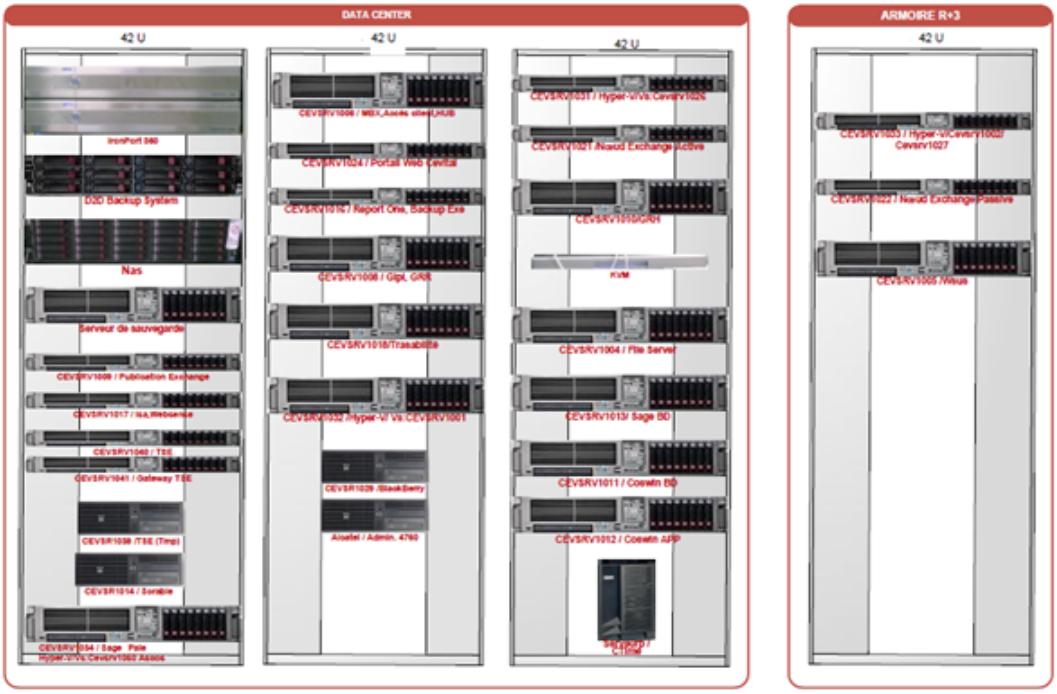


FIG. IV.3 – Data Center du Cevital.

III.1.3 Logiciels de service de base

Cevital utilise différents logiciels, et chaque logiciel est spécialisé dans un domaine.

a) Skeeper : C'est un logiciel qui permet d'avoir une fiche associe à chaque produit d'une façon unique.

b) Coswin : le logiciel qui gère l'ensemble des activités d'un service maintenance, il est de GMAO (Gestion Maintenance Assistée par Ordinateur). Dans le Data Center, il est installé sur :

- Le CEVSRV 1011 : pour la base de données de Coswin.
- Le CEVSRV 1012 : pour l'application de Coswin.

III.1.4 Les applications

Nous distinguons deux types d'applications :

a) Les applications de Sécurité Comme Cevital est une grande entreprise donc la surveillance de l'état de ces machines est important, pour cela Cevital utilise l'application " Kespersky Security Center ".

b) Les applications de Télécommunication Une application concerne la téléphonie estNMS : Network Management Système (Client Omni vista). Cette application permet d'organiser tous les informations nécessaires des utilisateurs, Il existe deux types : Locale et Mobile.

III.2 L'architecture réseau de Cevital

Le réseau du complexe Cevital s'étend actuellement sur six principaux pôles à savoir : Bejaia, Alger, Oran, El Kseur (Cojek) et Tizi Ouzou (Lalla Khedidja),en plus des connexions à internet via des FAI (Fournisseur d'accès à Internet) SLC et Anwarnet. Comme la montre figure suivante :

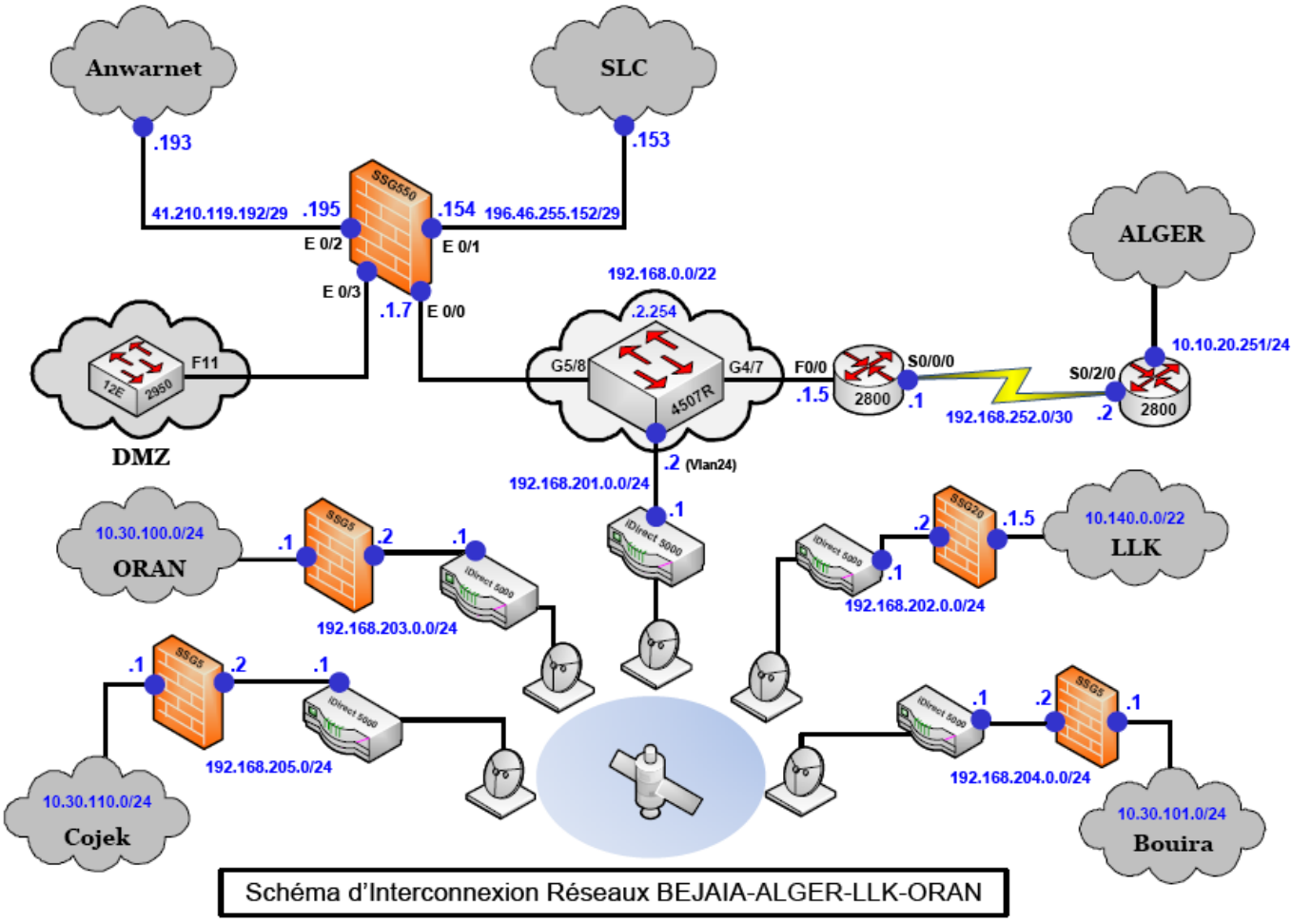


FIG. IV.4 – La topologie globale du réseau du complexe Cevital.

Au niveau Cevital-Bejaia Les différentes directions de l'entreprise sont relies au Data Center comme la montre figure suivante :

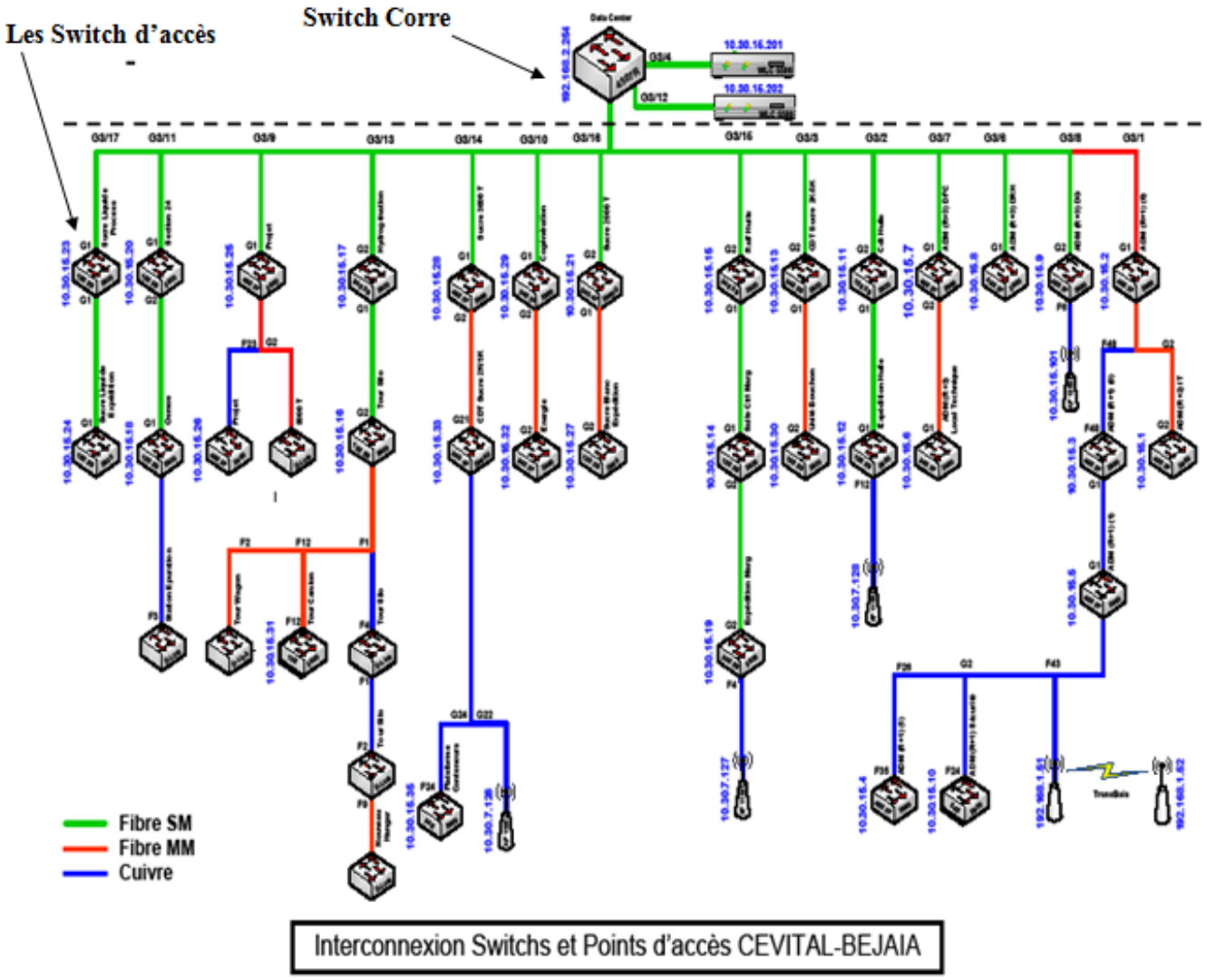


FIG. IV.5 – La topologie d'interconnexion du réseau local CEVITAL-BEJAIA.

III.2.1 Les systèmes de détection d'intrusions au niveau de cevital

Au niveau de cevital ils utilisent le pare-feu Junipe le modèle SSG550 (Secure Services Gateway) qui intègre l'option IDS, qui offre un foule de détails sur les règles et le trafic qu'il intercepte, jusqu'à l'affichage du contenu des paquets, si nécessaire, détecter les attaques sur la base de règles et l'observation d'anomalie dans le trafic.

III.3 Problématiques

Un pare-feu n'est désormais plus suffisant pour sécuriser un réseau. Il est indispensable d'adopter une approche intégrant la prévention contre les intrusions. Intégré les

fonctionnalités d'un IDS dans un pare-feu facilite la configuration (un seul équipement à configurer), cela permet aussi d'avoir une vue globale sur la sécurité du réseau dans une seule et même fenêtre et de gérer les différents paramètres plus facilement. Mais cela évite de multiplier les logiciels de protection pour avoir une meilleure sécurité (un firewall il sert à bloquer/protéger vis à vis de l'extérieur et un IDS c'est un autre produit à installer qui permet de détecter les attaques et les tentatives d'intrusions sur les ports ouverts et autorisés).

Si l'IDS est intégré dans un pare-feu, ces derniers peuvent entrer en conflits car ils analysent le même flux de données et cela peut provoquer un plantage ainsi la présence d'un grand trafic ralentira considérablement les performances de l'équipement : le taux d'utilisation du processeur explose, la mémoire baisse de manière drastique et il risque de ralentir le trafic.

III.4 La solution proposée

Configurer un IDS Appliance augmente le degré de sécurité, vu qu'il fonctionne indépendamment d'un autre équipement lui permet une capacité de détection plus performante. Il joue le rôle d'un complément aux firewalls en lui permettant une analyse plus intelligente du trafic.

Pour notre cas d'étude, nous avons choisi d'installer un IDS Cisco appliance et configurer cet équipement d'une manière sécurisée.

Cisco IDS et Juniper SSG550, ces deux appliances ne sont pas directement comparable, puisque Cisco IDS est un système de détection d'intrusions alors que Juniper SSG550 est un firewall multifonctions qui peut intégrer les fonctionnalités d'un système de détection d'intrusion.

Dans ce chapitre, nous avons présenté le cadre de travail dans lequel nous avons effectué le stage, ce qui nous a permis de mieux comprendre et apprécier le travail abattu

par l'ensemble du personnel du complexe Cevital, de comprendre la place qu'occupe cette structure dans le domaine, ainsi, l'étude du réseau Cevital nous a permis de bien comprendre son architecture et les stratégies utilisées pour sa sécurisation.

Dans le chapitre suivant nous allons mettre en œuvre notre solution et pouvoir l'a simulé sous GNS3.

Conclusion

Dans ce chapitre, nous avons présenté le cadre de travail dans lequel nous avons effectué le stage, ce qui nous a permis de mieux comprendre et apprécier le travail abattu par l'ensemble du personnel du complexe Cevital, de comprendre la place qu'occupe cette structure dans le domaine, ainsi, l'étude du réseau Cevital nous a permis de bien comprendre son architecture et les stratégies utilisées pour sa sécurisation.

Dans le chapitre suivant nous allons mettre en œuvre notre solution et pouvoir l'a simulé sous GNS3.

Chapitre V

La réalisation de la solution proposée

Introduction

L'étude en termes de sécurité du réseau de Cevital nous a permis de réaliser une nouvelle configuration plus au moins sécurisée qui consiste à configurer un système de détection d'intrusion Appliance (non intégré), qui est l'IPS Cisco série 4235.

Pour visualiser l'efficacité de notre travail et mettre en évidence la configuration de notre application, nous avons utilisé le simulateur GNS3 version 0.8.3.1 qui est un logiciel très pratique open source pour maquetter un réseau. Il pourra nous servir à reproduire une architecture physique ou logique complète avant la mise en production.

Dans ce chapitre nous allons présenter les outils utilisés et la procédure de configuration pour mettre en œuvre notre solution.

I Présentation de GNS3

I.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) **W10**.

I.2 Les composants du logiciel

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

. **Dynamips :** Dynamips est un émulateur de routeurs Cisco capable defaire 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**]. Écrit en langage C par Christophe Fillot. Il émule 1700, 2600, 3600, 3700, et 7200 plates-formes de matériel **W10**.

Pour permettre l'exécution d'une image IOS, Dynamips doit émuler le processeur ainsi que tous les périphériques de la plateforme cible : mémoire RAM (Random Access Memory), NVRAM (stockage de la configuration), mémoire Flash, interfaces réseau [**31**].

. **Dynagen :** 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. GNS3 reprend ces mêmes fonctionnalités sous forme d'interface graphique. Il s'appuie sur des modules de Dynagen [**31**]. Dynagen fournit aussi une CLI (Command-line Interpreter) de gestion pour les périphériques d'inscription, démarrage, arrêt, recharge, la suspension, la reprise et la connexion aux consoles de routeurs virtuels **W12**.

. **Qemu :** 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.

QEMU fonctionne sur les systèmes x86 courant le Linux, le Microsoft Windows, et quelques plates-formes d'UNIX, et peut accueillir des systèmes de cible d'une gamme de différents microprocesseurs comme détaillé sur le site Web de QEMU [1] **W17**.

. **Virtualbox :** 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

[1] La startup ou jeune pousse est une jeune entreprise à fort potentiel de croissance et qui fait la plupart du temps l'objet de levée de fonds. On parle également de startup pour des entreprises en construction qui ne se sont pas encore lancées sur le marché commercial (ou seulement à titre expérimental).

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 **W24**.

Grâce à ces composants, GNS3 nous permet **W9** :

- Le design de topologies réseaux de haute qualité et complexes.
- Emulation de plusieurs plate-formes 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.

I.3 L'objectif de GNS3

L'objectif de GNS3 est d'apporter aux étudiants et aux professionnelstravaillant dans le domaine de l'administration systèmes et réseaux des nouvelles technologies de communication. C'est un outil pour virtualiser et modéliser fidèlement des réseaux.

Grâce à GNS3, les utilisateurs peuvent tester et estimer, dans des conditions quasi réelles et sans avoir à financer le matériel, leurs configurations avant de les mettre en place physiquement **W9**.

I.4 Les avantages et les inconvénients de GNS3

I.4.1 Avantages

- C'est de l'émulation, donc vous aurez tous les protocoles disponibles en fonction de l'IOS ajouté contrairement au logiciel Cisco Packet Tracer où certains protocoles ne sont pas implémentés (VRF (virtual Routing and Forwarding), ...), vous pourrez

même ajouter à votre architecture une machine hôte ou une machine virtualbox **W8**.

- Avec GNS3 vous utilisez un IOS Cisco réel, de sorte que vous verrez exactement ce que l'IOS produit et auront accès à tous les paramètres de commande ou pris en charge par l'IOS **W10**.
- Il permet notamment l'interconnexion du laboratoire (lab) virtuel ainsi crée avec un réseau physique [**30**].
- Il permet aux administrateurs système de tester des nouvelles configurations de son réseau sans toucher au réseau en production ou au étudiants de découvrir l'administration réseau **W20**.

I.4.2 Inconvénients

- GNS3 est une excellente plate-forme pour émuler des routeurs Cisco, mais l'émulation de commutateurs Cisco Catalyst n'est pas prise en charge en raison de l'impossibilité d'imiter le processeur ASIC (Application-SpecificIntegrated Circuit) utilisés dans ces dispositifs, mais un module de switchingEthernet (référence Cisco NM-16ESW) peut être utilisé sur les plateformes de routeur 3600, 3700 et 2600, cela fournit un environnement trop limité de commutation pour les administrateurs et le personnel de réseautage vouloir faire des laboratoires de commutation les plus avancés. En ce moment, il est impossible d'imiter les commutateurs Catalyst avec Dynamips et/ou GNS3 **W10**.
- A l'heure actuelle, seules certaines plateformes de routeurs sont émulées ainsi que les plateformes PIX et ASA qui sont les Firewalls de la gamme Cisco [**30**].
- GNS3 ne fournit pas d'IOS, malheureusement ces images sont réservées aux propriétaires de matériels Ciscopour les télécharger il faut se procurer à l'aide d'un compte Cisco**W10**.

I.5 La configuration de GNS3

1. Voir l'annexe C pour les détails de l'installation.
2. Lors du lancement du logiciel une fenêtre similaire à celle-ci apparait, c'est l'espace de travail de GNS3.

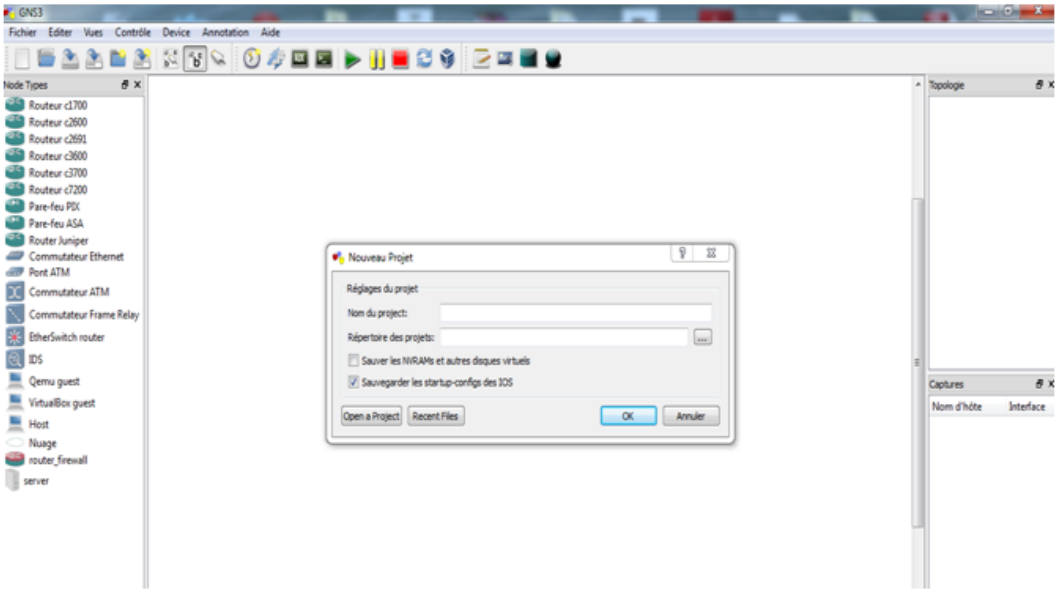


FIG. V.1 – L'espace de travail GNS3.

L'interface de GNS3 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.

La fenêtre qui apparait au milieu au lancement de GNS3, 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 cocher les deux cases.

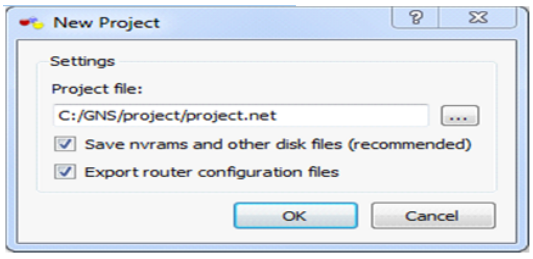


FIG. V.2 – Création d'un nouveau projet sous GNS3

L'interface de gns3 est très simple, elle fonctionne en grand partie sur le principe du glisser-déposer. Il suffit de prendre un élément à placer sur le schéma dans la liste de gauche et de le déposer dans l'espace central.

3. Pour commencer à travailler avec GNS3, nous devons avoir l'IOS image de Cisco, il faut donc télécharger les IOS dont on va se servir. Une fois effectué Nous allons renseigner pour chaque modèle de routeur que nous voulons utiliser, le chemin vers l'image IOS [2].

4. Pour ajouter l'IOS 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 téléchargé, puis choisir la plate-forme et le modèle du routeur adéquat puis cliquer sur save. La figure ci-dessous montre les IOS que nous avons ajoutés.

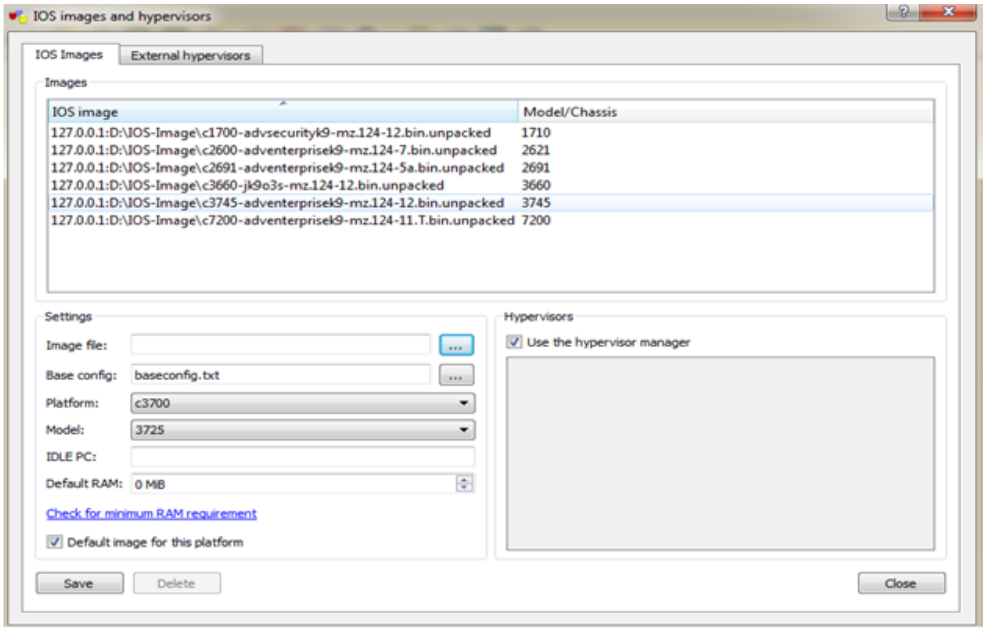


Fig. V.3 – L'ajout des IOS.

5. Maintenant pour ajouter 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. Un clic droit sur le routeur pour le démarrer.

6. Pour ajouter une machine virtuelle dans notre architecture GNS3, il nous faut d'abords préalablement installer Virtualbox et avoir déjà configuré au moins une machine virtuelle (voir l'annexe C).

7. Pour intégrer la machine virtuelle dans GNS3 Il faut d'abord l'importer comme suit : Aller dans Edit -Preferences -Virtualbox -VirtualboxGuest -RefreshVM List,

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

puis donner un nom à la machine et dans le menu VM list sélectionner la machine à importer en suit sélectionner le numéro de la carte réseau laquelle elle va utiliser (Number of NICs)pour se connecter, en fin save- Apply-OK.

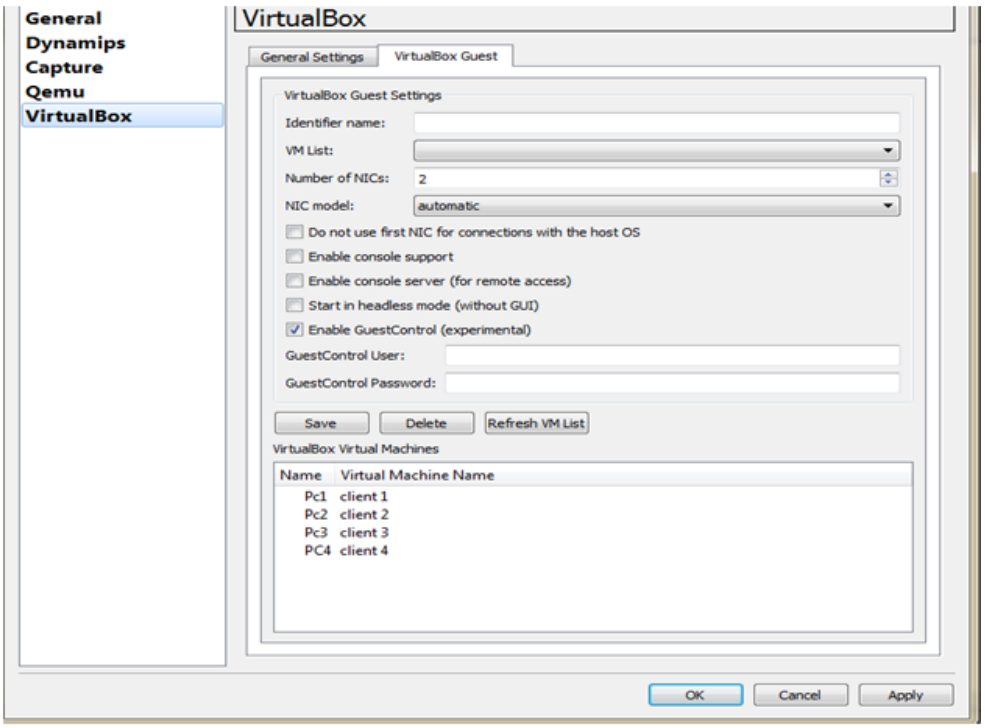


Fig. V.4 – L'ajout d'une machine virtuelle à la topologie GNS3.

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.

II La simulation de notre topologie

Notre cas d'étude va se porté sur le réseau local au niveau de Bejaia, où nous allons implémenter L'IDS.

Pour les besoins de la simulation et pour des raisons de manque de certains dispositifs, nous avons choisi de remplacer le firewall par un routeur firewall et 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 :

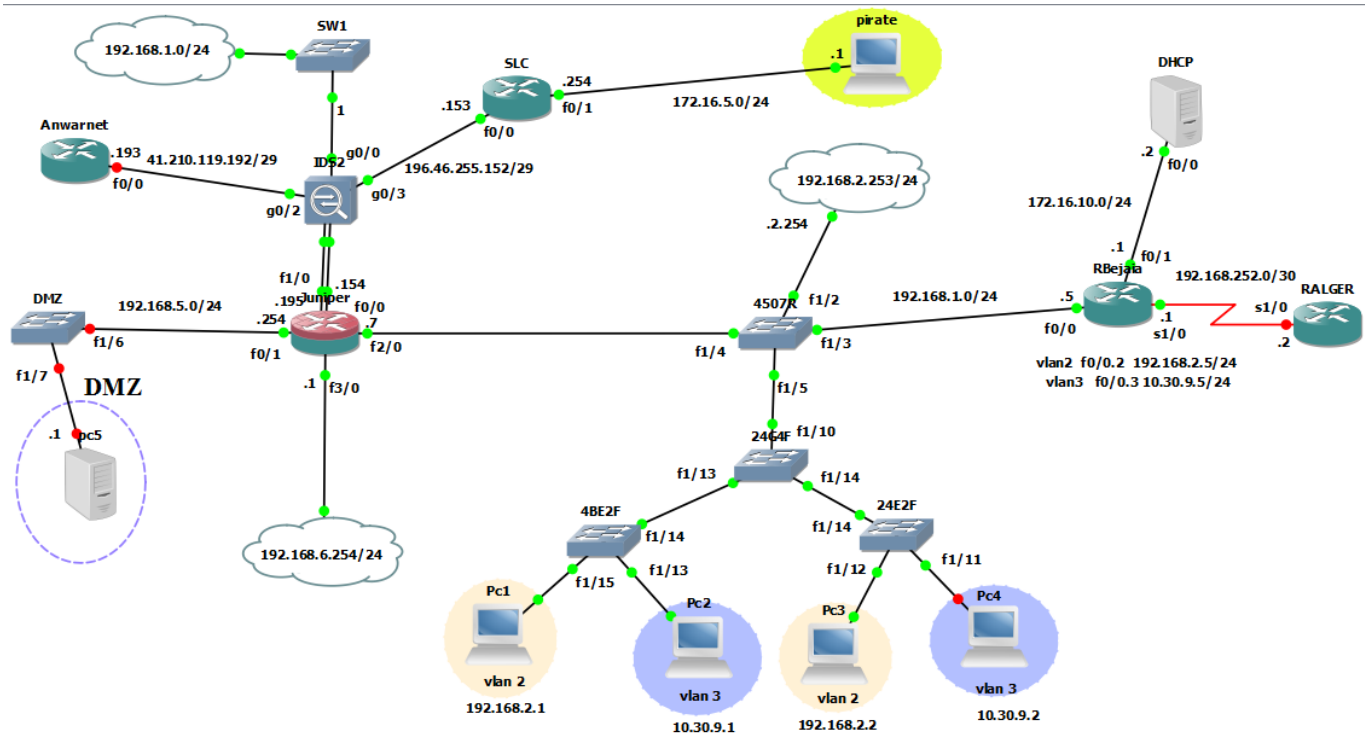


FIG. V.5 – La topologie du réseau local Cevital-Bejaia sous GNS3.

Cette figure montre l'attribution des adresses IP aux équipements réseaux et aux PC :

	Interface	@IP	Masque réseau	Passerelle	Vlan
RALGER	S1/0	192.168.252.2	255.255.255.252		
RBejaia	S1/0	192.168.252.1	255.255.255.252		
RBejaia	F0/0	192.168.1.5	255.255.255.0		
RBejaia	F0/1	172.16.10.1	255.255.255.0		
RBejaia	F0/0.2	192.168.2.5	255.255.255.0		
RBejaia	F0/0.3	10.30.9.5	255.255.255.0		
Juniper	F0/0	196.46.255.154	255.255.248.0		
Juniper	F0/1	192.168.5.254	255.255.255.255.0		
Juniper	F1/0	41.210.119.195	255.255.248.0		
Juniper	F2/0	192.168.1.7	255.255.255.0		
Juniper	F3/0	192.168.6.1	255.255.255.0		
SLC	F0/0	196.46.255.153	255.255.248.0		
SLC	F0/1	172.16.5.254	255.255.255.0		
Anwarnet	F0/0	41.210.119.193	255.255.255.248		
FTPserver					
DHCP		172.16.10.2	255.255.255.0	172.16.10.1	
Pc1		192.168.2.1	255.255.255.0	192.168.2.5	Administrateur
Pc2		10.30.9.1	255.255.255.0	10.30.9.5	Employes
Pc3		192.168.2.2	255.255.255.0	192.168.2.5	Administrateur
Pc4		10.30.9.2	255.255.255.0	10.30.9.5	Employes
Pirate		172.16.5.1	255.255.255.0	172.16.5.254	

II.1 La politique de sécurité

Notre topologie suit ces règles :

- 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.
- Les administrateurs réseau peuvent accéder à distance au Switch fédérateur.
- Aucun des utilisateurs autres que les administrateurs peuvent accéder au Switch.
- L'IDS est configuré selon quelques règles définis pour le contrôle de la circulation du trafic provenant de l'Internet en générant des alertes selon le type du trafic détecté :

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

  En suit, configurer l'IDS pour interdire la circculation de ce trafic.

  Pour réaliser cette politique, nous suivant ces étapes :

II.2 Configuration des routeurs

II.2.1 Configuration du routage inter-VLAN

Pour effectuer le routage inter-vlan, nous devons créer et configurer des sous interfaces au niveau de l'interface F0/0 du routeur RBejaia.

```
RBejaia#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RBejaia(config)#interface f0/0.2
RBejaia(config-subif)#encapsulation dot1q 2
RBejaia(config-subif)#ip address 192.168.2.5 255.255.255.0
RBejaia(config-subif)#exit
RBejaia(config)#interface f0/0.3
RBejaia(config-subif)#encapsulation dot1q 3
RBejaia(config-subif)#ip address 10.30.9.5 255.255.255.0
```

Fig. V.6 – Configuration des sous interfaces.

II.2.2 Configuration des interfaces des routeurs RBejaia, RALGER et activation du protocole rip

Pour la connectivité des réseaux, nous devons configurer les adresses IP des interfaces des routeurs et activer le protocole rip comme illustrer sur cette figure :

```
RBejaia#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RBejaia(config)#inter f0/0
RBejaia(config-if)#ip address 192.168.1.5 255.255.255.0
RBejaia(config-if)#no sh
RBejaia(config-if)#exit
*Mar  1 00:01:12.615: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:01:13.615: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
RBejaia(config-if)#exit
RBejaia(config)#inter s1/0
RBejaia(config-if)#ip address 192.168.252.1 255.255.255.252
RBejaia(config-if)#no sh
RBejaia(config-if)#
*Mar  1 00:01:53.987: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
*Mar  1 00:01:54.987: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
RBejaia(config-if)#exit
RBejaia(config)#router rip
RBejaia(config-router)#version 2
RBejaia(config-router)#network 192.168.252
*Mar  1 00:02:23.067: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to down
RBejaia(config-router)#network 192.168.1.0
RBejaia(config-router)#network 192.168.2.0
RBejaia(config-router)#network 192.168.252.0
RBejaia(config-router)#network 10.30.9.0
```

Fig. V.7 – Configuration des interfaces du routeur RBejaia.

```
DHCP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DHCP(config)#inter f0/0
DHCP(config-if)#ip address 172.16.10.2 255.255.255.0
DHCP(config-if)#no sh
DHCP(config-if)#exit
DHCP(config)#ip route 0.0.0.0 0.0.0.0 f0/0
DHCP(config)#ip dhcp excluded-address 192.168.2.5
DHCP(config)#ip dhcp excluded-address 10.30.9.5
DHCP(config)#ip dhcp pool cevital
DHCP(dhcp-config)#network 192.168.2.0 255.255.255.0
DHCP(dhcp-config)#default-router 192.168.2.5
DHCP(dhcp-config)#exit
DHCP(config)#ip dhcp pool cevital2
DHCP(dhcp-config)#network 10.30.9.0 255.255.255.0
```

FIG. V.8 – Configuration du serveur DHCP.

```
RBejaia#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RBejaia(config)#inter f0/1
RBejaia(config-if)#ip add 172.16.10.1 255.255.255.0
RBejaia(config-if)#no sh
RBejaia(config-if)#exit
RBejaia(config)#inter f0/0.2
RBejaia(config-subif)#ip helper-address 172.16.10.2
RBejaia(config-subif)#exit
RBejaia(config)#inter f0/0.3
RBejaia(config-subif)#ip helper-address 172.16.10.2
```

FIG. V.9 – Configuration de l'interface f0/1.

II.2.3 Configuration de l'interface f0/1 de RBejaia

II.3 La configuration et l'initialisation de l'IDS

Dans cette section nous allons montrer comment émuler un système de détection d'intrusions 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 placer dans le fichier d'installation de GNS3 et suivre ces étapes :

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

Dans le menu démarrer ouvrir un cmd et accéder au fichier d'installation GNS3 par la commande cd, puis saisir les commandes suivantes :

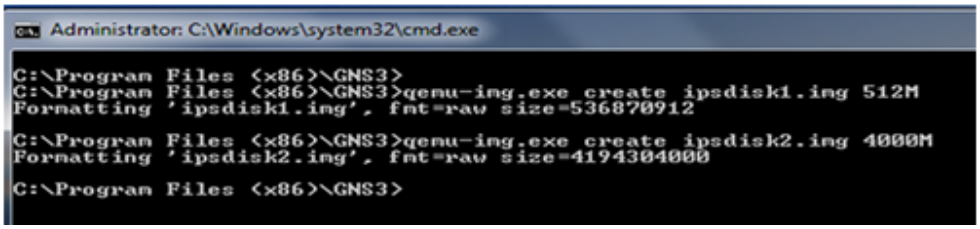


FIG. V.10 – Les commandes de création de disques pour l'IDS.

Cette étape nous permet de créer deux images disque dont l'un sert comme fichier boot système de l'IDS.

– **Étape 2 :** Charger une image IDS en utilisant Qemu

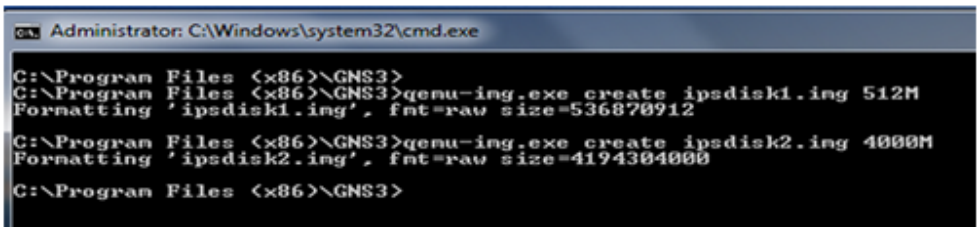


FIG. V.11 – Processus de récupération de l'image IDS.

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

Lorsque le système démarre, modifier l'entrée de démarrage GRUB (GRandUnified Bootloader) pour s'assurer que le système commence à niveau d'exécution 1 [3]. L'étape suivante consiste à démarrer à partir du disque.

[3]Promiscuous mode (traduit mode promiscuité), se réfère à une configuration de la carte réseau, qui permet à celle-ci d'accepter tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés. Ce mode est une fonctionnalité généralement utilisée pour écouter le trafic réseau

FIG. V.12 – Démarrage à partir du disque ré-imagé.

Dans le menu GRUB, appuyer 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. Et Changer l'option init = / loadrc à init = l, puis Enter suivi par "b" pour démarrer.

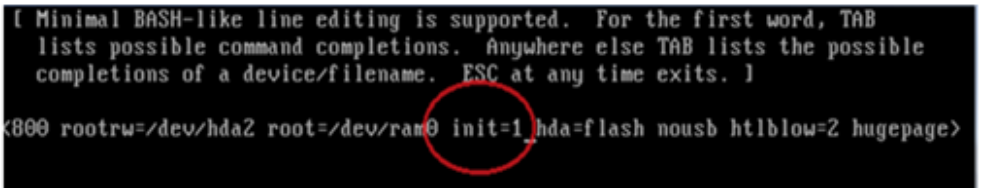


FIG. V.13 – Le menu GRUB d'initialisation de l'IDS.

Le logiciel IDS démarre maintenant au niveau d'exécution 1. Lorsque nous sommes invités, appuyer sur Enter et émettre les commandes suivantes :

```
/loadrc
 cd /etc/init.d
 ./rc.init
cpids_functionsids_functions.orig
vi ids_functions
```

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

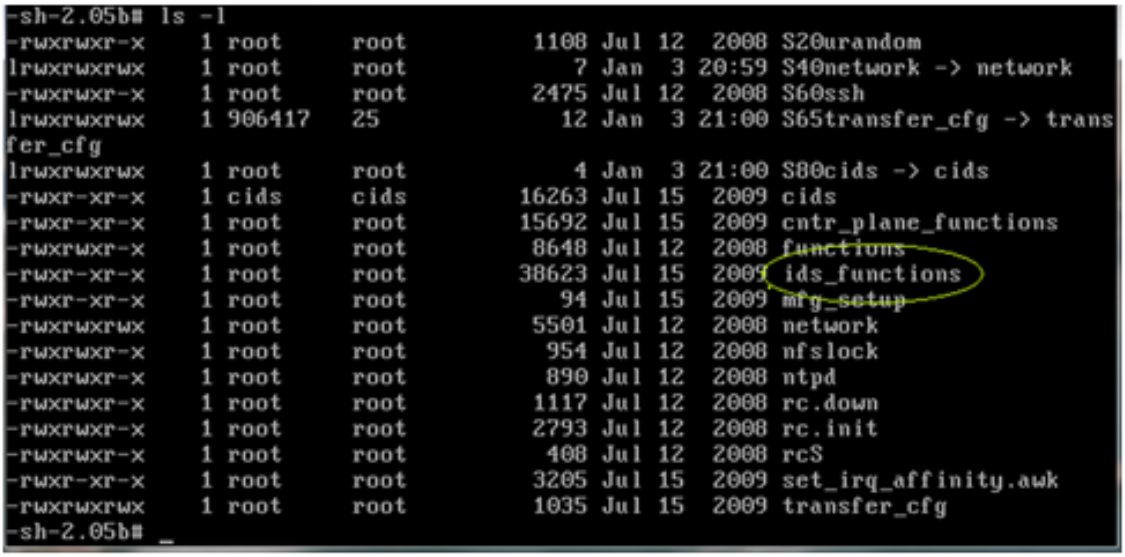


FIG. V.14 – La visualisation de la configuration.

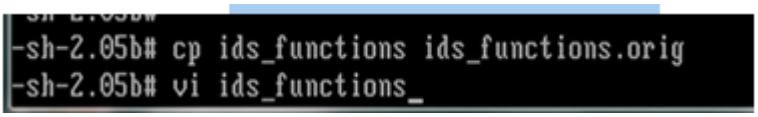


FIG. V.15 – Les commandes de configuration des fonctionnalités IDS.

Remplacer la première ligne (the elif statement) et les variables DEFAULT_MGT_OSetDEFAULT_MGT_CIDS à ce qui suit :

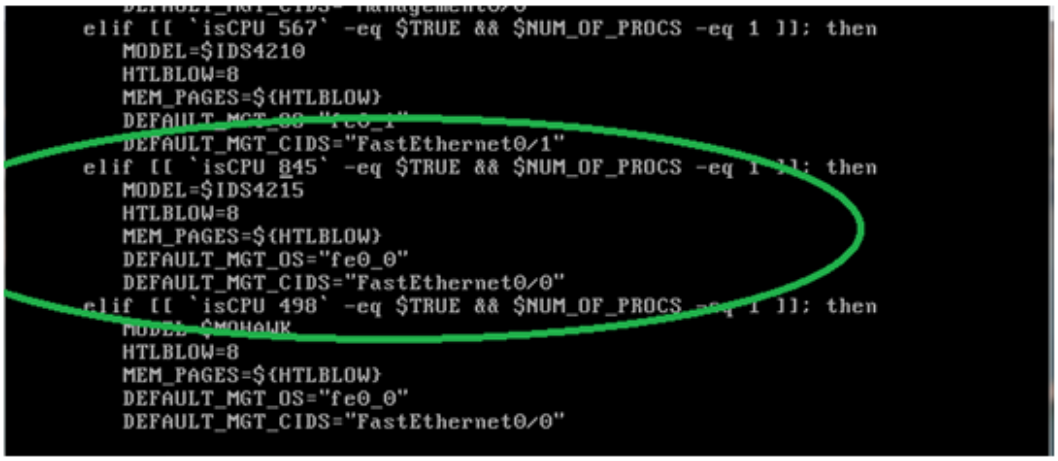


FIG. V.16 – La section du fichier 845.

```
elif [[ 1 -eq 1 ]]; then
        MODEL=$IDS4235
        HTLBLOW=32
MEM_PAGES=${HTLBLOW}
        DEFAULT_MGT_OS="ma0_0"
        DEFAULT_MGT_CIDS="Management0/0"
```

Sauvegardez et quittez vi.

– **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 :

FIG. V.17 – Les commandes de configuration d'interfaces IDS.

Avancer à la section qui traite la sonde 4235. Il faut seulement apporter des modifications aux sections [models/IDS-4250/interfaces/X] pour la configuration des interfaces.

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 :

FIG. V.18 – La configuration de l'interface Management.

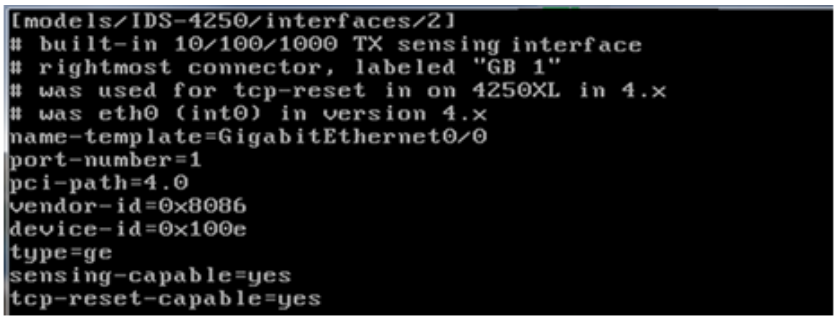


Fig. V.19 – La configuration de l'interface GigabitEthernet0/0.

Fig. V.20 – La configuration de l'interface GigabitEthernet0/1.

Fig. V.21 – La configuration de l'interface GigabitEthernet0/2.

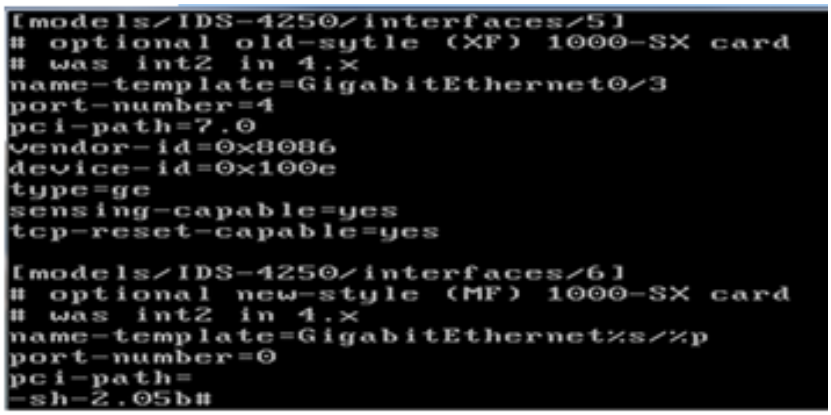


FIG. V.22 – La configuration de l'interface GigabitEthernet0/3.

Enregistrer les modifications, quitter vi et rechargerl'appareil.

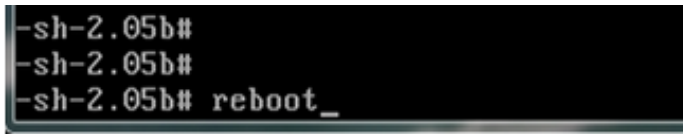


FIG. V.23 – Le redémarrage de la sonde.

Une fois redémarrer le sensor IDS demande un login et un mot de passe, les deux sont par défaut cisco. Nous avons la possibilité de les changés pour plus de sécurité.

II.3.1 L'intégration de l'IDS dans GNS3

Nous allons maintenant intégrer notre IDS dans GNS3 et le configurer pour qu'il soit installé aux points clés dans le réseau.

Aller dans Edit -Preferences -Qemu -IDS et apporter ces modifications :

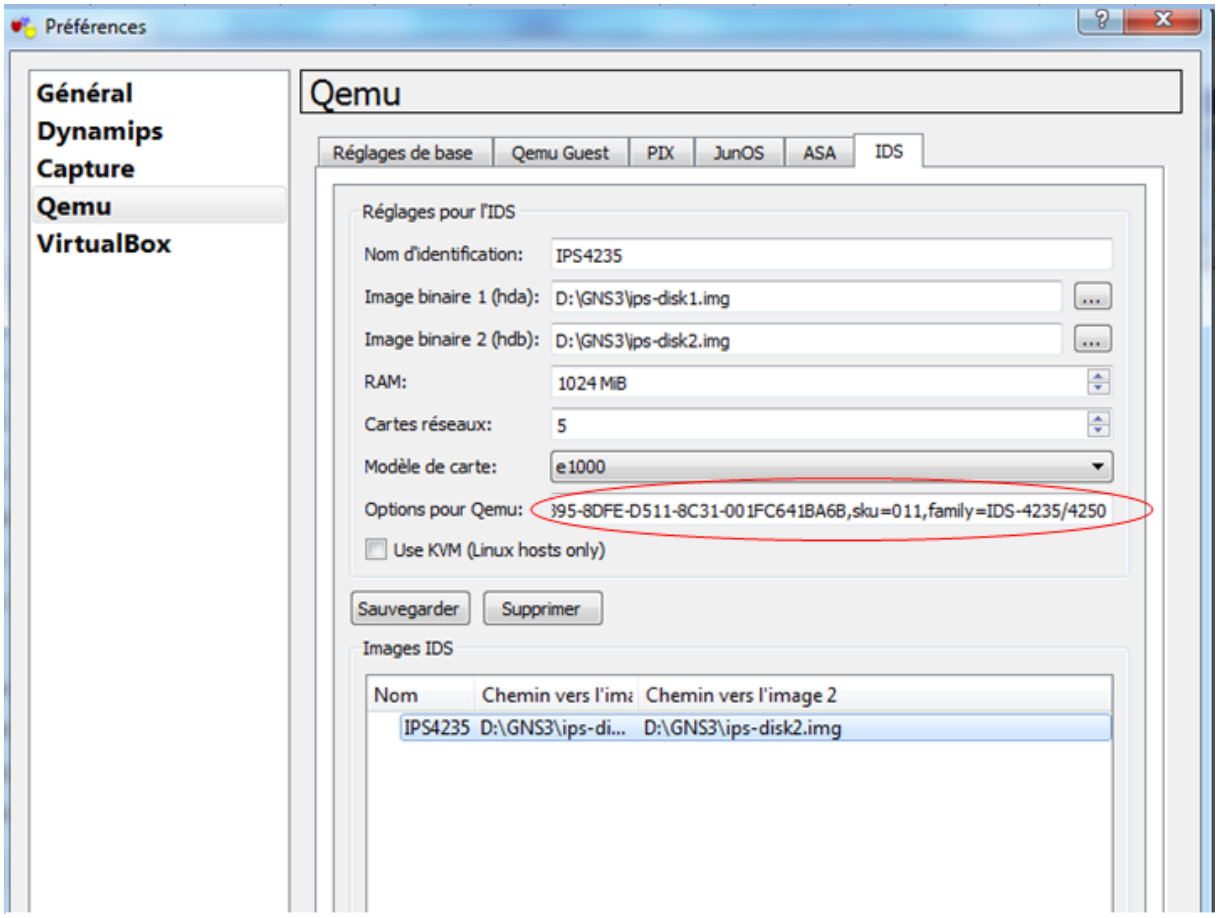


Fig. V.24 – Configuration de l'IDS sous GNS3.

Sous Qemu Options, modifier les paramètres SMBIOS [4]pour éliminer l'erreur de plate-forme non prise en charge comme illustrer ci-dessous.

```
-smbios type=1,product=IDS-4235,serial=12345789012,uuid=E0A32395-8DFE-D511-8C31-001FC641BA6B,sku=011,family=IDS-4235/4250
```

Fig. V.25 – Le paramètre SMBIOS pour la compatibilité de l'IDS

L'IDS est prêt maintenant à être configurer. Démarrer le à partir de GNS3, un accès CLI et aussi accès via IDM (IPS Device Manager) est possible pour la configuration de la sonde.

[4]Le démon syslogd permet d'enregistrer diverses activités du système, comme les messages de déboguage ou les avertissements affichés par le noyau. Son fichier de configuration, /etc/syslog.conf, permet de spécifier l'endroit où les informations doivent apparaître.

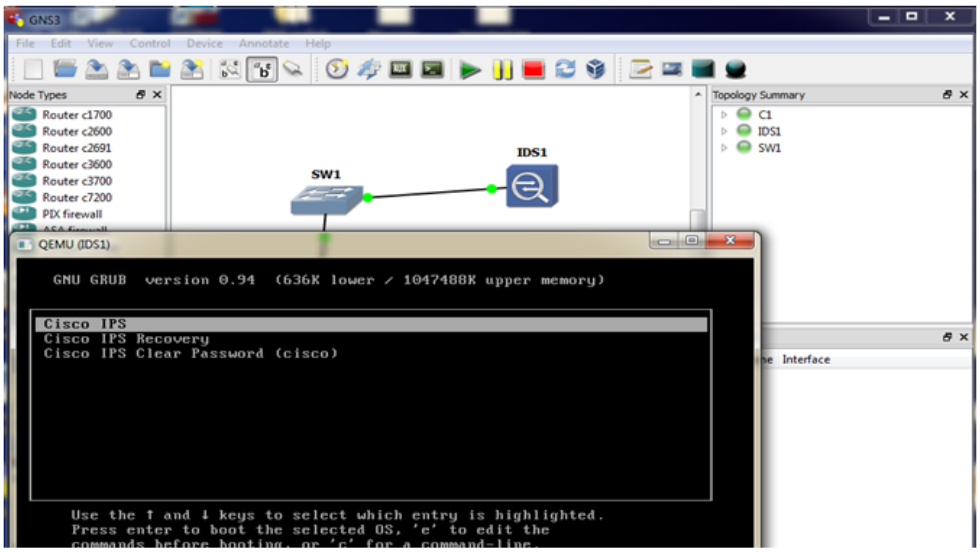


FIG. V.26 – Le démarrage de l'IDS sous GNS3.

– **Etape 1 : Initialisation du capteur via la CLI**

Avec la configuration de commande, nous pouvons configurer les paramètres de base du capteur, y compris les interfaces, le nom d'hôte IP, des listes de contrôle d'accès, et les paramètres du temps, etc.

L'utilisation de la configuration de commande est obligatoire pour l'initialisation du capteur, afin de pouvoir communiquer avec lui via le réseau, en suivant ces étapes :

1. saisir le sensor login et le Password par défaut (cisco).
2. Pour la première fois la CLI exige le changement de mot de passe par défaut.

   New password# nouveau mot de passe

   Retry password# nouveau mot de passe

3. Saisir setup puis Enter.

Dans cette section une suite de ligne s'affiche contenant des informations sur la configuration par défaut du capteur, continuer à taper sur Enter jusqu'à l'arrivée à une ligne ou s'affiche le message 'continue with configuration dialog ?

[Yes]', taper Enter pour pouvoir effectuer les configurations souhaiter et changer la configuration par défaut.

4. Changer le nom du capteur par défaut senssor
   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] :192.168.1.254/24,192.168.1.5
   Continuer à taper sur Enter jusqu'au linge où 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
6. Continuer à taper sur Enter jusqu'à ce que un message de demande de sauvegarde s'affiche, enregistrer et quitter.

Remarques

1. les valeurs qui s'affichent entre crochets dans la configuration par la CLI sont les valeurs par défauts.
2. Pour voir la configuration initiale du capteur taper show configuration.

```
Setup Configuration last modified: Thu Jun 13 02:29:56 2013

Continue with configuration dialog?[yes]:
Enter host name[sensor]: IDS
Enter IP interface[192.168.1.2/24,192.168.1.1]: 192.168.1.254/24,192.168.1.5
Enter telnet-server status[disabled]:
Enter web-server port[443]:
Modify current access list?[no]: yes
Current access list entries:
  No entries
Permit: 192.168.1.0/24
Permit:
Modify system clock settings?[no]:
Modify interface/virtual sensor configuration?[no]:
Modify default threat prevention settings?[no]: _
```

Fig. V.27 – La configuration initiale du capteur.

Nous pouvons continuer a utilisé la configuration avancée dans la CLI pour activer Telnet, configurer le serveur Web, et d'attribuer et activer les capteurs et les interfaces virtuelles, ou nous pouvons utiliser l'assistant de démarrage IDM.

Pour notre projet nous avons choisi la configuration par l'interface graphique IDM.

a. IDM (IPS Device Manager) : L'IDM Cisco est une interface web basé sur Java qui permet de configurer et de manipuler le fonctionnement des détecteurs 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 **W23**.

b. La configuration requise de l'IDM : IDM est une application basée sur le Web, l'exigence majeure du système est un navigateur web, avoir suffisamment de mémoire (minimum 256Mo) et une résolution de l'écran favorise également le fonctionnement efficace de l'IDM (minimum 1024 x 768 et 256 couleurs). Pour les besoins de configuration il est d'abords recommandé d'installer la version Java 1.5 et si elle existe la version 1.7 il faut la désinstaller.

– **Etape 2 : La configuration via l'interface graphique IDM**

1. Saisir l'adresse IP du capteur dans le navigateur web sous forme d'une URL et utiliser le protocole http sécurisé (https) : https ://192.168.1.254/
2. Une page de certification s'affiche, cliquer sur 'Pour suivre avec ce site Web (non recommandé)'.
3. une fenêtre s'affiche c'est la page d'accueil d'IDM, cliquer sur Run IDM afin d'accéder à l'interface graphique.

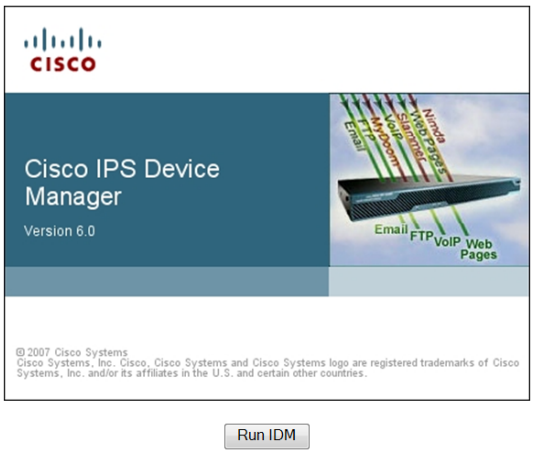


FIG. V.28 – L'interface d'accueil d'IDM.

Une fenêtre d'avertissement de sécurité s'affiche, cliquer sur oui en suite une seconde fenêtre d'authentification 'Cisco IDM Launcher' s'affiche, introduire le login et le mot de passe et cliquer sur Ok.

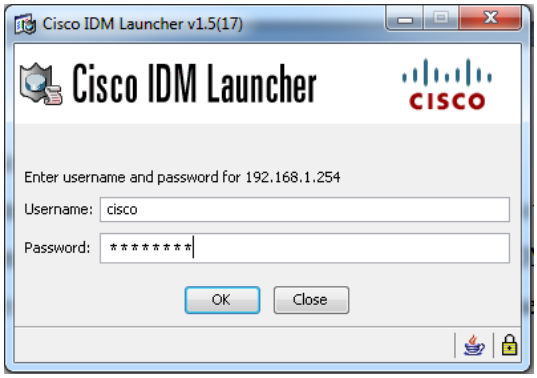


FIG. V.29 – Fenêtre d'authentification Cisco IDM Launcher

4. La fenêtre ci-dessous s'ouvre c'est la fenêtre de configuration d'IDM qui affiche les informations de l'appareil telles que le nom d'hôte, l'adresse IP, la version et le modèle.

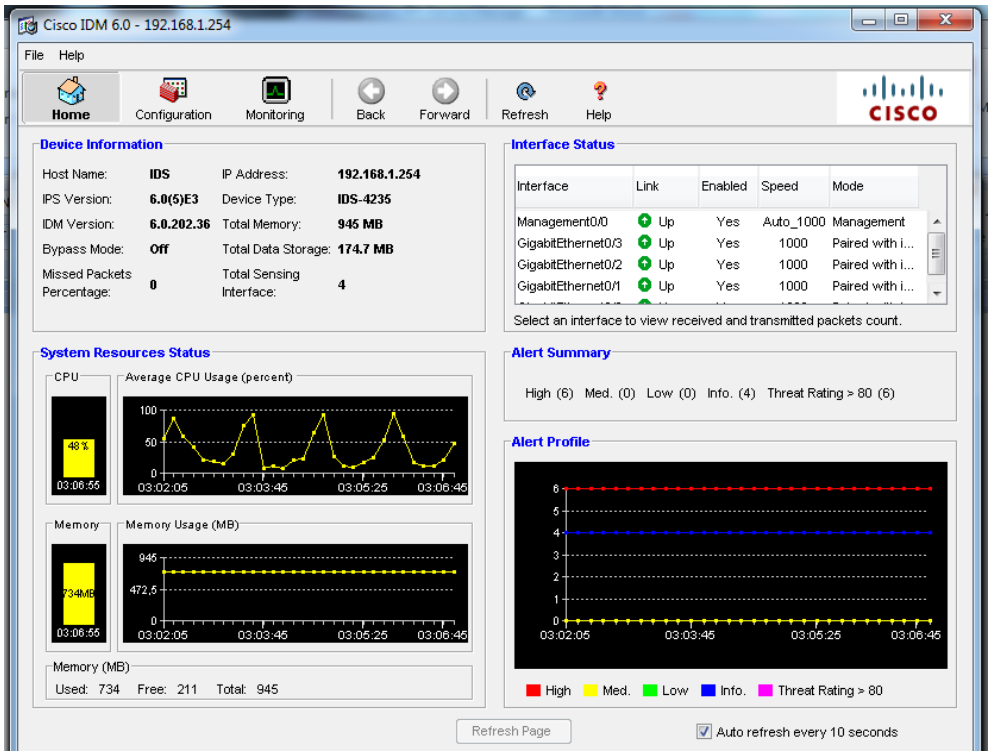


FIG. V.30 – Interface graphique d'IDM.

La configuration des caractéristiques du fonctionnement du capteur est la principale fonctionnalité fournie par l'IDM. En cliquant sur l'icône Configuration, une liste des éléments configurables s'affiche sur le côté gauche de l'écran. Ces éléments sont répartis dans les catégories opérationnelles suivantes :

A) 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. Nous pouvons appliquer une politique ou une configuration différente pour chaque capteur virtuel au sein d'un capteur physique ou également appliquer la même instance politique, à différents capteurs virtuels.

Le capteur VS0 est le capteur par défaut à qui nous avons appliqué une politique de configuration pour tous les flux de données surveillées.

Cette section montre la configuration des utilisateurs du système, les paramètres de temps du capteur,etc.

a. Allowed Hosts : permet de définir les adresses IP qui sont autorisés à accéder au capteur via son interface de gestion, donc ajouter l'adresse IP de l'administrateur qui est 192.168.2.1 et le masque réseau 255.255.255.255 en suivant les étapes montrer dans la figure suivante :

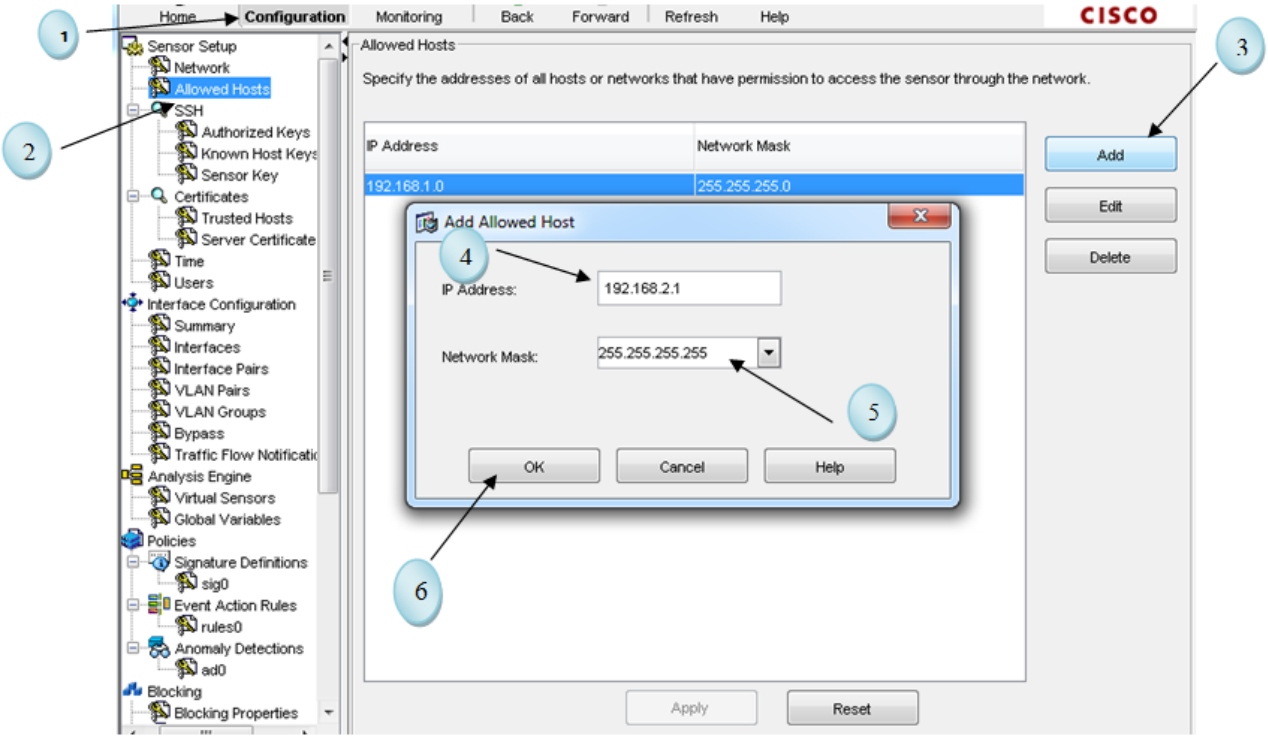


FIG. V.31 – Définir l'adresse IP à d'accès au capteur.

Cliquer sur **Apply** pour enregistrer la configuration.

b. Users : Permet de visualiser les utilisateurs actuellement configurés, ajouter des utilisateurs, et changer les mots de passe des utilisateurs via un compte privilégié. Sinon il est seulement possible de changer le mot de passe.

L'utilisateur par défaut est cisco avec des privilèges administrateur et mot de passe blablabla, il est impossible de le supprimer ou changer son nom(Username).

Changer les privilèges de l'utilisateur cisco en Viewer, en suite Ajouter un administrateur comme montrer ci-dessous :

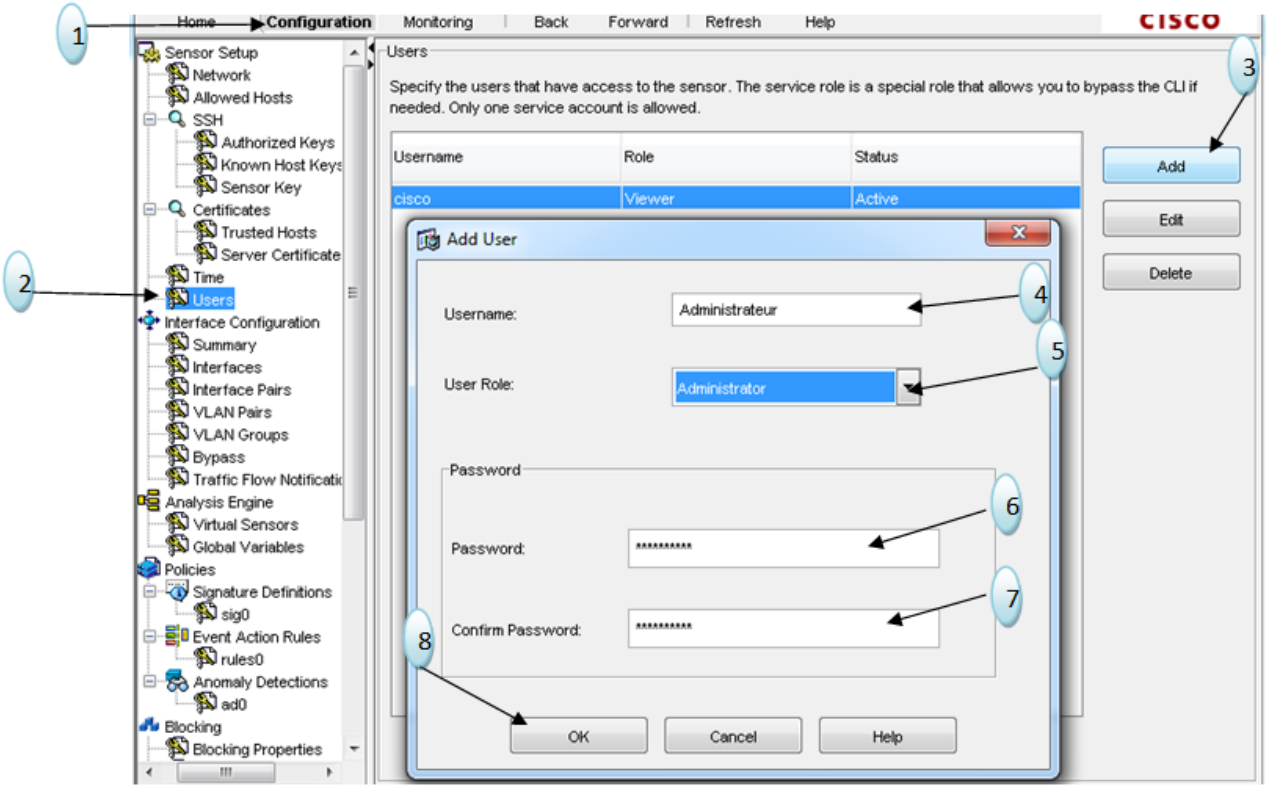


FIG. V.32 – Ajouter un utilisateur.

Cliquer sur **Apply** pour enregistrer la configuration.

B) Configuration des interfaces (Interface Configuration)

Chaque fois que le capteur est allumé, il détecte automatiquement les modules d'interfaces qui sont installés, et pour la surveillance du trafic, les interfaces doivent d'abord être activées.

1. Aller dans Configuration-Interface Configuration-Interfaces et sélectionner le nom de l'interface. Ensuite, cliquer sur Edit pour modifier l'interface de détection et configurer les informations Enable, Duplex, Speed et Default VLAN comme montrer sur la figure suivante :

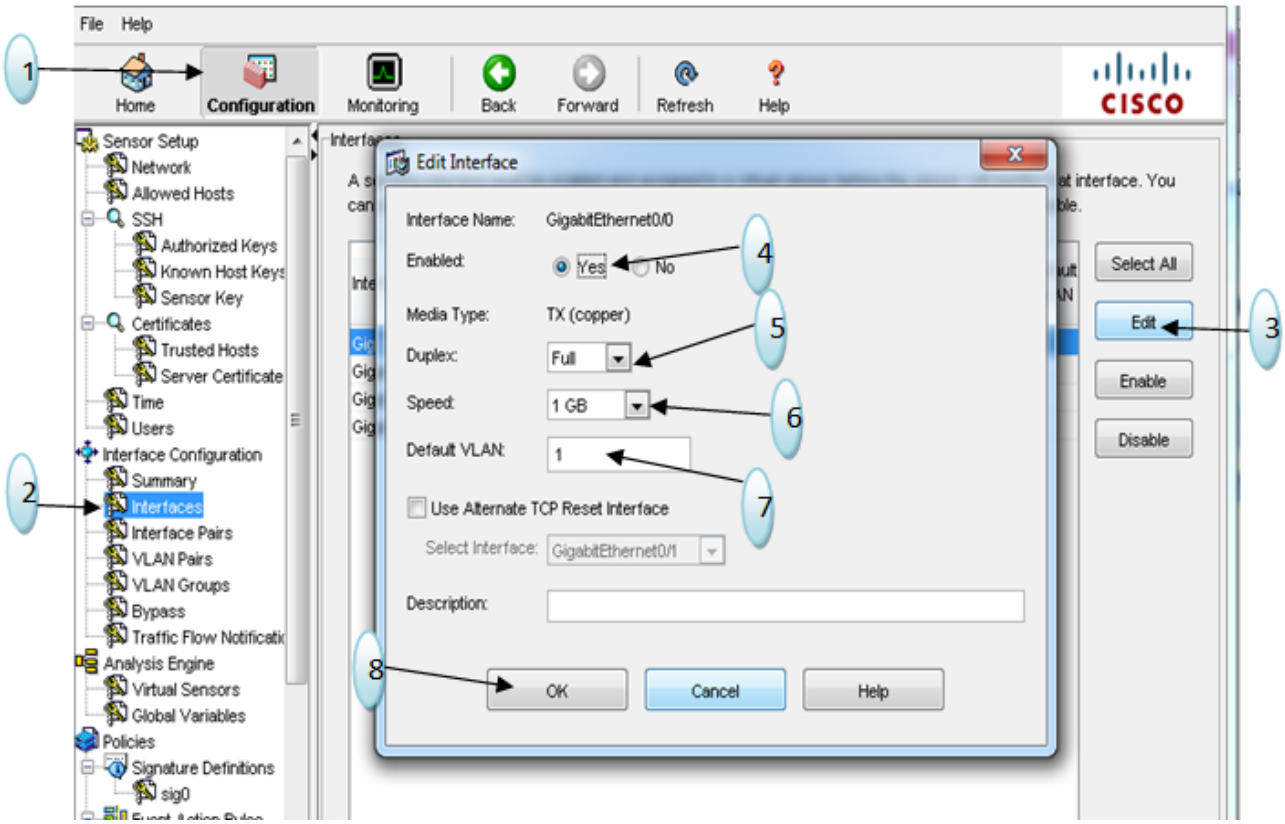


FIG. V.33 – Configuration des interfaces de détection.

Cliquer sur **Apply** pour enregistrer la configuration.

2. Les interfaces réseau permettent au capteur de surveiller le trafic réseau en utilisant des modes de fonctionnement en ligne. Donc créer d'abord ces paires d'interfaces en ligne tel que la première paire est composée des deux interfaces GigabitEthernet0/0 et GigabitEthernet0/3, la seconde paire de GigabitEthernet0/1 et GigabitEthernet0/2 comme suit :

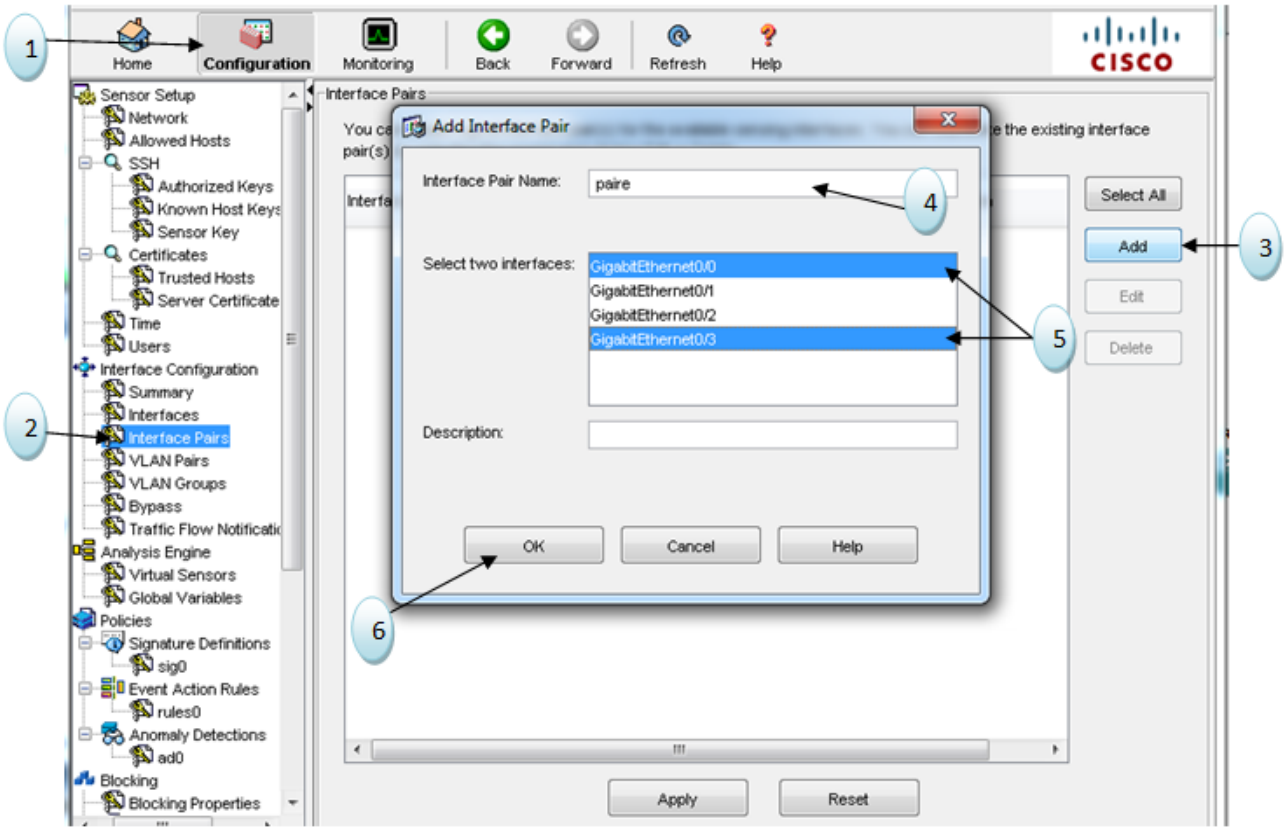


FIG. V.34 – Ajout d'une paire d'interface en ligne.

Idem pour la création de la seconde paire d'interface en ligne, en suite cliquer sur **Apply** pour enregistrer la configuration.

3. Aller dans l'option Bypass pour configurer le mode de dérivation de logiciel, qui détermine comment le trafic réseau est assuré pendant les interruptions opérationnelles dans les applications de contrôle de la sonde, choisir l'option "off (Always inspect inline traffic)" et Cliquer sur **Apply** pour enregistrer la configuration.

C) Le moteur d'analyse (Analysis Engin)

Le moteur d'analyse effectue une analyse de paquets et de détection d'alerte. Il surveille le trafic qui traverse une interface spécifique. Nous créons des capteurs virtuels dans le moteur d'analyse. Chaque capteur virtuel possède un nom unique avec une liste d'interfaces. Pour éviter les conflits ou les chevauchements dans

les affectations, nous attribuons une interface à un capteur virtuel spécifique afin qu'aucun paquet ne soit traité par plus d'un capteur virtuel. Chaque capteur virtuel est également associé à une définition spécifique (signatures, règles d'action d'événement, et la configuration de détection d'anomalies).

Attribuer les deux paires d'interfaces crées au capteur comme suit :

Aller dans Configuration-Virtual Sensors et dans la fenêtre qui s'affiche cliquer sur Edit une autre fenêtre s'affiche, suivre les étapes montrer sur cette figure :

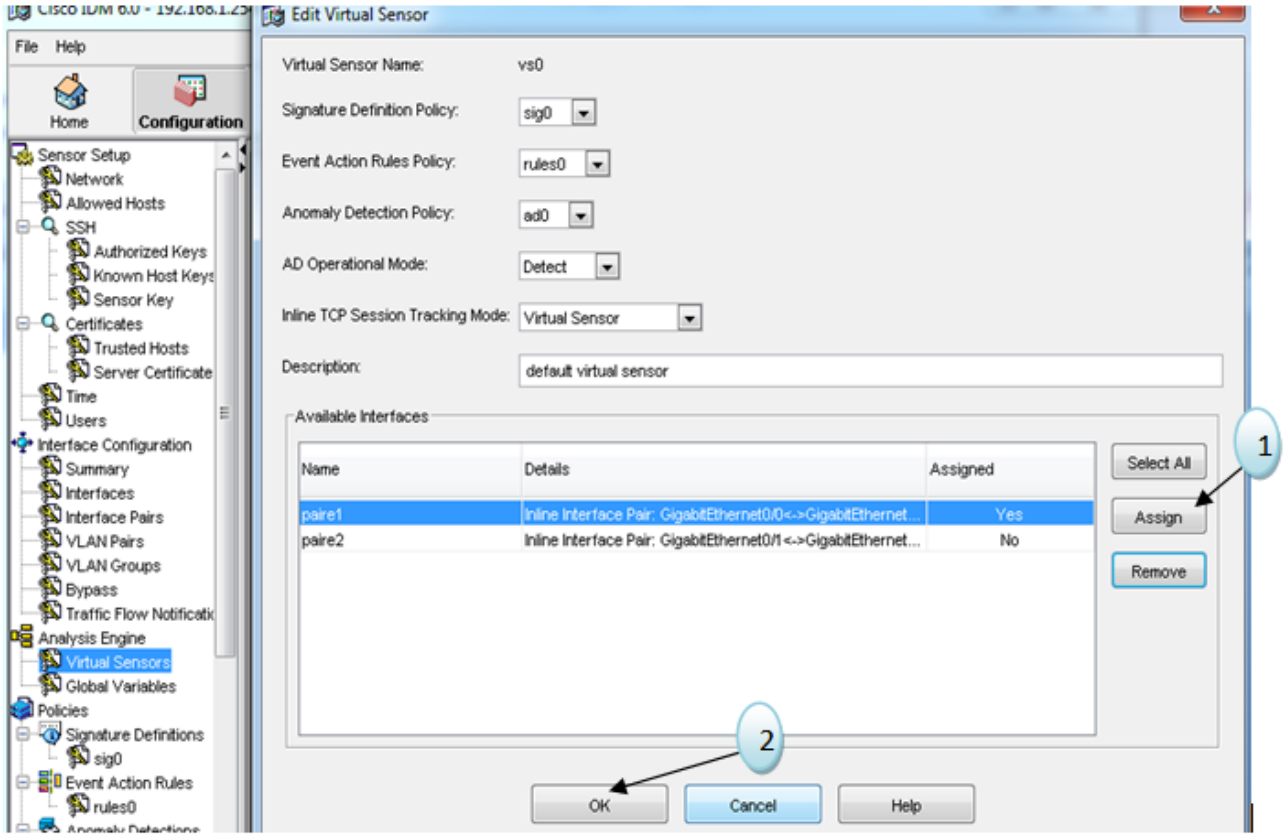


FIG. V.35 – Attribution de paire d'interfaces en ligne au capteur Vs0.

Idem pour la seconde paire d'interfaces, cliquer sur **Apply** pour enregistrer la configuration.

D) Définition de Signatures (Signature Definitions)

Une signature est un ensemble de règles qui utilise un capteur pour détecter l'activité intrusive. Comme le capteur analyse le trafic réseau, il recherche les correspondances aux signatures qu'il est configuré pour détecter. Quand un match à une signature est trouvé, le capteur prend ces mesures selon la configuration effectué pour cette signature.

L'option définition de signature comporte les options suivantes :

1. **Configuration de Signature (Signature configuration)**

   En utilisant l'option configuration de signature, il est possible de voir les signatures disponibles (en sélectionnant dans le champ Select By le type de recherche soit par le nom de signature, son identificateur, etc) et leurs propriétés, les activer ou désactiver ainsi que l'ajout de nouvelles signatures et modifier les propriétés des signatures existantes. Les deux signatures 2000 et 2004 permettent la fonction de ping, par défaut elles sont désactivées, pour les activées, procéder comme montrer ci-dessous :

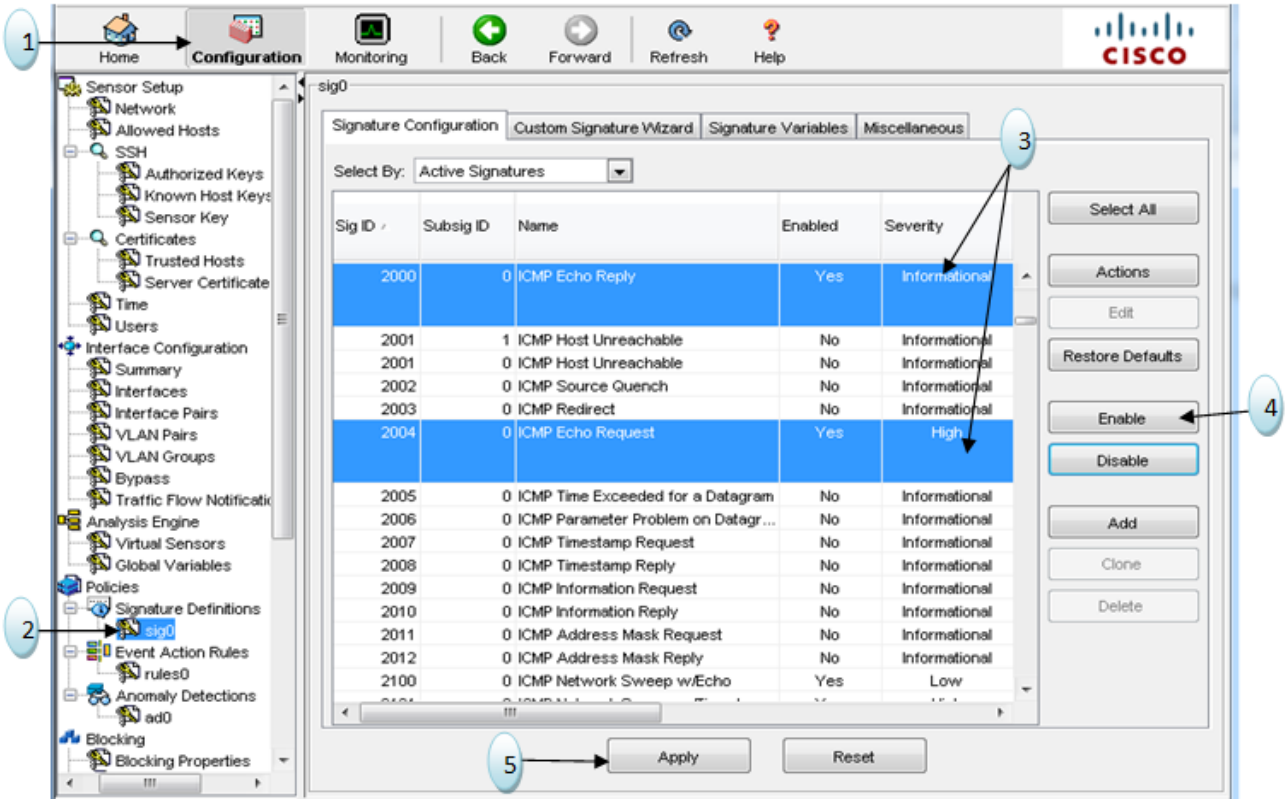


FIG. V.36 – Activation de signatures.

Il est possible de configurer les actions à prendre quand un match (motif)correspond à ces signature est trouvé, cliquer sur le bouton Action un Menu s'affiche et coucher les cases selon les action voulu prendre en cas d'attaque détecter.

2. **Variables de signature :** En utilisant l'option Variables Signature, il est possible de définir des plages d'adresses IP et utiliser ces variables de signature lors de la définition de signatures. Lors du modification de la valeur de la variable, le changement est automatiquement répliqué sur toutes les signatures où il est référencé, il est également possible de modifier la variable de signature prédéfini qui détermine quels ports sont examinés lors de l'analyse Web.

E) Règles d'action d'événement (Event Action Rules) : Les règles d'action d'événement définissent comment le capteur traite des événements spécifiques

quand elles sont détectées sur le réseau, ils définissent les fonctions suivantes sur le capteur :

a. L'événement action catégorie Règles offre les options suivantes :

- **Variables d'événements :** Il est possible de définir des variables à utilisez lors de la définition des filtres d'événements.
- **Valeur cible Note :** La valeur cible notes permet de configurer une note atout pour les plages d'adresses IP spécifiques. L'évaluation des biens peut être une des valeurs suivantes : Aucune valeur, Faible, Medium, Élevé ou Mission critique.Alors définir les plages d'adresses de notre réseau en mettant la note à Élevé (high) :

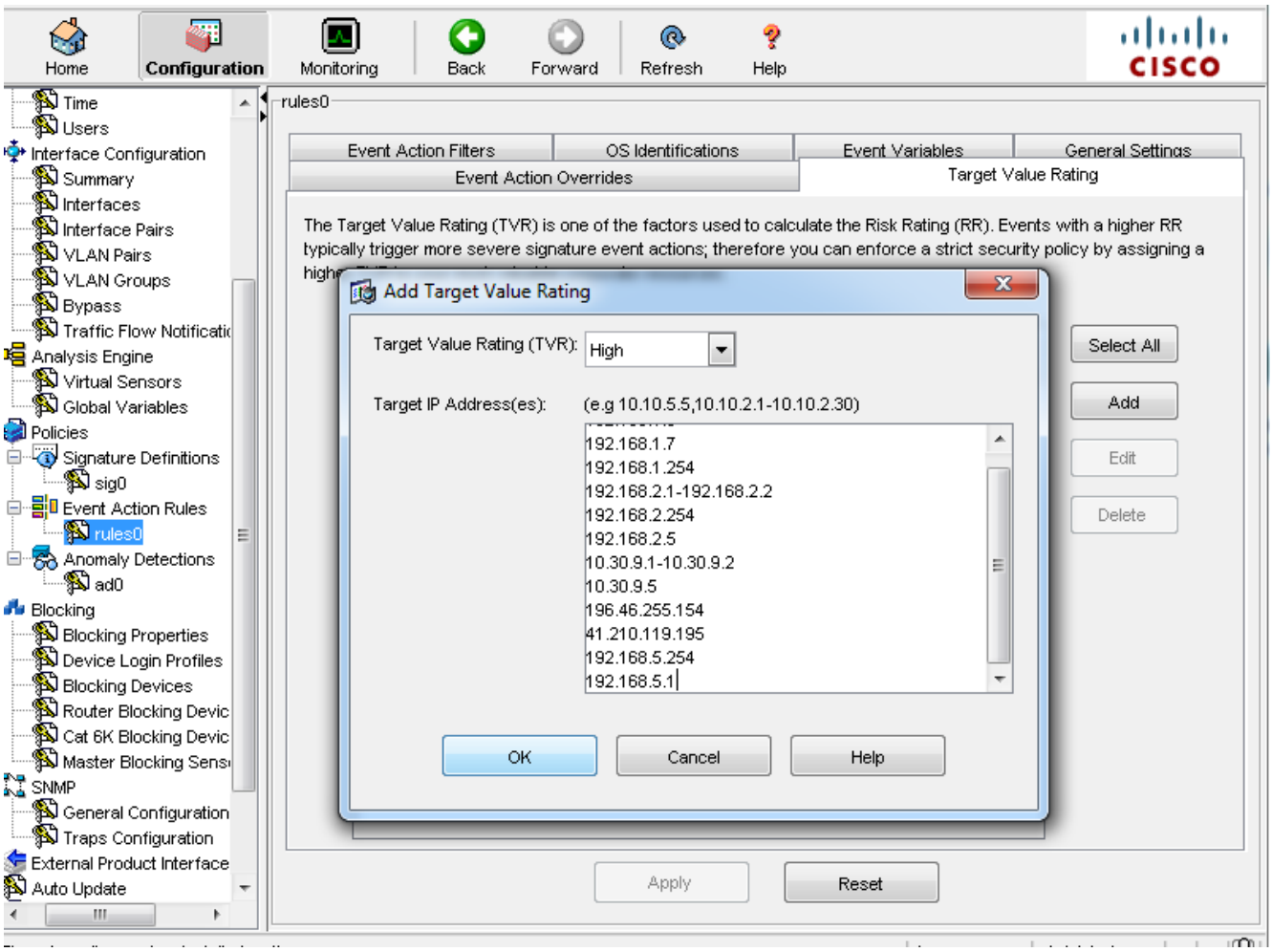


FIG. V.37 – Ajout de note.

b. Filtres d'actions d'événements

L'option filtres d'action d'événement permet de définir des filtres d'action d'événement. Ces filtres empêchent les actions(ou filtres) configurées d'être appliquée à des événements spécifiques. Les filtres peuvent être basés sur de nombreux facteurs tels que l'adresse IP, l'ID de la signature, et évaluation du risque.

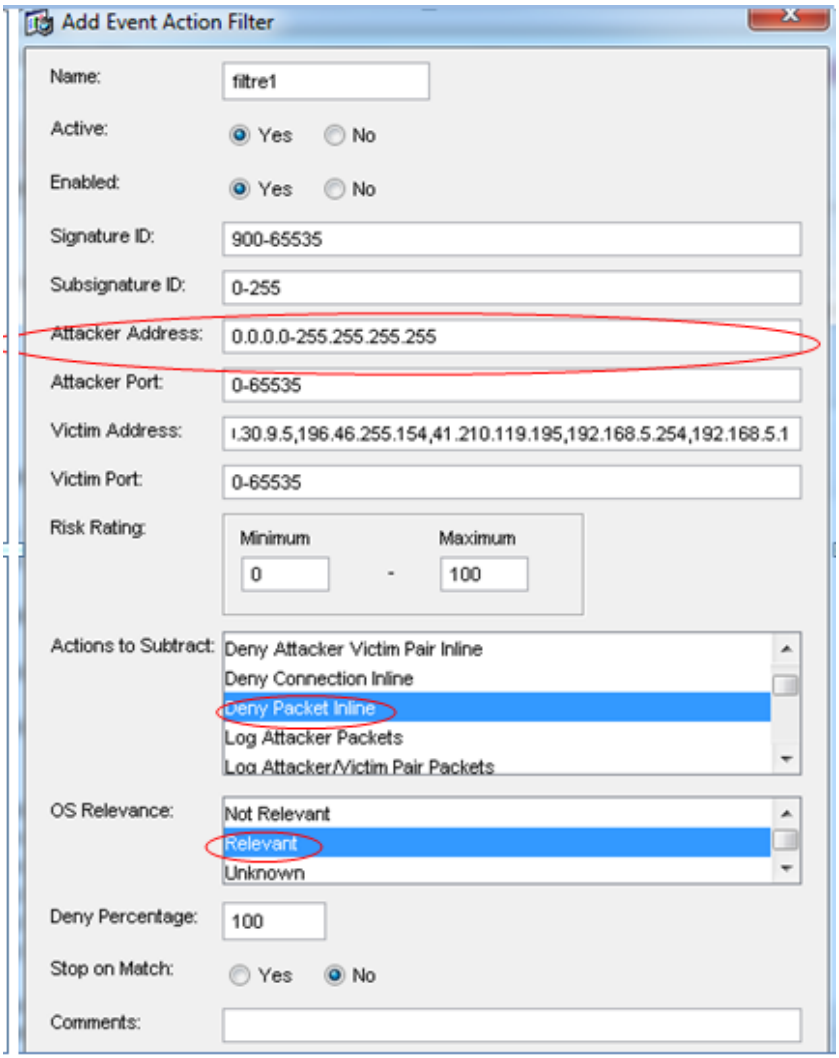


FIG. V.38 – Ajout d'un filtres d'actions d'événements

c. Paramètres généraux

L'option Paramètres généraux permet de définir les paramètres généraux qui s'appliquent à des règles d'action d'événement. Il s'agit notamment des paramètres suivants :

- La durée d'interdiction de l'attaquant.
- Durée de bloc d'action.
- Nombre maximum d'attaquants refusés.

F) Blocage (Blocking)

L'une des actions à configurer au capteur à prendre lors de déclenchement d'une signature consiste à bloquer le trafic du système qui a initié le trafic intrusif. Les deux types d'actions de blocage à configurer sont les suivantes :

- bloc d'accueil.
- Bloc de connexion.

Lorsqu'une signature est configurée pour bloquer une connexion, il bloque uniquement le trafic à partir de l'hôte qui a déclenché la signature au port de destination, le protocole (TCP ou UDP), ainsi que l'adresse IP de destination qui a déclenché la signature. Par conséquent, la décision de blocage est basée sur les paramètres suivants :

- adresse IP source.
- adresse IP de destination.
- Port de destination.
- Protocole.

Un bloc d'accueil, d'autre part, bloque tout le trafic de l'hôte attaquant quel que soit le port de destination, le protocole ou l'adresse IP de destination.

La catégorie de blocage présente les options de configuration suivantes :

. **Propriétés de blocage :** Utiliser l'option propriétés de blocage pour configurer les propriétés de blocage de base ainsi que les adresses IP que les dispositifs de blocage ne doivent jamais bloquer.

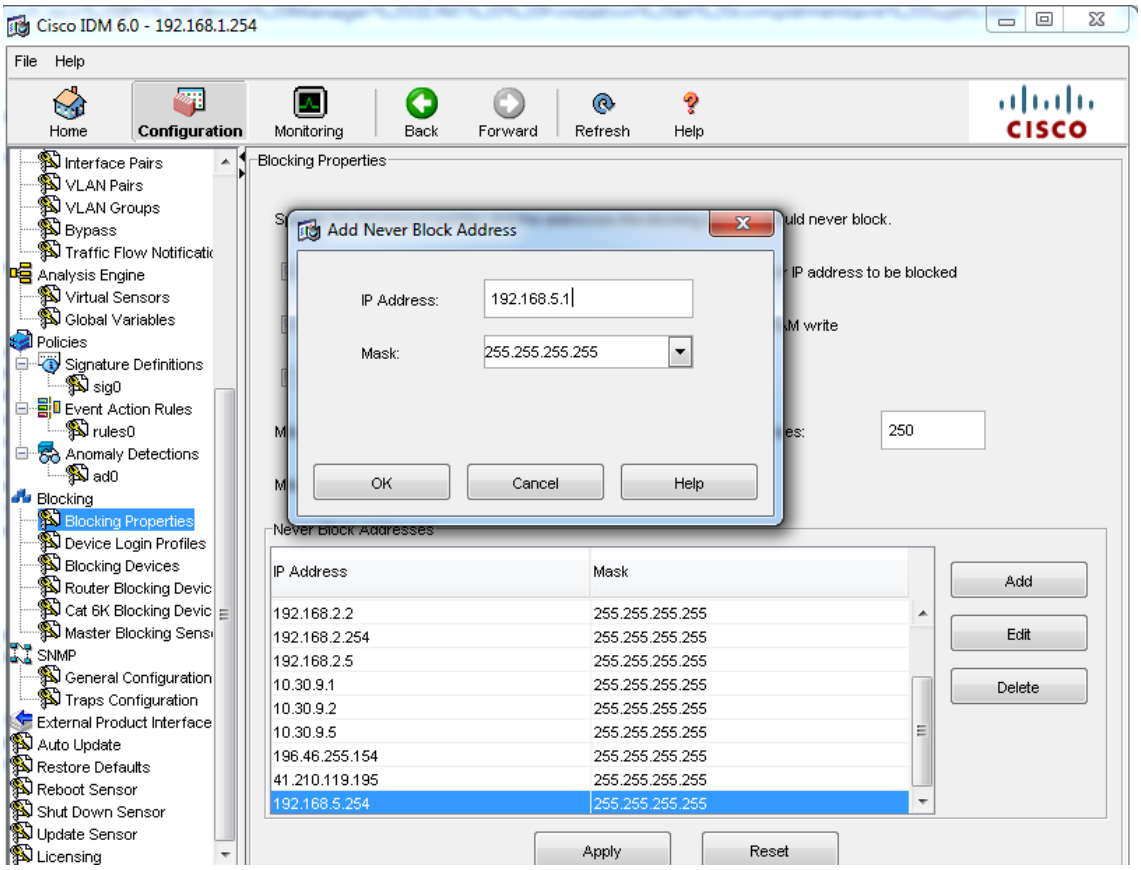


FIG. V.39 – Propriétés de blocage.

G) Surveillance

En plus de la configuration du capteur, IDM offre également la possibilité de surveiller l'état et le fonctionnement du capteur. La fonctionnalité de surveillance est divisée en ces options suivantes :

- **Les attaquants refusé :** permet d'afficher les adresses IP qui sont actuellement bloqués par le capteur.
- **Blocs hôte actif :** permet de bloquer manuellement des hôtes spécifiques pour une durée spécifiée.
- **activé blocs d'accueil :** permet de bloquer manuellement des hôtes spécifiques pour une durée spécifiée.
- **Blocs de réseau :** L'option Blocs de réseau permet d'établir manuellement un bloc pour l'ensemble du réseau.

. **Logging IP :** L'option de journalisation IP, pour spécifier la collection manuellement du trafic d'un hôte spécifié.

. **Events :** Afficher les événements générés par le capteur.

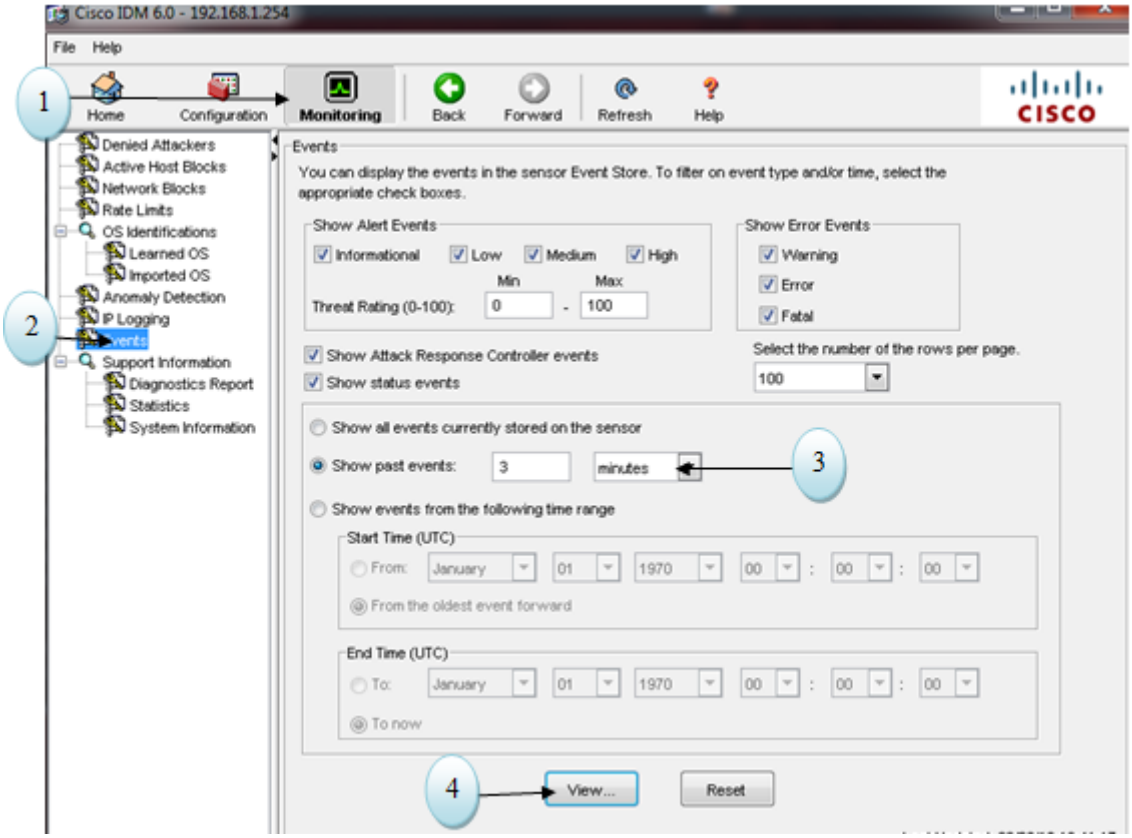


FIG. V.40 – Accéder au journal.

III Test

Nous avons traité deux scénarios :

III.1 Scénario 1

Dans le cas de la détection d'un trafic malveillant l'IDS génère une alerte, donc choisir l'option 'produce Alert ' pour notre signature comme suit :

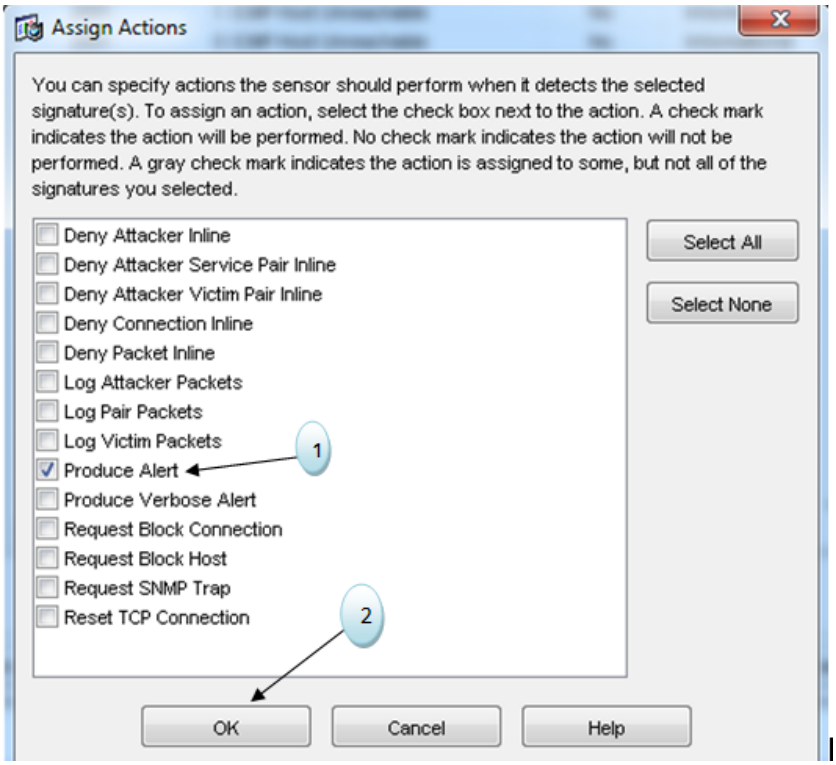


FIG. V.41 – Définir la politique 'produce Alert'

III.2 Scénario 2

Dans le cas de la détection d'un trafic malveillant l'IDS refuse ce trafic, donc choisir l'option 'Deny Attacker Inline' comme suit :

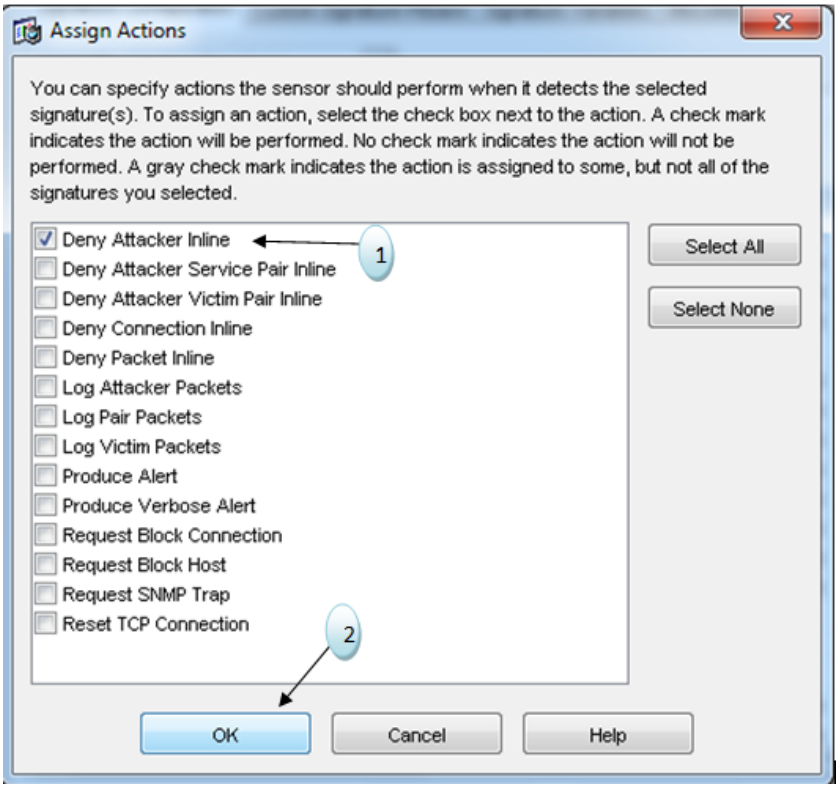


FIG. V.42 – Définir la politique 'Deny Attacker Inline'.

Dans ce qui suit, nous allons donner pour chaque test le résultat de chaque scénario.

a. La fonction ping

La fonction ping se base sur ces deux requêtes ICMP Echo Reply et ICMP Echo Request, alors activer ces deux signatures dont 'Sig ID' est 2000 et 2004 respectivement.

1. Pour le premier scénario faire un ping de la machine Pirate vers un équipement du réseau local (par exemple vers la machine Pc1) ça va générer une alerte, comme montrer ci-dessous :

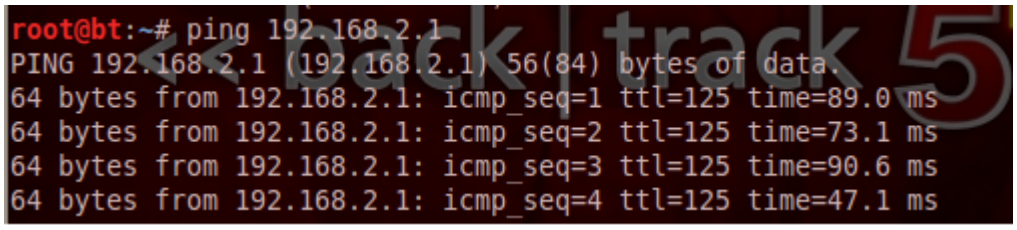


FIG. V.43 – Résultat du ping de Pirate vers Pc1.

Accéder au journal. Sur la fenêtre qui apparait modifier les paramètres d'affichage puis cliquer sur View.

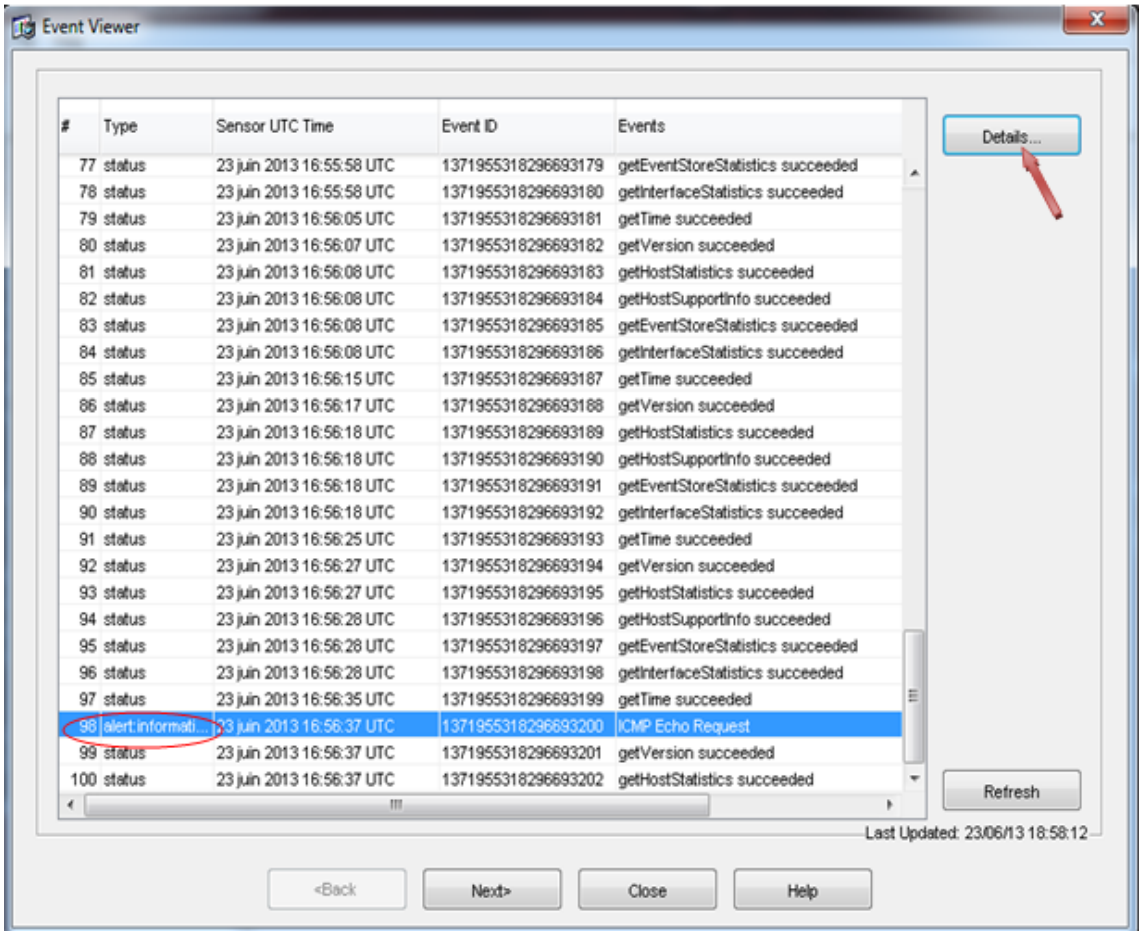


FIG. V.44 – Affichage d'une alerte.

Cliquer sur Détails pour voir les détailles de l'alert.

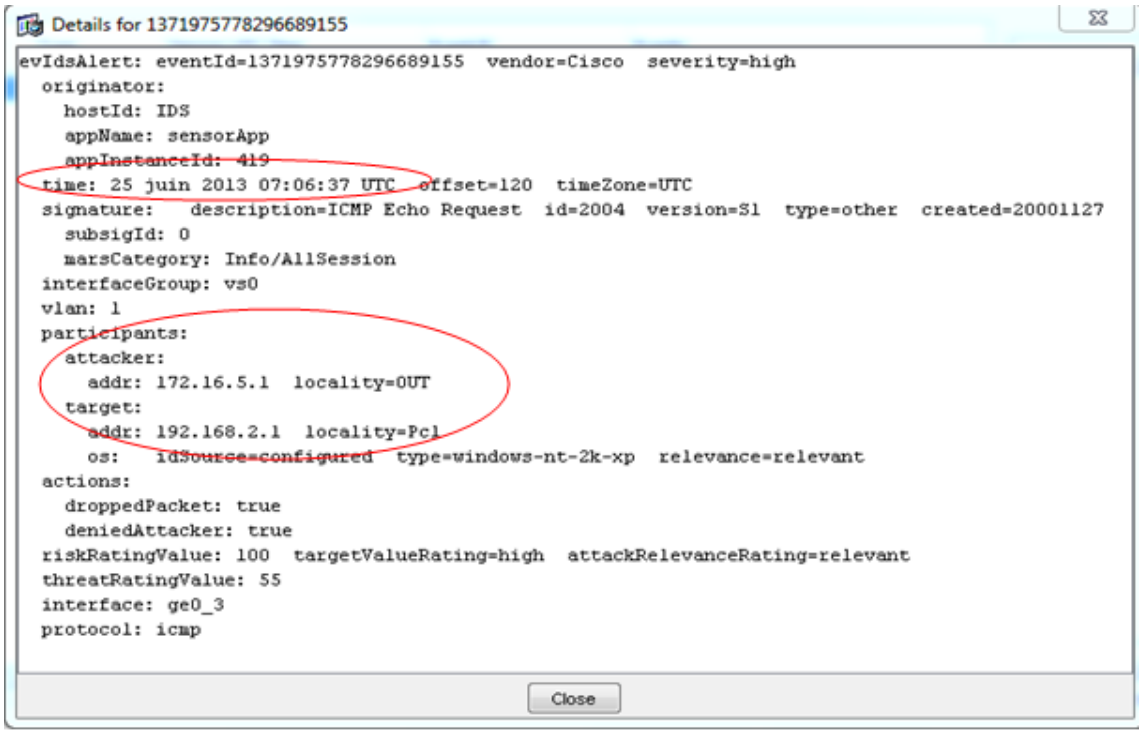
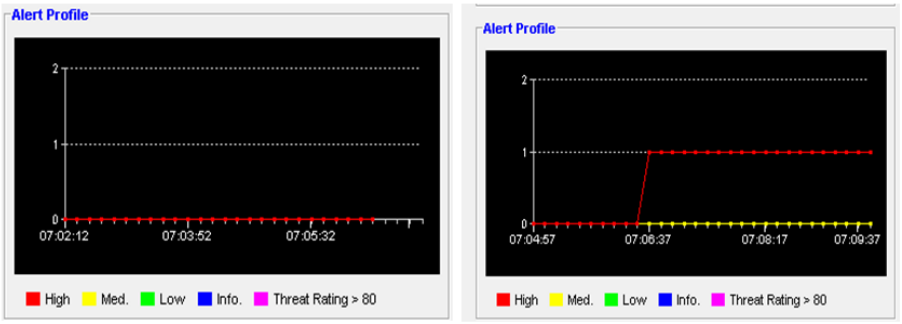


FIG. V.45 – Affichage des détails de l'alerte.

Sur le profil d'alerte qui s'affiche sur la page d'accueil en observe le changement de son état :



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

FIG. V.46 – Comparaison entre les deux états

L'axe des y représente l'estampille de l'événement et l'axe des x le nombre d'attaquant.

2. Pour le deuxième scénario lorsque le pirate essaye de faire un ping vers un équipement du réseau local (par exemple vers la machine Pc1) 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 :

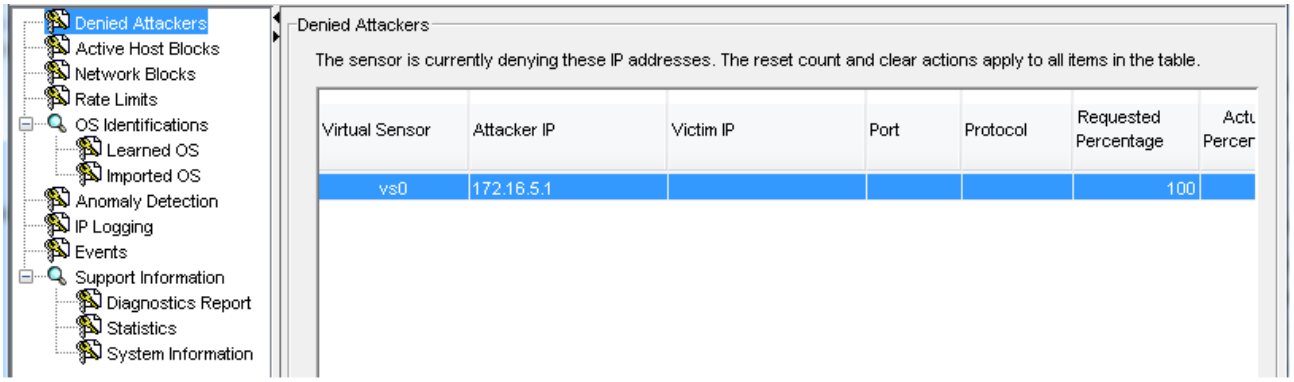


FIG. V.47 – Blocage du pirate par l'IDS

Par exemple faire un ping de Pc1 vers User ça ping par contre le sens inverse va bloquer User. (voir la figure)

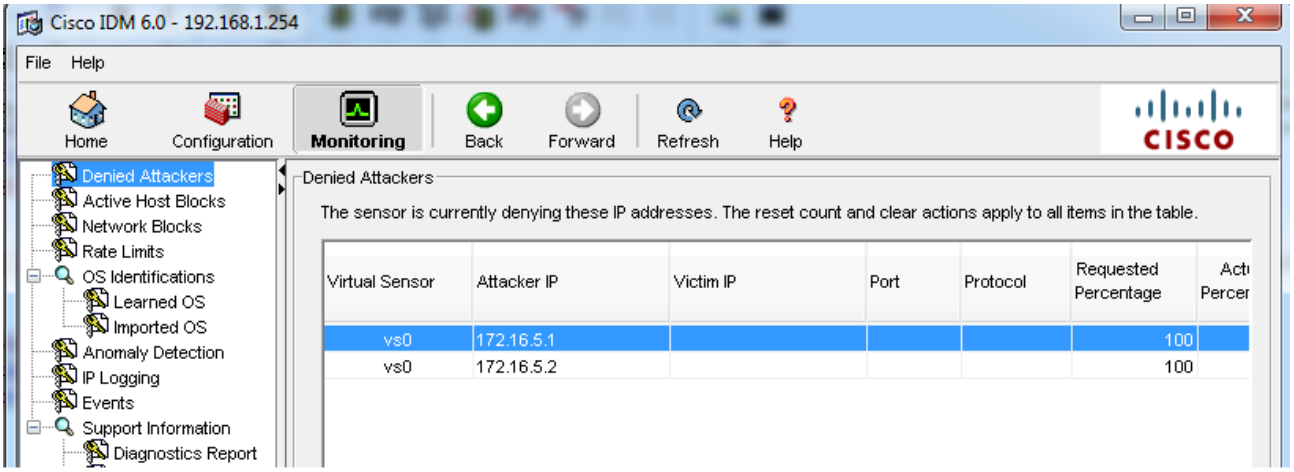
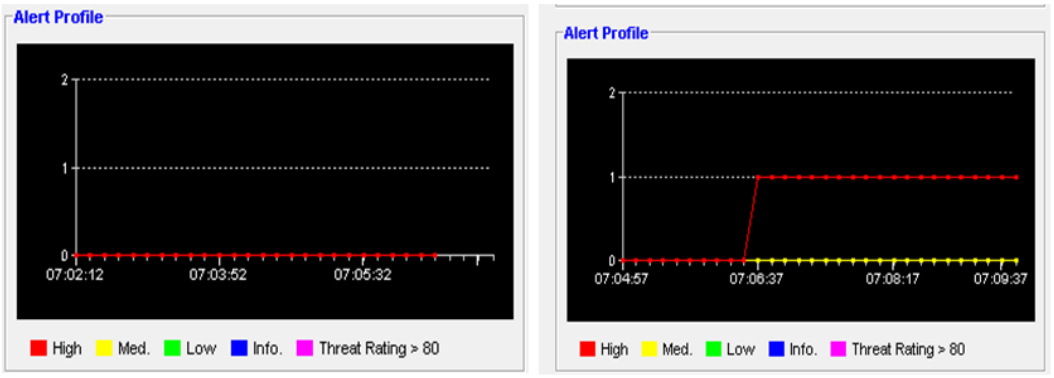


FIG. V.48 – Blocage du User par l'IDS

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'émetteur extérieure.

Cette figure montre le changement de la courbe, tel que le nombre d'attaquant augmente à deux



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

FIG. V.49 – Changement de l'état de la courbe

b. Le Scan réseau

Le Scan réseau se base sur le ping, et la requête ICMP Network Sweep w/Echo.

Voici d'abord le résultat du Scan réseau effectué par le Pirate

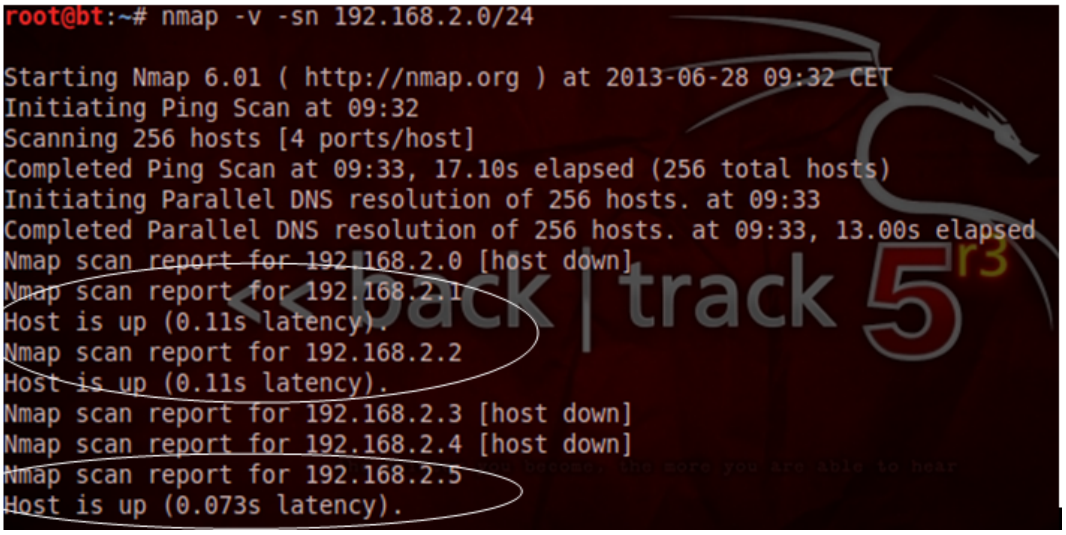


FIG. V.50 – Le Scan réseau

Dans cette figure illustre l'alerte déclencher par l'IDS.

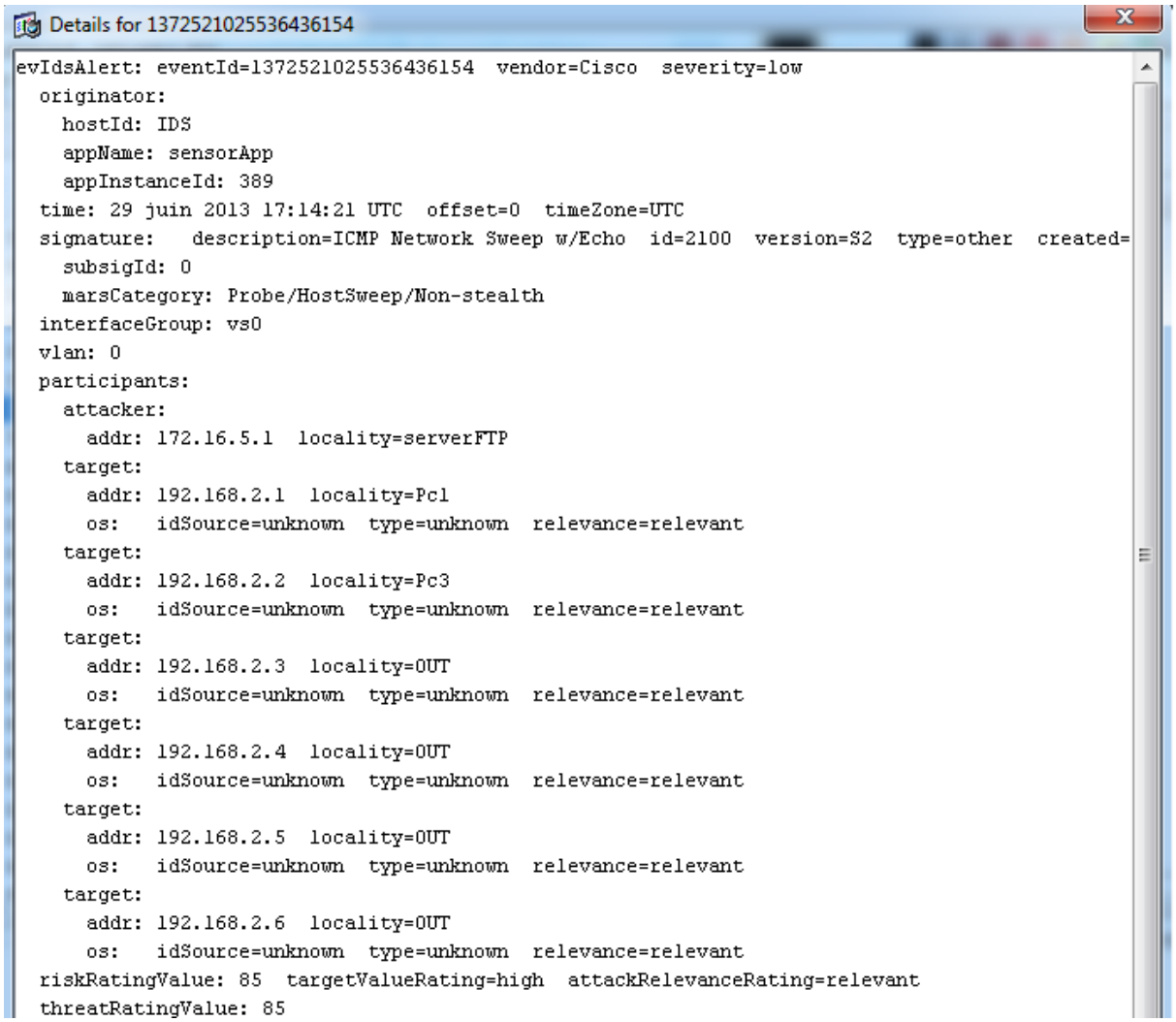


FIG. V.51 – L'affichage d'alerte par l'IDS

c. Le Scan de port Cette technique permet la collection d'informations soit sur un ensemble de machines d'un réseau précis ou bien d'un hôte.

1. La collection d'informations sur le réseau 192.168.2.0/24.

Fig. V.52 – Le Scan de port d'un réseau

Dans cette figure illustre l'alerte déclencher par l'IDS.

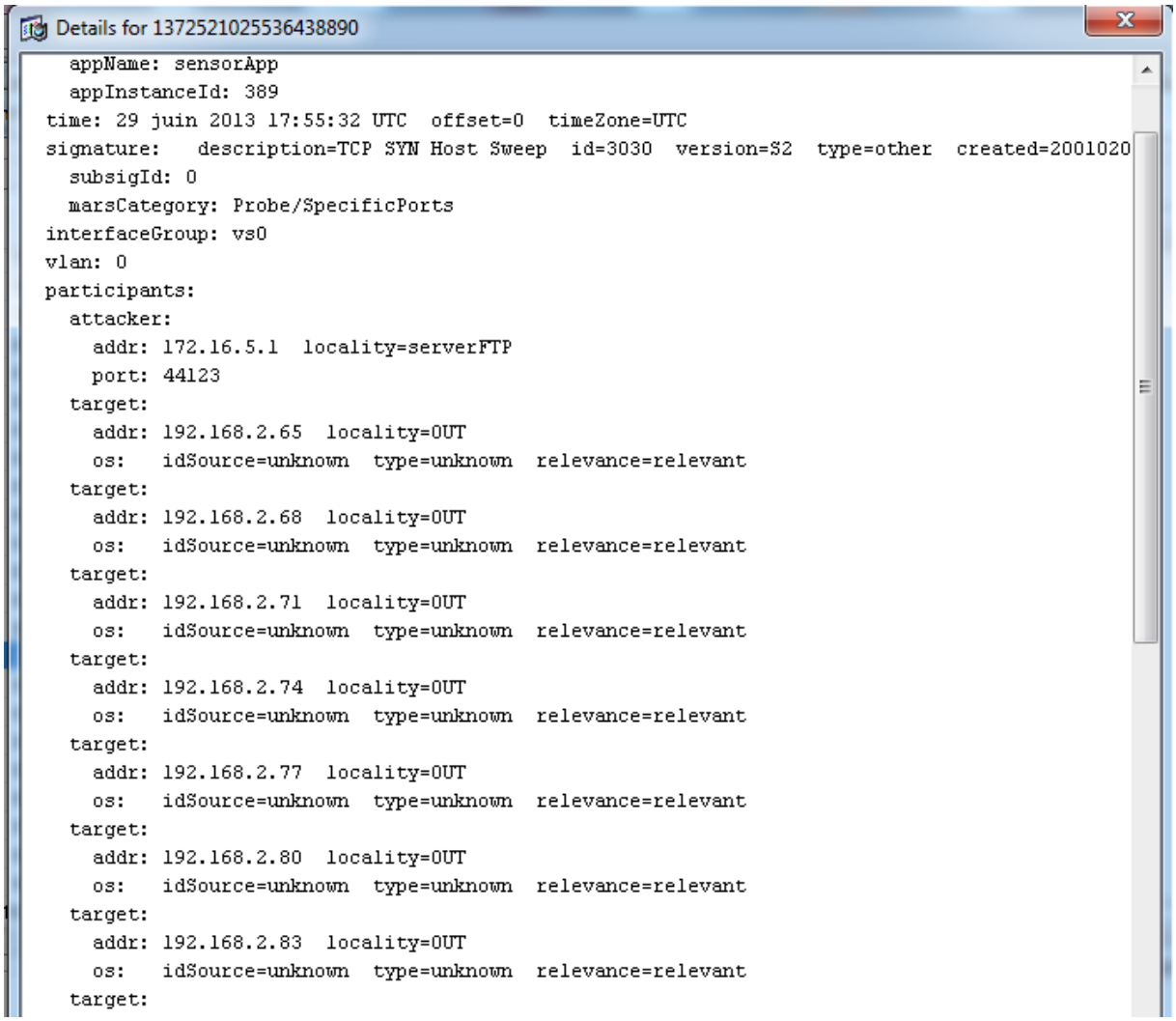


Fig. V.53 – Alerte déclencher par l'IDS.

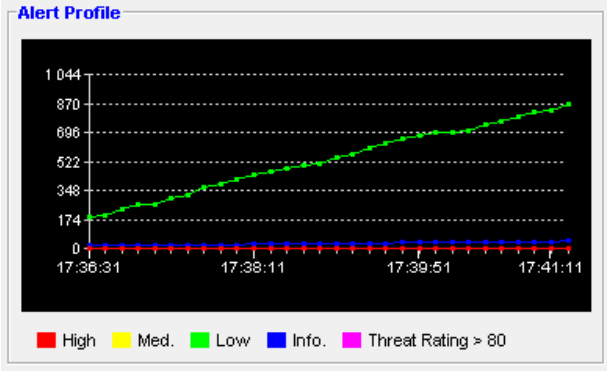


FIG. V.54 – L'affichage de l'alerte par l'IDS

2. La collection d'informations sur le serveur FTP.

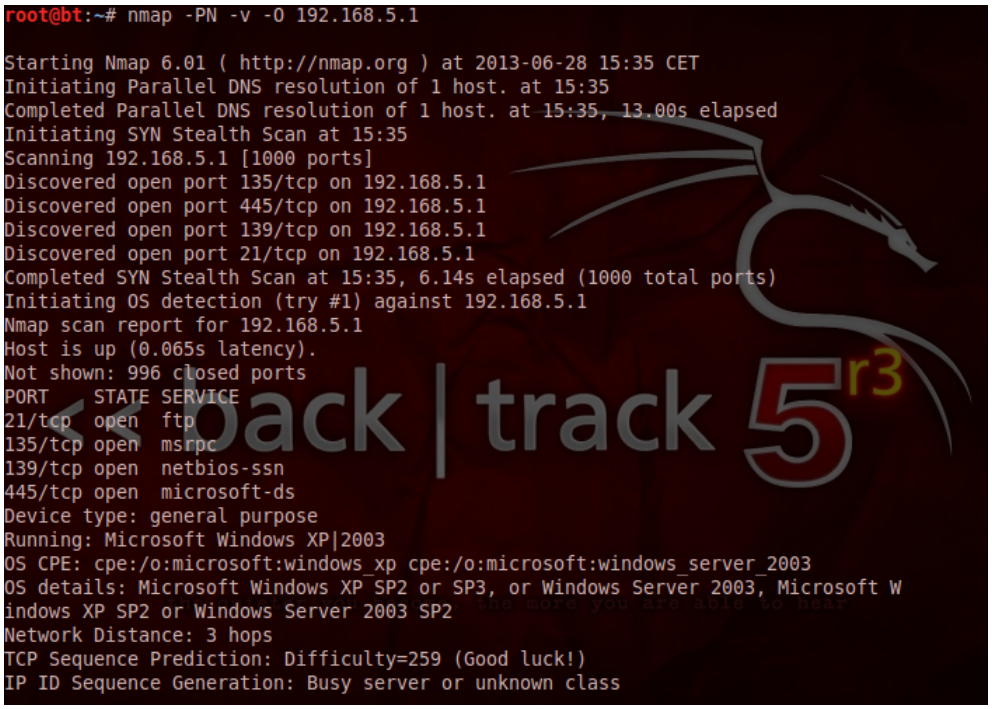


FIG. V.55 – Le Scan de port du serveur FTP

Dans cette figure illustre l'alerte déclencher par l'IDS.

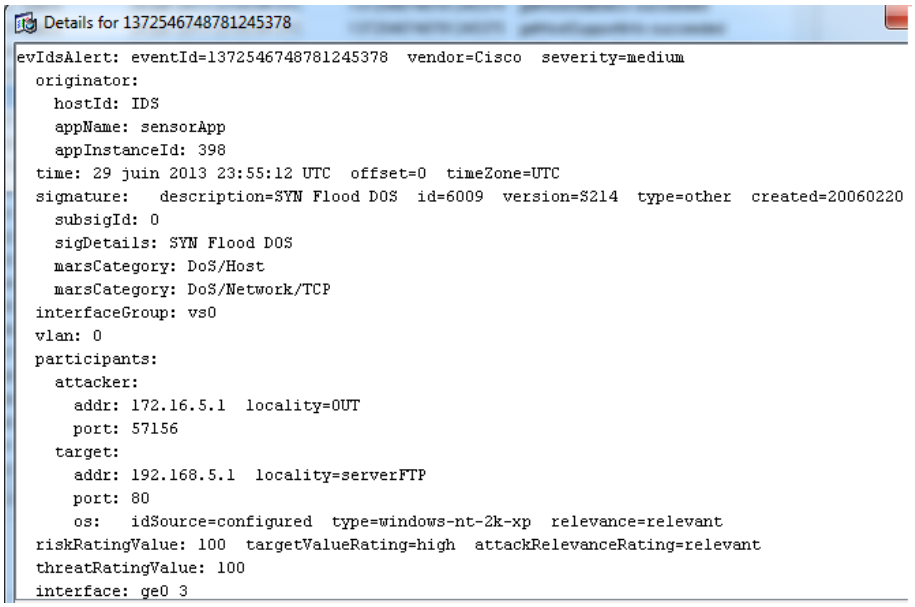


FIG. V.56 – Alerte déclencher par l'IDS

d. L'attaque DOS Dans ce cas le Pirate vise le serveur. Ce dernier va ce déconnecté et si un utilisateur essaye d'accéder, le serveur ne répond pas.

le pirate tape cette commande siege -b 192.168.5.1

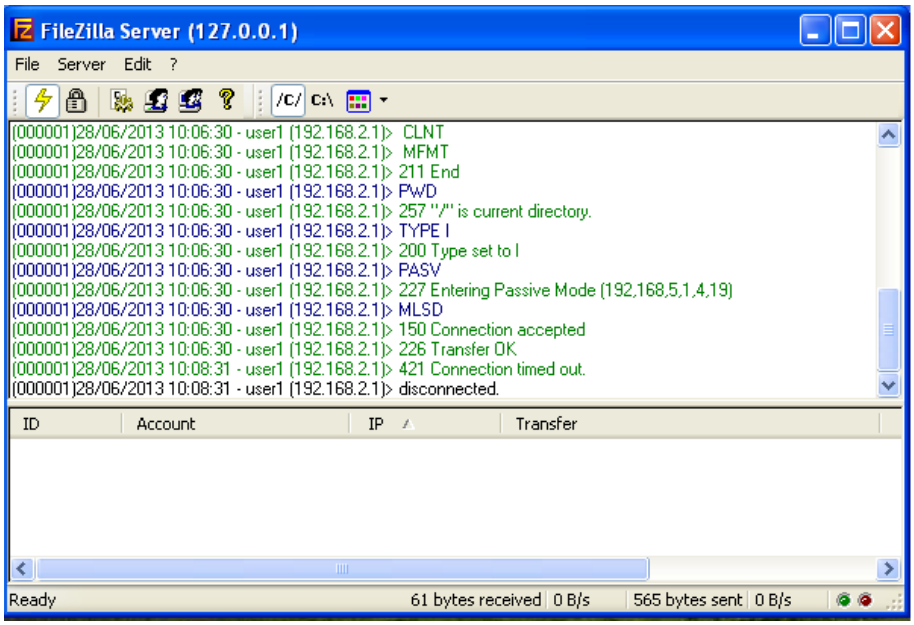


FIG. V.57 – La déconnection du serveur

Quand un utilisateur essaye d'accéder au serveur, ce dernier ne répond pas.

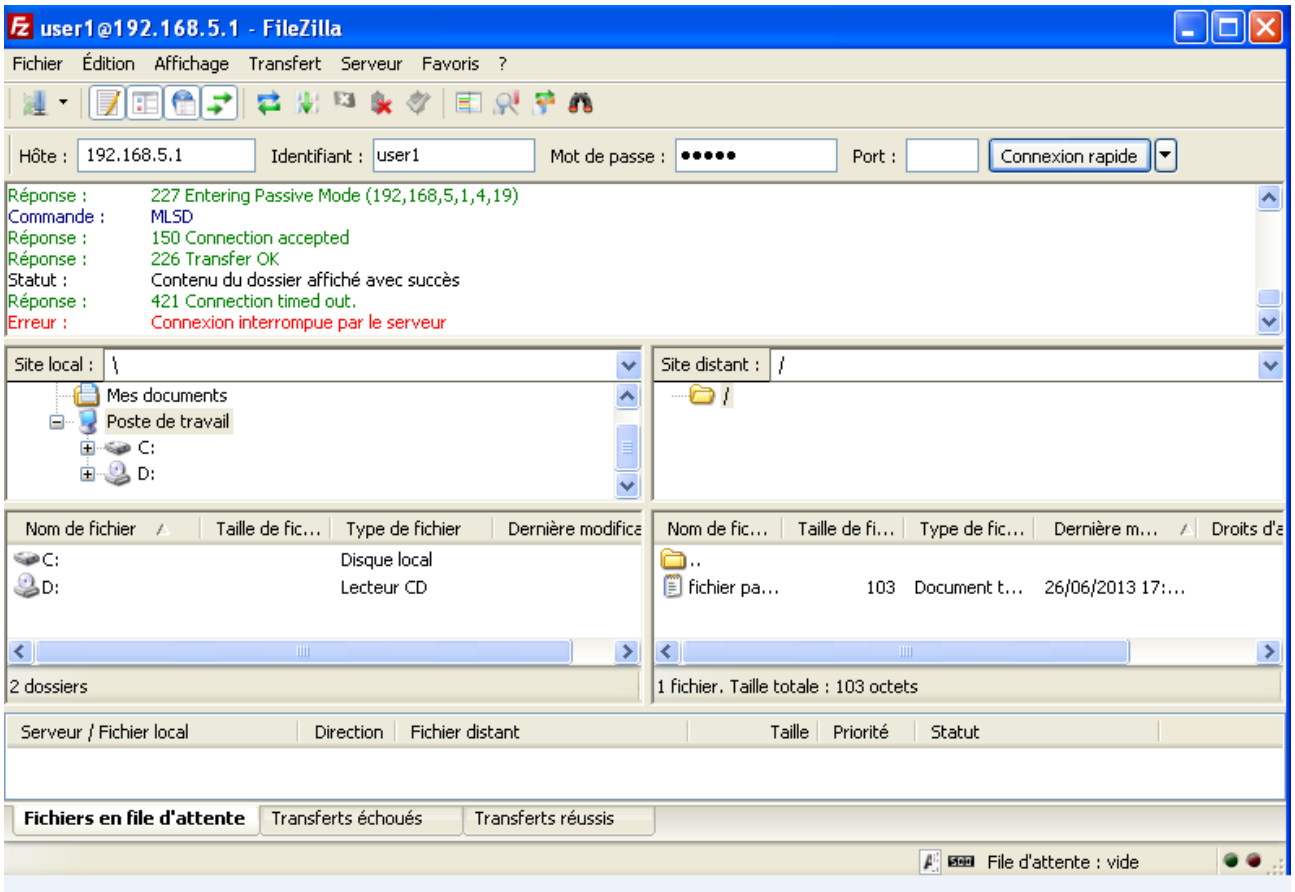


Fig. V.58 – L'indisponibilité du serveur

Cette figure montre la détection d'attaque par l'IDS

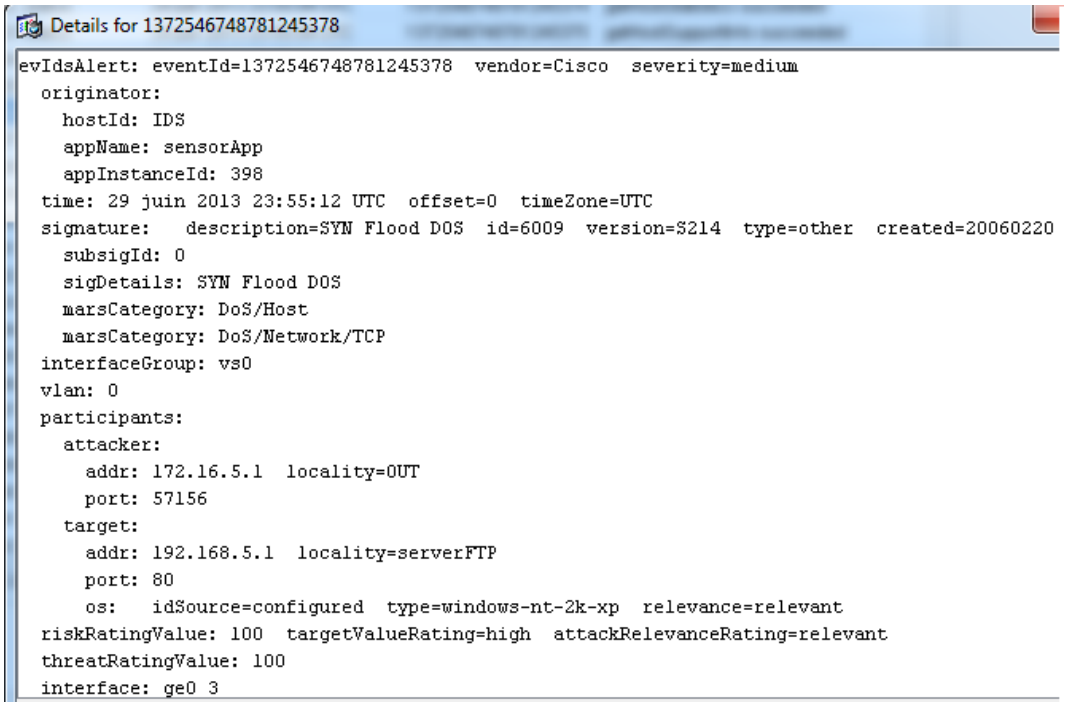


FIG. V.59 – L'affichage de l'alerte Dos

Conclusion

Dans ce chapitre nous avons opté à la mise en œuvre de notre solution dont nous avons présenté l'environnement et les outils de travail.

Le simulateur GNS3 nous a permis à partir de son interface graphique de concevoir et simuler notre topologie comprenant les périphériques suivants : les commutateurs, les routeurs et les stations de travail ainsi que leurs configurations qui nous a permis de bien concrétiser notre solution. Après la configuration nous avons exposé quelques tests afin de vérifier la fiabilité de l'IDS.

Conclusion Générale

Conclusion Générale

Devant la complexité croissante des menaces réseaux, il devient indispensable de mettre en place des solutions efficaces de protection du réseau contre les intrusions afin de garantir un niveau élevé de sécurité. Une protection vigilante contribue à garantir la continuité de l'activité de l'entreprise et minimise les conséquences onéreuses des intrusions.

Les outils de détection d'intrusions permettent de pallier aux insuffisances des mécanismes de sécurité. Ils détectent les actions malveillantes visant à remettre en cause l'intégrité, la disponibilité et/ou la confidentialité des ressources d'un système d'informations.

Pour une sécurité optimale, ces outils doivent être couplés à d'autres, comme l'indispensable pare-feu. Mais ils doivent aussi être mis à jour, aussi bien au niveau du cœur du logiciel comme la base de signatures, qui constitue la base d'une détection efficace. Il faut également coupler les systèmes de détection entre eux en prenant en compte la notion de complémentarité des solutions offertes pour assurer cette fonctionnalité : c'est-à-dire, ne pas hésiter à placer des NIDS, HIDS dans le même réseau. Leurs rôles sont différents, mais chacun apporte ses fonctionnalités.

Dans notre mémoire nous avons opté à la simulation et la mise en place d'un système de détection d'intrusions au niveau de l'architecture réseau de Cevital. Tout d'abords nous avons proposé une implémentation de cette architecture en s'appuyant sur le simulateur de réseau graphique GNS3 puis configurerles différents matériels nécessaires à 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 trafic sortant et/ou entrant à l'intérieur et/ou à l'extérieur du réseau local et en fin, présenté 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.

Même si une certaine maturité dans le domaine de la sécurité informatique commence à se sentir, le plus important reste de savoir de quoi il faut se protéger. Les failles les plus répandues proviennent généralement de l'intérieur de l'entreprise, et non de l'extérieur. Des mots de passe simples, des droits d'accès trop élevés, des services mal configurés, ou encore des failles dans les logiciels restent la bête noire en matière de sécurité.

Perspectives

Les résultat obtenus nous paraissent prometteurs et nous laissent envisager un certain nombre de perspectives.

- Améliorer les performances d'un système de détection d'intrusions à travers l'exploitation des fichiers logs générés par ce dernier en alertant l'administrateur réseau à chaque tentative d'intrusion de haut niveau par un mail ou un SMS.
- Réduire le taux de faux positif en améliorant la qualité des tests. Plus ces taux sont bas, plus la solution est performante.
- Améliorer les méthodes et les mécanismes permettant de détecter les scénarios d'attaques complexes.
- Coopérer les différents systèmes de détection d'intrusions pour une sécurité parfaite et complète.

Bibliographie

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

[**2**] Cédric Llorens, Denis Valois et Laurent Levier, Tableau de bord de la sécurité réseau,groupe Eyrolles, 2éme édition , 2006.

[**3**] Laboratoire MAFTIA Project Delivrable, Malicious and Accidental Fault Tolerance in Internet Applications : Towards Taxonomy of Intrusion Detection Systems and Attacks, article de recherche. Septembre 2001.

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

[**5**] Stéphane Lohier, Aurélie Quidelleur, Le réseau Internet, des services aux infrastructures,Edition Dunod, Paris, 2010.

[**6**] AUBEUF- HACQUIN Yoann, Mise en place d'un système de détection d'intrusion sur le réseau de l'entreprise, Rapport de stage, Université François-Rabelais Tours, juin 2009.

[**7**] Ludovic Mé, Véronique Alanou,Détection d'intrusion dans un système informatique : méthodes et outils, Article de recherche, Mars 2008.

[**8**] Philippe Biondi, Architecture expérimentale pour la détection d'intrusions dans un système informatique, Article de recherche, Avril-Septembre 2001.

[**9**] 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.

[**10**] Mme LABED Ines, Proposition d'un système immunitaire artificiel pour la détection d'intrusion, En vue de l'obtention du diplôme de magister en informatique option : information et computation, Université de MENTOURI de Constantine faculté des sciences de l'ingénieur, 2005-2006.

[**11**] Jean François CARPENTIER, La sécurité informatique dans la petite entreprise, Etat de l'art et bonnes pratiques, Edition ENI, Avril 2009.

[**12**] Guy Pujjolle, Les réseaux, groupe Eyrolles, 5éme édition, septembre 2006.

[13] 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.

[14] David ROUMANE, Nomadisme et sécurité sur les réseaux informatiques, Mémoire d'ingénieur de Centre National des Arts et Métiers de Rhône-Alpes, centre d'enseignement de GRENOBLE, décembre 2005.

[15] Xavier Carcelle, Livre Réseaux CPL par la pratique, édition EYROLLE,2006.

[16] GUY PUJOLL, Les Réseaux, EYROLLES, 5éme édition, Août 2006.

[17] GUY PUJOLL, Les Réseaux, EYROLLES, 6éme édition, 2008.

[18] Mr RIAHLA Doctorant à l'université de limoge (France), Introduction à la sécurité informatique, Conférence au Département de physique/Infotronique IT/S6 de l'université De Boumerdes, 2008-2009.

[19] 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.

[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, 2010/20111.

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

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

[23] G. Hiet, L. Mé, J. Zimmermann, C. Bidan, B. Morin et V. Viet Triem Tong, Détection fiable et pertinente de flux d'informations illégaux, Article, Avenue de la Boulaie, Cesson Sévigné Cedex, France.

[24] Hervé Debar, Benjamin Morin, Frédéric Cuppens, Fabien Autrel et Ludovic Mé, Détection d'intrusions : corrélation d'alertes. Article de synthèse, Caen, France, 2004.

[25] 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.

[26] Jean-Marc ROYER, Sécuriser l'informatique de l'entreprise, Enjeux, menaces, prévention et parades, Edition ENI.

[27] Groupe BVRP Software, RealSecure Desktop Protector, Article issue d'Internet security Systems, Distribué par AB soft France, avril 2003.

[28] Nathalie Dagorn, Détection et prévention d'intrusion : présentation et limites, Rapport de recherche, université de Nancy1, 2009.

[29] Klaus Müller alias, IDS - Systèmes de Détection d'Intrusion Partie I, Linux-Focus article numéro 292, janvier 2005.

[30] NOUCHTI Ouafa, El QASMI Med Zakaria et HILALI Tarik, Virtual Private Network Etude comparative et réalisation d´unVPN MPLS, Mini Projet, école marocaine des sciences de l'ingénieur (EMSI), 2009/2010.

[31] Christophe Fillot et Jean-Marc Berenguier, Dynamips : Un émulateur de routeur Cisco sur PC, Fiche technique, Université de Technologie de Compiègne, Service Informatique.

[32] 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.

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

[34] ROMDHANE BEN YOUNES, Etude et mise en œuvre d'une méthode de détection d'intrusions dans les réseaux sans-fil 802.11 basé sur la vérification formelle de modèle, mémoire, université du Québec à Montréal, Décembre 2007.

[35] Antonio Merola, Les systèmes de détection d'intrusion vus de l'intérieur.Article publié dans le numéro 4/2005 du magazine hakin9, Software - Wydawnictwo, Pologne, 2005.

[36] Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, Eugene Spafford, Diego Zamboni, traduit de l'anglais par Erwan Doceux, Architecture de détection d'intrusion par agents autonomes, Rapport technique, Ecole Supérieure d'Electronique de l'Ouest France, juillet 2000.

[37] Clément LORVAO, Dado KONATE, Guillaume LEHMANN, Prelude-IDS, Rapport de ter, Avril 2004.

[38] Pascal Nicolas, Cours de réseaux, Université d'Angers, Ma rs 2008.

[39] Guy Pujolle, cours réseaux et télécoms, 3éme édition EYROLLES, 2008.

Webliographie

W1 www.techno-science.net/ ?onglet=glossaire& definition=10841.

W2 www.iso.org/iso/fr/home/store/catalogue_ics/catalogue_detail_ics.htmcsnumber=56891.

W3 http ://www.vulgarisation-informatique.com/attaques-informatiques.php.

W4 www.developpez.com (site des professionnelles en informatique).

W5 http ://www.gendarmerie.interieur.gouv.fr/eng/Sites/Gendarmerie/A-la-loupe/Le-phishing.

W6 http ://www.ingenieurs2000.com université Paris-EST Marne-la-vallée par l'enseignant Etienne Duris, NT réseau IDS et IPS 2003/2004.

W7 http ://www.securiteinfo.com/conseils/choix_ids.shtml.

W8 http ://processnet-info.fr/software/gns3-ou-comment-emuler-son-reseau.

W9 http ://eip.epitech.eu/2013/gns3/fr/project.html.

W10 www.gns3.net.

W11 http ://cisco.goffinet.org/s2/ios_naming_convention.

W12 http ://dynagen.org/tutorial.htm.

W13 http ://en.wikibooks.org/wiki/QEMU.

W14 http ://www.forum-intrusion.com/trucs/affichastuce.phpid=17.

W15 http :// IDS T/IPS.html

W16 http ://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml.

W17 http ://wiki.qemu.org/Main/_Page.

W18 http ://www.frameip.com/entete-tcp/.

W19 http ://www.guill.net/index.phpcat=3&pro=1&tcpip=19.

W20 http ://www.noplay.net/GNS3.html.

W21 http ://www.gatoux.com/SECTION2/p12.php.

Annex A

Le modèle TCP/IP

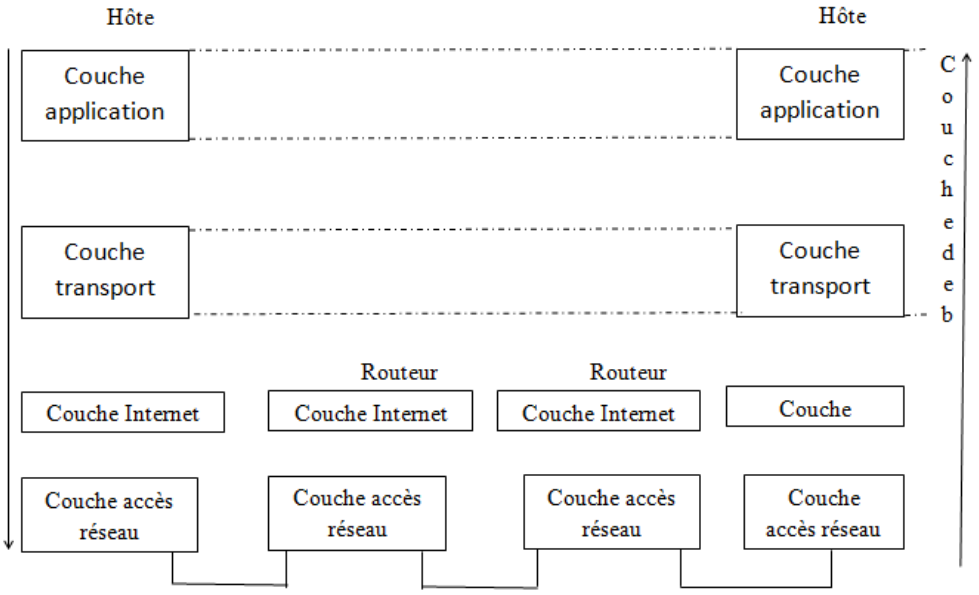
Dans les années 1970, le département de la Défense américain, ou DOD (Department Of Defense), décide, devant le foisonnement de machines utilisant des protocoles de communication différents et incompatibles, de définir sa propre architecture. Cette architecture, dite TCP/IP, est à la source du réseau Internet. Elle est aussi adoptée par de nombreux réseaux privés, appelés Intranet.

Les deux principaux protocoles définis dans cette architecture sont les suivants :

- IP (Internet Protocol), de niveau réseau, qui assure un service sans connexion.
- TCP (Transmission Control Protocol), de niveau transport, qui fournit un service fiable avec connexion.

Le modèle doit son nom à ses deux derniers [**17**].

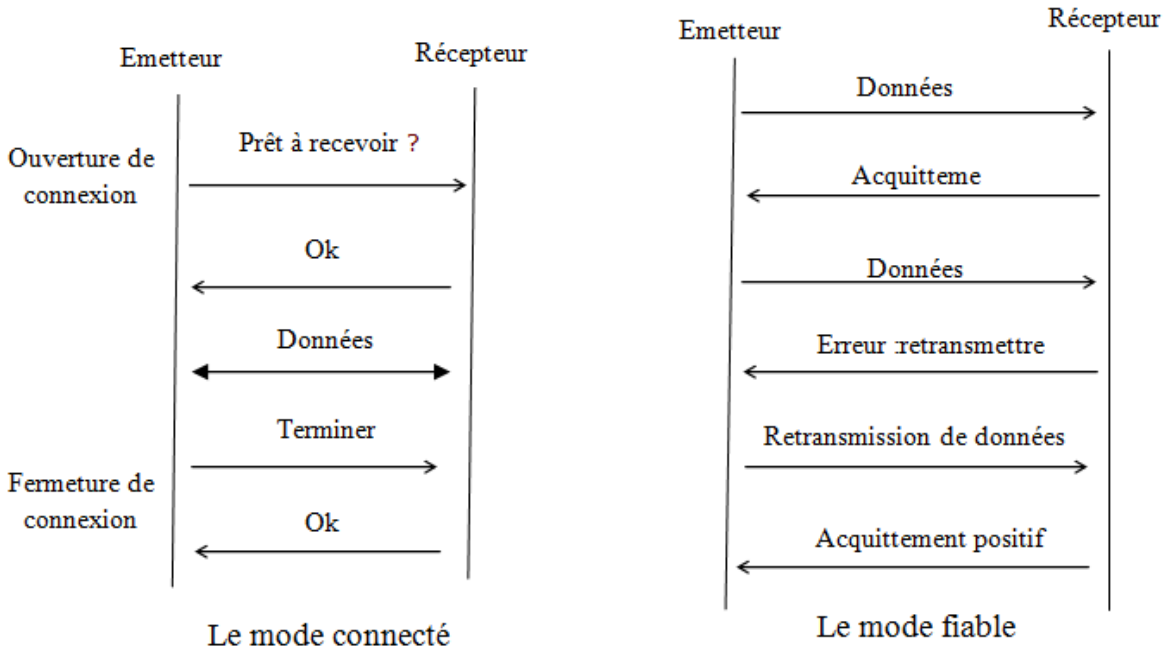
Le modèle TCP/IP est constitué de quatre couches (figure 1) [**5**].



La couche Internet contient un protocole essentiel, IP, qui a en charge l'adressage des machines et le routage des paquets. Ce protocole fonctionne en mode non connecté et non fiable.

La couche transport contient deux protocoles essentiels : TCP et UDP. Le protocole TCP fonctionne en mode connecté fiable, il assure donc la retransmission de paquets en cas de pertes, le séquencement des paquets, le contrôle de flux et le contrôle de congestion.

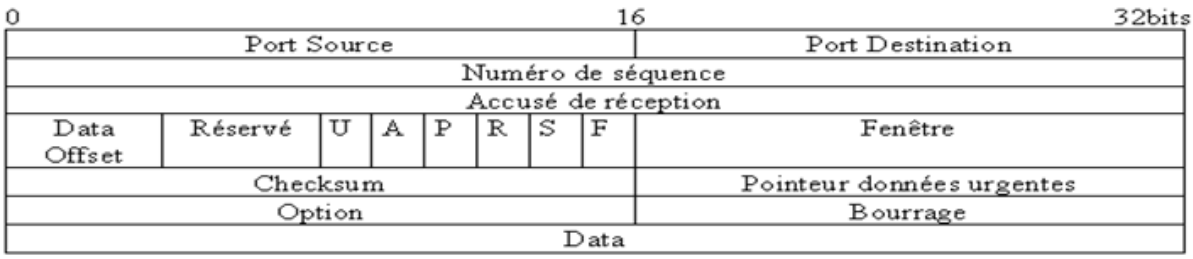
Le protocole UDP quant à lui ne réalise aucune de ces fonctions et travaille en mode datagramme et non fiable [**5**].



Le protocole TCP

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.

En-tête TCP



A) Indication de chaque champ du datagramme W19 :

- **Port Source (16 bits) :** numéro du port source.
- **Port Destination (16 bits) :** numéro du port destination.
- **Numéro de séquence (32 bits) :** Le numéro du premier octet de données par rapport au début de la transmission (sauf si SYN est marqué).

  1. Si SYN = 0, le numéro de séquence est celui du premier octet de données de ce segment.
  2. Si SYN = 1, il s'agit du numéro de séquence initiale ISN. Le premier octet de donnée est à ISN+1.

- **Accusé de réception (32 bits) :** si le bit ACK = 1, ce champ contient le numéro de séquence attendu par l'´émetteur du segment.
- **Data Offset (4 bits) :** La taille de l'en-tête TCP en nombre de mots de 32 bits. Il indique là ou commence les données.
- **Réservé (6 bits) :** champ réservé pour une utilisation ultérieure. Les 6 bits doivent être à 0.
- **Bits de contrôle (6 bits) :**

  1. **URG :** pointeur de données urgentes significatif.
  2. **ACK :** ausé de réception significatif.
  3. **PSH :** fction push.
  4. **RST :** réinitialisation de la connexion.
  5. **SYN :** synchronisation des numéros de séquence.
  6. **FIN :** fin de transmission.

- **Fenêtre (16 bit) :** le nombre d'octets à partir de la position marquée dans l'accusé de réception que le récepteur est capable de recevoir.
- **Checksum (16 bits) :** somme de contrôle sur 16 bits de l'en-tête et des données.
- **Pointeur de données urgentes (16 bits) :** ce champ est interprété uniquement si le bit de contrôle URG est à 1. Le pointeur donne le numéro de séquence de l'octet qui suit les données " urgentes ".

- **Options (variable) :** les champs d'option peuvent occuper un espace de taille variable à la fin de l'en-tête TCP. Ils formeront toujours un multiple de 8 bits. Toutes les options sont prises en compte par le Checksum. Un paramètre d'option commence toujours sur un nouvel octet. Il est défini deux formats types pour les options :
  - **Cas 1 :** Option mono-octet.
  - **Cas 2 :** Octet de type d'option, octet de longueur d'option, octets de valeurs d'option.
- **Bourrage (padding) :** (variable)Les octets de bourrage terminent l'en-tête TCP : de sorte que le nombre d'octet de celle-ci soit toujours multiple de 4 (32 bits) de sorte que l'offset de données marqué dans l'en-tête corresponde bien au début des données applicatives .

B) Mode de transfert : Voici les différents types de communication basés sur le mode connecté de TCP **W18** :

. Ouverture de session

$$\Rightarrow \mathsf{SYN} = 1 - \mathsf{ACK} = 0 - \mathsf{SeqNum} = 100 - \mathsf{AckNum} = \mathsf{xxx}$$

$$\Leftarrow \mathsf{SYN} = 1 - \mathsf{ACK} = 1 - \mathsf{SeqNum} = 300 - \mathsf{AckNum} = 101$$

$$\Rightarrow \mathsf{SYN} = 0 - \mathsf{ACK} = 1 - \mathsf{SeqNum} = 101 - \mathsf{AckNum} = 301$$

. Transfert des données

$$\Rightarrow \mathsf{ACK} = 1 - \mathsf{SeqNum} = 101 - \mathsf{AckNum} = 301 - \mathsf{Data} = 30\mathsf{octets}$$

$$\Leftarrow \mathsf{ACK} = 1 - \mathsf{SeqNum} = 301 - \mathsf{AckNum} = 131 - \mathsf{Data} = 10\mathsf{octets}$$

$$\Rightarrow \mathsf{ACK} = 1 - \mathsf{SeqNum} = 131 - \mathsf{AckNum} = 311 - \mathsf{Data} = 5\mathsf{octets}$$

$$\Leftarrow \mathsf{ACK} = 1 - \mathsf{SeqNum} = 311 - \mathsf{AckNum} = 136 - \mathsf{Data} = 10\mathsf{octets}$$

. Fermeture de session

$$\Leftarrow \mathsf{ACK} = 1 - \mathsf{FIN} = 1 - \mathsf{SeqNum} = 321 - \mathsf{AckNum} = 136$$

$$\Rightarrow \mathsf{ACK} = 1 - \mathsf{FIN} = 0 - \mathsf{SeqNum} = 136 - \mathsf{AckNum} = 321$$

. **Fermeture brutale de connexion**

premier cas possible :

$$\Rightarrow \mathsf{ACK} = 1 - \mathsf{RST} = 0 - \mathsf{SeqNum} = 200 - \mathsf{AckNum} = 400$$

$$\Leftarrow \mathsf{ACK} = 0 - \mathsf{RST} = 1 - \mathsf{SeqNum} = 400 - \mathsf{ACKNum} = xxx$$

second cas possible :

$$\Leftarrow \mathsf{ACK} = 0 - \mathsf{RST} = 0 - \mathsf{SeqNum} = 200 - \mathsf{Data} = 30\mathsf{octets}$$

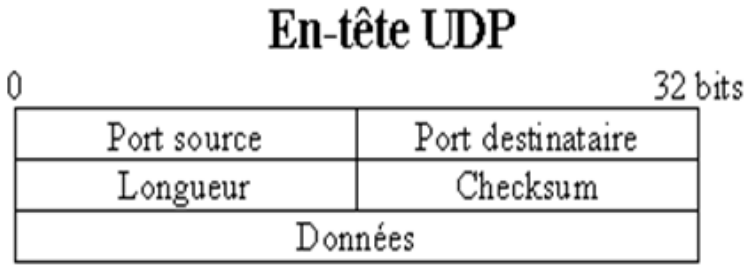
$$\Rightarrow \mathsf{ACK} = 0 - \mathsf{RST} = 1 - \mathsf{SeqNum} = 230 - \mathsf{Data} = xxx$$

.

Le protocole UDP

Le protocole UDP est un protocole non orienté connexion et non fiable. Bien qu'il soit chargé de la transmission des messages, il n'exécute aucune vérification logicielle sur l'acheminement des segments. L'avantage de ce protocole est sa vitesse. Comme il ne fournit pas d'accusés de réception, le trafic sur le réseau est plus faible, ce qui accéléré les transferts [**39**].

Ce protocole définit une procédure permettant à une application d'envoyer un message court à une autre application, selon un mécanisme minimaliste. Ce protocole est transactionnel, et ne garantit ni la délivrance du message, ni son éventuelle duplication. Les applications nécessitant une transmission fiabilisée et ordonnée d'un flux de données implémenteront de préférence le protocole TCP **W19**.



. Indication de chaque champ du datagramme :

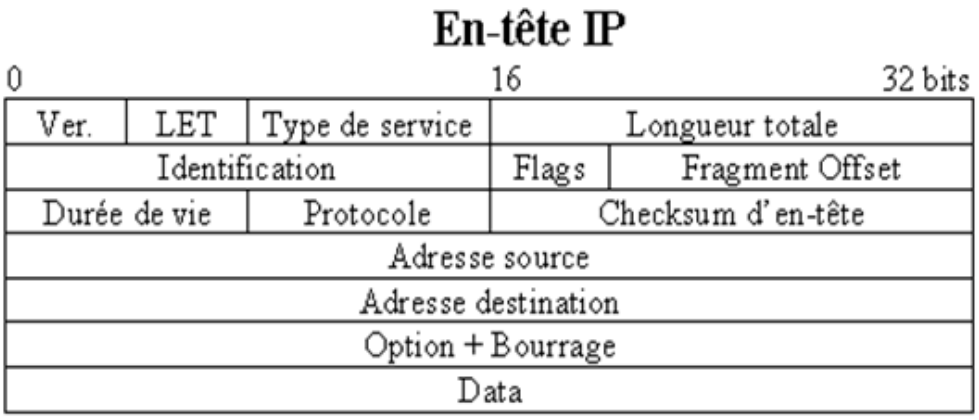
- **Port Source (16 bits) :** numéro du port source. Ce champ est optionnel.
- **Port Destination (16 bits) :** numéro du port destination.
- **Langueur (16 bits) :** longueur en octets du datagramme UDP incluant l'en-tête et les données.
- **Checksum (16 bits) :** somme de contrôle sur 16 bits de l'en-tête et des données [39].

Ce protocole sera utilisé principalement pour les communications avec les serveurs de noms de domaines, et dans les transactions utilisant le protocole Trivial File Transfer.

Ce protocole porte le numéro 17 (21 en octal) lorsqu'il est transporté par le Protocole Internet. D'autres numéros de protocoles pour d'autres couches support sont données dans la référence **W19**.

Le protocole IP

La fonction ou rôle du Protocole Internet est d'acheminer les datagrammes à travers un ensemble de réseaux interconnectés. Ceci est réalisé en transférant les datagrammes d'un module Internet à l'autre jusqu'à atteindre la destination. Les modules Internet sont des programmes exécutés dans des hôtes et des routeurs du réseau Internet. Les datagrammes sont transférés d'un module Internet à l'autre sur un segment particulier de réseau selon l'interprétation d'une adresse Internet. De ce fait, un des plus importants mécanismes du protocole Internet est la gestion de cette adresse Internet **W19**.



Expliquons un peu mieux à quoi servent ces octets :

. **Version(4 bits) :** Le champ Version renseigne sur le format de l'en-tête Internet.

. **Longueur d'En-Tête(4 bits) :** Le champ Longueur d'En-Tête (LET) code la longueur de l'en-tête Internet, l'unité étant les mots de 32 bits, et de ce fait, marque le début des données. Notez que ce champ ne peut prendre une valeur en dessous de 5 pour être valide.

. **Type de Service(8 bits) :** donne une indication sur la qualité de service souhaitée, qui reste cependant un paramètre "abstrait". Le "Type de Service" sert à préciser le traitement effectué sur le datagramme pendant sa transmission à travers Internet.

. **" Langueur totale (16 bits) :** Le champ "Longueur Totale" est la longueur du datagramme entier y compris en-tête et données, mesurée en octets. Ce champ ne permet de coder qu'une longueur de datagramme d'au plus 65,535 octets. Une telle longueur rendrait de toute façon les datagrammes impossible à gérer pour la plus grande partie des réseaux. Les hôtes devront au moins pouvoir accepter des datagrammes d'une longueur jusqu'à 576 octets (qu'il s'agisse d'un datagramme unique ou d'un fragment). Il est de même recommandé que des hôtes ne décident d'envoyer des datagrammes de plus de 576 octets que dans la mesure où ils sont sûrs que la destination est capable de les accepter **W19**.

. **le champ Identification (16 bits) :** c'est un numéro d'identification inscrit par l'émetteur du paquet. Tous paquets émis par une même machine à l'attention d'un même destinataire porte un numéro d'identification différent. En cas de fragmentation, ce numéro d'identification est recopié dans tous les fragments du paquet

d'origine. Ceci permettra au destinataire de repérer tous les fragments d'un même paquet et de reconstituer le paquet d'origine.

. **le champ Flag (3 bits) :** il permet de gérer la fragmentation **W21**.
  - **bit 0 :** réservé, toujours positionné à 0
  - **bit 1 :** dit bit DF (Don't Fragment) s'il est positionné à 0, la fragmentation est autorisée, s'il est positionné à 1 la fragmentation est interdite. Dans ce dernier cas, si le paquet est trop volumineux pour être encapsulé dans une trame, dont le MTU (Maximum Transmission Unit) est inférieur à la taille du paquet, la passerelle qui devrait réaliser la fragmentation retournera à l'émetteur du paquet un ICMP "Paquet non fragmentable".
  - **bit 2 :** dit bit MF (More Fragment). S'il est positionné à 0 il indique que le paquet reçu est le dernier du paquet d'origine. S'il est positionné à 1, il indique que le paquet reçu est un fragment du paquet d'origine mais pas le dernier fragment. Un paquet qui n'a pas été fragmenté aura donc toujours ce bit à 0.

. **le champ Fragment Offset :** indique la position du premier octet de données du paquet reçu dans la partie donnée du paquet d'origine. Le premier fragment à donc toujours la valeur 0 (position du premier octet), de même que tous paquets non fragmentés.

La fragmentation

La fragmentation du datagramme Internet devient nécessaire dès lors qu'un datagramme de grande taille arrive sur une portion de réseau qui n'accepte la transmission que de paquets plus courts.

Un datagramme Internet peut être spécifié "non fractionnable" Un tel datagramme Internet ne doit jamais être fragmenté quelques soient les circonstances. Si un datagramme Internet non fractionnable ne peut être acheminé jusqu'à sa destination sans être fragmenté, alors il devra être rejeté.

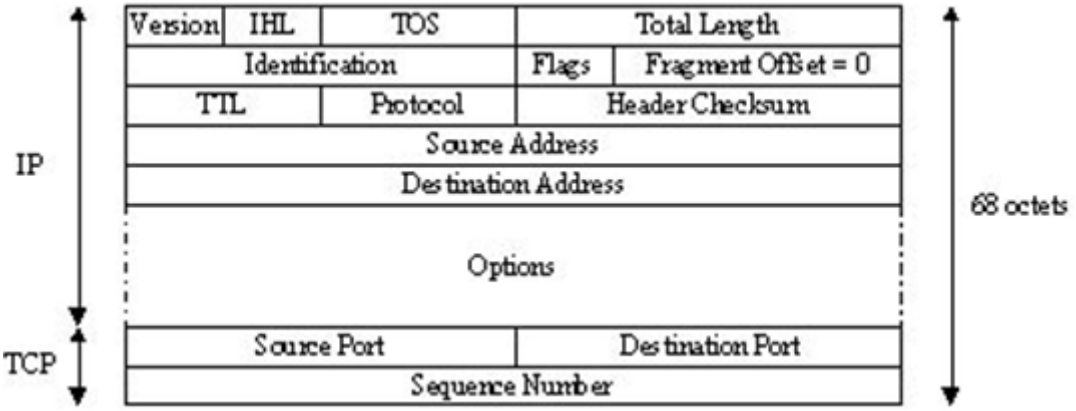
Les procédures de fragmentation et réassemblage Internet doivent pouvoir "casser" un datagramme Internet en un nombre de "fragments" arbitraire et quelconque pourvu que

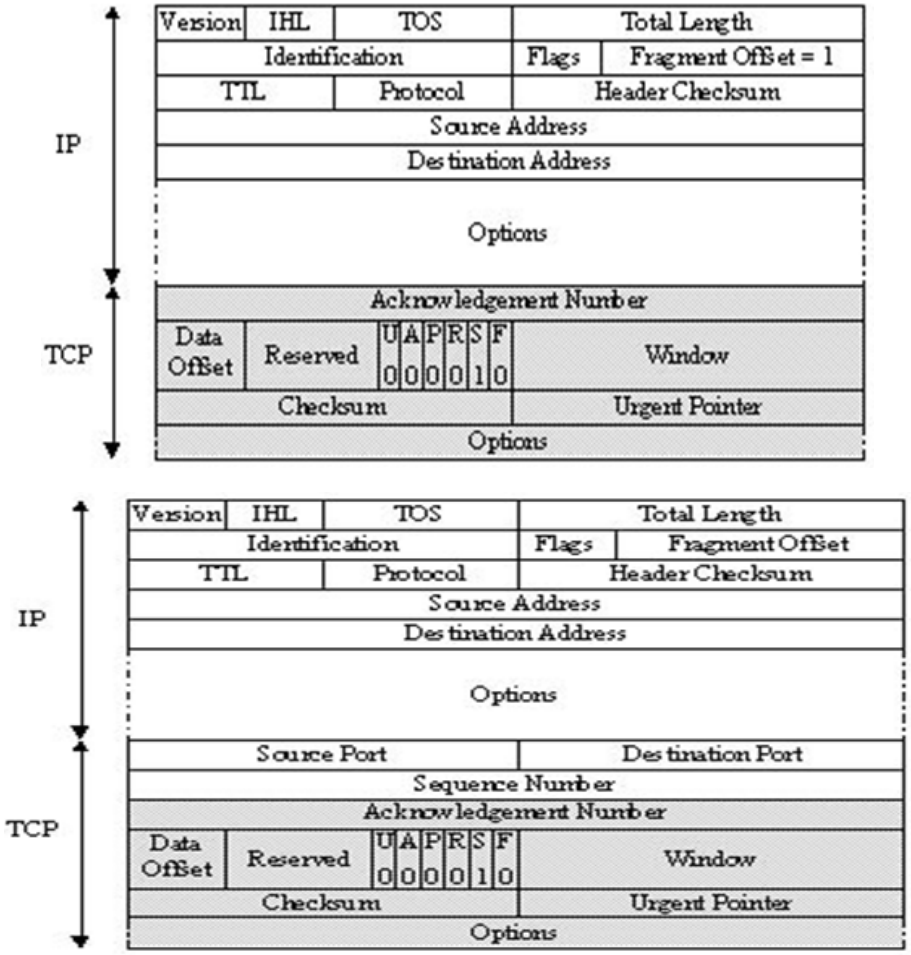
le réassemblage soit possible. Le récepteur des fragments utilise le champ d'identification pour s'assurer que des fragments de plusieurs datagrammes ne puissent être mélangés. Le champ "Fragment Offset" indique au récepteur la position du fragment reçu dans le datagramme original. Les champs "Fragment Offset" et "Longueur Totale" déterminent la portion du datagramme original que représente le fragment. L'indicateur bit "Dernier Fragment" indique (lors de sa remise à zéro) au récepteur qu'il s'agit du dernier fragment. Ces champs véhiculent suffisamment d'information pour réassembler les datagrammes.

Le champ d'identification sert à distinguer les fragments d'un datagramme de ceux d'un autre datagramme. Le module Internet émetteur d'un datagramme Internet initialise le champ d'identification à une valeur qui doit être unique pour cette paire source-destination et pour ce protocole pendant toute la durée de transmission de ce datagramme. Le module Internet terminant l'émission d'un datagramme met le bit "Dernier Fragment" et le champ "Fragment Offset" à zéro.

Pour réassembler les fragments d'un datagramme Internet, un module Internet (par exemple dans un hôte destinataire) recombine les datagrammes dont les valeurs des quatre champs suivants sont identiques : identification, source, destination, et protocole. La recombinaison est réalisée en replaçant la portion de donnée contenue dans chaque fragment dans un tampon à la position relative indiquée par le champ "Fragment Offset" lu dans l'en-tête correspondant. Le premier fragment sera donc placé en début de tampon, et le dernier fragment récupéré aura le bit "Dernier Fragment" à zéro **W19**.

Attaque par Fragment

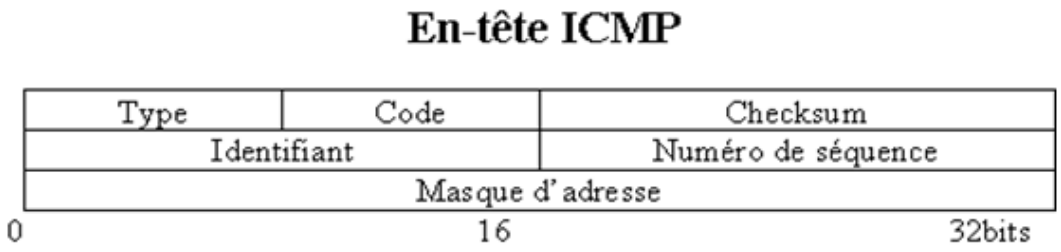




Fonctionnement du protocole ICMP

Le protocole ICMP (Internet Control Message) assiste le protocole IP dans la gestion du trafic. Il est implémenté dans les hôtes et les routeurs. Il définit deux types de messages, concernant les erreurs ou des demandes d'information.

Le protocole ICMP est un protocole de la couche Internet à part entière, cependant le paquet ICMP est encapsulé dans un en-tête IP. Son format est présenté dans la figure suivante :



. **Le type(1 octet) :** indique la nature du message ICMP (destination inaccessible, demande d'écho, réponse à une demande d'écho, etc.), il est complété par le champ code(1 octet).
. **Somme de contrôle (2 octet) :** permet la détection d'erreur sur l'en-tête ICMP.
. **Paramètre (4 octet) :** contient des informations supplémentaires qui peuvent être nécessaires à certains types de messages comme un identifiant pour demande d'écho par exemple.

Les données transportent dans un message d'erreur la copie partielle du datagramme qui a généré l'anomalie, dans le message d'écho et sa réponse, leur contenu est quelconque.

Il existe deux types de message ICMP : les messages d'erreur et les messages de demande d'information [**5**].

. **Exemple de message d'information**

Type	Code	Signification
8	0	Echo request : le datagramme écho teste la connectivité d'un équipement. Sa taille est limité 576 octets. Il est utilisé notamment par la commande ping.
0	0	Echo reply : le datagramme de réponse à une demande d'écho contient les mêmes données que la requête.

Fonctionnement du protocole ARP

Le protocole ARP (AddressResolution Protocol)convertitl'adresse IP en une adresse physique. ARP permet aux machines de résoudreles adresses sans utiliser de table statique. Une machine utilise ARP pour déterminer l'adresse physique du destinataire. Elle diffuse pour cela sur le sous réseau une requête ARP qui contient l'adresse IP à traduire. La machine possédant l'adresse IP concernée répond en renvoyant son adresse physique. Pour rendre ARP plus performant, chaque machine tient à jour, en mémoire, une table des adresses résolues et réduit ainsi le nombre d'émissions en mode diffusion [**39**].

Fonctionnement du protocole DNS

Le DNS (Domain Name Service) permet la mise en correspondance des adresses physiques et des adresses logiques.

La structure logique prend une forme hiérarchique et utilise au plus haut niveau des domaines caractérisant principalement les pays, qui sont indiqués par deux lettres, comme frpour la France, et des domaines fonctionnels comme :

- com(organisations commerciales).
- edu(institutions académiques) [**39**].

Annex B

Les images IOS Cisco

Définition

Une image est un fichier archivé proposant la copie conforme d'un disque réécrit sous forme d'un code (qui peut être compressé). Pour créer ce fichier il existe plusieurs norme de codage, correspondant chacune à une extension particulière.

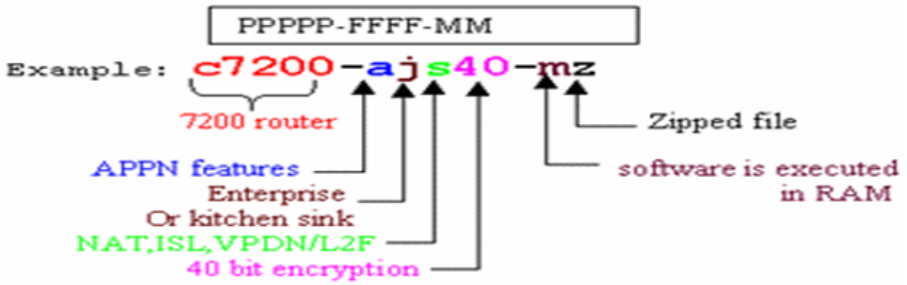
. **ISO :** le format le plus rependu, c'est la norme internationale ISO 9660.

. **IMG :** le format natif mac OS.

Tous les fichiers nécessaires à un système d'exploitation sont copiés dans un fichier image et refléter exactement le périphérique physique d'origine. Cette image peut servir directement avec l'ordinateur et un logiciel d'émulation et elle sert à faire ce qu'on appelle un disque virtuel émulé.

Convention de dénomination des images IOS Cisco

Cisco dispose d'une convention de dénomination des noms des images IOS logicielles. Un nom d'image comporte trois parties séparées par des tirets : [1] la plateforme matérielle, [2] les caractéristiques (features) et [3] l'endroit de chargement et le format de compression. Eventuellement, [4] on trouvera une extension de format de fichier précédée d'un point **W11**.



Annex C

L'installation de GNS3

Télécharger-le du site officiel www.gns3.net

La manière la plus facile d'installer GNS3 dans un environnement de Windows est d'employer le dossier supérieur : GNS3 v0.8.3.1 all-in-one.exe. Pour avoir tous les composants nécessaires pour le bon fonctionnement de GNS3. Cliquer le bouton de sauvegarde et puis choisir un endroit sur l'unité de disque dur pour sauvegarder le dossier.

Trouver le dossier téléchargé et double-clic là-dessus pour commencer à installer GNS3. Le magicien d'installation GNS3 commencera. Une fois le logiciel téléchargé et installé, lancez-le. Double-clic sur le raccourci GNS3.

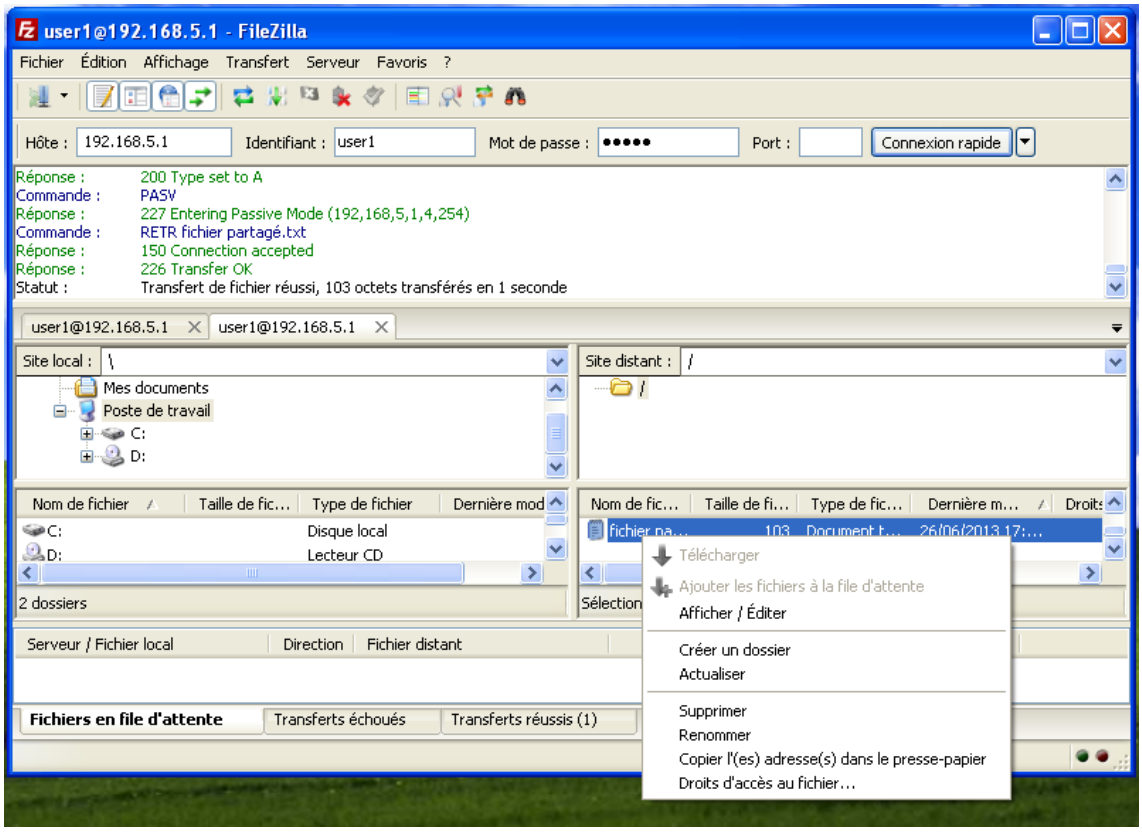
Une fenêtre apparait représente l'environnement de travail de GNS3.

```
-sh-2.05b# ls -l
-rwxrwxr-x    1 root     root          1108 Jul 12  2008 S20urandom
lrwxrwxrwx    1 root     root             7 Jan  3 20:59 S40network -> network
-rwxrwxr-x    1 root     root          2475 Jul 12  2008 S60ssh
lrwxrwxrwx    1 906417   25              12 Jan  3 21:00 S65transfer_cfg -> trans
fer_cfg
lrwxrwxrwx    1 root     root             4 Jan  3 21:00 S80cids -> cids
-rwxr-xr-x    1 cids     cids         16263 Jul 15  2009 cids
-rwxr-xr-x    1 root     root         15692 Jul 15  2009 cntr_plane_functions
-rwxrwxr-x    1 root     root          8648 Jul 12  2008 functions
-rwxr-xr-x    1 root     root         38623 Jul 15  2009 ids_functions
-rwxr-xr-x    1 root     root            94 Jul 15  2009 mfg_setup
-rwxrwxrwx    1 root     root          5501 Jul 12  2008 network
-rwxrwxr-x    1 root     root           954 Jul 12  2008 nfslock
-rwxrwxr-x    1 root     root           890 Jul 12  2008 ntpd
-rwxrwxr-x    1 root     root          1117 Jul 12  2008 rc.down
-rwxrwxr-x    1 root     root          2793 Jul 12  2008 rc.init
-rwxrwxr-x    1 root     root           408 Jul 12  2008 rcS
-rwxr-xr-x    1 root     root          3205 Jul 15  2009 set_irq_affinity.awk
-rwxrwxrwx    1 root     root          1035 Jul 15  2009 transfer_cfg
-sh-2.05b# _
```

```
-sh-2.05b# cp ids_functions ids_functions.orig
-sh-2.05b# vi ids_functions_
```

Le FileZila client

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 :



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

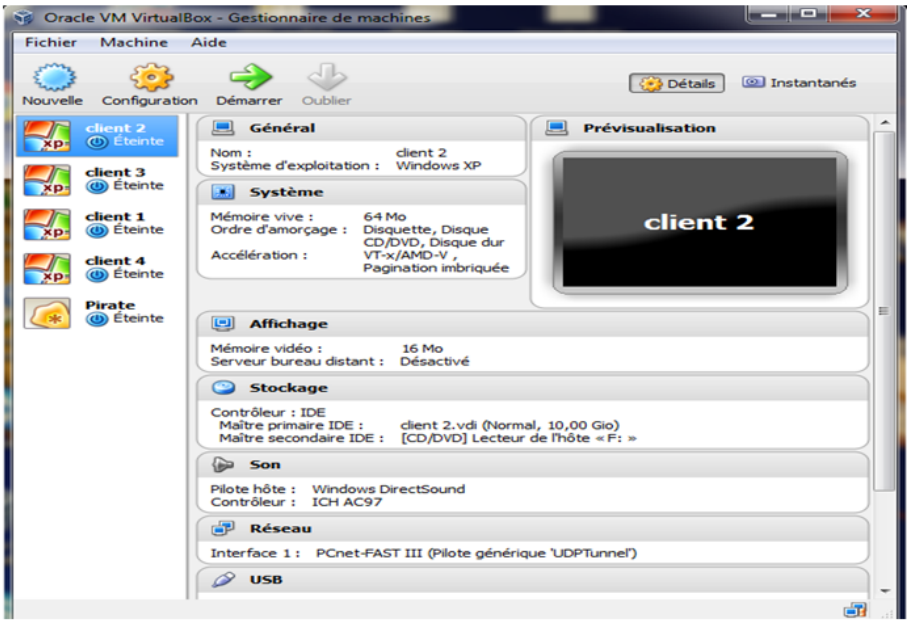
```
/loadrc
 cd /etc/init.d
 ./rc.init
cpids_functionsids_functions.orig
vi ids_functions
```

L'installation de Virtualbox

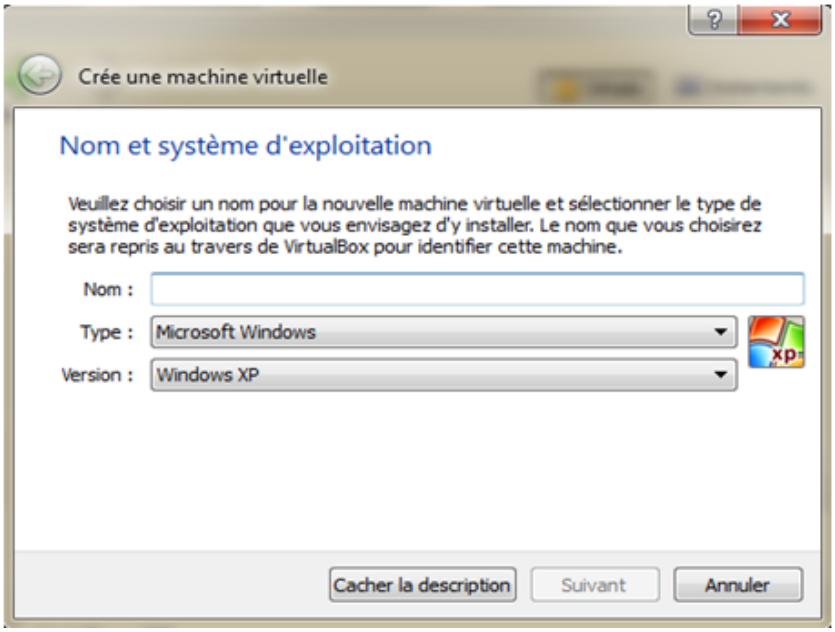
. Pour télécharger Virtualbox allez sur le site :https ://www.virtualbox.org/wiki/Downloads.

. Choisir la version adéquate au système et lancez l'installation.

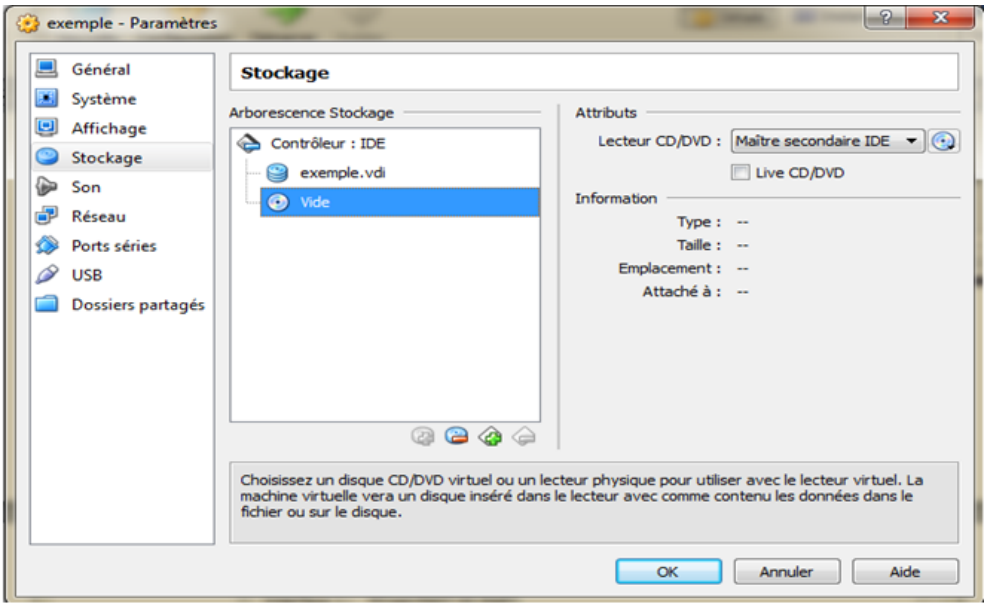
. Cliquer sur l'icône dans le bureau et une fenêtre apparait comme suit :



. Pour configurer une nouvelle machine aller sur nouvelle et suivre le guide d'assistant de création de machine virtuel.



. Une fois créer la machine apparait sur la liste gauche. Pour lui choisir un système d'exploitation sélectionner-la et cliquez sur configuration puis stockage.



. Cliquer sur la petite icône de CD la plus à droite. Puis cliquer sur " Choisissez un fichier de CD/DVD virtuel.

. Démarrer la machine virtuelle. OK à tous les messages. Cliquer sur Installer et le système choisit sera installer sur la machine.

La configuration d'un routeur en tant qu'un IDS

Il est possible de simuler un routeur au tant qu'un IDS pour cela réaliser les configurations suivantes :

La configuration au niveau du routeur

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname IDS
IDS(config)#interface f0/0
IDS(config-if)#ip address 192.168.1.2 255.255.255.0
IDS(config-if)#no shutdown
IDS(config-if)#
*Mar  1 00:02:35.319: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:02:36.319: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
IDS(config-if)#exit
IDS(config)#exit
IDS#
*Mar  1 00:02:47.239: %SYS-5-CONFIG_I: Configured from console by console
IDS# copy r s
Destination filename [startup-config]?
Building configuration...
[OK]
IDS#
```

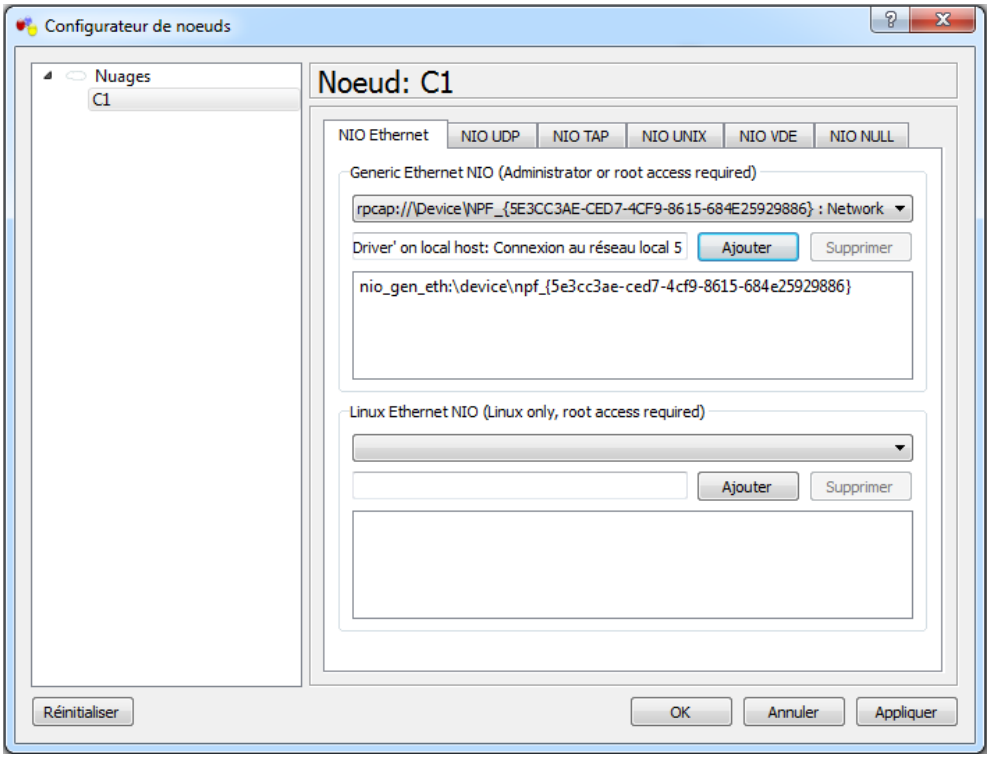
- Tester la connexion avec le PC en utilisant la commande Ping :

IDS#Ping192.168.1.2

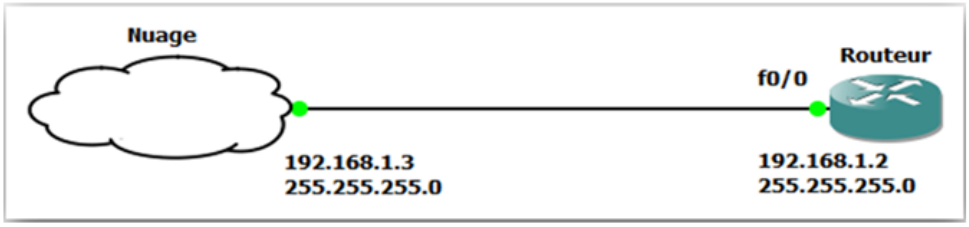
Configurer une carte de bouclage

1. aller sur menu démarrer, exécuter, cmd, taper la commande ” hdwwiz ”
2. une fenêtre d’ajout de matériel apparaitre, puis un clic sur Suivant
3. Installer le matériel que je sélectionne manuellement dans une liste (Avancé)
4. Cliquer sur Cartes réseau, puis sur Suivant
5. Sélectionner Microsoft comme le fabricant, puis sur Microsoft bouclage adaptateur sous Adaptateur réseau puis cliquer sur Suivant, puis de nouveau sur Suivant.
6. Ouvrir le Panneau de configuration -¿ Connexions réseau pour voir la carte en place.
7. Sélectionner cette carte, cliquer sur ” ajouter ”, en suite ” appliquer ”, et ” Ok ”.

Pour configurer le nuage un clique droit et dans le menu textuelle choisir Configure cette fenêtre apparait d’où lui attribuer la carte de bouclage créer :



8. Connecter-la à l’interface f0/0. Et vérifier que le câble est indiqué ’connecté’.



Configuration via SDM

Afin d'utiliser SDM, on doit attribuer une adresse IP à la carte de bouclage et configurer les commandes suivantes sur le routeur :

- **Etape 1 :** Activer le http en mode de configuration globale :

```
IDS # configure terminal
IDS (config) # ip http server
IDS (config) # ip http authentication local
IDS (config) # username cisco privilege 15 password Cisco123
```

- **Etape 2 :** Créer un compte utilisateur et définir le niveau de privilège en 15, et remplacer "username" et "password" par les chaînes souhaitéesà utiliser :

```
Router(config)# username "username" privilege 15 secret 0 "password"
```

Utiliser ce nom d'utilisateur et le mot de passe pour connecter à SDM.

- **Etape 3 :** Configurez SSH et Telnet pour la connexion locale avec un niveau de privilège de 15 :

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

Présentation de SDM (Security Device Manager)

Définition

Cisco SDM est un outil de configuration basé sur le Web qui simplifie et facilite la configuration par le biais assistants intelligents qui aident les clients rapidement et facilement pour déployer, configurer et surveiller n'importe quel équipement Cisco sans nécessiter de connaissances de l'interface ligne de commande (CLI) **W22**.

Le Cisco SDM permet de télécharger les fichiers de définition de signature SDF (Signature Definition Files) à partir de Cisco.com, les importer sur un routeur, d'activer l'IDS sur les interfaces du routeur, mise au point signatures IDS et fournir des signatures édités au routeur.

Fichiers de définition de signature

IOS IPS utilise un SDF pour maintenir la base de données de la menace d'un routeur. Chaque SDF contient de nombreuses définitions de signatures qui décrivent les conditions spécifiques auxquelles une menace est probable, et l'action par défaut (s) à prendre lorsqu'une menace est détectée.

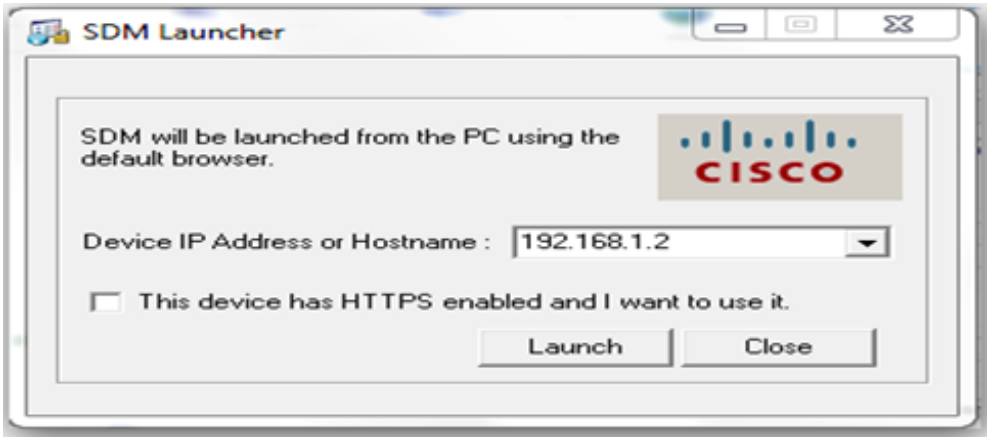
Cisco IOS IPS est livré avec 132 signatures intégrées prêtes à l'emploi. Trois fichiers SDF supplémentaires sont disponibles qui sont construits pour certains besoins en mémoire :

- atack-drop.sdf : Conçu pour les routeurs de moins de 128 Mo de mémoire. Contient 83 signatures.
- 28MB.sdf : Conçu pour les routeurs avec 128 Mo de mémoire ou plus. Contient 300 signatures.
- 256MB.sdf : Conçu pour les routeurs avec 256 Mo de mémoire ou plus. Contient 500 signatures.

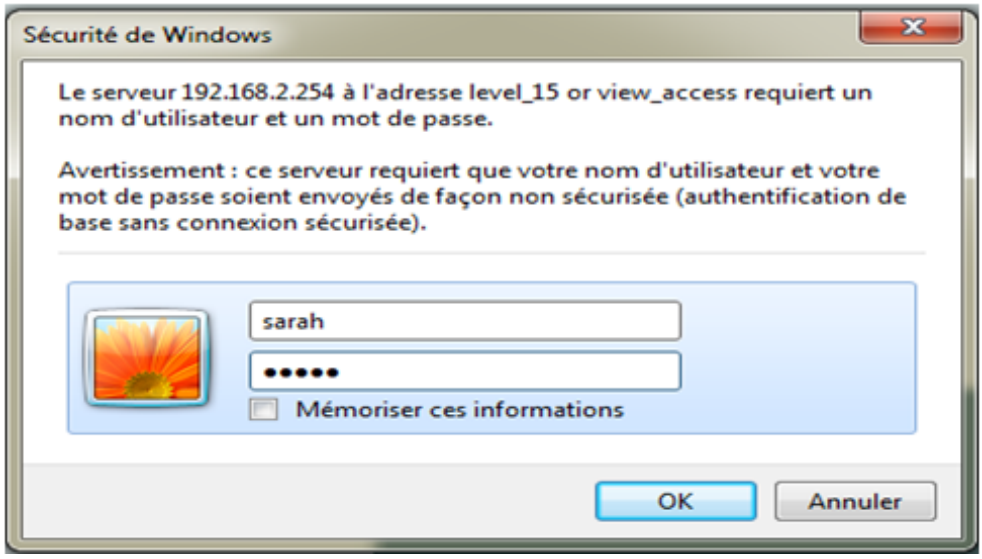
Cisco publie également et fréquemment des mises à jour des fichiers SDF qui peuvent être ajoutés au fichier SDF existant actuellement en service sur les routeurs.

Installer le logiciel SDM.

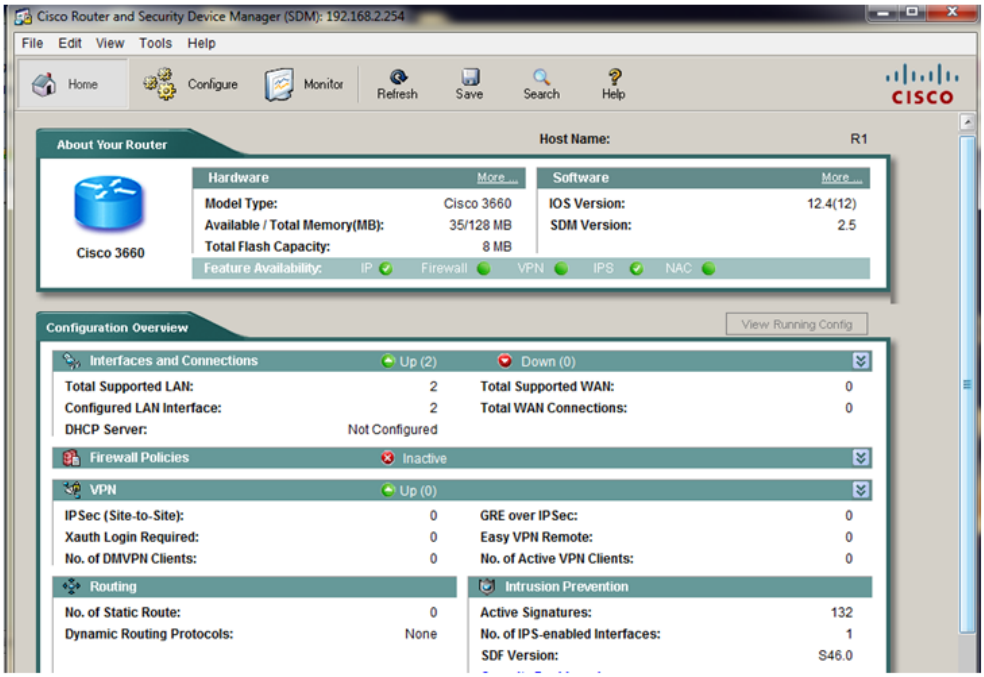
Suivre l'assistant d'installation, une fois terminer la fenêtre ci-dessous apparait elle permet d'accéder à notre équipement et cela en saisissant l'adresse IP de ce dernier.



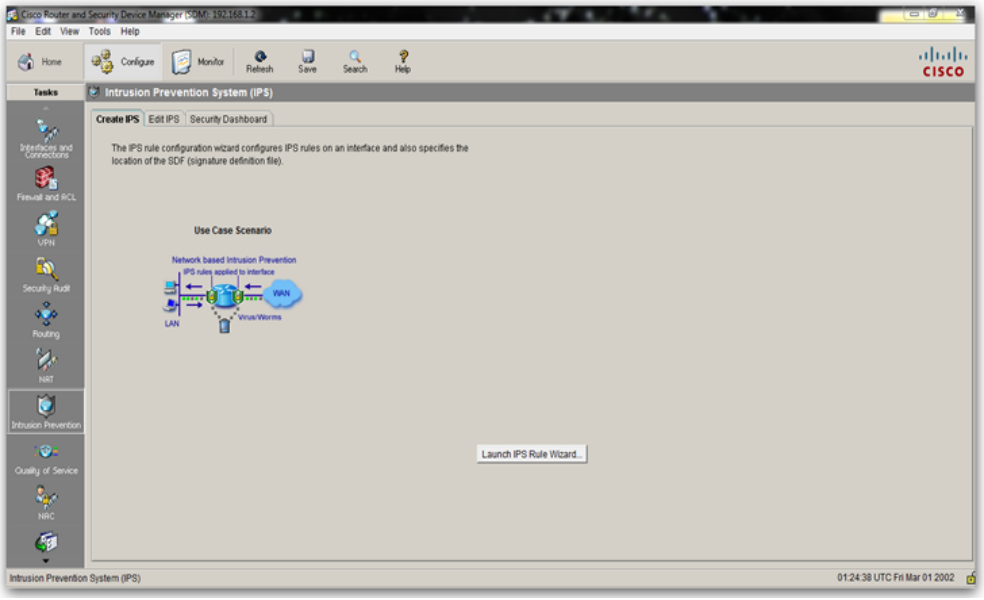
Cliquer Launch et une fenêtre d'authentification s'affiche comme suit :



Saisir le login et le mot de passe puis OK. La fenêtre ci-dessous s'affiche.

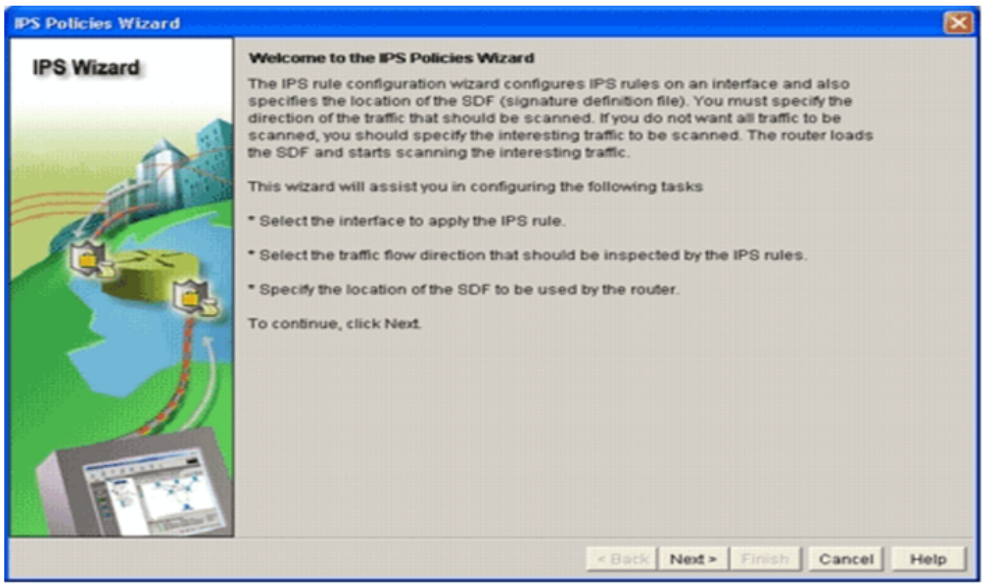


1. Dans l'application de SDM, cliquer Configure, et cliquer sur Intrusion Prevention.



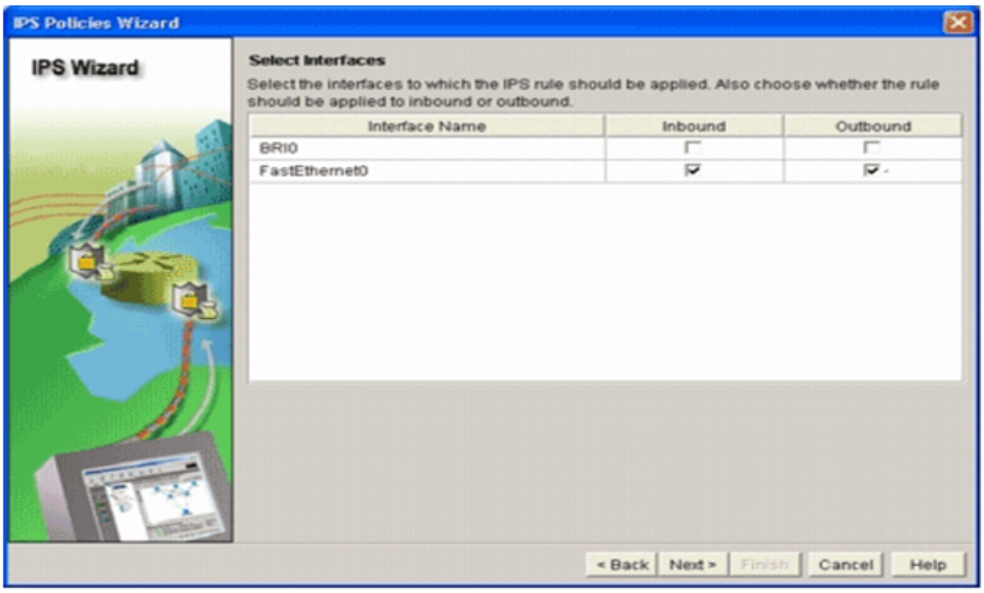
2. Cliquer sur Create IPSetcliquersur Launch IPS Rule Wizard.

3. Cliquer sur OK.



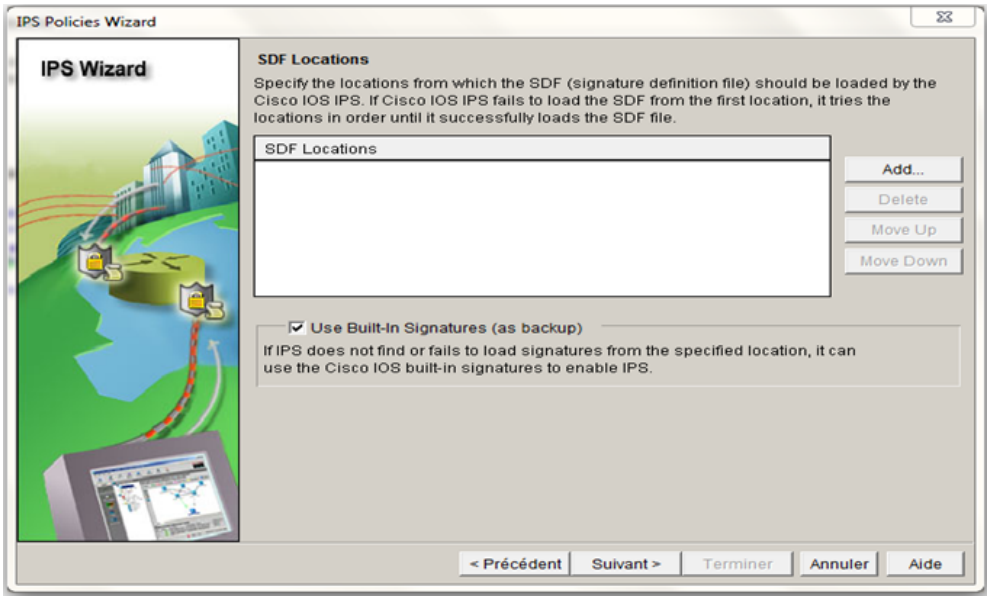
4. Cliquer Next.

5. La fenêtre de la sélection d'interfaces apparaît.



6. Choisi les interfaces pour lesquelles cocher Inbound.

7. Cliquer Next.



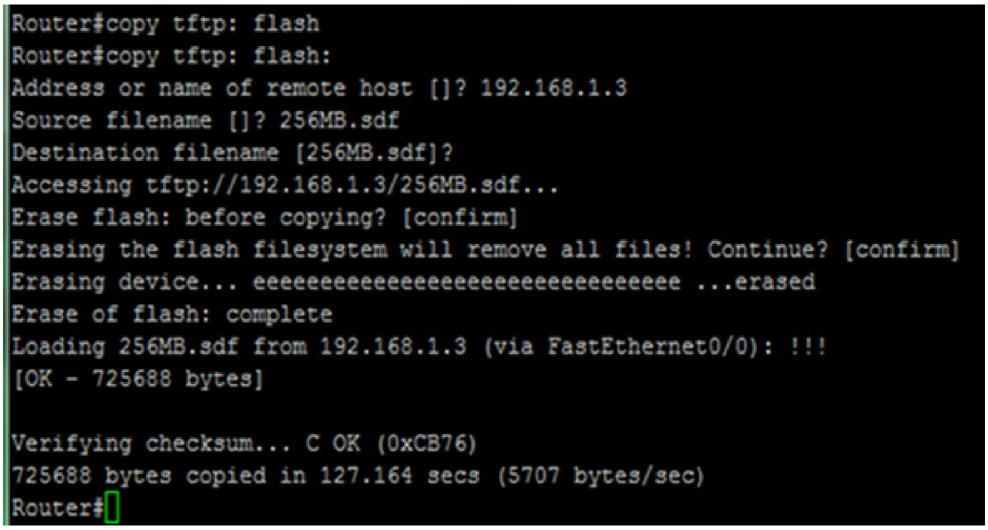
Pour additionner les signatures à l'endroit du SDF, on doit tout d'abord les télécharger sur la mémoire flash du Routeur via l'application TFTP (Trivial File Transfer Protocole).

8. Lancer l'application TFTP, et Insérer les commandes suivantes dans la console du Routeur.

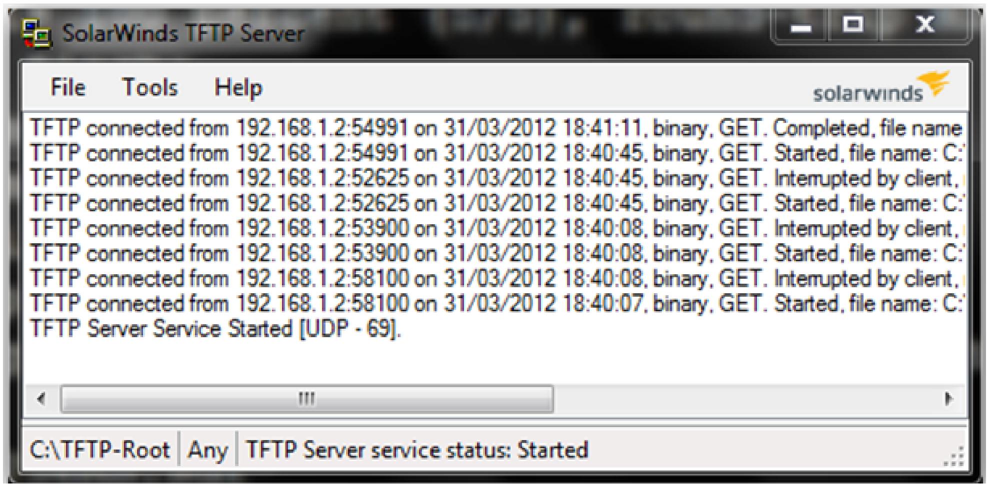
IDS # copy tftp : flash :

Address or name of remote host [ ] ? 192.168.1.3

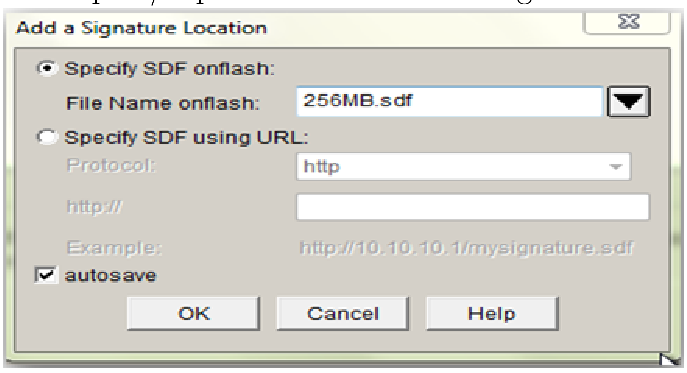
Source file name [ ] ? 256MB.sdf



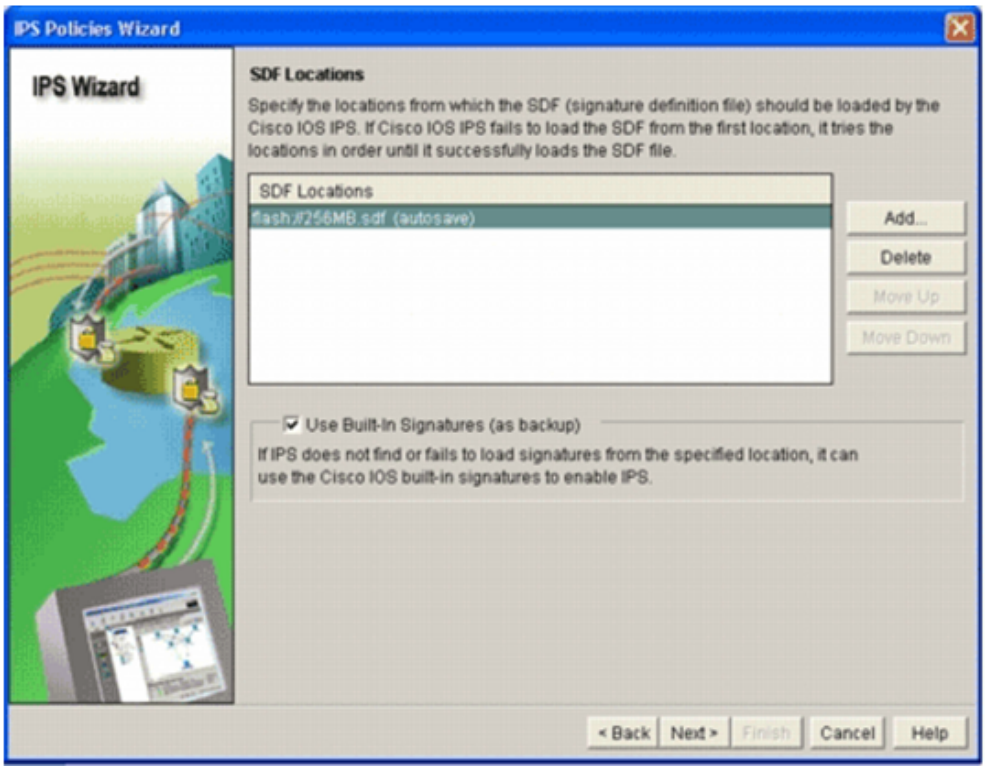
Le téléchargement via le serveur TFTP est comme suit :



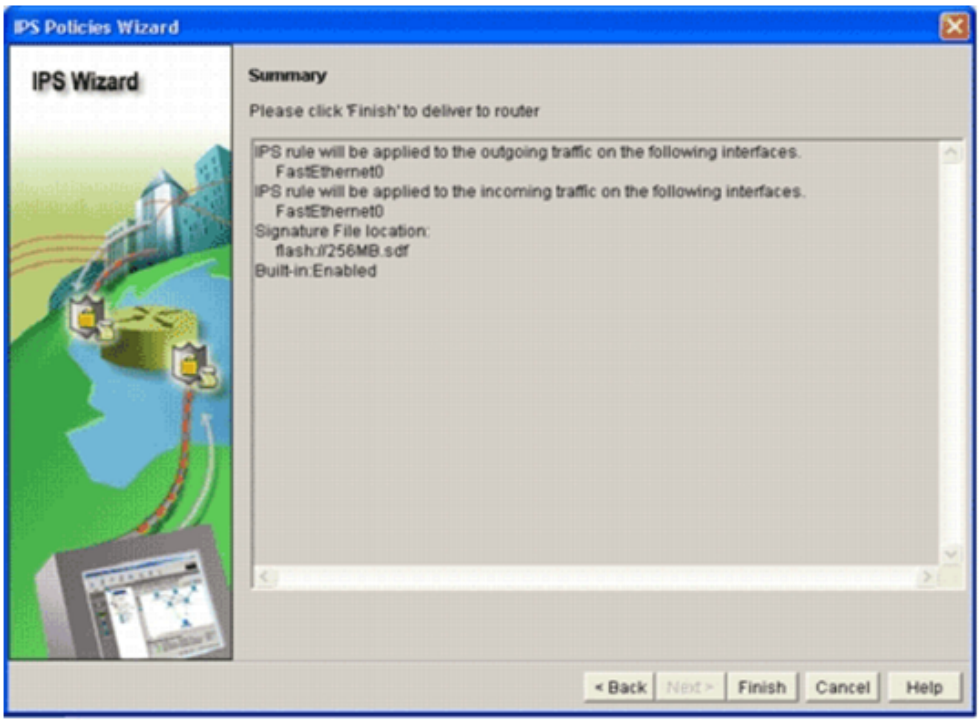
. **Serveur TFTP :** Import/export de fichiers de configuration.



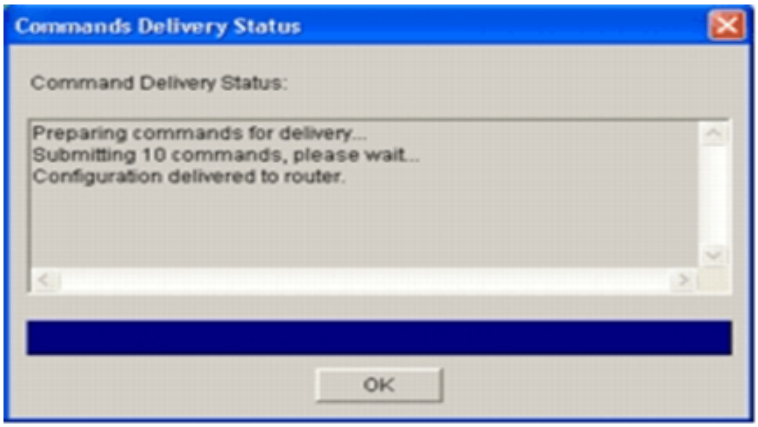
9. Cliquer sur Specify SDF on flash, et choisir 256MB.sdf du File Name on flash
10. Cliquer sur autosave,et cliquer sur Ok.



11. Cocher la case Use Built-In Signatures (as backup).
12. Cliquer Next afin de continuer.

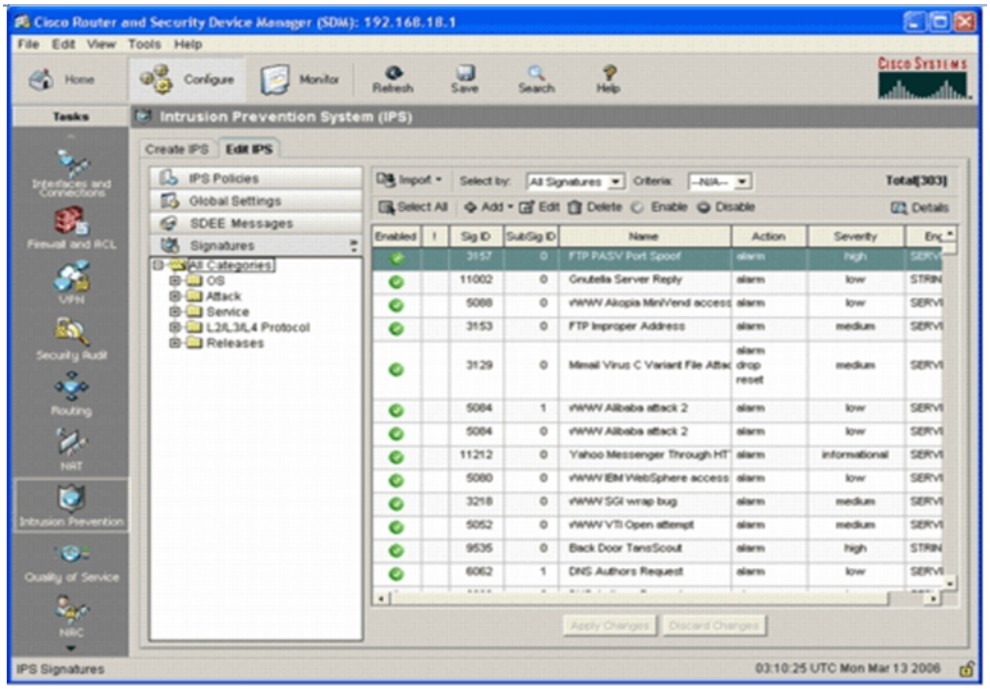


13. Cliquer Finish.



14. cliquer Ok.

Afin de vérifier quelles signatures sont actuellement chargées sur le Routeur, cliquer Configure, puis Intrusion Prevention, en suite sur l'étiquette Edit IPS.



Le serveur FTP

Un serveur FTP est utilisé dans le cas où l'on souhaite rendre disponible des fichiers (dans un réseaulocal ou sur internet) et ce que ce soit de manière anonyme ou grâce à des comptes utilisateurs.

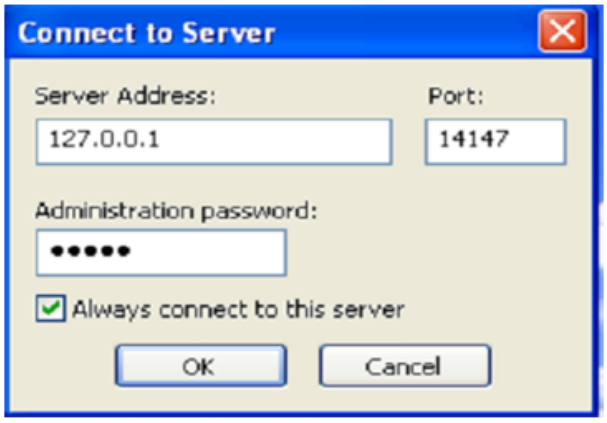
Le serveur ftp dont nous avons choisi d'installer et de configurer se nomme FileZila Server (License open source et par ailleurs gratuit).

Installation et configuration

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.

La configuration du FileZila Server

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

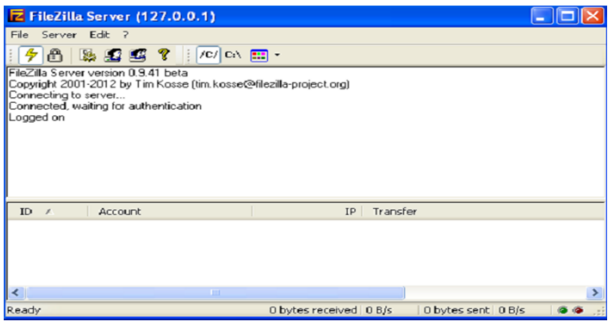


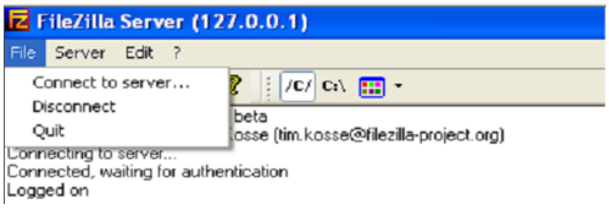
Cette boite de dialogue va permettre la connexion au serveur ftp. Saisir l'adresse IP du serveur ici c'est localhost, port d'administration du serveur ftp (14147 par défaut) et le mot de passe spécifier le mot depasse qui protège la partie administration du serveur.

Clique sur le bouton OK pour effectuer la connexion à l'interface d'administration du serveur ftp.

Pour se connecter ou déconnecter du serveur :

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

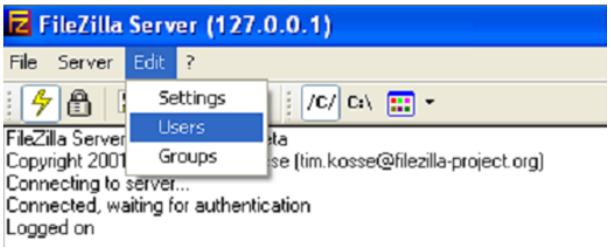


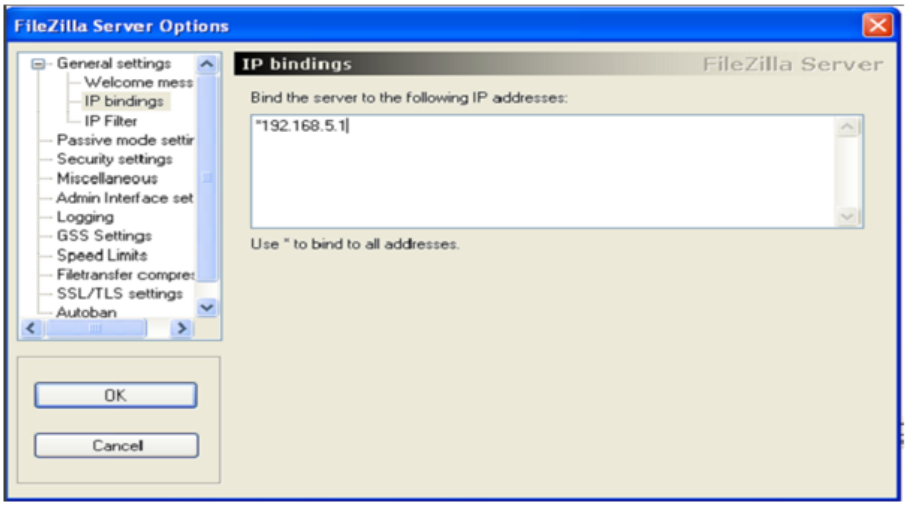


- **Le menu Settings :** Cette option affiche la fenêtre qui permet de définir les options du serveur ftp. En autres, nous pouvons définir les options de type message de bienvenue, port utilisé, etc.
- **Le menu Users :** Cette option affiche la fenêtre qui permet de définir les utilisateurs (ainsi les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

Nous avons configuré l'essentiel du serveur pour répondre à nos besoins de simulation :

1. Pour l'attribution d'adresse IP, aller sur le menu Edit - Settings -IP bindings, l'option IP bindings permet de définir l'adresse IP sur lequel le serveur ftp est disponible.Pour notre cas c'est l'adresse de la machine sur lequel est installé FileZila Sever.
2. L'option Passive mode Settings permet de configurer le serveur en mode PASV (passif) si ce dernier se trouve derrière un firewall ou un routeur
3. Pour ajouter les utilisateurs ayant le droit d'accéder au serveur : Edit -Users- General et cliquer sur Add. L'utilisateur sera ajouté comme suit :
4. Après l'ajout des utilisateurs il faut créer les fichiers à partager pour cela aller sur l'onglet sharedfolfers, cliquer sur ajouter puis cocher sur les droits d'accès associé à chacun des utilisateurs.





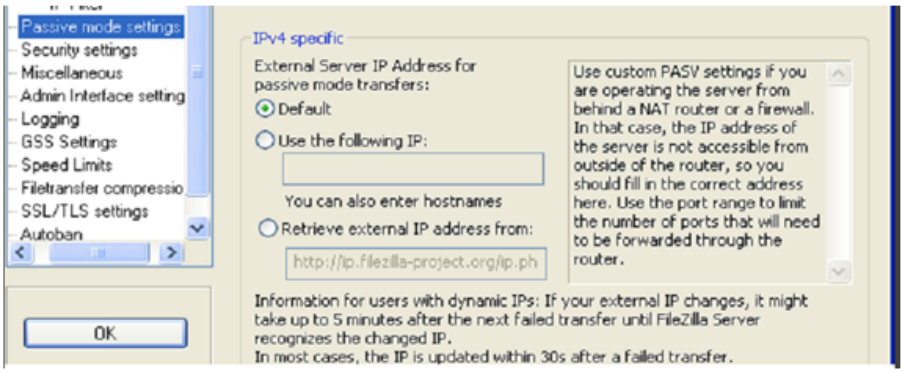
5. Et en fin ajouter un groupe pour les différents utilisateurs cela dans le menu Edit -Groups-General -¿Add

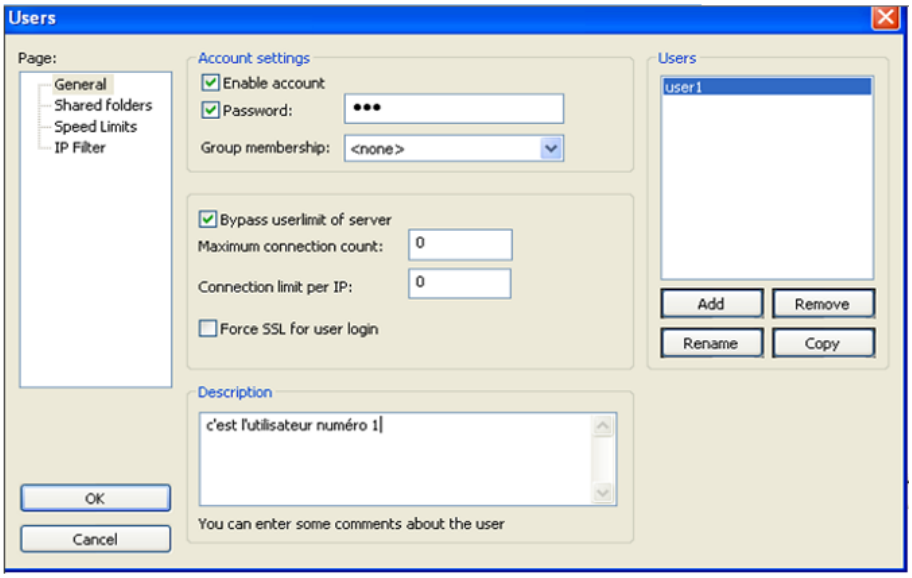
   Puis modifier le groupe des utilisateurs déjà créés.

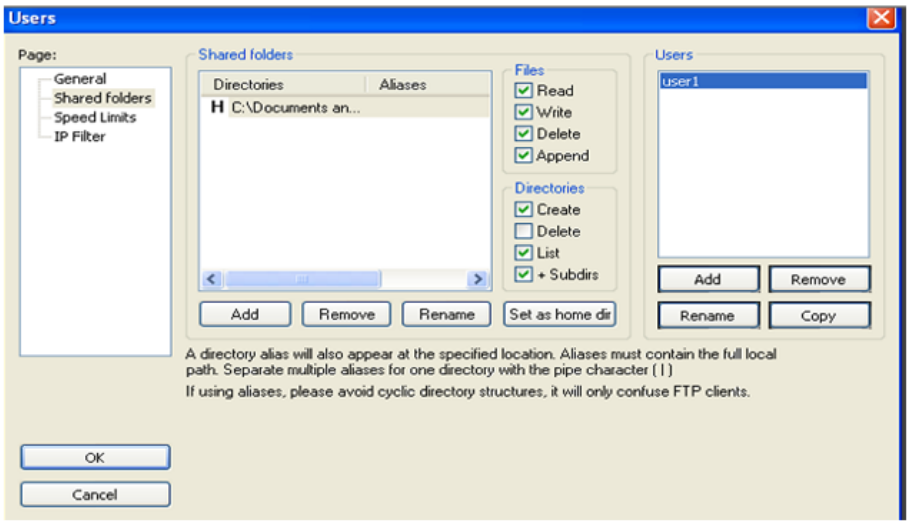
Le FileZila client

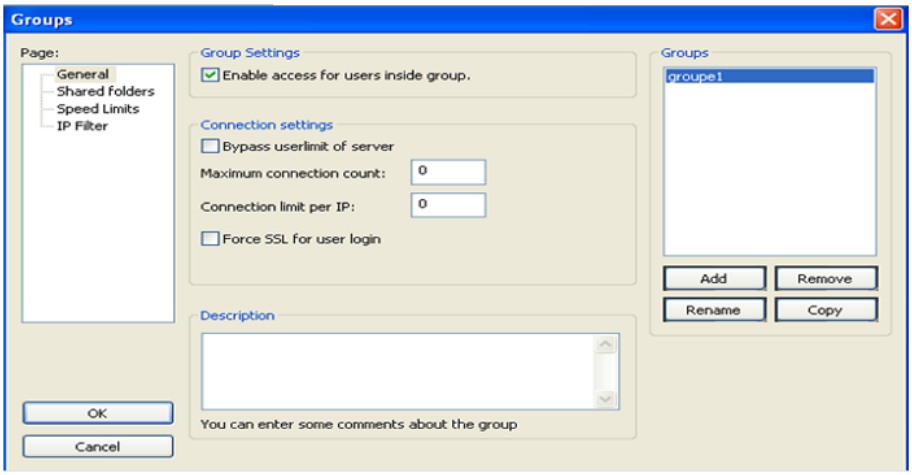
Une fois l'application est installée une fenêtre s'ouvre permet au client d'accéder au serveur ftp comme montrer dans la figure ci-dessous :

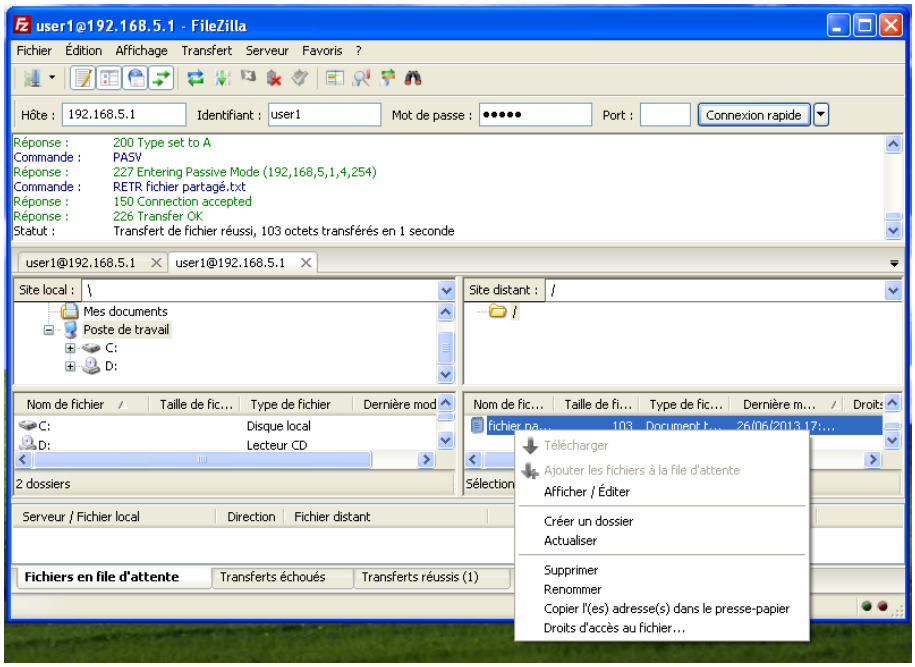
Le client maintenant peut effectuer tous ces droits sur les fichiers partagés et apporter des modifications selon ces besoins.


Passive mode settings
Security settings
Miscellaneous
Admin Interface setting
Logging
GSS Settings
Speed Limits
Filetransfer compressio
SSL/TLS settings
Autoban
OK
IPv4 specific
External Server IP Address for passive mode transfers:
Default
Use the following IP:
You can also enter hostnames
Retrieve external IP address from:
http://ip.filezilla-project.org/ip.ph
Use custom PASV settings if you are operating the server from behind a NAT router or a firewall. In that case, the IP address of the server is not accessible from outside of the router, so you should fill in the correct address here. Use the port range to limit the number of ports that will need to be forwarded through the router.
Information for users with dynamic IPs: If your external IP changes, it might take up to 5 minutes after the next failed transfer until FileZilla Server recognizes the changed IP.
In most cases, the IP is updated within 30s after a failed transfer.


Users
Page:
General
Shared folders
Speed Limits
IP Filter
Account settings
Enable account
Password:
Group membership:
<none>
Bypass userlimit of server
Maximum connection count:
0
Connection limit per IP:
0
Force SSL for user login
Description
c'est l'utilisateur numéro 1
You can enter some comments about the user
Users
user1
Add
Remove
Rename
Copy
OK
Cancel


Users
Page:
General
Shared folders
Speed Limits
IP Filter
Shared folders
Directories
Aliases
C:\Documents an...
Files
Read
Write
Delete
Append
Directories
Create
Delete
List
+ Subdirs
Add
Remove
Rename
Set as home dir
Users
user1
Add
Remove
Rename
Copy
A directory alias will also appear at the specified location. Aliases must contain the full local path. Separate multiple aliases for one directory with the pipe character (|)
If using aliases, please avoid cyclic directory structures, it will only confuse FTP clients.
OK
Cancel


Groups
Page:
General
Shared folders
Speed Limits
IP Filter
Group Settings
Enable access for users inside group.
Connection settings
Bypass userlimit of server
Maximum connection count:
0
Connection limit per IP:
0
Force SSL for user login
Description
You can enter some comments about the group
Groups
groupe1
Add
Remove
Rename
Copy
OK
Cancel


user1@192.168.5.1 - FileZilla
Fichier Édition Affichage Transfert Serveur Favoris ?
Hôte : 192.168.5.1
Identifiant : user1
Mot de passe :
Port :
Connexion rapide
Réponse : 200 Type set to A
Commande : PASV
Réponse : 227 Entering Passive Mode (192,168,5,1,4,254)
Commande : RETR fichier partagé.txt
Réponse : 150 Connection accepted
Réponse : 226 Transfer OK
Statut : Transfert de fichier réussi, 103 octets transférés en 1 seconde
Site local : \
Mes documents
Poste de travail
C:
D:
Site distant : /
Nom de fichier
Taille de fic...
Type de fichier
Dernière mod
C: Disque local
D: Lecteur CD
2 dossiers
Télécharger
Ajouter les fichiers à la file d'attente
Afficher / Éditer
Créer un dossier
Actualiser
Supprimer
Renommer
Copier l'(es) adresse(s) dans le presse-papier
Droits d'accès au fichier...
Serveur / Fichier local
Direction
Fichier distant
Fichiers en file d'attente
Transferts échoués
Transferts réussis (1)

Liste des avréviation

Liste des abréviations

ACL (**A**ccess **C**ontrol **L**ist)

ACID (**A**nalysis **C**onsole for **I**ntrusion **D**atabases)

AES (**A**dvanced **E**ncryption **S**tandard)

ARP (**A**ddress **R**esolution **P**rotocol)

ASIC (**A**pplication-**S**pecific **I**ntegrated **C**ircuit)

CLI (**C**ommand-**L**ine **I**nterpreter)

CPU (**C**entral **P**rocessing **U**nit)

DDoS (**D**istibuted **D**enial of **S**ervice)

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol)

DMZ (**D**e**M**ilitarized **Z**one)

DNS (**D**omain **N**ame **S**ystem)

DoS (**D**enial **o**f **S**ervice)

EMS (**E**nterprise **M**anagement **S**ystem)

FAI (**F**ournisseur d'**A**ccès **I**nternet)

FTP (**F**ile **T**ransfer **P**rotocol)

GPL (**G**eneral **P**ublic **L**icence)

GRUB (**G**Rand **U**nified **B**ootloader)

HTTP (**H**yper **T**ext **T**ransfer **P**rotocol)

ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol)

IDM (**I**PS **D**evice **M**anager)

IDS (**I**ntrusion **D**etection **S**ystem)

IDWG (**I**ntrusion **D**etection exchange format **W**orking **G**roup)

IETF (**I**nternet **E**ngineering **T**ask **F**orce)

IIS (**I**nternet **I**nformation **S**ervices)

IOS (**I**nternetwork **O**perating **S**ystems)

IP (**I**nternet **P**rotocol)

IPS (**I**ntrusion **P**revention **S**ystem)

ISO (**I**nternational **O**rganization for **S**tandardization)

ISS (**I**nternet **S**ecurity **S**ystems)

MAC (**M**edia **A**ccess **C**ontrol)

MAC (**M**essage **A**uthentication **C**ode)

MSS (**M**aximum **S**egment **S**ize)

NAT (**N**etwork **A**ddress **T**ranslation)

NIC (**N**etwork **I**nterface **C**ard)

PDA (**P**ersonal **D**igital **A**ssistant)

Ping (**P**acket **I**Nternet **G**roper)

RADIUS (**R**emote **A**uthentication **D**ialIn **U**ser **S**ervice)

RAM (**R**andom **A**ccess **M**emory)

RFC (**R**equest **F**or **C**omments)

RTC (**R**éseau **T**éléphonique **C**ommuté)

SDF (**S**ignature **D**efinition **F**iles)

SDM (**S**ecurity **D**evice **M**anager)

SMTP (**S**imple **M**ail **T**ransport **P**rotocol)

SSID (**S**ervice **S**et **ID**entifier)

SSG550 (**S**ecure **S**ervices **G**ateway)

TCP (**T**ransmission **C**ontrol **P**rotocol)

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocole)

TLS (**T**ransport **L**ayer **S**ecurity)

URL (**U**niform **R**esource **L**ocator)

VPN (**V**irtual **P**rivate **N**etwork)

VRF (**V**irtual**R**outing and **F**orwarding)

VsFTPd (**V**ery **s**ecure **FTPd**)

WPA (**W**i-Fi **P**rotected **A**ccess)

Glossaire

A :

ASIC (Application-Specific Integrated Circuit) : littéralement " circuit intégré propre à une application " est un circuit intégré (micro-électronique) spécialisé. En général, il regroupe un grand nombre de fonctionnalités uniques ou sur mesure.

C :

CLI (Command-line interpreter) : Un interpréteur de commandes est un programme faisant partie des composants de base d'un système d'exploitation. Sa fonction est d'interpréter les commandes qu'un utilisateur tape au clavier dans l'interface en ligne de commande.

G :

GRUB (GRand Unified Bootloader) : GNU GRUB (acronyme signifiant en anglais " GRand Unified Bootloader ") est un programme d'amorçage de micro-ordinateur. Il s'exécute à la mise sous tension de l'ordinateur, après les séquences de contrôle interne et avant le système d'exploitation proprement dit, puisque son rôle est justement d'en organiser le chargement. Lorsque le micro-ordinateur héberge plusieurs systèmes (on parle alors de multi-amorçage), il permet à l'utilisateur de choisir quel système démarrer.

I :

IDWG (Intrusion Detection exchange format Working Group) : Le but du groupe de travail de détection d'intrusion est de définir des formats de données et d'échanger des procédures pour partager l'information d'intérêt aux systèmes de détection et de réponse d'intrusion, et aux systèmes de gestion qui peuvent devoir agir l'un sur l'autre avec eux.

M :

MAC (Media Access Control) : est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire et utilisé pour attribuer mondialement une adresse

unique au niveau de la couche de liaison (couche 2 du modèle OSI).

MSS (Maximum Segment Size) : Quantité maximale de données, spécifiée en octets, qu'un ordinateur ou un périphérique de communication peut transmettre en une fois. Pour une communication optimale, le nombre d'octets du segment de données additionné du nombre d'octets du header doit être inférieur au MTU (maximum transmission unit).

P :

Ping (Packet INternet Groper) : est sans nul doute l'un des outils d'administration de réseau le plus connu. Il s'agit pourtant de l'un des outils les plus simples puisqu'il permet, grâce à l'envoi de paquets, de vérifier si une machine distante répond et, par extension, qu'elle est accessible par le réseau.

R :

RFC (Request For Comments) : littéralement " demande de commentaires ", sont une série numérotée de documents officiels décrivant les aspects techniques d'Internet, ou de différents matériels informatiques (routeurs, serveur DHCP). Peu de RFC sont des standards, mais tous les documents publiés par l'IETF sont des RFC.

S :

SSID (Service Set IDentifier) : est l'identifiant d'un réseau sans fil et il comprend jusqu'à 32 caractères alphanumériques. Pour vous connecter à un point d'accès, il est indispensable de le connaître. Ainsi, pour des questions de sécurité, il est vivement conseillé de modifier le nom du réseau par défaut.

V :

VRF (Routing and Forwarding virtuel) : est une technologie qui permet à plusieurs instances d'une table de routage de coexister dans le même routeur en même temps.

Parce que les instances de routage sont indépendantes, les mêmes ou qui se chevauchent adresses IP peuvent être utilisés sans entrer en conflit les uns avec les autres.

X :

MAS (Christmas, Noël en anglais) : La technique Xmas a été nommée ainsi en souvenir de l'attaque du serveur de Tsutomu Shimomura par Kevin Mitnick le jour de Noël 1994.

Résumé

Le travail réalisé dans ce mémoire consiste à la configuration d'un système de détection d'intrusions (en anglais, Intrusion Detection System ou IDS) et sa mise en œuvre au niveau de l'architecture réseau de Cevital. Un système de détection d'intrusion s'avère indispensable en complément d'outils de sécurité plus conventionnels. Il permet en effet de détecter des comportements qui peuvent mettre en cause la confidentialité ou la disponibilité d'un système. Nous avons étudié dansce mémoire les différents aspects relatifs à notre projet à savoir : les généralités sur la sécurité informatique et les attaques menaçant le réseau, présenter les différents mécanismes de sécurité (firewalls, proxy, ...), en suite décrire les systèmes de détection d'intrusions et en fin, nous avons terminé avec une réalisation, 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 : Sécurité informatique, Attaques, Systèmes de détection d'intrusions, Test.

Abstract

The work that has been done in this paper has aimed at configuring an intrusion detection system (IDS) and its implementation at the network of architecture in Cevital. An intrusion detection system is essential as a conventional security tool. It permits to detect behaviours that may jeopardize or threaten the confidentiality or availability of a system. In this work, we have examined the different aspects that are related to our project, namely : we have studied general computer security, attacks that threaten the network and presented the various security mechanisms (firewalls, proxy ...), then we have described the intrusion detection systems. To conclude, we have dealt with a realization in which we have used a set of tools : GNS3 for simulation and topology configuration, IDM for access and configuration of the IDS and BackTrack for reliability testing.

Keywords : Computer Security, Attacks, Intrusion Detection Systems, Test.