République Algérienne Démocratique et Populaire
Ministre de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira-Bejaia

Faculté des Sciences Exactes
Département Informatique

Projet fin de cycle en master

Option : Administration et Sécurité des Réseaux

T H È M E

Sécuriser un réseaux d'entreprise avec un firewall PFsense et un IDS/IPS snort

Réalisé par :

❖ BOUREDJIOUA *Amine* ❖ MEZHOUD *Rafik*

Composante de jury :

Présidente	**Mme ADEL** *Karima*	Université de béjaia.
Examinateur	**Mr ATMANI** *Mouloud*	Université de béjaia.
Encadrant	**Mr MOKTEFI** *Mohand*	Université de béjaia.

Année universitaire : 2022/2023

Dédicaces

Je commence cette dédicace en exprimant ma profonde gratitude envers ALLAH pour m'avoir accordé la force, la persévérance et la clarté d'esprit tout au long de cette étude.

À mes chers parents, aucune dédicace ne saurait exprimer mon respect. Vous êtes la source de vie, mes sources d'inspiration. Vos sacrifices et votre amour inconditionnel ont été le moteur de ma réussite. Je vous suis infiniment reconnaissant pour tous les efforts que vous avez déployés afin de me donner les meilleures opportunités de réussite.

À mes chères sœurs ***SIHAM*** *&* ***SARA*** *que je souhaite exprimer ma profonde gratitude pour votre soutien constant et qui m'ont porté dans leurs prières et m'ont encouragé tout au long de mes études. Je dédie plus précisément cette dédicace à mon cher amis fidèle* ***ZOUBIR****, je te remercie du fond du cœur. Tes encouragements ont été une force motrice pour atteindre mes objectifs.*

À mon binôme ***RAFIK****, pour ton encouragement et ta rigueur.*

Amine.

En ce moment précieux où j'achève ce mémoire, je souhaiterais dédier ces mots empreints de gratitude et d'affection :

À ma mère, ma confidente et ma source d'inspiration. Je souhaite te remercier du fond du cœur pour tout ce que tu fais pour moi.

À mon merveilleux père décédé et qui là où il est, continue de veiller sur moi. Toi qui a toujours voulu me voir réussir.

*À mon frère « **Belkacem** » et ma sœur « **Lina** » compagnons de joie et de partage.*

À mes grands-parents, mes tantes, mes oncles, mes cousins et cousines.

*À mon meilleur ami « **Belkacem** », mon pilier, à chaque étape de ce mémoire, tu étais là, prêt à m'écouter, et me conseiller. Tu as su m'encourager lorsque j'en avais le plus besoin.*

*Je termine avec la personne qui a partagé tout le travail, mon binôme et très cher ami Mr. **BOUREDJIOUA Amine**, je tiens à te remercier pour ta contribution inestimable à ce mémoire.*

Rafik.

Remerciements

Tout d'abord, nous tenons à remercier, le Dieu miséricordieux qui nous a donné la force et le courage d'achever cette réalisation.

À nos chers parents, qui nous ont toujours encouragé et soutenu durant toute la période de nos études jusqu'à atteindre ce stade de notre formation, nous disons simplement merci.

Nous souhaitons également adresser nos sincères remerciements à notre encadrant, ***M^r MOKTEFI. M****, pour son précieux soutien scientifique et moral. Ses conseils éclairés nous ont permis de progresser et d'atteindre notre objectif.*

Nous tenons à ne pas oublier dans nos remerciements toute l'équipe CEVITAL, en particulier le responsable infrastructure et production informatique ***M^r YESSAD. H****.*

Nous aimerions également adresser nos remerciements à tous les membres du jury, qui ont accepté d'évaluer notre travail.

Enfin, nous tenons à remercier tous les enseignants qui ont participé à notre formation, leur contribution a été essentielle et nous leurs sommes profondément reconnaissants.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

A

ARP : *Address Resolution Protocol.*

C

CPU : *Central Processor Unit.*

D

DDoS : *Distributed Denial of Service.*

DHCP : *Dynamic Host Configuration Protocol.*

DMZ : *Demilitarized Zone.*

DNS : *Domain Name Server.*

F

FAI : *Fournisseur d'Accès à Internet.*

FTP : *File Transfer Protocol.*

G

GNS : *Graphical Network Simulator.*

H

HTTP : *Hyper Tex Transport Protocol.*

I

ICMP : *Inernet Control Message Protocol.*

IDS : *Intrusion Detection System.*

IP : *Internet Protocol.*

IPS : *Intrusion Prevention System.*

L

LAN : *Local Area Network.*

M

MAC : *Media Access Control.*

MAN : *Metropolitan Area Network.*

N

NAT : *Network Address Translation.*

NIDS : *Network Intrusion DetectionSystem.*

NMAP : *Network MAPper.*

N

OSI : *Open System Interconnexion.*

P

PAN : *Personal Area Network.*

PAT : *Port Address Translation.*

S

SMTP : *Simple Mail Transfer Protocol.*

SQL : *Structured Query Language.*

S

TCP : *Transmission Control Protocol.*

U

UDP : *User Datagramm Protocol.*

V

VLAN : *Virtual Local Area Network.*

VPN : *Virtual Private Network.*

W

WAN : *Wide Area Network.*

X

XSS : *Cross-site scripting.*

Introduction générale

Les réseaux informatiques sont devenus des ressources vitales pour le bon fonctionnement des entreprises. De plus, ces réseaux sont ouverts de fait qu'ils sont pour la plus part connectés à l'internet. Cette ouverture qui permet de faciliter la communication, engendre malheureusement des risques importants dans le domaine de la sécurité informatique.

Les utilisateurs de l'internet ne sont pas forcements pleins de bonnes intentions, ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour réaliser leurs attaques non seulement à l'extérieur du réseau mais aussi des utilisateurs internes. Les conséquences de ces attaques peuvent être lourdes pour un particulier (pertes d'informations, ou pire encore vol d'informations, atteinte à la vie privée..) et pour une entreprise (perte du savoir-faire..). Pour cela, les administrateurs doivent déployer des solutions de sécurité efficace capable de protéger le réseau de l'entreprise.

Dans ce contexte, Nous allons d'abord lors du premier chapitre de ce mémoire présenter les réseaux informatiques en générale ainsi que leurs types, classes, architecture et topologies.

Puis on vas définir la sécurité informatique ainsi que ces objectifs et les types d'attaques, Ensuite nous allons présenter dans le deuxième chapitre le système d'intrusion et le système de prévention ainsi que leurs types, architecture, fonctionnement et leurs avantages et inconvénients. Et en troisième chapitre on vas présenter l'organisme d'accueil qui est dans notre cas CEVITAL.

Et en dernier lieu on vas s'intéresser sur la partie pratique.

I

Notions de bases sur les réseaux et sécurité informatique

I.1 Introduction

Les réseaux informatiques et la sécurité informatique sont des domaines importants de l'informatique. Voici quelques notions de base dans ces domaines :

Réseaux informatiques

Les réseaux informatiques sont des systèmes qui permettent à des ordinateurs et à d'autres périphériques de communiquer et de partager des ressources. Voici quelques éléments clés :

- **Protocoles réseau :** Les protocoles réseau sont des règles et des normes qui définissent comment les données sont échangées entre les périphériques d'un réseau. Les protocoles courants comprennent TCP/IP, qui est utilisé pour la communication sur Internet, et Ethernet, qui est utilisé pour les réseaux locaux (LAN).
- **Topologie réseau :** La topologie réseau fait référence à la structure physique ou logique d'un réseau. Elle détermine comment les périphériques sont connectés les uns aux autres. Les topologies courantes incluent l'étoile, le bus, l'anneau et le maillage.
- **Adresses IP :** Chaque périphérique connecté à un réseau possède une adresse IP (Internet Protocol) qui lui est attribuée. Une adresse IP est un identifiant unique qui permet d'identifier et de localiser un périphérique sur un réseau. Les adresses IPv4 (par exemple, 192.168.0.1) et IPv6 (par exemple, 2001 :0db8 :85a3 :0000 :0000 :8a2e :0370 :7334) sont utilisées pour identifier les périphériques sur Internet.

- **Routage :** Le routage consiste à acheminer les données à travers un réseau. Les routeurs sont des dispositifs qui analysent les adresses IP des paquets de données et déterminent le chemin optimal pour les transmettre à leur destination. Le routage permet de connecter différents réseaux entre eux.

I.2 Généralités sur les réseaux informatiques

Un réseau informatique est un système de communication qui permet à plusieurs appareils informatiques (ordinateurs, serveurs, périphériques, etc.) de se connecter et de partager des ressources entre eux. Voici quelques définitions et intérêts des réseaux informatiques :

I.2.1 Définition des réseaux informatiques

Un réseau informatique est une infrastructure qui permet la transmission de données entre les appareils connectés. Il permet le partage de ressources telles que les fichiers, les imprimantes, les connexions Internet, les bases de données, etc.

I.2.2 Intérêt des réseaux informatiques

Les réseaux informatiques désignent l'interconnexion de plusieurs systèmes informatiques permettant le partage de ressources et d'informations. L'intérêt des réseaux informatiques réside dans plusieurs aspects cruciaux pour les entreprises, les institutions et même les utilisateurs individuels :

- **Communication :** Les réseaux informatiques facilitent la communication entre les appareils connectés. Ils permettent l'échange de données, de messages et de fichiers entre les utilisateurs. Cela favorise la collaboration et le partage d'informations au sein d'une organisation.
- **Partage de ressources :** Les réseaux informatiques permettent le partage de ressources entre les appareils connectés. Par exemple, plusieurs ordinateurs peuvent partager une imprimante connectée au réseau, permettant ainsi à tous les utilisateurs d'imprimer des documents. De même, les fichiers peuvent être partagés et accessibles à partir de différents appareils connectés au réseau.
- **Accès aux services :** Les réseaux informatiques offrent l'accès à divers services et ressources. Par exemple, grâce à Internet, les utilisateurs peuvent accéder à des services en ligne tels que la messagerie électronique, le partage de fichiers, les réseaux sociaux, le commerce électronique, etc.
- **Centralisation des données :** Les réseaux permettent la centralisation des données. Les serveurs de fichiers peuvent être utilisés pour stocker et gérer les fichiers partagés, ce qui facilite la sauvegarde, la récupération et la sécurité des données.
- **Économies d'échelle :** Les réseaux informatiques permettent d'obtenir des économies d'échelle en partageant les ressources. Par exemple, au lieu d'avoir une imprimante pour

chaque utilisateur, une seule imprimante peut être partagée par plusieurs utilisateurs, réduisant ainsi les coûts.

- **Flexibilité et mobilité :** Les réseaux sans fil, tels que les réseaux Wi-Fi, offrent une plus grande flexibilité et mobilité. Les utilisateurs peuvent accéder aux ressources réseau et aux services depuis différents endroits sans être physiquement connectés à un câble.
- **Partage de connaissances :** Les réseaux informatiques favorisent le partage des connaissances et des compétences entre les utilisateurs. Les utilisateurs peuvent échanger des idées, des informations et collaborer plus efficacement grâce aux fonctionnalités de communication et de partage de ressources du réseau.

I.2.3 Classe des réseaux

Les réseaux informatiques peuvent être classés en différentes catégories en fonction de leur taille et de leur portée. Voici les principales classes de réseaux :

- **Réseau personnel (PAN - Personal Area Network) :** Il s'agit du plus petit type de réseau, généralement limité à une zone personnelle telle qu'une pièce ou un espace de travail. Les exemples courants de PAN sont les réseaux Bluetooth, utilisés pour connecter des périphériques tels que des téléphones mobiles, des claviers et des souris à courte distance.
- **Réseau local (LAN - Local Area Network) :** Les réseaux locaux couvrent une zone géographique restreinte, telle qu'un bureau, une maison ou un campus. Ils sont généralement propriété d'une organisation ou d'un individu. Les LAN permettent le partage de ressources et de services entre les appareils connectés, tels que les ordinateurs, les imprimantes, les serveurs de fichiers, etc.
- **Réseau étendu (WAN - Wide Area Network) :** Les réseaux étendus couvrent une plus grande distance géographique et peuvent connecter plusieurs réseaux locaux entre eux. Les WAN utilisent généralement des connexions de longue distance, telles que des lignes louées ou des connexions Internet, pour relier les sites distants. Internet est un exemple de réseau étendu mondial.
- **Réseau métropolitain (MAN - Metropolitan Area Network) :** Les réseaux métropolitains couvrent une région métropolitaine ou une zone urbaine. Ils sont généralement utilisés par les fournisseurs de services pour fournir une connectivité à haut débit aux entreprises et aux organisations dans une région spécifique.
- **Réseau d'accès (AN - Access Network) :** Les réseaux d'accès sont utilisés pour fournir une connectivité aux utilisateurs finaux, généralement dans leur domicile ou leur entreprise. Ils peuvent utiliser différentes technologies, telles que DSL, câble coaxial, fibre optique ou réseaux sans fil, pour offrir un accès à Internet.

Il convient de noter que cette classification est générale et que les réseaux peuvent être interconnectés pour former des architectures plus complexes, selon les besoins spécifiques des

organisations ou des utilisateurs.

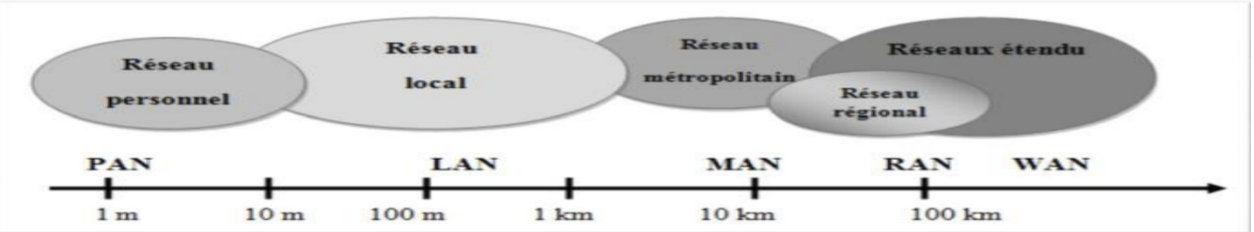


Figure I.1 – Classe des réseaux.

I.2.4 Topologies des réseaux informatiques

La topologie des réseaux fait référence à la structure physique ou logique du réseau, c'est-à-dire à la façon dont les périphériques sont connectés entre eux. Voici les principales topologies de réseau :

- **Topologie en étoile :** Dans une topologie en étoile, tous les périphériques du réseau sont connectés à un concentrateur central appelé commutateur ou routeur. Toutes les communications passent par ce concentrateur, ce qui facilite la gestion du réseau et la détection des problèmes. Cependant, si le concentrateur échoue, tout le réseau peut être affecté.

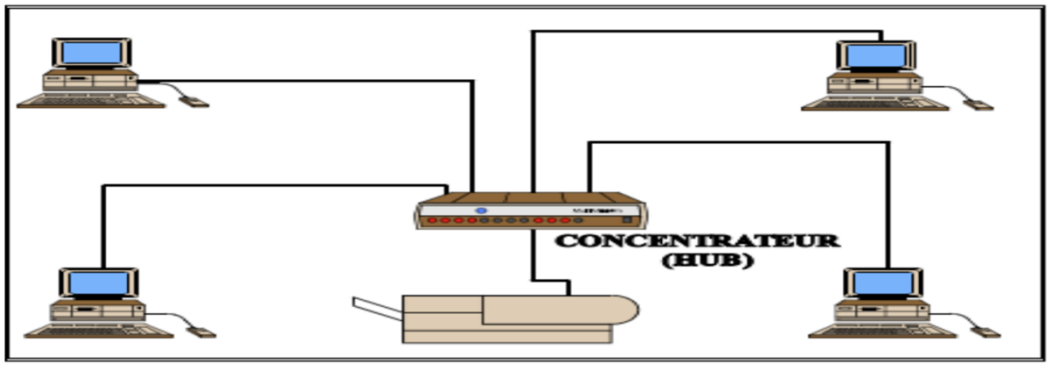


Figure I.2 – Topologie en étoile.

- **Topologie en bus :** Dans une topologie en bus, tous les périphériques sont connectés à une seule ligne de communication partagée appelée bus. Les données sont envoyées sur le bus et tous les périphériques reçoivent les données. Si un périphérique envoie des données, elles sont reçues par tous les périphériques du réseau. Si le bus échoue, tout le réseau peut être impacté.

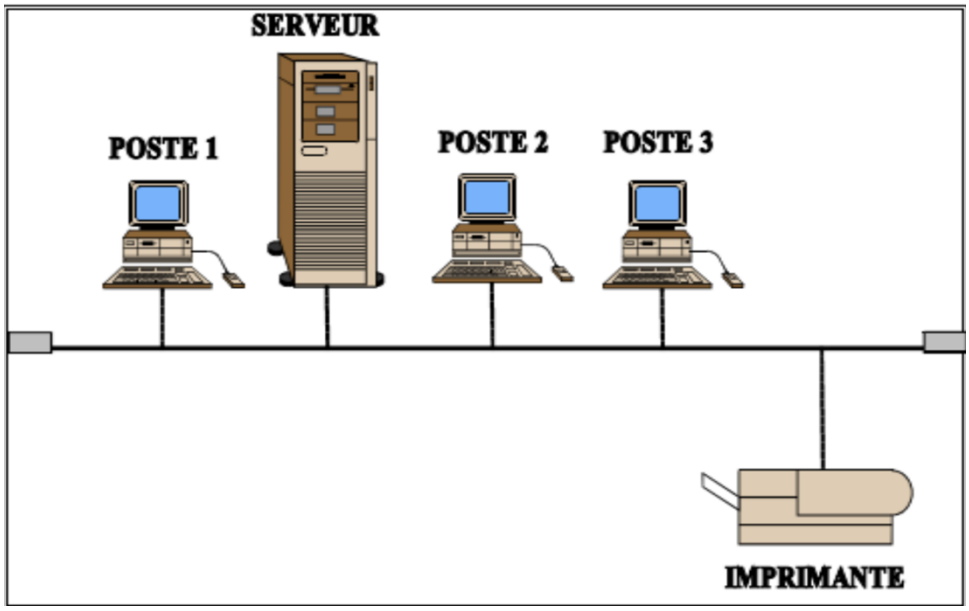


Figure I.3 – Topologie en bus.

- **Topologie en anneau :** Dans une topologie en anneau, les périphériques sont connectés en forme d'anneau fermé. Chaque périphérique est connecté à deux autres périphériques, formant une boucle. Les données circulent dans un seul sens autour de l'anneau, passant par chaque périphérique. Si un périphérique du réseau échoue, cela peut affecter tout le réseau.

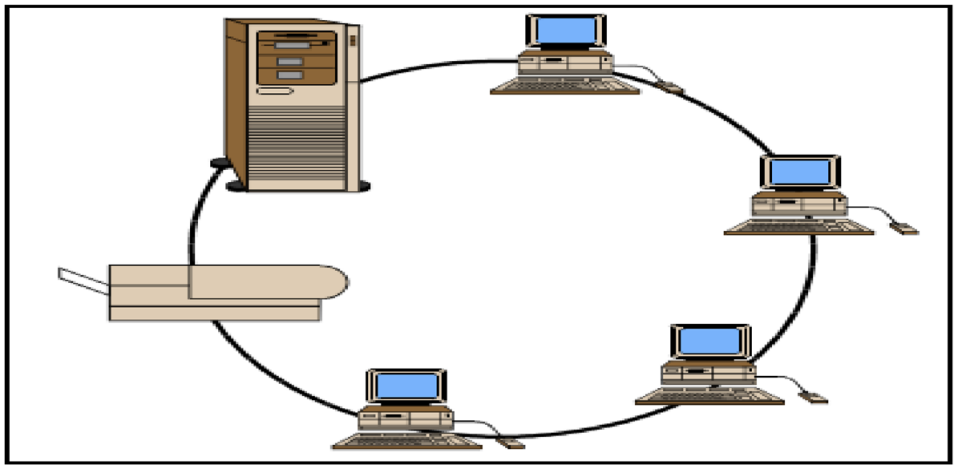


Figure I.4 – Topologie en anneau.

- **Topologie en arbre :** Dans une topologie en arbre, les périphériques sont organisés dans une structure hiérarchique, similaire à un arbre. Un périphérique central, tel qu'un commutateur racine, est connecté aux périphériques de niveau inférieur, qui peuvent à leur tour être connectés à d'autres périphériques. Cette topologie est souvent utilisée dans les réseaux d'entreprise où plusieurs succursales sont connectées à un réseau central.

Il est important de noter que ces topologies peuvent être combinées pour former des topologies hybrides selon les besoins spécifiques du réseau.

I.2.5 Types de réseaux

Voici une explication des trois types de réseaux les plus couramment utilisés : l'intranet, l'extranet et l'internet :

- **Intranet :** Un intranet est un réseau privé interne utilisé par une organisation pour faciliter la communication et le partage d'informations entre les employés, les départements et les filiales. Il utilise des technologies Internet (comme TCP/IP) pour fournir des services similaires à ceux de l'Internet, tels que l'accès aux sites Web internes, le partage de fichiers, la messagerie électronique, les applications internes, etc. Cependant, l'intranet est uniquement accessible aux membres autorisés de l'organisation et n'est pas accessible au public.

- **Extranet :** Un extranet est une extension d'un intranet qui permet aux utilisateurs externes, tels que les clients, les fournisseurs ou les partenaires commerciaux, d'accéder à certaines parties du réseau interne de l'organisation. L'extranet fournit un niveau de connectivité contrôlé et sécurisé avec des autorisations d'accès spécifiques. Par exemple, une entreprise peut créer un extranet pour permettre à ses clients de passer des commandes en ligne ou pour partager des informations avec ses partenaires commerciaux. L'extranet offre une collaboration et une communication sécurisées entre l'organisation et les entités externes.

- **Internet :** Internet est un réseau mondial d'ordinateurs interconnectés utilisant le protocole TCP/IP. Il s'agit d'un réseau public accessible à tous les utilisateurs du monde entier. Internet permet l'accès à une vaste gamme de services, tels que les sites Web, la messagerie électronique, le partage de fichiers, le streaming de médias, les réseaux sociaux, les services de cloud, etc. Il s'appuie sur des infrastructures de communication à grande échelle, notamment des fournisseurs d'accès Internet (FAI), des routeurs et des serveurs répartis à travers le monde.

En résumé, l'intranet est un réseau interne utilisé par une organisation, l'extranet étend l'accès à des utilisateurs externes autorisés, tandis qu'Internet est un réseau mondial accessible au public.

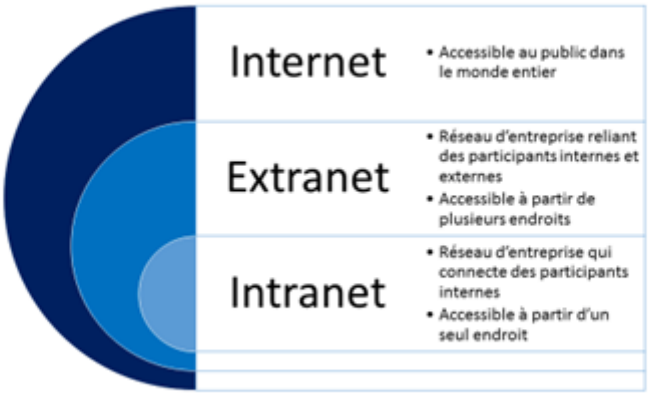


Figure I.5 – Types de réseaux.

I.2.6 Architecture réseaux

L'architecture réseau peut être mise en œuvre selon deux modèles principaux : l'architecture poste à poste (peer-to-peer) et l'architecture client/serveur. Voici une explication de ces deux modèles :

- **Architecture poste à poste (peer-to-peer) :** Dans une architecture poste à poste, chaque appareil du réseau est à la fois un client et un serveur. Les appareils sont connectés directement les uns aux autres et peuvent partager des ressources, tels que des fichiers, des imprimantes ou des connexions Internet, sans dépendre d'un serveur centralisé. Chaque appareil a un rôle égal et peut demander et fournir des services à d'autres appareils du réseau.

Les réseaux poste à poste sont couramment utilisés dans des environnements domestiques ou de petites tailles où les besoins de partage de ressources sont limités. Par exemple, un groupe d'ordinateurs connectés en réseau dans une maison pour partager des fichiers musicaux ou des imprimantes est un exemple typique d'architecture poste à poste.

- **Architecture client/serveur :** Dans une architecture client/serveur, le réseau est organisé autour d'un serveur central qui fournit des services et des ressources aux clients qui y accèdent. Le serveur est responsable de la gestion des ressources, du stockage des données et de la coordination des demandes des clients. Les clients, tels que des ordinateurs ou des appareils mobiles, se connectent au serveur pour accéder aux ressources partagées.

Ce modèle est couramment utilisé dans les environnements d'entreprise où des serveurs centralisés sont utilisés pour gérer des applications, des bases de données, des services de messagerie électronique, des fichiers partagés, etc. Les clients se connectent aux serveurs pour demander des services et accéder aux ressources. Cette architecture permet une gestion centralisée, un contrôle des accès et une meilleure sécurité des données.

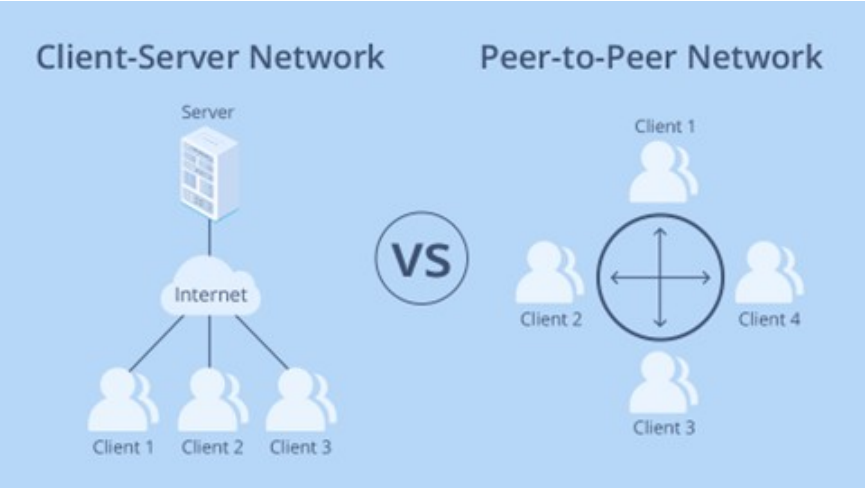


Figure I.6 – Architecture réseau.

I.2.7 Les normes de communication

Les normes de communication sont des ensembles de protocoles et de règles définis pour permettre l'interconnexion et la communication entre les systèmes informatiques. Deux des normes les plus largement utilisées sont le modèle OSI (Open Systems Interconnection) et le modèle TCP/IP (Transmission Control Protocol/Internet Protocol).

- **Modèle OSI (Open Systems Interconnection) :** Le modèle OSI est un modèle de référence qui divise le processus de communication en sept couches distinctes, chacune ayant des responsabilités spécifiques. Chaque couche est conçue pour fournir des services et des fonctionnalités spécifiques nécessaires à la transmission de données. Les sept couches du modèle OSI sont :
  - **Couche physique :** Elle définit les spécifications physiques du matériel de communication, tels que les câbles, les connecteurs et les signaux électriques.
  - **Couche liaison de données :** Elle gère la transmission des données entre les nœuds adjacents sur le réseau local, en détectant et en corrigeant les erreurs.
  - **Couche réseau :** Elle est responsable du routage des données à travers les différents réseaux et de l'adressage logique.
  - **Couche transport :** Elle assure la transmission fiable des données de bout en bout, en découpant les données en segments et en gérant les mécanismes de contrôle d'erreur et de flux.
  - **Couche session :** Elle établit, maintient et termine les sessions de communication entre les applications.
  - **Couche présentation :** Elle se charge de la représentation des données, de leur compression, de leur chiffrement et de leur conversion si nécessaire.
  - **Couche application :** Elle fournit les interfaces pour les applications réseau, permettant aux utilisateurs d'accéder aux services réseau.

Le modèle OSI fournit un cadre conceptuel pour la communication entre les systèmes, mais la plupart des implémentations pratiques se basent sur le modèle TCP/IP.

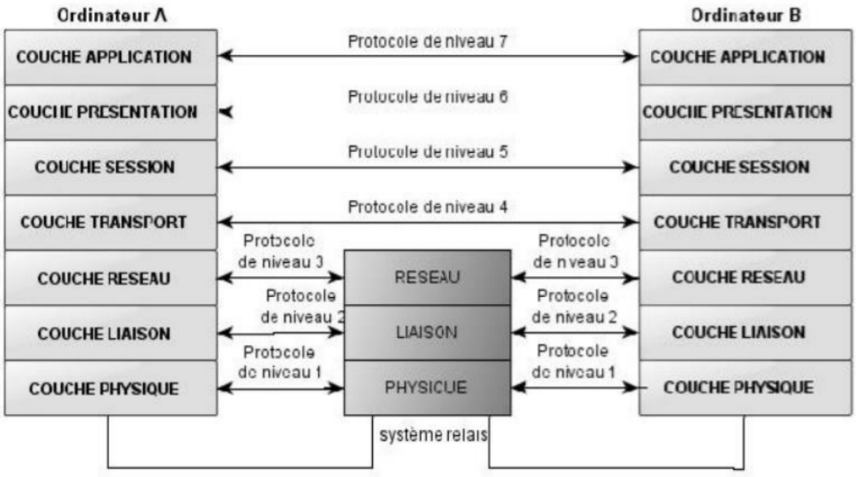


Figure I.7 – Modèle OSI.

- **Modèle TCP/IP (Transmission Control Protocol/Internet Protocol) :** Le modèle TCP/IP est le protocole de communication principal utilisé sur Internet et dans de nombreux réseaux locaux. Il est basé sur une architecture en quatre couches, qui sont généralement alignées avec les couches supérieures du modèle OSI. Les quatre couches du modèle TCP/IP sont :
  - **Couche réseau :** Elle équivaut à la couche réseau du modèle OSI et gère le routage des paquets de données entre les réseaux.
  - **Couche transport :** Elle équivaut à la couche transport du modèle OSI et fournit des services de transport fiables en utilisant les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).
  - **Couche Internet :** Elle équivaut à la combinaison des couches liaison de données et réseau du modèle OSI et s'occupe de l'adressage des paquets et de leur routage sur le réseau.
  - **Couche application :** Elle regroupe les fonctionnalités des couches session, présentation et application du modèle OSI et fournit les interfaces pour les applications réseau.

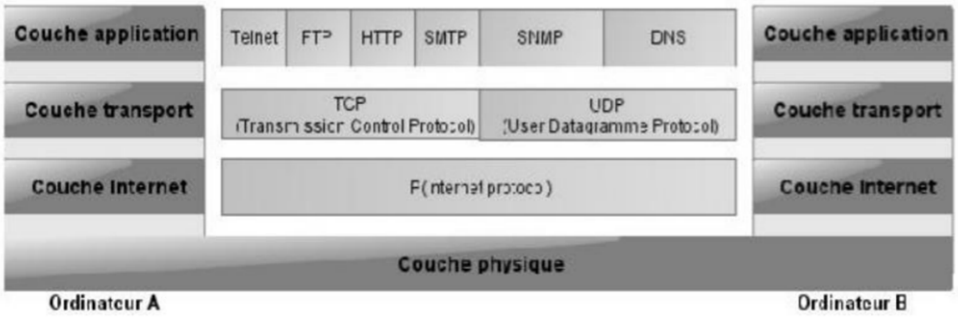


Figure I.8 – Modèle TCP/IP.

Le modèle TCP/IP est largement utilisé pour la communication sur Internet et est le fondement de nombreux services, tels que le World Wide Web (HTTP), le courrier électronique (SMTP), le transfert de fichiers (FTP) et bien d'autres.

I.2.8 Adressage IPv4 et IPv6

L'adressage IP (Internet Protocol) est un système utilisé pour identifier et localiser les appareils connectés à un réseau. Les deux versions principales de l'adressage IP sont IPv4 (Internet Protocol version 4) et IPv6 (Internet Protocol version 6).

- **IPv4 (Internet Protocol version 4) :** IPv4 est la version la plus ancienne et la plus couramment utilisée de l'adressage IP. Il utilise des adresses IP de 32 bits, représentées sous la forme de quatre nombres décimaux séparés par des points (par exemple, 192.168.0.1). Cela permet un total d'environ 4,3 milliards d'adresses uniques.

Cependant, en raison de l'expansion d'Internet et de la demande croissante d'adresses IP, le pool d'adresses IPv4 disponibles est rapidement épuisé. Cela a conduit à l'introduction d'IPv6 pour remédier à cette limitation.

- **IPv6 (Internet Protocol version 6) :** IPv6 est la dernière version de l'adressage IP et a été développée pour résoudre le problème de l'épuisement des adresses IPv4. Il utilise des adresses de 128 bits, représentées sous la forme de huit groupes de quatre caractères hexadécimaux, séparés par des deux-points (par exemple, 2001 :0db8 :85a3 :0000 :0000 :8a2e :0370 :7334). Cela permet un nombre colossal d'adresses IP uniques, environ $3,4 \times 10^{38}$.

En plus de l'augmentation du pool d'adresses, IPv6 offre également d'autres fonctionnalités et améliorations par rapport à IPv4, notamment une meilleure sécurité, une configuration automatique des adresses IP, une meilleure qualité de service et une prise en charge native des nouveaux services Internet.

Bien qu'IPv6 soit en déploiement progressif, il coexiste actuellement avec IPv4. La transition vers IPv6 se fait progressivement et de manière transparente, et de nombreux réseaux prennent en charge les deux versions d'IP pour assurer la compatibilité avec les anciens appareils et services.

I.2.9 NAT : Translation des adresses

La traduction d'adresses réseau (NAT - Network Address Translation) est une technique utilisée pour permettre à plusieurs appareils sur un réseau privé d'accéder à Internet en partageant une seule adresse IP publique. Le NAT fonctionne en modifiant les adresses IP et/ou les numéros de port des paquets de données qui transitent entre le réseau privé et Internet.

Voici les principes de base de la traduction d'adresses réseau (NAT) :

- **NAT avec adresse IP privée :** Dans de nombreux réseaux privés, les appareils sont attribués avec des adresses IP privées, qui ne sont pas routables sur Internet. Lorsque les appareils de ce réseau privé accèdent à Internet, le routeur NAT modifie l'adresse source IP des paquets sortants avec l'adresse IP publique du routeur, tout en conservant les numéros de port. Ainsi, les réponses de l'Internet sont dirigées vers le routeur NAT, qui effectue ensuite la traduction inverse et renvoie les paquets aux appareils appropriés du réseau privé.

- **NAT avec translation de port (Port Address Translation - PAT) :** Dans les situations où plusieurs appareils du réseau privé doivent accéder à Internet en utilisant une seule adresse IP publique, la traduction d'adresse de port (PAT) est utilisée. Le routeur NAT modifie non seulement l'adresse IP source des paquets sortants, mais il modifie également les numéros de port source des paquets en utilisant des ports différents pour chaque appareil. Ainsi, plusieurs sessions simultanées peuvent être établies en utilisant une seule adresse IP publique, car les numéros de port permettent de distinguer les connexions entrantes.

La traduction d'adresses réseau (NAT) offre plusieurs avantages, notamment :

- **Conservation des adresses IP publiques :** Avec NAT, un réseau privé peut utiliser des adresses IP privées, ce qui économise les adresses IP publiques limitées.

- **Sécurité renforcée :** La traduction d'adresses masque les adresses IP internes du réseau privé, ce qui ajoute une couche de sécurité supplémentaire en rendant les appareils du réseau moins visibles de l'extérieur.

- **Simplification du réseau :** NAT permet de réduire le nombre d'adresses IP publiques requises, simplifiant ainsi la gestion du réseau.

Cependant, NAT peut également poser des limitations, notamment en rendant difficile l'établissement de certaines connexions directes (comme les connexions peer-to-peer) et en introduisant une complexité supplémentaire pour les protocoles qui incluent les adresses IP dans les données échangées.

II

La sécurité informatique

II.1 Introduction

Les réseaux d'entreprises sont des systèmes inter-connectant diverses machines dans le but de faciliter leur communication. Ces infrastructures permettent notamment le partage de fichiers et l'échange de messages, ce qui en fait un outil indispensable pour optimiser les performances d'une entreprise. Toutefois, la sécurité du transport des données ainsi que l'accès aux informations sur les différents postes de travail constituent aujourd'hui une préoccupation majeure.

L'avènement d'Internet a exacerbé ces problématiques en raison des risques liés à la sécurité lors des échanges au sein de réseaux privés ou publics. Dans ce contexte, il est impératif que soient mis en place différentes stratégies et mécanismes visant à garantir une protection adéquate contre toute forme d'intrusion malveillante.

Le présent chapitre se divise essentiellement en deux sections distinctes : la première aborde les principes fondamentaux relatifs aux réseaux informatiques tandis que la seconde s'intéresse plus particulièrement aux attaques réseau susceptibles d'affecter ces derniers ainsi qu'aux technologies disponibles pour y faire face efficacement.

II.2 Définition de la sécurité informatique

La sécurité informatique fait référence à l'ensemble des pratiques, des mesures et des technologies mises en place pour protéger les systèmes informatiques, les réseaux, les données et les informations contre les menaces, les attaques, les accès non autorisés, les dommages et autres vulnérabilités potentielles.

L'objectif principal de la sécurité informatique est d'assurer la confidentialité, l'intégrité et la disponibilité des données et des ressources informatiques.

II.3 Les objectifs de la sécurité

Les objectifs de la sécurité informatique, également connus sous le nom de principes de la sécurité, sont les principes directeurs qui guident la mise en place de mesures de sécurité pour protéger les systèmes informatiques, les réseaux, les données et les informations. Ces objectifs visent à garantir la confidentialité, l'intégrité, la disponibilité, l'authenticité et la non-répudiation des données et des ressources informatiques. Voici les principaux objectifs de la sécurité informatique :

- **Confidentialité :** L'objectif de la confidentialité est de garantir que seules les personnes autorisées ont accès aux données et aux informations sensibles. Cela implique le chiffrement des données, la gestion des droits d'accès et la protection contre l'accès non autorisé.
- **Intégrité :** L'intégrité vise à garantir que les données ne sont pas altérées de manière non autorisée. Les mesures de sécurité doivent permettre de détecter toute modification non autorisée des données et de les prévenir.
- **Disponibilité :** L'objectif de la disponibilité est de garantir que les données et les systèmes sont accessibles lorsque cela est nécessaire. Cela implique la mise en place de mesures pour prévenir les interruptions de service, les dénis de service et les pannes.
- **Authenticité :** L'authenticité concerne l'identification et l'authentification des utilisateurs et des ressources. Les mécanismes d'authentification, tels que les mots de passe, les cartes d'accès ou la biométrie, sont utilisés pour garantir que les utilisateurs sont qui ils prétendent être.
- **Non-répudiation :** La non-répudiation vise à empêcher qu'une personne puisse nier avoir effectué une action ou une transaction. Les techniques de non-répudiation, comme les journaux d'audit et les signatures électroniques, permettent de prouver qu'une action a été réalisée par un utilisateur spécifique.
- **Gestion des risques :** La gestion des risques consiste à identifier, évaluer et atténuer les risques potentiels pour la sécurité informatique. Elle vise à minimiser les menaces et les vulnérabilités tout en maximisant la sécurité.
- **Conformité réglementaire :** Pour de nombreuses organisations, l'objectif de la sécurité informatique comprend également la conformité aux lois, aux réglementations et aux normes en matière de sécurité des données et de confidentialité.
- **Réactivité aux incidents :** Être en mesure de réagir rapidement et efficacement en cas d'incident de sécurité est un objectif important. Cela implique la détection précoce des incidents, leur gestion et leur résolution.
- **Éducation et sensibilisation à la sécurité :** Sensibiliser les utilisateurs et le personnel aux meilleures pratiques de sécurité informatique est essentiel pour réduire les risques liés aux erreurs humaines et aux attaques de phishing.

En mettant en œuvre ces objectifs de sécurité, les organisations peuvent réduire les risques liés aux menaces et aux attaques informatiques, tout en garantissant la protection des données et des ressources critiques.

II.4 La sécurité des réseaux d'entreprise

II.4.1 Attaques des réseaux

Les attaques réseau sont des tentatives malveillantes de compromettre l'intégrité, la confidentialité ou la disponibilité des données, des services ou des systèmes au sein d'un réseau informatique. Il existe de nombreuses formes d'attaques réseau, chacune ayant des objectifs et des méthodes différentes. Voici quelques-unes des attaques réseau les plus courantes :

- **Déni de service (DDoS - Distributed Denial of Service) :** Dans une attaque DDoS, un grand nombre d'ordinateurs zombies, souvent contrôlés par un attaquant, inondent un serveur ou un réseau de trafic légitime, le rendant inaccessible pour les utilisateurs légitimes. L'objectif est de perturber les services en ligne.
- **Ingénierie sociale :** L'ingénierie sociale n'implique pas toujours des attaques techniques. Elle consiste à manipuler les individus pour obtenir des informations confidentielles ou accéder à des systèmes. Cela peut inclure le phishing, l'ingénierie sociale par téléphone, ou la collecte d'informations sur les réseaux sociaux.
- **Intrusion :** Les attaquants tentent d'accéder à un système ou à un réseau en exploitant des vulnérabilités connues ou inconnues. Une fois à l'intérieur, ils peuvent voler des données, installer des logiciels malveillants ou prendre le contrôle du système.
- **Attaques par force brute :** Les attaques par force brute consistent à essayer de deviner les mots de passe en essayant toutes les combinaisons possibles jusqu'à ce que le mot de passe correct soit trouvé. Cela peut être utilisé pour accéder à des comptes utilisateur ou à des systèmes.
- **Injection SQL :** Les attaques par injection SQL visent à exploiter les vulnérabilités des bases de données en insérant du code SQL malveillant dans les formulaires web ou les requêtes de base de données, ce qui peut permettre aux attaquants d'accéder, de modifier ou de supprimer des données.
- **Attaques de déni de service ciblées (DoS) :** Les attaques DoS sont menées par un seul attaquant pour perturber les services en envoyant un flux excessif de demandes vers un serveur ou une application, le surchargeant et le rendant indisponible.
- **Attaques de l'homme du milieu (MITM - Man-in-the-Middle) :** Dans ce type d'attaque, l'attaquant intercepte la communication entre deux parties légitimes sans leur consentement. Cela peut être utilisé pour écouter des conversations, voler des données ou même altérer les données en transit.
- **Attaques de réseaux sans fil :** Les attaques sur les réseaux Wi-Fi, tels que le sniffing de paquets, le cracking de clés WEP/WPA, ou les attaques de type Evil Twin, visent à compromettre la sécurité des réseaux sans fil.

- **Attaques par débordement de tampon :** Ces attaques exploitent les vulnérabilités des applications en envoyant des données malveillantes pour dépasser la capacité d'un tampon (buffer) dans la mémoire, ce qui peut permettre à l'attaquant de prendre le contrôle du système.
- **Attaques par ransomware :** Les attaques par ransomware chiffrent les données d'une cible et exigent une rançon en échange de la clé de déchiffrement. Cela peut paralyser les opérations d'une organisation ou causer la perte de données.

II.5 Conclusion

Il est essentiel de mettre en place des mesures de sécurité appropriées, telles que des pare-feu, des systèmes de détection d'intrusion, des mises à jour régulières des logiciels, et de sensibiliser les utilisateurs pour se protéger contre ces types d'attaques.

III

IPS/IDS système de détection et prévention de l'intrusion informatique

III.1 Introduction

Dans le paysage complexe et interconnecté de la cybernétique moderne, la sécurité des systèmes informatiques est une préoccupation majeure. Les pare-feu, ou firewalls en anglais, jouent un rôle central dans la protection des réseaux informatiques contre les menaces potentielles. Un pare-feu est un dispositif ou un logiciel qui agit comme une barrière entre un réseau privé et les sources externes, en contrôlant le trafic entrant et sortant selon des règles prédéfinies.

III.2 Les firewalls

Les pare-feu jouent un rôle crucial dans la défense contre un large éventail de menaces, y compris les attaques par déni de service (DDoS), les intrusions, les logiciels malveillants et les tentatives d'accès non autorisé. Ils contribuent à garantir la confidentialité, l'intégrité et la disponibilité des données, éléments essentiels de la sécurité informatique.

III.2.1 Définition des firewalls

Un pare-feu est un dispositif de sécurité qui surveille et contrôle le trafic réseau afin de protéger un réseau informatique contre les attaques et les intrusions. Il agit comme une barrière de défense entre le réseau interne et les réseaux externes en appliquant des règles de sécurité pour décider quels paquets de données peuvent passer ou être bloqués.

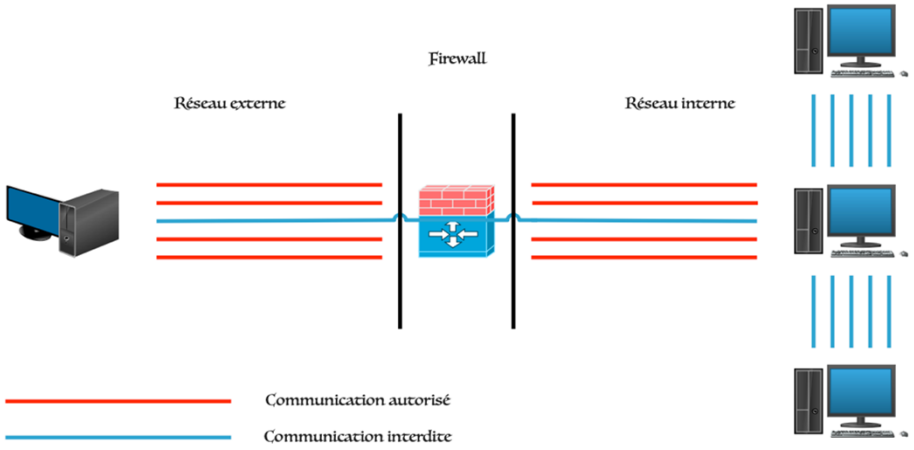


Figure III.1 – firewall.

III.2.2 Fonctionnement des firewalls

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 ().

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

- Autoriser uniquement les communications ayant été explicitement autorisées.
- Empêcher les échanges qui ont été explicitement interdits.

III.2.3 Filtrage simple de paquet

Ou stateless packet filtering, un système pare-feu fonctionne sur le principe du filtrage simple de paquets. Il analyse les en-têtes de chaque paquet de données échangé entre une machine du réseau interne et une machine extérieure. Ainsi, les paquets de données échangée entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- Adresse IP de la machine émettrice ;
- Adresse IP de la machine réceptrice ;
- Type de paquet (TCP, UDP, etc.) ;
- Numéro de port.

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

Le tableau ci-dessous donne des exemples de règles de pare-feu :

Règles	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	TCP	Any	25
2	Accept	Any	192.168.10.3	TCP	Any	80
3	Accept	192.168.10.0/24	Any	TCP	Any	80
4	Deny	Any	Any	Any	Any	Any

Table III.1 – Les règles de pare feu.

III.2.4 Filtrage dynamique

Filtrage d'état ou d'inspection des états de connexion, est une méthode de filtrage utilisée par les pares-feux pour renforcer la sécurité du réseau. Contrairement au filtrage simple de paquets, le filtrage dynamique prend en compte le contexte de la communication en suivant l'état des connexions réseau.

Le fonctionnement du filtrage dynamique dans un pare-feu est le suivant :

1. Établissement de la connexion : Lorsqu'un paquet sortant est détecté, le pare-feu autorise initialement son passage, car il s'agit d'une nouvelle connexion en cours d'établissement.
2. Création d'un état de connexion : Le pare-feu crée un enregistrement d'état pour la connexion en cours, enregistrant les informations de la source, de la destination, des ports et du protocole.
3. Suivi de l'état de la connexion : Le pare-feu suit les paquets entrants associés à cette connexion en fonction de l'état enregistré. Il vérifie si les paquets entrants correspondent à une connexion établie, une réponse attendue ou s'ils sont inattendus.
4. Prise de décision de filtrage : En fonction de l'état de la connexion, le pare-feu prend une décision de filtrage pour chaque paquet entrant. Si le paquet correspond à une connexion établie ou à une réponse attendue, il est généralement autorisé à passer. Si le paquet est inattendu ou ne correspond à aucune connexion enregistrée, il peut être bloqué.
5. Actualisation de l'état de la connexion : Le pare-feu met à jour l'état de la connexion en fonction des paquets entrants. Il peut ajuster les informations enregistrées telles que les numéros de séquence, les numéros d'acquittement, les décalages de fenêtre, etc., pour maintenir un suivi précis de la connexion.
6. Fermeture de la connexion : Lorsque la communication est terminée, le pare-feu supprime l'état de connexion correspondant, libérant les ressources associées.

Le filtrage dynamique offre plusieurs avantages, notamment la capacité à autoriser les paquets entrants en fonction du contexte de la connexion et à bloquer les paquets inattendus ou non sollicités. Cela aide à prévenir les attaques telles que les scans de ports, les paquets falsifiés ou les connexions non autorisées.

III.2.5 Filtrage applicatif

Le Filtrage de couche applicative ou inspection des applications, est une fonctionnalité avancée des pares-feux qui permet d'analyser le contenu des paquets à un niveau applicatif plus élevé. Contrairement au filtrage simple de paquets ou au filtrage d'état, qui se concentrent principalement sur les informations de l'en-tête des paquets, le filtrage applicatif examine également le contenu des données transportées par les paquets.

Le fonctionnement du filtrage applicatif dans un pare-feu est le suivant :

- **Analyse approfondie des paquets :** Le pare-feu inspecte le contenu des paquets en analysant les données au niveau applicatif, telles que les messages HTTP, les requêtes DNS, les commandes FTP, etc.
- **Comparaison aux règles de filtrage :** Le pare-feu compare les données applicatives des paquets aux règles de filtrage préconfigurées spécifiques aux applications. Ces règles peuvent être basées sur des motifs, des signatures, des expressions régulières ou des critères spécifiques à chaque application.
- **Prise de décision de filtrage :** En fonction de la comparaison avec les règles de filtrage, le pare-feu prend une décision de filtrage pour chaque paquet. Il peut autoriser, bloquer, analyser plus en détail ou appliquer des actions spécifiques en fonction des règles correspondantes.
- **Inspection des protocoles et des données :** Le pare-feu peut effectuer une inspection plus approfondie des protocoles applicatifs spécifiques pour identifier les comportements malveillants, tels que les attaques par injection SQL, les attaques de contournement d'authentification, les téléchargements de fichiers malveillants, etc.
- **Protection contre les menaces applicatives :** Le filtrage applicatif permet de détecter et de bloquer les tentatives d'exploitation des vulnérabilités spécifiques aux applications. Il peut également fournir une protection contre les attaques telles que les dénis de service (DoS), les attaques de script intersites (XSS), les injections de code, etc.

Le filtrage applicatif offre une couche de sécurité supplémentaire en permettant aux pares-feux de comprendre le contexte applicatif des données échangées sur le réseau. Cela permet d'identifier et de bloquer de manière plus précise les attaques ciblant des vulnérabilités spécifiques aux applications.

III.2.6 DMZ

Une DMZ (Zone démilitarisée) est un sous-réseau isolé du réseau local principal et d'Internet (ou d'un autre réseau) grâce à un pare-feu. C'est un espace intermédiaire entre le réseau local sécurisé et Internet, où les services accessibles depuis Internet sont placés. La DMZ permet d'héberger des machines qui nécessitent une accessibilité depuis Internet tout en étant séparées du réseau local pour des raisons de sécurité. Le pare-feu est configuré pour rediriger le trafic en provenance d'Internet vers la DMZ par défaut. Ainsi, si un service dans la DMZ est compromis, l'impact est limité à cette zone et ne s'étend pas au réseau local, préservant ainsi la sécurité des ressources internes.

En résumé, Une zone démilitarisée (DMZ) est une conception de pare-feu où il y a généralement une interface interne connectée au réseau privé, une interface externe connectée au réseau public et une interface DMZ.

- Le trafic provenant du réseau privé est inspecté lorsqu'il se dirige vers le réseau public ou DMZ. Ce trafic est autorisé avec peu ou pas de restriction.
- Le trafic inspecté revenant de la DMZ ou du réseau public vers le réseau privé est autorisé.
- Le trafic provenant du réseau DMZ et acheminé vers le réseau privé est généralement bloqué.
- Le trafic provenant du réseau DMZ et acheminé vers le réseau public est autorisé de manière sélective en fonction des exigences de service.
- Le trafic provenant du réseau public et se dirigeant vers la DMZ est sélectivement autorisé et inspecté. Ce type de trafic est généralement un trafic de messagerie, DNS, HTTP ou HTTPS. Le trafic de retour de la DMZ vers le réseau public est dynamiquement autorisé.
- Le trafic provenant du réseau public et acheminé vers le réseau privé est bloqué.

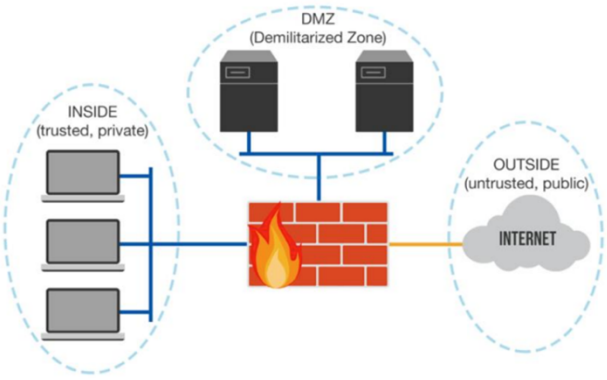


Figure III.2 – Zone démilitarisée DMZ

III.2.7 NAT

Est un mécanisme utilisé dans les réseaux informatiques pour convertir les adresses IP d'un réseau en adresses IP différentes d'un autre réseau. Cela permet de faire correspondre les adresses IP des périphériques d'un réseau privé avec l'adresse IP publique utilisée sur Internet. Le NAT agit comme un intermédiaire entre un réseau privé et Internet en modifiant les adresses IP source et destination des paquets de données qui traversent le pare-feu ou le routeur NAT. Il associe les adresses IP privées utilisées à l'intérieur du réseau local avec une seule adresse IP publique visible depuis Internet. Ainsi, le NAT permet de préserver les adresses IP privées des périphériques du réseau local tout en permettant à ces périphériques de communiquer avec des ressources situées sur Internet. Cela permet également de surmonter les limitations dues à la pénurie d'adresses IP publiques en utilisant un seul ensemble d'adresses publiques pour plusieurs périphériques du réseau local.

III.3 Système de détection d'intrusion IDS

III.3.1 Définition d'un IDS

Est un ensemble de composants logiciels et/ou matériels destiné à repérer des activités anormales ou suspectes sur la cible analysée, un réseau ou un hôte, son rôle est de surveiller les données qui transitent sur ce système. Il permet ainsi d'avoir une action d'intervention sur les risques d'intrusion. Il permet ainsi d'avoir une connaissance sur les tentatives réussie comme échouées des intrusions. En travaillant hors ligne, l'IDS compare le flux de trafic capturé avec des signatures malveillantes connues, similaires à un logiciel qui recherche les virus. Travailler hors ligne signifie plusieurs choses :

- L'IDS fonctionne passivement.
- Le périphérique IDS est physiquement positionné dans le réseau de sorte que le trafic doit être mis en miroir pour l'atteindre.
- Le trafic réseau ne passe pas par l'IDS à moins qu'il ne soit mis en miroir.
- Très peu de latence est ajoutée au flux de trafic réseau.

III.3.2 Types de l'IDS

Il existe différents types d'IDS selon l'endroit qu'ils surveillent et ce qu'ils contrôlent (les "sources d'information") ou selon leurs fonctions :

III.3.2.1 Les IDS réseaux (Network-based IDS)

Ils sont connus aussi sous le nom de NIDS. Les IDS réseaux analysent et interprètent les paquets circulant sur un réseau (ou un segment du réseau) afin de repérer les paquets à contenus malicieux. La trame est analysée sur toutes ses couches (réseau, transport, application). Par dissection des paquets et la connaissance des protocoles, les NIDS sont capables de détecter des

paquets malveillants conçus pour outrepasser un pare-feu.

Ce type d'IDS a l'avantage d'être plus facile à protéger (contre les attaques sur l'IDS lui-même) de la faite qu'ils ne font qu'une observation du trafic. Cependant, une des contraintes des NIDS est que, pour pouvoir écouter l'ensemble des paquets, ils nécessitent une bande passante qui est proportionnelle à l'importance du trafic. Aussi, le positionnement des NIDS dans le réseau doit être stratégique afin de pouvoir surveiller tout le trafic. Par ailleurs les NIDS présentent des limites dans la protection des réseaux aux trafics chiffrés.

Quelques exemples de NIDS sur le marché sont NetRanger, NFR, Snort, DTK et ISS RealSecure.

III.3.2.2 Les IDS hôtes (Host-based IDS)

Les systèmes de détection d'intrusion basés sur l'hôte, aussi appelés HIDS, analysent exclusivement les activités concernant l'hôte sur lequel ils sont installés (serveur, poste client, pare-feu, etc.), recherchant des activités suspectes. La détection peut se faire en utilisant les logs d'audit de sécurité, les logs systèmes, le trafic réseau de l'hôte, les processus en cours d'exécutions, les accès aux fichiers, les changements de configurations des applications, etc. Le plus souvent les HIDS sont déployés sur les hôtes critiques comme les serveurs contenant des informations de sensibilités élevées et les serveurs publiquement accessibles.

Étant focalisés sur la sécurité d'un seul hôte, les HIDS ont l'avantage d'avoir plus de précision sur les variétés d'attaques. Aussi l'impact d'une attaque peut être constaté et permet une meilleure réaction. Des attaques dans un trafic chiffré peuvent être détectées (impossible avec un IDS réseau). Cependant les HIDS sont plus vulnérables aux attaques de dénis de service. Aussi, en raison de leurs volumes de données, l'analyse des logs peut nécessiter d'importantes ressources (puissance de calcul et stockage).

Des exemples de HIDS sont OSSEC (Open Source Security), Tripwire, Radmind, EMERALD's eXpert-BSM AIDE (Advanced Intrusion Detection Environment) et PortSentry.

III.3.2.3 Les IDS hybrides (Hybrid-based IDS)

La nouvelle tendance en matière de détection d'intrusion est de combiner les NIDS et les HIDS pour concevoir des IDS hybrides. Les systèmes hybrides de détection d'intrusion sont flexibles et augmentent le niveau de sécurité. Ils combinent plusieurs localisations des systèmes IDS et recherchent si bien les attaques visant des éléments particuliers que celles visant l'ensemble du système. Un exemple d'IDS hybride est ISS RealSecure.

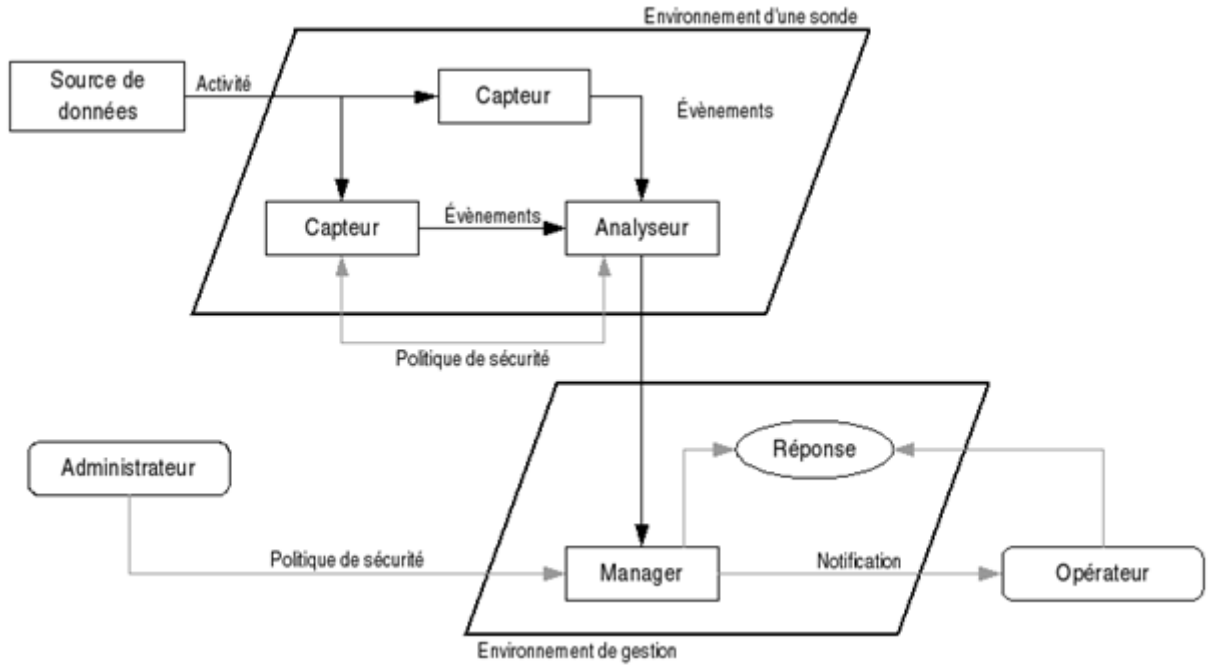


Figure III.3 – Architecture IDS.

III.3.3 Architecture de l'IDS

Nous nous intéressons maintenant à l'architecture et les modules de base d'un IDS. On retrouve souvent les IDS placés en première ligne du réseau à sécuriser, pour qu'il examine tous les paquets entrants ou sortants. Il réalise un ensemble d'analyses de détection sur chaque paquet individuel ainsi sur les conversations et motifs du réseau. En visualisant chaque transaction dans la figure suivante :

Un IDS est composé de plusieurs éléments dont chacun accompli un rôle bien précis, on trouve :

- **Analyseur :** Les analyseurs reçoivent comme entrée les données qui proviennent d'un ou plusieurs collecteurs ou à partir d'autres analyseurs qui auraient au préalable procédés à un premier traitement des données. Il génère des alertes lorsque le flux d'évènements fourni par le(s) capteur(s) contient des éléments caractéristiques d'une activité malveillante.
- **Manager :** Le manager collecte les alertes produites par l'analyseur, et les transmit ensuite à l'opérateur sous forme de notifications afin de lui permettre de gérer les alertes reçues et prendre des décisions.
- **Opérateur :** Personne chargée de l'utilisation de manager associé à l'IDS. Elle décide sur la réaction à prendre en cas d'alerte.
- **Administrateur :** Une personne chargée de mettre en place la politique de sécurité et configure les IDS et par conséquent de déployer et de configurer les IDS, via les interfaces utilisateur.
- **Interface utilisateur :** C'est un module qui permet à l'IDS d'interagir avec l'utilisateur (généralement un administrateur système), pour pouvoir configurer et fixer quelques paramètres en relation avec la politique de sécurité qu'on veuille mettre en œuvre.

III.3.4 Fonctionnement d'un IDS

Nous nous intéressons maintenant au fonctionnement d'un IDS, nous commençons par les méthodes d'analyse, après les techniques de détection.

III.3.4.1 Les méthodes d'analyse

Avec la localisation de l'analyse des données on peut faire une distinction entre les IDS :

- **Analyse centralisée :** certains IDS ont une architecture multi-capteurs. Ils centralisent les évènements (ou alertes) pour analyse au sein d'une seule machine. L'intérêt principal de cette architecture est de faciliter la corrélation entre évènements puisqu'on dispose alors d'une vision globale. Par contre, la charge des calculs ainsi que la charge réseau peuvent être lourdes et risquent de constituer un goulet d'étranglement.
- **Analyse locale :** si l'analyse du flot d'évènements est effectuée au plus près de la source de données (généralement en local sur chaque machine disposant d'un capteur), on minimise le trafic réseau et chaque analyseur séparé dispose de la même puissance de calcul. En contrepartie, il est impossible de croiser des évènements qui sont traités séparément et l'on risque de passer à coté de certaines attaques distribuées.
- **Analyse distribuée :**
  - **Partiellement distribuée :** dans ce cas un nombre limité de nœuds peuvent exécuter des tâches d'analyse locale et de détection mais ils sont commandés par un nœud maître, celui-ci collabore avec d'autres nœuds maîtres pour superviser la détection globale sous forme d'une structure hiérarchique.
  - **Entièrement distribuée :** la collecte d'informations, l'analyse et la détection ainsi que les alertes seront réalisées au niveau local de chaque nœud. Mais dans le cas d'information incomplète ou bien suspicion les nœuds peuvent déclencher des procédures de collaboration supervisées par des nœuds maitres.

III.3.4.2 Les techniques de détection d'intrusion

Le trafic réseau est généralement constitué de datagrammes IP. Un NIDS est capable de capturer les paquets lorsqu'ils circulent sur les liaisons physiques sur lesquelles il est connecté. Pour que le NIDS détecte les intrusions à travers les paquets qui circulent sur le réseau, il peut appliquer les techniques suivantes :

- **Approche comportementale :** Cette technique consiste à détecter une intrusion en fonction du comportement de l'utilisateur ou d'une application, autrement dit c'est créer un modèle basé sur le comportement habituel du système et surveiller toute déviation de ce comportement.
- **Approche par scénario ou par signature :** Cette technique s'appuie sur les connaissances des techniques utilisées par les attaquants contenus dans la base de donnée, elle compare l'activité de l'utilisateur à partir de la base de donnée, ensuite elle déclenche une alerte lorsque des événements hors profil se produisent Cette approche consiste à

rechercher dans l'activité de l'élément surveillé les empreintes (ou signatures) d'attaques connues, et cette approche est très similaire à celle des outils antivirus et présente les même inconvénients que celle-ci, il nécessite des mises à jour quotidiennes.

- **Vérification de la pile protocolaire :** par exemple « Ping-Of-Death » ont recours à des violations des protocoles TCP, IP, UDP, ICMP dans le but d'attaquer une machine. Une simple vérification protocolaire de nombre d'intrusions peut mettre en évidence les paquets invalides et signaler ce type de techniques très usitées.
- **Vérification des protocoles applicatifs :** Cette technique est rapide (il n'est pas nécessaire de chercher des séquences d'octets sur l'exhaustivité de la base de signatures), élimine en partie les fausses alertes et s'avère donc plus efficiente. Beaucoup d'intrusions utilisent des comportements protocolaires invalides, comme par exemple « WinNuke », qui utilise des données NetBIOS invalides (ajout de données OOB data). Dans le but de détecter efficacement ce type d'intrusions, le NIDS doit ré-implémenter une grande variété de protocoles applicatifs.

III.3.4.3 Comportement après détection

On peut classer les IDS par type de réaction lorsqu'une attaque est détectée :

- **Passive :** La plupart des systèmes de détection d'intrusion n'apportent qu'une réponse passive à l'intrusion. Lorsqu'une attaque est détectés, ils génèrent une alarme et notifient l'administrateur système par e-mail, message dans une console, voire même par beeper. C'est alors lui qui devra prendre les mesures qui s'imposent.
- **Active :** D'autres systèmes de détection d'intrusions peuvent, en plus de la notification à l'opérateur, prendre automatiquement des mesures pour stopper l'attaque en cours, et dans ce cas il devient un IPS.

III.3.4.4 Avantages et inconvénients

L'IDS (Intrusion Detection System) présente à la fois des avantages et des inconvénients. Voici une liste des principaux avantages et inconvénients associés à l'utilisation d'un IDS :

Avantages de l'IDS

1. Détection précoce des intrusions : L'IDS peut détecter les activités malveillantes dès leur apparition, permettant ainsi une réponse rapide avant que des dommages importants ne soient causés.
2. Surveillance continue : L'IDS surveille en permanence le réseau ou les hôtes, offrant une protection constante contre les attaques et les activités suspectes.
3. Diversité des méthodes de détection : Les IDS utilisent une variété de techniques de détection, telles que la détection basée sur la signature, la détection basée sur l'anomalie et l'apprentissage automatique, ce qui augmente les chances de détecter différentes formes d'attaques.

4. Réduction des fausses alertes : Les IDS modernes intègrent des mécanismes avancés pour réduire les fausses alertes, en améliorant la précision de la détection et en évitant les alarmes inutiles.
5. Visualisation des activités réseau : L'IDS fournit une visibilité détaillée sur le trafic réseau, les flux de données et les événements, ce qui permet une analyse approfondie de l'environnement de sécurité.

Inconvénients de l'IDS

1. Dépendance à la mise à jour des signatures : Les IDS basés sur la signature nécessitent des mises à jour régulières de la base de données de signatures pour détecter les nouvelles menaces. Si les signatures ne sont pas à jour, des attaques récentes pourraient passer inaperçues.
2. Détection limitée des attaques inconnues : Les IDS basés sur la signature peuvent avoir du mal à détecter les attaques pour lesquelles il n'existe pas encore de signatures connues. Cela peut rendre l'IDS vulnérable aux attaques zero-day et aux techniques d'évasion sophistiquées.
3. Charge de travail supplémentaire : L'installation et la configuration d'un IDS peuvent nécessiter des efforts et des ressources supplémentaires, ainsi qu'une surveillance et une gestion continues pour maintenir son efficacité.
4. Complexité de l'analyse des alertes : Les IDS génèrent souvent un grand nombre d'alertes, ce qui peut rendre la tâche d'analyse et de réponse aux incidents laborieuse et complexe pour les équipes de sécurité.
5. Possibilité de faux négatifs : Il est possible que certaines attaques passent inaperçues ou soient mal détectées, ce qui peut conduire à des faux négatifs et à un faux sentiment de sécurité.

III.4 Système de prévention d'intrusion IPS

III.4.1 Défintion d'un IPS

IPS (Intrusion Prevention System) est un système de prévention des intrusions qui travaille en tandem avec un IDS (Intrusion Detection System) pour détecter et prévenir les activités malveillantes dans un réseau ou sur un hôte. Contrairement à un IDS, qui se concentre principalement sur la détection des intrusions, un IPS est conçu pour prendre des mesures actives pour bloquer, arrêter ou atténuer les attaques en temps réel.

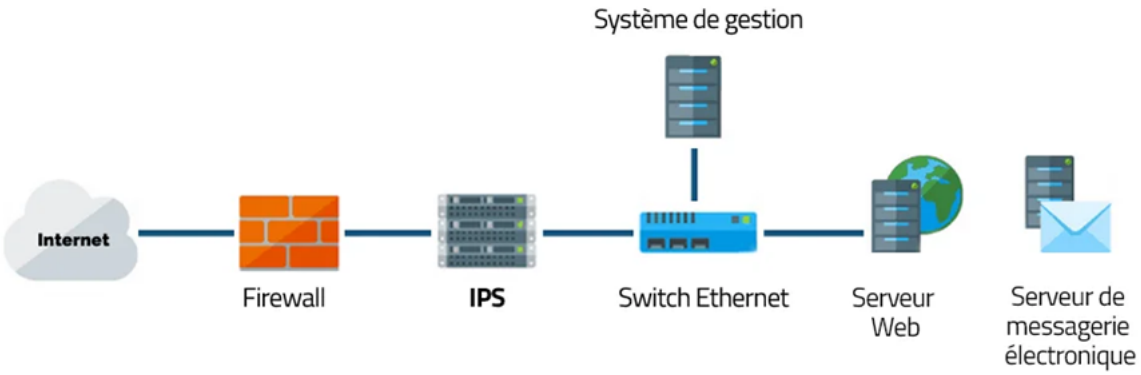


Figure III.4 – IPS

III.4.2 Types de l'IPS

Comme pour les IDS, les IPS peuvent être orientés hôtes (Host IPS), réseaux (Network IPS) ou noyau (kernel IPS). Mais, il n'existe pas d'IPS destiné à surveiller une application.

III.4.3 IPS orienté hôte (HIPS)

Un IPS basé hôte est un agent installé sur le système bloquant les comportements anormaux tels que la lecture ou l'écriture de fichiers protégés. L'accès à des ports non autorisés, une tentative de débordement de pile, un accès à certaines zones de la base de registres. En effet, un HIPS analyse exclusivement l'information concernant cet hôte pour le protéger des comportements dangereux. Les HIPS sont en général placés sur des machines sensibles, susceptibles de subir des attaques et possédantes des données importantes pour l'entreprise.

III.4.4 IPS orienté réseau (NIPS)

Le rôle d'un IPS basé réseau est d'analyser les paquets circulant dans le réseau. La principale différence entre un NIDS et NIPS tient principalement en deux caractéristiques. Le positionnement en coupure sur le réseau du NIPS, et non plus seulement en écoute comme pour le NIDS et la possibilité de bloquer immédiatement les intrusions quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce. Ce qui induit que le NIPS est constitué d'une technique de filtrage de paquets et de moyens de blocage. En effet, le positionnement en coupure, tel un firewall, est le seul mode permettant d'analyser les données entrantes ou sortantes et de réduire dynamiquement les paquets intrusifs avant qu'ils n'atteignent leurs destinations.

III.4.5 IPS orienté noyau (KIPS)

Leur particularité est de s'exécuter dans le noyau d'une machine, pour y bloquer toute activité suspecte. Le KIPS peut reconnaître des motifs caractéristiques du débordement de mémoire, et peut ainsi interdire l'exécution du code. Il peut également interdire le système d'exploitation d'exécuter un appel système qui ouvrirait un terminal de commande. Puisqu'un KIPS analyse les appels systèmes, il ralentit l'exécution. C'est pour-ça sont moins utilisés.

III.4.6 Fonctionnement d'un IPS

Le fonctionnement d'un IPS est similaire à celui d'un IDS. Il capture le trafic du réseau puis l'analyse. Mais au lieu d'alerter l'utilisateur d'une intrusion ou d'une attaque, l'IPS bloque directement les intrusions en supprimant les paquets illégitimes. Pour informer l'utilisateur, l'IPS peut aussi remplir un fichier de journalisation qui contiendra la liste des paquets supprimés et éventuellement un message indiquant la raison de cette suppression.

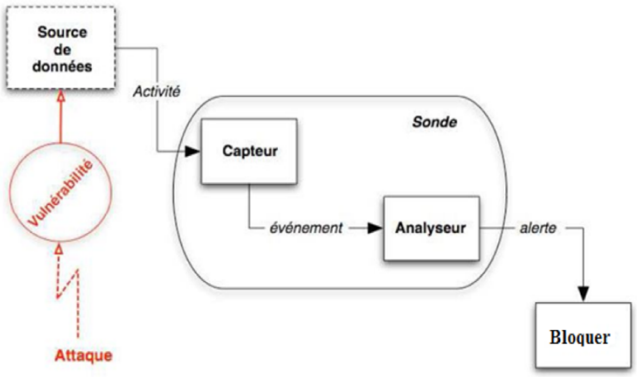


Figure III.5 – Fonctionnment IPS

III.4.7 Points forts IPS

- La plupart des logiciels IPS sont multi-plateforme (Linux, FreeBSD, Windows ... etc.).
- Empêche la transmission des paquets en fonction de ses règles tous comme un pare- feu bloque le trafic en se basant sur les adresses IP.
- La liberté de création des règles pour les actions à exécuter.
- Démineur le coût, pour installer plusieurs.
- Cette approche fait interagir des technologies hétérogènes : pare-feu, VPN, IDS, anti-virus, anti-spam, etc.
- Peut détecter des attaques sur plusieurs différents types des logiciels d'exploitation et d'applications, selon l'ampleur de sa base de données.
- Un dispositif simple peut analyser le trafic pour une grande échelle des centres serveurs sur le réseau, qui fait au NIPS une bonne solution qui diminue le coût d'entretien et de

déploiement.

- Un simple dispositif peut analyser le trafic et sécurisé un large réseau, qui fais au l'IPS ou NIPS une bonne solution qui diminue le coût d'entretien et le déploiement.

III.4.8 Points faibles

- L'IPS peuvent couper les connexions suspectes ou même, pour une attaque externe, reconfigurer le pare-feu pour qu'il refuse tout ce qui vient du site incriminé. Toutefois, il apparaît que ce type de fonctionnalité automatique est potentiellement dangereux car il peut mener à des dénis de service provoqués par l'IDS. Un attaquant déterminé peut, par exemple, tromper l'IDS en usurpant des adresses du réseau local qui seront alors considérées comme la source de l'attaque par l'IDS. Il est préférable de proposer une réaction facultative à un opérateur humain (qui prend la décision finale).
- La consommation des ressources (mémoire, CPU).
- Paralyse le réseau.

III.4.9 Différence entre IDS et IPS

La différence principale entre IDS et IPS est que IDS fonctionne comme un système de surveillance et de détection tandis qu'IPS fonctionne comme un système de prévention en dehors de la surveillance et de la détection. Certaines différences sont :

- **Réponse :** Les solutions IDS sont des systèmes de sécurité passifs qui surveillent et détectent uniquement les réseaux pour les activités malveillantes. Ils peuvent vous alerter mais ne prennent aucune mesure par eux-mêmes pour empêcher l'attaque. L'administrateur du réseau ou le personnel de sécurité affecté doit prendre des mesures immédiatement pour atténuer l'attaque. D'autre part, les solutions IPS sont des systèmes de sécurité actifs qui surveillent et détectent votre réseau pour les activités malveillantes, alertent et empêchent automatiquement l'attaque de se produire.
- **Placement :** l'IDS est placé à la périphérie d'un réseau pour collecter tous les événements, enregistrer et détecter les violations. Ce positionnement donne à l'IDS une visibilité maximale pour les paquets de données. Le logiciel IPS est placé derrière le pare-feu du réseau et communique en ligne avec le trafic entrant pour mieux prévenir les intrusions.
- **Mécanisme de détection :** IDS utilise la détection basée sur les signatures, la détection basée sur les anomalies et la détection basée sur la réputation pour les activités malveillantes. Sa détection basée sur les signatures n'inclut que les signatures face aux exploits. D'autre part, IPS utilise une détection basée sur les signatures avec des signatures orientées exploit et vulnérabilité. En outre, IPS utilise une détection statistique basée sur les anomalies et une détection d'analyse de protocole avec état.
- **Directory :** Si vous êtes menacé, l'IDS pourrait être moins utile car votre personnel de sécurité doit trouver comment sécuriser votre réseau et nettoyer le système ou le réseau immédiatement. IPS peut effectuer une prévention automatique par lui-même.

- **Faux positifs :** Si IDS donne un faux positif, vous pouvez trouver une certaine commodité. Mais si IPS le fait, l'ensemble du réseau en souffrira car vous devrez bloquer tout le trafic - entrant et sortant du réseau.
- **Les performances du réseau :** Comme IDS n'est pas déployé en ligne, il ne réduit pas les performances du réseau. Cependant, les performances du réseau peuvent être réduites en raison du traitement IPS, qui est en phase avec le trafic.

III.5 SNORT

III.5.1 Définition SNORT

Est un logiciel open source utilisé pour la détection d'intrusions dans les réseaux informatiques. Il analyse le trafic réseau à la recherche d'activités suspectes ou de comportements malveillants. En se basant sur des règles prédéfinies, Snort identifie les signatures d'attaques connues ou les modèles de trafic anormaux et génère des alertes pour informer les administrateurs réseau des potentielles intrusions. Il peut être configuré pour fonctionner en tant que système de détection d'intrusion (IDS) pour la surveillance ou en tant que système de prévention d'intrusion (IPS) pour bloquer activement les attaques.

IV

Présentation de l'organisme d'accueil

IV.1 Introduction

Le Groupe Cevital est un conglomérat algérien de l'industrie agroalimentaire, la grande distribution, l'industrie et les services. Créé par l'entrepreneur Issad Rebrab en 1998, Cevital est le premier groupe privé algérien, présent également à l'international et la troisième entreprise algérienne par le chiffre d'affaires. Il emploie 18 000 salariés. Le groupe Cevital est le leader du secteur agroalimentaire en Afrique.

IV.2 Historique

Cevital est spécialisée dans l'industrie agroalimentaire, elle possède une raffinerie d'huile et de sucre.

- ➢ En 2007, Mediterranean Float Glass est créée, spécialisée dans la production, la transformation et distribution du verre pour la construction, les applications solaires et certaines industries spécialisées (électroménager, applications high-tech). Le 28mai 2007, l'usine MFG de Larbaâ est inaugurée par le président de la République Abdelaziz Bouteflika.
- ➢ En 2007, Numilog est créée, elle est spécialisée dans logistique et la gestion de la chaîne logistique (supply chain management).
- ➢ Le 31 mai 2013, Cevital rachète le Français Oxxo, spécialisée dans la menuiserie PVC.
- ➢ Le 15 avril 2014, Cevital reprend les activités françaises du groupe Fagor-Brandt. Le groupe Cevital prévoyait de reprendre également les activités espagnoles et polonaises du groupe Fagor, mais l'offre de reprise de l'activité en Espagne n'a pas été retenue par la justice espagnole et l'usine polonaise du groupe Fagor a finalement été reprise par BSH.

➢ Le 31 mars 2022, Omar Ouali, ancien relecteur en chef de Liberté, a révélé que le journal liberté en lien avec détenue par cevital va cesser de paraître à partir du 6 avril 2022enraison de problèmes financiers. La procédure du dépôt de bilan par l'entreprise éditrice du journal Liberté sera lancée le 6 avril 2022 et le journal Liberté continuera à paraître jusqu'à la fin du mois d'avril 2022.

➢ Fin juin 2022, Issad Rebrab annonce quitter ses fonctions et mandats au sein del'entreprise pour partir à la retraite. Malik Rebrab, son fils, prend sa succession entant que PDG à partir du 30 juin 2022.

IV.3 Organigramme

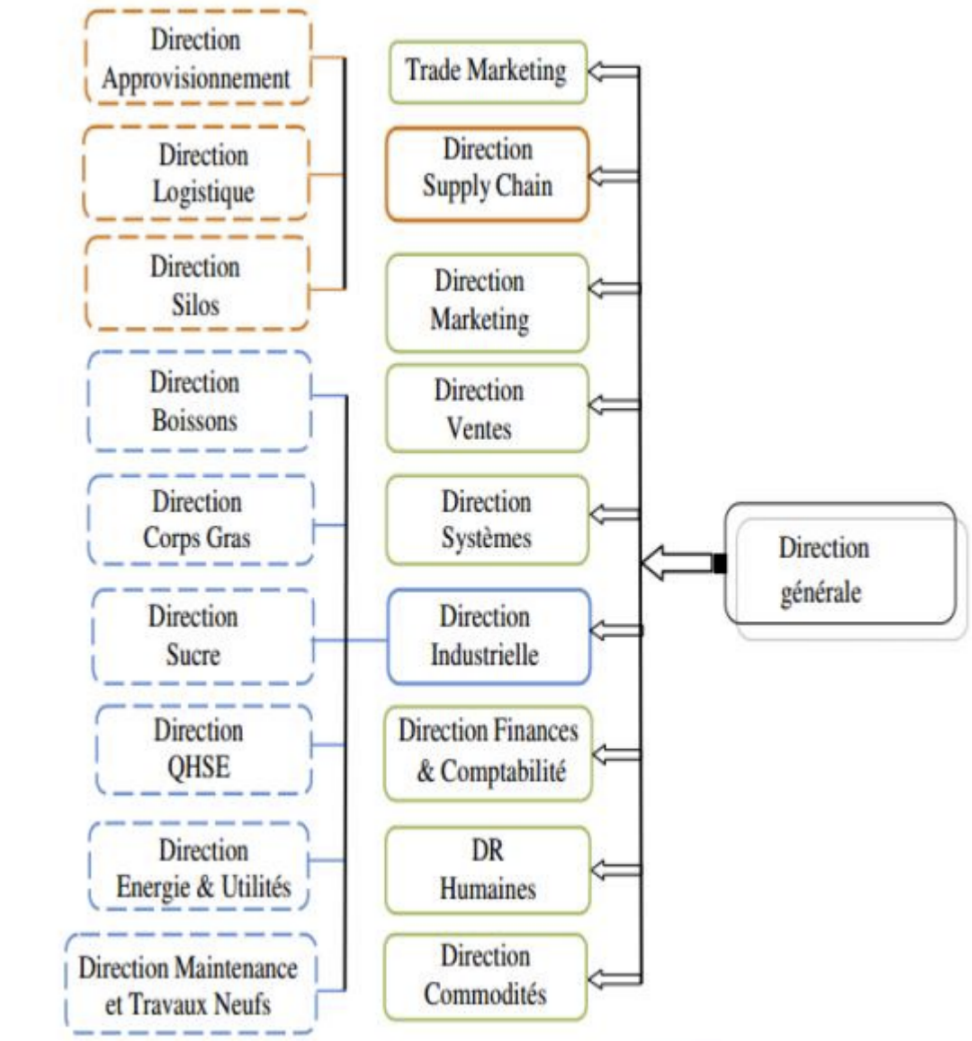


Figure IV.1 – Source : document interne CEVITAL.

IV.4 Mission de l'entreprise

L'entreprise a pour mission principale de développer la production et d'assurer la qualité et le conditionnement des huiles, des margarines et du sucre à des prix nettement plus compétitifs et cela dans le but de satisfaire le client et le fidéliser. Les objectifs visés par CEVITAL peuvent se présenter comme suit :

- ➢ L'extension de ses produits sur tout le territoire national ;
- ➢ L'importation de graines oléagineuses pour l'extraction directe des huiles brutes ;
- ➢ L'optimisation de ses offres d'emploi sur le marché du travail ;
- ➢ L'encouragement des agriculteurs par des aides financières pour la production locale de graines oléagineuses.

IV.5 Problématique

Aujourd'hui l'internet apporte une réelle valeur ajoutée aux entreprises, en permettant la communication avec de nombreux partenaires, fournisseurs et clients, ceux-ci exposent les systèmes des entreprises à de nouvelles formes de menaces. Le véritable défi est la sécurisation du réseau informatique pour conserver un haut degré de fiabilité du trafic sur le réseau.

Après un entretien effectué avec le chef de département technique I.T (S.P.A CEVITAL), nous avons pu parler des différentes techniques pour administrer et dépanner un réseau d'entreprise, ainsi que les problèmes qu'il rencontre pendant ses missions quotidiennes au sein de l'entreprise, et aussi les différentes menaces qu'ils ont subits, nous avons pu donc résumer les problématiques majeures qui affectent négativement un réseau comme suit :

- ➢ Vulnérabilités de sécurité, surtout les attaques « zero day».
- ➢ Un manque ou faiblesse des outils de sécurité, et manque de tests de sécurité.
- ➢ Abus des privilèges des comptes d'utilisateurs, et excès de confiance.
- ➢ Ignorance de la sécurité au niveau des couches inférieurs des maillons les plus faibles.
- ➢ Utilisateurs insensibilisés envers la sécurité.

IV.6 Objectifs

L'objectif de ce projet, est de travailler sur la cyber security, network security, et s'introduire à l'Ethical hacking, nous voulons créer une architecture capable d'assurer la sécurité d'un réseau d'entreprise en rependant aux problématiques mentionnés, et s'assurer que les stratégies et les politiques de sécurité implémentés font l'objet d'une mise en œuvre cohérente et mesurable. Nous avons pour objectifs :

- ➢ Implémentation des équipements et des technologies logicielles qui assure la sécurité et la robustesse du réseau (NGFW, VPN, IPS/IDS, Proxy, CISCO IOS ...
- ➢ Se protéger contre les hackers, en limitant l'accès au réseau.
- ➢ Effectuer des simples tests de sécurité.
- ➢ Savoir comment analyser les états du pare-feu, et gérer les logs.

IV.7 Conclusion

Dans ce chapitre, nous avons appris à mieux comprendre la structure et l'organisation du réseau de Cevital, et d'étudier notre problématique afin de proposer les solutions adéquates et les objectifs à atteindre.

V

Partie pratique

V.1 Études et analyses des besoins

V.1.1 Introduction

Nous avons vu lors des chapitres précédant (partie théorique) les différents types de réseaux, ainsi la sécurité informatique et celle des réseaux d'entreprise. On a pu voir aussi le domaine des firewalls, au final les différentes fonctionnalités qu'offre un système de détection d'intrusion et le système de prévention d'intrusion, ainsi que les types de filtrage et le fonctionnement du snort.

Dans la partie pratique, nous allons mettre en œuvre tout les mécanismes de sécurité possibles affin d'atteindre un niveau maximal de sécurité. Ce travaille sera simulé/émulé(GNS3, Vmware, Qemu ... etc) et a l'aide de plusieurs templates (GNS3 VM, kali LINUX,CISCO IOU, Microsoft Windows, pare-feu ... etc).

Pour présenter les configurations que nous avons réalisées, nous nous sommes servies des captures d'écran qui illustrent les étapes de la configuration. Enfin, des tests de validation pour Confirmer le bon fonctionnement du réseau, seront réalisés.

V.1.2 Présentation des solutions

V.1.2.1 Simulation/émulation

V.1.2.1.1 Les outils

- **Cisco Packet Tracer**

  Packet Tracer est un simulateur de matériel réseau Cisco (routeurs, commutateurs). Cet outil est créé par Cisco Systems qui le fournit gratuitement aux centres de formation, étudiants et diplômés participant, ou ayant participé, aux programmes de formation

Cisco(Cisco Networking Academy). Le but de Packet Tracer est d'offrir aux élèves et aux professeurs un outil permettant d'apprendre les principes du réseau, tout en acquérant des compétences aux technologies spécifiques de Cisco. Il peut être utilisé pour s'entraîner, se former, préparer les examens de certification Cisco, mais également pour de la simulation réseau.

- **GNS 3**

  GNS3, ou Graphical Network Simulator-3, est un logiciel open-source qui offre un environnement de simulation de réseau pour les professionnels des technologies de l'information (TI) et les ingénieurs réseau. Il permet aux utilisateurs de créer des topologies réseau virtuelles en utilisant des routeurs, des commutateurs, des pare-feu et d'autres périphériques réseau virtuels, le tout sur un ordinateur local.

- **Vmware Workstation**

  VMware Workstation est un outil de virtualisation de poste de travail créé par la société VMware, il peut être utilisé pour mettre en place un environnement de test pour développer de nouveaux logiciels, ou pour tester l'architecture complexe d'un système d'exploitation avant de l'installer réellement sur une machine physique. VMware Workstation permet l'installation de plusieurs instances de différents systèmes d'exploitation, y compris les systèmes d'exploitation client et serveur. Il aide les administrateurs réseau ou système à vérifier, tester et vérifier l'environnement client-serveur. L'administrateur peut également basculer entre différentes machines virtuelles en même temps.

- **Pfsense**

  Ce logiciel est totalement gratuit. Il s'agit d'une distribution personnalisée de FreeBSD spécialement conçue pour être utilisée comme pare-feu et routeur entièrement gérée via une interface Web.. pfSense peut être installé sur une variété d'appliances matérielles, même du matériel de très faible spécification peut être utilisé. Pour les ingénieurs réseau hautement technique, il est conseillé d'opter pour pfSense pour bénéficier d'une flexibilité et d'une variété d'options pour configurer chaque aspect en profondeur. Le tableau de bord est disponible avec des widgets configurables où la surveillance du matériel, du trafic réseau et de l'utilisation peut être effectuée. Il donne la possibilité de voir qui fait quoi et quand. Negate publie périodiquement de nouvelles versions contenant de nouvelles fonctionnalités, des mises à jour, des corrections de bogues et diverses autres modifications. Dans la plupart des cas, la mise à jour d'une installation est facile.

V.1.2.2 Implémentation

Après avoir analysé et même essayé certaines solutions qu'on a proposé, nous avons donc décidé pour ce projet du GROUPE CEVITAL sous thème «sécuriser un réseau d'entreprise avec un firewall pfsens et IDS,IPS/Snort », simuler/émuler le travail sur GNS3 car il décrit parfaitement les deux termes simuler/émuler c'est à dire : reproduire l'architecture d'un réseau et cela sans utiliser de machine physique, et reproduire à l'identique le comportement des logiciels et leurs architecture matérielle, et surtout que GNS3 est gratuit et open source ce qui disqualifie d'entrée un bon nombre de ses concurrents. Permet en plus de tester tout type de machines, et pas seulement celui d'un constructeur en particulier, en résumé GNS3est gratuit, open source, multiplateforme, et permet de tester toutes les machines possibles et de les connecter entre elles. De plus, il est aujourd'hui l'un des plus fiables, étant utilisé par un grand nombre de professionnels et d'universités dans le monde.

Donc dans le prochain chapitre (réalisation) nous allons voir comment installer GNS3 et VMware, ainsi que le pare-feu Pfsense.

Cependant on va mettre en place une solution de filtrage afin de limiter l'accès aux utilisateurs à des sites inappropriés. Le filtrage est basé sur plusieurs listes de domaines qui peuvent être placées soit en liste blanche (sites autorisés) soit en liste noire (sites interdits).

Nous allons configurer sur pfSense un bon nombre d'éléments de base, ainsi que les configurations des interfaces et effectuer des opérations et des tests de pénétration a l'aide de KALI LINUX.

V.2 Réalisation

V.2.1 Installation de Vmware workstation 17 pro

V.2.1.1 Introduction

VMware Workstation Pro est un hyperviseur hébergé fonctionnant sur les versions x64dessystèmes d'exploitation Windows et Linux (une version x86 des versions précédentes était disponible) ; il permet aux utilisateurs de configurer des machines virtuelles (VM) sur une seule machine physique et de les utiliser simultanément avec la machine hôte.

Pendant ce temps, VMware Workstation facilite le pont des adaptateurs réseau hôtes existants et le partage des lecteurs de disques physiques et des périphériques USB avec une machine virtuelle. Il peut simuler des lecteurs de disque ; un fichier image ISO peut être monté en tant que lecteur de disque optique virtuel et les lecteurs de disque virtuels peuvent être montés en tant que fichiers .vmdk.

V.2.1.2 Téléchargement

Il faut noter que les stations de travail VMware ne sont pas des logiciels gratuits et peuvent être achetées sur VMware Store. Ils ont un essai de 30 jours, donc pour une version gratuite de l'application, il est possible d'essayer VMware Player, qui est gratuit pour un usage personnel.

Le téléchargement de l'application est assez simple. Tout ce qu'il faut faire c'est de télécharger le programme d'installation pour Windows à partir du site Web

https://www.vmware.com/products/workstation-pro.html, de l'exécuter et de suivre les instructions.

V.2.1.3 Installation

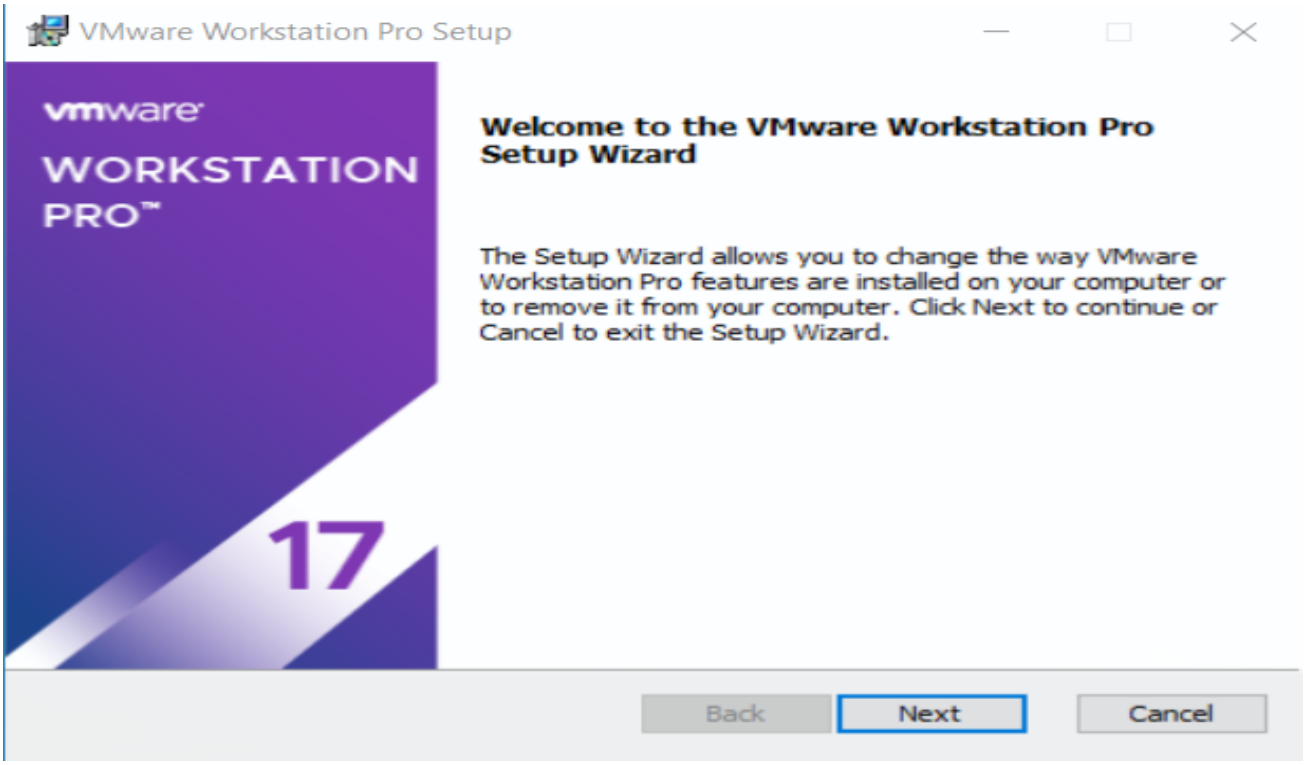


Figure V.1 – Vmware Workstation Pro Setup.

- **Étape 1 :** Après voir lu le contrat de licence. Accepter -Next-.
- **Étape 2 :** Choisir le lieu souhaité pour l'installation puis - Next -.
- **Étape 3 :** VMware nous invite à sélectionner "Vérifier les mises à jour" et "Aidez à améliorer VMware Workstation Pro". l'utilisateur fait comme il souhaite. Pour notre cas on souhaite vérifier les mises à jour. - Next -.
- **Étape 4 :** Cliquer sur Licence pour ajouter la licence.
- **Étape 5 :** Saisissez votre clé de licence personnelle afin d'activer votre installation de VMware Workstation Pro. Vous pouvez aussi effectuer cette étape plus tard. Cliquez sur **"Enter"**.

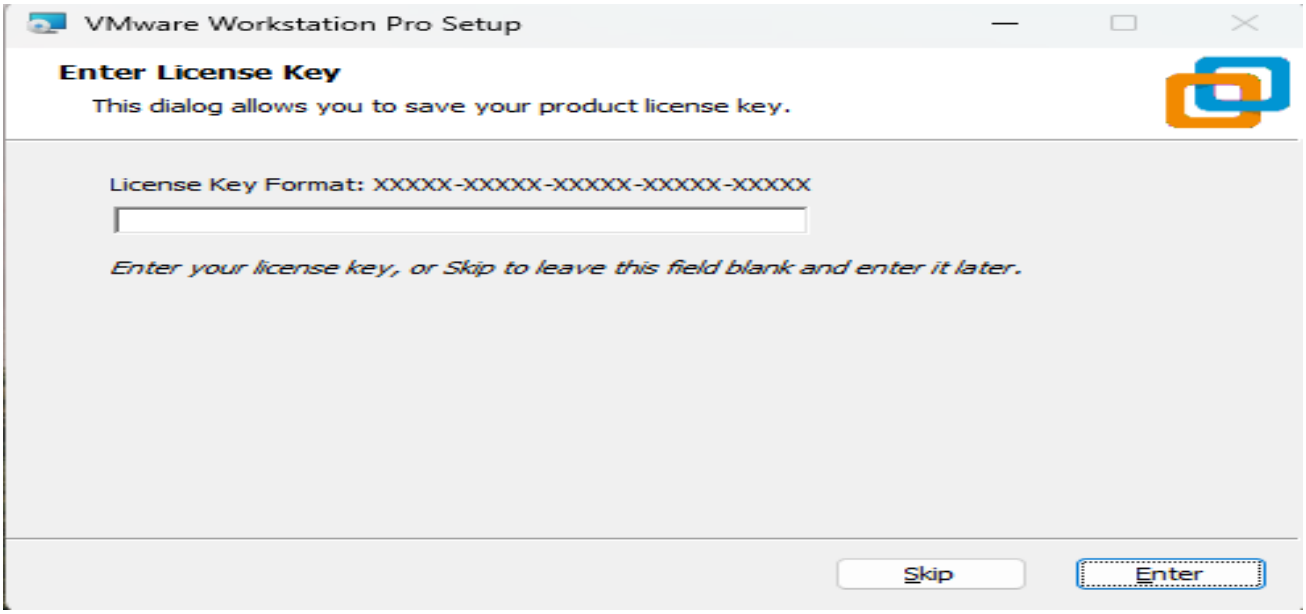


Figure V.2 – VMware workstation 17 pro license key.

Une fois que l'installation est effectuée, vous pouvez accéder à la console de gestion de VMware Workstation. Au centre, trois boutons :

- **Create a new virtual machine** pour créer une nouvelle machine virtuelle.
- **Open a virtual machine** pour ouvrir une machine virtuelle existante.
- **Connect to a remote server** pour se connecter sur un hyperviseur VMware ESXi (fonction spécifique à l'édition Pro).

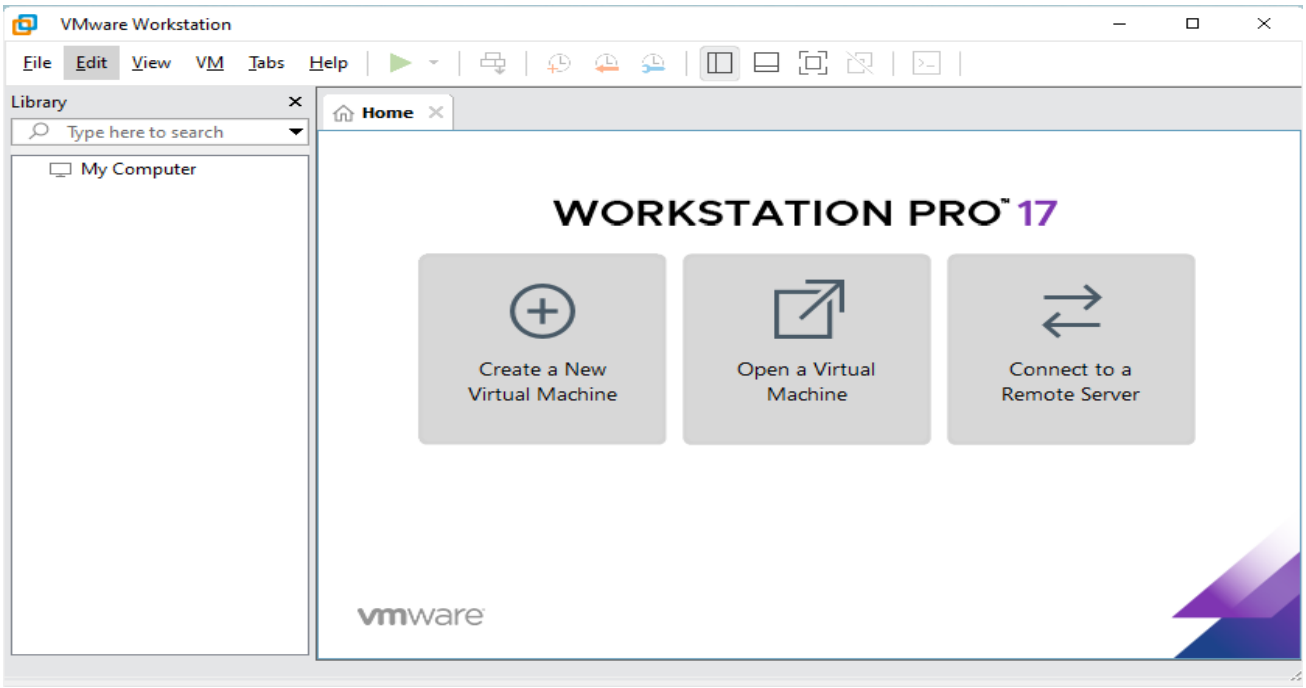


Figure V.3 – VMware workstation 17 pro.

V.3 Installation GNS3

V.3.1 Indroduction

GNS3 est une plateforme de virtualisation de réseau open-source largement utilisée par les professionnels des réseaux informatiques pour la conception, la simulation et le test de réseaux informatiques. Il permet aux utilisateurs de créer des topologies réseau virtuelles en utilisant des routeurs, des commutateurs, des pare-feu et d'autres périphériques réseau virtuels, tout en offrant un environnement de laboratoire sécurisé pour expérimenter et apprendre les concepts de réseau.

V.3.2 GNS3

L'interface de GNS3 est conçue pour être conviviale et intuitive, permettant aux utilisateurs de créer, configurer et gérer des topologies de réseau virtuelles. Voici une brève description des principaux éléments de l'interface de GNS3 :

- **Barre de menu :** La barre de menu située en haut de la fenêtre de l'application contient des options pour les actions courantes telles que le démarrage et l'arrêt des périphériques virtuels, l'importation/exportation de projets, la gestion des préférences, etc.
- **Barre d'outils :** La barre d'outils contient des icônes pour des actions fréquemment utilisées, telles que l'ajout de périphériques, la connexion de câbles, le démarrage/arrêt de la simulation, etc.
- **Zone de travail :** C'est la zone principale où vous créez et configurez votre topologie réseau. Vous pouvez faire glisser et déposer des périphériques virtuels depuis la palette des périphériques et les connecter en utilisant des câbles.
- **Palette des périphériques :** La palette des périphériques est située généralement à gauche de l'interface. Elle contient une liste de périphériques virtuels que vous pouvez ajouter à votre topologie, y compris des routeurs, des commutateurs, des pare-feu, etc. Vous pouvez rechercher et faire glisser ces périphériques dans la zone de travail.
- **Vue des appareils :** Cette fenêtre affiche les détails et la liste des périphériques que vous avez ajoutés à votre topologie. Vous pouvez y accéder pour configurer les paramètres spécifiques de chaque périphérique.
- **Console des périphériques :** Une fois que vous avez ajouté des périphériques à votre topologie, vous pouvez ouvrir une console pour chaque périphérique pour interagir avec eux via la ligne de commande. C'est ici que vous pouvez configurer les périphériques comme vous le feriez dans un vrai réseau.
- **Gestionnaire de projets :** GNS3 permet de gérer différents projets, chaque projet pouvant avoir sa propre topologie. Vous pouvez créer, ouvrir, enregistrer et gérer des projets à partir du gestionnaire de projets.
- **Barre d'état :** La barre d'état située en bas de l'interface affiche des informations sur l'état de la simulation, telles que la consommation de ressources CPU et mémoire, l'état des périphériques, etc.

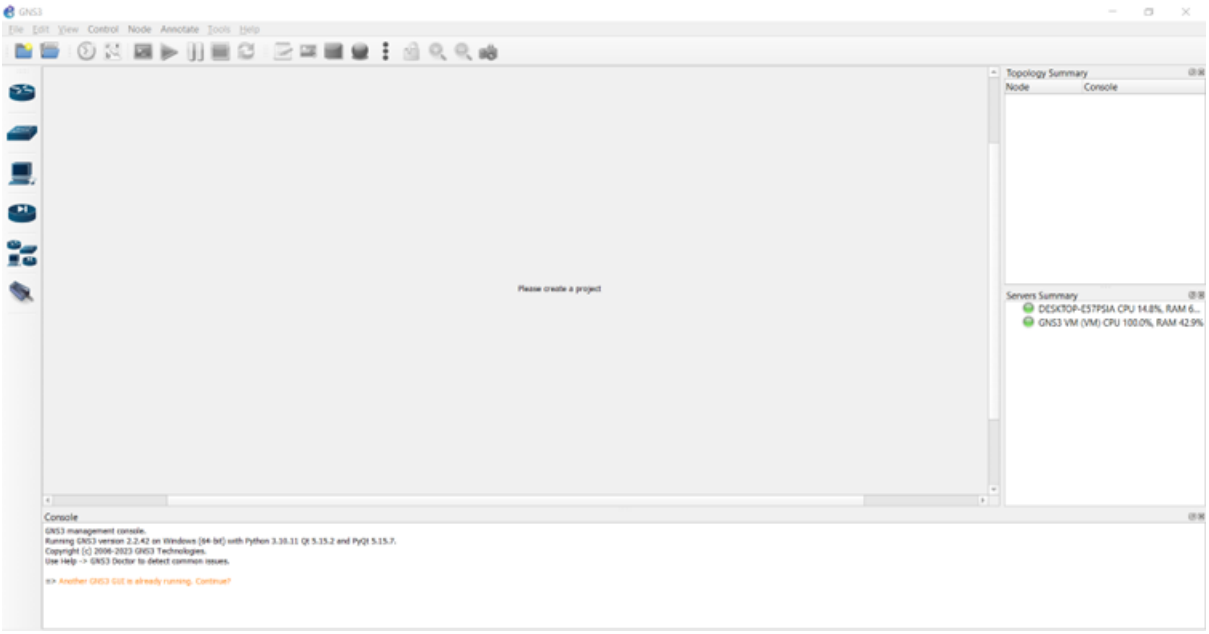


Figure V.4 – Interface GNS3.

V.4 Installation pfsense

Accédez au site officiel : https://www.pfsense.org/

Sur le portail de téléchargement Pfsense, vous devrez trouver la dernière version de Pfsense Firewall.

Sélectionnez le logiciel Pfsense Archictecture, sélectionnez le format d'installation ISO et cliquez sur le bouton download.

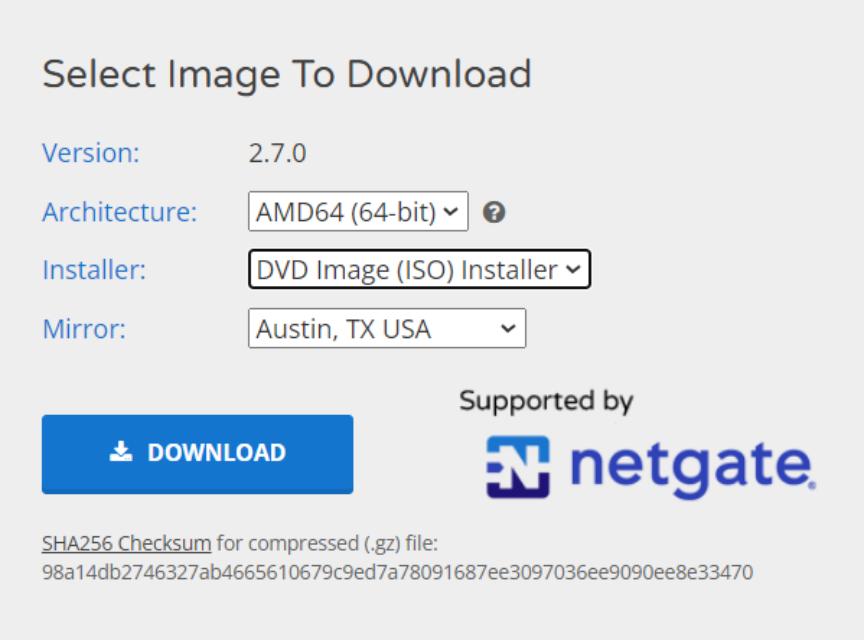


Figure V.5 – Interface de téléchargement.

Après avoir insérer l'ISO de pfsense dans VM dédiée, vous pouvez démarrer la machine. Le setup va démarrer automatiquement.

Figure V.6 – Setup automatique de PFsense.

L'installation va s'effectuer au clavier. Appuyez sur la touche Entrée pour Accepter.

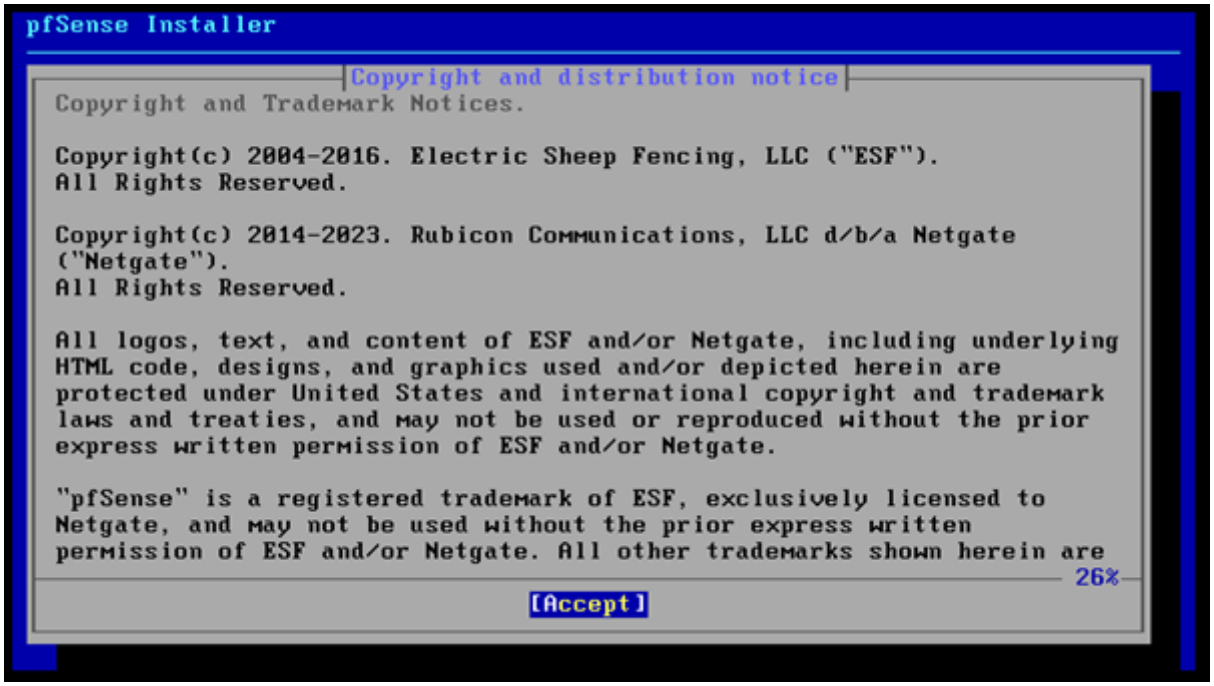


Figure V.7 – Étape d'installation.

Vérifiez que vous êtes bien sur « Install » et appuyez sur Entrée pour faire OK.

Figure V.8 – Installation.

Sélectionnez la disposition de clavier Pfsense souhaitée.

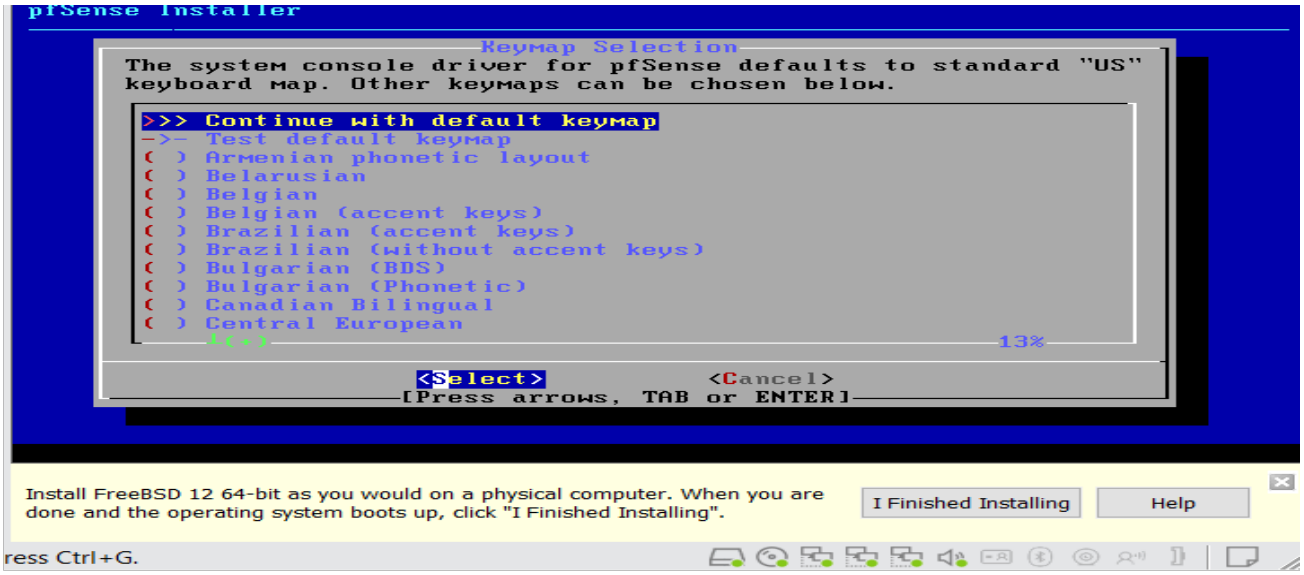


Figure V.9 – Sélection d'une disposition de clavier.

Sélectionnez l'option Auto (ZFS) pour effectuer automatiquement le partitionnement du disque.

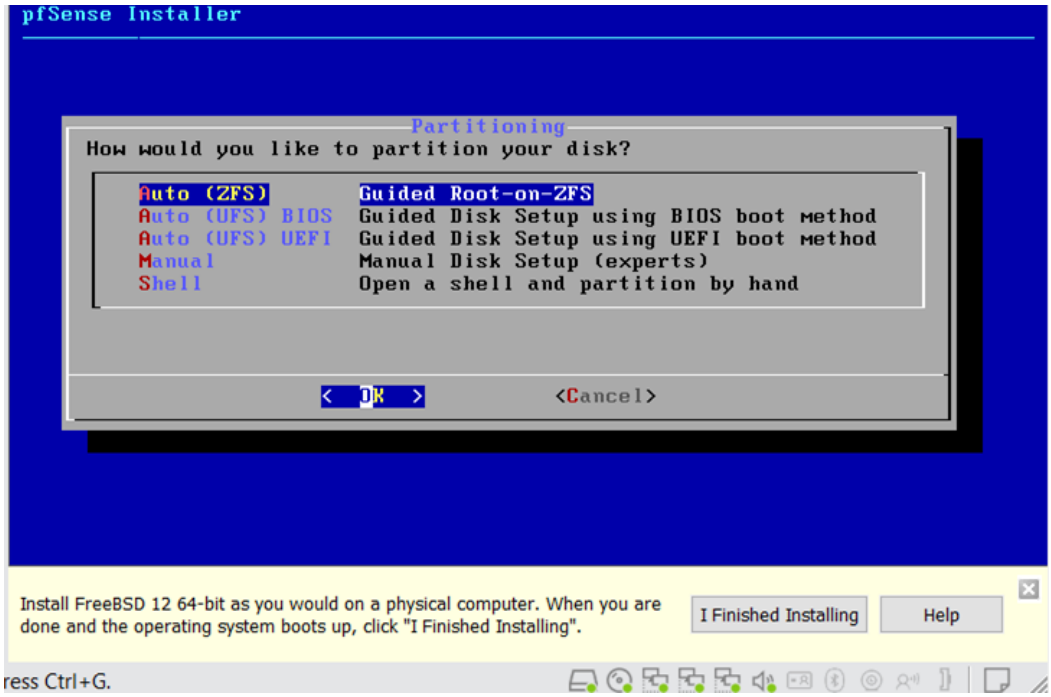


Figure V.10 – Partirionnement automatique du disque.

Le système démarrera l'installation du serveur Pfsense.

Attendez que l'installation se termine.

Une fois l'installation est terminer, vous aurez le shell de pfsense.

Dans notre cas l'interface WAN à obtenue automatiquement l'adresse : 192.168.147.134/24

On as configurer les deux interfaces LAN et DMZ statiquement :

Interface LAN : 192.168.0.1/24

Interface DMZ : 172.16.0.1/24

Connexion au tableau de bord PFSense

Après avoir terminé la configuration de l'adresse IP, vous pouvez accéder à l'interface Web de PFsense.

Ouvrez un logiciel de navigateur, entrez l'adresse IP de votre pare-feu Pfsense et accédez à l'interface Web.

Dans notre exemple, l'URL suivante a été saisie dans le navigateur :

https ://192.168.0.1

L'interface web Pfsense doit être présentée.

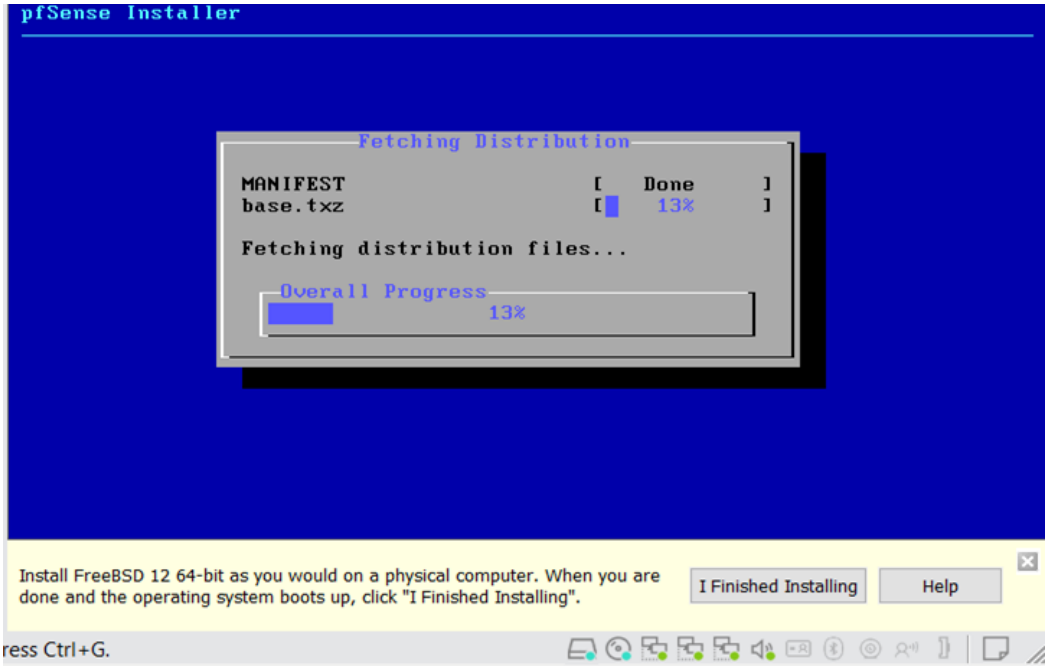


Figure V.11 – Lancement de l'installation.

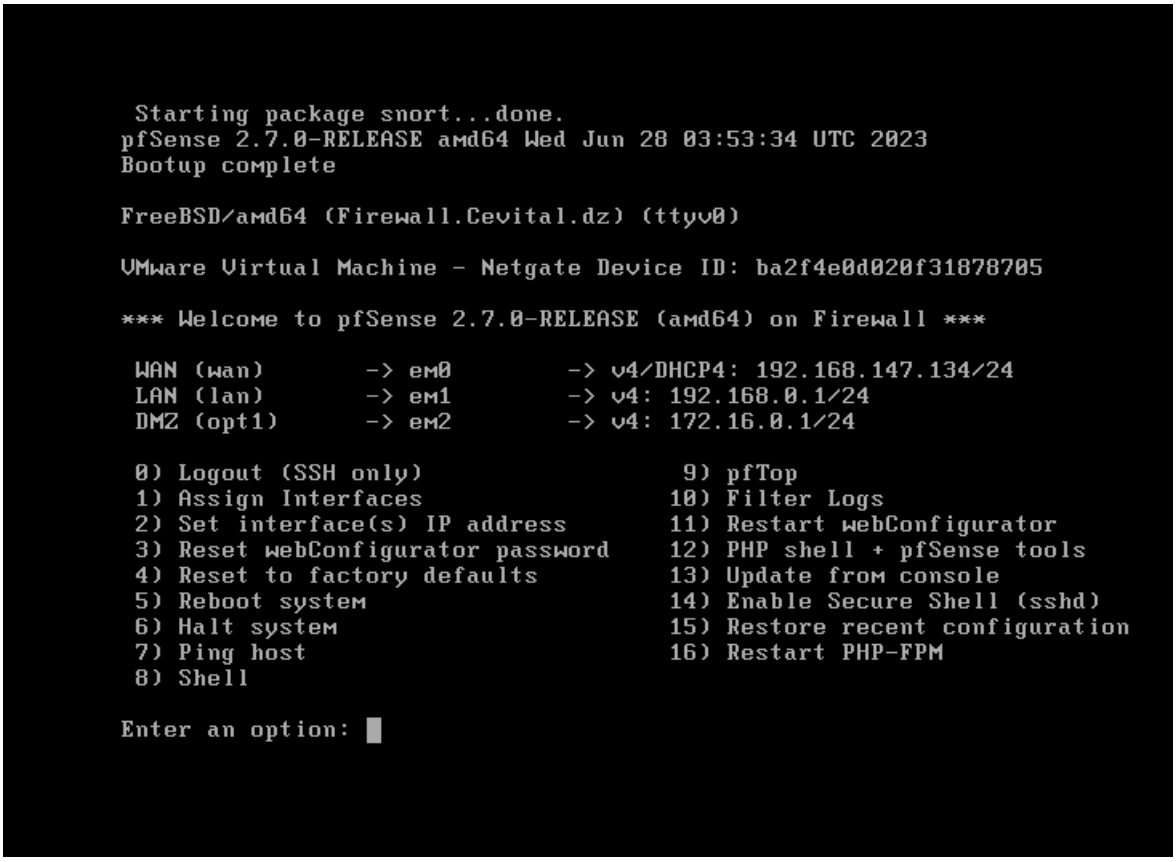


Figure V.12 – Shell PFsense.

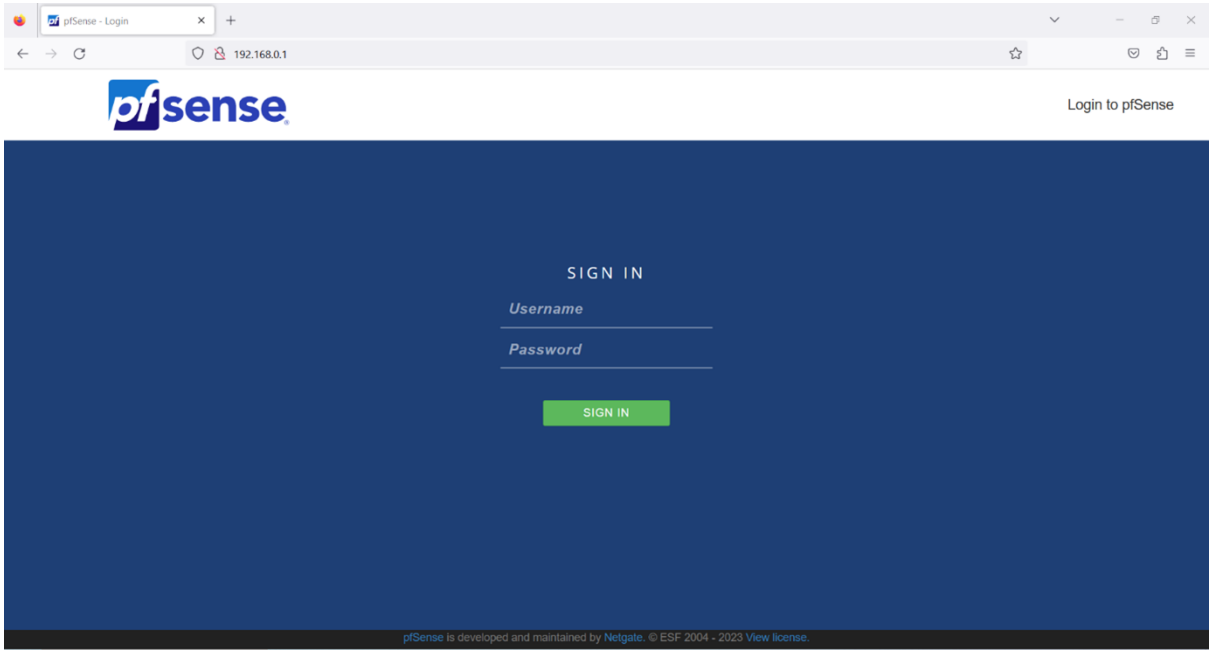


Figure V.13 – Interface web Pfsense.

Sur l'écran rapide, entrez les informations de connexion Pfsense Default Password.
Username : admin
Mot de passe : pfsense
Après une connexion réussie, vous serez envoyé au tableau de bord Pfsense.

Figure V.14 – Tableau de bord Pfsense.

V.5 Installation Snort

Accédez au menu Pfsense System et sélectionnez l'option Package Manager.

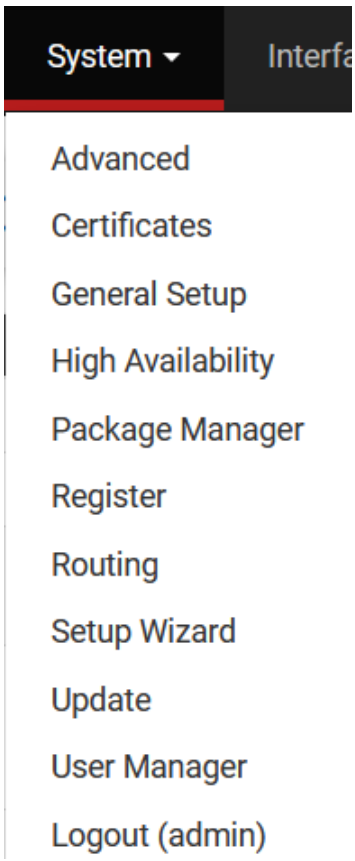


Figure V.15 – Menu Pfsense système.

Sur l'onglet Paquets disponibles, recherchez SNORT et installez le paquet Snort.

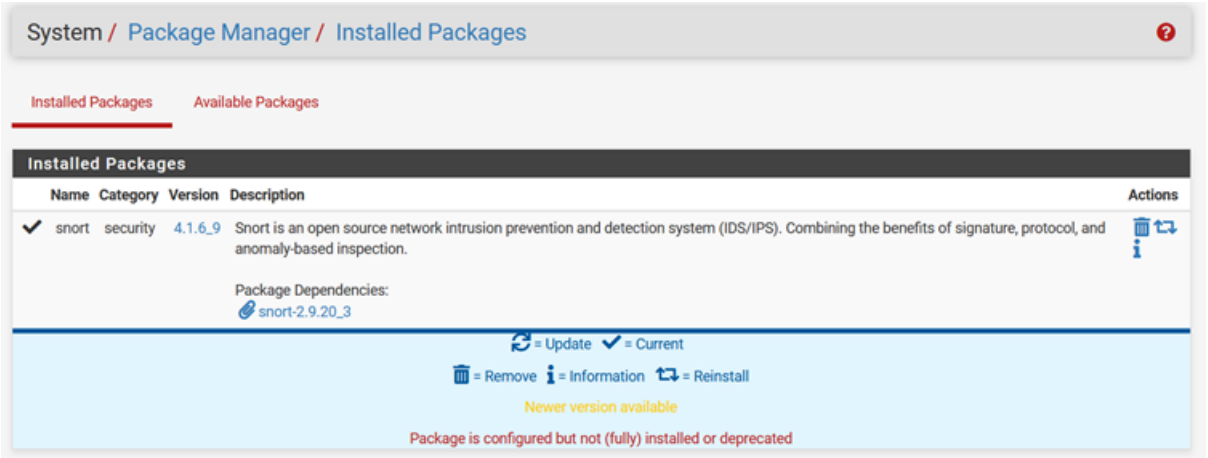


Figure V.16 – Interface paquets disponibles.

Figure V.17

Sur l'onglet Paramètres Global, localisez les règles d'abonné Snort et effectuez la configuration suivante :

Activer Snort VRT - Oui

Code Snort Oinkmaster - Entrez-vous OikCode

Si vous n'avez pas d'Oinkcode, accédez au site Web Snort,créez un compte et obtenez un Oinkcode gratuit.

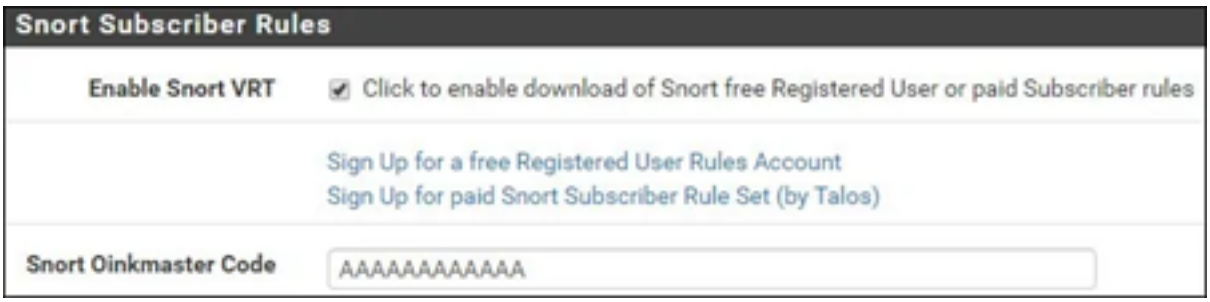


FIGURE V.18

Localiser la zone Paramètres de mise à jour des règles et effectuer la configuration suivante :

- Intervalle de mise à jour - Sélectionnez l'intervalle de mise à jour souhaité.

- Heure de démarrage de mise à jour - Définir l'heure désirée pour mettre à jour les règles Snort.

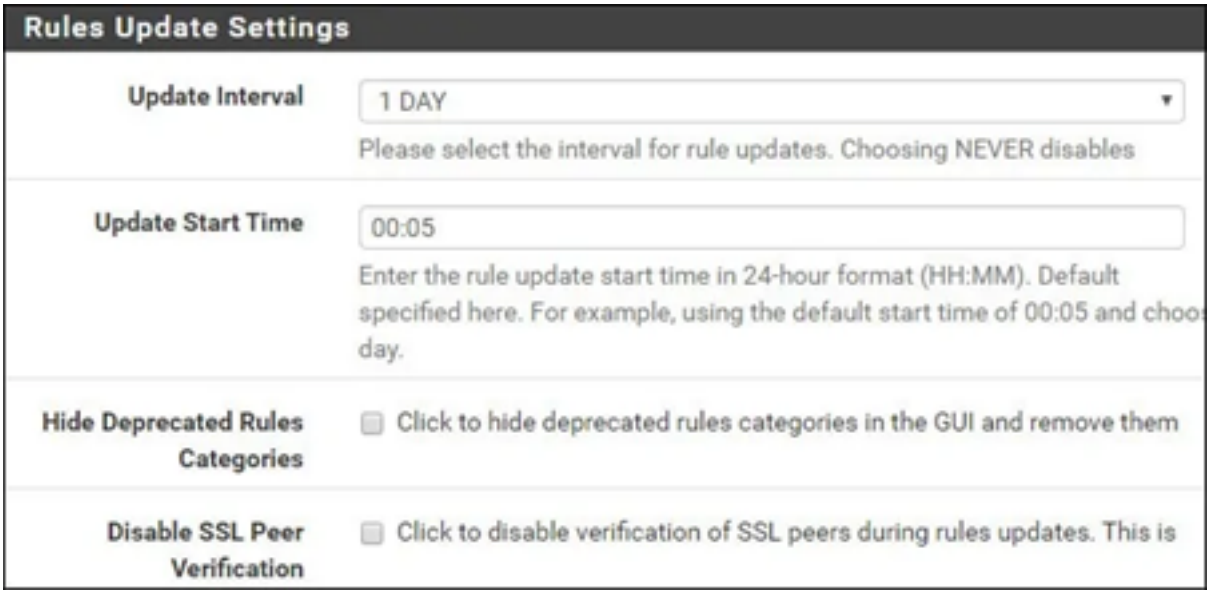


FIGURE V.19

Localiser la zone Paramètres généraux et effectuer la configuration suivante :

Supprimer l'intervalle des hôtes bloqués - 1 heure

Supprimer les hôtes bloqués après la désinstallation - Non

- Conserver les paramètres snort après la désinstallation - Oui

- Intervalle de mise à jour de démarrage/shutdown – non

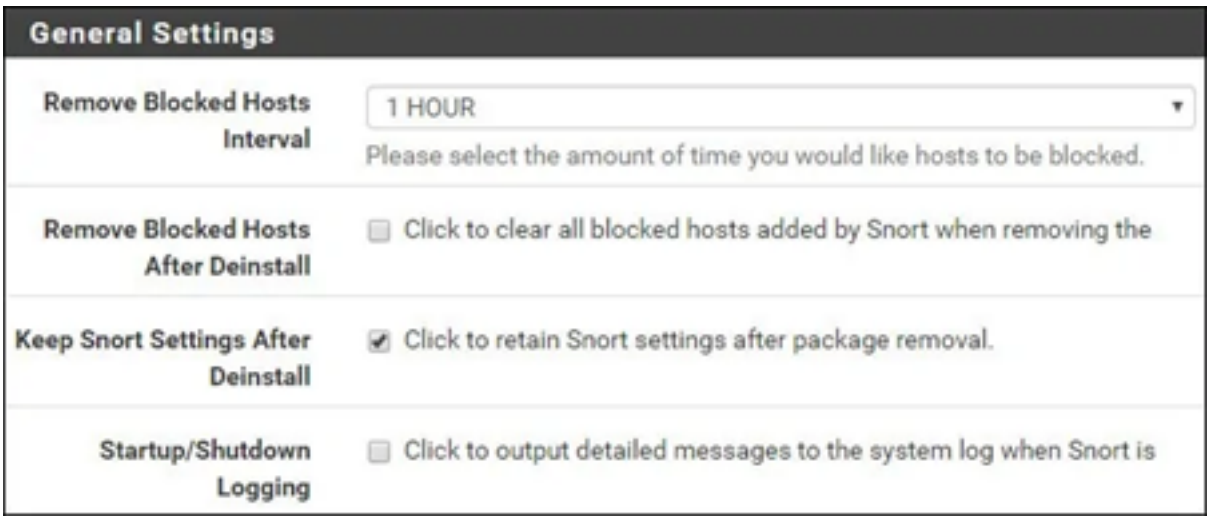


FIGURE V.20

Sur l'onglet Mises à jour, cliquez sur le bouton Règles de mise à jour pour télécharger les règles Snort.

FIGURE V.21

Sur l'onglet Interfaces Snort, cliquez sur le bouton Ajouter et effectuez la configuration suivante.

Activer - Oui

Interface - Sélectionnez l'interface désirée pour surveiller

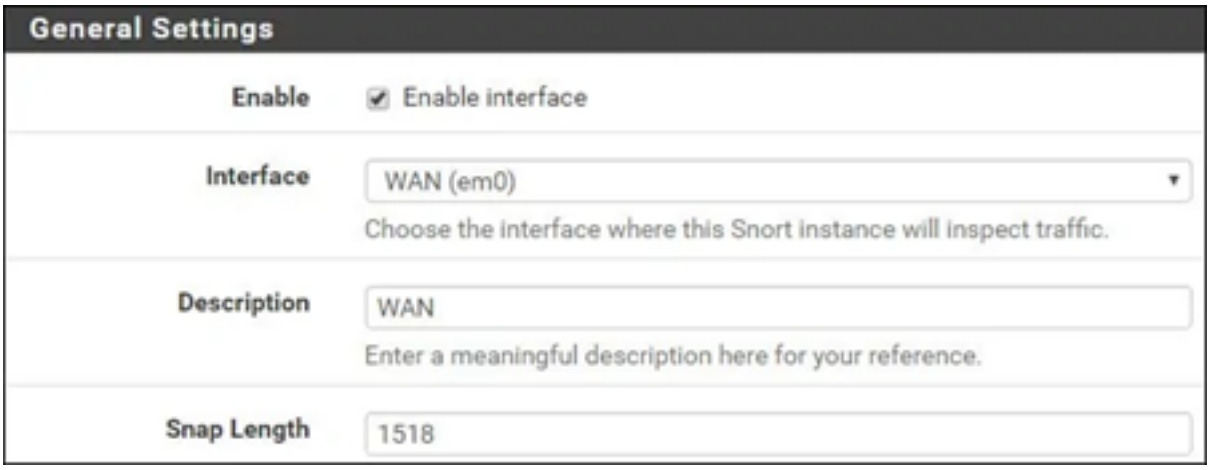


FIGURE V.22

Localiser la zone Paramètres d'alerte et effectuer la configuration suivante :

Envoyer des alertes au journal du système - Oui

- Bloquer les contrevenants - Activer si vous voulez bloquer les délinquants.

États de tuer - Oui
Quel IP bloquer - BOTH

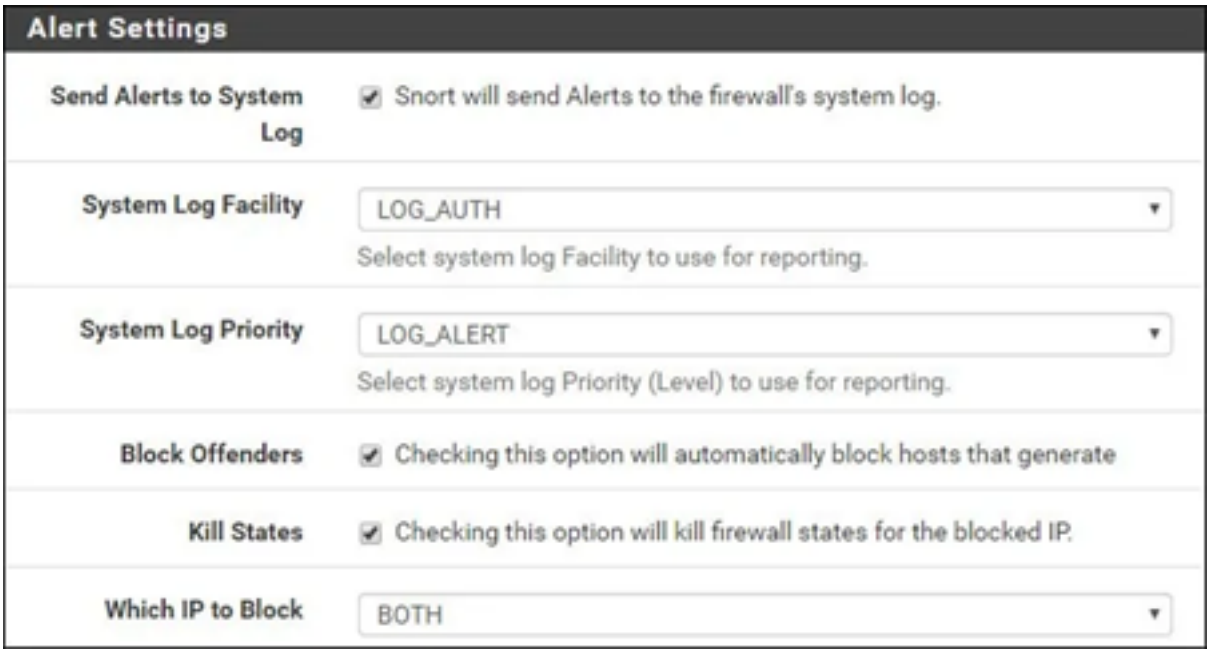


FIGURE V.23

Après avoir terminé la configuration, cliquez sur le bouton Enregistrer.

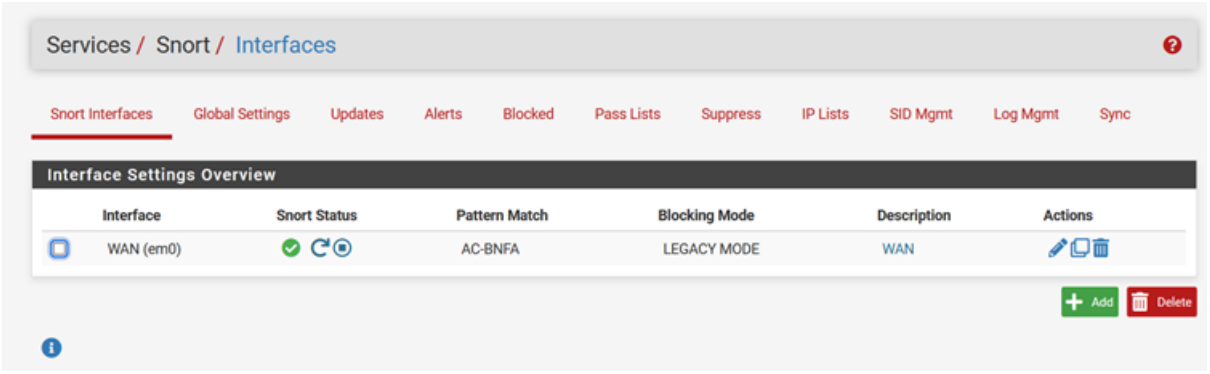


FIGURE V.24

V.6 Topologie du projet

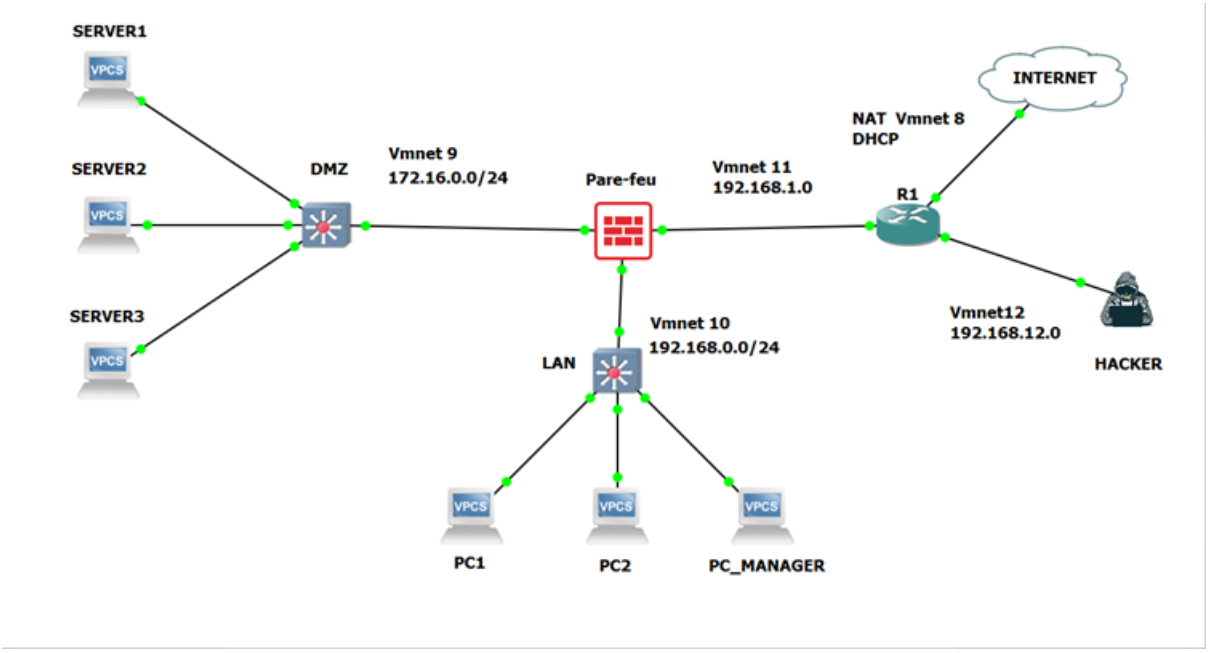


Figure V.25 – Topologie.

Pour commencer nous allons configurer les trois interfaces sur pfsense (LAN(em1), WAN(em0), DMZ (em2)).

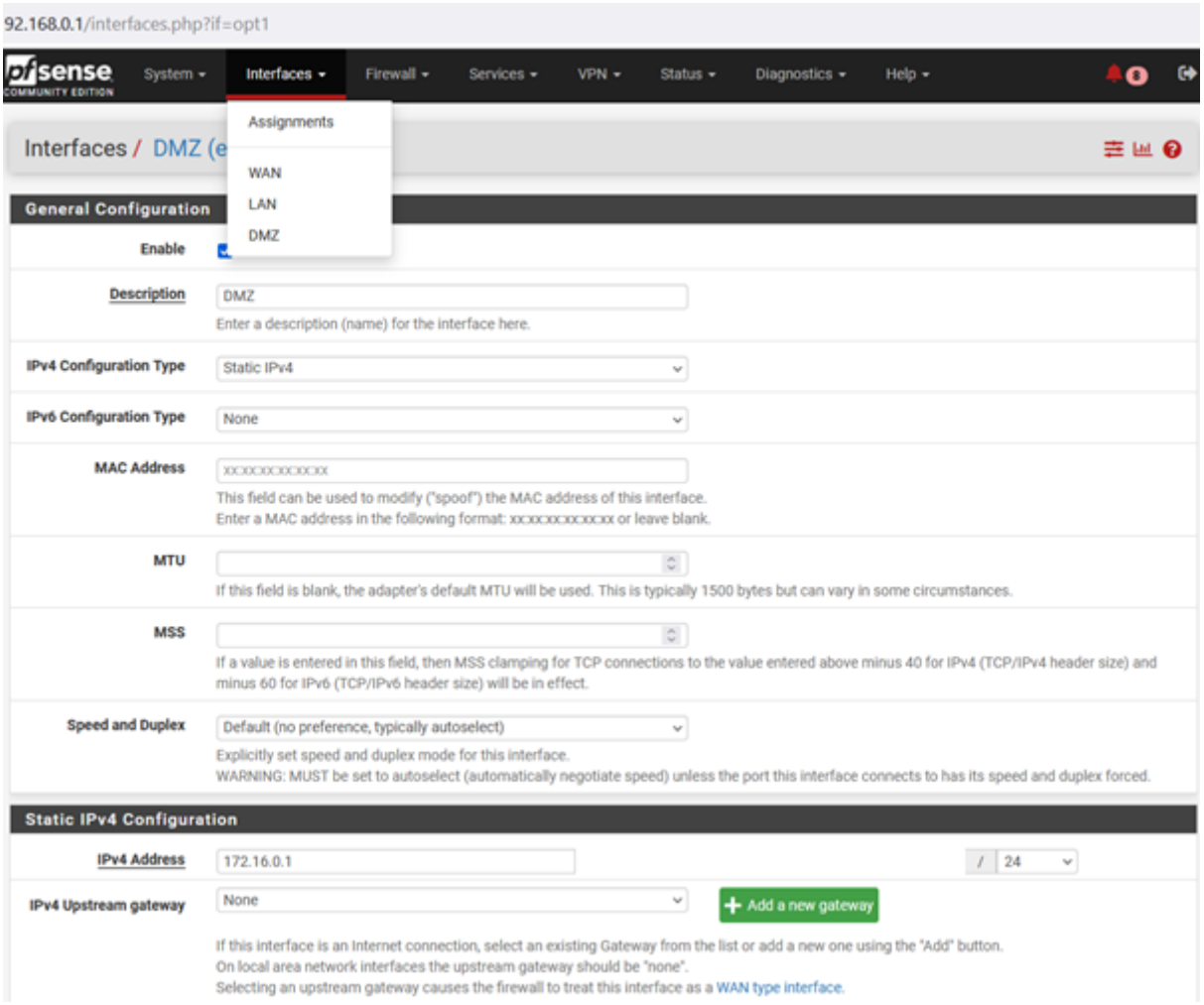


Figure V.26 – Exemple de création d'une interface -DMZ-

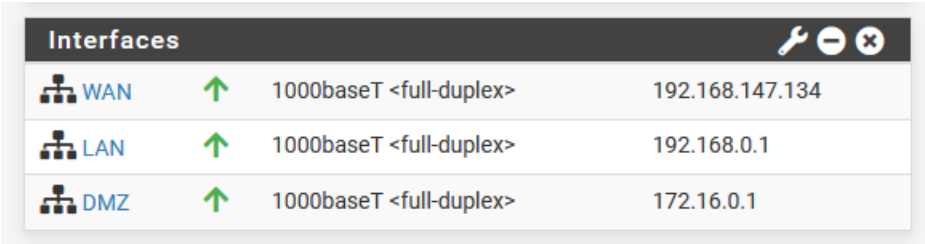
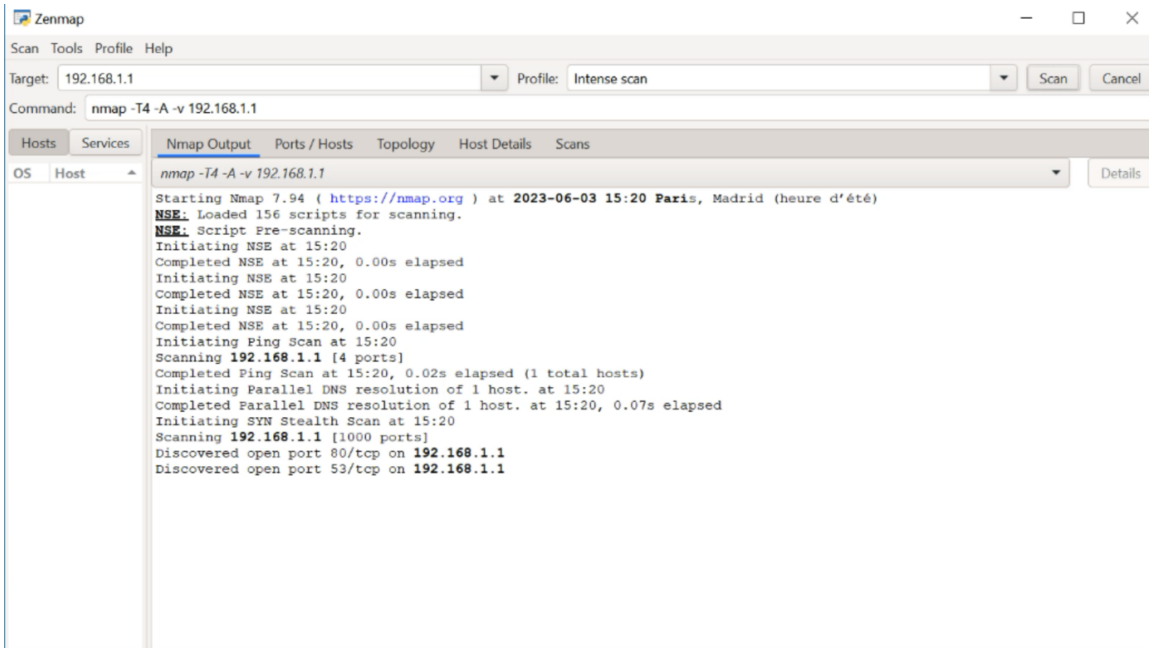
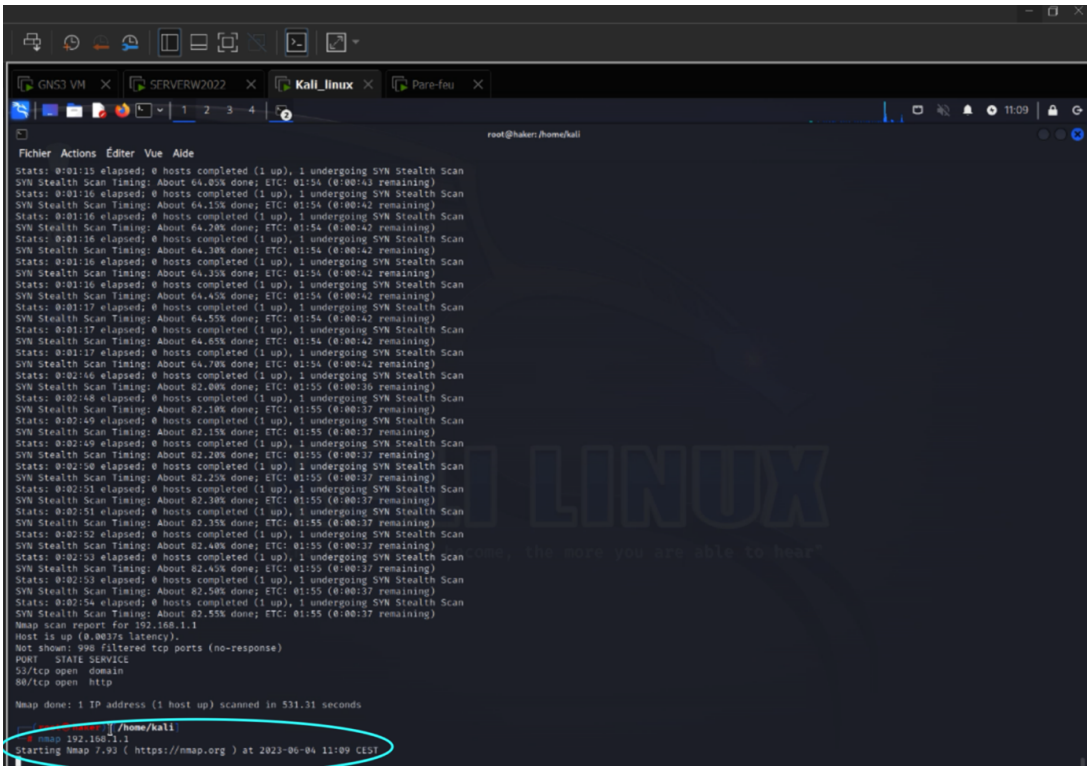


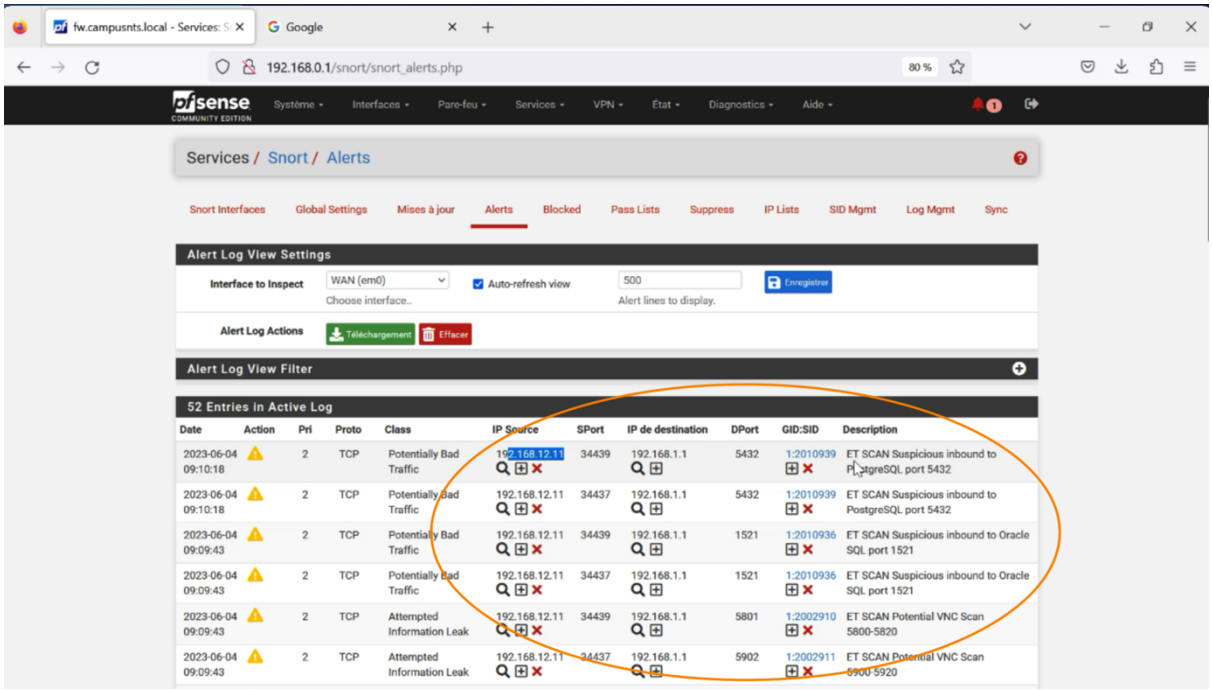
Figure V.27 – Interfaces crées sur Pfsense

On vas ensuite simuler une attaque de type Scan :





On remarque sur la figure qui suit les différentes alertes :



Nous constatons clairement que SNORT a détecté l'attaque, et affiche même les adresses de l'attaquant.

Conclusion générale

Les entreprises représentent une cible privilégiée pour les cybercriminels, toujours plus inventifs et ingénieux. Les conséquences de leurs attaques sont dramatiques : perte de chiffre d'affaires, arrêt de la production, image de marque dégradée... Dans de nombreux cas, la cyberattaque entraîne même la fermeture des entreprises visées.

Afin de garantir la sécurité des réseaux informatiques devant la multitude des risques et menaces, il devient indispensable d'imaginer et de réaliser des solutions efficaces de protection, qui garantissent la continuité des différentes activités de l'entreprise.

Ce travail consiste en premier lieu à présenter les failles de sécurité courantes au niveau des réseaux, et à l'aide de l'expérience du département technique IT de S.P.A CEVITAL, nous avons pu construire un réseau de référence vis-à-vis la cyber sécurité et Network security.

Une architecture dont la sécurité est basée et assurée par l'utilisation d'un pare-feu open source Pfsence, et des périphériques réseau du grand constructeur CISCO.

Afin de démontrer la fiabilité de notre solution, nous avons simulé/émulé l'architecture réseau sécurisée en utilisant les deux outils GNS3 et Vmware workstation 17 pro. Les tests effectués à l'aide de Kali linux confirment que la solution de sécurité proposée est satisfaisante. De plus, les différentes possibilités de configuration proposée par Pfsence démontrent que les pare-feu possèdent de multiples capacités d'utilisation qui peuvent différer en fonction du réseau étudié, en parallèle le matériel CISCO explique la raison de sa réputation en proposant des mécanismes de sécurité simples et efficaces pour atténuer les attaques de niveau 2.

Bibliographie

[1] N. Belhadj, Etude et conception d'une plate-forme de réseau informatique couplant entre sécurité et supervision pour l'entreprise ENIEM, mémoire fin d'étude, MAST, UMMTO, 2013.

[2] A. Boussad, La mise en place de la protection d'accès au réseau NAP associe au serveur DHCP, mémoire fin d'étude, MAST, UMMTO, 2012.

[3] A. COSTANZO, D. GRILLAT, L. LEFRANCOIS, Étude des principaux services fournis par pfSense, PfSense, 2009.

[4] M. Tran Van Tay, « Le Sèstème de dètection des intrusions et le système d'empêchement des intrusions (ZERO DAY) », Rapport de stage de fin d'études, Université du Québec à Montéal, Février 2005.

[5] Nicolas Baudoin, Marion Karle, « NT Réseaux IDS et IPS », 2003/2004.

[6] M. ABBAS Massinissa, M. AOUADI Djamel, « Détection d'intrusion dans les réseaux LAN :IDS Snort sous LINUX », Mémoire de fin de cycle Master, Université Abderrahmane Mira de Bejaia, 2016/2017.

[7] C. MICHEL, « Langage de description d'attaque pour la détection d'intrusion par corrélation d'évènements ou d'alertes en environnement réseau hétérogéne » Thése de doctorat, Université de Rennes 1, Décembre 2003.

[8] http : //www.tele.ucl.ac.be/EDU/ELEC/1997/firewall/Firewalls.html.

[9] http ://www.formations-virtualisation.fr/vmware-definition-vmware.php : Définition de VMware

[10] https ://geekflare.com/fr/ids-vs-ips-network-security-solutions/

[11] https ://www.ummto.dz/dspace/bitstream/handle/ummto/13183/Selmani%20E..pdf?sequence=1

[12] https ://www.securiteinfo.com/conseils/choix_ids.shtml

[13] https ://www.commentcamarche.net/contents/237-systemes-de-detection-d-intrusion-ids

[14] https ://www.researchgate.net/profile/PoulmanogoIlly/publication/335639245_Les_systemes_de_detection_d%27intrusion_IDS/links/5d7175fb4585151ee4a0c508/Les-systemes-de-detection-dintrusion-IDS.pdf

[15] https ://www.lemagit.fr/definition/HIDS-NIDS

Résumé

De nos jours, les réseaux informatiques sont de plus en plus exposés à des attaques et intrusions de par l'évolution des outils utilisés par les pirates modernes. C'est pourquoi il est dit qu'un réseau totalement sécurisé est simplement impossible à concevoir. Cependant, détecter et bloquer les tentatives d'intrusions reste un atout non négligeable dans le processus de sécurisation d'un réseau informatique. Cela est possible grâce notamment aux pare-feux et aux IDS. Le travail réalisé dans ce mémoire consiste à étudier les différents aspects relatifs aux réseaux et la sécurité informatique et les attaques menaçant le réseau, et aprésenter les différents outils de sécurité (firewalls, proxy, VPN ...), ensuite configurer un système de détection d'intrusions qui est en l'occurrence SNORT, qui a été associé au pare-feu PfSense, et mettre tout ça en œuvre au niveau de l'architecture réseau de CEVITAL Bejaia. SNORT s'est imposé comme le système de détection d'intrusions le plus performant et utilisé, il peut effectuer une analyse du trafic réseau en temps réel et détecter ainsi de nombreux types d'attaques.

Mots clés : Sécurité, Attaques, Intrusion, Snort, PfSense, Firewall, IDS, , CEVITAL.

Abstract

Today, computer networks are increasingly exposed to attacks and intrusions due to the evolution of tools used by modern hackers. This is why it is said that a completely secure network is simply impossible to design. However, detecting and blocking intrusion attempts remains a significant asset in the process of securing a computer network. This is possible thanks to firewalls and IDS. The work carried out in this brief consists in studying the various aspects related to networks and computer security and attacks threatening the network, presenting the various security tools (firewalls, proxy, VPN, etc.), then configure an intrusion detection system that is in this case SNORT, which has been associated with the PfSense firewall, and implement all this at the level of the CEVITAL Bejaia network architecture. SNORT has established itself as the most efficient and used intrusion detection system, it can perform real-time network traffic analysis and thus detect many types of attacks.

Keywords : Security, Attacks, Intrusion, Snort, PfSense, Firewall, IDS, CEVITAL.