République **A**lgérienne **D**émocratique et **P**opulaire
Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de Fin d'Etudes
De MASTER ACADEMIQUE

Domaine : **Sciences et Technologies**
Filière : **Génie électrique**
Spécialité : **Réseaux et Télécommunications**

Présenté par

Souhad El NAWAJHA
Imane AIT MOHAMMED

Thème

Simulation du firewall Asa et de L'IDS /IPS Cisco en vue de sécuriser un réseau d'entreprise

Mémoire soutenu publiquement le 09/07/ 2015 devant le jury composé de :

Mr M. LAZRI
Mr Président

Mr F. OUALLOUCHE
Grade, Lieu d'exercice, Encadreur

Mr S. HAMEG
Grade, Lieu d'exercice, Examinateur

Mr D. ALOUACHE
Grade, Lieu d'exercice, Examinateur

2014-2015

Remerciements

Avec un grand plaisir on remercie ***Allah*** *qui nous a aidés et nous a donné la patience, le courage et la force d'achever ce travail.*

Nous tenons à remercier en cette occasion tout le corps professoral et administratif de département de génie électrique et d'informatique de l'université mouloud Mammeri de Tizi-Ouzou pour la richesse et la qualité de leurs enseignements et qui déploient de grands efforts pour assurer à leurs étudiants une formation actualisée.

Nous tenons à remercier sincèrement ***Mr ouallouche fethi****, qui, en tant que promoteur, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour ses orientations, la confiance, l'aide et le temps qu'il a bien voulu nous consacrer et sans lui ce mémoire n'aurait jamais vu le jour.*

Nous exprimons également notre gratitude aux membres du jury, qui nous a honorés en acceptant de juger ce modeste travail.

Nous tenons à remercier sincèrement nos parents, qui nous ont donné le courage.

Nous souhaitons d'adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire.

Dédicaces

*A l'aide de **DIEU** tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce modeste travail que je dédie à :*

*Ma très chère **mère** qui n'a pas cessé de m'encourager et de se sacrifier pour que je puisse franchir tout obstacle durant toutes mes années d'étude que Dieu me la garde en très bonne santé ; Aucune dédicace ne pourra compenser les sacrifices de ma **mère** ;*

*Mes très chères sœurs **Suzane** et **Sanaa** que je leur souhaite une longue vie pleine de joie et de réussite.*

*Mes très chers frères **Achraf** , **Oussama** et **salama** que je leur souhaite une longue vie pleine de joie et de réussite.*

*Mes **amis (es)**.*

*Mes **oncles tantes**.*

*Mes **cousins et cousines**.*

*Mes pensées vont particulièrement à mon défunt **père** qui repose en paix.*

Qu'ils trouvent ici toute ma gratitude.

Souhad

Dédicaces

A l'aide de DIEU tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce

Modeste travail que je dédie:

A la mémoire de ma grande mère paternel ;

A mon très cher père et ma très chère mère qui n'ont pas cessé de m'encourager et de se sacrifier pour que je puisse franchir tout obstacle durant toutes mes années d'étude que Dieu me les garde en très bonne santé ; Aucune dédicace ne pourra compenser les sacrifices de mes parents;

A mon fiancé Massi, celui à qui je souhaite une longue vie pleine de joie, de bonheur et de santé;

Mes deux chères sœurs Sarah et Lamia, que je leur souhaite une longue vie pleine de joie et de réussite.

A mon cher frère Anis,

A mes oncles, mes tantes, mes cousines, mes cousins, et à toute ma Famille.

Imane

Glossaire

ACL: **A**ccess **C**ontrol **L**ist

AH: **A**uthentification **H**eader

BPD: **B**order **P**rotection **D**evice

CD: **C**ollision **D**etection

CSMA: **C**arrier **S**ense **M**ultiple **A**ccess

DHCP: **D**ynamic **H**ost **c**onfiguration **P**rotocol

DNS: **D**omain **N**ame **s**ervice

DOS: **D**enial **o**f **s**ervice

ESP: **E**ncapsulation **S**ecurity **p**ayload

FDDI: **F**iber **D**istributed **D**ata **I**nterface

FTP: **F**ile **T**ransfer **P**rotocol

HIDS: **H**ost **I**ntrusion **D**etection **S**ystem

HTTP: **H**yper **T**ext **T**ransfer **P**rotocol

ICMP: **I**nternet **c**ontrol **M**essage **P**rotocol

IDS: **I**ntrusion **D**etection **S**ystem

IP: **i**nternet **P**rotocol

IPS: **I**ntrusion **P**revention **S**ystem

LAN: **L**ocal **A**rea **N**etwork

MAN: **M**étropolitain **A**rea **N**etwork

NIDS: **N**etwork **I**ntrusion **D**etection **S**ystem

NNIDS: Noeud **N**etwork **I**ntrusion **D**etection **S**ystem

POP3: Post **O**ffice **P**rotocol

SMTP: Simple **M**ail **T**ransfer **P**rotocol

SNMP: Simple **N**etwork **M**anagement **P**rotocol

SSH: Secure **S**hell

SSL: Secure **S**ocket **L**ayer

TCP: Transport **C**ontrol **P**rotocol

TFTP: Trivial **F**ile **T**ransfer **P**rotocol

UDP: User **D**atagram **P**rotocol

VPN: Virtual **P**rivate **N**etwork

WAN: Wilde **A**rea **N**etwork

Sommaire

Sommaire

Listes des figures

Introduction

Dans la « société de l'information », la sécurité des systèmes informatiques constitue un enjeu crucial. Le contrôle de l'information traitée et partagée au sein de ces systèmes est un problème d'autant plus délicat que le nombre d'utilisateurs de ces systèmes est important. Relier ces systèmes entre eux au sein de réseaux informatiques, eux-mêmes interconnectés, complexifie la tâche des responsables de sécurité.

La sécurité d'un système informatique repose en premier lieu sur la mise en place d'une politique de sécurité [1]. Celle-ci est basée sur l'utilisation de différents outils. Parmi lesquels, les firewalls, VPN (Virtual Private Network), antivirus,….etc [2].

Le choix d'un outil de sécurité est du ressort de l'administrateur réseau. En effet, ce dernier doit d'abord étudier les failles de sécurité du réseau pour en proposer la solution.

Notre travail consiste à simuler deux méthodes de sécurité sur un réseau de départ. La première consiste à utiliser le firewall et la deuxième est basée sur IDS/IPS (Intrusion Detection System / Intrusion Prevention System). A cet effet, nous commençons par présenter l'architecture réseau existante et ses failles de sécurité. Ensuite, nous allons appliquer deux méthodes de sécurité. La première est basée sur l'utilisation d'un firewall et la deuxième sur l'utilisation de l'IDS/IPS. Apres avoir configuré les firewalls nous allons faire de même pour IDS/IPS.

Nous avons structuré notre mémoire en 4 chapitres.

Le premier chapitre est un chapitre descriptif de la sécurité des réseaux. Nous avons définit les menaces, les logiciels malveillants et la politique de sécurité ainsi les principaux mécanismes de sécurité.

Le second chapitre est consacré à la présentation de l'architecture globale d'un firewall, ainsi les différents types de filtrage.

Dans le troisième chapitre, nous présentons une architecture globale d'un IDS et la classification des IDS et le fonctionnement d'un IPS.

Le dernier chapitre est consacré à la réalisation de notre application qui consiste en la configuration des deux solutions et en leur comparaison.

Nous terminons notre mémoire par une conclusion et une bibliographie.

Chapitre 1

1. Préambule

Les réseaux recouvrent tous les domaines informatiques, pour cela les entreprises ne peuvent pas réaliser un bon fonctionnement sauf si ce dernier est mis en service.

La sécurité des réseaux informatiques est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines. Un seul mot " sécurité " recouvre des aspects très différents à la fois techniques, organisationnels et juridiques.

Dans ce chapitre nous allons présenter des notions générales sur la sécurité des réseaux informatiques

2. Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipements et d'autres dispositifs reliés entre eux dans le but d'échanger des informations et partager les ressources matériels et logicielles.

3. Classification des réseaux informatiques

La classification se fait par rapport à un critère donné, ainsi nous pouvons classifier les réseaux informatiques de la manière suivante :

3.1. Classification selon leur étendue géographique

3.1.1. Les réseaux locaux LAN (Local Area Network)

C'est un réseau local, il s'agit d'un ensemble d'ordinateur appartenant à une même organisation et relies entre eux dans une petite géographique par un réseau, souvent à l'aide d'une même technologie (la plus répondue étant Ethernet).

L'étendue géographique des réseaux locaux ne dépasse pas 10 km, la vitesse de communication varie à 100Mb/s.

3.1.2. Les réseaux MAN (Métropolitain Area Network)

Les MAN interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de Km) à un débit important (supérieur a 100Mb/s). Ainsi un MAN permet à deux distants de communiquer comme si ils faisaient partie d'un même réseau local.

3.1.3. Les réseaux étendus WAN (Wilde Area Network)

Un WAN interconnecte plusieurs LAN à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le cout des liaisons (qui augmente avec la distance et peuvent être faibles.

Les débits varient entre 56kb/s à 625Mb/s.

3.2. Classification selon la topologie

3.2.1. Topologie en bus

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial.

3.2.2. Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur.

Il s'agit d'une boite comprenant un certain nombre de jonction au quel il est possible de raccorder les câbles réseaux.

3.2.3. Topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

3.2.4. Topologie en arbre

Le réseau est divisé en niveaux le sommet, le haut niveau, est connecté à plusieurs nœuds de niveau inferieur, dans la hiérarchie. Ces derniers peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inferieur, le tout dessine alors un arbre, ou une arborescence.

3.2.5. Topologie maillée

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autre unité. Chaque terminale est reliée à tous les autres.

Classification selon la méthode d'accès

Méthode d'accès CSMA /CD

Ce protocole est de type persistant car la station persiste à écouter le canal jusqu'à ce que celui-ci devienne libre, avant d'émettre sa trame.

Méthode d'accès par Token Ring

Est un protocole de réseau local qui fonctionne sur la couche liaison du modèle OSI. Il utilise une trame spéciale de trois octets, appeler jeton, qui cercle dans une seule direction au Toure d'un anneau. Les trames Token Ring parcourent l'anneau dans un seul sens

Méthode d'accès par standard FDDI

La technologie FDDI (Fiber Distributed Data Interface) est une technologie d'accès au réseau sur des lignes de type fibre optique. C'est un anneau à jeton à détection et correction des erreurs.

3.4. Classification selon le mode de connexion

Mode avec connexion

Les blocs de données sont acheminés sur le même chemin physique

Mode sans connexion

Les blocs de données sont acheminés indépendamment les uns aux autres

4. les protocoles réseaux

4.1. Protocole DNS (Domaine Name service) :

Est un serveur qui assure la résolution de noms des réseaux TCP /IP et il permet aussi aux utilisateurs d'ordinateurs client d'adopter des noms à la place des adresses IP numériques pour identifier les hôtes distants [3].

4.2. Protocole TCP (Transport Contrôle Protocole) :

Est un protocole qui assure un service de transmission de donnée fiable avec une détection et une correction d'erreur de bout en bout [3].

4.3. Protocole ICMP (internet control message Protocol) :

Est un protocole qui permet de gérer les informations relatives aux erreurs aux machines connectées étant donnée le peu de contrôle que le protocole IP réalise, c'est grâce à ce protocole qu'une machine émettrice peut s'avoir qu'il y a eu un incident de réseaux [3].

4.4. Protocole DHCP (Dynamic Host configuration Protocole) :

Est un protocole qui offre une configuration des réseaux TCP /IP fiable et simple, empêche les conflits d'adresse et permet de contrôler l'utilisation des adresses IP de façon centralisée. DHCP peut aussi configurer l'adresse de la passerelle par défaut [3].

4.5. Protocole POP3 :

Est un protocole qui permet de récupérer son courrier sur un serveur distant (le serveur POP). Cette opération nécessite une connexion à un réseau TCP /IP. Les ports utilisés est le 110 [12].

4.6. Protocole FTP (File Transfer Protocol) :

Est un protocole de communication dédié à l'échange informatique de fichier sur un réseau TCP/IP. Il permet de copier des fichiers depuis ou vers un autre ordinateur du réseau. L'utilisation de FTP depuis un poste client nécessite de la part de l'utilisateur de se connecter avec un non et un mot de passe. Donc si l'utilisateur n'est pas reconnu la connexion ne sera pas établie [3].

4.7. SMTP (Simple Mail Transfer Protocol) :

Ce protocole est utilisé pour transférer les messages électroniques sur les réseaux, son principal objectif est de router les mails à partir de l'adresse du destinataire. C'est un service qui écoute sur le port 25 [3].

4.8. HTTP (Hyper Text Transfer Protocol) :

Est un protocole qui permet l'échange de données entre client et serveur de manière sécurisée hyper texte contenant des donnée sous forme de texte, d'image fixe ou animées et de son. Tout client web communique avec le port 80 d'un serveur http [3].

4.9. Protocole Telnet :

Est un protocole standard d'internet permettant l'interfaçage de terminaux et d'application à travers internet .il se repose sur une connexion TCP sur le port 23 pour envoyer des données [3].

4.10. SNMP (Simple Network Management Protocol) :

C'est un protocole qui permet aux administrateurs réseaux de gérer l'équipement des réseaux et de diagnostiquer les problèmes des réseaux [3].

4.11. TFTP (Trivial File Transfer Protocol ou Protocole simplifie de Transfer de fichier) :

Est un protocole simplifier de Transfer de fichier il fonctionne en UDP sur le port 69, au contraire du FTP qui utilise lui TCP .TFTP reste très utiliser pour la mise a jours des logicielle embarquer sur les équipements réseaux (routeur, pare-feu, etc.) ou pour démarrer un PC a partir d'une carte réseau [3].

Pour assurer le bon fonctionnement du réseau et faire aux menaces éventuelles qui peuvent le mettre hors service il est nécessaire de le sécuriser .pour cela le concept de sécurité des systèmes d'information recouvre un ensemble de méthodes, technique et outils chargés de protéger les ressources d'un système d'information.

5. Définition de sécurité

La sécurité informatique est l'ensemble de moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre les menaces accidentelle ou intentionnelle, ce qui implique la réalisation des fonctions essentielle suivante :

_ **Disponibilité** : les services (ordinateurs, réseaux, périphérique, application …) et les informations (données, fichier) doivent être accessibles aux personnes autorisées quand elles en ont besoin

_ **La confidentialité** : les informations n'appartiennent pas à tout le monde : seule peuvent y accéder ceux qui en ont le droit

_ **L'intégrité** : les services et les informations (fichier, messages…….) ne peuvent être modifié que par les personnes autorisées (administrateur, propriétaire…).

_ **Non répudiation** : permet de garantir qu'une transaction ne peut être niée.

_ **Authentification** : consistant à assurer que seules les personnes autorisées aient accès aux ressources.

6. Politique de sécurité

Une politique de sécurité informatique est un plan d'actions définie pour maintenir un certain niveau de sécurité aux besoins de l'organisation. Elle a pour objectif :

Élaborer des règles et des procédures, installer des outils techniques dans les différents services de l'organisation (autour de l'informatique) ;

Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une intrusion ;

Sensibiliser les utilisateurs aux problèmes liés à la sécurité des systèmes d'informations ;

Préciser les rôles et respective.

7. Type de menaces

La menace informatique représente le type d'actions susceptibles de nuire dans l'absolu à un système informatique, elles viennent d'individus compétents à cause des vulnérabilités de système de sécurité.

7.1. Les menaces accidentelles

Les menaces accidentelles peuvent ce manifester ou résulter de l'exposition ou de la modification d'un objet, elles peuvent être des erres des utilisateurs ou administrateurs, matériel ou accident de nature industrielle.

7.2. Les menaces intentionnelles

Une menace intentionnelle est une action exécutée par une entité pour violer la sécurité de l'information et l'utilisation non autorisé des ressources.

Les attaques intentionnelles peuvent être :

7.2.1. Menaces passives

Basée sur l'écoute de l'exécution, son rôle est de collecter les informations. En générale il est très difficile de détecter une attaque passive car elle n'interagit pas dans le fonctionnement du système.

7.2.2. Menaces actives (attaque)

Les menaces actives ou attaques envers un système provoque l'altération d'information contenues dans ce système, ou des modifications de l'état de fonctionnement du système, ce type de menaces est facile à détecter.

8. les faiblesses de sécurité

8.1. Faiblesses technologiques

Les technologies informatiques et de réseaux ont des faiblesses de sécurité intrinsèques. Celles-ci comprennent :

Les faiblesses des protocoles TCP/IP : par exemple http (Hyper Texte Transfer Protocol), FTP (File Transfer Protocol) et ICMP (Internet Contrôle Message Protocol) sont intrinsèquement non sécurisés.

Les faiblesses du système d'exploitation : tout les systèmes d'exploitations (UNIX, Linux, Windows NT, XP ET Vista) présentent des problèmes de sécurité qui doivent être résolus.

Les faiblesses de l'équipement réseau : tels que les routeurs, les commutateurs, ont des de sécurité qui doivent faire l'objet d'une détection et d'une protection. Ces faiblesses concernent la protection des mots de passes, le manque d'authentifications, les protocoles de routage et les ouvertures dans les pare-feu.

8.2. Faiblesses de configuration

Les administrateurs réseau et les ingénieurs système doivent apprendre ce que sont les faiblesses de configurations et les compensées en configurant convenablement leurs équipements informatiques et réseau. Les exemples fréquents qu'on peut citer sont les suivants :

Paramètres par défaut non sécurisés dans les produits logiciels Equipement réseau mal configuré : par exemple, des listes d'accès, des protocoles de routage ou des chaines de communauté SNMP mal configurées peuvent ouvrir de larges failles dans la sécurité.

8.3. Faiblesses dans la stratégie de sécurité

Il existe des risques de sécurité pour le réseau si les utilisateurs ne respectent pas la stratégie de sécurité.

9. les techniques d'attaques

9.1. Attaque contre la communication

Est un type d'attaque contre la confidentialité, qui consiste à accéder sans modification aux informations transmises ou stockées, l'information n'est pas altérée pas ce lui qui en

prélève une copie. Ces attaques sont donc indétectables par le système et peuvent seulement êtres parées par des mesures préventives.

9.2. Interposition

Il s'agit d'un « déguisement » en émission ou en réception, il consiste à tromper les mécanismes d'authentification pour ce faire passer pour un utilisateur (personne ou service disposant des droits dont on a besoin) pour compromettre la confidentialité, l'intégrité ou la disponibilité.

Exemple le vol d'adresse (IP spoofing) Ce type d'attaque n'implique rien de plus que l'usurpation d'une adresse source. Cela consiste à utiliser une machine en se faisant passer pour une autre.

9.3. Coupure

Est un accès avec modification à des informations transmises sur des voies de communication, il s'agit donc d'une attaque contre l'intégrité.

9.4. Attaques logicielles

9.4.1. Les virus

Un ‘’virus’’ est un bout de programme glissé volontairement dans une application dans le but de nuire.

Il est possible d'attraper un virus avec n'importe qu'elle application que l'on a installée et que l'on exécute, ce n'est pas un problème typique d'une connexion permanente.

Un virus ne peut être introduit dans sa machine que si l'on exécute une application infectée, application récupérée sur internet ou sur n'importe quel autre support informatique : disquette, CD ROM etc.

Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

Téléchargement de logiciel puis exécution de celui-ci sans précautions.

Ouverture sans précaution de documents contenant des macros.

Pièce jointe de courrier électronique (exécutable, scripte type VBs…).

Ouverture d'un courrier au format HTML contenant du JavaScript exploitant une faille de sécurité de logiciel de courrier (normalement JavaScript est sans danger).

9.4.2. Le cheval de Troie

Un cheval de Troie ou troyen (Trojan horse ou trojan) n'est ni un virus ni un ver, pace qu'il ne se reproduit pas. Un cheval de Troie introduit sur une machine a pour but de détruire ou de récupérer des informations confidentielles sur celle-ci. Généralement il est utilisé pour créer une porte dérobée sur l'hôte infecté afin de mettre à disposition d'un pirate un accès à la machine depuis internet. Les opérations suivantes peuvent être effectuées par l'intermédiaire d'un chevale de Troie :

Récupération des mots de passes grâce à un keylogger.

Administration illégale à distance d'un ordinateur.

Relais utilisé par les pirates pour effectuer des attaques.

Serveur de spam (envoi en masse des e-mails).

9.4.3. Les vers

Un vers est un programme indépendant, qui se copie d'ordinateur en ordinateur. La différence entre un ver et un virus est que le ver n'a pas besoin d'un autre programme pour ce reproduire. Il va simplement se copier via un réseau ou Internet, d'ordinateur en ordinateur. Ce type de réplication peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise.

Comme un virus, un ver peut contenir une action nuisible du type destruction de données ou envoi d'information confidentielle

9.4.4. L'écoute du réseau (le sniffing)

Grace à un logiciel appelé ''sniffer'', il possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées.

Si quelqu'un se connecte par Telnet par exemple à ce moment-la, son mot de passe transitant en clair sur le net, il sera aisé de le lire. De même, il est facile de s'avoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception.

9.5. Autres attaques

9.5.1. Attaque par dénie de service (Dos)

Une attaque par déni de service (Dos, Dinial of service) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services aux ressources d'une organisation. Il s'agit la plut part de temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.

Le principe de ses attaques consiste à envoyer des paquets IP ou des données de taille afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer des services réseau qu'elles proposent.

9.5.2. Intrusion

L'intrusion dans un système informatique a pour but la réalisation d'une menace et donc une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, incident diplomatique…etc.

Pour pouvoir s'introduire dans le réseau, le pirate a besoin d'accéder à des comptes valides sur les machines qu'il a recensé, pour ce faire, plusieurs méthodes sont utilisées par le pirate.

L'ingénierie sociale, c'est-a-dire rn contactant directement certains utilisateurs du réseau (par mail ou par téléphone) afin de leur soutirer des informations concernant leur identifiant de connexion et leurs mont de passe.

La consultation de l'annuaire ou bien des services de messagerie ou de partage de fichiers, permettant de trouver des nos d'utilisateurs valides.

L'exploitation des vulnérabilités des logiciels.

Les attaques par force brute, consistant à essayer de façon automatique différent mot de passe sur une liste de compte.

9.5.3. Attaque de l'homme de milieu

L'attaque de l'homme de milieu ou main in the middle est une attaque qui a pour but d'intercepter la communication entre deux parties, sont que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elle a été compromis.

Pour mettre en œuvre l'échange réseau approprier, il faut soit que la machine du pirate se trouve physiquement sur le chemin réseau emprunte par les flux de données, soit que le pirate réussisse à modifier le chemin réseau afin que sa machine devienne un des points de passages.

9.5.4. Usurpation d'adresse IP (IP spoofing)

L'usurpation d'adresse IP est une technique consiste à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer les paquets anonymement.

La technique de l'usurpation d'adresse IP peut permettre a un pirate de faire passer des paquets sur un réseau sans que ceux-ci ne soient interceptés par le Système de filtrage des paquets (pare-feu). Ainsi, un paquet écoué avec l'adresse IP d'une machine interne semblera provenir d'un réseau interne et sera relayé a la machine cible.

9.5.5. Le craquage de mot de passe

Cette méthode consiste à faire beaucoup d'essais pour déterminer un mot de passe. Elle peut s'effectuer à l'aide d'un dictionnaire car la plupart des mots ne sont pas des chaines aléatoires mais des mots ou des phrases faciles à retenir. Ce la permet d'écarter une très grande quantité de possibilités, ou par la méthode de la force brute qui consiste à essayer tout les combinaisons possibles. Elle est rapidement efficace sur les petite chaines (moins de 8 caractères) mais devient rapidement trop à exécuter quand la langueur du mot de passe augmente (plus de 16 caractères).

10. les protocoles de sécurité

10.1. Protocole SSL

Le protocole SSL (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur TCP/IP. (Http, FTP, etc.…). Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, mais également les services de confidentialité et d'intégrité.

Le principe d'une authentification du serveur avec SSL est le suivant :

le navigateur du client fait une demande de transaction sécurisée au serveur.

Suite à la requête du client, le serveur envoi son certificat au client.

Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.

Le client choisit l'algorithme.

Le serveur envoi son certificat avec les clés cryptographiques correspondent au client.

Le navigateur vérifie que le certificat délivré est valide.

Si la vérification est correcte alors le navigateur du client envoi au serveur une clé secrète chiffre a l'aide de la clé publique du serveur qui sera donc le seule capable de déchiffrer puis d'utiliser cette clé secrète. cette clé est un secret uniquement partager entre le client et le serveur afin d'échanger des données en tout sécurité.

10.2. Le protocole SSH

Le protocole SSH (Secure Shell) est un protocole permettant un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commande ou des fichiers de manier sécuriser : les données circulant entre le client et le serveur sont chiffrées, ce qui garantie leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des partie croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

10.3. Le protocole IP sec

IP sec est un protocole permettant de sécuriser les échanges au niveau de la couche réseau.

Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.

Le protocole IPsec est basé sur trois modules

IP authentification Header(AH) concernant l'intégrité, l'authentification et la protection contre le rejet des paquets à encapsuler

Encapsulation Security payload (ESP) définissant le chiffrement de paquet, ESP fournit la confidentialité, l'intégrité, l'authentification et la protection contre le rejet.

Security association (SA) définissant l'échange des clés et des paramètres de sécurité.

Les SA rassemble ainsi l'ensemble des informations sur le traitement à appliquer au paquet IP.

10.4. Le protocole Secure http

S-http (Secure http, ce qui signifie protocole http sécurise) permet l'échange de donnée entre client et serveur de manière sécurisée en ayant recoures au cryptage (garantir aux clients la confidentialité de toute informations personnelles).

Contrairement au SSL qui travaille au niveau de la couche de transport, S-http assure une sécurité basée sur des messages au-dessus du protocole http, en marquant individuellement les documents HTML à l'aide de certificat alors que SSL est indépendant de l'application utiliser et chiffre l'intégralité de la communication.

S-http est fortement lie au protocole http et chiffre individuellement chaque message.

11. les méthodes de protections

11.1 .Antivirus

Un antivirus est un logiciel informatique permettant d'identifier et effacer des logiciels malveillants dans n'importe quel périphérique de stockage (disque dur, clé USB, mémoire flash …etc.). Pour être efficace ce type de logicielle demande des mises à jours très fréquentes au cours desquelles il mémorise les nouvelles formes de virus en circulation.

11.2. Réseau privé virtuel(VPN)

Il est dit virtuel car il relie deux réseaux locaux par l'intermédiaire d'internet et prive car seuls les ordinateurs faisant partie du réseau VPN peuvent accéder au données.

Lorsqu'on ne peut se permettre de relier deux réseaux locaux par une ligne spécialisée (en raison de cherté), une solution existe.

Celle de relier par support de transmission qui est internet. Sur internet les données sont facilement captées et écoutées, se qui nuit à la sécurité et la confidentialité de l'entreprise.

D'où l'utilité de placer un proxy (faisant souvent office d'un firewall) sur chacun des réseaux locaux à relier. Ainsi lorsqu'un ordinateur envoie un message d'une partie d'un VPN vers une autre partie, il passe d'abord par un proxy qui va crypter le message (par des algorithmes de cryptage). Il l'envoie en suite au proxy correspondant a d'autre partie. Celui-ci décrypte le message et le remet a son destinataire.

11.3. La cryptographie

La cryptographie est un ensemble de technique permettant de transformer les données dans le but de cacher leurs contenue, empêcher leurs modifications ou leurs utilisation illégales. Ceci permet d'obtenir un texte chiffré dont seul celui qui possède les clés de chiffrement pourra accéder à ce texte, en effectuent des transformations inverses(ou encore des algorithmes de déchiffrements). Désormais, elle sert non seulement à préserver la confidentialité des données mais aussi a garantir leurs intégrité et leurs authenticité.

La taille des clés de chiffrement dépend de la sensibilité des données à protéger.

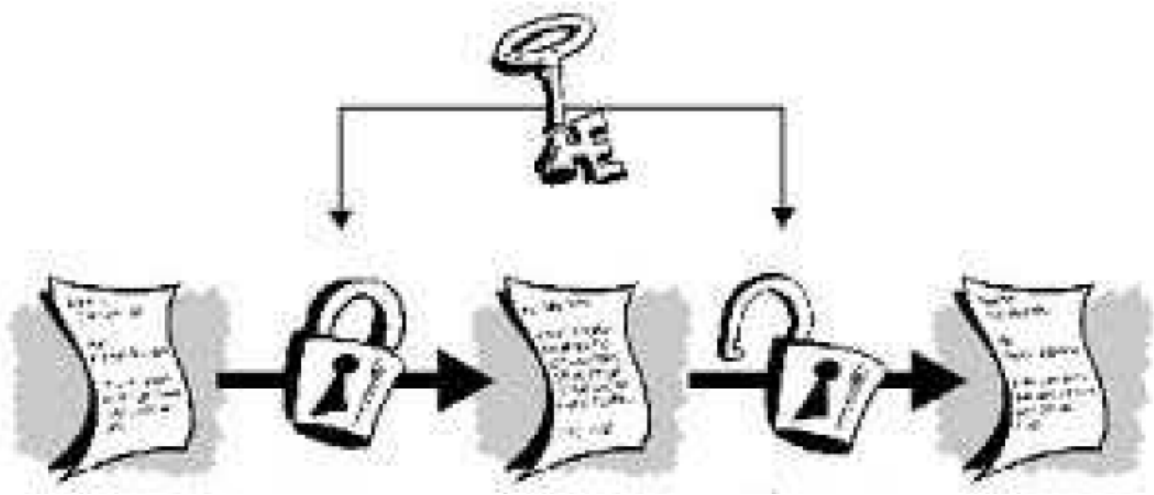
Plus ces clés sont longues plus le nombre de possibilité de clés est important, par conséquent il sera difficile de deviner la clé qui a été utilisée (cette difficulté réside dans la puissance et le temps nécessaire pour deviner la clé).

Les algorithmes de chiffrement se divisent en deux catégories :

11.3.1. Chiffrement symétrique

Ce type de chiffrement est basé sur une clé (algorithme) partagée entre les deux parties communiquant. La même clé sert à chiffrer et à déchiffrer les messages.

Ce cryptage a un inconvénient, puisqu'il faut que les deux parties possèdent la clé secrète, il faut donc la transmettre d'un bout a l'autre, ce qui est risqué sur un réseau non fiable comme internet car la clé peut ainsi être interceptée.



Texte en clair **cryptage** **texte chiffrée** **décryptage** **texte en clair**

Fig1 le fonctionnement de chiffrement symétrique

11.3.2. Chiffrement asymétrique

Ce système utilise deux clés différentes pour chaque utilisateur. Une qui privée et n'est connue que par le destinataire, qui est utiliser pour déchiffrer un texte. L'autre qui est publique et donc accessible par tout le monde, est utiliser pour chiffrer un texte en claire.

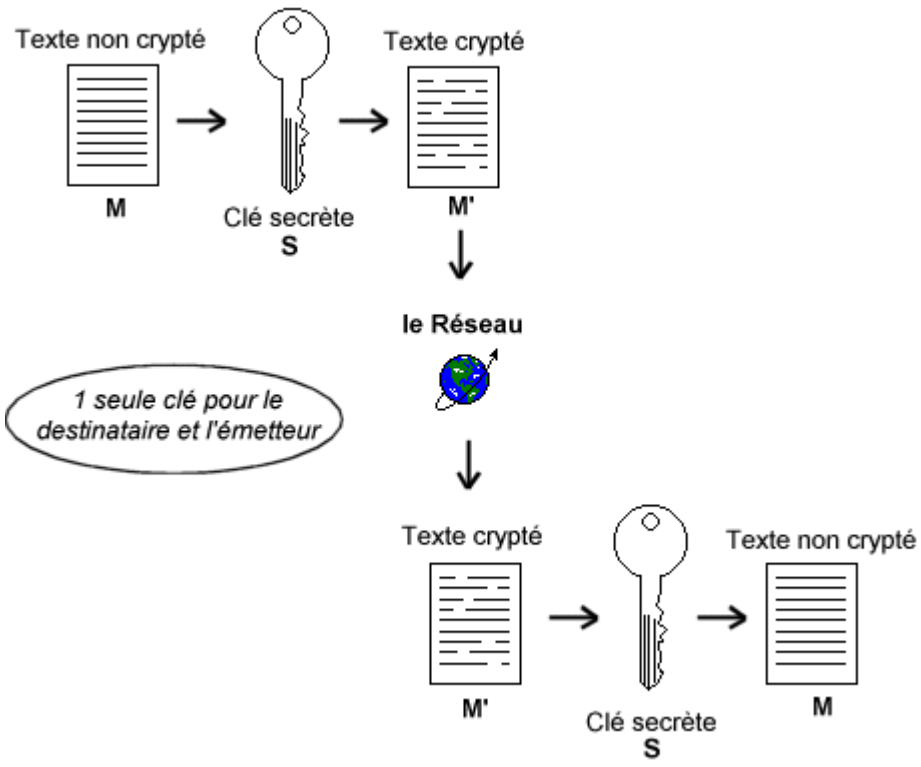


Fig2 le fonctionnement de chiffrement Asymétrique

12. les services réseaux

12.1. Serveur Web (HTTP)

Est un logiciel capable d'interpréter les requêtes http qu'il reçoit et fournie une réponse dans ce même protocole. Apache et le serveur http le plut répondue sur internet. Ce dernier, permet en effet d'ajouter des modules supplémentaire qui enrichissement le serveur au terme de fonctionnalités.

12.2. Serveur DNS

Un serveur DNS (Domain Name Service) assure la résolution de noms des réseaux TCP/IP il permet à l'utilisateur d'ordinateurs clients d'adopter des noms à la place des adresses IP numérique pour identifier les hôtes distants. Un ordinateur client envoie le nom d'un hôte distant a un serveur DNS, le quel répond avec l'adresse IP correspondante.

12.3. Serveur FTP

Un serveur FTP est utilisé dans le cas ou l'on souhaite rendre disponible des fichiers (dans un réseau local ou sur internet) et ce que se soit de manière anonyme.

Il permet de transférer des fichiers par internet ou par le biais d'un réseau informatique local (intranet). Toute personne en ayant l'autorisation, peut télécharger et envoyer des fichiers sur un ordinateur distant faisant fonctionner un tel serveur.

12.4. Le serveur DHCP

Un serveur DHCP signifie Dynamic host configuration Protocol est un protocole client / serveur qui fournit automatiquement un hôte IP (Internet Protocol) avec son adresse IP et d'autre information de configuration connexes tel que la passerelle par défaut et le masque sous réseau.

12.5. Le proxy

Un serveur est à l' origine une machine qui fait fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. Les serveurs proxy isolent les réseaux locaux et

protègent les hôtes des menaces extérieures. L'efficacité des serveurs proxy repose sur leurs capacité a mettre en cache les pages Web. La possibilité d'utiliser un service proxy pour http constitue un réel avantage. De nombreux client peuvent accéder au contenu http avec un meilleur délai de réponse.

13. Discussion

Dans ce chapitre, nous avons présenté les principales notions et concepts de la sécurité des systèmes informatiques et des réseaux, ainsi nous avons décrit plus particulièrement les menaces provenant des logiciels malveillants et introduit une politique de sécurité.

A partir de cette étude, nous pouvons dire qu'il n'existe pas de méthodes de sécurité parfaite.

A cet effet, nous établissons une politique de sécurité basée tout d'abord sur l'étude des défaillances puis sur l'utilisation d'un ensemble de méthodes et de règles.

Chapitre 2

1. Préambule

Un pare-feu est un élément du réseau informatique, logiciel et/ou matériel, qui a pour fonction de sécuriser un réseau domestique ou professionnel en définissant les types de communication autorisés ou interdits.

L'origine du terme pare-feu se trouve au théâtre. Le pare-feu ou coupe-feu est un mécanisme qui permet, une fois déclenché, d'éviter au feu de se propager de la salle vers la scène. En informatique un pare-feu est donc une allégorie d'une porte empêchant feu est appelé Périphérique de protection en bordure (en anglais : Border Protection Device, ou BPD).

Peu importe le domaine dans lequel on parle de pare-feu, la définition nous ramène toujours à quelque chose bloquant ou empêchant autre chose de pénétrer librement quelque part.

2. Définition d'un pare-feu

C'est un ensemble de différents composants matériels (physique) et logiciels (logique) qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité.

Un système pare-feu fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines aux réseaux, il s'agit ainsi d'une passerelle filtrante.

Le pare-feu permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne. D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau.

.

La figure.1 schématise le fonctionnement d'un pare-feu.

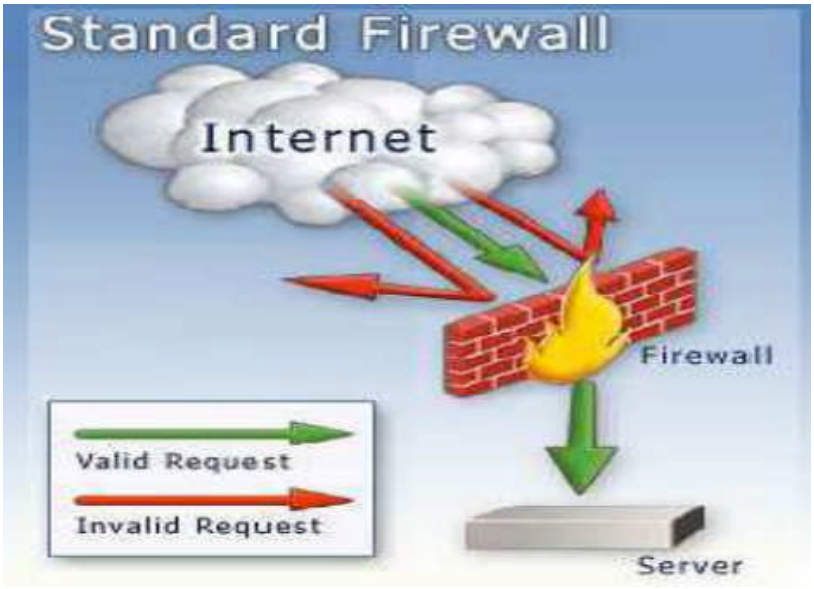


Fig.3. Le principe d'un pare-feu [3].

3. Les avantages d'un pare-feu

Les pare-feux sont configurés pour protéger contre les accès non authentifiés du réseau externe. Ceci, plus qu'autre chose, empêche les vandales de se loger sur des machines de votre réseau interne, mais autorise les utilisateurs de communiquer librement avec l'extérieur.

Les pare-feux sont également intéressants dans le sens où ils constituent un point unique où l'audit et la sécurité peuvent être imposés. Tous les échanges passeront par lui. Il pourra donner des résumés de trafic, des statistiques sur ce trafic, ou encore toutes les connexions entre les deux réseaux.

4. Les inconvénients d'un pare-feu

Les pare-feux ne protègent pas très bien des virus car il existe plusieurs méthodes pour coder des fichiers et pour les transférer.

Il est impossible de confirmer la source des données qui traverse un pare-feu, ainsi ce dernier ne peut ni en assurer l'intégrité ni protéger leurs source. Il ne fait que transférer les données d'un réseau à l'autre et incapable de détecter si elles ont été modifiées en transite.

Un pare-feu est incapable d'assurer la confidentialité des données. Une fois qu'il a permis l'accès à des données, il ne peut en maintenir le contrôle. De cette manière, les messages électroniques ou mot de passe d'authentification en claire peuvent être lus pendant leurs traverser du réseau. En fin, les firewalls ne prémunissent pas les réseaux des techniques d'écoute ou de sniffing

5. Les différents types de pare-feux.

5.1. Les pare-feux matériels

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en terme de configuration, ils sont aussi peu vulnérables aux attaques, car présent dans la « boite noire » qu'est le routeur. De plus, étant souvent très liés au matériel, l'accès à leur code est assez difficile, et le constructeur a eu toute latitude pour produire des systèmes de codes « signés » afin d'authentifier le logiciel (système RSA ou assimilés). Ce système n'est implanté que dans les pare-feux haut de gamme, car cela évite un remplacement du logiciel par un autre non produit par le fabricant, ou toute modification de ce dernier, rendant ainsi le pare-feu très sûr. Son administration est souvent plus aisée que les pare-feu bridges, les grandes marques de routeurs utilisant cet argument comme argument de vente. Leur niveau de sécurité est de plus très bon, sauf découverte de faille éventuelle comme tout pare-feu. Néanmoins, il faut savoir que l'on est totalement dépendant du constructeur du matériel pour cette mise à jour, ce qui peut être, dans certains cas, assez contraignant. Enfin, seules les spécificités prévues par le constructeur du matériel sont implémentées. Cette dépendance induit que si une possibilité nous intéresse sur un pare-feu d'une autre marque, son utilisation est impossible. Il faut donc bien déterminer à l'avance ses besoins et choisir le constructeur du routeur avec soin.

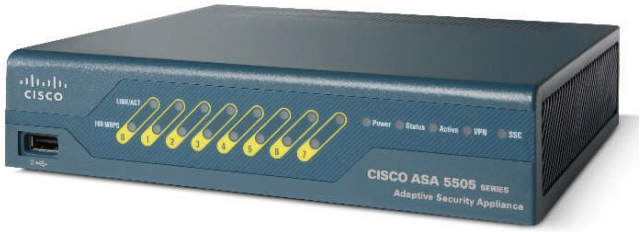


Fig4. Pare-feu "matériel"

Les avantages d'utilisation d'un pare-feu matériel sont :

- Intégré au matériel réseau.

- Administration relativement simple.

- Bon niveau de sécurité.

Les pare-feux matériels possèdent les inconvénients suivants :

- Dépendant du constructeur pour les mises à jour.

- Souvent peu flexibles.

5.2. Les pare-feux bridge

Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de pare-feu, ils ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le pare-feu est indétectable pour un hacker lambda. En effet, quand une requête ARP est émise sur le câble réseau, le pare-feu ne répondra jamais. Ses adresses MAC ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le pare-feu, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles de drop. Toute attaque devra donc « faire » avec ses règles, et essayer de les contourner.

Dans la plupart des cas, ces derniers ont une interface de configuration séparée. Un câble vient se brancher sur une troisième interface, série ou même Ethernet, et qui ne doit être utilisée que ponctuellement et dans un environnement sécurisé de préférence.

Ces pare-feux se trouvent typiquement sur les Switch.

Les avantages d'un pare-feu bridge sont :

- Impossible de l'éviter (les paquets passeront par ses interfaces)

- Peu coûteux

L'utilisation des pare-feux bridge sur les Switch peut avoir les inconvénients suivant :

- Possibilité de le contourner (il suffit de passer outre ses règles)

- Configuration souvent contraignante

- Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

5.3. Les pare-feux logiciels

Présents à la fois dans les serveurs et les routeurs « faits maison », on peut les classer en plusieurs catégories :

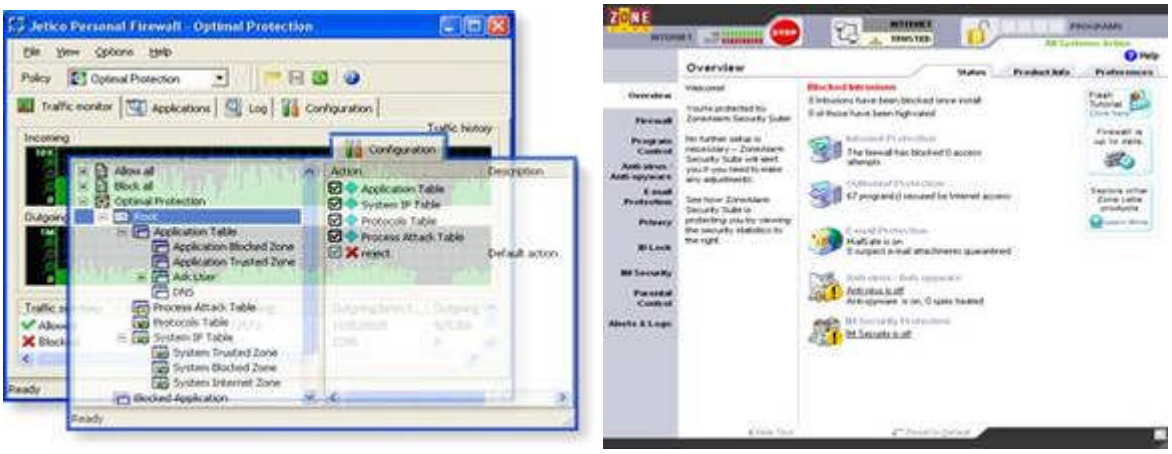


Fig5. Exemple de 2 pare-feux logiciel: jetico et zone alarm.

5.4. Les pare-feux personnels

Ils sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants

et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

Les avantages de ce type de pare-feu :

- Sécurité en bout de chaîne (le poste client)
- Personnalisable assez facilement

Ces pare-feux personnels peuvent être :

- Facilement contournable
- Difficiles à départager de par leur nombre énorme.

6. le fonctionnement d'un pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

D'autoriser la connexion (allow) ;

De bloquer la connexion (deny) ;

De rejeter la demande de connexion sans avertir l'émetteur (drop).

de L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

Soit d'autoriser uniquement les communications ayant été explicitement autorisées

Soit d'empêcher les échanges qui ont été explicitement interdits.

7. les différents types de filtrages

7.1 Le filtrage simple de paquet (Stateless)

7.1.1 Le principe

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur :

- L'adresse IP Source/Destination.
- Le numéro de port Source/Destination.
- Et bien sur le protocole de niveaux 3 ou 4.

Cela nécessite de configurer le pare-feu ou le routeur par des règles de filtrages, généralement appelées des ACL (Access Control Lists).

7.1.2 Les limites

Le premier problème vient du fait que l'administrateur réseau est rapidement contraint à autoriser un trop grand nombre d'accès, pour que le pare-feu offre une réelle protection. Par exemple, pour autoriser les connexions à Internet à partir du réseau privé, l'administrateur devra accepter toutes les connexions TCP provenant de l'Internet avec un port supérieur à 1024. Ce qui laisse beaucoup de choix à un éventuel pirate.

Il est à noter que de définir des ACL sur des routeurs haut de gamme - c'est à dire, supportant un débit important - n'est pas sans répercussion sur le débit lui-même. Enfin, ce type de filtrage ne résiste pas à certaines attaques de type IP Spoofing / IP Flooding, la mutilation de paquet, ou encore certaines attaques de type DOS. Ceci est vrai sauf dans le cadre des routeurs fonctionnant en mode distribué. Ceci permettant de gérer les ACL directement sur les interfaces sans remonter à la carte de traitement central. Les performances impactées par les ACL sont alors quasi nulles.

7.2 Le filtrage de paquet avec état (Stateful)

7.2.1 Le Principe

L'amélioration par rapport au filtrage simple, est la conservation de la trace des sessions et des connexions dans des tables d'états internes au pare-feu. Le pare-feu prend alors ses décisions en fonction des états de connexions, et peut réagir dans le cas de situations protocolaires anormales. Ce filtrage permet aussi de se protéger face à certains types d'attaques DOS.

Dans l'exemple précédent sur les connexions Internet, on va autoriser l'établissement des connexions à la demande, ce qui signifie que l'on aura plus besoin de garder tous les ports supérieurs à 1024 ouverts. Pour les protocoles UDP et ICMP, il n'y a pas de mode connecté. La solution consiste à autoriser pendant un certain délai les réponses légitimes aux paquets envoyés. Les paquets ICMP sont normalement bloqués par le pare-feu, qui doit en garder les traces. Cependant, il n'est pas nécessaire de bloquer les paquets ICMP de type 3 (destination inaccessible) et 4 (ralentissement de la source) qui ne sont pas utilisables par un attaquant. On peut donc choisir de les laisser passer, suite à l'échec d'une connexion TCP ou après l'envoi d'un paquet UDP.

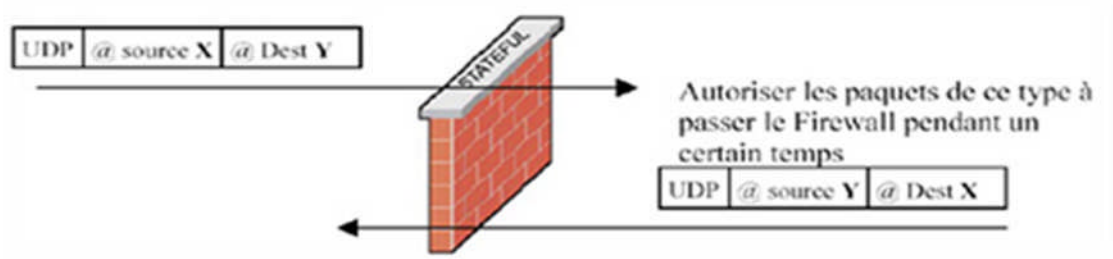


Fig6. Pare-feu en Stateful.

Pour le protocole FTP (et les protocoles fonctionnant de la même façon), c'est plus délicat puisqu'il va falloir gérer l'état de deux connexions. En effet, le protocole FTP, gère un canal de contrôle établi par le client, et un canal de données établi par le serveur. Le pare-feu devra donc laisser passer le flux de données établi par le serveur. Ce qui implique que le pare-

feu connaisse le protocole FTP, et tous les protocoles fonctionnant sur le même principe. Cette technique est connue sous le nom de filtrage dynamique (Stateful Inspection) et a été inventée par Checkpoint. Mais cette technique est maintenant gérée par d'autres fabricants.

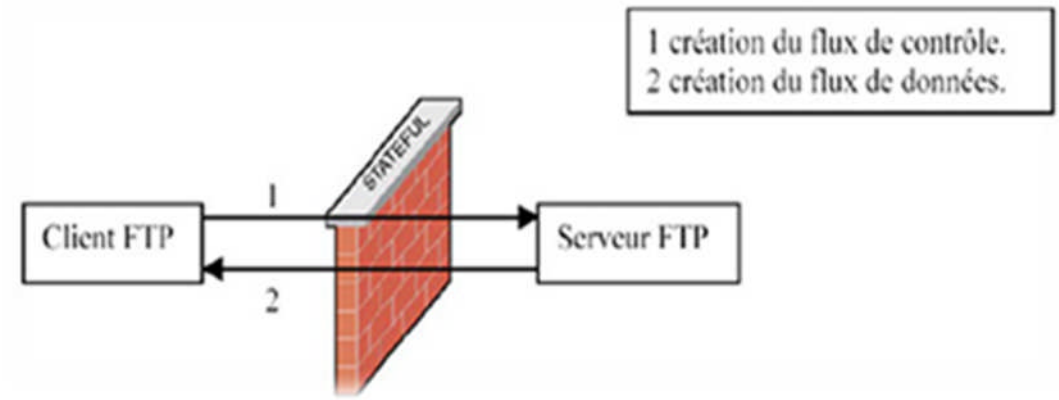


Fig7. Pare-feu en stateful connections FTP.

7.2.2 Les limites

Tout d'abord, il convient de s'assurer que les deux techniques sont bien implémentées par les pare-feux, car certains constructeurs ne l'implémentent pas toujours correctement. Ensuite une fois que l'accès à un service a été autorisé, il n'y a aucun contrôle effectué sur les requêtes et réponses des clients et serveurs. Un serveur Http pourra donc être attaqué impunément (Comme quoi il leur en arrive des choses aux serveurs WEB !). Enfin les protocoles maisons utilisant plusieurs flux de données ne passeront pas, puisque le système de filtrage dynamique n'aura pas connaissance du protocole.

.

7.3 Le filtrage applicatif (ou pare-feu de type proxy ou proxying applicatif)

7.3.1 Le principe

Le filtrage applicatif est comme son nom l'indique réalisé au niveau de la couche Application. Pour cela, il faut bien sûr pouvoir extraire les données du protocole de niveau 7 pour les étudier. Les requêtes sont traitées par des processus dédiés, par exemple une requête de type Http sera filtrée par un processus proxy Http. Le pare-feu rejettera toutes les requêtes qui ne sont pas conformes aux spécifications du protocole. Cela implique que le pare-feu proxy connaisse toutes les règles protocolaires des protocoles qu'il doit filtrer.

7.3.2 Les limites

Le premier problème qui se pose est la finesse du filtrage réalisé par le proxy. Il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7. En outre le fait de devoir connaître les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles ou des protocoles maisons.

Mais il est indéniable que le filtrage applicatif apporte plus de sécurité que le filtrage de paquet avec état, mais cela se paie en performance. Ce qui exclut l'utilisation d'une technologie 100 % proxy pour les réseaux à gros trafic au jour d'aujourd'hui. Néanmoins d'ici quelques années, le problème technologique sera sans doute résolu.

8. Discussion

Nous avons vu, dans ce chapitre, les différents types de pare-feux, les différentes attaques et parades. Il ne faut pas perdre de vue qu'aucun pare-feu n'est infaillible et que tout pare-feu n'est efficace que s’il est bien configuré. De plus, un pare-feu n'apporte pas une sécurité maximale et n'est pas une fin en soi. Il n'est qu'un outil pour sécuriser et ne peut en aucun cas être le seul instrument de sécurisation d'un réseau. Un système comportant énormément de failles ne deviendra jamais ultra-sécurisé juste par l'installation d'un pare-feu.

Chapitre 3

1. Préambule

L'IDS (Intrusion Detection System) et l'IPS (Intrusion Prevention System) sont deux 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.

En effet de plus en plus d'entreprises subissent des attaques qui peuvent entraîner des pertes conséquentes. Le besoin des entreprises en sécurité informatique est de plus en plus important et un élément essentiel d'une bonne politique de sécurité est l'utilisation d'un IDS.

Dans ce chapitre nous présenterons tout d'abord la notion de système de détection d'intrusion ainsi que son architecture et les différents types d'IDS.

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

2. Définition d'un IDS

La détection des intrusions est le processus de surveillance des événements se trouvant dans un système des ordinateurs ou du réseau et les analysant pour détecter les signes des intrusions, défini comme des tentatives pour compromettre la confidentialité, l'intégrité, la disponibilité ou éviter des mécanismes de sécurité de l'ordinateur ou du réseau. L'intrusion est causée par les attaques accédant au système via l'Internet, autorisée l'utilisateur du système qui essaye de gagner les privilèges supplémentaires pour lesquels ils n'ont pas autorisés, et autorisé les utilisateurs qui abusent les privilèges donnés. Le système de détection des intrusions est un logiciel ou un matériel qui automatise des surveillances et les processus analysés [4].

L'IDS est composé de capteur, analyseur et manager comme le montre la figure ci-dessous.

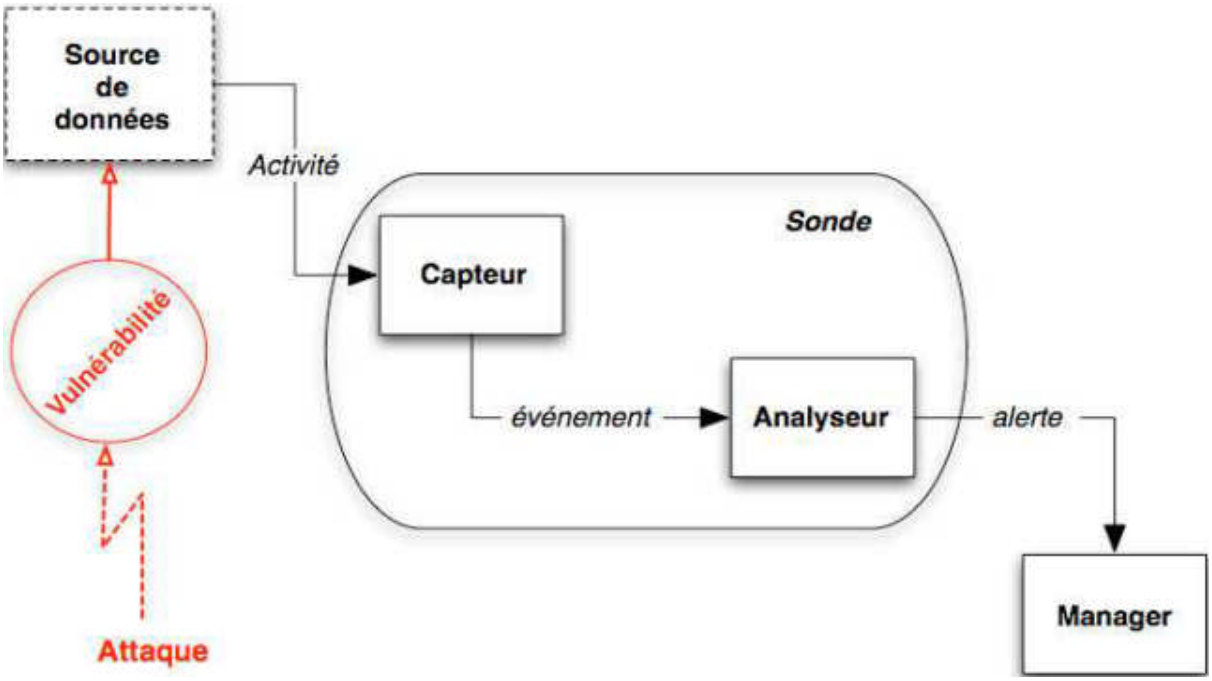


Fig.8. Architecture d'un IDS [5].

2.1. Capteur :

Le capteur observe l'activité du système par le biais d'une source de données et fournit à l'analyseur une séquence d'événements qui renseignent de l'évolution de l'état du système. Le capteur peut se contenter de transmettre directement ces données brutes, mais en général un prétraitement est effectué.

On distingue classiquement trois types de capteurs en fonction des sources de données utilisées pour observer l'activité du système : les capteurs système, les capteurs réseau et les capteurs applicatifs [5].

2.2. Analyseur :

L'objectif de l'analyseur est de déterminer si le flux d'événements fourni par le capteur contient des éléments caractéristiques d'une activité malveillante [5].

2.3. Manager

Le manager collecte les alertes produites par le capteur, les met en forme et les présente à l'opérateur. Éventuellement, le manager est chargé de la réaction à adopter qui peut être [5] :

• Confinement de l'attaque, qui a pour but de limiter les effets de l'attaque ;

• Eradication de l'attaque, qui tente d'arrêter l'attaque ;

• Recouvrement, qui est l'étape de restauration du système dans un état sain ;

• Diagnostic, qui est la phase d'identification du problème.

3. Les différentes sortes d'IDS

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

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

Les systèmes de détection d'intrusion basés sur l'hôte ou HIDS (Host IDS) analysent exclusivement l'information concernant cet hôte. Comme ils n'ont pas à contrôler le trafic du réseau mais "seulement" les activités d'un hôte ils se montrent habituellement plus précis sur les types d'attaques subies.

De plus, l'impact sur la machine concernée est sensible immédiatement, par exemple dans le cas d'une attaque réussie par un utilisateur. Ces IDS utilisent deux types de sources pour fournir une information sur l'activité de la machine : les logs et les traces d'audit du système d'exploitation.

Chacun a ses avantages : les traces d'audit sont plus précises et détaillées et fournissent une meilleure information alors que les logs qui ne fournissent que l'information essentielle sont plus petits.

Ces derniers peuvent être mieux contrôlés et analysés en raison de leur taille, mais certaines attaques peuvent passer inaperçues, alors qu'elles sont détectables par une analyse des traces d'audit.

Ce type d'IDS possède un certain nombre d'avantages : il est possible de constater immédiatement l'impact d'une attaque et donc de mieux réagir. Grâce à la quantité des informations étudiées, il est possible d'observer les activités se déroulant sur l'hôte avec précision et d'optimiser le système en fonction des activités observées.

De plus, les HIDS sont extrêmement complémentaires des NIDS. En effet, ils permettent de détecter plus facilement les attaques de type "Cheval de Troie", alors que ce type d'attaque est difficilement détectable par un NIDS. Les HIDS permettent également de détecter des attaques impossibles à détecter avec un NIDS, car elles font partie de trafic crypté.

Néanmoins, ce type d'IDS possède également ses faiblesses, qui proviennent de ses qualités : du fait de la grande quantité de données générées, ce type d'IDS est très sensible aux attaques de type DOS, qui peuvent faire exploser la taille des fichiers de logs.

Un autre inconvénient tient justement à la taille des fichiers de rapport d'alertes à examiner, qui est très contraignante pour le responsable sécurité. La taille des fichiers peut en effet atteindre plusieurs Mégaoctets.

Du fait de cette quantité de données à traiter, ils sont assez gourmands en CPU et peuvent parfois altérer les performances de la machine hôte.

Enfin, ils ont moins de facilité à détecter les attaques de type hôte que les IDS réseaux.

Les HIDS sont en général placés sur des machines sensibles, susceptibles de subir des attaques et possédantes des données sensibles pour l'entreprise. Les serveurs, web et applicatifs, peuvent notamment être protégés par un HIDS [6].

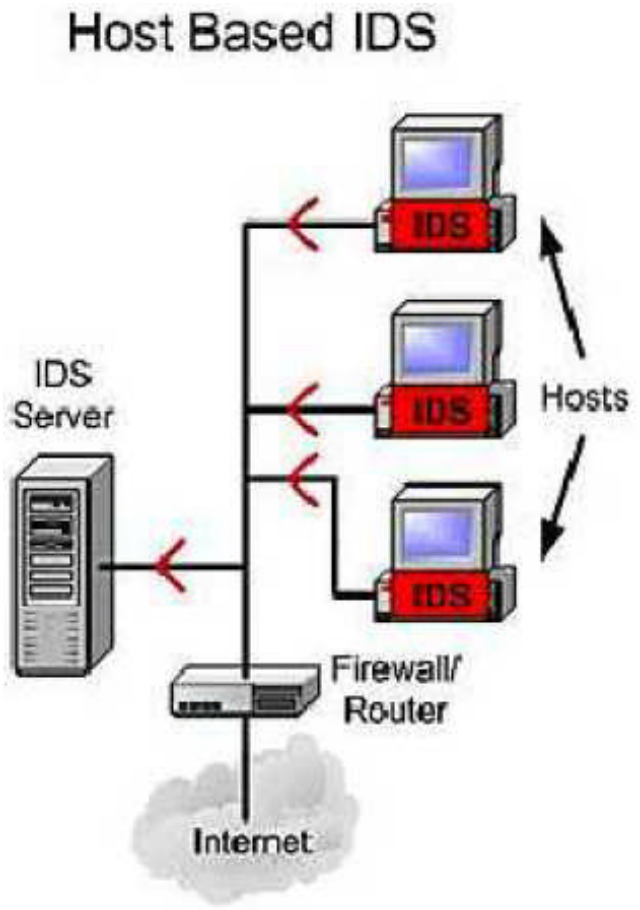


Fig9. L'architecture d'un HIDS [7].

3.2. Détection d'Intrusion basée sur une application

Les IDS basés sur les applications sont un sous-groupe des IDS hôtes.

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

L'avantage de cet IDS est qu'il lui est possible de détecter et d'empêcher des commandes particulières dont l'utilisateur pourrait se servir avec le programme et de surveiller chaque transaction entre l'utilisateur et l'application. De plus, les données sont décodées dans un contexte connu, leur analyse est donc plus fine et précise.

Par contre, du fait que cet IDS n'agit pas au niveau du noyau, la sécurité assurée est plus faible, notamment en ce qui concerne les attaques de type "Cheval de Troie".

De plus, les fichiers de log générés par ce type d'IDS sont des cibles faciles pour les attaquants et ne sont pas aussi sûrs, par exemple, que les traces d'audit du système.

Ce type d'IDS est utile pour surveiller l'activité d'une application très sensible, mais son utilisation s'effectue en général en association avec un HIDS. Il faudra dans ce cas contrôler le taux d'utilisation CPU des IDS afin de ne pas compromettre les performances de la machine [6].

3.3. La Détection d'Intrusion Réseau (NIDS)

Le rôle essentiel d'un IDS réseau est l'analyse et l'interprétation des paquets circulant sur ce réseau.

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

Les capteurs

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

Un capteur possède en général deux cartes réseaux, une placée en mode furtif sur le réseau, l'autre permettant de le connecter à la console de sécurité.

Du fait de leur invisibilité sur le réseau, il est beaucoup plus difficile de les attaquer et de savoir qu'un IDS est utilisé sur ce réseau.

Placer les capteurs

Il est possible de placer les capteurs à différents endroits, en fonction de ce que l'on souhaite observer. Les capteurs peuvent être placés avant ou après le pare-feu, ou encore dans une zone sensible que l'on veut protéger spécialement.

Si les capteurs se trouvent après un pare-feu, il leur est plus facile de dire si le pare-feu a été mal configuré ou de savoir si une attaque est venue par ce pare-feu [6].

Les capteurs placés derrière un pare-feu ont pour mission de détecter les intrusions qui n'ont pas été arrêtées par ce dernier. Il s'agit d'une utilisation courante d'un NIDS.

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

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

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

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

Les avantages des NIDS sont les suivants : les capteurs peuvent être bien sécurisés puisqu'ils se contentent d'observer le trafic et permettent donc une surveillance discrète du réseau, les attaques de type scans sont facilement détectées, et il est possible de filtrer le trafic .

Les NIDS sont très utilisés et remplissent un rôle indispensable, mais ils présentent néanmoins de nombreuses faiblesses. En effet, la probabilité de faux négatifs (attaques non détectées comme telles) est élevée et il est difficile de contrôler le réseau entier. De plus, ils doivent principalement fonctionner de manière cryptée d'où une

complication de l'analyse des paquets. Pour finir, à l'opposé des IDS basés sur l'hôte, ils ne voient pas les impacts d'une attaque [6].

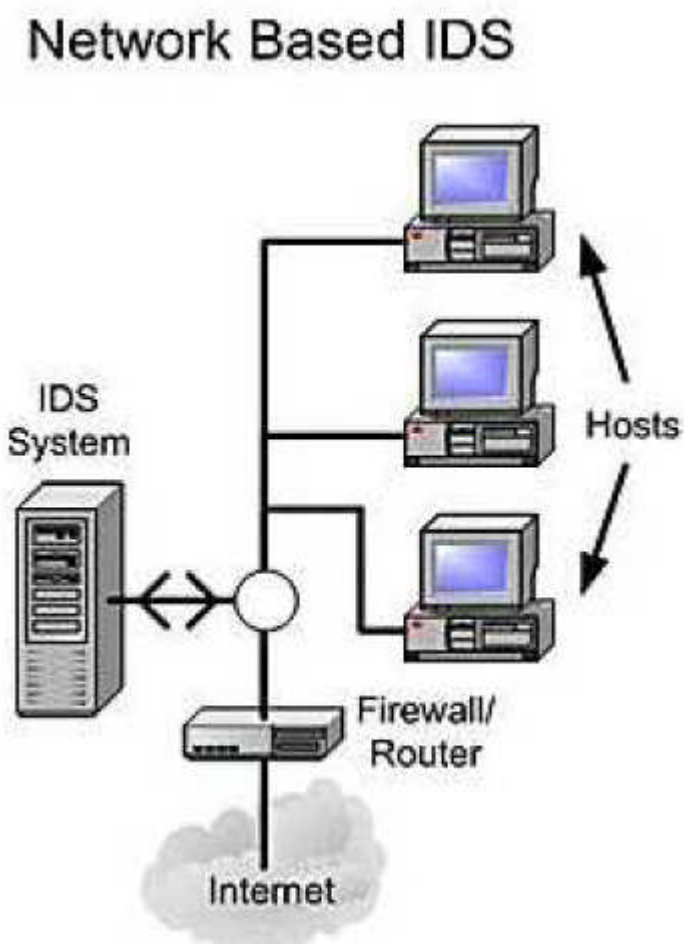


Fig.10. Architecture d'un NIDS [7].

3.4. La détection d'intrusion Hybride

Les IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, en un seul outil, de surveiller le réseau et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser le tout, et agréger/lier les informations d'origines multiples. Ainsi, on comprend que les IDS hybrides sont basés sur une architecture distribuée, où chaque

composant unifie son format d'envoi. Cela permet de communiquer et d'extraire des alertes plus pertinentes. Les avantages des IDS hybrides sont multiples : [7]

• Moins de faux positif.

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

• Possibilité de réaction sur les analyseurs.

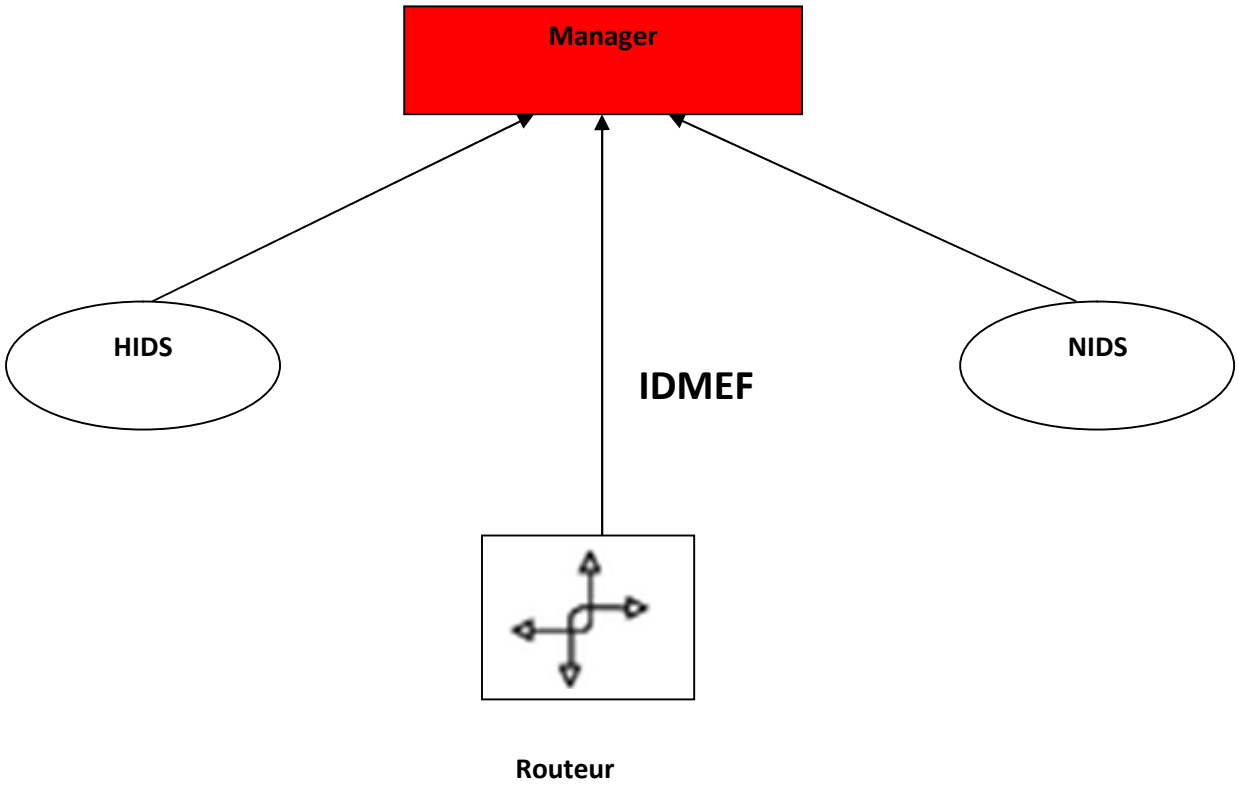


Fig11. Architecture d'un IDS Hybride [7].

3.5. Système de Détection d'Intrusion de Nœud Réseau (NNIDS)

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

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

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

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

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

Les recherches en cours visent également à améliorer les performances des IDS, notamment dans ce qui concerne les faux positifs et faux négatifs et la complexité d'administration (actuellement il faut souvent une personne dédiée à la gestion de l'IDS) [7].

4. Mode de fonctionnement d'un IDS

Il faut distinguer deux aspects dans le fonctionnement d'un IDS : le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion. Il existe deux modes de détection, la détection d'anomalies et la reconnaissance de signatures. De même, deux types de réponses existent, la réponse passive et la réponse active [6].

4.1. Modes de détection

4.1.1 La détection d'anomalies

Elle consiste à détecter des anomalies par rapport à un profil "de trafic habituel". La mise en œuvre comprend toujours une phase d'apprentissage au cours de laquelle les IDS vont "découvrir" le fonctionnement "normal" des éléments surveillés. Ils sont ainsi en mesure de signaler les divergences par rapport au fonctionnement de référence [6].

4.1.2. La reconnaissance de signature

Cette approche consiste à rechercher dans l'activité de l'élément surveillé les empreintes (ou signatures) d'attaques connues. Ce type d'IDS est purement réactif ; il ne peut détecter que les attaques dont il possède la signature. De ce fait, il nécessite des mises à jour fréquentes [6].

De plus, l'efficacité de ce système de détection dépend fortement de la précision de sa base de signature.

Une signature permet de définir les caractéristiques d'une attaque, au niveau des paquets ou au niveau protocole.

4.2. Réponse passive et active

Il existe deux types de réponses, la réponse passive et la réponse active.

4.2.1. La réponse passive :

La réponse passive d'un IDS consiste à enregistrer les intrusions détectées dans un fichier de log qui sera analysé par le responsable sécurité. Certains IDS permettent de logger l'ensemble d'une connexion identifiée comme malveillante.

Ceci permet de remédier aux failles de sécurité pour empêcher les attaques enregistrées de se reproduire, mais elle n'empêche pas directement une attaque de se produire [6].

4.2.2. La réponse active

La réponse active au contraire a pour but de stopper une attaque au moment de sa détection [6].

5. les avantages et les inconvénients

Pour finir cette présentation des IDS on résume les points forts et les points faibles de ces équipements.

5.1. Les avantage.

5.1.1Une surveillance continue et détaillée

Dans cette optique, on s'intéresse aux flux valides, mais aussi au flux non-valides qui transitent sur le réseau dont nous avons la responsabilité.

Les IDS ce sont des sondes en mode promiscuité. Ils peuvent donc analyser tout le trafic (dans le même domaine de collision), et relever des attaques, alors même qu'ils n'en sont pas la cible directe .

Bien sûr, nous évoquons ici le fonctionnement des NIDS. Les HIDS vont au contraire établir une surveillance unique du système sur lequel ils sont installés. De plus, toutes les alertes sont stockées soit dans un fichier, soit dans une base de données, ce qui permet de concevoir un historique, et d'établir des liens entre différentes attaques.

Ainsi, le responsable sécurité n'a pas besoin de surveiller le réseau en permanence pour être au courant de ce qui se passe. Une attaque de nuit ne passera plus inaperçue. Tous les IDS renvoient de nombreuses informations avec une alerte. Le type supposé d'attaque, la source, la destination, ... Tout cela permet un bonne compréhension d'un incident sécurité, et en cas de faux-positif, de le détecter rapidement .

Un autre point important dans la sécurité : nous avons maintenant des outils de filtrage très intéressants qui nous permettent de faire du contrôle par protocole (ICMP, TCP, UDP), par adresse IP, jusqu'à du suivi de connexion (couches 3 et 4).

Même si cela écarte la plupart des attaques, cela est insuffisant pour se protéger des attaques passant par des flux autorisés. Si cela est assez marginal, car difficile à mettre en place, l'ouverture de l'informatique au grand public et l'augmentation de ce type de connaissances font qu'il faudra un jour savoir s'en protéger efficacement [6].

5.1.2. Modularité de l'architecture

Il y a plusieurs solutions pour le positionnement de sondes réseaux. Il peut être intéressant de positionner les sondes pour étudier l'efficacité des protections mises en place.

Par exemple dans un réseau se cachant derrière un firewall, nous mettrons une sonde côté extérieur du firewall, et une autre côté intérieur du firewall. La première sonde permet de détecter les tentatives d'attaques dirigées contre le réseau surveillé.

La seconde sonde va remonter les attaques (préalablement détectées par la première sonde) qui ont réussi à passer le firewall. On peut ainsi suivre une attaque sur un réseau, voir si elle arrive jusqu'à sa victime, en suivant quel parcours, ...

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

Par cette méthode, nous réduisons le nombre de sondes, car il n'y a pas de doublons dans la surveillance d'une partie du réseau. Une alerte n'est remontée qu'une seule fois ce qui allège d'autant l'administration des IDS. Et pour finir, le fait de placer les sondes après les protections est plus logique, car le but premier des IDS est d'étudier les intrusions malgré les protections [6].

5.1.3. Les HIDS et les NIDS se complètent

Nous avons évoqué jusqu'ici principalement le cas des NIDS. Les IDS se cantonnent à la surveillance des systèmes sur lesquels ils sont hébergés. Mais ils sont extrêmement utiles. Par exemple dans le suivi d'une attaque évoqué précédemment, grâce aux sondes NIDS, nous pouvons suivre son parcours, mais le NIDS ne gère pas les équipements terminaux pour reconnaitre l'impact final sur la machine. C'est ici que le HIDS se révèle utile. De plus, la remontée d'alerte est locale et vers un manager. Ainsi, la surveillance réseau et des équipements terminaux est centralisée [6].

5.2. Les inconvénients

5.2.1. Besoin de connaissances en sécurité

La mise en place de sonde sécurité fait appel à de bonnes connaissances en sécurité. L'installation en elle-même des logiciels est à la portée de n'importe quel informaticien. En revanche l'exploitation des remontées d'alertes nécessite des connaissances plus pointues.

Les interfaces fournissent beaucoup d'informations, et permettent des tris facilitant beaucoup le travail, mais l'intervention humaine est toujours indispensable.

La configuration, et l'administration des IDS nécessitent beaucoup de temps, et de connaissances.

C'est un outil d'aide, qui n'est en aucun cas complètement automatisé [6] .

5.2.2. Problème de positionnement des sondes

La mise en place est importante. Il faut bien définir là où placer les sondes. Il ne s'agit pas de mettre une sonde partout où l'on veut surveiller. Il faut étudier les champs de vision des sondes suivant leur placement, si on veut recouper ces champs de vision (pour par exemple faire des doublons de surveillance ou faire un suivi d'attaque), quel détail d'analyse (à l'entrée d'un réseau, ou dans chaque domaine de collision). On découpe souvent le réseau global en un LAN, une DMZ, puis Internet. Mais il faut aussi envisager les domaines de collisions, les sous-réseaux, ...

Les connaissances réseaux sont importantes. Il faut aussi faire attention à comment sont remontées les alertes (passage par un réseau sécurisé et isolé du réseau surveillé) [6].

5.2.3. Vulnérabilités des sondes NIDS

De part leur fonctionnement en mode promiscuité, les sondes sont vulnérables. Elles captent tout le trafic, et même si un ping flood est réalisé sur une autre machine, les sondes NIDS le captureront aussi et donc en subiront les conséquences, comme si l'attaque leur était directement envoyée. Les Dos classiques seront donc très nocifs pour les sondes NIDS [6].

5.2.4. Problèmes intrinsèques à la plateforme

Beaucoup d'IDS (et plus particulièrement les IDS libres) sont des logiciels reposant sur un système d'exploitation non dédié aux IDS. Ainsi, la faiblesse d'un IDS est liée à la faiblesse de la plate-forme.

Un même logiciel sera par exemple plus vulnérable sur un PC Win98 que sur un PC Open BSD, de part la solidité de la pile IP face aux attaques, ou tout simplement de part la stabilité du système. La mise en place d'un IDS requiert donc des compétences dans la sécurisation de la plate-forme.

Une saturation de la mémoire, de la carte réseau, ou du processeur porte atteinte directement au bon fonctionnement de tout le système et donc du logiciel IDS de la machine.

Le problème de ces dysfonctionnements est que si la sonde ne peut plus remplir son rôle, le réseau n'en est pas coupé pour autant. Le responsable sécurité ne peut donc pas voir que, la sonde étant tombée, une partie du réseau n'est plus surveillée. Une redondance des surveillances sur certaines zones devrait momentanément résoudre le problème.

Comme nous venons de le voir, les IDS sont des outils indispensables à la bonne sécurité d'un réseau, néanmoins leur utilisation reste complexe et contraignante. Ces outils sont malgré tout fiables et plutôt sûrs, mais il est possible de passer outre aux réponses d'un IDS. C'est ce que nous allons voir à présent [6].

6. Contourner la réponse active d'un IDS

L'interruption de session provoquée par un IDS peut être contournée de plusieurs manières. La plupart d'entre elles se basent sur le laps de temps qui existe entre la détection d'une attaque et la prise en compte du TCP Reset par la machine cible.

Dans le cas où l'exploit à réaliser par un attaquant ne nécessite pas de session interactive, celui-ci pourra simplement positionner le flag PUSH au sein de ses paquets TCP.

En général, les piles TCP/IP ne délivrent pas chaque portion de données à l'application dès que celles-ci arrivent, cela revient trop cher en terme d'interruption logicielles. La pile accumule les données dans un buffer et dès que celui-ci est plein, elle réalise un PUSH du buffer tout entier pour envoyer les données en une seule fois [6].

7. Définition d'un IPS

Un système de prévention d'intrusion (ou IPS, Intrusion Prévention System) est un outil similaire aux IDS, sauf que ce système peut prendre des mesures afin de diminuer les risques d'impact d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement [8].

8. Principes de fonctionnement

De l'avis des analystes, le concept d'IPS (systèmes de prévention des intrusions) vise à anticiper les attaques de pirates informatiques dès lors que leur empreinte est connu. Il ne s'agit plus seulement de réagir à une attaque en cours, mais d'empêcher que celle-ci puisse seulement débuter.

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

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

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

Deux voies principales sont actuellement explorées par les promoteurs d'IPS. La première est l'approche des constructeurs d'IDS dont les produits n'ont que faiblement convaincu le marché français alors qu'ils sont utilisés dans plus d'une entreprise sur deux aux Etats-Unis. Comme pour les IDS, les IPS peuvent être orientés Host ou Réseaux.

La seconde approche touche les fournisseurs de pare-feu qui commencent à intégrer des systèmes IPS au sein de leurs matériels qui savent fonctionner "en ligne". Cela passe par exemple par l'intégration de signatures et d'un contrôle des protocoles HTTP, FTP et SMTP, mais aussi pour certains constructeurs de la mise en Asic (Application specific integrated circuit) de leurs IPS afin de s'intégrer facilement à leurs matériels [6].

9. Propriétés requises pour l'appellation IPS

Afin de pouvoir prétendre à l'appellation IPS, il faut que le produit mis en œuvre s'articule autour de fonctionnalités essentielles [6] :

- La compréhension des réseaux IP (les architectures existantes, les protocoles utilisés…) et des couches applicatives de niveau 7 doit permettre de détecter les anomalies protocolaires qui sont synonymes d'attaques.

- La connaissance des serveurs dédiés et de leur architecture logicielle afin de les enrichir de nouvelles fonctions et de les sécuriser encore plus.

- La maîtrise des sondes réseau et l'analyse des logs dans le but de déceler les attaques et d'écrire les scripts de commande qui piloteront les firewalls.

- Comprendre les besoins du client afin de consacrer en priorité la politique de défense aux fonctions vitales des réseaux de l'entreprise.

- Fonctionner à vitesse de ligne afin d'éviter tout effet néfaste sur la performance ou la disponibilité du réseau.

- Fonctionner en mode "statefull Inspection" dans le but de connaître à chaque instant le contexte de l'analyse en cours [6].

10. Bilan

Il serait illusoire de penser que les IPS constituent la parade ultime aux intrusions. D'une part, parce que le problème de la sécurité informatique existera toujours, une personne mal intentionnée, persévérante et compétente trouvera toujours un moyen de contourner, tôt ou tard les protections mises en place.

D'autre part, car les IPS mettent en œuvre des technologies immatures et qui n'ont pas encore faites leurs preuves. Beaucoup d'administrateurs hésitent encore à les intégrer dans leur réseaux fautes d'informations et de connaissance de leur fonctionnement.

De plus la diversité des technologies et des stratégies pouvant être utilisées au sein des IPS rend impossible la définition d'un standard de fait. Il est, dès lors, nécessaire de les

appréhender à travers un dialogue approfondi avec leurs concepteurs (et souvent intégrateurs…) afin d'évaluer la solution la plus appropriée aux cas d'utilisations.

Même si de plus en plus de constructeurs commencent à s'intéresser à la protection de protocoles variées, la plupart des IPS du marché sont encore largement orientées autour du port 80 et souvent inefficaces contre des attaques portés sur d'autres protocoles que le http.

A la mode, les IPS sont présents sous de nombreuses formes, on retrouve ainsi énormément de solutions "tout en un" pouvant mêler pare-feu, VPN, IDS et anti-virus. Certains pouvant même y intégrer des fonctions anti-spams. Il faut alors faire attention à la mise en œuvre car l'utilisation de certains anti-virus heuristiques, par exemple, peut faire chuter dramatiquement les performances.

L'effet marketing est très important, il est à l'origine des IPS, on prendra donc garde de bien étudier un produit et les personnes qui l'ont conçues avant de l'intégrer dans sa politique de sécurité [7].

11. Discussion

La plupart des IDS/IPS sont fiables, ce qui explique qu'ils sont souvent intégrés dans les solutions de sécurité. Toutefois, les meilleurs IDS/IPS présentent aussi des lacunes et quelques inconvénients. Donc, les IDS/IPS sont nécessaires mais ne peuvent pas se passer de l'utilisation d'autres outils de sécurité visant à combler leurs défauts.

Chapitre 4

1. Préambule

Le but de ce chapitre est de simuler deux outils de protection sur une architecture réseau de départ. Celle-ci représente le cahier de charges. L'application des deux outils de sécurité permet de découvrir la capacité de sécurisation de chaque outil. Nous commençons par présenter les différents services et rôles introduits dans les serveurs. Ensuite, nous exposerons la simulation effectuée par GNS3. Ce logiciel sera utilisé pour la configuration des éléments du réseau.

2. Le logiciel GNS3 :

GNS3 est un simulateur graphique d'équipement réseau qui nous permet de créer des topologies de réseaux complexes et d'établir des simulations. De plus, il est impossible de s'en servir pour tester les fonctionnalités des IOS Cisco. L'IOS est le système d'exploitation des routeurs, Switch et firewall Cisco. Il permet d'entrer dans l'interface graphique de chaque élément. Le GNS3 est compatible avec les systèmes d'exploitation Windows et linux.

La figure suivante présente l'emplacement des différents outils de GNS3 que nous utiliserons pour simuler un réseau.

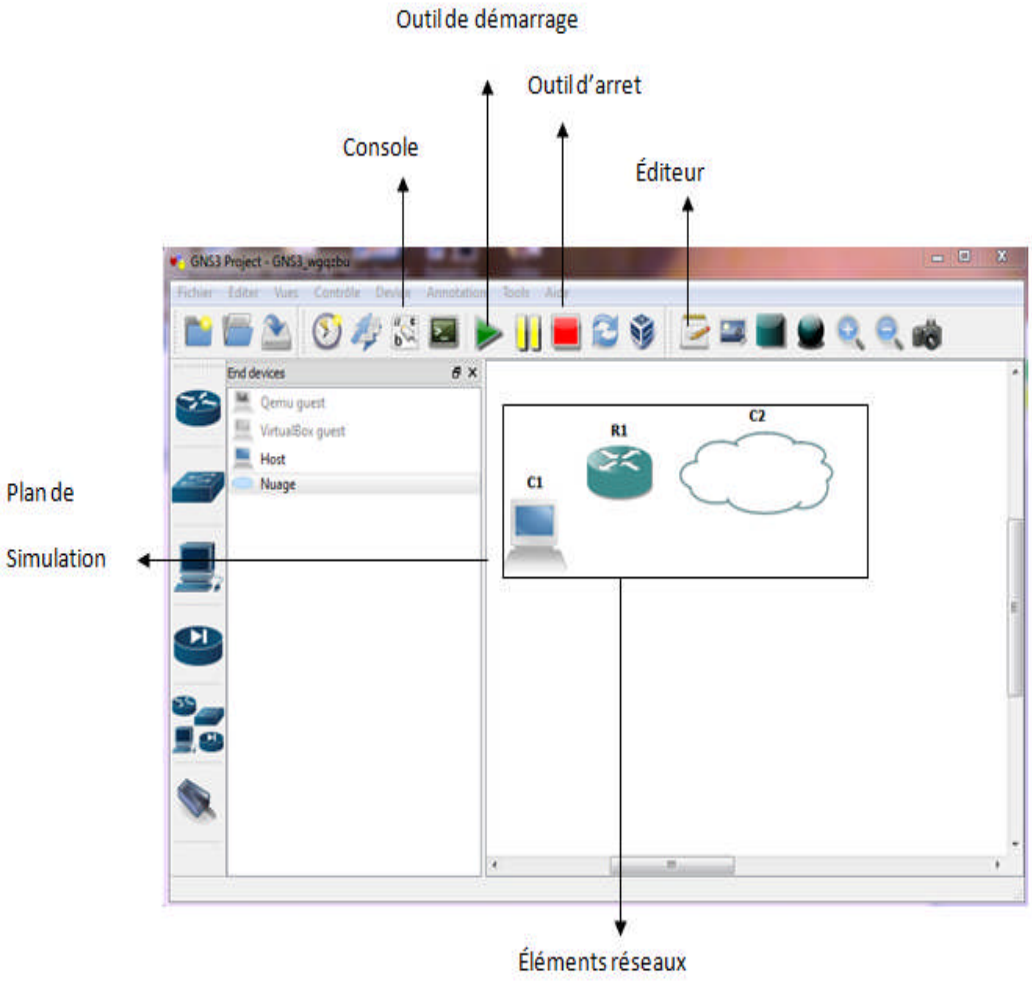


Fig.12. La fenêtre principale du GNS3.

3. Etude de l'architecture réseau du départ

Avant d'appliquer les deux méthodes de sécurité. Nous avons tout d'abord étudié les failles de sécurité du réseau de la figure 13.

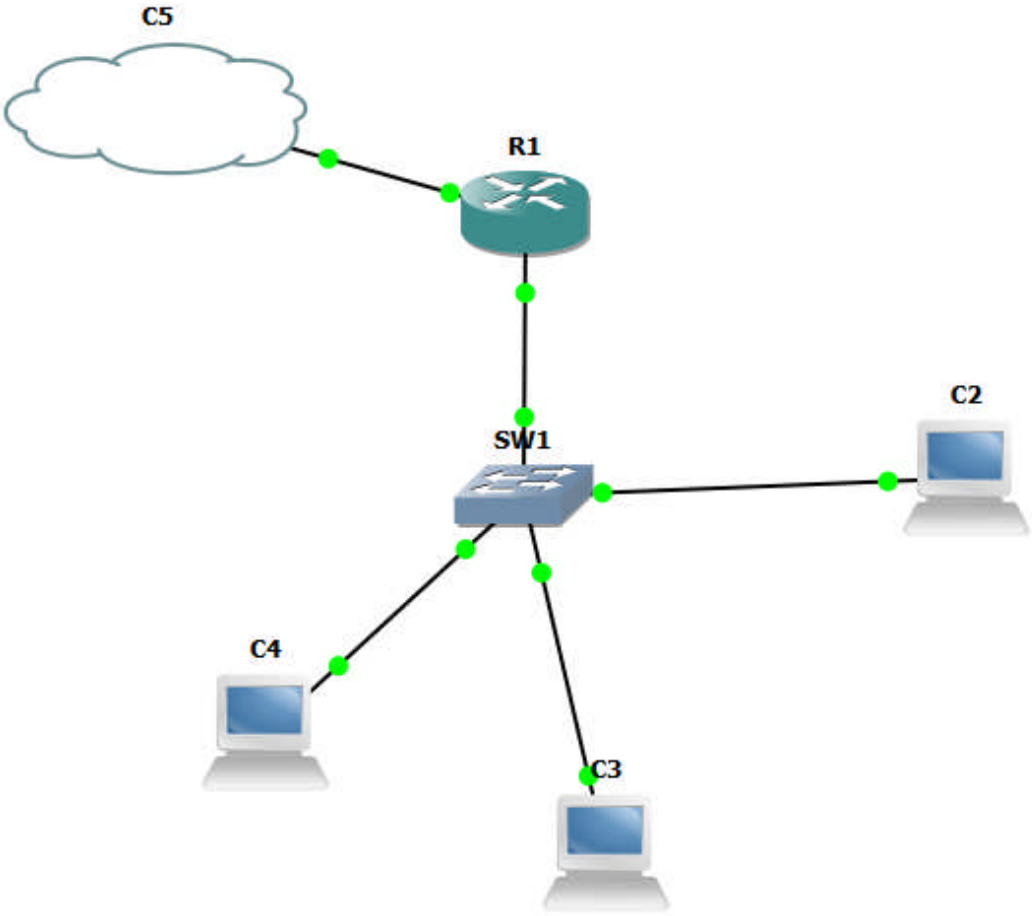


Fig.13 Architecture du réseau du départ.

Les failles de sécurité de cette architecture réseau sont :

- **Problème des filtrages des paquets :** les paquets entrants de l'extérieure sont accompagnés de différentes attaques. Les paquets sortants des clients provoquent une mauvaise communication entre eux.
- **Absence de détections des attaques :** absence de signal d'alerte pendant l'échange de paquets sur le réseau.
- **Le dysfonctionnement du système :** à force d'avoir plusieurs attaques sur le réseau, le système d'exploitation sera mis hors service et provoque un dysfonctionnement du système.

4. Nouvelle architecture en utilisant le pare-feu ASA

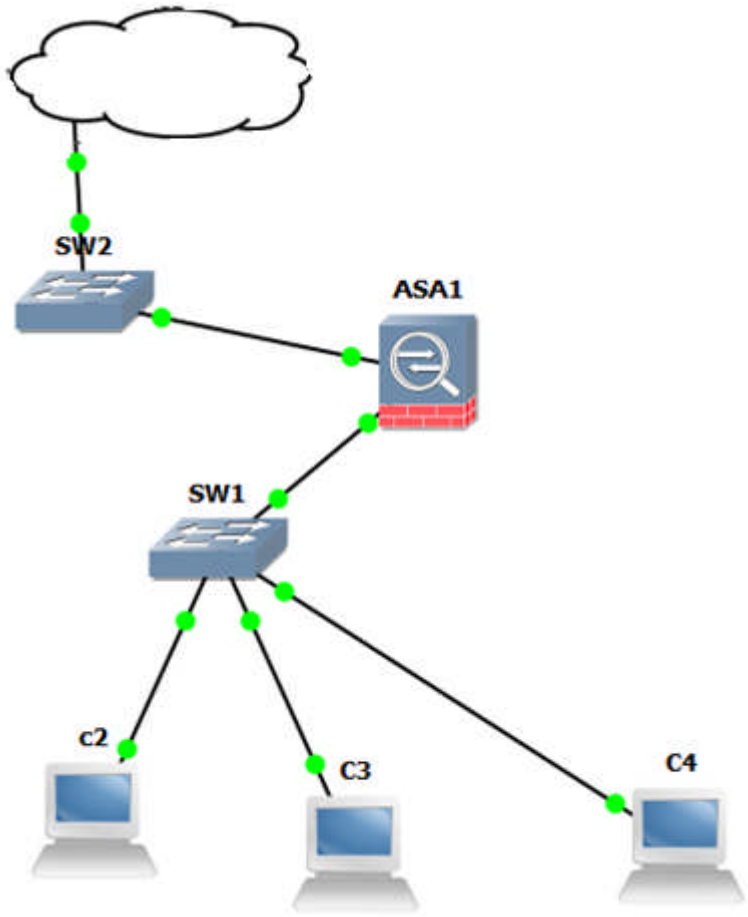


Fig.14 Nouvelle Architecture en utilisant le pare-feu

Pour ce qui concerne la configuration d'un pare-feu ASA, on clique sur EDIT puis préférences la figure s'ouvre. Puis on suit les étapes suivantes :

- Sélectionner l'onglet **Qemu**
- Dans le champ binary image on clique sur parcourir pour indiquer l'emplacement de l'IOS du ASA, on charge l'image « Initrd » et l'image « kernel »
- On clique sur « Save » puis « APPLY » et « OK »

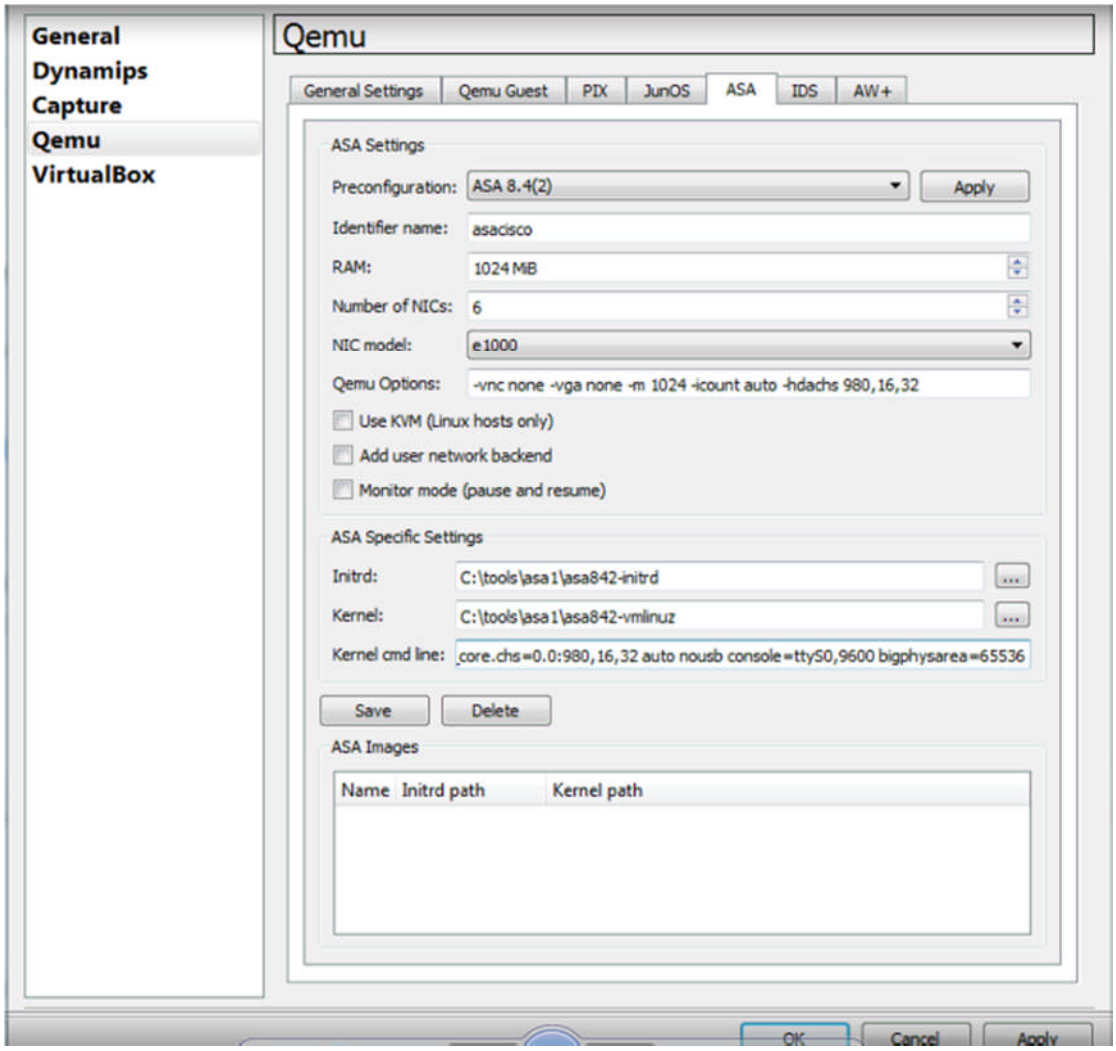


Fig.15 Configuration de Qemu dans le cas de l'ASA

5. Configuration des interfaces de l'ASA

Le principe de fonctionnement de L'ASA est : Chaque interface d'ASA possède un niveau de sécurité compris entre 0 et 100. Si nous accordons une grande confiance au réseau ce trouvant derrière une interface (le réseau dont nous avons la

métrise par exemple), nous allons lui attribuer un niveau de sécurité élever (100). A l'inverse, si nous n'avons pas confiance en un réseau (par exemple internet), nous lui attribuerons un niveau de sécurité 0.

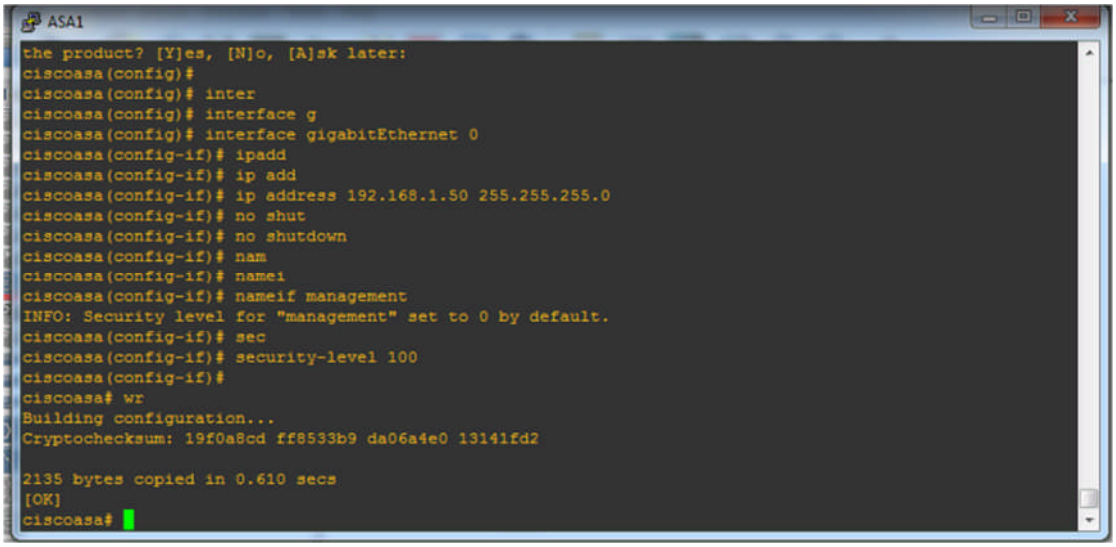


Fig.16 la configuration de l'ASA

Le réseau est protégé de l'Internet par un Firewall dont les règles de filtrage sont :

- Autoriser le trafic HTTP (port 80) de l'Internet vers le serveur Web,
- Autoriser le trafic SMTP (port 25) de l'Internet vers le serveur Web (il s'agit ici d'une erreur de configuration, le serveur n'est pas censé héberger un service de messagerie),
- Autoriser tout trafic du serveur vers l'Internet
- Interdire tout le reste.

6. Nouvelle architecture en utilisant l'IDS/IPS

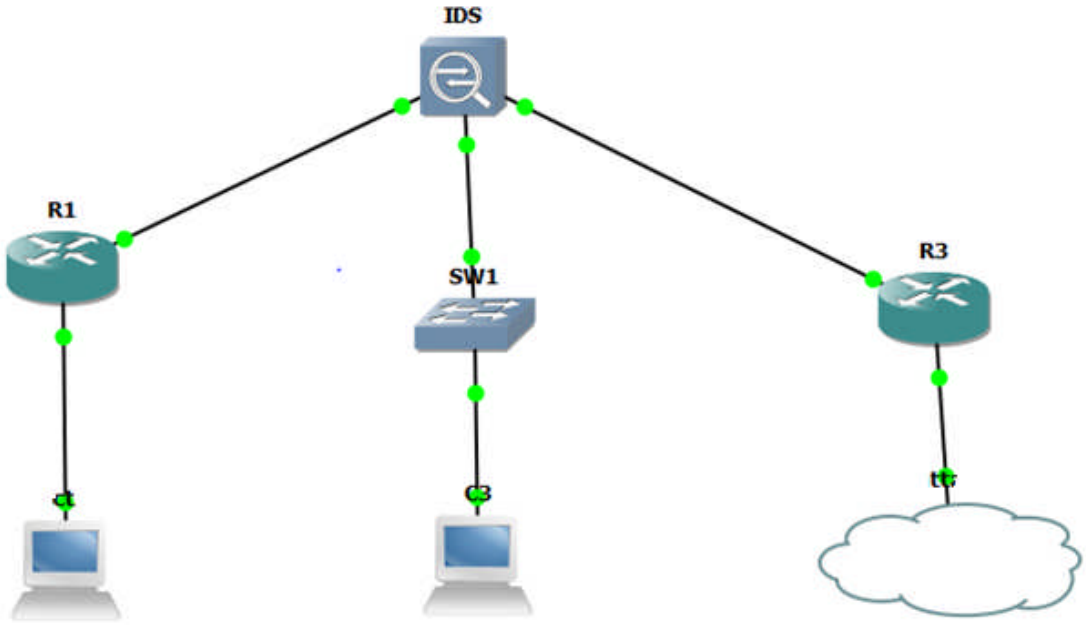


Fig.17 Nouvelle Architecture en utilisant l'IDS/IPS

Pour ce qui concerne la configuration d'un IDS/IPS, on clique sur EDIT puis préférences la figure s'ouvre. Puis on suit les étapes suivantes :

- Sélectionner l'onglet **Qemu**
- Dans le champ binary image on clique sur parcourir pour indiquer l'emplacement de l'IOS de l'IDS/IPS, on charge l'image « Initrd » et l'image « kernel »
- On clique sur « Save » puis « APPLY » et « OK »

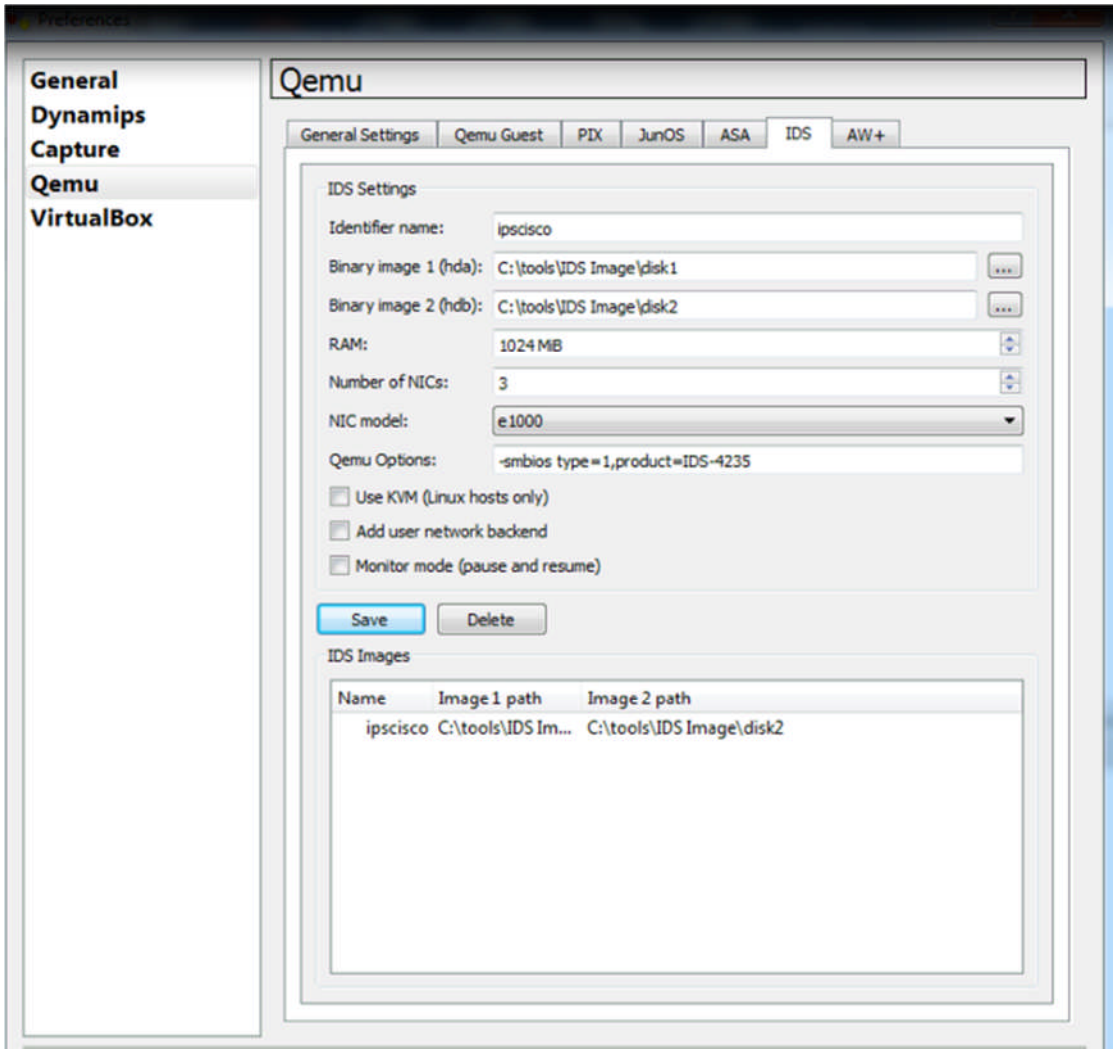


Fig.18. Configuration de Qemu dans le cas de l'IDS/IPS

7 .Configuration des interfaces de l'IDS/IPS

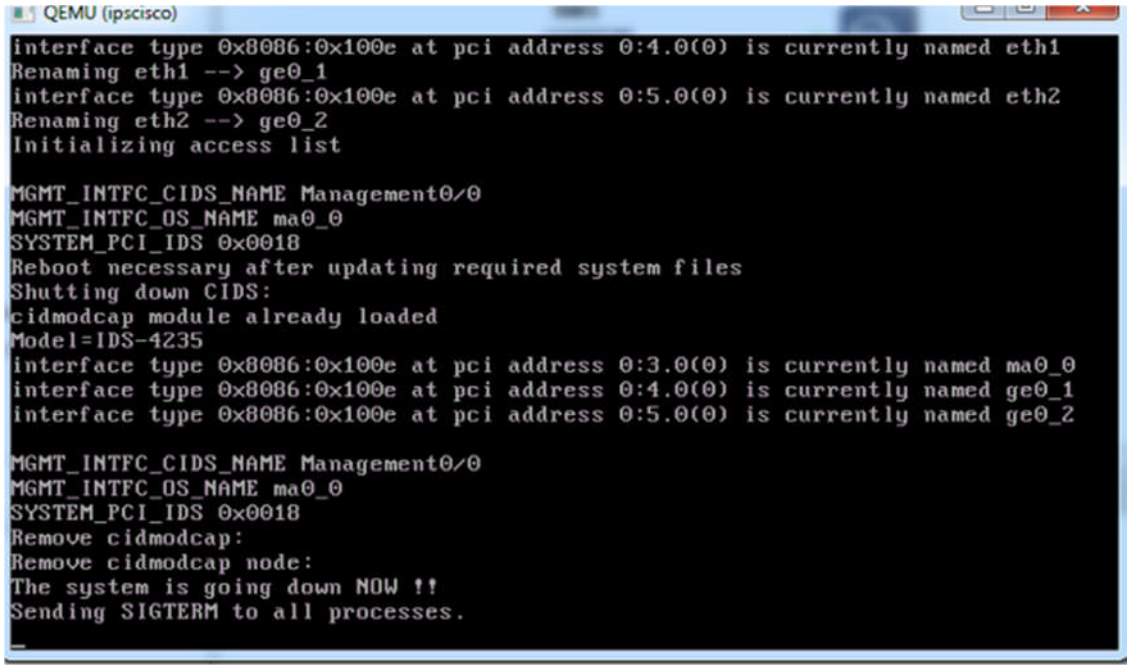


Fig.19 La configuration de l'IDS/IPS

L'efficacité d'un système de détection d'intrusions est déterminée par les mesures suivantes :

Exactitude : Le système de détection d'intrusions n'est pas exact s'il considère les actions légitimes des utilisateurs comme atypiques ou intrusives.

Performance : La performance d'un système de détection d'intrusions est mesurée par le taux de traitement des traces d'audits. Si la performance du système de détection d'intrusions est pauvre, donc la détection en temps réel n'est pas possible.

Perfection : Un système de détection d'intrusions est imparfait s'il n'arrive pas à détecter une attaque.

Tolérance aux pannes : Un système de détection d'intrusions doit être résistant aux attaques, en particulier dans le cas des attaques de déni de service.

Opportunité : Un système de détection d'intrusions doit exécuter et propager son analyse d'une manière prompte pour permettre une réaction rapide dans le cas d'existence d'une attaque.

D'aprés l'effficacité du firewall et celle de l'IDS, nous constatons que les faux négatifs qui sont realisés par le firewall sont de faux positifs lors de l'utilisation de l'IDS ainsi, les faux négatifs de l'IDS sont de faux positifs du firewall. Par conséquent, les deux outils sont complémentaires.

Pour cela, une nouvelle architecture du réseau est proposée afin de simuler les deux outils de protection pour sécuriser au maximum le réseau. Voir figure 18.

8. L'architecture réseau en utilisant les deux outils

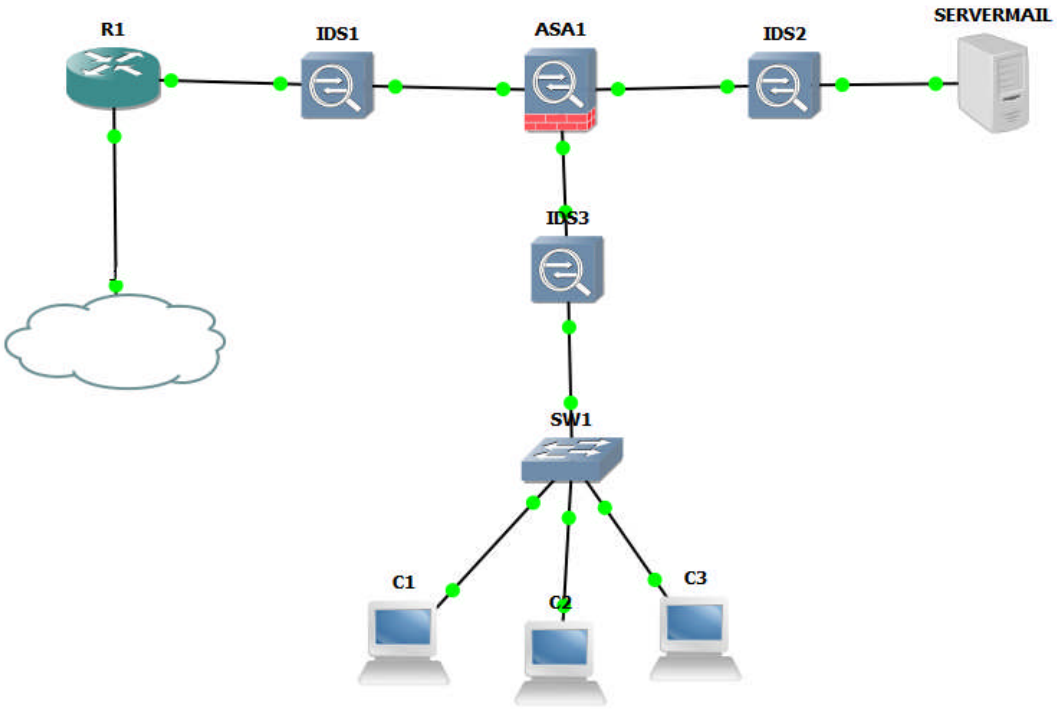


Fig.20. l'architecture du réseau du départ en utilisant les deux outils

L'emplacement des senseurs lors du déploiement d'un IDS est très important et permet de répondre à certaines problématiques selon la position du senseur par rapport au pare-feu.

- **Position 1:**

Tout le trafic entre Internet et le réseau interne ou le serveur mail est analysé. Par contre le trafic entre le réseau interne et le serveur mail 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 le serveur mail 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.

De plus le choix matériel a également une grande importance puisque le trafic réseau doit être reçu par les sondes IDS pour l'analyser quelque soit le destinataire.

Du coup le choix d'un Switch ou d'un hub doit être fait pour assurer cette fonctionnalité.

9. Discussion

D'après notre simulation, nous constatons que l'IDS / IPS est complémentaire avec les firewalls. En effet, les concepteurs de systèmes de sécurité ont tendance à intégrer les IDS et IPS directement dans les firewalls, de façon à renforcer la coopération entre ces équipements de sécurité complémentaires.

Conclusion

Conclusion

La défense en profondeur des réseaux passe par une bonne stratégie préventive pour penser ses réseaux et leurs interconnexions de façon sécurisée. Cette approche doit être complétée une fois le réseau en opération pour permettre de détecter des anomalies qui peuvent être révélatrices.

Une architecture a été choisie afin d'étudier les points forts et faibles de chaque solution de sécurité. Les deux solutions sont les pare-feux et IDS/IPS.

Afin de détecter un firewall on s'est intéressé à sa fiabilité qui assure le filtrage des paquets sur un réseau. Ensuite on s'est intéressé à la fiabilité d'un IDS et sa capacité à émettre une alerte pour toute violation de la politique de sécurité, et à sa pertinence, qui est sa capacité à n'émettre une alerte qu'en cas de violation de la politique de sécurité.

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

Il nous est paru évident que ces systèmes sont à présent indispensables aux entreprises afin d'assurer leur sécurité informatique.

Cependant, nous avons pu constater également que les produits existants ne sont pas encore suffisamment fiables (notamment en ce qui concerne les faux positifs et faux négatifs) et qu'ils restent lourds à administrer.

Les IPS, qui tentent de pallier en partie à ces problèmes, ne sont pas encore suffisamment efficaces pour être utilisés dans un contexte de production. Ils sont actuellement utilisés dans des environnements de tests afin d'évaluer leurs fiabilités. Ils manquent également d'un principe de fonctionnement "normalisé", comme il en existe pour les IDS.

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

Conclusion

Comme perspectives, nous proposons d'appliquer les deux méthodes complémentaires sur l'architecture de départ et de simuler les attaques afin de vérifier l'efficacité de l'association entre firewall et IDS/IPS.

Bibliographie

Références bibliographiques

[1] Elie MABO, «La sécurité des systèmes informatiques (Théorie) », support de cours, 2010.

[2] J.F.PILLOU : « tout sur la sécurité informatique », 2éme édition, Ed. Dunod,

2009, 232p.

[3] Ramarao Kanneganti, « sécurité des réseaux », 1ere édition, Ed. Manning, 1 juin 2008, 500 p.

[4] Tran Van Tay, « LE SYSTEME DE DETECTION DES INTRUSIONS ET LE SYSTEME D'EMPECHEMENT DES INTRUSIONS», mémoire d'ingénieur spécialité informatique et télécommunication, 2005.

[5] Jacob Zimmermann, « Vers une détection d'intrusion à fiabilité et pertinence prouvable», Thèse de doctorat, Université de Technology, Australie,

2006.

[6] Etienne Duris , « NT Réseaux –IDS et IPS », 2000, support de cours 2003-2004.

[7] Michaël AMAND et Mohamed NSIRI , « Etude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire », Rapport de projet ENAC(École nationale de l'aviation civile) , 2011

[8] Elies Jebri, « Introduction à la sécurité», support de cours, 2008 disponible sur url : https://www.google.fr/search?newwindow=1&q=ddata.Over-blog.com%2F...%2F0%2F...%2FIntroduction_a_la_securite_2008_elies.pdf, consulté le : Mai 2013.