N° d'ordre:
N° de série:

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université d'El-Oued

Faculté de Sciences et de Technologie

Mémoire fin de cycle présenté en vue de l'obtention du diplôme de

LICENCE ACADEMIQUE

Domaine Mathématiques et Informatique

Département d'Informatique

Filière : Informatique

Thème

La protection d'un réseau local contre les attaques: La mise en place le firewall

Présenté par:

Hemici maroua

Senigra Safa

Encadré par:

Mr.Gherbi kaddour

Devant le Jury composé de:

Président: Yagoube Amine

Examineur: KouladiNadjoua

Année Universitaire 2013/2014

REMERCIEMENTS :

Je remercie Allah le tout puissant, qui nous a donné la force et la patience pour l'accomplissement de ce travail.

Mes remerciements, les plus vifs, ma profonde gratitude et mes respects s'adressent à mon directeur de recherche

M.gherbikaddour.

Pour avoir accepté de m'encadrer, pour les conseils et orientations tant précieux qu'il m'a prodigué durant ce Mémoire Sans son aide, notre travail n'aurait pas vu la lumière. Je remercie vivement les membres du jury qui m'ont fait l'honneur D'accepter de juger notre travail.

Notre reconnaissance va aussi à tous ceux qui ont collaboré à notre Formation en particulier les enseignants du département D'Informatique, de l'université d'El-Oued.

Aussi à nos collègues de la promotion 2013-2014 Licence Informatique

Table des Sommaire:

Table des figures:

Liste des table:

ملخص:

يتلخص مشروعنا هذا في إنشاء شبكة محلية محمية من العوامل الخارجية و الاختراق بواسطة الجدار الناري هو برنامج أو جهاز يمنع المخترقين من الوصول إلى الكمبيوتر من خلال إحدى الشبكات أو من خلال الإنترنت. يقوم بإجراء ذلك من خلال مراجعة المعلومات الواردة من الإنترنت أو من إحدى الشبكات، ثم يقوم إما بحظرها أو السماح بها للوصول إلى الكمبيوتر.

الكلمات المفتاحية: **للشبكة** المحلية، **الاختراق**، **الجدار الناري**، الحماية.

Abstract :

Our project boils down to set up local network protected from external factors by a firewall .the firewall I sa program or device that prevent hackers and some type of malware from access to the computer through a network or through the internet. it performs by analyzing the information flow the internet and decide blocked or allowed to get into the network

KEYWORDS:

Local network(LAN),firewall, security

Résumé :

Notre projet se résume à mettre en place un réseau local protégé par des facteurs extérieurs par un pare-feu. Le pare-feu est un programme ou un périphérique qui empêche les pirates et un certain type de logiciels malveillants de l'accès à l'ordinateur via un réseau ou via Internet. il effectue en analysant le flux d'informations à l'Internet et de décider bloqué ou autorisé à entrer dans le réseau

MOTS-CLÉS :

Réseau local (LAN), pare-feu, la sécurité

Introduction Générale

Il faut assurer la sécurité des infrastructures critiques lors de la connexion. Les systèmes de commande et l'acquisition de données embarqués dans les infrastructures critiques sont menacés par des attaques externes. Une architecture sécurisée est nécessaire lors de l'établissement de la connectivité.

Il faut mettre en application des architectures plus bloquées et des technologies de sécurité, par exemple, en segmentant le réseau par des pare-feu robustes, utilisant l'authentification forte, mettant en application les programmes efficaces de gestion de la sécurité qui incluent la sécurité de tous les systèmes de commande.

Une solution aux problèmes de la sécurité est le firewall. Ce dispositif dispose de règles lui permettant de savoir comment réagir en fonction des données qui transitent par lui.

Par exemple, s'il détecte un paquet en provenance d'Internet qui possède une adresse IP correspondant à une adresse du réseau local (cas de figure ou quelqu'un essayerai de pénétrer sur le réseau local depuis l'extérieur en falsifiant l'adresse source afin de faire croire qu'il est non pas sur Internet, mais sur le réseau local), le firewall rejettera le paquet détectant une anomalie.

Parmi les autres fonctionnalités potentielles d'un firewall, on notera la possibilité de mettre en place des tunnels VPN. Les VPN (Virtual Private Network) ou réseaux privés virtuelles en français, permettant d'établir un tunnel de données cryptés et authentifiés entre un utilisateur distant et le réseau local tout en passant par l'Internet.

Partie I: Générale sur les firewall

Partie II: Conception et implication

I

Générale sur les Firewall

I.les attaques

1. Introduction

Les informations ou les systèmes d'informations d'une entreprise peuvent subir des dommages de plusieurs façons : certains intentionnels (malveillants), d'autres par accident. Ces événements seront appelés des « attaques ».

Les attaques peuvent être réalisées grâce à des moyens techniques ou par ingénierie sociale.

L'ingénierie sociale consiste à employer des méthodes non techniques pour obtenir un accès non autorisé. (4)

2. Définition d'attaques:

Les attaques réseaux s'appuient sur des vulnérabilités liées directement aux protocoles ou à le urimplémentation. Il en existe un grand nombre. Néanmoins, la plupart d'entre elles ne sont que des variantes des cinq attaques réseaux les plus connues aujourd'hui.

3. Type d'attaques:

3.1 Les attaques d'accès:

Une attaque d'accès est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information.

- **Le sniffing**

Cette attaque est utilisée par les pirates informatiques pour obtenir des mots de passe. Grâce à un logiciel appelé renifleur de paquets (sniffer), on peut intercepter toutes les paquets qui circulent sur un réseau même ceux qui ne nous sont pas destinés.

- **Les chevaux de Troie**

Les chevaux de Troie sont des programmes informatiques cachés dans d'autres programmes.

- **Porte dérobée**

Lorsqu'un pirate informatique arrive à accéder à unserveur à l'aide d'une des techniques présentées dans cette section, il souhaiterait y retourner sans avoir à tout recommencer. Pour cela, il laisse donc des portes dérobées (backdoor)qui lui permettrons de reprendre facilement le contrôle du système informatique.

Il existe différents types de portes dérobées :

-Création d'un nouveau compte administrateur avec un mot de passe choisi par le pirate.

-réation de compte ftp

-Modification des règles du pare-feu pour qu'il accepte des connections externes.

- L'ingénierie sociale

L'ingénierie sociale (social engineering en anglais) n'est pas vraiment une attaque informatique, c'est plutôt une méthode pour obtenir des informations sur un système ou des mots de passe.

3.2 Les attaques par saturation (déni de service):

Les attaques par saturation sont des attaques informatiques qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dansle but de submerger les serveurs d'une société, de bloquer pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes.

Il existe différente attaque par saturation :

-Le flooding

-Le TCP-SYN flooding

-Le smurf

-Le débordement de tampon

- **Le flooding**

Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.

- **Le TCP-SYN flooding**

Le TCP-SYN flooding est une variante du flooding qui s'appuie sur une faille du protocole TCP . En effet, on envoie un grand nombre de demande de connexions au serveur (SYN) à partir de plusieurs machines. Le serveur va envoyer un grand nombre de paquet SYN-ACK et attendre en réponse un paquet ACK qui ne viendra jamais. Si on envoie les paquets plus vite que le timeout des « demi-connexion » (connexions autorisées mais non terminé), le serveur sature et finit par se déconnecter.(4)

3.3 Attaques du type DOS et DDOS:

Commençons tout d'abord par comprendre comment fonctionnent ces attaques afin de mieux les détecter ou e les contrer. Il existe de nombreux outils pour réaliser des attaques du type DoS et DDoS.
La plupart d'entre eux sont conçus pour fonctionner avec les systèmes d'exploitation Unix et Linux, mais de plus en plus sont développés sous les systèmes

- Attaques du type DoS

Logiciel	**Type d'attaques**
Hping	UDP/TCP/ICMP flooding,Smurf
Slowloris	SYN- Flood over http
LetDown	TCP/TCP SYN flooding
Sockstress	TCP Session flooding

Table 3: Logiciels attaques du type DoS.

Pour simuler les attaques du type Déni de Service, nous utiliserons l'outil « Hping ». Celui-ci permet de réaliser l'envoi de paquets via les protocoles TCP, UDP ou ICMP en modifiant leurs en-têtes. Il est disponible sous Unix, Linux, MacOS X et Windows. Dans ce type d'attaque, le hacker lance seul son attaque contre la victime. La plupart du temps, le hacker cache son identité réseau (adresse IP et ports UDP/TCP) en se faisant passer pour une, voire plusieurs autres machines (IP Spoofing). Ainsi, il ne peut pas être reconnu par la victime. L'IP Spoofing peut être également utilisé pour faire du DNS Spoofing.
Avantages :
Il permet de générer des paquets TCP, UDP, ICMP et Raw IP contrairement à l'utilitaire d'Unix, qui ne permet lui que d'envoyer des paquets ICMP. « Hping » est principalement utilisé comme un outil de sécurité, mais il peut être utilisé sous diverses formes comme :
- Test de firewall et du réseau
- Trace route avancé
- Outil d'illustration, lors d'une formation à TCP/IP

Inconvénients :
Les attaques ne proviennent que d'une seule machine, de ce faite les attaques du type PING Flood (ICMP flooding) ralentissent la machine mais pas suffisamment pour l'empêcher d'émettre les RST qui mettent fin à la connexion (la connexion est réinitialisée).

- Attaques du type DDoS

Logiciel	**Type d'attaques**
Trinoo	UDP flooding
Tribe Flood Network (TFN) et TFN2N	UDP/TCP/TCP SYN flooding, smurf
Stacheldraht	UDP/TCP/TCP SYN flooding, smurf
Schaft	UDP/TCP/ICMP flooding
MStreamt	ACK flooding

Table 2: Logiciels attaques du type DDoS.

Compte tenu des performances actuelles des serveurs et de la généralisation des techniques de répartition de charge et de haute disponibilité, il devient de plus en plus difficile de réaliser une simple attaque DoS. De ce fait, les attaques du type Déni de service distribué sont de plus en plus prisées par les pirates informatiques car elles permettent de décupler les effets d'une attaque initiale. Malgré tout, elles restent complexes à mettre en œuvre. L'efficacité du déni de service étant liée au nombre de machines compromises, de telles attaques nécessitent donc au préalable une phase de corruption de machines sur Internet, afin d'y installer des agents, et de pouvoir plus tard utiliser cette armée d'attaquants.

Fonctionnement :

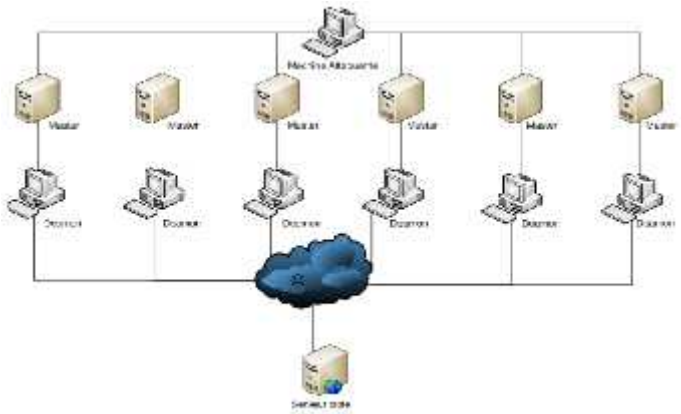

Figure I.1: Topologie l'attaque DDOS

L'architecture ci-dessus comporte 4 types d'hôtes différents: le(s)client(s) (Hacker), le(s) serveur(s) (Master), les agents (Zombies) et enfin la cible (Victime). Le client, utilisé par l'attaquant, contrôle un ou plusieurs Serveurs, lesquels communiquent avec les Agents chargés de la mise en œuvre du déni de service. Pour éviter que les Agents et les Serveurs ne puissent être utilisés par autrui (administrateur légitime de l'hôte, autres pirates) toutes les commandes vers ces programmes nécessitent des mots de passe ou des informations supplémentaires. De plus, afin d'éviter le blocage des commandes par un outil de détection ou de filtrage, les communications peuvent être cryptées.

Avantages :

- Effet multiplicateur par rapport à l'attaque DoS initiale.
- Possibilité de lancer une attaque massive de déni de service, coordonnée, par les machines infectées contre un ou plusieurs sites.
- Saturation de la bande passante du réseau en Amont.
- Avec le support d'authentification et de cryptage BlowFish, il est impossible de détecter les commandes passées, de cette manière le maitre est quasi-indétectable.

Inconvénient :

La mise en place est beaucoup plus complexe, elle nécessite au préalable une phase de corruption de machines sur Internet afin d'y installer des agents.

II: Firewall

1. Définition firewall :

Ouvrir l'entreprise vers le monde extérieur signifie aussi laisser une porte ouverte a divers acteurs étrangers. Cette porte peut être utilisée pour des actions qui, si elles ne sont pas contrôlées, peuvent nuire à l'entreprise (piratage de données, destruction,...). Les mobiles pour effectuer de tel actions sont nombreux et variés: attaque visant le vol de données, passe-temps, ...

Pour parer à ces attaques, une architecture de réseau sécurisée est nécessaire. L'architecture devant être mise en place doit comporter un composant essentiel qui est le firewall. Cette outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr.

Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il perm et d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu. Tout ceci sans l'encombrer avec des activités inutiles, et d'empêcher un éperonne sans autorisation d'accéder à ce réseau de données. (2)

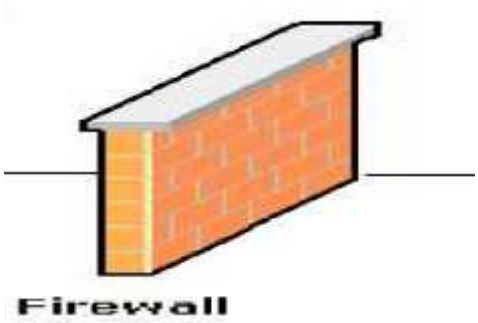

Figure: II. 1: firewall

2. Les avantages d'un firewall :

Les avantages d'un firewall peuvent être résumés dans les points suivants :

- La protection contre des services vulnérables.
- Le contrôle d'accès aux systèmes.
- La concentration de la sécurité au niveau d'un seul point.
- Les statistiques sur l'utilisation du réseau. (1)

3. Les problèmes et les limites des firewalls :

Malgré les avantages cités ci-dessus, un firewall présente un certain nombre de désavantages qui sont cités dans ce paragraphe.

- Un potentiel pour l'exploitation des backdoors (portes dérobées).
- Une protection peu efficace contre les fuites d'information.
- Les firewalls ne protègent pas contre le chargement de programmes infectés de virus à partir d'Internet.
- Un système firewall est faillible comme tout autre système.(2)

4.Les types de firewalls

Dans le cadre de ce rapport nous allons étudier deux types de firewalls le premier ce le firewall ASA de Cisco et le deuxième et celle de l'open source pfsense.

4.1. Cisco ASA :

(Cisco Adaptive Security Appliance) Une famille de dispositifs de sécurité réseau de Cisco qui fournissent des firewall, la prévention d'intrusion(IPS) et de réseau privé virtuel(VPN) de capacités. Introduite en 2005, la marque ASA remplacé autonomes ASA les firewall de Cisco(voir Cisco ASA), dispositifs IP Set VPN.

Figure:II.2: firewall ASA

4.2 pfsense:

pfSense est un logiciel gratuit, open source on peut l'utiliser comme un pare-feu ou un routeur. Il comprend une liste de fonctionnalités et un système de packages permettant de configurer selon les besoins du réseau.

4.2.1 fonctions supporté par Pfsense :

Pfsense peut être dédié à divers usage :

-Firewall .

-LAN/WAN routeur.

-point d'accès frondaison (avec portail captif).

-Sniffer.

-VPN.

-proxy et inverse proxy.

-Serveur DHCP, DNS.

-Serveur de VOIP.

5. Les composants d'un firewall :

Les composants d'un système firewall sont principalement :

- une politique de sécurité du réseau,
- des mécanismes d'authentification avancée,
- le filtrage de paquets,
- des passerelles application.

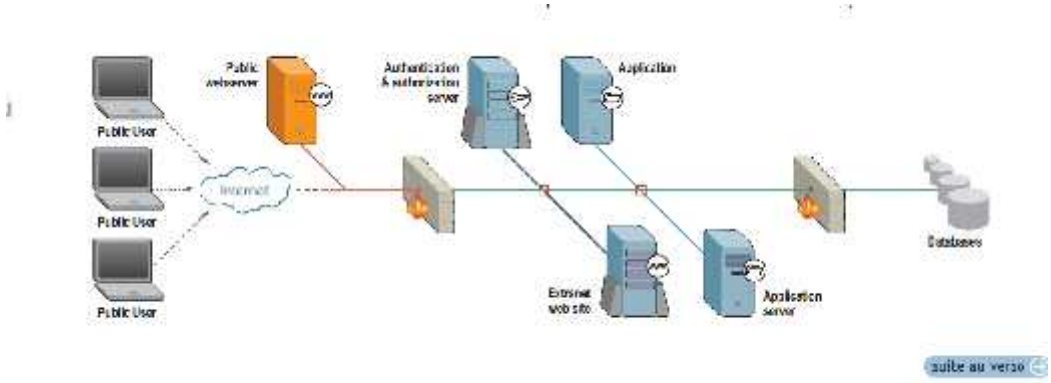

Figure: II.3: topologie d'un firewall

6.Différentes configurations de firewalls :

Dans ce qui suit est présenté un échantillon de configurations possibles de firewalls possibles :

- Parquets filtrate firewall,
- Dual-homed gateway firewall,
- Scene hot firewall,
- Screened subnet firewall.

6.1. Paquets filtrage firewalls :

Le firewall de filtrage de paquet est peut être le plus commun et le plus facile à employer pour des sites petits et non complexes. Cependant, il est le moins efficace parmi les firewalls cités dans ce paragraphe.

Le routeur de filtrage de paquets est installé au niveau de la passerelle de connexion avec Internet ou tout autre sous-réseau, et les règles de filtrage de paquets y sont configurées.

Les systèmes hôtes du site protégé ont accès direct à Internet alors que tous ou la plupart des accès émanant d'Internet vers les systèmes du site sont bloqués. Cependant, le routeur pourrait autoriser les accès sélectifs aux systèmes et aux services selon la politique d'accès prédéfinie. Un "paquet filtrage firewall"présente les inconvénients d'un routeur de filtrage de paquets.

6.2. Dual-home Gateway firewall :

Ce type de passerelle est une meilleure solution que la précédente.

Le terme "dual-home" décrit un hôte qui a deux interfaces, l'une connectée au réseau externe et l'autre au réseau interne. La capacité de routage IP de cette passerelle est inhibée(c'est-à-dire, par défaut le système n'assure pas la fonction de routage entre les deux réseaux). De plus, un routeur de filtrage de paquets peut être placé à la connexion Internet. Ceci permettrait de créer un sous-réseau intérieur (entre la passerelle et le routeur) qui serait utilisé pour la localisation de systèmes spécialisés tels que des serveurs d'information et une réserve de modems.

Les services et les accès sont fournis à travers des "proxy servers" situés sur la passerelle. Ce type de firewall permet d'implémenter la politique n'autorisant l'accès qu'à des services spécifiés explicitement puisque seuls les services pour lesquels des

"proxy servers" ont été prévus sont accessibles. La capacité de routage de l'hôte étant inhibée, on est alors sûr que d'autres paquets ne passeront pas vers le sous-réseau protégé. On peut atteindre un haut degré de discrétion(privacy) du moment que les chemins (routes) vers le sous-réseau protégé n'ont a être connu que par le firewall et non par les autres systèmes Internet(car ces derniers ne peuvent pas router les paquets directement aux systèmes protégés).

Une simple configuration de ce type de passerelle serait de fournir des services praxies pour Telnet et FTP, un service e-mails. Comme le firewall utilise un système hôte, il peut héberger des logiciels d'authentification avancés.

Ce type de configuration firewall ainsi que la configuration qui sera présentée Dans le paragraphe suivant offre la possibilité de différencier le trafic concernant un serveur d'information désastres trafic.

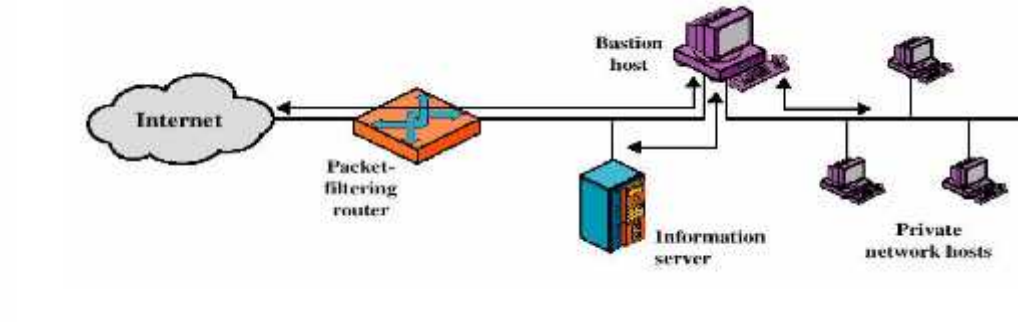

Figure II. 4 : Dual-homed gateway firewall with router

L'inflexibilité du "dual-home Gateway" pourrait être un inconvénient car tous les services seront bloqués sauf ceux dont les pyroxiles existent. Pour cela les systèmes qui nécessitent l'accès devront être placés entre la passerelle et le routeur. Il ne faut pas perdre de vue que le système hôte utilisé pour le firewall devra être très sécurisé, car si ce dernier vient à être compromis c'est tous le site qui le sera.

6.3. Scéenne hôte firewall :

Cette configuration est plus flexible que la précédente mais au prix d'une sécurité moins rigoureuse. En effet, il s'agit du même principe, mais la différence réside dans le fait que la passerelle nécessite une seule interface réseau et ne nécessite pas de sous-réseau entre le routeur et la passerelle. Ceci permet au routeur de passer certains services sûrs sans passer par la passerelle vers les systèmes internes. Les services considérés sûrs sont ceux pour lesquels des "proxies" n'existent pas mais dont les risques encourus en les utilisant ont été considérés acceptables(par exemple le service DNS). Dans cette configuration, le firewall implémente une combinaison des deux politiques avec des proportions qui dépendent du nombre et des types de services qui sont directement dirigés vers les systèmes du site.

Deux inconvénient peuvent découler de la flexibilité de ce firewall. Le premier c'est d'avoir à configurer deux systèmes; le routeur et la passerelle. Or les règles de filtrage du routeur peuvent être très complexes et difficiles à tester. Cependant, le routeur n'est amené à filtrer que le trafic se dirigeant vers la passerelle, les règles ne seront pas aussi complexes que dans le cas de l'utilisation d'un "paquet filtrent firewall" qui doit générer le traffic vers de multiples systèmes. Le deuxième est le même que celui

du "paquet filtrent firewall", c'est-à-dire que des risques de violation de sécurité existent vu qu'un certain trafic est autorisé du routeur vers le site.

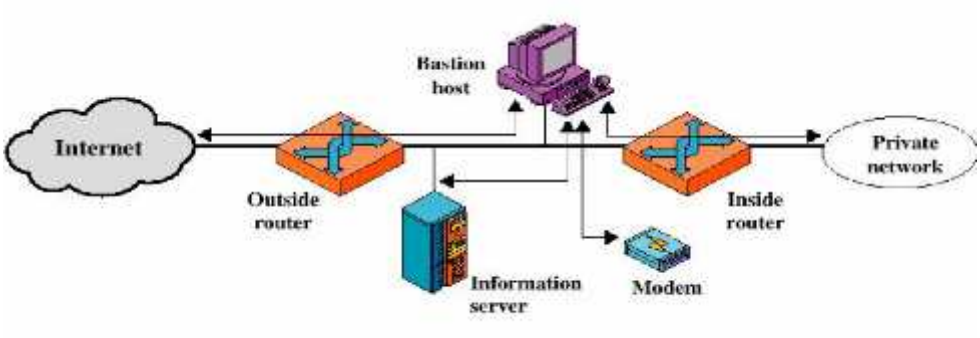

Figure II.5 : Screened host firewall

6.4. Screened subnet firewall:

Il s'agit d'une variante du "dual-home Gateway firewall" et du "scéenne hôte firewall" qui a pour objectifs d'avoir les avantages de ces deux solutions. Elle peut donc être utilisée pour localiser chaque composant du firewall sur un système séparé, afin d'atteindre un plus grand débitait une bonne flexibilité. Chaque système composant du firewall, implémentera seulement une tâche spécifique, rendant ainsi la configuration moins complexe. (1)

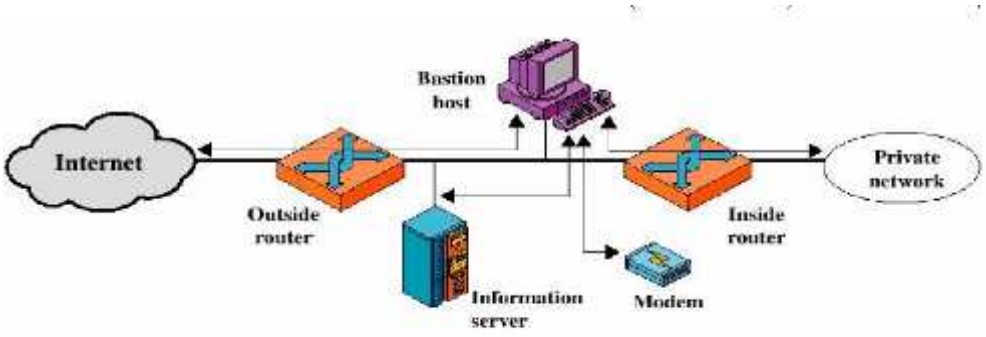

Figure II .6 : Screened subnet firewall with additional systems

7. DMZ :

Définition DMZ: réseau des machines publiant des services sur Internet. Si une de ces machines est compromise, elle ne pour rap as accéder directement aux machines du LAN.

7.1. Avantages :

- On commence à avoir une belle architecture.
- Tous les équipements sont redondés.
- Deux niveaux de firewalls de deux constructeurs différents.

7.2. Inconvénients :

- Manque de segmentation des DMZ.
- Pas de filtrage entre les utilisateurs et le Datacenter (ie la zone ressources partagées).
- Le proxy est dans le même LAN que les utilisateurs.
- Pas de prise en compte des connexions VPN, du wifi. (3)

8.les diagrammes de fonctionnement de notre système préventive:

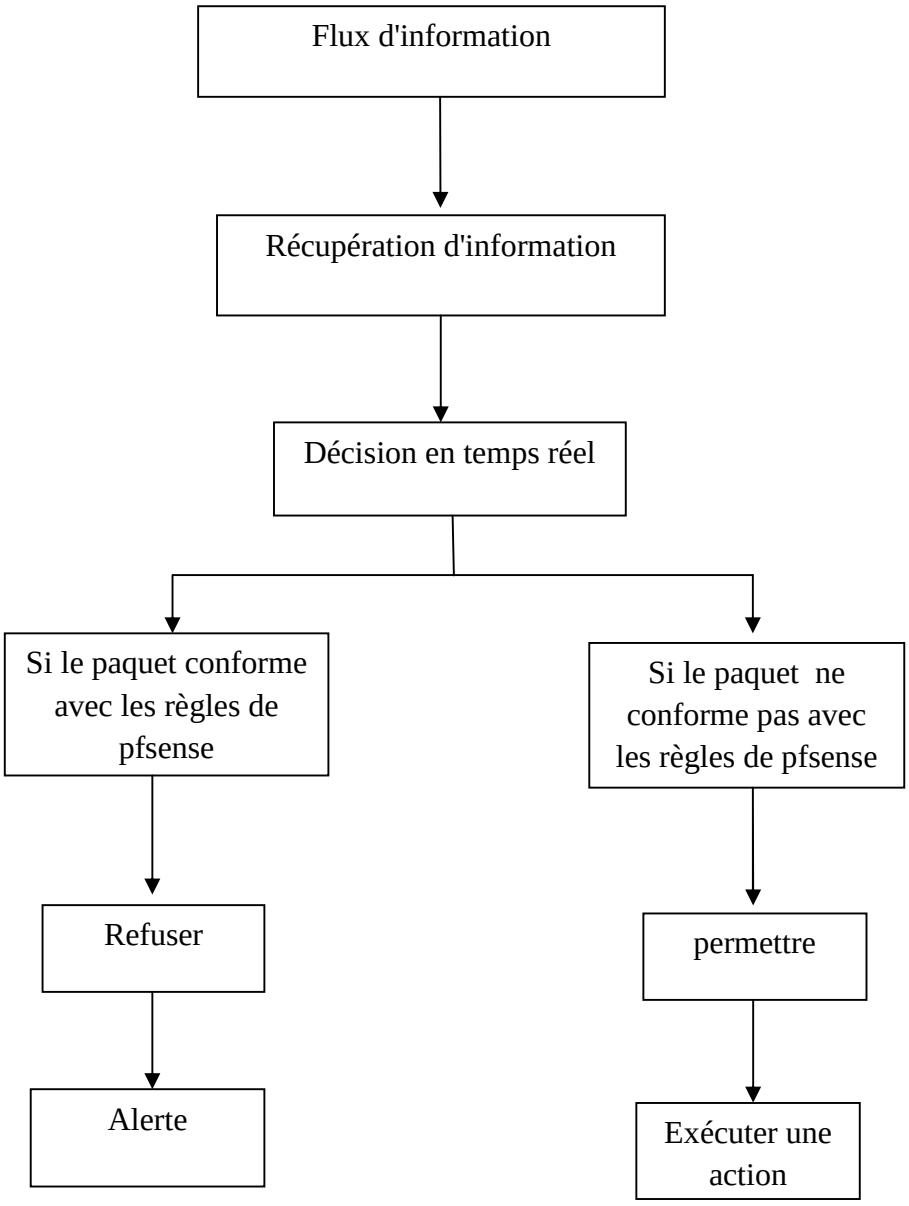

Figure II .7 : fonctionnement des firewall

Les règles de pfsense

Action : (pass, bloke)
Interface : (LAN, WAN, TCP , UCP ……..)
Protocol : any
Source : (LAN Subnet, WAN ……..)
Destination : any
Gateway : Default

II

Implementation

II. Implémentation

1.Intrication :

Ce document est un tutoriel qui vous permettra de comprendre comment pfSense et votre FreeBOX peuvent fonctionner ensemble harmonieusement.

J' ai utilisé de nombreuses images afin de rendre ce tutoriel le plus simple possible. Il est basé sur la version 1.2.3-RC3 dernière version disponible ce jour.

Afin de limiter les cas de figure et compte-tenu de la bonne adéquation entre la FreeBOX et ce type de firewall, j' ai limité mes exemples d' installation à un firewall de type Alix / WRAP. Rien ne vous empêche de fonctionner avec un autre type de matériel.

2. Interface LAN :

Si vous n' avez pas de câble série et que vous n' avez pas fait les manipulations précédentes, il est possible de vous connecter directement au firewall après son démarrage.

Préalablement vous devez avoir connecté un câble et Herent entre votre ordinateur et votre boitier (sur les cartes Alix, le port LAN est celui situé le plus à droite). Votre ordinateur doit être en mode DHCP, il recevra automatiquement une IP de la part du boitier pfSense (le service «serveur DHPC» est activé par défaut sur l' interface LAN).

Par défaut après une première installation pfSense démarre en configurant son interface LAN avec l' adresse IP 192.168.1.1. Il est donc possible d' accéder à cette interface à l' URL suivante : http://192.168.1.1- un login et un mot de passe sera exigé : login : admin --

password : pfsense

Interface Web

Si tout s' est passé comme prévu, vous devriez maintenant être capable de vous connecter à l' interface Web de pfSense. Connectez-vous à un ordinateur connecté sur votre LAN et ouvrez un navigateur Web vers l' adresse http://ip_que_vous_avez_saisi_pour_votre_LAN/

vous devriez maintenant voir un écran de bienvenue. Connectez-vous avec les identifiants

suivants :

Utilisateur : admin

Password : pfsense

3.Interface WAN :

Si ce n' est pas le cas vous avez très probablement assigné une mauvaise interface réseau à votre interface LAN, recommencez à l' étape «Premier démarrage» et veillez à bien noter les paramètres de vos interfaces LAN et WAN. Si vous ne parvenez toujours pas à vous connecter, il y a peut-être un problème avec votre câble réseau.

Votre interface WAN doit être configurée avec l' IP de votre FreeBox. Le plus simple est d' activer le service DHCP sur l' interface :

Vous pouvez aussi configurer cette interface manuellement : 87.xxx.yyy.242/24

La gateway par défaut dans mon cas est 87.xxx.yyy.254

Sélectionnez toutes les options situées sous «FTP Helper» ceci évitera de vous retrouver avec des paquets frauduleux sur votre réseau. Enregistrez votre configuration en cliquant

sur «save».

A ce stade vous avez un firewall qui fonctionne, il convient maintenant de sécuriser votre boitier (après tout c' est bien l' objectif).

3. GNS3:

3.1 Définition GNS3 :

GNS3 (Graphical Network Simulator) est un simulateur de réseau graphique qui permet l'émulation des réseaux complexes. Vous connaissez peut-être avec VMWare ou Virtual Box qui sont utilisées pour émuler les différents systèmes d'exploitation dans un environnement virtuel. Ces programmes vous permettent d'exécuter plusieurs

systèmes d'exploitation tels que Windows ou Linux dans un environnement virtuel. GNS3 permet le même type d'émulation à l'aide de Cisco Inter network Operating Systems. Il vous permet d'exécuter un IOS Cisco dans un environnement virtuel sur votre ordinateur. GNS3 est une interface graphique pour un produit appelé Dinesen.

3.2. Installation de GNS3:

1. TéléchargerGNS3 dehttp://gns3.net/downloadwin32-tout-en-un.

2. Double-cliquez sur installer avec toutes les options par défaut; Continuez à cliquer sur «Suivant» jusqu'à ce que l'installation est terminée.

3. Ouvrir GNS3 de bureau; assistant de configuration s'ouvre; Cela peut être fermé à partir de maintenant.

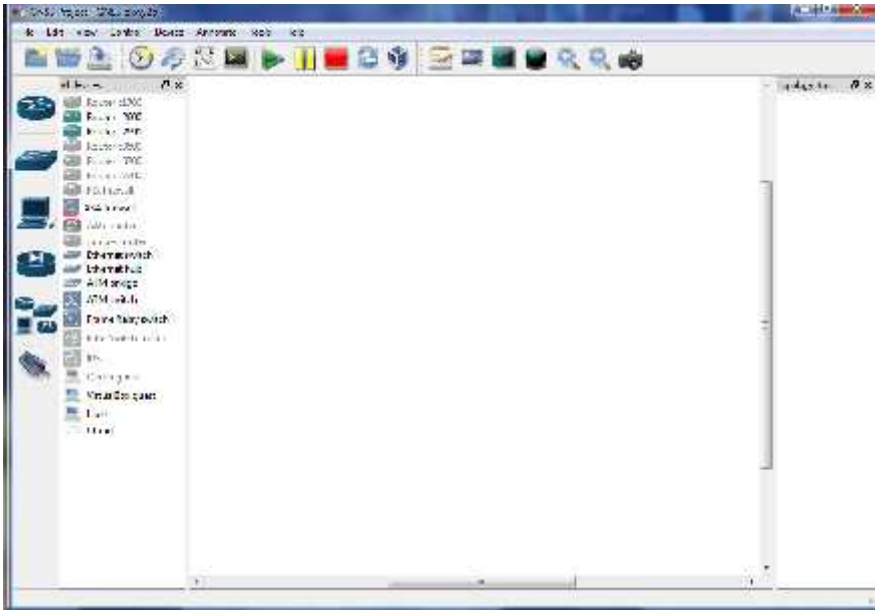

Figure III.1:L'interface générale GNS3

4. Pour commencer à travailler avecGNS3, vous devez avoir Cisco IOS.

5.Mettez le chemin du fichier Cisco IOS(type de fichier Bin)dans l'image déposer: option. Et assurez-vous que la plate-forme et le modèle est approprié pour le fichier image ont choisi.

3.3 ISO des routeurs Cisco :

Dans le menu Edition, choisissez se IOS image and hyprvisors.

Sous l'onglet IOS Images, cliquez sur puis trouver votre logiciel IOS de Cisco déposer et cliquez sur Ouvrir. Le fichier apparaît sous la forme de votre fichier image.

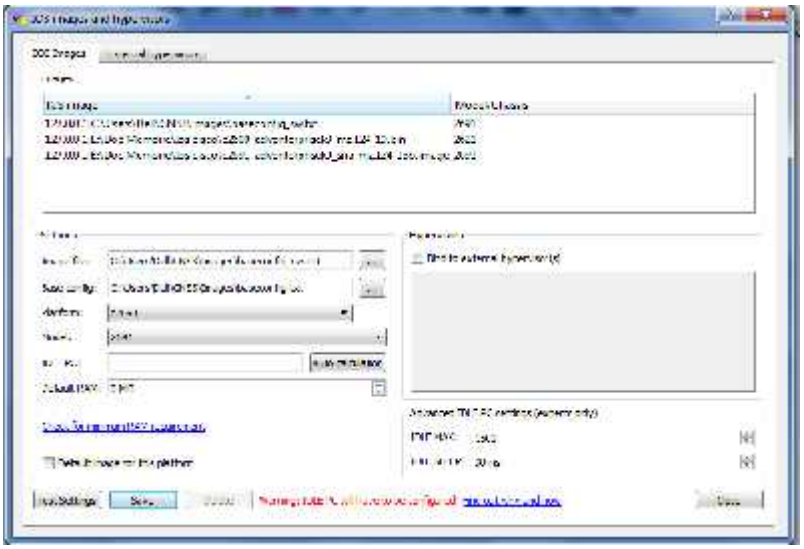

Figure III.2:L'interface de modifie ISO des routeurs par GNS3

3.4La configuration de GNS3:

Vous allez voir dans cette partie que la configuration de l'ASA dans GNS3 peut se réduire à quelques clics et ne demande, tout au plus, que 5 petites minutes. Il faut tout simplement aller dans **[Edit]**, sélectionner **[préférences ...]**. Voici ce que vous devez obtenir :

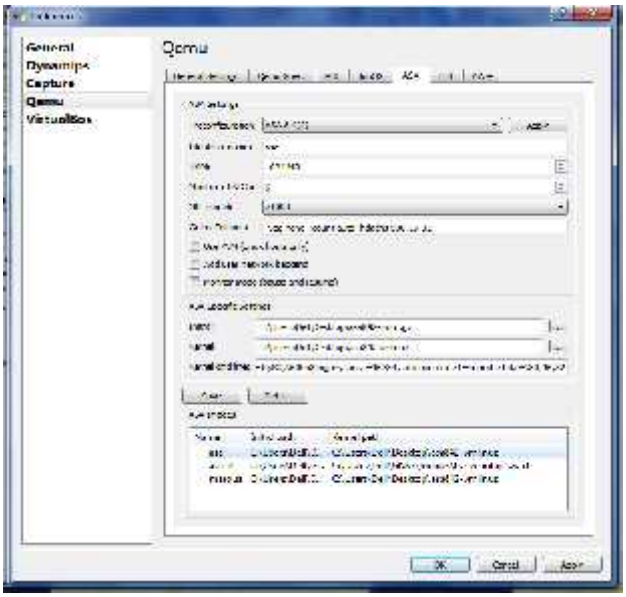

Figure III.3:L'interface de modifie firewall ASA par GNS3

Sur l'image ci-dessus vous pouvez voir la configuration initiale de GNS3. Il ne vous reste plus qu'à faire de même en copiant les informations données dans aux bons endroits, c'est à dire :

- configurer la mémoire à **1024Mo**.
- Copier la commande Qemu dans le champ **Qemu Options.**

- Champ **Initrd:** Aller chercher dans le fichier initrd dans le répertoire où vous l'avez téléchargé.
- Champ **Initrd:** Faire de même en prenant le fichier image IOS (wmlinuz) "désarchivé".
- Copier la commande kernel dans le champ **Kernel cmd line.**
- Sauvegarder votre configuration en cliquant sur **Save**.
- Enfin, appliquée la en cliquant sur **Apply** puis sur **OK.**

Et voilà, il ne vous reste plus qu'à redémarrer GNS3 pour profiter de la configuration que vous venez de réaliser.

4.Virtualbox:

4.1 Définition VirtualBox:

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

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

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

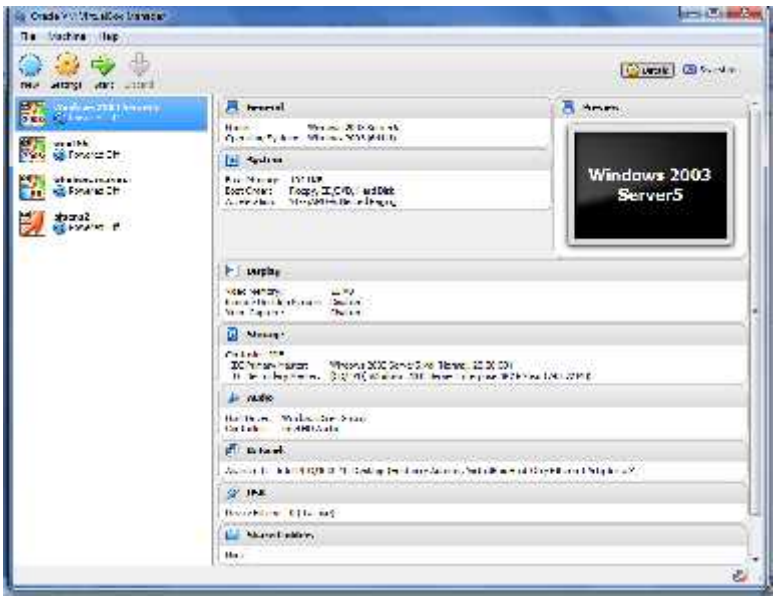

Figure III.4:L'interface générale de virtualbox

4.2 Connecter les hôtes GNS3 a VirtualBox:

A partir du menu fichier sélectionner Paramètres

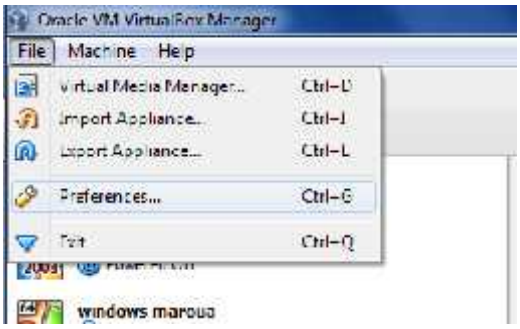

Figure III.5:L'interface paramètre sous Vbox

Cliquer sur pour ajouter des cartes réseaux.

Figure III.6:modifie réseaux par Vbox

A partir du de l'Onglet Réseau dans les configurations de la machine virtuel attribuer à elle une carte réseau de votre choix.

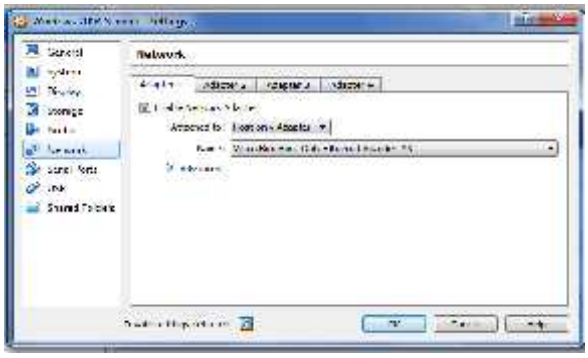

Figure III.7:choix réseau de VB

Bouton droit sur le nuage et sélectionner Configure

Figure III.8: configure cloud

Depuis l'Onglet NIO Ethernet choisissez la carte réseau qui est précédemment attribué à l'hôte dans VirtualBox et cliquer sur "Add".

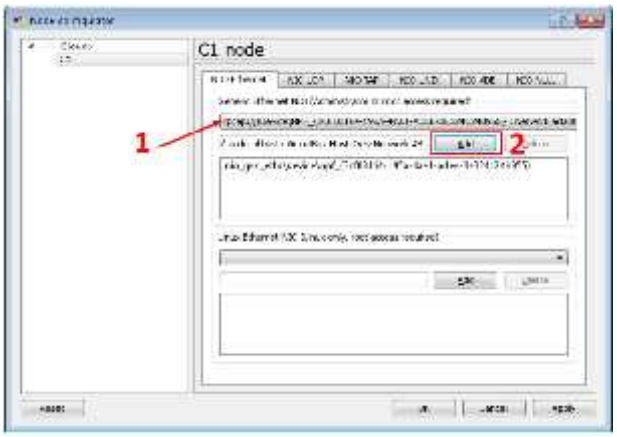

Figure III.9:L'interface modifie l'hôte réseau VB dans GNS3

Maintenant manuellement inter connecter l'interface du routeur (par exemple Fa0/0).

En déplaçant le curseur à la ligne sur le nuage d'une ligne avec un adaptateur réseau précédemment configuré apparaît.

Remarque: Si nous a vous précédemment configuré plusieurs adaptateurs pour le nuage, il y aura plusieurs lignes disponible les Maintenant des que l'hôte VB est connecter à GNS3, nous devrions démarrer le routeur et l'hôte VB. Les configurer avec des adressés IP valides pour leurs interfaces réseau et enfin vérifier l'inter-connectivité.

4.3 installation de pfsense en virtulBox:

Maintenant, la configuration d'une machine virtuelle pfSense dans votre VirtualBox, sélectionnez Paramètres, puis de stockage Vous remarquerez peut-être que j'ai deux dis que virtuel, que je vais utiliser comme le citeur primaire (8 Go) pour pfSense et Lecteur secondaire (40 Go) pour le stockage Lussac-cache

Figure III.10:L'interface Storage pfsense en VB

Ensuite, la configuration du réseau pour l'interface WAN et LAN allez à l'onglet Réseau, puis1 adaptateur pour votre interface WAN, Réglez- Pont adaptateur où il joint à Choisissez votre interface WAN où la connexion Internet de votre ordinateur hôte est connecté Cliquez sur la petite flèche pour réduire la section Advance, Réglez le mode Promiscues Refuser pour refuser les paquets dans et hors de votre hôte et la machine virtuelle Cochez la case à coche connecté par câble, il devrait être en échec état Puis cliquez sur OK.

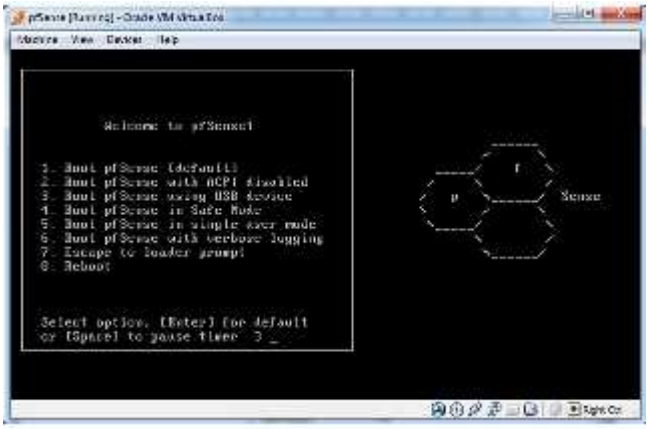

Figure III.11:L'interface pfsense par installation

Puis allumez votre machine virtuelle pfSense

Ensuite, l'assistant d'installation apparaît, sélectionnez Accepter ces paramètres

Sélectionnez Formater cette Disque puis Formatad0disque

Sélectionnez Oui, partitionad0

Sélectionnez Accepter et installer Bootblocks.

Cliquez sur OK. ATTENTION! Toutes les données dans la partition primaire seront supprimés. Soyez sûr que vous n'avez pas les fichiers importassent elle. Et vous savez ce que vous faites.

Maintenant en partitionnement que nous n'avons pas besoin de modifier simplement ,sélectionnez Accepter et Créer Maintenant, nous de vans appuyer sur Echade votre clavier plusieurs fois jus qu'à ce que vous êtes de retour sur la page principaleInstall.

Lorsque vous êtes de retour sur la page d'installation principale, sélectionnez Installer pfSense puis appuyez sur entrée.

Sélectionnez Utiliser cette géométrie, et Sélectionner le disque de partage. Puis Sélectionnez Accepter et créer à l'aide de flèche vers le bas. Et Sélectionnez Oui, partitionad1.

Ensuite, ilvous demandera de l'installation de blocs de démarrage. Vous devez justesauter cette étape. Parce que nous avons supprimé la partition de swap et de ne pas installer pfSense, l'installation sera confus et revient avec une erreur.

Mais ne vous inquiétez pas c'est normal, il vous suffit de procéder. Cliquez sur OK pour continuer.

À ce stade, vous êtes maintenant dans le menu principal de pfSense qui vous avez des privilèges d'installation d'autres fonctionnalités comme favorable. Mais pour cette instance, je dois changer l'adresse IP LANdepfSenseà192.168.5.1. J'ai donc nous avons besoin de taper2pourSetinterface (s) adresse IP.

Maintenant, nous allons aller à configurer le pfSense en utilisant l'interface web, Allez à votre boîte Virtual Manager, sélectionnez la machine virtuelle cliente appropriée que vous allez utiliser pour tester votre connexion internet. Dans ce cas, je vais utiliser Windows XP Service Pack3pourdes fins de test. Ensuite, appuyez sur le bouton Paramètres.

Maintenant, nous pou vons configurer pfSense, lancez votre Google Chrome ou tout autre navigateur Web de votre choix, et entrez la passerelle par défaut(routeur) adresse IP qui est lepfSense192.168.5.1.

Tapez admin comme Nom d'utilisateur et pfSense comme mot de passe.

4.4 La Topologie Proposée GNS3:

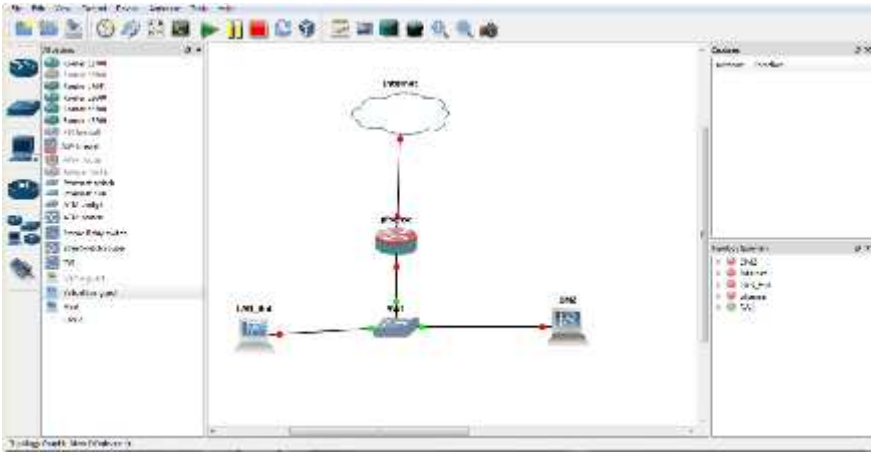

Figure III.12: Interface la topologie proposée GNS3

4.5 D'importation de pfsence au GNS3:

Maintenant notre machine virtuelle est configurée, nous allons préparer GNS3 pour intégrer cette machine. Allez au menu "**Editer**" puis "**Préférences**" et enfin "**VirtualBox**".

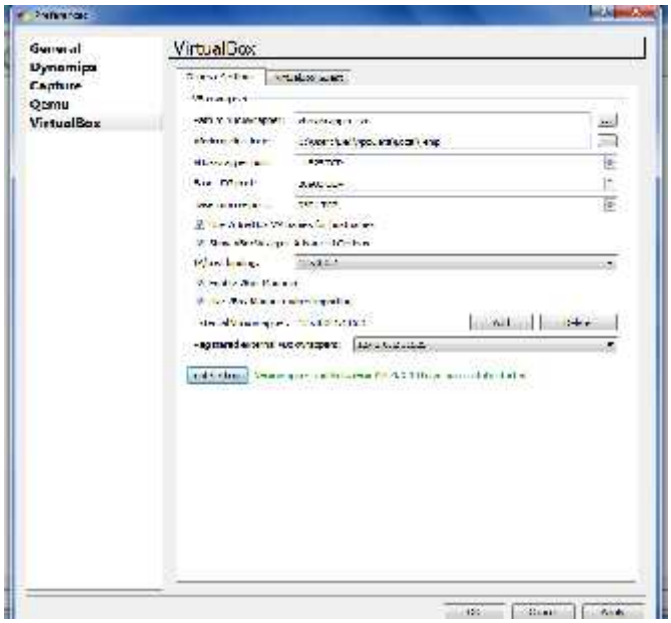

Figure III.13:L'interface configuration pfsense en GNS3

Nous allons maintenant étudier les différents para. Mètres de VirtualBox sous GNS3. On doit dans un premier temps indiquer le chemin vers "**vboxwrapper.exe**" qui est le module capable de démarrer et arrêter les machine VirtualBox à partir de GNS3. Il faut ensuite indiquer son répertoire de travail temporaire ou il gérera les échanges avec les machines virtuelles et les ports d'échanges.

Nous pouvons maintenant passer à l'onglet "**VirtualBoxGuest**" où nous allons réellement importer la machine virtuelle dans GNS3. le chose à faire dans cet onglet et de cliquer sur " **VM List**" puis cliquer sur une parmi les VM disponibles .

Figure III.14:choix pfsense dans "VM List"

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

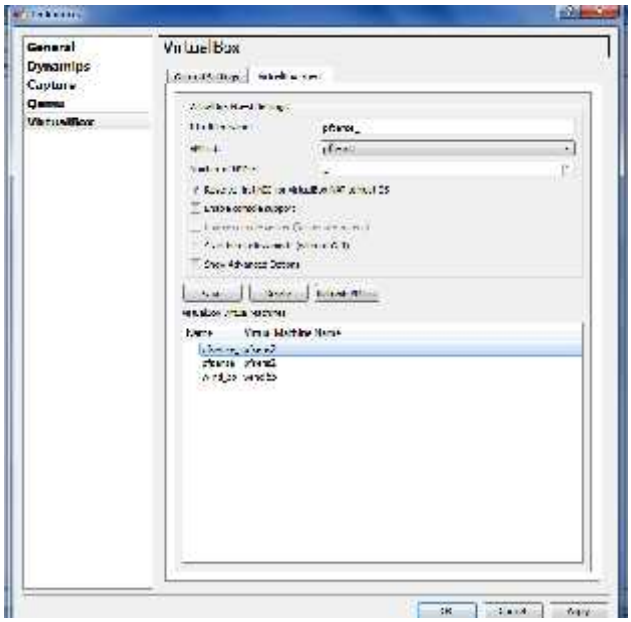

Figure III.15:L'interface ajouté pfsenseenGNS3

Puis entrer le nom de la machine après l'avoir sélectionnée, le nombre des les cartes réseau de la machine virtuelle que nous voulons connecter à notre réseau GNS3, puis le modèle de carte (laisser ce paramètre en "**automatique**" suffira).

Glissez la VM sous l'interface principale de GNS3, Pour finir, il faut cliquer sur "**Appliquer**" pour valider l'importation de la machine.

4.6 Les règles de pfsense:

Figure III .16. Interface de règle

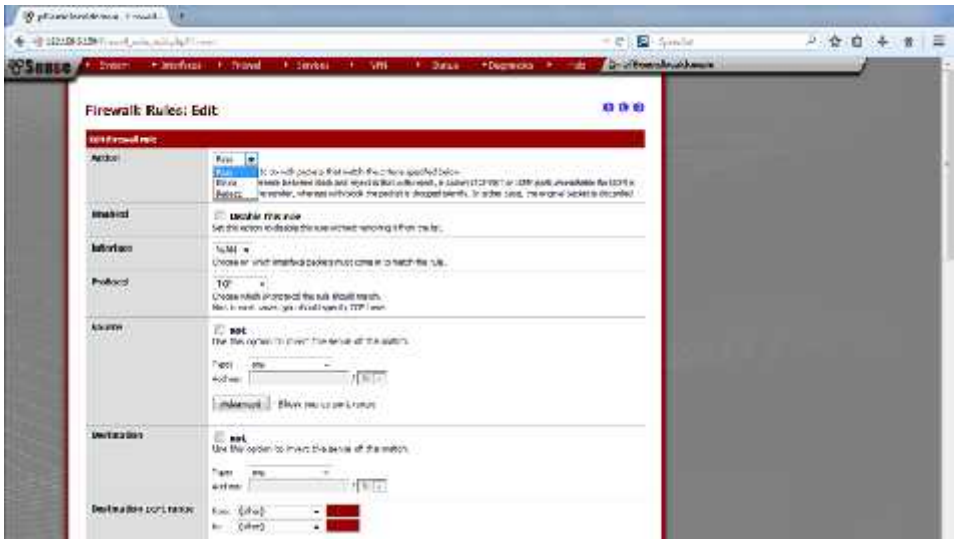

Figure III .17. La création d'une nouvelle règle

4 .7 . Quelques configuration:

4 .7.1 Configuration d'un DHCP

- **Définition:**

DHCP (Dynamic Host Configuration Protocol) permet à un ordinateur pour rejoindre un réseau basé sur IP sans avoir une adresse IP préconfigurée. DHCP est un protocole qui attribue des adresses IP uniques à des appareils, puis diffuse et renouvelle ces adresses en tant que dispositifs partent et rejoindre au réseau. Ignorer les certificats afférents avertissements de sécurité:

1. Dans la fenêtre suivante utiliser les informations d'identification par dé faut pour accéder à l'interface d'admin itération en Utilisant admin comme utilisateur et pfsence comme mot de passe

Figure III.18:La connection au pfsence

2. Maintenant vous êtes dans la fenêtre principale: le tableau de bord. Mettre à jour pfSense si nécessaire(aussi, n'oubliez pas de changer vos identifiants de connexion):

3. Cliquez sur Services DHCP Server .Assurez-vous que (enable DHCP serveur on WAN interface)sur l'interface LAN est cochée. Le système devrait avoir créé les paramètres par défaut pour le service DHCP:

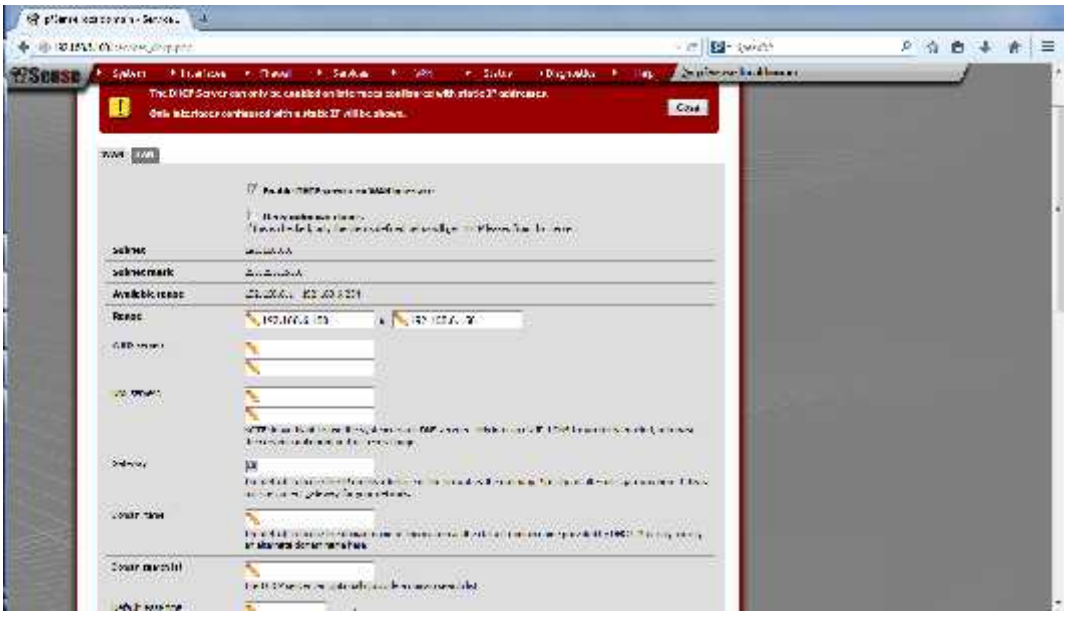

Figure III.19. création d'un serveur DHCP

4. Maintenant, Accédez à votre Centre Réseau et partage de Windows, cliquez sur Modifier les paramètres de la carte sur la gauche, puis dans la fenêtre principale d'identifier votre carte réseau physique et faites un clic droit sur elle .Cliquez sur

Propriétés, puis décochez les cases pour Internet Protocol Version 6etInternet Protocol Version4.et ourlez sur la case de DHCP

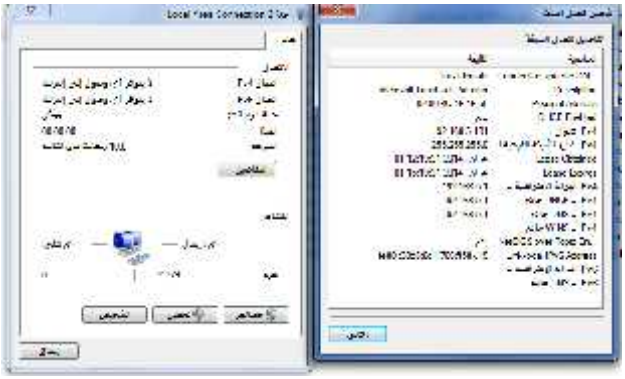

Figure III.20.DHCP pour interface local

Conclusion générale

A la fin de ce travail, je peux dire que j'ai bien pu avoir une visibilité concrète sur un domaine bien spécifique qui est la sécurité informatique.

En plus, ce travail m'a été profitable en terme d'acquérir une bonne expérience professionnelle, à travers laquelle j'ai eu l'occasion d'appliquer mes connaissances scientifiques et de confronter la notion théorique à la pratique.

Dans la deuxième partie de mémoire trouvé plusieurs inconvénients dans pfsense de la plus importante: Ne pas détecter les virus et les empêcher de pénétrer et de contrôle pfsense Spécifications techniques d'une personne sans travail dynamique . Dans ce travail, nous avons essayé traiter ces inconvénients et la création d'un programme qui nous permet de détecter et d'empêcher les pirates en même temps sans avoir le contrôle sur l'information ou assisté .

Bibliographies

(1):Nadia Nouali-Taboudjemat" Les firewalls comme solution aux problèmes de sécurité" Communication présentée au SICOM’97

(2):cour le firewalls 3éme informatique et réseaus, 2000

(3):Firewalls et autres éléments d'architecture de sécurité ,Atelier sécurité Rabat – RALL 2007.

(4):stéphane Gill" type d'attaques (Stéphane GIU)" Copyright 2003