Université Mouloud Mammeri Tizi Ouzou
Faculté de Génie Electrique et Informatique
Département Informatique

MÉMOIRE DE FIN D'ÉTUDES

En vue de l'obtention du diplôme Master en informatique

Option: Réseaux, Mobilité Et Systèmes Embarqués

Thème:

Implémentation d'un IPS Cisco dans une entreprise

Cas: ENIEM

Réalisé par :

- **M^{elle}.AYACHE Karima**
- **M^{elle}.ZIANI Nora**

Dirigé par :

M^{me}. BOURKACHE Ghenima

Co-promoteur : **M$_r$ Taleb Ferhat**

2015

Sommaire

Introduction générale

Chapitre 1: généralité sur la sécurité informatique

Introduction 8
I.1)Concepts de base 8
I.2)Les enjeux de la sécurité informatique 9
I.3)Les différentes étapes d'une attaque 9
I.4)Les types d'attaques 10
I.4.1) Les attaques virales 10
I.4.2) Attaques de reconnaissance 10
I.4.2.1) Packet Sniffer 10
I.4.2.2) Balayage par Ping 11
I.4.2.3) Port scanning 12
I.4.2.4) L'ingénierie sociale 12
I.4.3) Les attaques d'accès 12
I.4.3.1) Le craquage de mots de passe 12
I.4.3.2) Trust exploitation 13
I.4.3.3) Redirection de Port 13
I.4.3.4) Attaque Man-in-the-middle 15
I.4.3.5) Buffer Overflow 15
I.4.3.6) Porte dérobée 15
I.4.4) Les attaques DOS et DDoS 15
I.4.4.1) Ping of Death 16
I.4.4.2) Smurf 16
I.4.4.3) TCP SYN Flood 17
I.5)Les mécanismes de défense 18
I.5.1) Les mots de passe 18
I.5.2) Cryptographie 19
I.5.3) Les antivirus 21
I.5.4) Les pare-feux 21
I.5.5) VPN 22
I.5.6) Présentation générale des IDS et IPS 22
Conclusion 23

Chapitre 2 : les systèmes de détection et de prévention d'intrusions

Introduction 24
II.1) Système de détection d'intrusions (IDS) 24
II.1.1) Présentation 24
II.1.2) Principe de détection d'intrusion 24
II.1.2.1) APPROCHE PAR SCENARIO 24
II.1.2.1.1) Analyse de motif 25
II.1.2.1.2) Recherches génériques 25
II.1.2.1.3) Contrôle d'intégrité 25
II.1.2.2) APPROCHE COMPORTEMENTALE 25

II.1.2.2.1) Approche probabiliste 25
II.1.2.2.2) Approche statistique 26
II.1.2.2.3) Réseaux de neurones 27
II.1.3) Type d'IDS 27
II.1.3.1) Network based IDS (NIDS) 27
II.1.3.2) Host Based IDS (HIDS) 30
II.2) IPS (Système de Prévention d'Intrusions) 30
II.2.1) Présentation 30
II.2.2) Type d'IPS 30
II.2.2.1) Network based IPS 30
II.2.2.2) Host Based IPS (HIPS) 31
II.2.3) Type de réponses aux attaques 31
II.2.3.1) Réponse Active 31
II.2.3.2) Réponse Passive 32
II.2.4) IDS/IPS 33
II.2.5) IPS/Firewall 33
Conclusion 33

Chapitre 3 : Les solutions IPS de Cisco Systems

Introduction 35
III.1) Caractéristiques des IDS et IPS 35
III.2) Les signatures des IPS Cisco 35
III.2.1) Types de Signatures 36
III.2.1.1) Signature atomique 36
III.2.1.2) Signature composite 36
III.2.2) Le fichier de Signatures IPS Cisco 36
III.2.3) Les alarmes de signatures Cisco 37
III.2.4) Actions de Signature IPS 39
III.3) Les différents produits IPS de Cisco 40
III.3.1) Les capteurs Cisco IPS 4200 Series 41
III.3.2) Cisco Catalyst 6500 Series IDSM-2 Module 42
III.3.3) Cisco ASA 500 44
III.3.4) Routeurs Cisco à Services Intégrés (ISR) 45
III.3.4.1) Cisco ISR avec AIM-IPS et NME-IPS 45
III.3.4.2) Cisco ISR avec IOS IPS 46
III.4) Les composants d'un routeur 47
III.5) Le système d'exploitation IOS 48
III.5.1) L'architecture de l'IOS 48
III.5.2) Les technologies de sécurité dans le Cisco IOS 50
Conclusion 50

Chapitre 4 : Présentation de l'organisme d'accueil ENIEM

Introduction 51
IV.1) Présentation de l'ENIEM 51

IV.1.1) Missions et objectifs 52
IV.1.2) Organisation générale de l'ENIEM 52
IV.1.2.1) Les directions 52
IV.1.2.2) Les unités de production 53
IV.2) Présentation du champ d'études 54
IV.2.1) Organigramme de l'unité prestation technique 54
IV.2.2) Caractéristiques du réseau informatique de l'ENIEM 55
IV.2.3) L'aspect logiciel des composants du réseau 56
IV.2.4) L'aspect humain du département informatique 57
IV.3) Critique des systèmes de sécurité 57
IV.4) Solution proposée 58
Conclusion 58

Chapitre 5 : implémentation de la solution Cisco IOS IPS
Introduction 61
V.1) Présentation des outils utilisés 61
V.1.1) Le simulateur graphique de réseaux GNS3 61
V.1.2.) Virtual Box 4 .3.1 62
V.1.3) Server syslog 62
V.1.4) Backtrack 5 r3 65
V.1.5) Les protocoles utilisés 65
V.1.5.1) Le protocole OSPF (Open Shortest Path First) 65
V.1.5.2) Le protocole NAT (Network Address Translation) 66
V.2) Implémentation de l'IOS IPS 66
V.2.1) La nouvelle architecture de l'ENIEM 66
V.2.2) Configuration du routeur 68
V.2.2.1) Les méthodes utilisées pour la configuration d'un routeur 68
V.2.2.2) Configuration de base du routeur 69
V.2.3) Configuration de l'IOS IPS du routeur 72
V.3) Test de quelques exemples d'attaques 78
V.3.1) Test de la signature Demande D'echo Request 78
V.3.2) Test d'IPS avec Nmap de backtrack 79
Conclusion 80
Conclusion générale 80

Table des figures

Figure 1-1 : Exemple d'un renifleur de paquets Wireshark
Figure 1-2 : exemple de balayage par Ping
Figure 1-3 : exemple du Scanneur de port NMAP
Figure 1-4 : Attaque par Trust exploitation
Figure 1-5 : Attaque par redirection de port
Figure 1-6 : Example de l'attaque Man in The Middle
Figure 1-7 : Exemple d'attaque Buffer Overflow
Figure 1-8 : Attaque de type ping of death
Figure 1-9 : Attaque de type Smurf
Figure 1-10 : attaque de type TCP SYN Flood
Figure 1-11 : la confidentialité avec le chiffrement de données
Figure 1-12 : Schéma de fonctionnement de signatures numériques
Figure 1-13 : Schématisation des pare-feux et VPN entre 2 réseaux locaux
Figure 2-1 : Placement de la sonde sur le réseau
Figure 2-2 : placement de la sonde en coupure
Figure 2-3 : placement de la sonde en recopie de port
Figure 3-1 : Exemple montrant quelques propriétés des signatures
Figure 3-2 : Les 4 niveaux de gravité d'une signature avec CCP
Figure 3-3 : La famille des IPS Cisco
Figure 3-4 : Le débit des produits Cisco IPS 4200 Series
Figure 3-5 : Caractéristiques des Supervisors Engines
Figure 3-6 : Module Cisco ASA AIP-SSM
Figure 3-7 : Caractéristiques de la gamme Cisco ASA 5500
Figure 3-8 : Les modules IPS Cisco AIM et NME
Figure 3-9 : Les composants d'un routeur
Figure 3-10 : architecture de l'IOS
Figure 4-1 : image correspond ENIEM de l'intérieur et de l'extérieur
Figure 4-2 : Organisation générale d'ENIEM
Figure 4-3 : Organigramme de l'unité prestation technique
Figure 4-4 : Architecture du réseau local ENIEM
Figure 4-5 : la gamme Cisco 3900
Figure 5-1: L'interface de travail de GNS3
Figure 5-2: Virtual Box 4.3.1.
Figure 5-3 : La surveillance d'un IPS
Figure 5-4 : description détaillée du message syslog
Figure 5-5: Interface du serveur syslog de 3CDaemon
Figure 5-6: Backtrack 5 r3
Figure 5-7: la nouvelle architecture ENIEM après l'ajout du routeur
Figure 5-8: l'architecture simplifiée du réseau sur GNS3
Figure 5-9 : interface graphique de CCP
Figure 5-10: l'interface de commandes CLI
Figure 5-11: Téléchargement des fichiers de signature
Figure 5-12: Fichier de clé de chiffrement d'IOS IPS

Figure 5-13 : Fichier de signature chargé à partir du server TFTP
Figure 5-14: Les Messages de journalisation d'alertes au niveau de serveur syslog
Figure 5-15 : Scan Null effectué par Nmap
Figure 5-16 : Résultats obtenus après l'attaque effectuée par Nmap.
Figure 5-17: Scan Null effectué par Nmap après l'activation de la signature 3040.

Remerciements

Nous remercions tout d'abord le bon Dieu de nous avoir donné la force, la volonté et la patience pour l'élaboration de notre travail.

Nous tenons à exprimer notre profonde gratitude et nos sincères remerciements à notre chère promotrice, Madame BOURKACHE qui nous a fait l'honneur de diriger ce travail et ses précieux conseils furent d'un apport considérable.

Aussi nous tenons à lui reconnaître le temps précieux qu'elle nous a consacré.

Les plus vifs remerciements partent aux membres de jury pour avoir accepté d'honorer par leur jugement de notre travail.

Nous remercions tout le personnel de l'ENIEM surtout Mr Talbi, qui nous a généreusement aidé durant notre stage.

Nos sincères sentiments vont à tous ceux qui, de prés ou de loin, ont contribué à la réalisation de ce projet. En particulier nos chères familles, nos amis et toute la section RMSE.

Introduction générale

De plus en plus les entreprises subissent des attaques qui peuvent entraîner des pertes conséquentes. Donc, le besoin en sécurité informatique est de plus en plus important.

La sécurité informatique est l'ensemble de stratégies, de mesures conçues et mises en œuvre pour détecter, prévenir et lutter contre une attaque, dans le but d'empêcher l'utilisation non autorisée et le mauvais usage d'un ensemble de connaissances, de faits, de données ou de moyens.

Les solutions de sécurité réseau émergées dans les années 1960, n'ont pas de place dans l'ensemble complet de solutions pour les réseaux modernes jusqu'aux années 2000. Comme les médecins tentent de prévenir une nouvelle maladie tout en traitant les problèmes existants, les professionnels de sécurité du réseau tentent d'empêcher les attaques potentielles, tout en minimisant les effets des attaques en temps réel.

Les défis de sécurité auxquels sont confrontés les administrateurs de réseau d'aujourd'hui ne peuvent pas être gérés avec succès par application toute seule. Bien que la mise en œuvre du contrôle d'accès et des fonctions de pare-feu sont une partie d'un réseau correctement sécurisé. Ces solutions ne peuvent toujours pas sécuriser le réseau contre les vers et les attaques d'Internet. Un réseau doit être capable de reconnaître instantanément et atténuer les vers, les virus et les menaces.

Un élément essentiel d'une bonne politique de sécurité est l'utilisation d'un système de prévention d'intrusions (IPS). Un IPS s'agit de techniques permettant de détecter les intrusions et éventuellement de les prévenir. Ces techniques sont utilisées en association avec tous les éléments d'une politique de sécurité.

L'objectif de ce mémoire est d'étudier le fonctionnement des systèmes de détection et de prévention d'intrusions en générale, ensuite on choisi la solution IPS convenable, à l'entreprise ENIEM, parmi ceux qui existes sur le marché de Cisco Systems, enfin on met en œuvre cette solution et on la teste avec le simulateur GNS3.

Toute cette étude sera présentée dans les cinq chapitres suivants :

Chapitre 1 : Généralités sur la sécurité informatique

Dans ce chapitre nous allons expliquer les risques informatiques que les entreprises reçoivent depuis longtemps en indiquant les types d'attaques et les techniques utilisées qui montrent comment les pirates arrivent à accéder aux réseaux, aux systèmes et aux informations confidentielles et faire des dégâts avec. Puis nous allons voir comment se défendre contre ces attaques et les mécanismes de sécurité existants pour protéger nos informations.

Chapitre 2 : les systèmes de détection et prévention d'intrusions

Ici nous présentons les principes et les approches de détection d'intrusions en détail pour comprendre la base de fonctionnement de ces systèmes, les types d'IDS et IPS et la différence entre eux.

Chapitre 3 : les solutions IPS de Cisco Systems

Où nous mettons l'accent sur les solutions IPS que propose Cisco Systems dans son matériel et leurs caractéristiques.

Chapitre 4 : présentation de l'organisme d'accueil ENIEM

Dans ce chapitre nous présentons l'organisme d'accueil, ses missions, ces objectifs, ses moyens financiers et humains etc. Nous étudions aussi l'architecture de son réseau local, le matériel et les logiciels utilisés, nous retirons quelques anomalies dans son système de sécurité, puis nous présentons le choix de la solution IOS IPS Cisco adaptées.

Chapitre 5 : implémentation

Dans ce chapitre nous allons faire une implémentation de notre solution IOS IPS Cisco, en la simulant avec l'émulateur GNS3 pour la tester et voir son fonctionnement.

Et on termine avec une conclusion générale sur le travail

CHAPITRE 1:

Généralités sur la sécurité informatique

Introduction

Dans ce chapitre nous allons expliquer les risques informatiques que les entreprises reçoivent depuis longtemps en indiquant les types d'attaques et les techniques utilisées qui montrent comment les pirates arrivent à accéder aux réseaux, aux systèmes et aux informations confidentielles et faire des dégâts avec. Puis nous allons voir comment se défendre contre ces attaques et les mécanismes de sécurité existants pour protéger nos informations.

On a déjà connue plusieurs attaques de plus au moins graves, on cite quelques-unes : [16]

SQL Slammer en 2003 : est un ver informatique qui a provoqué le 25 janvier 2003 un déni de service sur certains ordinateurs hôtes d'Internet et un ralentissement grave du trafic Internet.

Estonie - 2007 : La première cyberattaque recensée visant une structure étatique durant plusieurs semaines, et causer un déni de service prolongé, a émané de sites russes contre des sites de l'administration estonienne, ainsi que ceux de banques et de journaux de ce pays.

Géorgie 2008 : la Russie lance une invasion militaire classique, mais juste auparavant de vastes cyberattaques mettent à genou toutes les infrastructures du pays.

Stuxnet et Flame 20010-2011 : sont deux vers supposés développés conjointement par les États-Unis et Israël pour s'attaquer à des systèmes nucléaires iraniens.

I.1) *Concepts de base :*

- ✓ **Une intrusion** : opération qui consiste à accéder sans autorisation, aux données d'un système informatique ou d'un réseau, en contournant ou en désamorçant les dispositifs de sécurité mis en place. Elle peut causer des dégâts divers (vol ou la modification des données confidentielles, contaminer ou détruire les données du système)
- ✓ **Une menace :** est un événement ou action susceptible de violer la sécurité d'un système informatique.
- ✓ **Vulnérabilité des systèmes informatiques :** défaut ou faiblesse dans la conception d'un système, son implémentation, fonctionnement ou administration et qui peut être exploité pour violer la politique de sécurité.
- ✓ **Une attaque [18] :**c'est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système.
- ✓ **hacker [19]:** En général, les hackers sont des individus qui possèdent un niveau très avancé en informatique, et ce sont également des personnes avides de connaissances, qui désirent tout comprendre sur le mécanisme de fonctionnement d'un système informatique, ce dernier s'appelle pirate informatique, afin d'en localiser les failles de sécurité et les exploiter à son avantage.

I.2) *Les enjeux de la sécurité informatique:*

La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. Elle doit maitriser les enjeux suivants :

- **La confidentialité :** La confidentialité consiste à assurer qu'une information ne doit être lue que par les personnes aux quelle est transmise.

- **L'intégrité [1] :** L'intégrité consiste à assurer la conformité de l'information, elle permet aux utilisateurs d'avoir la certitude que l'information est correcte et qu'elle n'a pas été modifiée par un individu non autorisé.

- **Disponibilité (système et données) [2] :** Les utilisateurs autorisés doivent avoir un accès ininterrompu aux importantes ressources et des données. Elle couvre aussi les systèmes de communications qui transmettent les informations entre sites et entre systèmes.

- **Authentification [16]** :C'est la vérification de l'identité des utilisateurs qui est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.

- **Non-répudiation [2]**: les acteurs impliqués dans la communication ne peuvent nier y avoir participé.

I.3) *Les différentes étapes d'une attaque [7]*

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma :
Identification de la cible : cette étape est indispensable à toute attaque 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'utilisation des bases Whois, l'interrogation des serveurs DNS,….

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 (OS, versions des services, subnet, 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 (ou system) 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 ,…).

I.4) *Les types d'attaques:* [12]

Pour atténuer les attaques, il est utile de les classer et de les traiter en différents types plutôt qu'individuellement. Il n'y a pas de manière standardisée pour les catégoriser. On a utilisé la méthode qui les classe en trois grandes catégories :

I.4.1) Les attaques virales

Il existe une grande variété de virus. On peut cependant définir un virus comme un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs.

Les dégâts causés vont du simple programme qui affiche un message à l'écran au programme qui formate le disque dur après s'être multiplié. On ne classe cependant pas les virus d'après leurs dégâts mais selon leur mode de propagation et de multiplication :

- Les vers capables de se propager dans le réseau;
- Les « chevaux de Troie » créant des failles dans un système;
- Les bombes logiques se lançant suite à un événement du système;
- Les canulars envoyés par mail.

I.4.2) Les attaques de reconnaissance

Attaques de reconnaissance impliquent la découverte non autorisée et la cartographie des systèmes, des services, ou vulnérabilités. Attaques de reconnaissance emploient souvent l'utilisation de renifleurs de paquets, balayeurs de ping et les scanners de ports, qui sont largement disponibles en téléchargement gratuit sur Internet.

I.4.2.1) Packet Sniffer (Renifleurs de paquets)

Packet Sniffer est un logiciel qui utilise la carte réseau en mode proximité pour capturer tous les paquets qui sont envoyés à travers un réseau local. Mode de proximité est un mode dans lequel la carte réseau envoie tous les paquets qui sont reçus à une demande de traitement. Certaines applications de réseau distribuent les paquets réseau en clair non chiffré. Parce que les paquets de réseau ne sont pas chiffrés, ils peuvent être compris par toute application qui peut les cueillir du réseau et les traiter. De nombreux renifleurs de paquets freeware et shareware, comme Wireshark, sont disponibles.

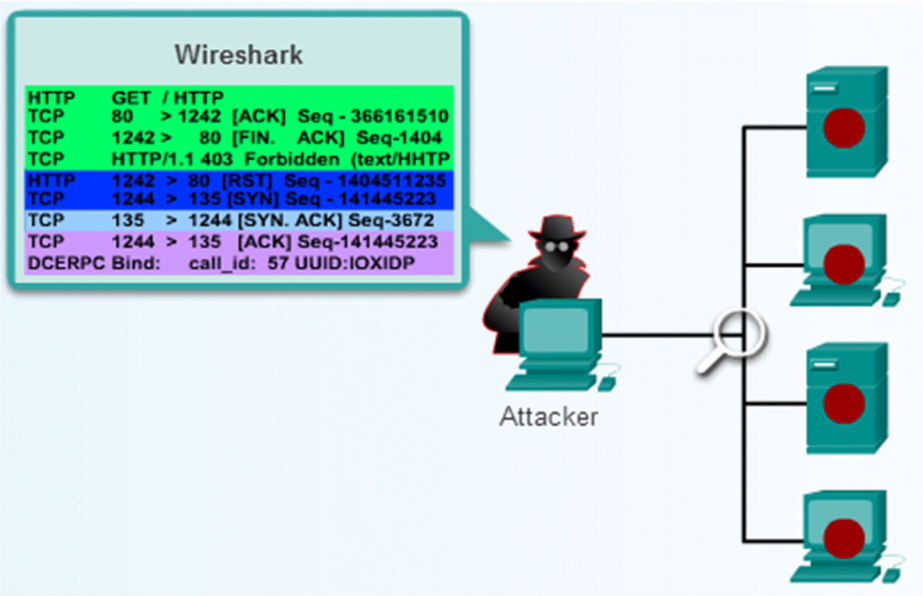

Figure 1-1 : Exemple d'un renifleur de paquets Wireshark

I.4.2.2) Balayage par Ping

Un balayage de ping est une technique de base pour le scan de réseau qui détermine les adresses IP des cartes des hôtes connectés. Un seul ping indique si un ordinateur hôte spécifié existe sur le réseau. Un balayage de ping se compose de demandes d'écho ICMP envoyés à plusieurs hôtes. Si une adresse donnée est en direct, l'adresse renvoie un ICMP réponse d'écho. Balayages par ping sont parmi les méthodes les plus anciennes et plus lentes utilisés pour numériser un réseau.

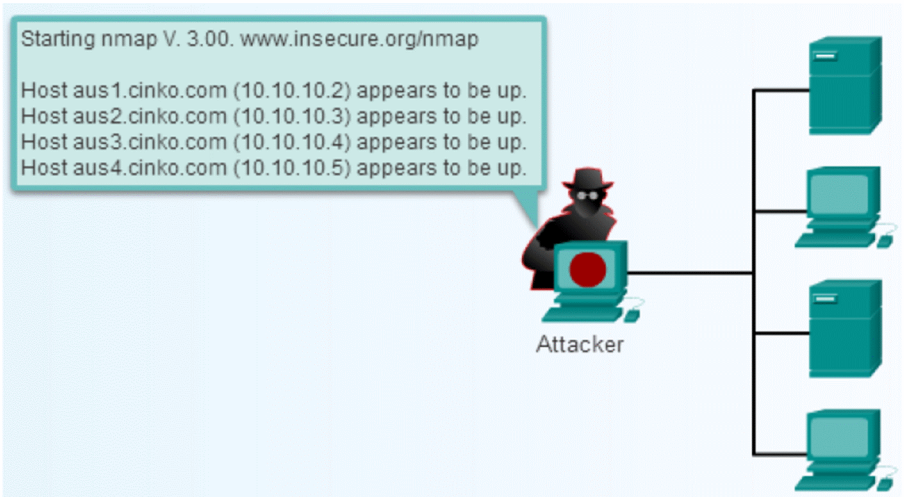

Figure 1-2 : exemple de balayage par Ping

I.4.2.3) Port scanning (Scanneur de port)

Chaque service sur un ordinateur hôte est associé à un numéro de port bien connu. Le balayage de ports est un balayage d'une série de TCP ou numéros de ports UDP sur un hôte pour détecter les services d'écoute. Elle consiste à envoyer un message à chacun des ports sur un hôte. La réaction que l'expéditeur reçoit indique si le port est utilisé.

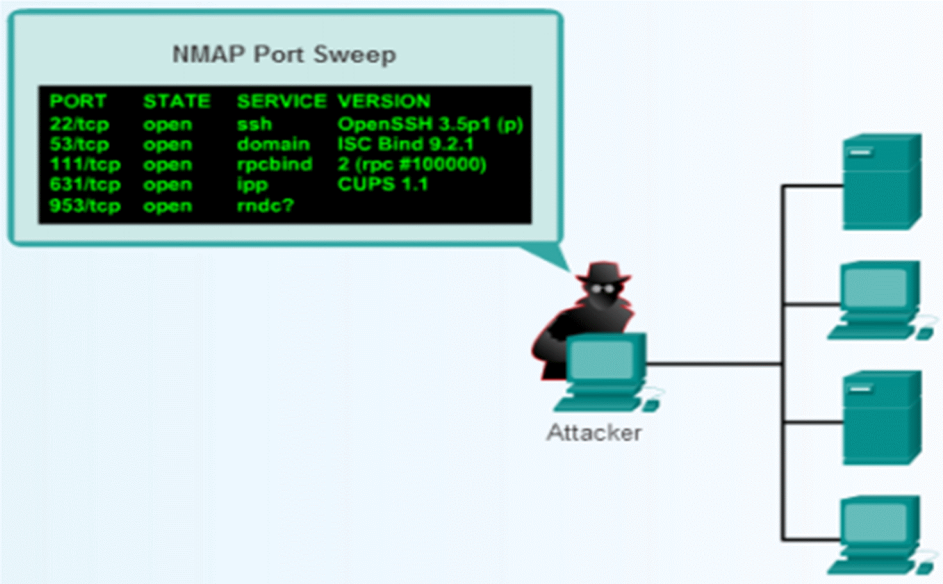

Figure 1-3 : exemple du Scanneur de port NMAP

I.4.2.4) L'ingénierie sociale

L'ingénierie sociale (social engineering en anglais) n'est pas vraiment une attaque informatique, c'est plutôt une méthode pour obtenir des informations sur un système ou des mots de passe.
Elle consiste surtout à se faire passer pour quelqu'un (en général un des administrateurs du serveur que l'on veut pirater) et de demander des informations personnelles (login, mots de passe, accès, numéros, données…) en inventant un quelconque motif (plantage du réseau, modification de celui-ci…). Elle se fait soit au moyen d'une simple communication téléphonique ou par courriel.

I.4.3) Les attaques d'accès

Attaques d'accès exploitent les vulnérabilités connues dans les services d'authentification, les services FTP, et des services Web à gagner l'entrée à des comptes Internet, bases de données confidentielles et d'autres informations sensibles. Une attaque d'accès peut être effectuée de nombreuses manières différentes.

I.4.3.1) Le craquage de mots de passe

Le craquage consiste à faire de nombreux essais jusqu'à trouver le bon mot de passe.

Il existe deux grandes méthodes :

- **L'utilisation de dictionnaires :** le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci (à l'envers, avec un chiffre à la fin…). Les dictionnaires actuels contiennent dans les 50 000 mots et sont capables de faire une grande partie des variantes.

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

I.4.3.2) Trust exploitation (exploitation fiducie)

Un attaquant utilise les privilèges accordés à un système d'une manière non autorisée, conduisant éventuellement à compromettre la cible.

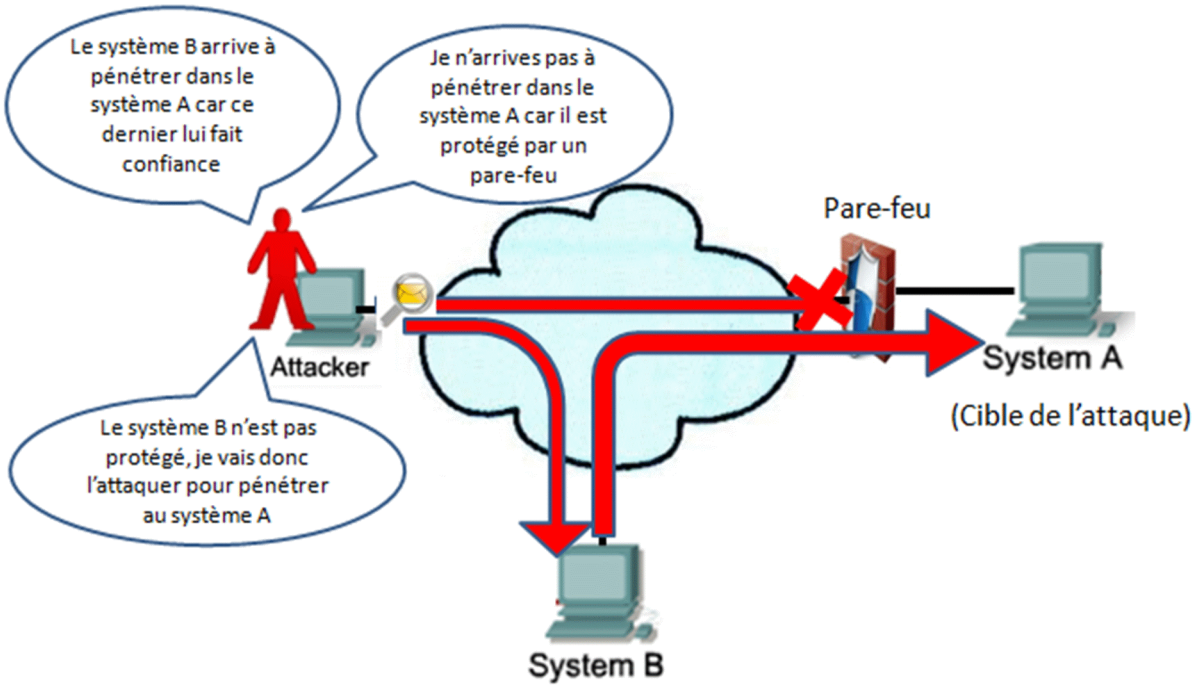

Figure 1-4 : Attaque par Trust exploitation

I.4.3.3) Redirection de Port

Un système compromis est utilisé comme un point jump-off pour des attaques contre d'autres cibles. Un type de Trust- exploitation qui utilise un hôte compromis comme un point jump-off pour des attaques contre d'autres cibles. Une intrusion est installée sur le système compromis pour la redirection de session. Elle le fait dans le but de transmettre du trafic via un pare-feu qui, autrement, serait supprimée.

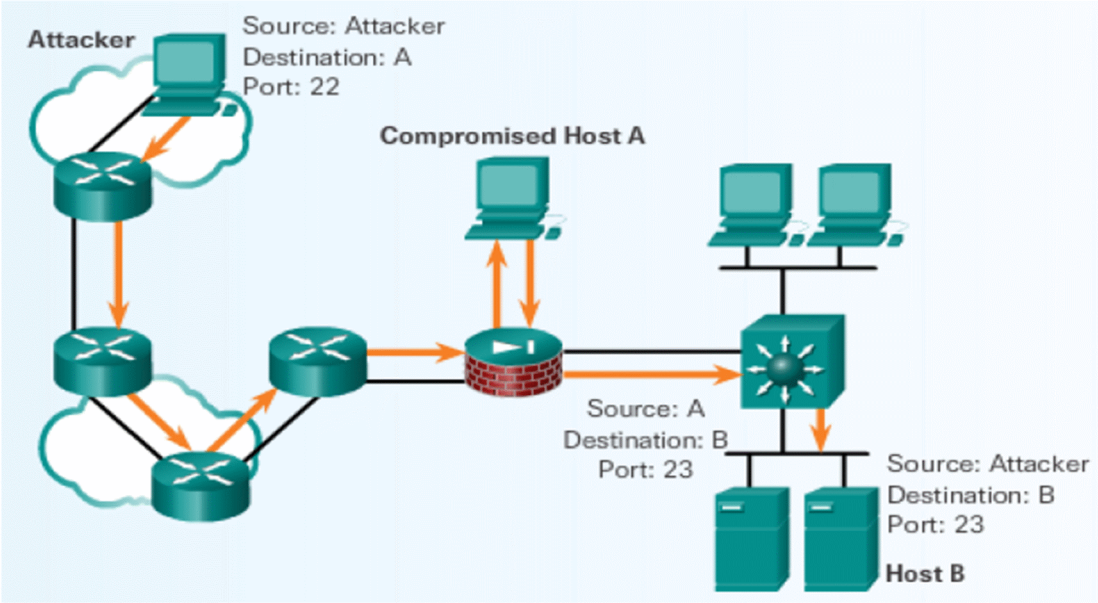

Figure 1-5 : Attaque par redirection de port

I.4.3.4) Attaque Man-in-the-middle

Un attaquant est positionné dans le milieu des communications entre les deux entités légitimes pour lire ou modifier les données qui passe entre les deux parties. Une attaque populaire man-in-the-middle implique un ordinateur portable agissant comme un point d'accès wifi ou passerelle pour centraliser les communications à son niveau. La victime peut se connecter et utiliser normalement le réseau sans savoir que le flux passe par une tiers personne.

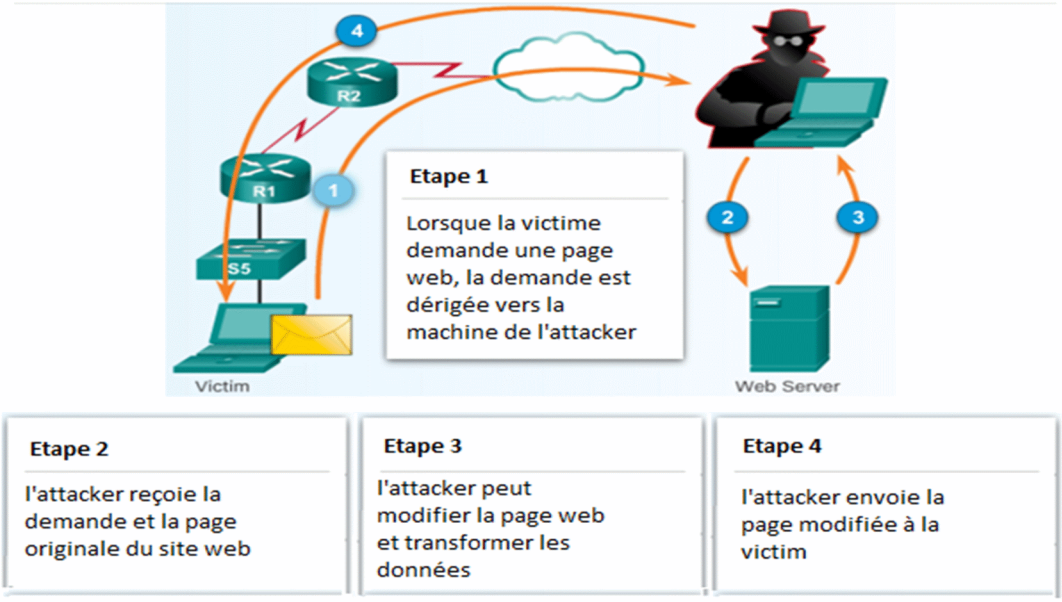

Figure 1-6: Example de l'attaque Man in The Middle

I.4.3.5) Buffer Overflow (débordement de tampon)

Un programme écrit des données au-delà de la mémoire tampon allouée. Les dépassements de tampon généralement se posent comme une conséquence d'un bug dans un programme C ou C++. L'intrus injecte plus de données dans le buffer de l'application que ce qui a été prévu dans le but de le saturer et d'arriver à l'adresse de retour. Ensuite, l'intrus écrase l'adresse de retour dans le but de se brancher vers un programme malicieux.

Figure 1-7 : Exemple d'attaque Buffer Overflow

Dans cet exemple, un attaquant exploite une faiblesse dans une application en soumettant une extra-longue entrée au programme, la création d'un débordement de tampon. Le trop-plein peut être utilisé pour modifier les valeurs des variables du programme et causer un saut à des endroits inattendus, ou même remplacer les instructions de programme valides avec un autre code.

I.4.3.6) Porte dérobée (backdoors)

Lorsqu'un pirate informatique arrive à accéder à un serveur à l'aide d'une des techniques présentées dans cette section, il souhaiterait y retourner sans avoir à tout recommencer. Pour cela, il laisse donc des portes dérobées qui lui permettront de reprendre facilement le contrôle du système informatique.
Il existe différents types de portes dérobées :

- Création d'un nouveau compte administrateur avec un mot de passe choisi par le pirate.
- Création de compte ftp
- Modification des règles du pare-feu pour qu'il accepte des connections externes.

Dans tous les cas, l'administrateur perd le contrôle total du système informatique. Le pirate peut alors récupérer les données qu'il souhaite, voler des mots de passe ou même détruire des données.

I.4.4) Les attaques DOS et DDoS

Une attaque de déni de service produit l'interruption d'un service ou son ralentissement, deux méthodes peuvent produire un déni de services :

- ✓ générer un grand volume de trafic en le faisant passer pour un trafic légitime. Ce trafic sature le réseau et empêche le trafic normal de passer
- ✓ Générer un trafic mal formé produisant un comportement erroné des applications

Une attaque de déni de service distribuée (DDOS) est une attaque de déni de service produite par plusieurs sources coordonnées entre elles.

Trois attaques DoS communes comprennent:

I.4.4.1) Ping of Death (Ping de la mort)

Cette attaque exploite les anciennes implémentations de TCP/IP de certains systèmes d'exploitation. L'intrus envoie un paquet IP d'une taille supérieure à la normale (> 65535 Octet). La pile TCP/IP n'ayant pas prévu un tel paquet, elle se comportera d'une manière anormale induisant le dysfonctionnement du réseau.

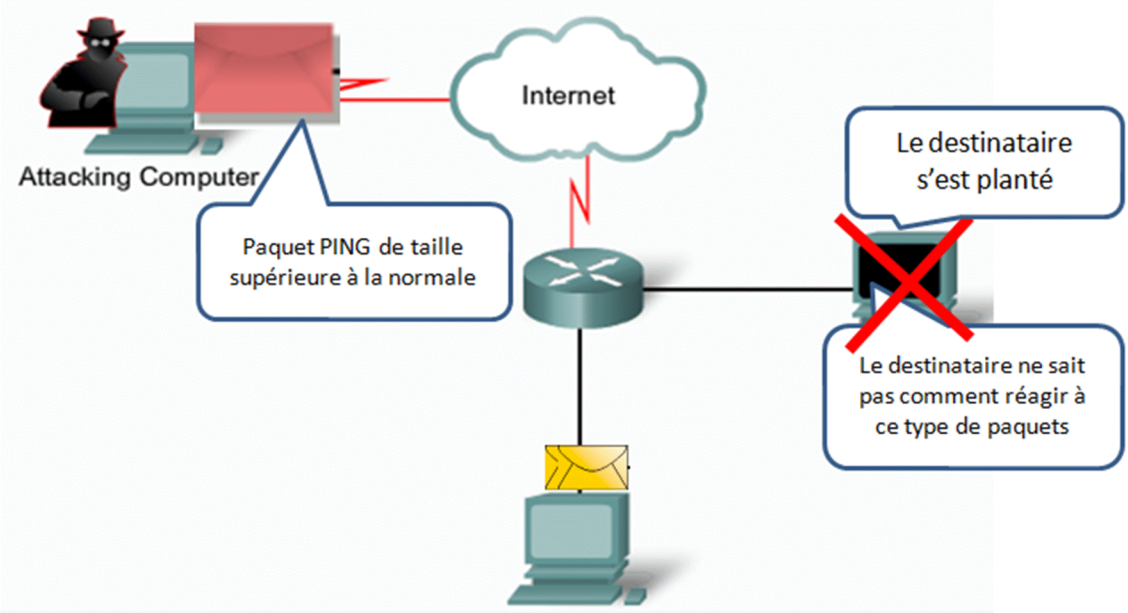

Figure 1-8: Attaque de type ping of death

I.4.4.2) Smurf

L'intrus inonde la victime par un grand nombre de Ping pour le saturer. La technique la plus utilisée s'exécute en deux phases :

- ✓ Dans la première phase, l'intrus usurpe l'adresse IP de la cible pour l'utiliser comme adresse source
- ✓ Dans la deuxième phase, l'intrus envoie un maximum de Ping en diffusion directe à destination d'un réseau contenant un grand nombre d'hôtes. L'adresse source étant transformée en l'adresse de la victime

Si le routeur d'entrée accepte de faire passer les diffusions directes, tous les hôtes du réseau vont répondre à l'adresse source qui est l'adresse de la victime. La victime est saturée.

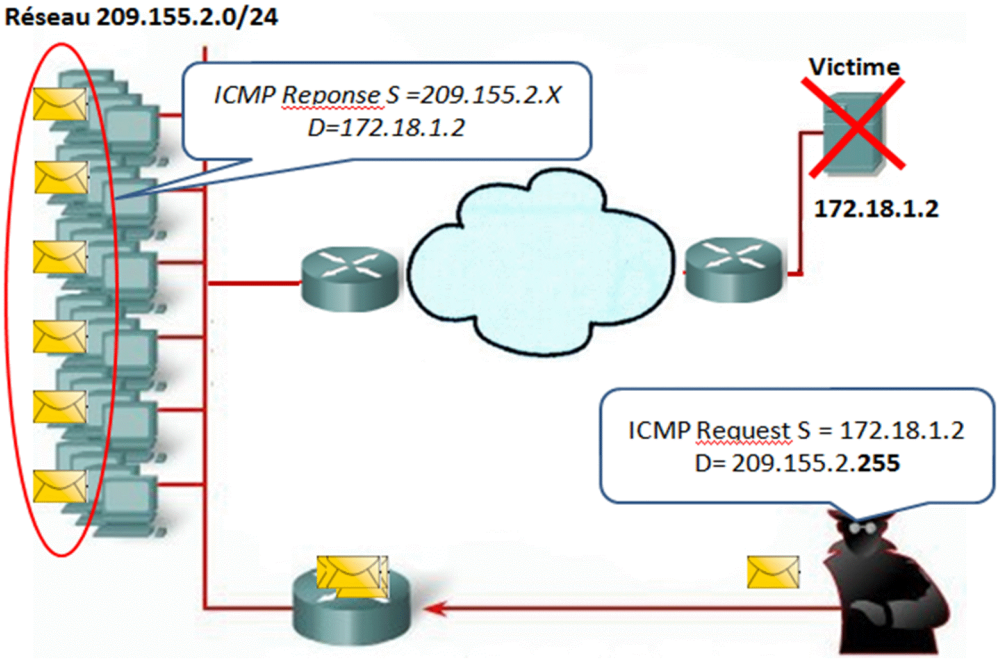

Figure 1-9 : Attaque de type Smurf

I.4.4.3) TCP SYN Flood

L'intrus inonde la victime par un grand nombre TCP SYN pour lui faire croire qu'une demande de connexion est arrivée. L'intrus utilise une fausse adresse de retour pour ne pas recevoir les réponses de la victime. La victime répond par un paquet SYN ACK et se met en attente d'un paquet ACK de l'intrus. Chaque demande est mise dans une file d'attente en attendant que l'ACK correspondant arrive. Les réponses étant destinées à une fausse adresse, la victime ne recevra jamais de paquet ACK et la file est vite débordée. Ayant la file débordée, la victime ne pourra plus répondre à une demande légitime de connexion.

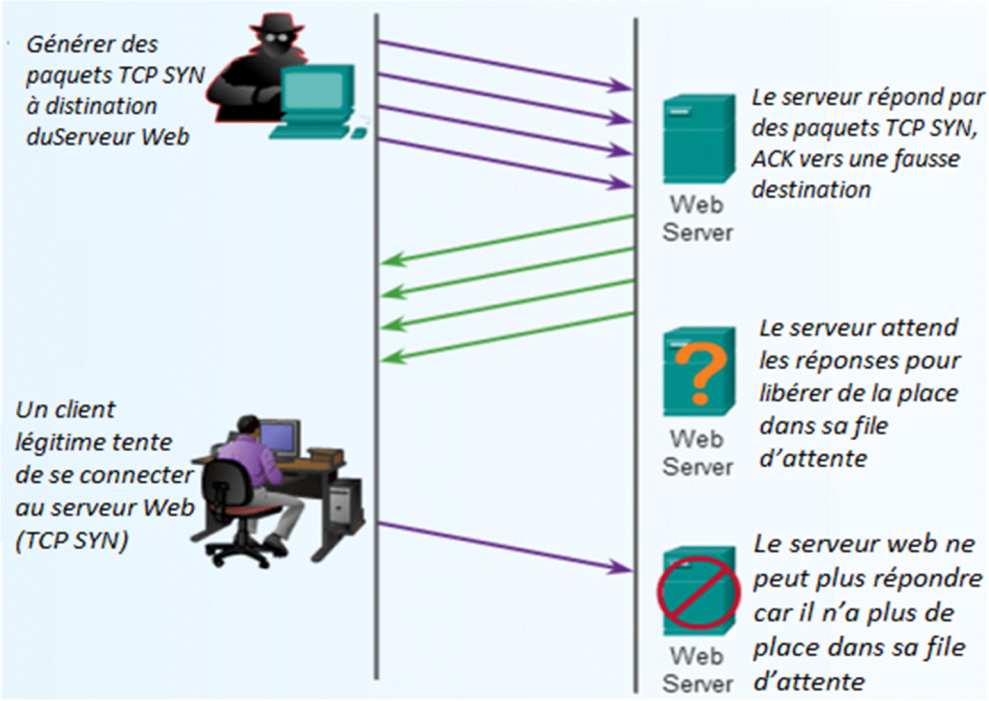

Figure 1-10 : attaque de type TCP SYN Flood

I.5) *Les mécanismes de défense :*

I.5.1) Les mots de passe [16]:

Un mot de passe est un moyen d'authentification pour utiliser une ressource ou un service dont l'accès est limité et protégé. Il doit être tenu secret pour éviter qu'un tiers non autorisé puisse accéder à la ressource ou au service.

La qualité et la longueur du mot de passe sont des éléments cruciaux pour la sécurité. Un mot de passe trop court ou provenant d'un dictionnaire est susceptible d'être attaqué via une recherche dans une table contenant une liste de mots de passe. D'une manière plus systématique, une attaque par force brute tente toutes les possibilités et, avec suffisamment de temps, il est théoriquement possible de retrouver le mot de passe.

La robustesse d'un mot de passe dépend de plusieurs critères :

- **Sa simplicité** : 123456, 111111, Love, 0000, azerty... sont à proscrire, de même que les dates de naissance, le nom du chien...
- **Sa longueur**. Il est conseillé d'utiliser des mots de passe de plus de dix caractères.
- **Le nombre de types de caractères différents**. Il est conseillé de mélanger des majuscules, des minuscules, des chiffres et des caractères spéciaux.
- **Sa durée de vie.** Un mot de passe est d'autant plus robuste qu'il est changé régulièrement (par exemple, tous les six mois).

I.5.2) La cryptographie : [16]

Par un sniffing, ou un autre procédé de détournement de paquets, on peut lire en clair le contenu de ces derniers. Par un spoofing, on peut falsifier son identité, et (ré)-émettre des messages ou copies de messages déjà émis à la place de quelqu'un. Ainsi, des technologies de cryptographie ont été établies pour contourner les risques.

La cryptographie représente la science qui permet de rendre un texte clair en un texte chiffré. La personne qui pratique cette science est appelée Cryptographe. Le processus de transformer un message en clair en un message illisible est appelé cryptage ou chiffrement. L'opération inverse est appelée décryptage ou déchiffrement.

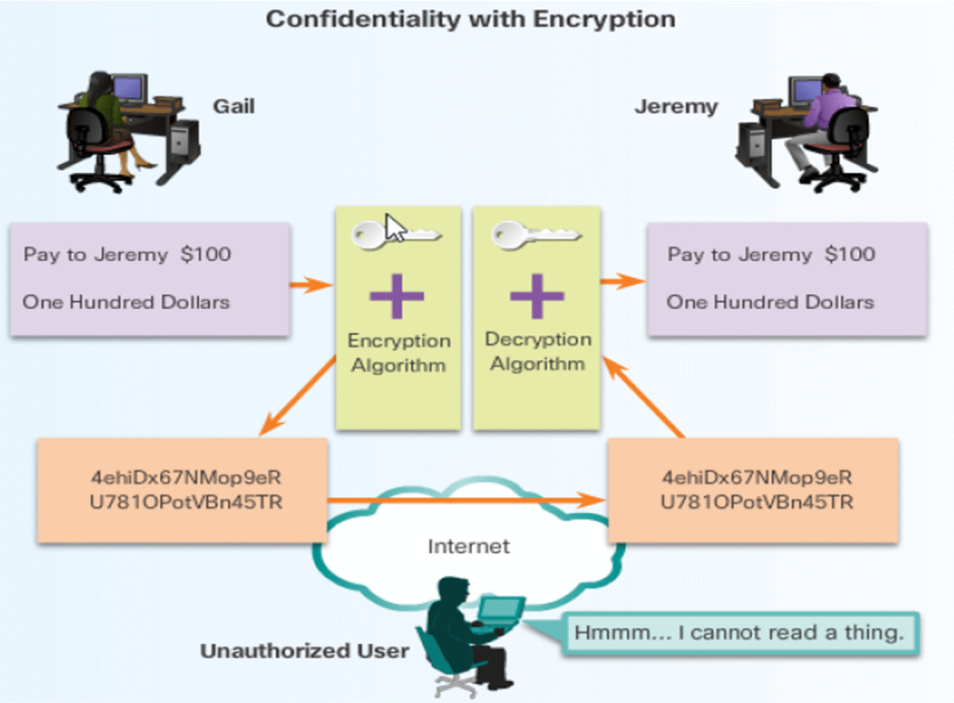

Figure 1-11 : la confidentialité avec le chiffrement de données

Quelques techniques de cryptographie :

- **Algorithmes de chiffrement faibles (facilement cassables)**

Les premiers algorithmes utilisés pour le chiffrement d'une information étaient assez rudimentaires dans leur ensemble. Ils consistaient notamment au remplacement de caractères par d'autres. La confidentialité de l'algorithme de chiffrement était donc la pierre angulaire de ce système pour éviter un décryptage rapide.

Exemples d'algorithmes de chiffrement faibles :

- **ROT13** (rotation de 13 caractères, sans clé) ;
- **Chiffre de César** (décalage de trois lettres dans l'alphabet sur la gauche).
- **Chiffre de Vigenère** (introduit la notion de clé)

- **Algorithmes de cryptographie symétrique (à clé secrète) :**

Les algorithmes de chiffrement symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message. L'un des problèmes de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre. La mise en œuvre peut s'avérer difficile, surtout avec un grand nombre de correspondants car il faut autant de clés que de correspondants.

Quelques algorithmes de chiffrement symétrique très utilisés : Chiffre de Vernam, DES, 3DES, AES, RC4, RC5 et MISTY1

- **Algorithmes de cryptographie asymétrique (à clé publique et privée)**

Pour résoudre le problème de l'échange de clés, la cryptographie asymétrique a été mise au point dans les années 1970. Elle se base sur le principe de deux clés :

- une publique, permettant le chiffrement
- une privée, permettant le déchiffrement

Comme son nom l'indique, la clé publique est mise à la disposition de quiconque désire chiffrer un message. Ce dernier ne pourra être déchiffré qu'avec la clé privée, qui doit rester confidentielle.

Quelques algorithmes de cryptographie asymétrique très utilisés : RSA (chiffrement et signature), DSA (signature) et Protocole d'échange de clés Diffie-Hellman (échange de clé).

Le principal inconvénient de RSA et des autres algorithmes à clés publiques est leur grande lenteur par rapport aux algorithmes à clés secrètes. RSA est par exemple 1000 fois plus lent que DES. En pratique, dans le cadre de la confidentialité, on s'en sert pour chiffrer un nombre aléatoire qui sert ensuite de clé secrète pour un algorithme de chiffrement symétrique.

- **Signature numérique :**

La signature numérique est un mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité, par analogie avec la signature manuscrite d'un document papier. Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de nombres. La signature électronique n'est devenue possible qu'avec la cryptographie asymétrique.

Fonctionnement de la signature numérique :

Le principe se repose sur le chiffrement par l'émetteur d'un condensat généré par un algorithme de hachage tel que MD5 ou SHA-1. Il utilisera pour cela sa clé privée. Le message et la signature sont ensuite envoyés au destinataire qui déchiffrera la signature avec la clé publique de l'émetteur. Le condensat obtenu est comparé avec le condensat généré par le destinataire à partir du même message. S'ils sont identiques, le message est authentifié.

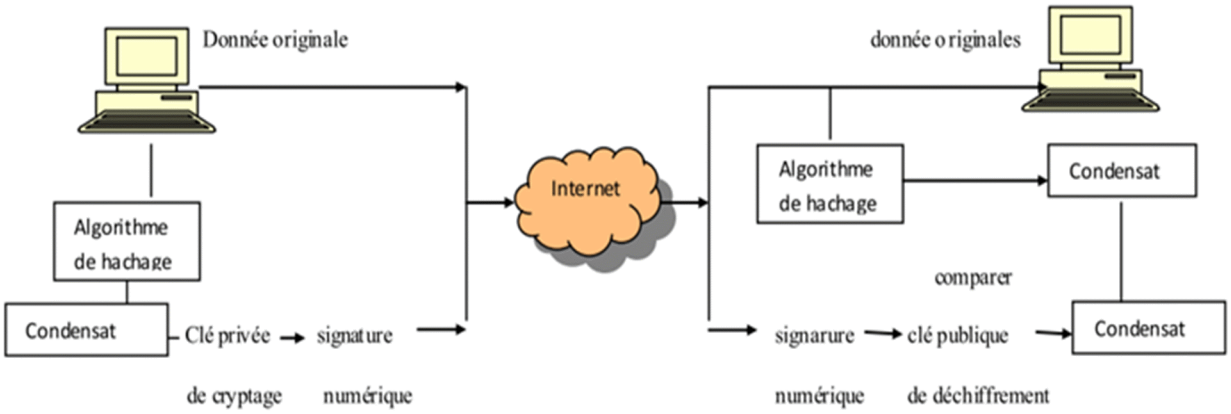

Figure 1-12 : Schéma de fonctionnement de signatures numériques

- **Certificat numérique : [4]**

Dans un environnement de clé publique, il est essentiel de s'assurer que la clé publique avec laquelle on chiffre les données est celle du destinataire concerné et non une contrefaçon.

Un certificat numérique est une information attachée à une clé publique, et qui permet de vérifier que cette clé est authentique, ou valide. Les certificats numériques sont utilisés pour contrecarrer les tentatives de substituer une clé falsifiée à la clé véritable.

Un certificat numérique comporte trois éléments :
- Une clé publique.
- Une information de certification (''l'identité'' de l'utilisateur, comme son nom, son adresse e-mail, etc.)
- Une ou plusieurs signatures numériques.

I.5.3) Les Antivirus [12]:

Le principal moyen d'atténuer les attaques de virus et de chevaux de Troie est un logiciel antivirus. Il aide à prévenir les hôtes de l'infection et la propagation du code malveillant. Il nécessite beaucoup plus de temps à nettoyer des ordinateurs infectés qu'il le fait pour maintenir la mise à jour de l'antivirus.
Un logiciel antivirus est le produit de sécurité le plus largement déployée sur le marché aujourd'hui. Plusieurs sociétés créent des logiciels antivirus, tels que Symantec, Computer Associates, McAfee et Trend Micro.

I.5.4) Les pare-feux (firewalls) [20]:

Un firewall permet de protéger un réseau informatique des intrusions indésirables en filtrant les communications autorisées ou non entre deux réseaux informatiques (généralement dans un contexte d'un réseau privé et le réseau Internet).

Un pare-feu se présente essentiellement sous deux formes :

- **Logicielle :** un programme qui fonctionne dans votre ordinateur personnel ou de bureau et assure le rôle de filtrage des connexions. Un pare-feu logiciel doit être installé dans chaque ordinateur ;
- **Matérielle :** un composant physique de votre réseau domestique qui inclut un logiciel de pare-feu. Un pare-feu matériel doit être présent une seule fois dans un réseau informatique – au passage entre un réseau privé et un réseau public.

I.5.5) VPN (Virtual Private Network)

Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Avec le développement d'Internet, il est intéressant de permettre ce processus de transfert de données sécurisé et fiable. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées.

Le principe du VPN est basé sur la technique du tunnelling. Cela consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Ensuite la source chiffre les données et les achemine en empruntant ce chemin virtuel.

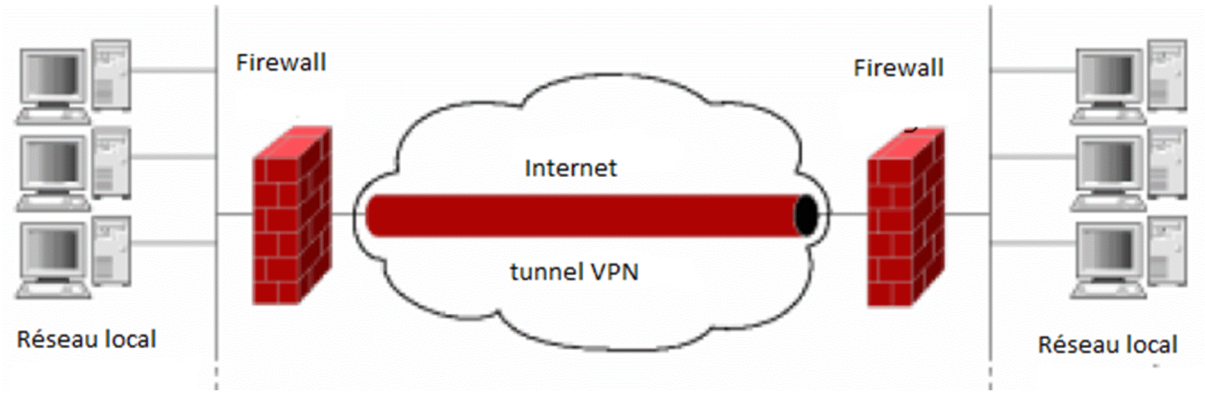

Figure 1-13 : Schématisation des pare-feux et VPN entre 2 réseaux locaux

I.5.6) Présentation générale des IDS et IPS [7]

Nous appelons un IDS (Intrusion Détection System) un mécanisme permettant d'écouter le trafic réseau et de contrôler les activités réseau afin de repérer toutes activités anormales ou suspectes et ainsi remonter des alertes sur les tentatives d'intrusion à un système informatique. Quant à l'IPS (Intrusion Prévention System), il gère les mêmes tâches qu'un IDS, sauf qu'il mène des actions pour la protection du système informatique contre les risques intrusifs.

Un IDS est constitué essentiellement d'un sniffer couplé avec un moteur qui analyse du trafic selon des règles. Ces règles donnent une description des caractéristiques des trafics réseau à signaler. Ainsi un IDS remplit des fonctionnalités de contrôle réseau et réagit selon la nature du trafic.

Notons qu'un IDS ne remplace, en aucun cas, un pare-feu ou tout autre mécanisme de sécurisation des systèmes d'information. Cependant il renforce la sécurité en ajoutant une couche de sécurité et permettant ainsi la mise en place d'une défense en profondeur sur l'architecture réseau.

Conclusion

Cette étude nous a permis de découvrir les techniques d'attaques aux systèmes informatiques et les dégâts provoqués dans l'histoire aux internautes, surtout aux entreprises. D'où, l'indispensabilité de la sécurité informatique dans les entreprises afin d'assurer leur fonctionnement normal.

Ensuite nous avons vu quelques solutions logicielles et matérielles existantes pour se défendre contre ces attaques, leurs principes de fonctionnements et leurs limites de sécurité.

Puisque notre thème est limité sur le système de détection et de prévention d'intrusions, dans le chapitre qui suit nous allons faire une étude plus détaillée sur ce dernier afin de comprendre son intérêt dans la sécurité des entreprises, ses bases de fonctionnement et son implémentation dans les entreprises et les réseaux en générale.

CHAPITRE 2:

Les systèmes de détection et prévention d'intrusions

Introduction

Les entreprises commencent à prendre conscience de l'importance de la sécurité informatique et intègrent des mécanismes de sécurité dans leurs architectures réseaux. De plus la mise en place d'une politique de sécurité informatique autour de ces systèmes d'information et détecter d'éventuelles intrusions devient une nécessité pour estimer la complétude de cette politique de sécurité.

Dans ce chapitre nous allons faire une étude détaillée sur les systèmes de détection et prévention d'intrusions, dans le but de comprendre la différence entre eux, leurs fonctionnement de base, les techniques utilisées pour la détection des intrusions, leurs avantage et inconvénients et leurs limites de sécurité.

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

II.1.1) Présentation:[6]

Les IDS, ou systèmes de détection d'intrusions, sont des systèmes software ou hardware conçus afin de pouvoir automatiser le processus d'analyse des événements survenant dans un réseau ou sur une machine particulière, et de pouvoir signaler à l'administrateur système, toute trace d'activité anormale sur ce dernier ou sur la machine surveillée. L'IDS est un système de détection passif. L'administrateur décidera ou non de bloquer cette activité.

II.1.2) Principe de détection d'intrusion

La détection d'intrusion se repose sur deux approches de base qui sont :

- ✓ Approche par scénarios
- ✓ Approche comportementale.

II.1.2.1) APPROCHE PAR SCENARIOS [6]

Cette méthode se base sur la connaissance des techniques utilisées par les attaquants Pour déduire des scénarios typiques. Elle ne tient pas en compte des actions passées de l'utilisateur et utilise des signatures d'attaques connues (ensemble de caractéristiques Permettant d'identifier une activité intrusive : une chaine alphanumérique, une taille de paquet inhabituelle, une trame formatée de manière suspecte,…).

On va présenter ici quelques cas typiques de détection utilisant cette approche :

II.1.2.1.1) Analyse de motif :

Cette méthode se base sur la recherche de motifs (chaines de caractères ou suite d'octets) au sein du flux de données. L'IDS comporte une base de signature où chaque signature contient les protocoles et ports utilisés par l'attaque ainsi que le motif qui permettra de reconnaitre les paquets suspects.

II.1.2.1.2) Recherches génériques :

Adaptée pour les virus. On regarde dans le code exécutable les commandes qui sont potentiellement dangereuses. Par exemple, une commande DOS non référencée est détectée, des émissions de mails, des instructions liées à des attaques connues.

II.1.2.1.3) Contrôle d'intégrité :

Cette méthode permet d'effectue une photo de tous les fichiers d'un système .Il génère une alerte en cas d'altération de l'un des fichiers.

- ✓ **Avantages et inconvénients de l'approche par scénario :**

  - **Avantages :**

- Reconnaissance des attaques sans générer trop de fausses alarmes (faux positifs).
- Capable de diagnostiquer rapidement l'utilisation d'une technique d'attaque ou d'un outil d'attaque spécifique.
- Possibilité d'aider les administrateurs systèmes (moyennant leur niveau d'expertise) à traquer un problème de sécurité en initiant des procédures de gestions d'incidents.

  - **Inconvénients :**

- Impossibilité de détecter des attaques non connues, et donc nécessité de mettre à jour régulièrement la base de signature.
- Une attaque n'est pas toujours identique à 100% à sa signature, le moindre octet différent provoquera la non détection de l'attaque.

II.1.2.2) APPROCHE COMPORTEMENTALE [8]

La détection d'anomalies consiste à définir, dans une première phase, un certain comportement du système, des utilisateurs, des applications, etc. considéré comme «normal» ; dans une seconde phase, on observe l'entité ainsi modélisée et tout écart par rapport au comportement de référence est signalé comme étant suspect.
Cette approche recouvre en fait deux problèmes distincts : la définition du comportement « normal » (souvent appelé profil) d'une part, et la spécification des critères permettant d'évaluer le comportement observé par rapport à ce profil d'autres part. Les différentes approches de détection d'anomalies se distinguent essentiellement par le choix des entités modélisées dans le profil et l'interprétation qui est faite des divergences par rapport à ce profil.
On va présenter ici quelques cas typiques de détection utilisant cette approche :

II.1.2.2.1) Approche probabiliste

Cette méthode consiste à établir des probabilités 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.

II.1.2.2.2) Approche statistique

L'approche la plus fréquemment utilisée pour la génération d'un modèle de comportement normal d'un utilisateur ou d'un système est une approche statistique. Elle consiste à utiliser des mesures statistiques pour modéliser un profil de comportement et détecter des comportements intrusifs. Ces mesures peuvent être par exemple :

- le temps CPU utilisé,
- le nombre de connexions durant une certaine période de temps,
- les fichiers les plus fréquemment utilisés
- les entrées/sorties utilisées,

Chacune de ces valeurs est associée à un seuil ou à un intervalle de valeurs, dans lequel une activité est considérée comme normale. Tout dépassement de seuil ou situation de valeurs à l'extérieur des bornes de l'intervalle indique une activité anormale.

II.1.2.2.1) Réseaux de neurones

Une troisième technique vise plus particulièrement à contrôler le comportement des utilisateurs du système. L'objectif est de protéger le système des attaques dont ils pourraient être les auteurs, mais surtout de vérifier leur identité tout au long de la session. Cette approche convient donc particulièrement pour détecter des chevaux de Troie et des attaques visant à déjouer l'authentification ou des détournements d'identité.

Le principe repose sur le fait que chaque utilisateur peut être identifié à son comportement : ses activités, ses outils préférés, ses habitudes de travail, mais aussi d'autres paramètres tels que la vitesse de sa frappe au clavier, sa préférence vis-à-vis de l'interface graphique ou des commandes texte, etc. Le profil associé à chaque utilisateur reflète donc ces informations dans le cadre d'une utilisation «normale», c'est-à-dire légitime.

Il est possible de représenter efficacement ce profil par un réseau de neurones, conçu pour reconnaître des suites d'opérations caractéristiques de l'utilisateur. Le réseau enregistre les opérations de l'utilisateur durant une fenêtre temporelle donnée, puis tente de prédire la prochaine opération. Un échec de prédiction correspond ainsi à une déviation par rapport au profil et donne potentiellement lieu à une alerte.

Avantages et inconvénients de l'approche comportementale :

- **Avantages :**

La détection d'anomalies permet de :
- détecter un comportement non usuel et ainsi offrent la possibilité de trouver des symptômes d'une attaque sans en connaitre les détails.
- Permet de produire de l'information qui peut être utilisée pour définir des signatures utilisables pour les systèmes à signatures.

- **Inconvénients :**

- Produit une quantité énorme de fausses alertes à cause du caractère imprévisible des utilisateurs et des réseaux (ruptures…).
- Demande une intense phase d'apprentissage pour caractériser la normalité des comportements.
- Si un pirate attaque pendant cette phase, ses actions seront assimilées à un profil utilisateur, et donc passeront inaperçues lorsque le système de détection sera complètement opérationnel.
- Un pirate peut s'introduire dans le système et modifier le fichier contenant les profils des utilisateurs, ce qui lui permettra de mettre en place son attaque sans qu'elle soit détectée.

II.1.3) Types d'IDS [8]

Les IDS peuvent se classer en deux catégories qui correspondent à ce que s'attache à surveiller l'IDS.

II.1.3.1) Network Based IDS (NIDS)

L'IDS réseau ou Network Based IDS (NIDS) surveille comme son nom l'indique le trafic réseau. Il se place sur un segment réseau et "écoute" le trafic. Ce trafic sera ensuite analysé afin de détecter les signatures d'attaques ou les différences avec le fonctionnement de référence. On notera une contrainte à ce système, en effet le cryptage du trafic sur les réseaux commutés rend de plus en plus difficile l' "écoute" et donc l'analyse du segment réseau à analyser, car le contenu des paquets est crypté. De plus, un trafic en constante augmentation sur les réseaux contraint les NIDS à être de plus en plus performants pour analyser le trafic en temps réel.

Placement de la sonde sur le réseau

On peut placer les NIDS à différents endroits sur le réseau, mais bien sûr la politique de sécurité menée définira leur emplacement.

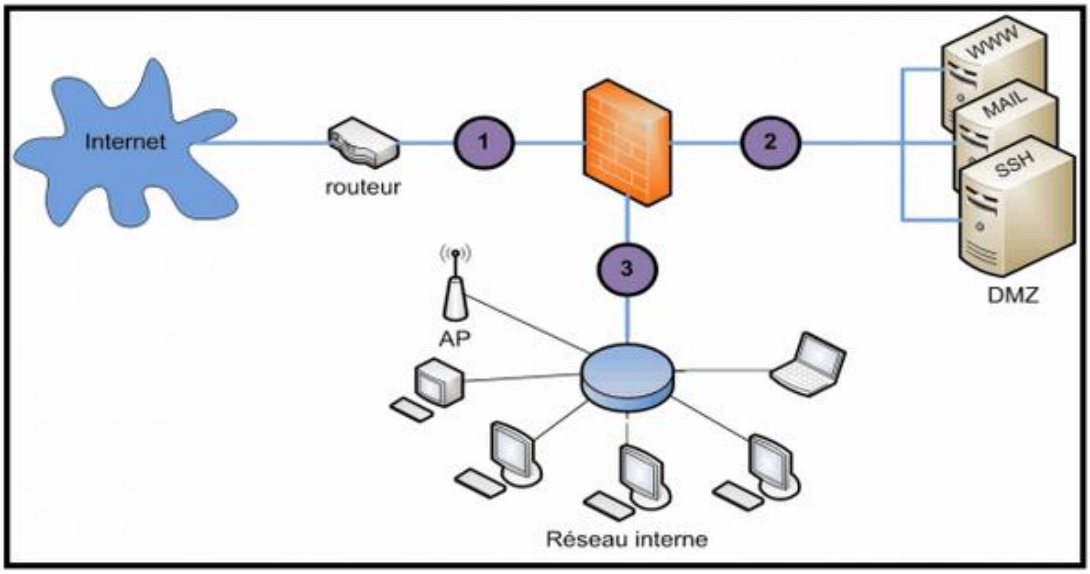

Figure 2-1 : Placement de la sonde sur le réseau

- **Position 1:**

Tout le trafic entre internet et le réseau interne ou la DMZ (DeMilitarized Zone) est analysé. Par contre le trafic entre le réseau interne et la DMZ est invisible pour l'IDS. De plus mettre un senseur à cette position génère des fichiers de log complets, mais trop complexe à analyser.

- **Position 2:**

Seul le trafic entre la DMZ et internet ou le réseau interne est analysé. De plus, placer un senseur à cet emplacement nous permet de détecter les attaques non filtré par le pare-feu et donc minimise le trafic réseau à analyser. Cependant le trafic entre le réseau interne et internet n'est pas visible pour l'IDS.

- **Position 3:**

Placer le senseur à cette position nous assure une analyse du trafic sur le réseau interne et la détection des attaques au niveau du réseau interne.

En général, il est souvent préférable de placer le senseur après le firewall du côté interne. Ainsi seuls les flux acceptés par le firewall sont analysés et donc nous obtenons une forte réduction en matière de charge des sondes de l'IDS.

Après le firewall, il y a deux positions possibles pour la sonde:

- **En coupure**

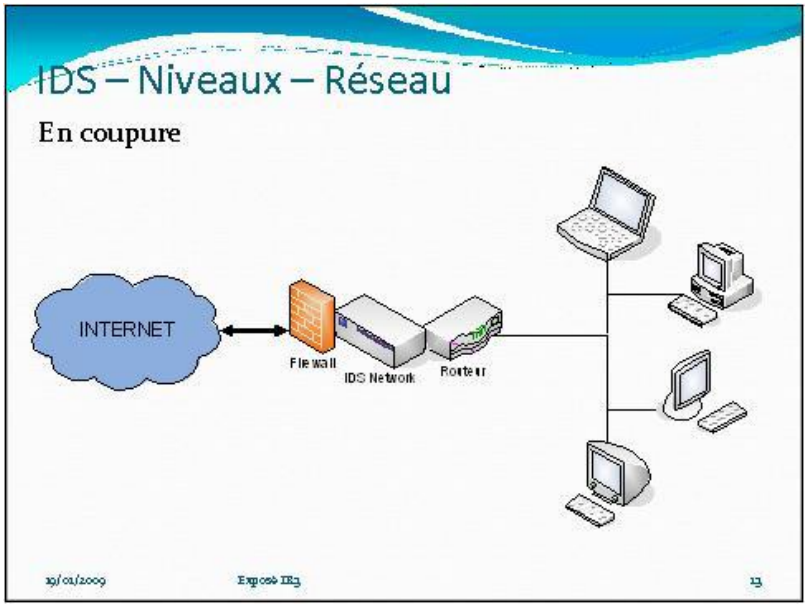

Figure 2-2 : placement de la sonde en coupure

Ici il a une faiblesse d'architecture, si la sonde tombe (par exemple à cause d'une attaque de dénis de service) c'est tout le réseau qui tombe.

- **En recopie de port**

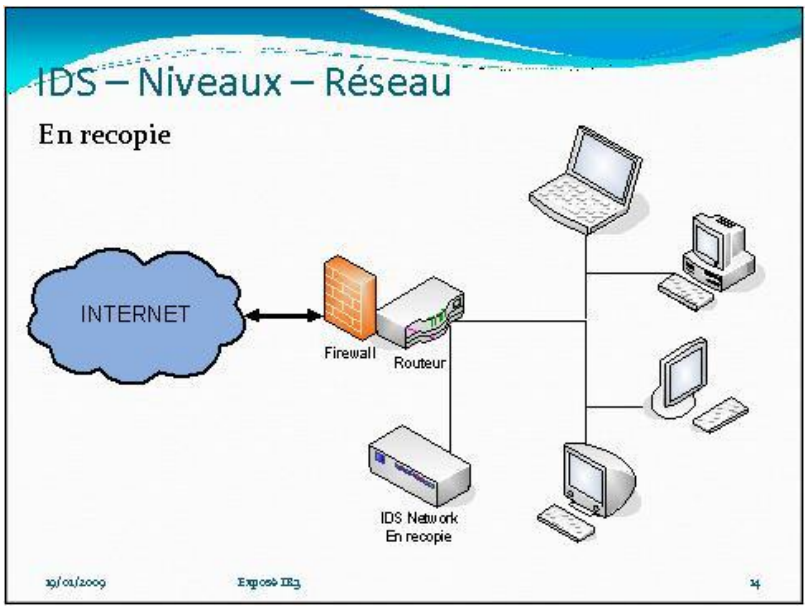

Figure 2-3 : placement de la sonde en recopie de port

Ici la sonde analyse aussi bien le réseau que en mode coupure sauf que si elle tombe due à une attaque cela ne pose aucun problème à l'architecture réseau. Et la sonde étant passive cette solution est la meilleure

Voici quelques NIDS connus : ***Snort, Bro, Enterasys, Check Point etTipping point***

II.1.3.2) Host Based IDS (HIDS)

Le HIDS surveille le trafic sur une seule machine. Il analyse les journaux systèmes, les appels systèmes et enfin vérifie l'intégrité des systèmes de fichiers. Les HIDS sont de par leur principe de fonctionnement dépendant du système sur lequel ils sont installés. Ce système peut s'appuyer ou non sur le système propre au système d'exploitation pour en vérifier l'intégrité et générer des alertes.
Il peut aussi capturer les paquets réseaux entrant/sortant de l'hôte pour y déceler des signaux d'intrusions (Déni de Services, Backdoors, chevaux de Troie, tentatives d'accès non autorisés, exécution de codes malicieux, attaques par débordement de buffers…). Il permet:

- Détection de compromission de fichiers (contrôle d'intégrité)
- Analyse de la base de registre (Windows) ou des LKMs (Linux)
- Analyse et corrélation de logs en provenance de firewalls hétérogènes
- Analyse des flux cryptés (ce que ne peut réaliser un NIDS !)

L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levées. Par nature, ces IDS sont limités et ne peuvent détecter les attaques provenant des couches réseaux.

Voici quelques HIDS connus: ***AIDE, Chkrootkit, DarkSp et IceSword***

II.2) *Système de Prévention d'Intrusions (IPS)*

II.2.1) Présentation:[6]

Le principe de rendre compte après coup d'une intrusion, a vite évolué pour chercher des IDS capables de réagir en temps réel. Le constat des dégâts ne suffisait plus : il fallait réagir et pouvoir bloquer les trafics douteux détectés. Ces techniques de réponse impliquèrent les **IDS actifs** ou **IPS**

On peut 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.

Un système de prévention d'intrusions 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.

II.2.2) Type d'IPS [6]

II.2.2.1) Network Based IPS (NIPS)

Même principe que le NIDS, à la grande différence, il peut bloquer des flux suspects. Pour le NIPS, le positionnement en coupure, tel un firewall ou un Proxy, est le seul mode permettant d'analyser à la volée les données entrantes ou sortantes et de les bloquer. Le mode recopie de port n'est pas faisable si l'on veut une interaction entre le réseau et la sonde.
L'IPS crée donc une faiblesse d'architecture, si un attaquant le découvre il sera simple pour lui de faire tomber le réseau. Il a deux types d'analyses:

- Analyse statique des flux
  - Selon les RFC
  - Selon une base de signatures
- Analyse dynamique des flux
  - Corrélation entre un événement et une signature

Lors de la détection d'une attaque, le système réagit et modifie l'environnement du système attaqué. Cette modification peut être le blocage de certains flux, de certains ports ou l'isolation pure et simple de certains systèmes du réseau.

Le point sensible de ce genre de dispositif de prévention est qu'en cas de faux positif, c'est le trafic du système qui est directement affecté. Les erreurs doivent donc d'être les moins nombreuses possibles car elles ont un impact direct sur la disponibilité des systèmes (sécurité vs. disponibilité).

II.2.2.2) Host Based IPS (HIPS)

Même principe que le HIDS, à la grande différence comme a déjà expliqué, qu'il peut bloquer des trafics anormaux.

Il Bloc les trafics anormaux selon plusieurs critères:

- Lecture / écriture de fichiers protégés
- Accès aux ports réseau
- Comportements anormaux des applications
- Bloc les accès en écriture par exemple, bloc les tentatives de récupération de droits ROOT
- Connexions suspectes (sessions RPC actives anormalement longues sur des machines distantes, etc.)

II.2.3) Type de réponses aux attaques [7]

L'établissement pourra mettre en place une politique de sécurité pour faire face à ces dangers. Deux politiques (pouvant être complémentaire) seront alors mises en œuvre :

07

II.2.3.1) Réponse Active

Les réponses actives consistent à répondre directement à une attaque, la plupart du temps en générant des requêtes de fin de connexion vers la source de manière à la contraindre à cesser son activité intrusive sur le champ. Dans le cas de données TCP, ceci se traduit par l'envoi de paquets RST qui marquent la fin d'une session aussi bien vers la source que la destination. Dans le cas des protocoles ICMP ou UDP, ça se fait en générant des requêtes ICMP Network Unreachable ou UDP Port Unreachable en espérant que la source reçoive ces requêtes et cesse d'émettre.

En fait, le fait de générer des paquets de réponse à une intrusion peut fournir à l'attaquant d'éventuelles informations révélant la présence d'un système de protection actif, tel un IPS. En observant la valeur de certains paramètres des trames de réponse, il est parfois possible de déduire quel est l'IDS qui les a émis. On cite par exemple les cas de Snort qui utilisait systématiquement un champ TTL de 253 ou de Dragon avec des numéros de séquences incrémentés de 15 entre 2 trames consécutives. Ces deux problèmes ont été corrigés depuis, mais il en existe certainement d'autres de même nature sur les IDS et IPS actuels. Si un pirate parvient à détecter la nature du système utilisé, il peut arriver à le contourner plus facilement. C'est pourquoi il est souvent préférable de rendre les IDS le plus furtifs possible.

Le deuxième problème est l'authenticité de la source de l'attaque (par exemple par le spoofing).Si l'attaquant usurpe l'identité d'un réseau nécessaire à notre entreprise, cette méthode peut nous couper du monde (ex : proxy libre)

Une des premières solutions serait de créer une liste blanche de ce qu'il ne faut absolument pas bloquer.La liste blanche bloque le paquet suspect mais ne coupe pas le flux

II.2.3.2) Réponse Passive

Cette technique consiste à bloquer les flux associés à une activité intrusive sans en informer la source, c'est-à-dire sans générer de paquets spécifiques à destination du pirate. Les réponses passives se traduisent la plupart du temps par des opérations de reconfiguration automatique d'un firewall (NIDS) le fait avec packetfilter (firewall) afin de bloquer les adresses IP source impliquées dans les intrusions.

En revanche, le problème de l'authenticité de la source de l'attaque est le même. Avec un firewall on a aussi la possibilité de nous couper d'un réseau important.

En effet, si le pirate usurpe une adresse IP sensible telle qu'un routeur d'accès ou un serveur DNS, l'entreprise qui implémente une reconfiguration systématique d'un firewall risque tout simplement de se couper elle-même et du monde extérieur.

II.2.4) IDS/IPS [7]

Les IPS sont souvent considérés comme des IDS de deuxième génération. Bien qu'il s'agisse d'un abus de langage, cette expression traduit bien le fait que les IPS remplacent petit à petit les IDS. Il est pour autant prématuré de dire que les IDS sont morts, comme l'avait prétendu Gartner Group il y a 2 ans.

- En fait, les IPS ont avant tout été conçus pour lever les limitations des IDS en matière de réponse à des attaques. Alors qu'un IDS n'a aucun moyen efficace de bloquer une intrusion, un IPS pourra, de son positionnement en coupure, bloquer une intrusion en temps réel.
- Une autre limite à laquelle devaient faire face les IDS il y a quelques années était due à leur incapacité à gérer les hauts débits du fait d'une architecture logicielle. Plusieurs constructeurs ont intégré des circuits spécifiques (ASICs) dans leurs sondes IPS, si bien que le débit devient de moins en moins une problématique.

II.2.5) IPS/Firewall [7]

Contrairement à un firewall « traditionnel », un IPS se caractérise par les points suivants :

- il doit être complètement furtif. Ceci implique que les interfaces de la sonde ne doivent pas être visibles (pas d'adresse IP, pas d'adresse MAC) et que l'équipement ne doit pas se comporter comme un proxy ou implémenter des mécanismes de manipulation des adresses (comme NAT par exemple)
- l'IPS analyse l'intégralité des paquets en transit, depuis les couches réseaux jusqu'au niveau applicatif.

Conclusion

Dans ce chapitre on a apporté plus de détail sur les systèmes de détection et de prévention d'intrusions. On connaît désormais les différentes sortes d'implémentation desIPS et IDS pour sécuriser un réseau et/ou un hôte, les positions possibles dans un réseau et la différence entre eux. On a vu les approches existantes pour détecter les anomalies, leurs avantages et inconvénients.

Dans le chapitre qui suit, nous allons présenter les IPS données par l'entreprise Cisco Systems pour choisir la meilleure solution pour notre organisme d'accueil ENIEM.

CHAPITRE 3:

Les solutions IPS de Cisco Systems

Introduction

Cisco Systems est une entreprise informatique américaine spécialisée, à l'origine, dans le matériel réseau (routeur et commutateur Ethernet), et depuis 2009 dans les serveurs et les réseaux. Il existe plusieurs et différentes gammes de produits Cisco qui donne des solutions pour la sécurité des réseaux, parmi ces solutions on trouve le IPS.

Dans ce chapitre, nous allons jeter l'œil sur les produits Cisco Systems et les caractéristiques de leurs solutions, pour comprendre la différence entre eux et selon quels critères on fait le choix de la gamme à utiliser pour une entreprise.

Pourquoi choisir les services Cisco ?

Les Services Cisco développent des réseaux et des applications permettant une collaboration plus efficace entre les personnes qui les utilisent. Cisco propose un ensemble complet de produits et services de sécurité afin de nous aider à éviter les interruptions d'activité.

Les Services Cisco pour IPS aide notre réseau à se défendre contre de nombreuses menaces et nous permet de réagir rapidement et efficacement en cas d'attaque. Que nous utilisions la technologie IPS dans des routeurs ou commutateurs, ou que nous comptions sur la protection transparente fournie par ses appareils de sécurité, Cisco fournit un grand nombre de périphériques de défense contre les menaces qui permettent d'identifier et de bloquer rapidement les menaces réseau.

Le réseau fonctionne mieux lorsque les services, associés aux produits, créent des solutions adaptées aux besoins et aux opportunités des entreprises.

III.1) Caractéristiques des IDS et IPS Cisco [12]

Les technologies IDS et IPS partagent plusieurs caractéristiques. Les technologies IDS et IPS sont toutes les deux déployées comme des capteurs. Un capteur IDS ou IPS peut être l'un des dispositifs suivants:

- Un routeur configuré avec le logiciel Cisco IOS IPS
- Une Appliance spécifiquement conçu pour fournir des services IDS ou IPS dédiés
- Un module de réseau installé dans un appareil de sécurité adaptative (ASA), un commutateur ou routeur.

En utilisant une de ces technologies n'exclut pas l'utilisation de l'autre. En fait, les technologies IDS et IPS peuvent se compléter mutuellement. Par exemple, un IDS peut être mis en œuvre pour valider le fonctionnement IPS parce que l'IDS peut être configuré pour approfondir d'inspection de paquets. Cela permet à l'IPS de se concentrer sur moins de paquets. La décision de l'implémentation à utiliser est basée sur les objectifs de sécurité de l'organisation.

Les implémentations Network- Based IPS sont un élément essentiel de la prévention d'intrusion; alors qu'il y a les solutions Host- Based IDS/IPS, celles-ci doivent être intégrées avec une mise en œuvre NIDS pour assurer une robustesse à la sécurité de l'architecture.

III.2) Les signatures des IDS/IPS Cisco [12]

Les technologies IDS et IPS utilisent des signatures pour détecter les paquets suspects dans le trafic réseau. Une signature est un ensemble de règles qu'un IDS ou IPS utilise pour détecter une activité malveillante. Les signatures peuvent être utilisés pour détecter les violations graves de la sécurité, pour détecter les attaques de réseau commun, et de simplement recueillir des informations. Les technologies IDS et IPS peuvent détecter des modèles de signature atomiques ou des modèles de signature composites.

Comme les capteurs scannent les paquets réseau, ils utilisent des signatures pour détecter les attaques connues et répondre avec des actions prédéfinies. Un flux de paquets malveillants a un type d'activité spécifique et une signature. Un capteur IDS/IPS examine le flux de données à l'aide de signatures différentes. Lorsqu'un capteur correspond une signature avec un flux de données, il prend des mesures, telles que l'enregistrement de l'événement ou l'envoi d'une alarme au logiciel de gestion IDS/IPS. Les signatures ont trois attributs distinctifs:

- Type
- Trigger (alarme)
- Action

III.2.1) Types de Signatures

Les types de signature sont généralement classés comme atomique ou composite.

III.2.1.1) Signature atomique

Une signature atomique est le type le plus simple de la signature. Il s'agit d'un seul paquet, une activité ou un événement qui est examiné pour déterminer si elle correspond à une signature configurée.

Avec les signatures atomiques, l'ensemble de l'inspection peut être réalisée en une opération atomique qui ne nécessite pas de connaissance des activités passées ou futures. La détection des signatures atomiques consomme un minimum de ressources, telles que la mémoire, sur l'appareil IPS/IDS. Ces signatures sont faciles à identifier et à comprendre parce qu'elles sont comparées à un événement ou un paquet spécifique.

Par exemple, une attaque LAND a une signature atomique, car il envoie un paquet de mystification TCP SYN avec la même adresse IP source et destination de l'hôte cible et de même port source et destination comme un port ouvert sur la cible. La raison d'une attaque LAND est parce qu'il provoque la machine pour répondre à lui-même en permanence. Un paquet est nécessaire pour identifier ce type d'attaque.

III.2.1.2) Signature Composite

Ce type de signature identifie une séquence d'opérations réparties sur plusieurs hôtes sur une période de temps arbitraire. Contrairement aux signatures atomiques, les signatures composites exigent habituellement plusieurs paquets de données pour correspondre à une signature d'attaque, et un dispositif IPS doit maintenir l'état. La période de temps pendant lequel les signatures doivent maintenir l'état est connu comme l'espace d'événement.

Un IPS utilise un espace d'événements configuré pour déterminer combien de temps il cherche une signature spécifique d'attaque quand une composante initiale de signature est détectée. La Configuration de la longueur de l'espace des événements est un compromis entre les ressources consommables du système et étant capable de détecter une attaque qui se produit sur une longue période de temps.

III.2.2) Le fichier de Signatures IPS Cisco

Les menaces de sécurité réseau sont plus fréquentes et la diffusion est plus rapide. Comme de nouvelles menaces sont identifiées, de nouvelles signatures doivent être créés et téléchargés sur un IPS. Pour faciliter ce processus, toutes les signatures sont contenues dans un fichier de signatures par exemple, IOS-S595-CLI.pkg est téléchargé sur un IPS sur une base régulière. Cette base de données de signatures est utilisée par la solution IPS pour comparer le trafic réseau contre les modèles de données au sein du fichier de signature afin de détecter le trafic réseau malveillant suspect. Par exemple, l'attaque LAND est identifié dans la signature "Impossible paquets IP" (signature 1102,0).

Généralement, les fichiers de signatures IPS de moindre priorité sont publiés toutes les deux semaines. Si la menace est sévère, Cisco publie des fichiers de signatures en quelques heures d'identification.

La récupération périodique et automatique des mises à jour de signatures IPS de Cisco.com peut être configurée sur un appareil ISR deuxième génération après l'installation des certificats SSL VeriSign sur le dispositif.

Ces signatures sont de différents types, elles ont toutes les mêmes propriétés suivantes :

- **Nom de la Signature:** est le nom convivial de la signature, il fournit habituellement une courte description de l'attaque que la signature est conçue pour la détecter ou la prévenir
- **ID de la Signature:** est un entier qui identifie de manière unique la signature.
- **Statut de la Signature :** décrit la signature comme activée ou désactivée ou retirée.
- **Indice de gravité:** détermine la gravité qui est attribuée par défaut à des événements causant le déclenchement de la signature.
- **Stratégie de récapitulation:** décrit comment la signature génère souvent des alarmes
- **Actions d'intervention:** sont prises par le capteur lorsqu'une alarme est déclenchée.

L'extrait du tableau ci-dessous, pris du site officiel de Cisco, montre quelques signatures et leurs propriétés :

IPS Signatures

Signature ID	Signature Name	Latest Release Date	Alarm Severity
3541/0	Siemens S7 1200 Cross Site Request Forgery	2015 Jan 08	Medium
3542/0	Siemens S7-1200 Cross Site Scripting	2015 Jan 08	Medium
3543/0	Siemens S7-1200 Cross Site Scripting	2015 Jan 08	Medium
3544/0	Siemens S7-1200 Cross Site Scripting	2015 Jan 08	Medium
3040/0	TCP NULL Packet	2001 Feb 02	High
2004/0	ICMP Echo Request	2012 Sep 11	Informational
3338/1	Windows LSASS RPC Overflow	2011 Dec 14	High
33319/0	Apache HTTP Request Long Headers	2011 Dec 07	High
5513/1	SNMP Community String Public	2011 Oct 01	High
32920/0	TWiki Search Function Arbitrary Command Execution	2011 Sep 23	High
26479/0	Medal Of Honor Allied Assault Remote Buffer Overflow ...	2011 Sep 23	High
3342/2	Windows NetDDE Overflow	2011 Apr 19	High
5452/1	Office XP URL Processing Buffer Overflow	2011 Jan 28	High

Figure 3-1: Exemple montrant quelques propriétés des signatures

III.2.3) Les alarmes de signatures Cisco :

Les mécanismes de déclenchement peuvent générer des alarmes qui sont des faux positifs ou des faux négatifs. Ces alarmes doivent être abordées lors de la mise en œuvre d'un capteur IPS. Les quatre types d'alarmes sont les suivants:

- **Un faux positif** est un résultat attendu, mais indésirable. Un faux positif survient lors d'une intrusion, le système génère une alarme après le traitement du trafic utilisateur normal qui ne devrait pas avoir déclenché une alarme. L'analyse des faux positifs limite le temps qu'un analyste de la sécurité met pour examiner l'activité réelle intrusive sur un réseau. Si cela se produit, l'administrateur doit régler l'IPS pour changer ces types d'alarmes à de vrais négatifs.

- **Un faux négatif** est quand un système d'intrusion ne parvient pas à générer une alarme après le traitement des attaques dans le trafic que le système d'intrusion est configuré à détecter. Cela signifie que les attaques connues ne sont pas détectées.

- **Un vrai positif** décrit une situation dans laquelle un système d'intrusion génère une alarme en réponse à un trafic d'attaque connue.

- **Un vrai négatif** décrit une situation dans laquelle le trafic normal du réseau ne génère pas d'alarme.

III.2.4) Actions de Signature IPS

Les alarmes se déclenchent lorsque les paramètres spécifiques sont remplis. Un administrateur doit équilibrer le nombre d'alarmes incorrectes qui peuvent être tolérées par la capacité de la signature pour détecter les intrusions réelles. S'il y a trop peu d'alarmes, les paquets suspects pourraient être autorisés à entrer dans le réseau. Cependant, si les systèmes IPS utilisent des signatures non accordées, ils produisent beaucoup de fausses alarmes.

Une signature est accordée sur l'un des quatre niveaux, basé sur la gravité perçue de la signature, conformément à la figure 3-2:

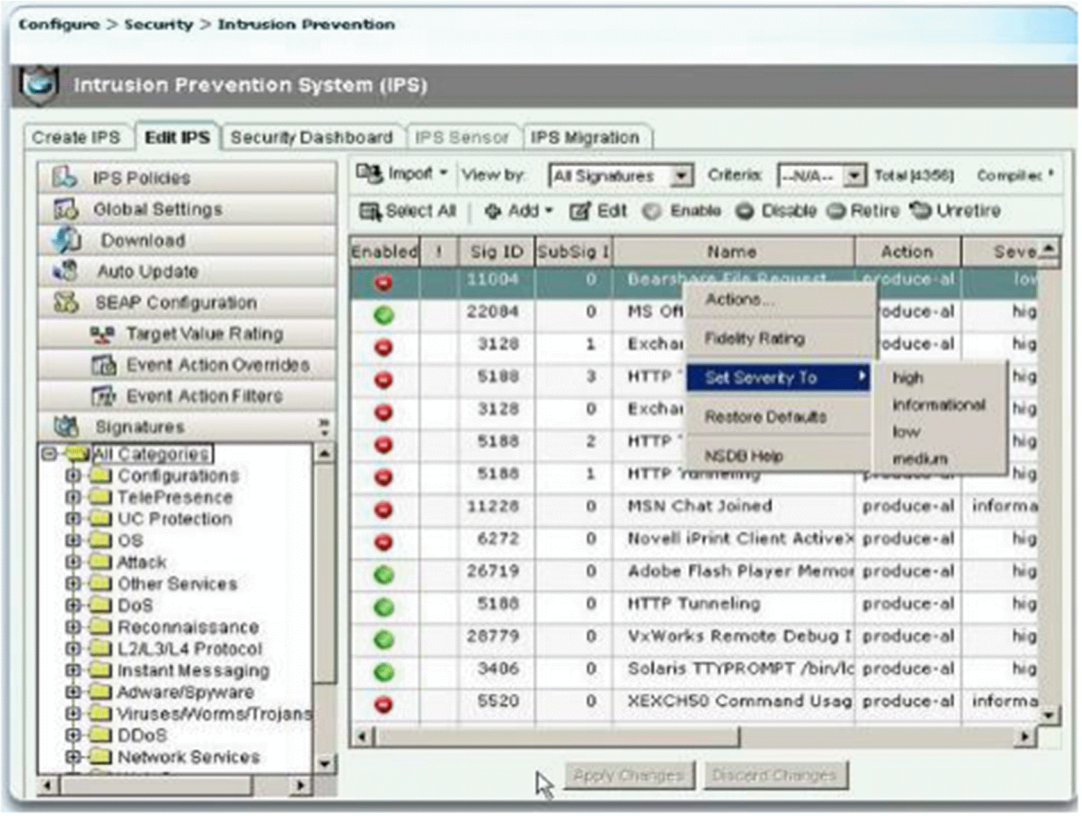

Figure 3-2: Les 4 niveaux de gravité d'une signature avec CCP

- ✓ **élevé** - Attaques utilisés pour accéder ou de provoquer un déni de service sont détectées, et une menace immédiate est extrêmement probable.
- ✓ **Moyen** - Activité réseau anormale est détectée qui pourrait être perçu comme malveillant et une menace immédiate est probable.
- ✓ **Faible** - activité réseau anormale est détectée qui pourrait être perçu comme malveillant; cependant une menace immédiate n'est pas probable.

- ✓ **informationnel** - Activité qui déclenche une signature qui n'est pas considérée comme une menace immédiate; cependant, les renseignements fournis sont des informations utiles.

Il y a plusieurs facteurs à considérer lors de la mise en œuvre des alarmes qui utilisent une signature:

- ✓ Le niveau attribué à la signature détermine le niveau de gravité d'alarme.
- ✓ Lors de réglage d'une alarme de signature, le niveau de sévérité de la signature doit être maintenue identique au niveau de gravité déterminée par celle de la signature.
- ✓ Pour minimiser les faux positifs, l'administrateur doit étudier les modèles de trafic réseau existants et puis affiner les signatures de reconnaître des modèles d'intrusion qui sont atypiques.

Chaque fois qu'une signature détecte l'activité pour laquelle elle est configurée, la signature déclenche une ou plusieurs actions. Plusieurs catégories d'actions peuvent être invoquées :

- ✓ Générer une alerte.
- ✓ Enregistrer l'activité.
- ✓ Baisse ou empêcher l'activité.
- ✓ Réinitialiser une connexion TCP.
- ✓ bloquer l'activité future.
- ✓ Autoriser l'activité.

Les actions disponibles dépendent du type de signature et la plate-forme.

III.3) Les différents produits IPS de Cisco: [12]

Le choix d'un capteur IPS varie en fonction des exigences de l'organisation. Il existe plusieurs facteurs qui affectent la sélection du capteur IPS et le déploiement:

- Montant du trafic réseau
- La topologie du réseau
- Le budget de sécurité
- Le personnel de sécurité disponible pour gérer l'IPS.

Les plates-formes des capteurs Cisco IPS intègre dans une variété de topologies et architectures réseaux. Les plates-formes de détection sont réparties dans les groupes principaux suivants, comme illustré sur la Figure 3-3:

■ Appareils IPS autonomes sous la forme de **capteurs Cisco IPS 4200 Series**
■ **Cisco Catalyst 6500** Series, Modules à Système de détection d'intrusion (IDSM-2)
■ **Cisco ASA 5500 Series Integré,** Modules Intégrés de services de sécurité à inspection avancée et prévention (AIP SSC-5, AIP SSM-10, AIP SSM-20, et de l'AIP SSM-40)
■ Des routeurs de Services intégrés Cisco **(ISR):** intégrés à l'IOS ou sous forme de modules AIP ou NM.

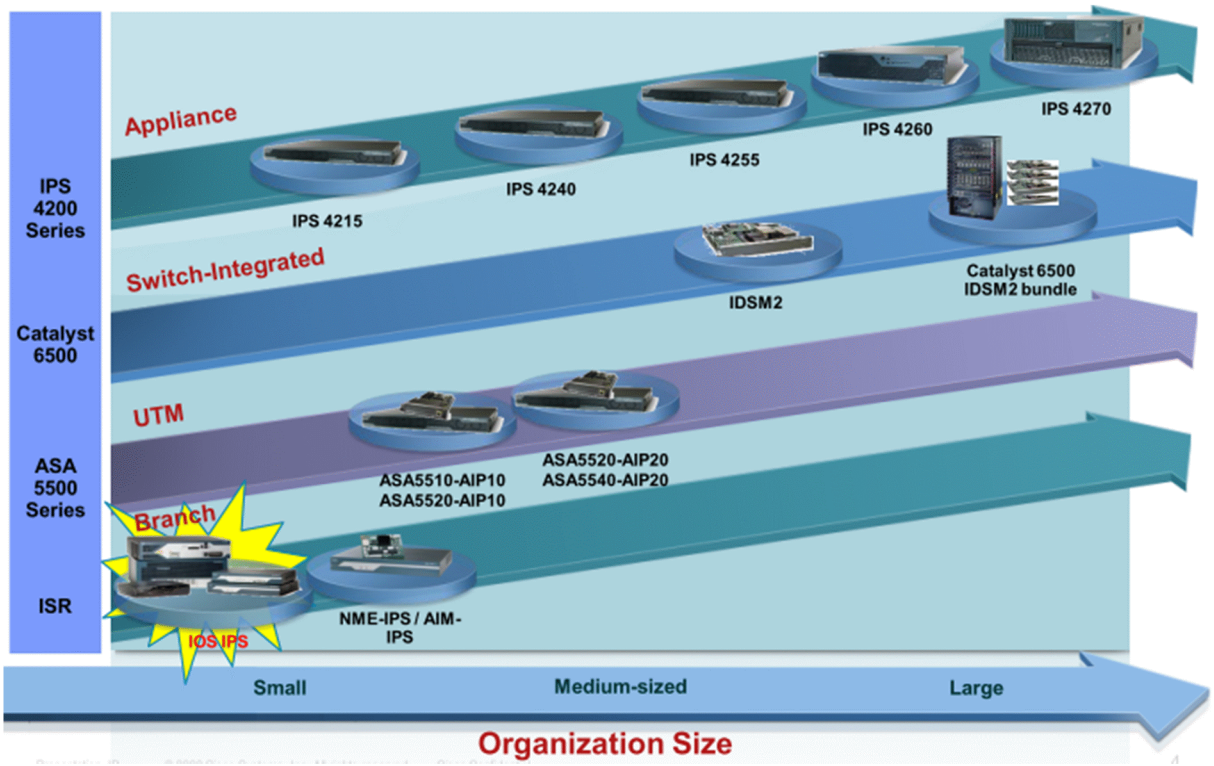

Figure 3-3 : La famille des IPS Cisco

Comme le montre la figure 3-3, les petites implémentations telles que les succursales pourraient ne nécessitent qu'un Cisco IOS IPS routeur ISR permis. Comme le trafic des modèles augmentent, l'ISR peut être configuré pour se décharger des fonctions IPS utilisant un IPS de type Network Module Enhanced (NME) ou IPS Advanced Integration Module (AIM).

Des installations plus importantes peuvent être déployées à l'aide d'un appareil existant ASA 5500-X.

Les entreprises et les fournisseurs de services peuvent nécessiter un appareil IPS dédié ou un Catalyst 6500 en utilisant un module de réseau IDSM-2.

III.3.1) Les capteurs Cisco IPS 4200 Series [9]

Les IPS Cisco 4200 forment une gamme d'appareils IPS dédiés qui identifient avec précision et interrompent l'activité malicieuse, comme les vers, les attaques ciblées, le déni de service, les violations des protocoles et les attaques qui viennent des couches basses aux couches applicatives.
Plusieurs boîtiers dédiés sont disponibles avec des débits allant jusqu'à 4 Gbps, avec des interfaces cuivre ou fibre, qui peuvent être déployés en ligne (coupure) ou en mode promiscuité (écoute).

Les fonctionnalités de Cisco IPS 4200 Series: [21]

- Détecter les menaces pour la propriété intellectuelle et les données des clients, avec l'inspection modulaire tout au long de la pile réseau
- Arrêtez les attaquants sophistiqués en détectant les anomalies de comportement, à l'évasion, et les attaques contre les vulnérabilités
- Prévenir les menaces en toute confiance avec ensemble d'actions de prévention de la menace la plus complète de l'industrie
- Réponse de discussion avec les évaluations des menaces dynamiques et la journalisation détaillée
- Fournir une protection contre les dernières menaces et vulnérabilités

Intégration dans toute architecture de réseau LAN est simplifiés avec les capteurs de l'appareil car ils ne nécessitent pas une autre plate-forme de réseau et peuvent être facilement déplacés dans un réseau en cas de besoin.

Les **Cisco IPS 4240 et 4255** sont des capteurs qui comprennent un nombre fixe d'interfaces LAN à configuration fixe.

Les capteurs **Cisco 4260 et 4270** comprennent un certain nombre d'interfaces LAN par défaut, et offrent la possibilité d'accueillir des interfaces réseau supplémentaires, y compris des interfaces fibre optique 1000 BASE-SX.

Spécification du débit de quelques produits Cisco IPS 4200 Series

Cisco IPS 4240	Cisco IPS 4255	Cisco IPS 4260	Cisco IPS 4270
			
300 Mbps	600 Mbps	2 Gbps	4 Gbps

Figure 3-4 : Le débit des produits Cisco IPS 4200 Series

III.3.2) Cisco Catalyst 6500 Series [10]

En tant que commutateur modulaire multicouche haut de gamme, la famille de produit Cisco Catalyst 6500 fournit des services sécurisés pour le commutateur d'étage comme pour le commutateur de cœur, pour les centres de données, et l'accès au WAN.
Le Catalyst 6500 supporte actuellement trois systèmes d'exploitation: CatOS, natif IOS et IOS modulaire.[1]
Le Cisco Supervisor Engine est le cœur de beaucoup des commutateurs Cisco.
Le superviseur 6500 comprend un multicouche Fonction Bouton Card (MSFC) et une carte d'entité politique (PFC). Le MSFC exécute tous les processus de logiciels, tels que les protocoles de routage. Le PFC prend des décisions de renvoi dans le matériel.

Le Supervisor Engine a évolué à plusieurs reprises. La dernière génération de superviseur est le superviseur 2T. Ce superviseur a été introduit en 2011. Il offre 80 gigabits par emplacement sur tous les emplacements de châssis 6500-E.

Le Catalyst 6500/7600 peut intégrer un certain nombre de modules de services de sécurité :

- **Le module Cisco Firewall Services Module (FWSM)** permet d'intégrer au Catalyst 6500/7600 des fonctions avancées de firewall haute performance (5Gbps de débit, 100.000 connexions/seconde, 1 Million de connexions simultanées). Jusqu'à quatre FWSMs peuvent être installées dans un châssis, fournissant ainsi un maximum de 20Gbps de firewall. Le module FWSM intègre par ailleurs de nombreuses fonctionnalités avancées, comme par exemple la virtualisation du firewall avec réservation de ressources, le mode transparent, afin d'offrir évolutivité, simplicité d'exploitation, et protection de l'investissement.

- **Le module Cisco IDSM-2** intègre directement les fonctions de prévention d'intrusion Cisco dans le châssis Catalyst. Cette intégration permet de surveiller le trafic directement sur le fond de panier du Catalyst 6500/7600, et, combiné aux fonctions de détection avancées de l'IPS version 6.0, permet de détecter et bloquer les attaques connues et inconnues avec un niveau de confiance inégalé.

- **Le module IPSec SPA** pour Catalyst 6500/7600 permet d'intégrer des fonctions de VPN IPSec à haut débit directement dans le châssis. Les débits peuvent atteindre 2.5Gbps de trafic chiffré en AES, ainsi que la terminaison simultanée de 8.000 tunnels.

Caractéristiques des Supervisors Engines [16]

Supervisor Engine	Mpps*	couche de commutation	Bande passante	Fréquence CPU	Max Ram	OS
1	15	2	1,2 à 32	25 MHz	128 Mo	CatOS
2	30	2	18	150 MHz	128 Mo	CatOS
2+	48	4	64	266 MHz	256 Mo	CatOS / IOS
3	15	4	?	150-300 MHz	256 Mo	IOS
4	48	4	64	333 MHz	512 Mo	IOS
5	136	4	102	400-800 MHz	512 Mo	IOS
6	250	4	320	1.3 GHz	1GB	IOS
720	400-450	5	720	600 MHz	2 Go	CatOS / IOS
32		5	32	300 MHz		IOS
2T	720	5	2080		4 GO	IOS

Figure 3-5 : Caractéristiques des Supervisors Engines

III.3.3) Cisco ASA 5500 (adaptatifs serveurs de sécurité) [11]

La gamme complète des services disponibles avec la famille Cisco ASA 5500 permet de répondre aux besoins spécifiques de chaque site grâce à des éditions produits conçues pour les PME comme pour les grandes entreprises.

Ces différentes éditions offrent une protection de qualité supérieure en apportant à chaque installation les services dont elle a besoin. Chaque édition de la gamme Cisco ASA 5500 regroupe un ensemble spécialisé de services – firewall, VPN SSL et IPSec, protection contre les intrusions, services Anti-X, etc. – qui répondent exactement aux besoins des différents environnements du réseau d'entreprise.

Cisco IPS Modules de services de sécurité et d'inspection avancée et prévention (AIP SSM), et de la carte de services de sécurité (AIP SSC) - améliore les capacités IPS pour Cisco ASA 5500. La figure 3-3 affiche un AIP SSM-10 pour Cisco ASA 5510 et 5520 modèles. L'AIP SSC-5 est conçu spécifiquement pour la gamme Cisco ASA 5505.

Figure 3-6: Module Cisco ASA AIP-SSM

Caractéristiques de la gamme Cisco ASA 5500

	Cisco ASA 5505	**Cisco ASA 5510**	**Cisco ASA 5520**	**Cisco ASA 5540**	**Cisco ASA 5550**
					
Débit du firewall	Jusqu'à 150 Mbits/s	Jusqu'à 300 Mbits/s	Jusqu'à 450 Mbits/s	Jusqu'à 650 Mbits/s	Jusqu'à 1,2 Gbits/s
Débit de protection simultanée (firewall + services IPS)	Non disponible	Jusqu'à 150 Mbits/s avec l'AIP-SSM-10 Jusqu'à 375 Mbits/s avec l'AIP-SSM-20	Jusqu'à 225 Mbits/s avec l'AIP-SSM-10	Jusqu'à 450 Mbits/s avec l'AIP-SSM-20	Non disponible
Débit du VPN 3DES/AES	Jusqu'à 100 Mbits/s	Jusqu'à 170 Mbits/s	Jusqu'à 225 Mbits/s	Jusqu'à 325 Mbits/s	Jusqu'à 425 Mbits/s
Nouvelles sessions/S	3 000	6 000	9 000	20 000	28 000

Ports réseau intégrés	Commutateur Fast Ethernet 8 ports (dont 2 ports PoE)	3 ports Fast Ethernet + ; 1 port de gestion ; 5 ports Fast Ethernet*	4 ports Gigabit Ethernet ; 1 port Fast Ethernet	4 ports Gigabit Ethernet ; 1 port Fast Ethernet	8 ports Gb Ethernet, 4 ports fibres SFP ; 1 port Fast Ethernet
Mémoire	256 Mo	256 Mo	512 Mo	1024 Mo	4096 Mo

*Disponible par l'intermédiaire d'une licence de mise à niveau

Figure 3-7 : Caractéristiques de la gamme Cisco ASA 5500

III.3.4) Routeurs Cisco à Services Intégrés (ISR)

Avantages de routeur à services intégrés

- ✓ **Obtenir une protection supplémentaire sans avoir à déployer un nouveau matériel:** Activer nouvelles fonctionnalités de sécurité réseau sur les routeurs existants en utilisant le logiciel Cisco IOS.
- ✓ **Renforcer la sécurité au plus besoin:** Appliquer des fonctions de sécurité, telles que pare-feu et IPS, partout dans le réseau, y compris les succursales éloignées.
- ✓ **Gain du temps et de l'argent:** Réduire le nombre total de périphériques de réseau, ce qui diminue les coûts de support et de gestion en cours.

III.3.4.1) Cisco ISR avec AIM-IPS et NME-IPS [9]

Le Cisco IPS Advanced Integration Module (AIM) est conçu pour les petites et moyennes tailles d'entreprises et les petits déploiements de succursales.

Le Cisco IPS Network Module Enhanced (NME) est conçu pour les petites entreprises et les grands déploiements de succursales.

L'IPS AIM est appuyé sur Cisco 1841, 2800 Series et 3800 Series ISR. L'IPS NME est pris en charge sur 2800 Series, 3800 Series, 2900 Series et 3900 Series ISR.

Les modules surveillent le trafic de toute interface routeur du système Cisco IOS et prennent également en charge l'encapsulation générique de routage (GRE) et l'inspection du trafic IPsec qui a été décrypté au niveau du routeur. La virtualisation n'est pas supportée par les modules.

Le module AIM-IPS n'a pas d'interface externe, alors que le NME-IPS dispose d'un port Ethernet Gigabit externe qui est utilisé comme une interface de commande et de contrôle pour la gestion out-of-band.

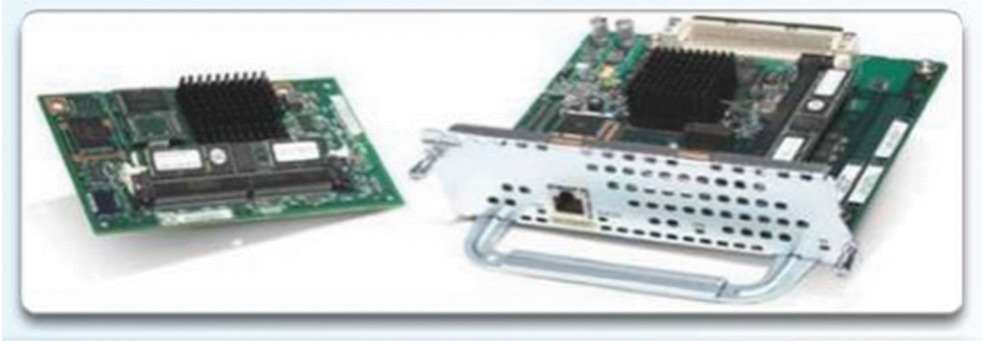

Figure 3-8 : Les modules IPS Cisco AIM et NME

III.3.4.2) Cisco ISR avec IOS IPS [21]

Voici les principales gammes ISR de deuxième génération existantes et leurs caractéristiques. Ainsi que la production ne s'arrête pas là car il y en a toujours de nouveaux produits :

- **Cisco 800 Series :**

  Ils intègrent des services pour les petits bureaux ou mobiles, Pour obtenir des services complets et innovants avec la gamme Cisco 800 routeurs, y compris:

  - ✓ La sécurité de niveau entreprise
  - ✓ Cisco voix unifiée, vidéo et données
  - ✓ Intégré dans l'optimisation WAN
  - ✓ Visibilité et le contrôle d'application
  - ✓ Connectivité Cloud-demande

Ces routeurs de services intégrés (ISR) offrent des performances de pointe et des services IP avancés sur tout, y compris les technologies WAN XDSL, Gigabit Ethernet, 3G et 4G, et de fibres.

- **Cisco 1900 Series :**

Ils sont conçus pour répondre aux exigences des applications de petites branches d'aujourd'hui et d'évoluer à des services basés sur le Cloud. Ils offrent des applications virtualisées et collaboration hautement sécurisée à travers le plus large éventail de connectivité WAN à haute performance qui offre des services simultanés à jusqu'à 25 Mpps (Million Packets Per Second).

Tous les routeurs de la gamme Cisco 1900 à services intégrés (ISR) ont une conception modulaire qui permet la réutilisation d'un large éventail de modules existants qui répondent aux besoins de l'entreprise tout en maximisant la protection des investissements. Ils offrent:

- ✓ **Services d'application Agile,** y compris la capacité d'héberger plusieurs applications tierces Cisco ou sur les modules ISM pour les applications à mission critique à la succursale.

- ✓ **Connectivité WAN** à travers les plus larges choix de l'industrie, y compris WLAN 802.11a / g / n, T1 / E1, T3 / E3, 4G / LTE, xDSL, le cuivre et fibre Gigabit Ethernet.

- ✓ **Optimisation WAN** avec un support pour, à la demande d'optimisation WAN et l'application accélération routeur intégré à travers le module de service

- ✓ **Hautement intégré de la sécurité** avec une suite complète de technologies VPN IPSec et VPN SSL renforcée par l'accélération de chiffrement à bord le soutien de la défense de la menace par pare-feu et de prévention d'intrusion système (IPS) des options et comprend en outre un soutien pour le chiffrement de la prochaine génération et de la sécurité Cloud basée.

- ✓ **Haute performance** avec des processeurs puissants et économes en énergie multicœurs.

- **Cisco 2900 Series :**

Ils offrent la même conception avec Cisco 1900 à une connectivité WAN à un peu plus de performance jusqu'à 75 Mbps, et les mêmes caractéristiques aussi : Services d'application Agile, Connectivité WAN, Optimisation WAN et Hautement intégré de la sécurité, en plus les deux suivants :

- ✓ **Communications unifiées** qui soutiennent les services de traitement et de messagerie vocale appels.
- ✓ **Medianet** services qui offrent une expérience plus visuelle, sociale et personnelle grâce à des solutions de réseautique vidéo pour les utilisateurs des succursales.

Spécifications en bref

Les Cisco 2900 Series Integrated Services Routers comprennent:

- Jusqu'à 50 ports de commutation LAN, 4 haut-débit WAN Interface Card (EHWIC) slots améliorées
- Sécurité
    - ➢ Chiffrement VPN avec accélération matérielle embarquée, et Cisco Web Cloud Security
    - ➢ Commande intégrée des menaces en utilisant Cisco IOS Firewall et IPS Cisco IOS

- **Cisco 3900 Series**

Ils offrent la même conception avec Cisco 2900 à une connectivité WAN à haute performance à jusqu'à 375 Mpps, et mêmes caractéristiques aussi : Services d'application Agile, Connectivité WAN, Optimisation WAN, Hautement intégré de la sécurité, Communications unifiées et Median et à quelques petites déférences dans les applications hébergées et ses capacités.

Spécifications en bref

Les Cisco 3900 Series Integrated Services Routers comprennent:

- Jusqu'à 4 modules de service, 1 module de service intégré (ISM)
- Jusqu'à 98 ports de commutation LAN, 4 haut-débit WAN Interface Card (EHWIC) slots améliorées
- Possibilité d'ajouter une deuxième alimentation intégrée
- Sécurité
    - Chiffrement VPN intégré accélération matérielle et Cisco Web Cloud Security
    - Commande intégrée des menaces en utilisant Cisco IOS Firewall et IPS Cisco IOS

Le routeur Cisco ASR 1000 représente une nouvelle génération de routeurs modulaires, intégrant de multiples services en hardware et conçu avec la flexibilité autorisant des performances de l'ordre de 4-8 Mpps avec 5-10 Gbps de bande passante pour la première disponibilité. Des releases ultérieures du module de commutation permettront d'aller jusqu'à 40 Gbps.

La gamme de routeurs Cisco ASR 1000 adresse le segment de marché compris entre le Cisco 7200 et le Cisco 7600.

III.4) Les composants d'un routeur :[15]

Comme un ordinateur un routeur est composé de:

- **Microprocesseur (CPU) :** il est responsable de l'exécution du système d'exploitation du routeur.
- **Mémoire Flash :** représente une sorte de ROM effaçable et programmable. Sur beaucoup de routeurs, la mémoire flash est utilisée pour maintenir une image d'un ou plusieurs systèmes d'exploitation.
- **ROM :** contient le code pour réaliser les diagnostics de démarrage (POST : Power On Self Test). En plus, la ROM permet le démarrage et le chargement du système d'exploitation contenu sur la mémoire flash.
- **RAM :** est utilisé par le système d'exploitation pour maintenir les informations durant le fonctionnement. Elle peut contenir la configuration qui s'exécute, les tables de routage, la table ARP, etc. Et comme c'est de la RAM, lors de la coupure de l'alimentation, elle est effacée.
- **NVRAM (RAM Non Volatile) :** Le problème de la RAM est la non conservation des données après la coupure de l'alimentation. La NVRAM solutionne le problème, puisque les données sont conservées même après la coupure de l'alimentation. La configuration est maintenue dans la NVRAM.
- **Modules (Portes I/O) :** L'essence même d'un routeur est l'interfaçage vers le monde extérieur. Il existe un nombre impressionnant d'interfaces possibles pour un routeur (Liaison série asynchrone, synchrone, Ethernet, ATM, FO, ...).

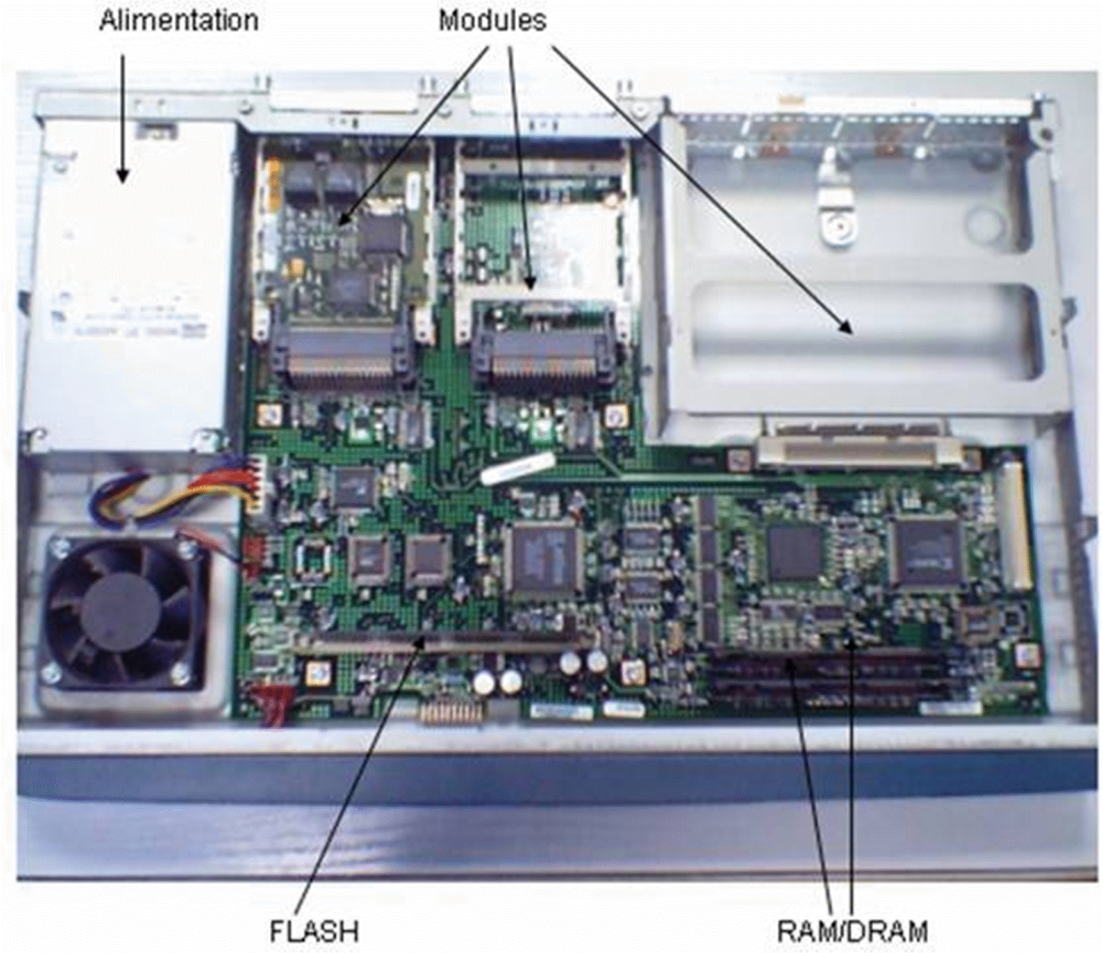

Figure 3-9 : Les composants d'un routeur

III.5) Le système d'exploitation IOS

III.5.1) L'architecture de l'IOS [16] [14]

IOS (*Internetwork Operating System)*, le système d'exploitation pour les connexions réseau) est le système d'exploitation produit par Cisco Systems et qui équipe la plupart de ses équipements. Gère le matériel, les interfaces Offre l'accès à un vaste éventail d'applications stratégiques de routage, multiservice, de modélisation de trafic, de sécurité/pare-feu et de contrôle du trafic etc.…

IOS est muni d'une interface en ligne de commande (accessible via Telnet, port série et SSH). IOS peut disposer d'une interface web.

Différentes versions de l'IOS sont utilisées sur la gamme de routeurs, de points d'accès Wifi et des commutateurs de la marque.

Ce système de description a comme particularité de prendre immédiatement chaque changement de configuration en compte. Il utilise deux espaces distincts pour stocker sa configuration :

- la **running-config**, typiquement stockée en mémoire vive (RAM) et qui contient la configuration actuellement utilisée ;
- la **startup-config**, typiquement stockée en mémoire non volatile (NVRAM) et qui contient la configuration au démarrage du matériel.

C'est pourquoi lors de la fin de la configuration de l'IOS il ne faut pas oublier de copier la **running-config** à l'intérieur de la **startup-config**.

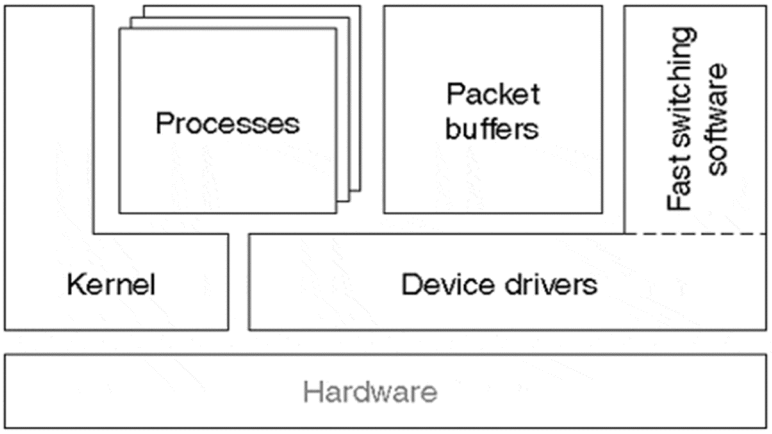

Figure 3-10 : architecture de l'IOS

- **Processes :** processus individuelles et des données associées qui effectuent des tâches, telles que la maintenance du système, de commutation de paquets, et la mise en œuvre des protocoles de routage.

- **Kernel** : le noyau fournit des services de base du système vers le reste de l'IOS, comme la gestion de la mémoire et l'ordonnancement des processus. Il fournit le matériel (CPU et mémoire) la gestion des ressources au processus.

- **Packet Buffers :** buffers de mémoire globale et leurs fonctions de gestion associés utilisés pour maintenir les paquets étant commutés.

- **Device Drivers :** fonctions qui contrôlent matériel de l'interface réseau et les périphériques (comme une carte flash). Interface des pilotes de périphériques entre les processus IOS, le noyau IOS et le matériel. Ils assurent aussi l'interface du logiciel de commutation rapide.

- **Fast Switching Software :** fonctions de commutation de paquets hautement optimisées.
Chacun de ces éléments, à l'exception des logiciels de commutation rapide, est examinée plus en détail dans les sections suivantes.

III.5.2) Les technologies de sécurité dans le Cisco IOS [21]

Le logiciel Cisco IOS peut délivrer de nombreuses fonctionnalités de sécurité, directement intégrées dans l'infrastructure, afin d'offrir une approche de sécurité complète en tous points du réseau.
Les services sécurité de l'IOS (par exemple sur les Routeurs à Services Intégrés) comprennent, entre autres :

- ✓ Des fonctions de firewall avec un outil de gestion graphique intégré puissant et simple.
- ✓ Des fonctions de prévention d'intrusions intégrant une inspection approfondie des paquets permettant de se prémunir de nombreux types d'attaques.
- ✓ Des fonctions de VPN SSL, directement intégrées dans les routeurs.
- ✓ Des fonctions de VPN IPSec. Basés sur le standard IPSec, Cisco propose de nombreuses architectures innovantes permettant de faciliter le déploiement et l'administration de réseau utilisant cette technologie, comme EasyVPN, Dynamic Multipoint VPN, ou encore GET VPN. Ces fonctions avancées permettent de réaliser l'infrastructure V3PN (voice, video-enabled VPN), supportant ainsi la convergence des données, de la voix et de la vidéo sur un réseau IPSec sécurisé avec qualité de service.

Conclusion

Dans ce chapitre on a vu les solutions IPS Cisco existantes et les critères du choix de la solution convenable à une entreprise. Nous pouvons désormais choisir la solution convenable à une entreprise.

Dans le chapitre qui suit nous allons étudier les caractéristiques et capacités de l'entreprise ENIEM, ses moyens, son architecture réseau et son personnel, pour lui choisir une solution IPS qui lui convient.

CHAPITRE 4:

Présentation de l'organisme d'accueil ENIEM

Introduction

On a vu dans le chapitre précédant les solutions IPS Cisco existantes sur le marché, et les critères selon lesquels on choisit une solution convenable pour une entreprise.

Alors dans ce chapitre on va étudier l'architecture du réseau local de notre organisme d'accueil ENIEM, ainsi que les moyens humains, matériels et logiciels existants et la capacité financière de l'entreprise. On finira par choisir la bonne solution qui répond aux maximums des besoins de sécurité.

IV.1) Présentation de l'ENIEM

ENIEM est une entreprise algérienne consacrée à la fabrication des appareils électroménagers (cuissons, climatiseurs, lave-linge, chauffages, ...), elle a été créé en 1974 en tant qu'une filiale de SONELEC avant qu'elle se transforme en une société par action en 1983 avec un capital social de 10 279.800.000 DA.

La compagnie dispose de plusieurs unités de productions dont les unités de froid, cuisson et climatisation sont implantées à la zone industrielle d'Oued-Aissi alors que son siège social se situe à Tizi-Ouzou. L'unité sanitaire est installée à Miliana wilaya d'Ain Defla et la filiale Lampes de Mohammedia à la wilaya de Mascara.

L'ENIEM est la première entreprise du Maghreb à être certifiée par ISO depuis 1998 par les experts de l'association française de l'assurance de la qualité (AFAQ), puis graffiti en 2003 de l'ISO. Les produits de l'ENIEM sont 0% CFC (Chlora Fluora Carbones) depuis 1997.

Figure 4-1 : image correspond ENIEM de l'intérieur et de l'extérieur

IV.1.1) Missions et objectifs :

La mission de L'ENIEM est d'assurer la production, le montage, la commercialisation, le développement et la recherche dans les différentes branches de l'électroménager.

Son objectif est améliorer la qualité des produits, les capacités d'études et développement et augmenter le volume de production et les taux d'intégration interne et externe**.**

IV.1.2) Organisation générale de l'ENIEM:

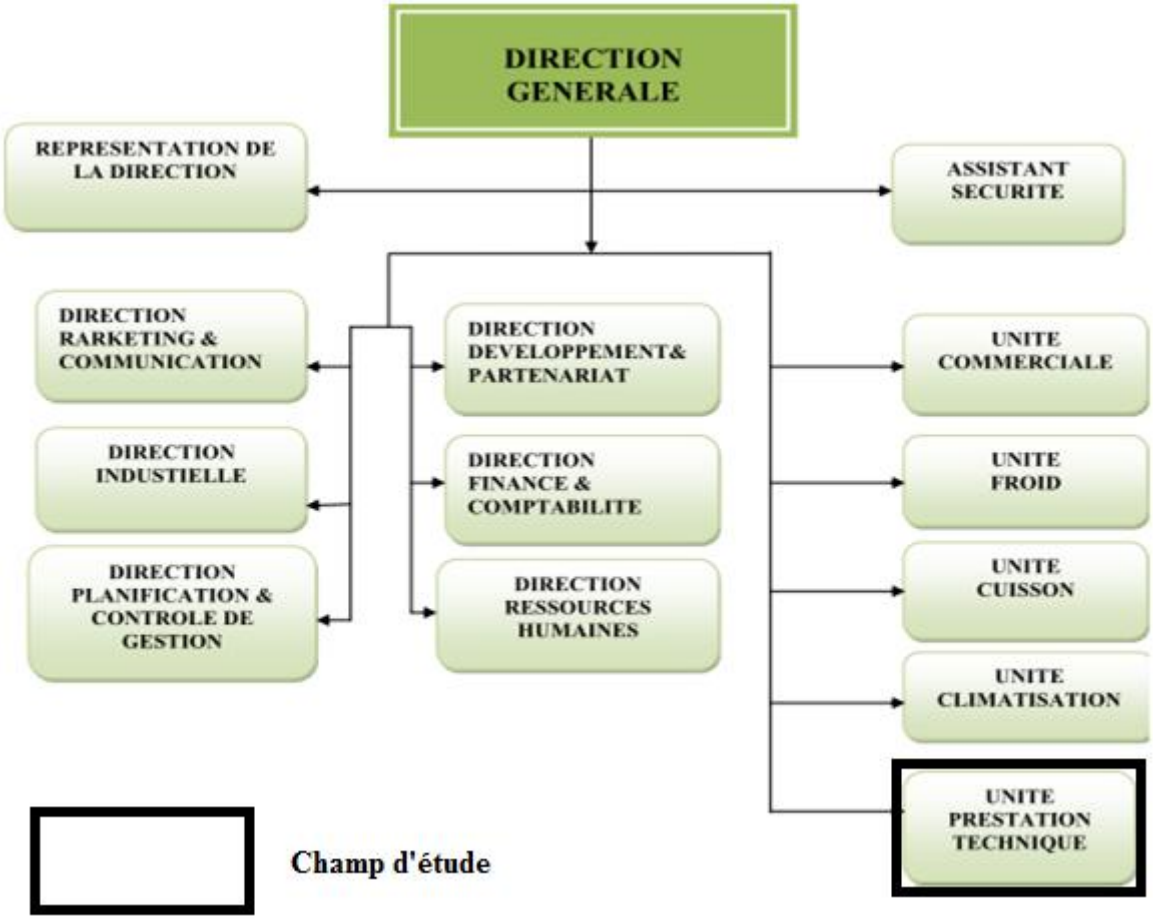

Figure 4-2 : Organisation générale d'ENIEM

ENIEM est organisée en directions et unités suivantes :

IV.1.2.1) Les directions :

- ✓ **Direction générale :** La direction générale est l'unique entité qui est responsable de la stratégie et du développement de l'entreprise. Elle exerce son autorité hiérarchique et fonctionnelle sur l'ensemble des directions et unités.

- ✓ **Direction planification et contrôle de gestion :** La direction assure le contrôle de gestion. De l'audit finance ainsi que le budget de l'entreprise.

- ✓ **Direction développement et partenariat** : Cette direction assure l'étude et le développement du produit fini ainsi que des actions de partenariat et de sous-traitance.

- ✓ **Direction des finances et comptabilité :**Elle a pour rôle l'analyse des équilibres financiers de l'entreprise et la tenue de la comptabilité.

- ✓ **Direction du marketing et la communication :** Cette direction assure des politiques commerciales et de communication et les met en œuvre par la conception et l'élaboration des méthodes et outils de gestion nécessaires.

- ✓ **Direction industrielle** : La direction industrielle est chargée de développer et de mettre en place les moyens et l'organisation industrielle nécessaire à la réalisation de la production en agissant sur les approvisionnements, les moyens et les techniques de production.

- ✓ **Direction des ressources humaines :** Elle pilote le recrutement, l'accueil, l'information et gère le plan de carrière du personnel et les pouvoirs publics.

IV.1.2.2) Les unités de production:

- ✓ **Unité froid :**elle produit des réfrigérateurs petits modèles à une capacité de 110.000 réfrigérateurs par an, dont les modèles sont fabriqués sous licence BOSCH Allemagne 1977, grands modèles à une capacité de 390.000 réfrigérateurs par an fabriqués sous licence TOSHIBA- JAPON6-1987 et des congélateurs bahut et réfrigérateurs de 520 L à une capacité de 60.000 appareils par an sous licence LEMATIC-Liban- 1993.

- ✓ **Unité Cuisson:** Elle assure la production des cuisinières, et les capacités installées sont de 150000 cuisinières par an fabriquées sous licence TECHNO GAZ- Italie – 1991.

- ✓ **Unité Climatisation:** Les capacités existantes sont de 60.000 climatiseurs par an sous Licence AIWELL - France 1977.

- ✓ **Unité Commerciale :** Son activité et la distribution et l'exportation des produits ENIEM et le service après-vente.

- ✓ **Unité Prestations Techniques :** Cette unité assure les fonctions de soutien aux unités de production dans les domaines de réparation des outils et moules, Fabrication de pièces de rechange mécanique, Conception et réalisation d'outillages, Gardiennage et sécurité, Travaux d'imprimerie et Prestation informatique.

IV.2) Présentation du champ d'études :

Cette partie nous permettra de mieux définir le domaine d'étude « l'unité prestation technique » et de mieux apercevoir ses objectifs, elle nous aidera aussi à relever les éventuels manques et anomalies dans le système existant dans notre champ d'étude qui est l'unité de prestation technique.

IV.2.1) Organigramme de l'unité prestation technique :

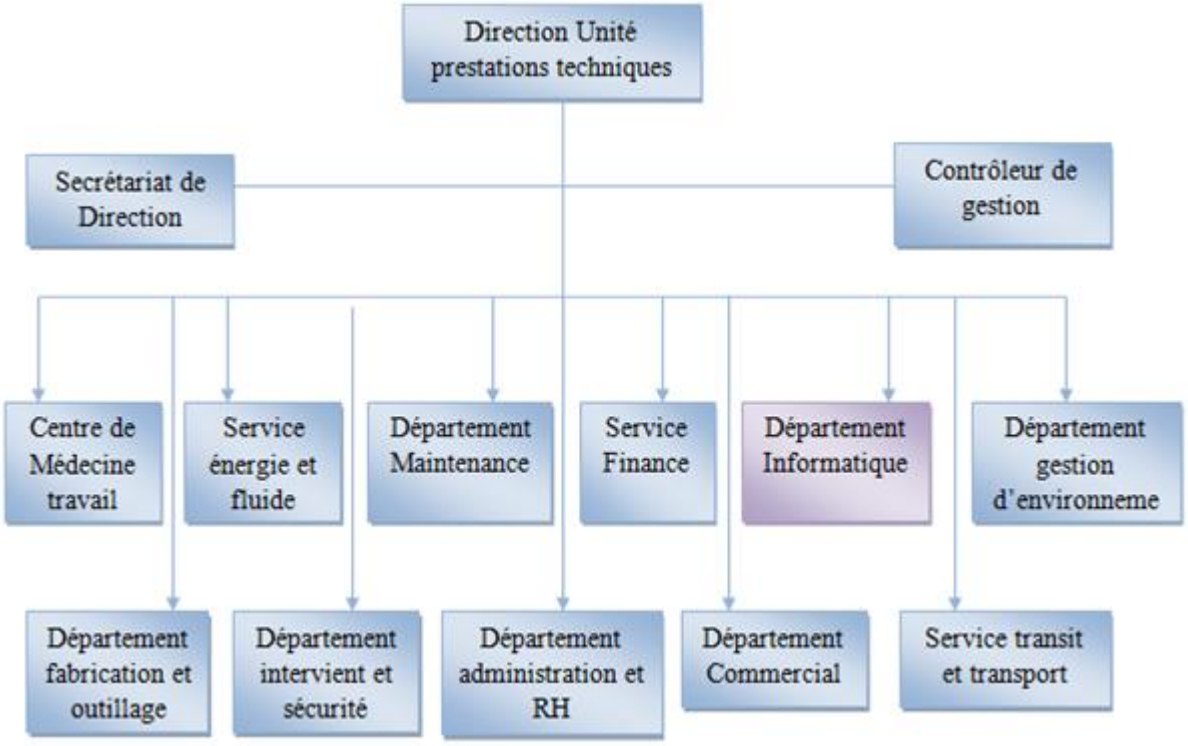

Figure 4-3 : Organigramme de l'unité prestation technique

IV.2.2) Caractéristiques du réseau informatique de l'ENIEM :

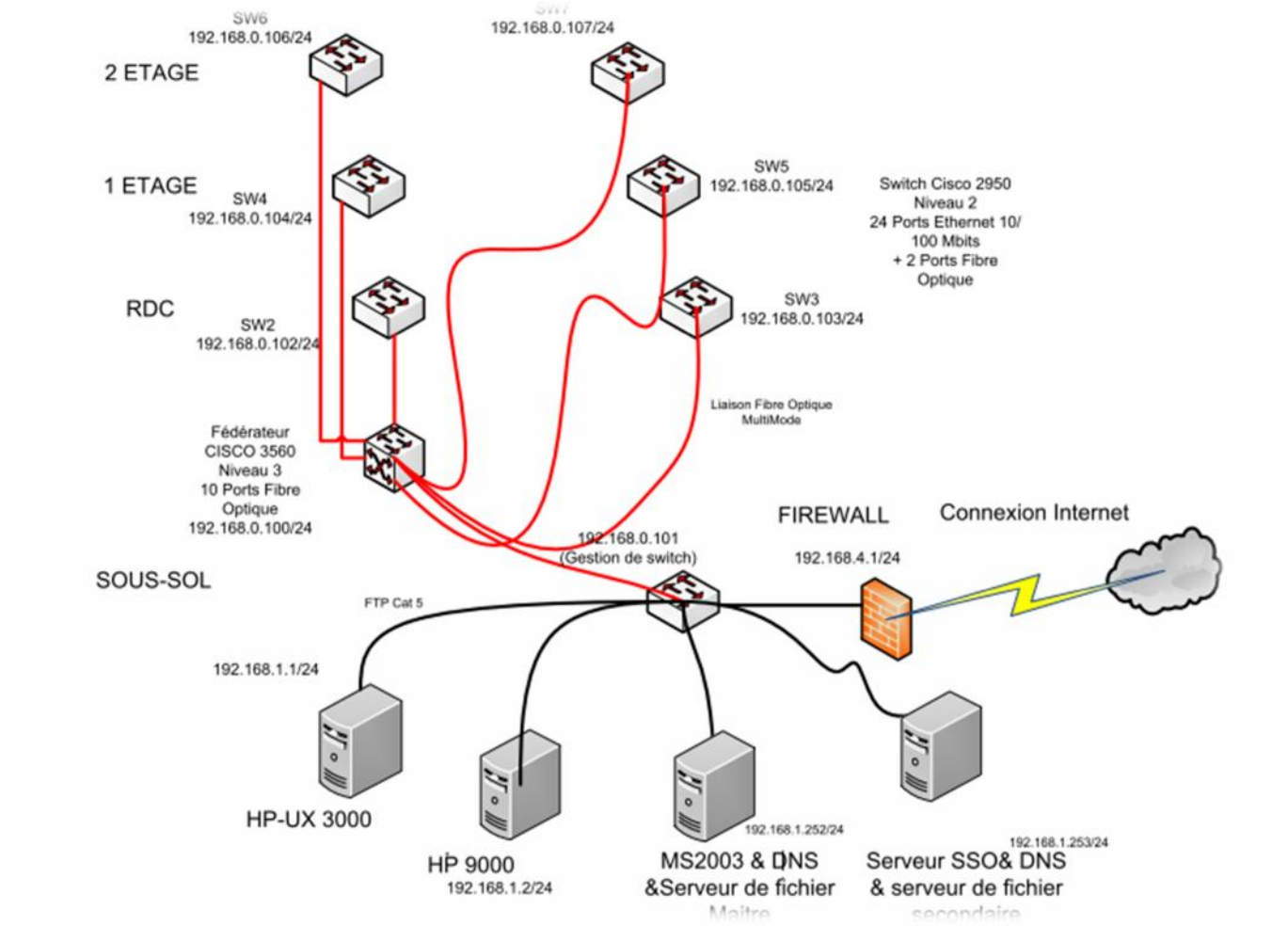

Figure 4-4 : Architecture du réseau local ENIEM

Le réseau LAN de ENIEM utilise les techniques de communication d'Internet (adressage IP, serveurs http, etc), et il est constitué de :

- ✓ **Un Serveur HP-UX 3000:**relié à 39 terminaux, dont 27 écrans et 12 imprimantes, par des liaisons directes, modem (pour les distances supérieures à 1200mètres), et multiplexeur modem (pour les installations de plusieurs terminaux distants). Il contient la base de données des applications client/serveur et d'autres fichiers partagés.
- ✓ **Un Serveur HP 9000:** successeur du serveur HP-UX 3000, il est prévu pour la gestion de paie, mais pas encore exploité.
- ✓ **Un Serveur MS2003 et DNS:** serveur primaire
- ✓ **Un Serveur SSO et DNS:** serveur secondaire
- ✓ **Pare-feu de type PIX:** ancienne version
- ✓ **Débit de la connexion internet :**2 Mbits/s
- ✓ **7 Switch :** le réseau possède :

- 6 Switch de type Cisco 2950 niveau 2 chacun possède 24 ports Ethernet, 10/100 Mbs et 2 ports fibre optique pour la liaison avec le Switch fédérateur.
- 1 Switch fédérateur de type Cisco 3560 de niveau 3, il possède 10 ports fibre optique pour relier les 6 Switch Cisco 2950 avec les ports de fibre optique

La topologie choisie pour le réseau local est celle dite étoile, vue la configuration du site, à savoir : deux bâtiments en formes de T.

Le schéma général du câblage est défini selon le nombre de bureaux et le nombre d'utilisateurs par bureau.

Tous les bureaux sont dotés d'au moins une prise. Il en existe en tous 170prises (actuellement il n'y a que 65 micro- ordinateurs connectés). Tous les ordinateurs d'un même étage avec ses différentes unités et fonctions sont reliés à un Switch contenu dans une armoire, cette dernière est reliée par un câble fibre optique à un Switch dit fédérateur contenu dans l'armoire centrale installée au niveau de la salle machine au sous-sol du bâtiment B.

Le réseau est composé de 06 armoires départagées dans 03 bâtiments, une à chaque étage. L'emplacement est dicté par la distance maximale entre un Switch et un poste de travail, qui ne doit pas dépasser 100 mètres.

IV.2.3) L'aspect logiciel des composants du réseau :

Les différents logiciels utilisés :

- ✓ **Réflexion x :** est un émulateur d'accès au serveur depuis les différentes fonctions.
- ✓ **EASY** : est une application installée dans le serveur pour gérer la comptabilité des différentes unités.
- ✓ **COBOL :** L'engage de programmation avec lequel toutes les applications opérationnelles sont développées.
- ✓ **ACPAE** : Gestion de la paie (calcul de la paie).
- ✓ **Système MM0909 :** pour la pièce de recharge.
- ✓ **Système MM ref :** gestion de la production pour l'unité froid.
- ✓ **Système MM cuis** : gestion de la production pour l'unité cuisson.
- ✓ **Système achat :** tout ce qui est relatif à la fonction achat.
- ✓ **Système MM3000 pour la gestion de production :** il se charge de la production et tenue du stock des matières premières et pièce de recharges.
- ✓ **Gestion de la comptabilité** : on trouve la comptabilité clients, fournisseurs, générale, analytique, budget et d'autres.
- ✓ **Windows server 2008** installé sur les serveurs
- ✓ **Windows 7et Windows XP :** les 2 systèmes d'exploitation utilisés pour les autres machines des utilisateurs.

IV.2.4) L'aspect humain du département informatique

Chef de département: Anime et contrôle tous les travaux de conception, de mise en place, maintenance et de développement des systèmes de gestion informatique des unités.

Chef de service exploitation: Il veille sur la gestion d'ensemble de moyens informatique de saisie, de traitement de transmissions et de restitutions de l'informatique assiste les utilisateurs et intervient sur les incidents.

Agent maintenance et réseau informatique: Surveille le réseau et maintient la machine dans un état propre.

Le gestionnaire de système d'exploitation: Procède au chargement des énergies (air conditionné électricité via onduleur) des ordinateurs et du système d'exploitation.

Chef de service développement système informatique : La tâche de ce poste consiste à assurer la maintenance des différents systèmes et leurs adaptations aux exigences nouvelles. Elle assure également le développement de nouveaux systèmes conformément au plan informatique.

Administrateur système informatique : (stock, pièce de rechange, gestion personnelle, etc) : assure l'analyse organique de l'étude, à savoir l'élaboration de la solution qui a été retenue par:

- ✓ Une reprise de la chaîne fonctionnelle pour la découper en unité de traitement qui correspond à des programmes définissants pour chacune d'elles, un monde de stockage des programmes, fichiers, etc. et de l'enchaînement des opérations à effectue r(chaine organique).
- ✓ La confection de dossier d'exploitation définissant les conditions

Administrateur système informatique: Assure l'analyse fonctionnelle du projet conformément au planning de réalisation préétabli par hiérarchie

IV.3) Critiques des systèmes de sécurité

Après avoir fait une étude mené sur les différents services de l'organisme d'accueil, L'ENIEM est une entreprise bien organisée et possédant une bonne structure fonctionnelle. Cependant, nous avons pu tirer quelques anomalies dans leurs systèmes de sécurité qui est un point non négligeable de nos jours, on site :

- Un pare-feu de type PIX ancienne version.
- L'accès des utilisateurs à internet n'est pas sécurisé.
- Les paquets échangés entre les utilisateurs eux même et internet ne sont pas chiffrés
- Les serveurs de données ne sont pas sécurisés contre les attaques interne ni externe, surtout avec la possibilité d'accès de l'internet.
- Non existence des systèmes de sécurité contre les attaques comme VPN, Proxy, IPS et autres.
- Quelques utilisateurs utilisent le système d'exploitation XP, celui-là ne possède plus maintenant des mises à jours, alors c'est une proie aisée pour les pirates.
- Le réseau ne possède pas un routeur mais un Switch à option de routage qui n'admet pas des mesures de sécurité.

IV.4) Solution proposée

Le réseau informatique et les serveurs de données dans l'ENIEM ne sont pas bien sécurisés, il y a un grand risque d'être espionnée ou piratée, surtout avec l'existence des concurrents.

Pour trouver une solution qui répond à plusieurs problèmes cités précédemment, notamment la non existence des systèmes de sécurité contre les attaques comme le système de prévention d'intrusions, nous proposons une solution de niveau moyen qui est l'utilisation d'un Routeur à Services Intégrés ISR de Cisco. Ce dernier possède un système IOS qui donne des services de sécurité dont ENIEM a besoin. Nous choisissons la gamme 3900car elle a plus de performance et les services nécessaires pour le bon fonctionnement du réseau de cette entreprise.

Fiche technique sur la gamme Cisco 3900

La gamme Cisco 3900 propose deux plates-formes (Figure 4-5) : les routeurs à services intégrés Cisco 3925 et 3945.

Tous les routeurs de cette gamme intègrent l'accélération matérielle des fonctions de chiffrement, des slots pour DSP compatibles voix et vidéo, le traitement des appels, la messagerie vocale et des services d'applications. En outre, ces plates-formes prennent en charge l'éventail le plus complet du marché en termes de connectivité filaire et sans fil, telles que T1/E1, T3/E3, xDSL et Gigabit Ethernet cuivre ou fibres optiques. Cette gamme supporte les versions 15M&T du logiciel Cisco IOS.

Il embarque grâce à son système d'exploitation IOS plusieurs fonctions de sécurité dans un même équipement:

- ✓ VPN site à site, VPN d'accès distant IPsec et SSL
- ✓ Firewall de niveau applicatif, filtrage d'URL
- ✓ Système de prévention des intrusions en ligne
- ✓ Contrôle d'Admission au Réseau (NAC) et administration sécurisée.

Le déploiement de ces services s'opère à moindre coût sans ajout de matériel spécifique.

Figure 4-5 : la gamme Cisco 3900

Les modules de services et cartes d'interface :

La gamme Cisco 3900 propose des fonctionnalités modulaires améliorées de manière significative (figure 4-6) constituant pour les clients un investissement sûr et protégé. La plupart des modules disponibles pour les générations précédentes sont pris en charge par la gamme Cisco 3900. De plus, on peut utiliser ces modules sur d'autres plates-formes Cisco les supportant. On cite les modules utilisés par cette gamme :

- ✓ **EHWIC(carte d'interface WAN haut débit optimisée):**Cartes d'interface (WAN ou LAN)
- ✓ **ISM(Module de Service Interne):**Module interne pour exécuter des services qui ne requièrent pas de ports d'interface, d'unité centrale et de mémoire dédiées.
- ✓ **SM (Module de Service):**Unité centrale et mémoire indépendantes pour l'hébergement de services *ou* ports d'interface à haute densité.
- ✓ **PVDM3(Packet Voice Digital Signal Processor (DSP) Module) :**Modules vidéo et à contenu multimédia haute densité

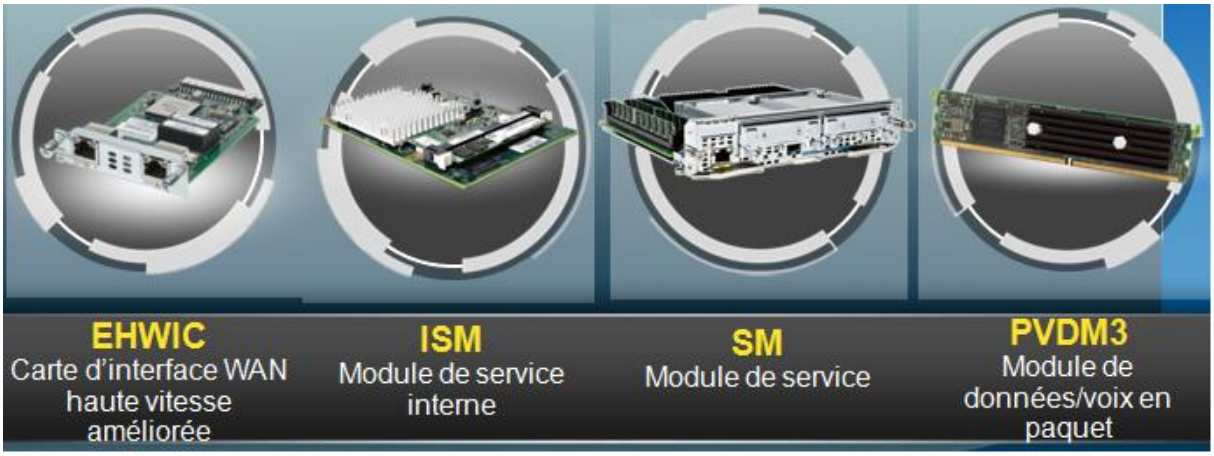

Figure 4-6 : Les modules de services et cartes d'interface

Spécifications des modèles Cisco 3925 et 3945

Services et densité des slots	Cisco 3925	Cisco 3945
Nombre total de ports WAN LAN 10/100/1000 intégrés	3	3
Ports RJ-45 (3 sur 3 ports)	3	3
Ports SFP (désactive un port RJ-45 - 2 sur 3 ports)	2	2
Slots SM	2	4
Slots EHWIC	4	4
Slots ISM	2	2
Slots (PVDM) de DSP intégrés	2	2

Mémoire DDR2 ECC DRAM	1-2 Go	1-2 Go
Compact Flash (externe) par défaut	Slot 0 : 256 Mo Slot 1 : aucune	Slot 0 : 256 Mo Slot 1 : aucune
Compact Flash (externe) maximum	Slot 0 : 4 Go Slot 1 : 4 Go	Slot 0 : 4 Go Slot 1 : 4 Go
Slots USB 2.0 externes (type A)	2	2
Port de console USB (Type B) (jusqu'à 115,2 Kbits/s)	1	1
Port de console série (jusqu'à 115,2 Kbits/s)	1	1
Port auxiliaire série (jusqu'à 115,2 Kbits/s)	1	1

Figure 4-7 : Spécifications des modèles Cisco 3925 et 3945

Conclusion

Dans ce chapitre nous avons présenté l'entreprise ENIEM précisément son architecture, nous avons critiqué ses moyens de sécurité de réseau, ensuite on lui a proposé une solution Cisco.

Dans le chapitre suivant, nous allons présenter l'implémentation de cette solution et nous allons tester son fonctionnement dans le simulateur GNS3.

CHAPITRE 5:

Implémentation du IOS IPS Cisco

Introduction

Apres avoir choisi et présenté notre solution IOS IPS Cisco, nous allons dans ce qui suit présenter les différentes étapes suivies de son implémentation avec des captures d'écran illustratives. Toute fois avant cela on doit présenter les outils que nous avons utilisés pour la réalisation de notre solution ainsi que l'environnement sur lequel elle repose.

V.1 Présentation des outils utilisés

V.1.1 Le simulateur graphique de réseaux GNS3

Dans le but de se rapprocher le plus possible de la mise en place d'une architecture réseau réelle, nous avons opté pour l'utilisation de GNS3 1.3.4 (Graphical Network Simulateur). Un logiciel open source et multi-plates-formes (Mac OS X, Windows et Linux) qui est à la fois simulateur et émulateur, simulateur de réseaux LAN et WAN et émulateur de routeurs et firewalls CISCO. Autant que simulateur il imite le comportement de l'équipement, comme émulateur il exécute directement le système d'exploitation de l'équipement, ce qui permet d'assurer les mêmes résultats dans le cas réel.

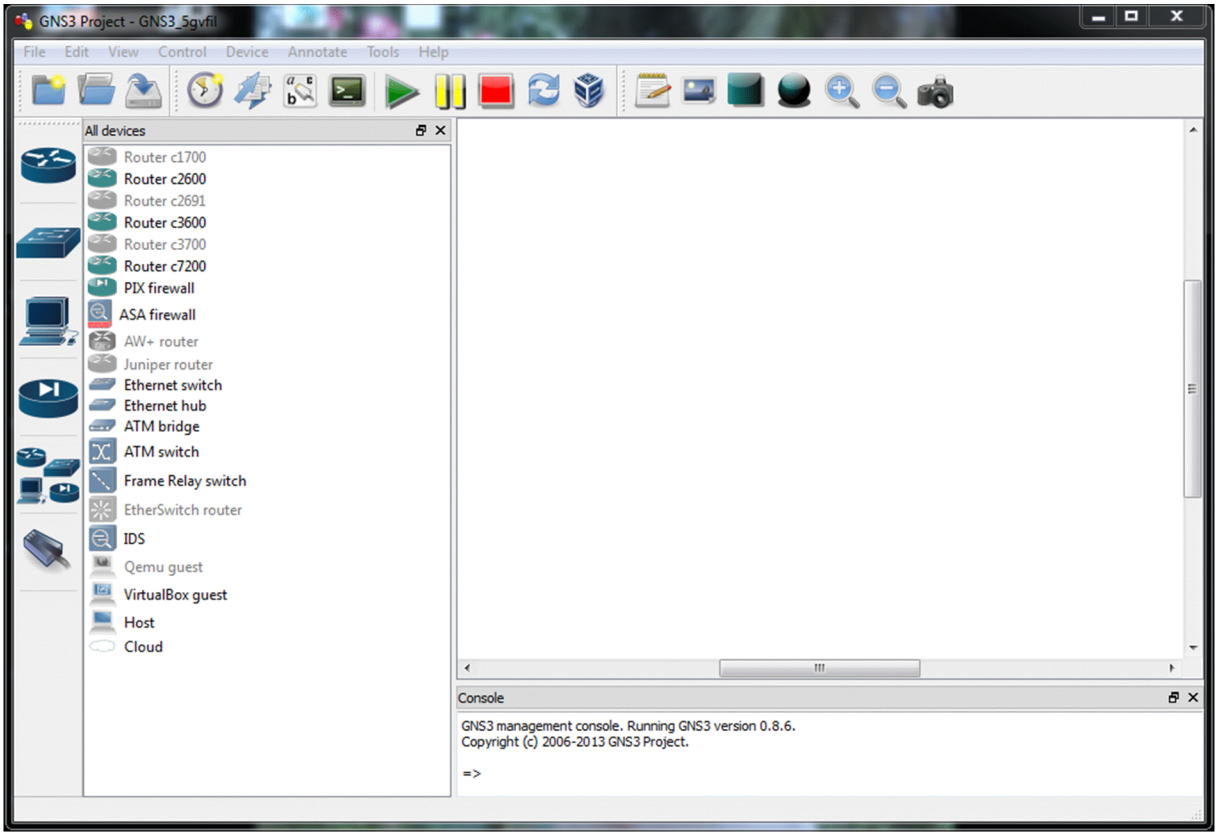

Figure 5-1: L'interface de travail de GNS3

V.1.2. Virtual Box 4 .3.1

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la Virtual Box 4.3.1. Cette dernière permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation, ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique. Cette version exécute les applications les plus exigeantes, elle utilise le dernier matériel pour répliquer l'environnement des serveurs postes de travail tout en étant accessible de n'importe quel périphérique grâce à son interface Web.

Figure 5-2: Virtual Box 4.3.1.

V.1.3 Server syslog

Syslog est un mécanisme de journalisation dans des dispositifs de réseau (Cisco Network équipements, des serveurs Unix, serveurs GNU / Linux etc…) utilisé pour collecter les journaux système qui contient des informations essentielles sur l'état, erreurs, avertissement, journaux de configuration, etc., des dispositifs. Cisco Routeurs et commutateurs utilisent Syslog pour le suivi des logs et des alertes systèmes.

Cisco IOS IPS génèrent des alarmes lorsqu'une signature active est déclenchée. Ces alarmes sont stockées sur le capteur et peuvent être consultés sur place. Lors de la détection d'une attaque, la fonctionnalité Cisco IOS IPS peut envoyer un message syslog ou une alarme de format SDEE (Secure Device Event Exchange), comme il est montré dans la figure suivante :

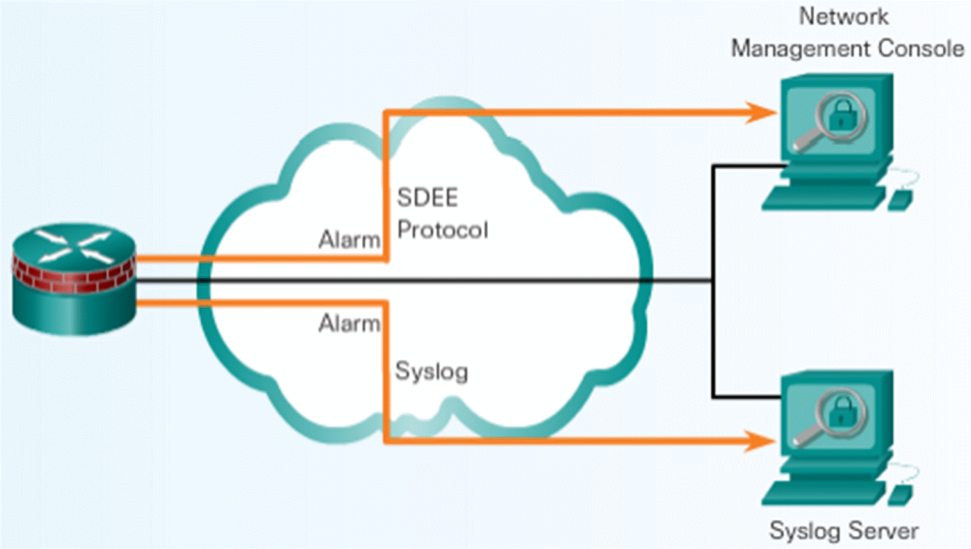

Figure 5-3 : La surveillance d'un IPS

Le protocole SDEE a été développé pour améliorer la communication des événements générés par les dispositifs de sécurité. Il est destiné à être extensible. Cisco IOS IPS peut surveiller syslog et événements SDEE générés et de garder trace des alarmes qui sont communs dans les messages du système de SDEE, y compris les alarmes de signature IPS. Un message d'alarme du système de SDEE a le type de format suivant:

<Date_time_stamp>% <facility> - <gravité> - <mnémonique>: <texte_message>

Exemple :

Sep 14 14 :09 :09 % IPS-4-signature: Sig: 1107 Subsig: 0 Sev: 2 adresse RFC1918 [192.168.121.1:137 -> 192.168.121.255:137]

Une description plus détaillée du format du message Syslog est illustré ci-dessous :

Syslog message Element	**Description**
<Date_time_stamp>	Utilisé pour enregistrer la date et l'heure du message Syslog. <Date_time_stamp> a généralement le format suivant: "mm / jj hh: mm: ss".
<Facility>	Contient le nom de l'équipement ayant généré le message syslog
<Gravité>	La gravité est utilisée pour spécifier le niveau de gravité du message Syslog utilisant un nombre entier compris entre 0 et 7. Suite et les

	messages Syslog entiers et de leur signification. 0 - urgence (système est inutilisable) 1 - alerte (mesures doivent être prises immédiatement) 2 - critiques (conditions critiques) 3 - Erreur (conditions d'erreur) 4 - Avertissement (conditions d'avertissement) 5 - Avis (condition normale, mais importante) 6 - information (messages d'information) 7 - Debug (messages de niveau de débogage)
<Mnémonique>	<Mnémonique> identifie de façon unique le message Syslog.
<Texte_message>	<Texte_message> est le texte qui décrit le message Syslog et peut contenir des détails sur le message Syslog.

Figure 5-4 : description détaillée du message syslog

Dans notre cas on a utilisé le **3CDaemon** comme serveur syslog, ayant l'interface principale suivante:

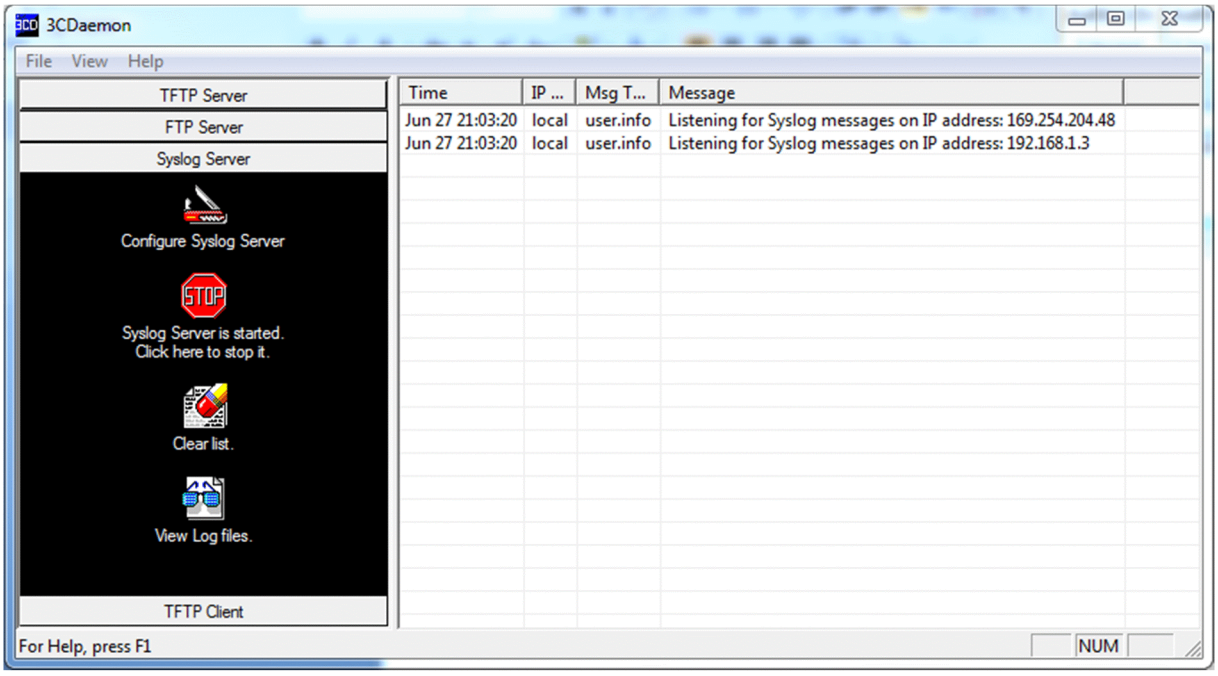

Figure 5-5: Interface du serveur syslog de 3CDaemon

V.1.4 Backtrack 5 r3

BackTrack : est une distribution Linux, Son objectif est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un réseau. Depuis 2013, Backrack est devenu Kali Linux .Il inclut de nombreux logiciels comme wireshark ,nmap…….etc.

Dans notre cas on a utilisé **nmap** qui est un scanneur de ports open source, qui existe aussi en mode graphique sous le nom « Zenmap GUI », qui est conçu pour détecter les ports ouverts, identifier les hôtes, les services hébergés et les informations sur le système d'exploitation d'un ordinateur distant. Dans le but de solliciter des réponses de la machine cible pour montrer la présence ou non d'une application ou d'un service et rechercher les serveurs non autorisés, ou pour les ordinateurs qui ne sont pas conformes aux normes de sécurité.

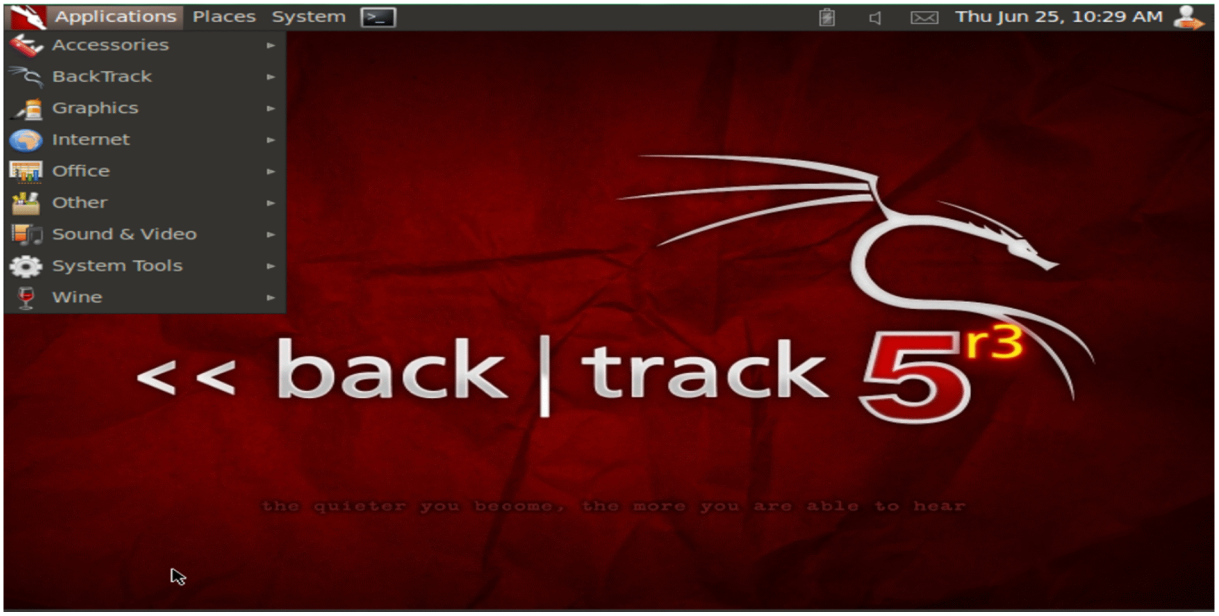

Figure 5-6: Backtrack 5 r3

V.1.5 Les protocoles utilisés :

On a utilisé deux protocoles pour effectuer le routage entre les éléments de notre architecture qui sont : **OSPF** et **NAT.**

V.1.5.1 Le protocole OSPF (Open Shortest Path First):

Le protocole (OSPF) est un protocole de routage d'état des liaisons qui utilise le concept de zones pour son évolutivité. Il a été développé suite au besoin de la communauté Internet d'utiliser un protocole intérieur IGP (Internal Gateway Protocol) dans la pile des protocoles TCP/IP, non-propriétaire et hautement fonctionnel. Ce protocole est de couche 3, basé sur l'algorithme de Djikistera, annoncé dans le paquet IP avec le numéro de protocole 89.

V.1.5.2 Le protocole NAT (Network Address Translation):

Il se base sur le mécanisme de translation d'adresses .Il consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau interne et au moins une interface réseau connectée à Internet (possédant une adresse IP routable), pour connecter l'ensemble des machines du réseau.

Il existe plusieurs types de translations NAT qui sont :

- ✓ **Le NAT statique :** permet d'associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) fait la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

- ✓ **Le NAT dynamique :** permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP.

- ✓ **Le PAT(Port Adress Translation) :** c'est l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.

V.2. Implémentation de l'IOS IPS

V.2.1. La nouvelle architecture de l'ENIEM

La mise en place de notre politique de sécurité se concentre sur La DMZ et le réseau interne. La DMZ contient l'ensemble des serveurs de notre entreprise étant susceptibles d'être accédées depuis l'Internet ou du réseau interne par des personnes qui n'ont pas l'autorisation d'accès. Donc pour garantir la sécurité de ces serveurs et du réseau interne, on doit configurer l'IPS de sorte que les paquets qui seront analysés seront ceux entrants de l'extérieur et réseau interne vers les serveurs et ceux entrants de l'extérieurs vers le réseau interne.

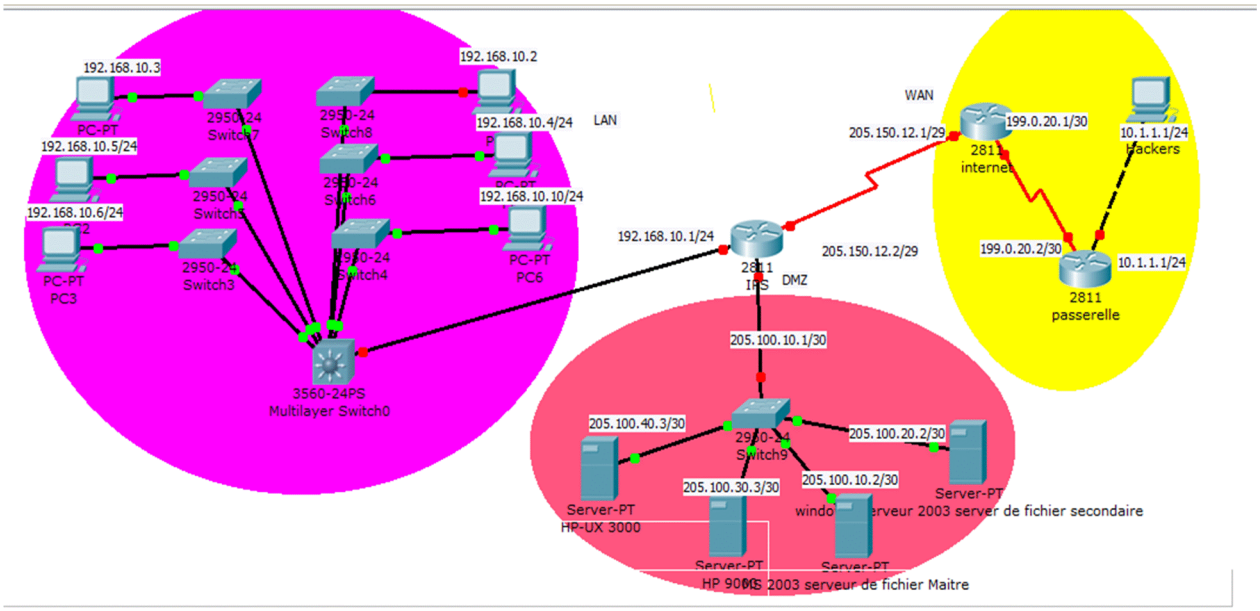

Figure 5-7: la nouvelle architecture ENIEM après l'ajout du routeur

Vu qu'il n'est pas important de simuler sur GNS3 toute l'infrastructure réseau de l'entreprise ENIEM pour tester la solution IPS. Nous avons simplifié l'architecture aux nécessaires seulement, comme le montre la figure suivante :

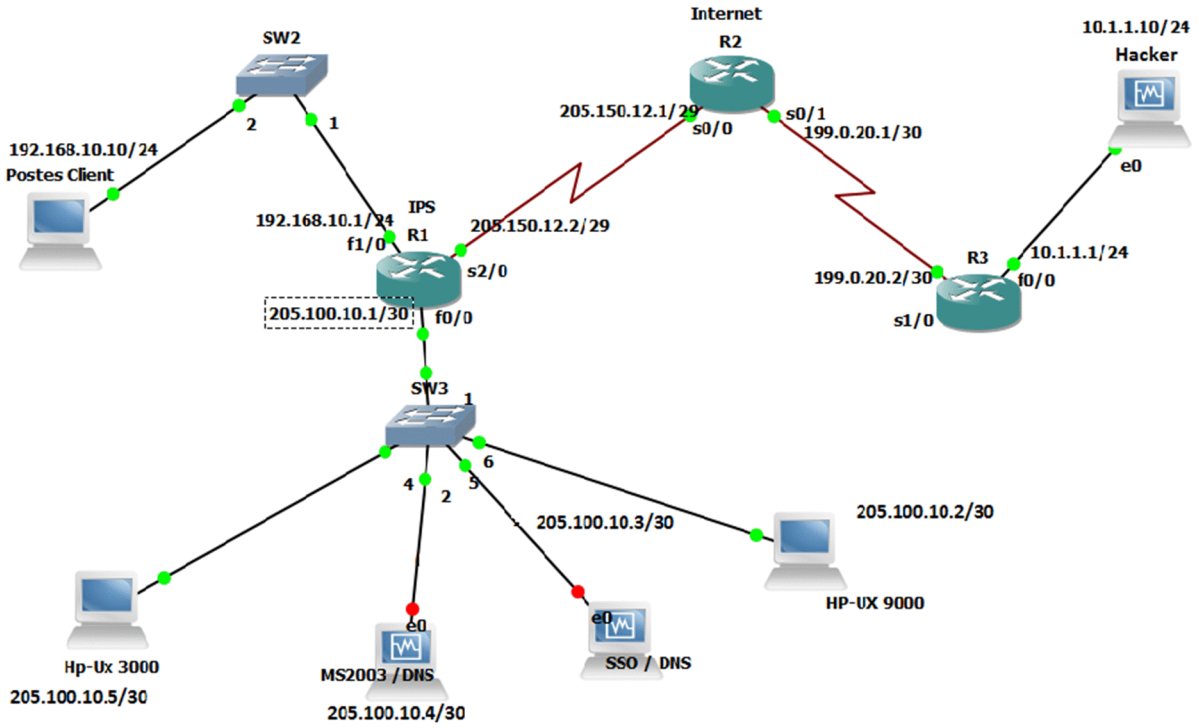

Figure 5-8: l'architecture simplifiée du réseau sur GNS3

Dans ce qui suit, nous présentons les différentes étapes à suivre pour la configuration de l'IOS IPS

V.2.2. Configuration du routeur

V.2.2.1. Les méthodes utilisées pour la configuration d'un routeur:

Les deux méthodes les plus utilisées pour configurer l'IPS CISCO sont**:**

- La première méthode se fait à l'aide de **CCP (Cisco configuration professionnel)** qui est un outil de gestion de périphérique de l'interface graphique à base de routeurs d'accès Cisco qui permet des configurations de réseau local grâce à des assistants à interface graphique. CCP est un outil précieux qui améliore la productivité pour les administrateurs réseau et les partenaires de distribution pour le déploiement de routeurs avec une confiance accrue et une utilisation facile. Il surveille également l'état du routeur. CCP est téléchargeable gratuitement.

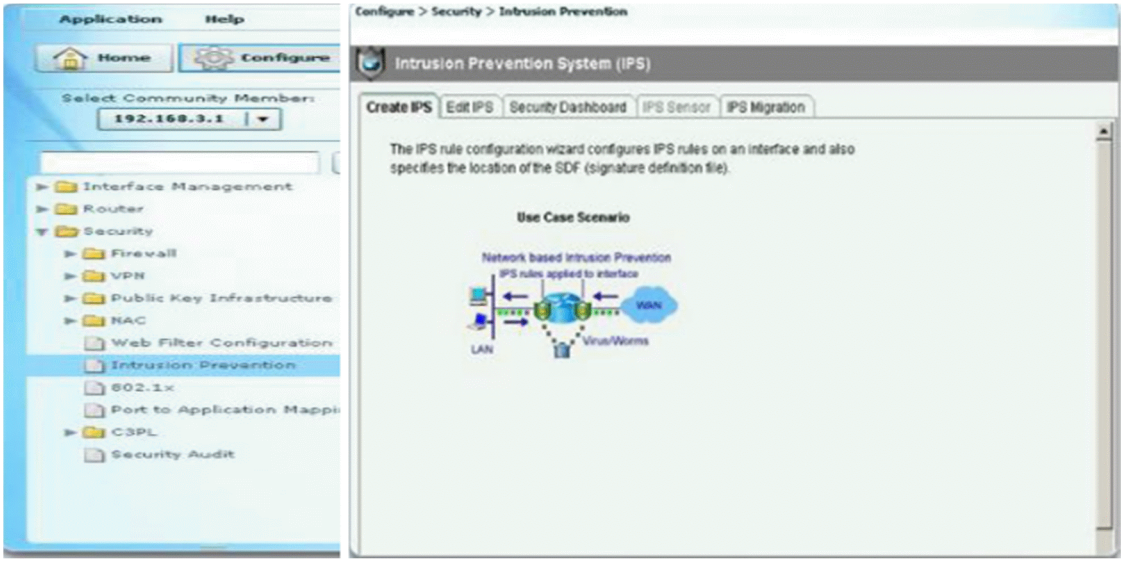

Figure 5-9 : interface graphique de CCP

- La deuxième méthode se fait à l'aide de **CLI (command line interface)** : qui permet la configuration du router à travers une interface de ligne de commandes.
  Pour notre cas on a choisi cette méthode, afin de suivre d'une manière détaillée les commandes à taper pour la configuration du routeur.

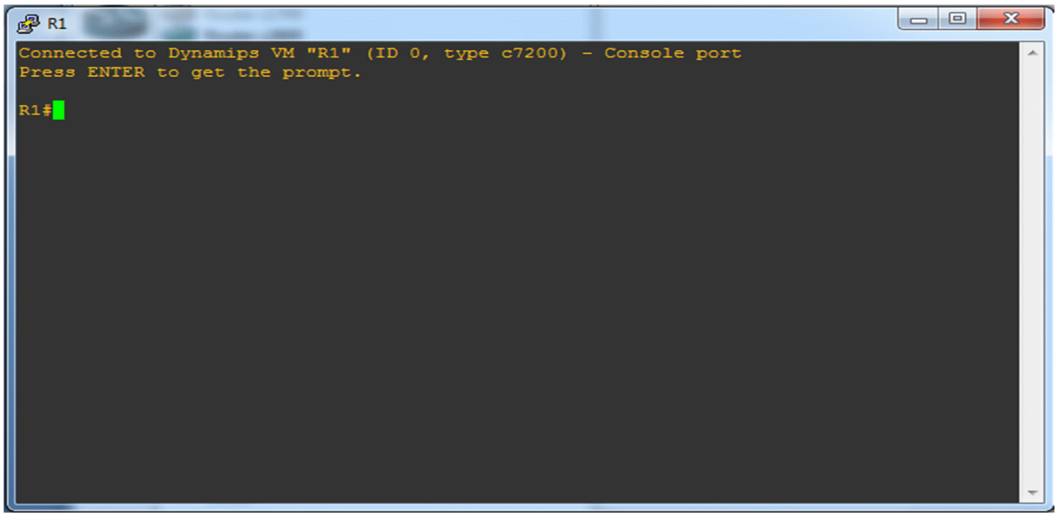

Figure 5-10: l'interface de commandes CLI

V.2.2.2 Configuration de base du routeur

Voici les principales commandes de bases à taper pour utilisation d'un routeur :

- **Attribution d'un nom au routeur :** se fait à l'aide de la commande **Hostname**
- **Chiffrement de mot de passe, nom d'utilisateur et le privilège se fait à l'aide de la commande : username privilege[0-15] password**
  - ✓ **username :** qui permet d'associer un nom d'utilisateur qui est **cisco** dans notre cas.
  - ✓ **privilege :** qui permet d'empêcher n'importe qui d'accéder à des services statiques. L'IOS Cisco permet toutefois de définir des tables d'utilisateurs et de leur accorder jusqu'à 16 niveaux (de 0 à 15) de privilèges (définir, par exemple, les commandes accessibles par privilège). Lorsque les services sont restreints par défaut, c'est le plus haut niveau qui est défini (15).
  - ✓ **password (mots de passe) :** qui permet de sécuriser l'accès à notre routeur qui est dans notre cas **1234**
- **La commande ip http server :** permet de sécuriser le server http
- **La commande ip http secure server :** permet de sécuriser le server https
- **La commande ip http authentication local :** Pour spécifier une méthode d'authentification particulière pour les utilisateurs du serveur http
- **Les commandes line vty et transport input telnet ssh :** Permettent d'autoriser uniquement des connexions SSH et Telnet sur les 4 consoles définies (vty 0 3)
- **La commande copy running-config startup-config** : pour l'enregistrement des modifications apportées à notre routeur

La figure ci-dessous montre toutes ces commandes :

```
R1(config)#hostname IPS
IPS(config)#username cisco privilege 15 password 1234
IPS(config)#ip http server
IPS(config)#ip http secure-server
IPS(config)#ip http authentication local
IPS(config)#line vty 0 3
IPS(config-line)#privilege level 15
IPS(config-line)#transport input telnet ssh
IPS(config-line)#exit
IPS(config)#exit
IPS#copy running-config startup-config
*Jun 26 00:13:52.608: %PKI-4-NOAUTOSAVE: Configuration was modified.  Issue "write memory" to save new certificate
IPS#copy running-config startup-config
*Jun 26 00:13:52.628: %SYS-5-CONFIG_I: Configured from console by console
IPS#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

On commence d'abord par la vérification de la connectivité entre tous les éléments de notre architecture:

Tout d'abord on doit vérifier les connectivités de R1 vers R2, R2 vers R1, R3 vers R2, R2 vers R3, serveur primaire vers R2, de serveur secondaire vers R2 et de réseau local vers R2, R3 et R1. Et on doit avoir une réponse comme la montre la figure ci-dessous :

R1 vers le server primaire :

```
IPS#ping 205.100.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.100.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/18/36 ms
```

Ce n'est pas possible d'établir une connectivité entre les serveurs et l'internet, les postes clients et l'internet. Donc afin d'atteindre cela on a besoin d'utiliser des protocoles de routage par exemple **l'OSPF** et **le NAT.**

Configuration d'OSPF:

Les commandes utilisées sont :

- **commande routeur OSPF:**

  OSPF est activé à l'aide de la commande de configuration globale « **router ospf process-id** ». Le process-id (id de processus) est un nombre compris entre 1 et 65535 choisi par l'administrateur réseau. Ce dernier doit correspondre pour que 2 voisins deviennent contigus. Dans notre topologie, nous allons activer OSPF sur les trois routeurs en utilisant le même ID de processus (12) à des fins de cohérence.

```
IPS(config)#router ospf 12
IPS(config-router)#
```

- **Commande réseau:**

  La commande network signifie toute interface de routeur qui correspond à l'adresse réseau. Elle est activée pour envoyer et recevoir des paquets OSPF.

Ce réseau (ou sous-réseau) sera inclus dans les mises à jour de routage OSPF.
Cette commande utilise une combinaison **d'adresse réseau** et de **masque générique** qui servent à spécifier l'interface ou la plage d'interfaces qui seront activées pour OSPF.
area-id qui fait référence à la zone OSPF qui signifie un groupe de routeurs qui partagent les informations d'état des liaisons. Tous les routeurs OSPF de la même zone doivent avoir les mêmes informations dans leur base de données d'état des liaisons, ce qui est possible parce que tous les routeurs diffusent leur état des liaisons individuel à tous les autres routeurs de la zone. Dans notre topologie, nous configurerons tous les routeurs OSPF d'une zone unique, et obtiendrons ainsi un protocole OSPF à zone unique (donc cela nécessite le même id de zone sur tous les routeurs).
R1:

```
IPS(config-router)#network 205.150.12.0 0.0.0.7   area 0
IPS(config-router)#network 205.100.10.0 0.0.0.3   area 0
IPS(config-router)#do wr
```

R2

```
R2(config-router)#network 205.150.12.0 0.0.0.7 area 0
R2(config-router)#network 199.0.20.0 0.0.0.3 area 0
R2(config-router)#do wr
Building configuration...
[OK]
```

R3

```
R3(config)#router ospf 12
R3(config-router)#network 199.0.20.0 0.0.0.3 area 0
R3(config-router)#do wr
```

Configuration de NAT
La première chose à faire lorsque l'on configure du NAT, quel qu'en soit le type, c'est d'indiquer au routeur où se situe le réseau privé et où se situe le réseau public.
Dans notre cas, les interfaces Fa0/0 et Fa1/0 sont du côté privé et seront déclarées comme **« inside »,** les interfaces S1/0 et S 2/0 par contre, étant du côté publique, seront configurées comme **« outside ».**
R1

```
IPS(config)#int f 1/0
IPS(config-if)#ip nat inside
IPS(config-if)#exit
IPS(config)#int s 2/0
IPS(config-if)#ip nat outside
IPS(config-if)#exit
```

R3

```
R3(config)#int f 0/0
R3(config-if)#ip nat inside
R3(config-if)#int s 1/0
R3(config-if)#ip nat outside
R3(config-if)#exit
```

Il nous faut ensuite définir quelles adresses IP sources seront susceptibles d'être translatées pour cela il faut créer une **ACL**.
On autorise donc à être translatée l'adresse ip du réseau 192.168.10.0/24 et celle de réseau 10.1.1.0/24

R1 :

```
IPS(config)#access-list 10 permit 192.168.10.10 0.0.0.255
```

R3

```
R3(config)#access-list 10 permit 10.1.1.1 0.0.0.255
```

Ensuite nous configurons les routeurs pour translater les paquets provenant des adresses décrites dans les ACL 10 (192.168.10.10) et (10.1.1.10) et de remplacer l'adresse IP source par celle configurée sur les interfaces Serial 2/0 et serial 1/0) en les surchargeant pour permettre à plus d'une machine de communiquer avec l'extérieur (PAT).

R1 :

```
IPS(config)#ip nat inside source list 10 int s 2/0 overload
IPS(config)#do wr
Building configuration...
[OK]
```

R3

```
R3(config)#ip nat inside source list 10 int s 1/0 overload
%Dynamic mapping in use, cannot change
R3(config)#do wr
Building configuration...
[OK]
```

V.2.2.5 Création des routes par défaut :

La passerelle par défaut pour R1 est 205.150.12.1

```
IPS(config)#ip route 0.0.0.0 0.0.0.0 205.150.12.1
IPS(config)#
```

La passerelle par défaut pour R3 est 199.0.20.1

```
R3(config)#ip route 0.0.0.0 0.0.0.0 199.0.20.1
R3(config)#do wr
```

V.2.3 Configuration de l'IOS IPS du routeur :

Pour la configuration de l'PS on procède aux cinq étapes suivantes :

Etape 1: Téléchargement des fichiers de signatures IOS IPS
Etape 2: Création de répertoire de configuration IOS IPS dans la mémoire flash
Etape 3: Configuration de la clé
Etape 4: Activation d'IOS IPS

Etape 1 :Téléchargement des fichiers de signatures
dehttp://software.cisco.com/download/release.html?mdfid=281442967&flowid=4836&softwareid=280775022&release=S807&relind=AVAILABLE&rellifecycle=&reltype=latest

Figure 5-11: Téléchargement des fichiers de signature

Les fichiers à télécharger sont :

- **IOS-Sxxx-CLI.pkg :** téléchargement du dernier package de signatures.
- **Royaume-cisco.pub.key.txt :** Clé publique Crypto - qui est la clé de chiffrement utilisée par IOS IPS

Etape 2: Création d'un répertoire de configuration d'IOS IPS sur le flash

La deuxième étape consiste à créer un répertoire de configuration IOS IPS en flash exactement dans le disk0 pour stocker les fichiers et les configurations de signatures requises en utilisant la commande **MKDIR** à l'invite du routeur, comme le montre la figure suivante:

```
R1#mkdir ips
Create directory filename [ips]?
Created dir disk0:/ips
```

Vérification de la présence de répertoire crée à l'aide de la commande **dir disk0 :**

```
IPS(config)#exit
IPS#dir
*Jun 17 02:14:48.511: %SYS-5-CONFIG_I: Configured from console by console
IPS#dir disk0:
Directory of disk0:/

    1  drw-           0  Jun 17 2015 01:38:32 +00:00  ips

268005376 bytes total (268001280 bytes free)
```

Etape 3: Configuration de la clé

La troisième étape consiste à configurer la clé de chiffrement utilisée par IOS IPS. Cette clé se trouve dans le fichier royaume-cisco.pub.key.txt qui a été téléchargé à l'étape 1.

La clé de chiffrement est utilisée pour vérifier la signature numérique du fichier de signatures de maître (sigdef-default.xml) dont le contenu est signé par une clé privée Cisco pour garantir son authenticité et son intégrité à chaque nouvelle version.

Pour configurer la clé de chiffrement IOS IPS, nous allons ouvrir le fichier texte, comme indiqué dans la figure 5-9, et copier le contenu du fichier, et coller le contenu au routeur à l'invite de configuration globale. Le fichier texte émet les différentes commandes pour générer la clé RSA. Voici un exemple de clé

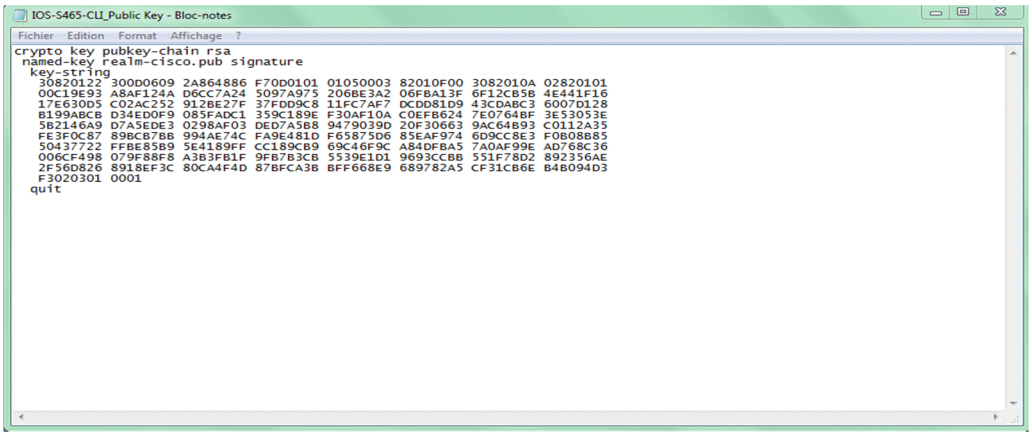

Figure 5-12: Fichier de clé de chiffrement d'IOS IPS

```
IPS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IPS(config)#crypto key pubkey-chain rsa
IPS(config-pubkey-chain)#named-key realm-cisco.pub signature
Translating "realm-cisco.pub"

IPS(config-pubkey-key)#key-string
Enter a public key as a hexidecimal number ....

IPS(config-pubkey)#$64886 F70D0101 01050003 82010F00 3082010A 02820101
IPS(config-pubkey)#$D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
IPS(config-pubkey)#$912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
IPS(config-pubkey)#$085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
IPS(config-pubkey)#$0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
IPS(config-pubkey)#   FE3F0C87 89BCB7BB 994AE74C FA9E481D
IPS(config-pubkey)#F65875D6 85EAF974 6D9CC8E3 F0B08B85
IPS(config-pubkey)#$5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
IPS(config-pubkey)#$A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
IPS(config-pubkey)#$80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
IPS(config-pubkey)#   F3020301 0001
IPS(config-pubkey)#  quit
IPS(config-pubkey-key)#exit
IPS(config-pubkey-chain)#exit
IPS(config)#
```

Remarque : Au moment de la compilation de signature, un message d'erreur est généré si la clé publique de chiffrement est invalide. Si la clé est mal configurée, la clé doit être supprimée, puis reconfigurée.

Etape 4: Activation d'IOS IPS

La quatrième étape consiste à configurer l'IOS IPS en utilisant la séquence d'étapes suivante:

i. Création d'un nom pour la règle d'IPS et spécification de son emplacement

Pour identifier le nom d'une règle IPS et spécifier son emplacement de stockage, on utilise la commande « **ips ip name [nom de la règle]** » pour la règle et la commande « **ips ip location [emplacement] : nom de répertoire** ». Comme il est montré ci-dessous :

```
IPS(config)#ip ips name iosips
IPS(config)#ip ips config location disk0:ips
IPS(config)#
```

ii. Activation de protocole SDEE et la notification d'événements

Pour utiliser SDEE, le serveur HTTP doit d'abord être activé avec la commande « **ip http server** ». Si le serveur HTTP n'est pas activé, le routeur ne peut pas répondre aux clients parce qu'il ne peut pas voir les demandes. La notification SDEE est désactivée par défaut et doit être explicitement activée. Pour se faire, Nous allons utiliser la commande « **ip ips notify SDEE** ».

IOS IPS prend également en charge l'utilisation de **Syslog** pour envoyer la notification d'événements. SDEE et Syslog peuvent être utilisés indépendamment ou activés en même temps comme il est montré ci-dessous. La notification Syslog est activée par défaut ou on utilisant la commande « **ip notify log** ». Si la console de journalisation est activée, nous allons voir messages syslog de l'ips.

```
IPS(config)#ip http server
IPS(config)#ip ips notify ?
  SDEE  Send events to SDEE
  log   Send events as syslog messages

IPS(config)#ip ips notify SDEE
IPS(config)#ip ips notify log
```

iii. Configuration de l'une des catégories de signatures

L'IOS IPS fonctionne avec des catégories de signature qui sont regroupées en catégories hiérarchiques. Ceci aide à classifier les signatures pour le groupement et l'accord faciles. Les trois catégories existantes sont :

- ✓ **Catégorie de bases :** La catégorie de base de signatures est appropriée pour les routeurs avec moins de 128 Mo de mémoire flash,
- ✓ **Catégorie avancées :** la catégorie de signatures avancées est appropriée pour les routeurs avec plus de 128 Mo de mémoire flash
- ✓ **Toutes les catégories :** contient les deux catégories de bases et avancées.

Les signatures que l'IOS IPS utilise pour analyser le trafic peuvent être retirées ou non retirées.

- **une signature retirée:** signifie que l'IOS IPS ne compile pas la signature dans la mémoire.
- **une signature non retirée :** signifie que l'IOS IPS compile la signature dans la mémoire et l'utilise pour analyser le trafic.

Lorsqu'un IOS IPS est configuré, toutes les signatures de la catégorie devraient toutes être retirées. Puis les signatures sélectionnées devraient être non retirées dans une catégorie de mémoire moins intensive. Pour mettre les signatures dans l'un de ces modes, nous allons entrer d'abord dans le mode de catégorie IPS en utilisant la commande **« ip ips signature catégorie »**. Ensuite, nous allons utiliser la commande « **catégorie nom de catégorie »** pour changer une catégorie et la commande « **retired true »** pour retirer une catégorie. Pour une catégorie non retirée, nous allons utiliser la commande « **retired false»**.
Dans l'exemple suivant, la catégorie all est retirée et la catégorie basic est non retirée.

```
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#category ios_ips ?
  advanced  Advanced
  basic     Basic
  default   Default
  <cr>

R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#end
Do you want to accept these changes? [confirm]
R1#
*Jun 17 20:51:34.515: Applying Category configuration to signatures ...
```

iv. Activation d'une règle IPS sur l'interface désirée et spécification de la direction dans laquelle la règle sera appliquée.

Dans cet exemple l'analyse du trafic se fait sur les paquets entrants de l'interface S 2/0 vers les interface F 1/0, F 0/1 et F 1/0 et celui entrant de F 1/0 vers F 1/0 ;F 0/1

```
IPS(config)#int f 1/1
IPS(config-if)#ip ips iosips in
IPS(config-if)#ip ips iosips out
IPS(config-if)#exi
IPS(config)#int f 1/0
IPS(config-if)#ip ips iosips out
IPS(config-if)#ip ips iosips in
IPS(config-if)#exi
IPS(config)#
```

v. Chargement de paquet de signature dans la RAM

La dernière étape consiste à charger le paquet de signature téléchargé au routeur. La façon la plus courante est de charger le paquet de signature pour le routeur est d'utiliser l'un des serveurs de fichiers FTP ou TFTP. En utilisant le serveur TFTP et le paramètre « **idconf** » à la fin de la commande pour charger au routeur un fichier de configuration, comme il est montré ci-dessous :

```
IPS(config)#copy tftp://cisco:cisco@192.168.10.1/IOS-S465-CLI.pkg idconf
                  ^
% Invalid input detected at '^' marker.

IPS(config)#exit
IPS#conf t
*Jun 18 12:35:15.807: %SYS-5-CONFIG_I: Configured from console by console
IPS#copy tftp://cisco:cisco@192.168.10.10/IOS-S465-CLI.pkg idconf
Loading IOS-S465-CLI.pkg from 192.168.10.10 (via FastEthernet1/0): !!!!
*Jun 18 12:36:16.607: %IPS-4-LICENSE_BYPASSED: IOS IPS subscription licensing has been bypassed
*Jun 18 12:36:18.623: %IPS-5-PACKET_UNSCANNED: atomic-ip - fail open - packets passed unscanned!!!!!!!!!!
*Jun 18 12:37:18.639: %IPS-5-PACKET_UNSCANNED: atomic-ip - fail open - packets passed unscanned!!!!!!!!!!
*Jun 18 12:38:18.647: %IPS-5-PACKET_UNSCANNED: atomic-ip - fail open - packets passed unscanned!!!!!!!!!!
*Jun 18 12:39:18.651: %IPS-5-PACKET_UNSCANNED: atomic-ip - fail open - packets passed unscanned!!!!!!!!
[OK - 11236690 bytes]

*Jun 18 12:40:31.555: %IPS-6-ENGINE_BUILDS_STARTED:  12:40:31 UTC Jun 18 2015
*Jun 18 12:40:31.563: %IPS-6-ENGINE_BUILDING: atomic-ip - 374 signatures - 1 of 16 engines
*Jun 18 12:40:39.367: %IPS-6-ENGINE_READY: atomic-ip - build time 7804 ms - packets for this engine will be sc
anned
*Jun 18 12:40:39.367: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 2 of 16 engines
*Jun 18 12:40:39.371: %IPS-6-ENGINE_READY: normalizer - build time 4 ms - packets for this engine will be scan
ned
*Jun 18 12:40:39.387: %IPS-6-ENGINE_BUILDING: service-http - 809 signatures - 3 of 16 engines
*Jun 18 12:40:42.395: %IPS-6-ENGINE_READY: service-http - build time 3008 ms - packets for this engine will be
 scanned
*Jun 18 12:40:42.399: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 49 signatures - 4 of 16 engines
*Jun 18 12:40:42.503: %IPS-6-ENGINE_READY: service-smb-advanced - build time 104 ms - packets for this engine
will be scanned
*Jun 18 12:40:42.503: %IPS-6-ENGINE_BUILDING: service-msrpc - 35 signatures - 5 of 16 engines
*Jun 18 12:40:46.535: %OSPF-5-ADJCHG: Process 12, Nbr 205.150.12.1 on FastEthernet1/1 from LOADING to FULL, Lo
ading Done
IPS#
*Jun 18 12:40:51.891: %IPS-6-ENGINE_READY: string-tcp - build time 8832 ms - packets for this engine will be s
canned
*Jun 18 12:40:51.899: %IPS-6-ENGINE_BUILDING: service-rpc - 76 signatures - 9 of 16 engines
*Jun 18 12:40:52.119: %IPS-6-ENGINE_READY: service-rpc - build time 220 ms - packets for this engine will be s
canned
*Jun 18 12:40:52.119: %IPS-6-ENGINE_BUILDING: service-dns - 39 signatures - 10 of 16 engines
```

Vérification de l'arrivé du fichier dans le répertoire ips :

```
IPS#dir disk0:iosips
%Error opening disk0:/iosips (File not found)
IPS#dir disk0:ips
Directory of disk0:/ips/

    2  -rw-         255  Jun 18 2015 12:29:10 +00:00  iosips-sig-delta.xmz
    3  -rw-       14978  Jun 18 2015 12:36:06 +00:00  iosips-sig-typedef.xmz
    4  -rw-       46166  Jun 18 2015 12:36:16 +00:00  iosips-sig-category.xmz
    5  -rw-         304  Jun 18 2015 12:29:12 +00:00  iosips-seap-delta.xmz
    6  -rw-         835  Jun 18 2015 12:29:12 +00:00  iosips-seap-typedef.xmz
    7  -rw-      633570  Jun 18 2015 12:40:10 +00:00  iosips-sig-default.xmz

536436736 bytes total (535699456 bytes free)
IPS#
```

Vérification de l'arrivé du fichier dans le serveur syslog:

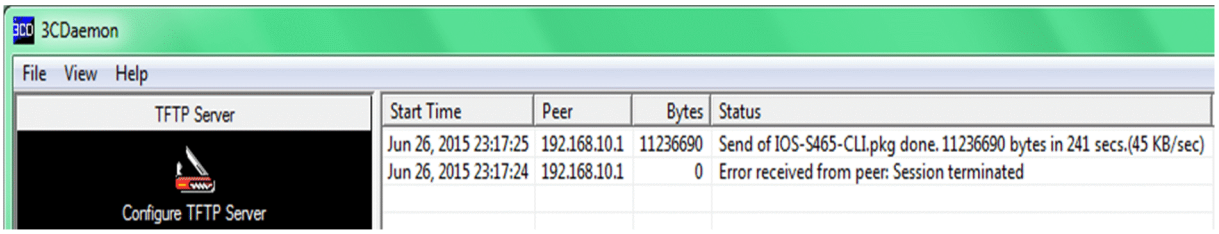

Figure 5-13 : Fichier de signature chargé à partir du server TFTP

Pour vérifier que le package de signature est correctement compilé, on utilise la commande « **show ip ips signature count** » comme il est montré ci-dessous :

```
IPS#show ip ips signature count

Cisco SDF release version S465.0
Trend SDF release version V0.0

Signature Micro-Engine: atomic-ip: Total Signatures 374
      atomic-ip enabled signatures: 88
      atomic-ip retired signatures: 353
      atomic-ip compiled signatures: 21
      atomic-ip obsoleted signatures: 3

Signature Micro-Engine: normalizer: Total Signatures 9
      normalizer enabled signatures: 8
      normalizer retired signatures: 1
      normalizer compiled signatures: 8

Signature Micro-Engine: service-http-v2 (INACTIVE)

Signature Micro-Engine: service-http: Total Signatures 806
      service-http enabled signatures: 136
      service-http retired signatures: 751
      service-http compiled signatures: 55

Signature Micro-Engine: service-smb-advanced: Total Signatures 49
      service-smb-advanced enabled signatures: 40
      service-smb-advanced retired signatures: 38
      service-smb-advanced compiled signatures: 11
      service-smb-advanced obsoleted signatures: 2
      service-smb-advanced disallowed signatures: 3

Signature Micro-Engine: service-msrpc: Total Signatures 35
      service-msrpc enabled signatures: 17
      service-msrpc retired signatures: 30
      service-msrpc compiled signatures: 5
      service-msrpc obsoleted signatures: 2

Signature Micro-Engine: service-smtp-v1 (INACTIVE)

Signature Micro-Engine: state: Total Signatures 37
      state enabled signatures: 16
      state retired signatures: 26
      state compiled signatures: 11

 --More--
```

V.3) Test de quelques exemples d'attaques :

V.3.1) Test de la signature Demande D'echo Request

Pour confirmer le bon fonctionnement de notre IPS on précède à tester une signature.

On a choisi la signature ayant l'identifiant 2004 qui correspond à la **DEMANDE D'ECHO REQUEST.**

On peut modifier l'état et les actions de celle-ci à l'aide de la commande **événement-action (**utilisé en mode moteur**).** Les actions disponibles dépendent de la signature, il y en plusieurs, on va citer quelques-unes :

- **Action de réinitialisation de la connexion TCP :** est une action de base qui peut être utilisée pour mettre fin aux connexions TCP (avec TCP RST).
- **Action de Production d'une alerte :** signifie qu'un message d'alarme sera généré.

- **Action de Refus de paquets en ligne :** signifie la transmission de paquets ne peuvent pas être effectuées.
- **Action de nier l'attaquant en ligne :** signifie que l'attaquant qui est connecté à partir de l'internet ne peut plus se connecter.

```
IPS(config)#ip ips signature-definition
IPS(config-sigdef)#signature 2004 0
IPS(config-sigdef-sig)#status
IPS(config-sigdef-sig-status)#retired false
IPS(config-sigdef-sig-status)#enabled true
IPS(config-sigdef-sig-status)#engine
IPS(config-sigdef-sig-engine)#event-action produce-alert
IPS(config-sigdef-sig-engine)#event-action deny-packet-inline
IPS(config-sigdef-sig-engine)#event-action reset-tcp-connection
IPS(config-sigdef-sig-engine)#exit
IPS(config-sigdef-sig)#exi
IPS(config-sigdef)#exi
Do you want to accept these changes? [confirm]y
IPS(config)#
```

Maintenant on va effectuer une demande d'ECHO REQUEST à partir de l'internet vers le server primaire, on obtient :

```
R2#ping 205.100.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 205.100.10.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

On voit que le server primaire ne répond plus à cette demande, car L'IPS la bloqué, et il a considéré cette demande comme étant une attaque on déclenchant une alarme.

Pour afficher les messages de journalisation d'alerte effectuées, on doit activer la console de server syslog à l'aide de la commande **Loggin host @ip de server syslog**

```
IPS(config)#loggin host 192.168.10.10
IPS(config)#do wr
Building configuration...
[OK]
```

Maintenant on peut voir cet affichage comme le montre la figure suivante :

Time	IP Address	Msg Type	Message
Jun 27 00:49:23	192.168.10.1	local7.warn	280: *Jun 27 00:49:11.675: %IPS-4-SIGNATURE: Sig:2004 Subsig:0 Sev:25 ICMP Echo Request [205.150.12.1:8 -> 205.100.10.2:0]

Figure 5-14: Les Messages de journalisation d'alertes au niveau de serveur syslog

On voit que le server primaire ne répond plus à la requête d'echo request ce qui signifie que notre IPS a bien bloqué cette demande.

V.3.2) Test d'IPS avec Nmap de backtrack :

Nmap est un outil puissant pour l'analyse du trafic de réseau .Il permettra de tester les capacités d'IPS .Donc pour cela les règles iosips d'IPS entrantes qui sont situées sur R3 F0 / 1 doivent intercepter le scan car il faut être prudent, un scan est équivalent à une tentative d'intrusion car certaines méthodes de scan peuvent entraîner des dysfonctionnements sur une

machine donc éviter pour ceci notre IPS doit réagir immédiatement et automatiquement ,on envoyant des messages d'alertes au serveur syslog pour nous prévenir de cette attaque.
Plusieurs techniques de scans de ports sont gérées par Nmap, en combinant ses diverses options, il offre une grande souplesse qui permet d'analyser tout le réseau, tester le filtrage.., donc on a effectué notre attaque a l'aide de la commande **Nmap –sN -O @ip de l'hôte cible** qu'on désire attaquer :

- ✓ **-sN** (Scan NULL) **:** Cette option envoie des paquets TCP avec aucun des drapeaux TCP définis dans le paquet. Si l'analyse retourne un paquet **RST**, elle signifie que le port est **fermé**, si **rien** retourné, il est soit **filtré** ou **ouvert.**

- ➢ **Application de l'attaque :**

Donc après avoir effectué cette attaque, on obtient ces résultats :

```
root@bt:~# nmap  -sN 205.100.10.2

Starting Nmap 6.01 ( http://nmap.org ) at 2015-06-24 17:35 EDT
Nmap scan report for 205.100.10.2
Host is up (0.041s latency).
All 1000 scanned ports on 205.100.10.2 are closed

Nmap done: 1 IP address (1 host up) scanned in 26.81 seconds
```

Figure 5-15 : Scan Null effectué par Nmap

Les résultats montrent que tous les ports de la machine cible sont **fermés** cela signifie que la machine cible est accessible, elle reçoit et répond aux paquets envoyés par Nmap mais il n'y a pas d'application à l'écoute sur ce port.
Après cette attaque notre IPS a réagi et il a déclenché une alarme comme le montre la figure ci-dessous :

```
Message
258: *Jun 27 00:32:35.267: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:125] VRF:NONE RiskRating:100
257: *Jun 27 00:32:35.155: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:555] VRF:NONE RiskRating:100
256: *Jun 27 00:32:35.135: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:720] VRF:NONE RiskRating:100
255: *Jun 27 00:32:34.827: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:19] VRF:NONE RiskRating:100
254: *Jun 27 00:32:34.791: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:714] VRF:NONE RiskRating:100
253: *Jun 27 00:32:34.775: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:563] VRF:NONE RiskRating:100
252: *Jun 27 00:32:34.743: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:32] VRF:NONE RiskRating:100
251: *Jun 27 00:32:34.679: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:85] VRF:NONE RiskRating:100
250: *Jun 27 00:32:34.639: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:700] VRF:NONE RiskRating:100
249: *Jun 27 00:32:34.551: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:801] VRF:NONE RiskRating:100
248: *Jun 27 00:32:34.451: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:514] VRF:NONE RiskRating:100
247: *Jun 27 00:32:34.371: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:43] VRF:NONE RiskRating:100
246: *Jun 27 00:32:34.175: %IPS-4-SIGNATURE: Sig:3040 Subsig:0 Sev:100 TCP NULL Packet [199.0.20.2:42139 -> 205.100.10.2:99] VRF:NONE RiskRating:100
```

Figure 5-16 : Résultats obtenus après l'attaque effectuée par Nmap.

- ➢ **Explication des messages de journalisation obtenus au niveau de server syslog :**

On voit dans le serveur qu'une signature a répondu à notre attaque :

- **La signature 3040 :** qui correspond à la signature **TCP NULL PACKET** qui est déclenchée quand un paquet TCP unique avec aucun des SYN; FIN, ACK a été envoyé a un hôte.

Donc ces alarmes ont été envoyées à l'aide de protocole SDEE à l'PS pour le prévenir contre cette attaque .Ce dernier doit la bloquer donc pour faire cela on va activer la signature 3040 et on va lui appliquer quelques actions qu'on a cité précédemment.

```
IPS(config)#ip ips signature-definition
IPS(config-sigdef)#signature 3040 0
IPS(config-sigdef-sig)#status
IPS(config-sigdef-sig-status)#retired false
IPS(config-sigdef-sig-status)#enabled true
IPS(config-sigdef-sig-status)#engine
IPS(config-sigdef-sig-engine)#event-action produce-alert
IPS(config-sigdef-sig-engine)#event-action deny-packet-inline
IPS(config-sigdef-sig-engine)#event-action reset-tcp-connection
IPS(config-sigdef-sig-engine)#event-action deny-attacker-inline
IPS(config-sigdef-sig-engine)#exit
IPS(config-sigdef-sig)#exit
IPS(config-sigdef)#exit
Do you want to accept these changes? [confirm]
IPS(config)#
*Jun 27 00:36:03.267: %IPS-6-ENGINE_BUILDS_STARTED: 00:36:03 UTC Jun 27 2015
*Jun 27 00:36:03.687: %IPS-6-ENGINE_BUILDING: atomic-ip - 374 signatures - 1 of 16 engines
*Jun 27 00:36:09.355: %IPS-6-ENGINE_READY: atomic-ip - build time 5668 ms - packets for this engine will be sc
anned
*Jun 27 00:36:09.643: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 6376 ms
IPS(config)#
```

Après avoir activé cette signature, on va refaire la même attaque comme le montre la figure suivante:

```
root@bt:~# nmap  -sN 205.100.10.2

Starting Nmap 6.01 ( http://nmap.org ) at 2015-06-24 17:38 EDT
Nmap scan report for 205.100.10.2
Host is up (0.051s latency).
All 1000 scanned ports on 205.100.10.2 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 65.08 seconds
```

Figure 5-17: Scan Null effectué par Nmap après l'activation de la signature 3040.

Les résultats montrent que tous les ports de la machine cible sont **Open | Filtered** .Cela signifie que Nmap est incapable de déterminer si le port est ouvert ou filtré car la machine cible ne donne plus de réponse .L'absence de réponse veut dire également que notre IPS a fait le filtrage de paquet généré par Nmap.
Ces résultats obtenus assurent que notre réseau est bien sécurisé et que notre IPS fonctionne vraiment bien.

Conclusion :

Dans ce chapitre nous avons présenté les outils utilisés pour simuler le réseau d'ENIEM avec la solution IPS. Puis on a montré les étapes à suivre pour la configuration de l'IOS IPS. A la fin, nous l'avons testé avec succès et on a confirmé son bon fonctionnement.

Nous estimons avoir réalisé un système qui répond à l'objectif que nous avons fixé à savoir la mise en œuvre d'un système de surveillance de la sécurité et de la prévention d'intrusion.

Conclusion générale

Puisque ENIEM ne possède pas un système de contrôle de sécurité, alors on ne peut pas savoir si elle a subit déjà des attaques ou pas, surtout sur la confidentialité. Si c'est le cas, on ne connait pas les sources. L'utilisation de notre solution par l'administrateur de la sécurité va confirmer cela. Si les hypothèses précédentes sont justes ENIEM doit renforcer plus son niveau de sécurité en ajoutant à la zone sécurisée des appareils de sécurité plus puissante comme un appareil IPS 4200, un module AIP-SSM qui intègre la gamme ASA ou un module Cisco IDSM-2 intégrant un Catalyst 6500 qui détecte aussi les attaques inconnues.

Bien que répandus dans les organisations aujourd'hui, les systèmes de détection et prévention d'intrusions ne représentent qu'un maillon d'une politique de sécurité. En effet, même s'ils permettent la détection, parfois l'arrêt, des intrusions, ils restent néanmoins vulnérables eux aussi face aux attaques externes.

C'est pourquoi, 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 et prévention 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 NIPS et HIPS dans le même réseau. Leurs rôles sont différents mais chacun apporte ses fonctionnalités.

L'efficacité des détections passe aussi par une bonne implémentation des nouvelles règles de détection d'intrusion. L'étude que nous avons menée sur l'écriture de ces dernières nous a permis d'observer combien il est indispensable de maîtriser le formalisme de description des attaques et d'adapter ces règles à l'architecture du réseau à défendre. Mais ce n'est pas tout, au-delà de ce formalisme, doit résider un savoir-faire important de la part du (des) concepteur(s) de ces règles.

Toutefois, et nous terminerons par ceci, même si une certaine maturité dans ce domaine 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.

Bibliographie :

[1]: Eric Cole, «Hackers Beware », first edition, New Riders Publishing, 2001.

[2]: CCNA Security 640-554 Official Cert Guide, 2012

[3]: Stéphane Gill, Type d'attaques, 2003

[4]: Solange Ghernaouti-Hélie, Sécurité internet Strategie et technologie, 2000.

[5]: « Sécurité informatique Principes et méthode » ÉDITIONS EYROLLES, 2007

[6]: Thibault PALUD, les sondes de sécurité IDS/IPS, 2010

[7]: Nicolas Baudoin, Marion Karle "NT Réseaux, IDS et IPS" ,2004

[8]: Jacob Zimmermann et Ludovic Mé, Les systèmes de détection d'intrusions : principes algorithmiques.

[9]: David Burns, CCNP Security IPS, 642-627, 2012.

[10]: Fiche technique, CISCO CATALYST 6500 SERIES SUPERVISOR ENGINE 720, 2006

[11]: Fiche technique, Description des Serveurs de Sécurité Adaptatifs de la gamme Cisco ASA 5500, 2007.

[12]: Cisco Networking Academy, CCNA Security: Implementing Network Security 1.2, 2014

[13]: Verizon RISK Team with the United States Secret Service, DATA BREACH INVESTIGATIONS REPORT, 2010

[14]: CCIE Professional Development, Inside Cisco IOS Software Architecture, 2000

[15]: AFNOG VI – MAPUTO, Introduction aux routeurs CISCO, 2005

Référence WEB :

[16]: www.Wikipédia.org

[17]: www.memoireonline.com

[18]: www.commentcamarche.net

[19]: www.anti-cybercriminalite.fr

[20]: www.doc.ubuntu-fr.org/pare-feu

[21] : www.cisco.com