République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Abderrahmane Mira
Faculté de la Technologie

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunication

Spécialité : Réseaux et Télécommunications

Thème

Mise en place d'un système de sécurité pour la détection et la prévention d'intrusion

Cas pratique « Groupe CEVITAL »

Préparé par :

- MEZIANI SARAH
- RAGUEM YASMINE

Dirigé par :

Mme GHERBI MERIEM

Mr N. BENOUARET

Examiné par :

Mme MAMMERI

Mme ZENADJI

Année universitaire : **2023/2024**

Dédicace

“

À mes précieux parents,

Je souhaite prendre ce moment pour vous exprimer ma profonde gratitude et mon amour sincère. Votre soutien inconditionnel a été la lumière qui a éclairé chacun de mes pas sur les chemins de la réussite. Chaque succès que j'ai eu jusqu'à présent est le fruit de vos sacrifices, de vos prières et de votre amour infini,

Ce mémoire est dédié à vous, car c'est grâce à votre amour, votre patience et votre dévouement que j'ai accompli cette étape importante dans ma vie académique. Je suis infiniment reconnaissante pour tout ce que vous avez fait et continuez de faire pour moi. Mes mots ne suffisent pas à exprimer la profondeur de mon amour pour vous,

Enfin, cette dédicace est également destinée à tous ceux qui m'ont entourée de leur amour et de leur soutien indéfectibles.

”

- Sarah

Dédicace

“

A mes chers parents

Je voulais prendre un moment pour vous exprimer toute ma gratitude et mon amour. Votre soutien inconditionnel a été la lumière qui a guidé chacun de mes pas sur les chemins de la réussite. Chaque succès que j'ai eu jusqu'à présent est le fruit de vous sacrifices et douaa et votre amour infini

Ce mémoire est dédié à vous, car c'est grâce à votre patience et votre dévouement que j'ai accompli cette étape importante dans ma vie académique. Je suis infiniment reconnaissante pour tout ce que vous avez fait et continuez de faire pour moi. Les mots ne suffisent pas à exprimer l'ampleur de mon amour pour vous,

Je dédie également ce travail A mes très chers frères (Ahmed et Youcef) et à mes chères sœurs(Siham et Lydia) , pour leurs amours et compréhension,

Enfin, cette dédicace s'adresse à tous ceux qui m'ont entouré de leur amour et de leur soutien indéfectibles.

”

- Yasmine

Remerciements

Avant tout, nous tenons particulièrement à exprimer nos remerciements au bon Dieu de nous avoir donné la force et la volonté pour mener à bien l'élaboration de ce projet.

Nos remerciements vont tout d'abord au corps professoral et administratif de département de technologie (ATE) de l'université **ABDERAHAMENE MIRA** de **BEJAIA** pour la richesse et la qualité de ses enseignements et qui déploie des grands efforts pour assurer à leurs étudiants une formation de qualité

On tient à remercier particulièrement madame **Gharbi Meriem** d'avoir accepté à nous encadrer ainsi pour sa grande disponibilité,sa patience et son encouragement. Son œil critique a été très précieux pour structurer le travail et pour améliorer la qualité des différentes sections .Ses orientations et son expertise ont été des éléments clés dans l'aboutissement de ce mémoire.

On souhaite faire part de nos sincères reconnaissances pour l'ensemble des ressources et du soutien que vous avez généreusement accordées durant notre stage. Un merci tout particulier à **Monsieur Benouaret** et **Monsieur Arab** pour leur engagement et l'excellence de leur accompagnement, qui ont grandement contribué à l'enrichissement de cette expérience professionnelle.

Que les membres de jury trouvent, ici, l'expression de nos sincères remerciements pour l'honneur qu'ils nous font en prenant le temps de lire et d'évaluer ce travail.

Enfin, nous adressons nos plus sincères remerciements à nos familles, tous nos proches et amis pour leur soutien indéfectible.On remercie sincèrement tous ceux qui ont contribué de prés et de loin à la réalisation de ce travail.

Table des matières

Table des figures

Liste des tableaux

Liste des acronymes

AAA	*Authentication, authorization, and accounting*
ACL	*Access Control List*
DHCP	*Dynamic Host Configuration Protocol*
DMZ	*Demilitarized Zone Network*
DNS	*Domain Name System*
DOS	*Denial of service*
FDDI	*Fiber Distributed Data Interface*
FTP	*File Transfer Protocol*
HTTP	*Hypertext Transfer Protocol*
IDS	*Intrusion Detection System*
IMAP	*nternet Messaging Access Protocol*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
NIDS	*Network Intrusion Detection System*
NIPS	*Network Intrusion Prevention System*
HIDS	*Host based Intrusion Detection System*
HIPS	*Host based Intrusion Prevention System*
OS	*operating system*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Path First*
P2P	*Peer To Peer*
POP	*point-of-presence*
RIP	*Routing Information Protocol*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SNORT	*Simple Network Intrusion Detection System*
STP	*Spanning Tree Protocol*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
VLAN	*virtual local area network*
VPN	*Virtual Private Network*
VTP	*Vlan Trunking Protocol*
WIPS	Wireless Intrusion Prevention System
Wi-Fi	*Wireless Fidelity*

Introduction générale

La sécurité des systèmes informatiques est devenue une préoccupation primordiale pour les entreprises. Avec l'augmentation exponentielle des connexions Internet et des échanges de données sensibles, les risques de cyber attaques et d'intrusions malveillantes se multiplient.

Les entreprises font face à de nombreux problèmes de sécurité informatique. Des mécanismes comme les pare-feu et les antivirus ont été mis en place pour prévenir les attaques, mais ils se sont avérés limités face à l'évolution rapide des techniques de piratage, Pour mieux se protéger, la mise en place de systèmes de détection et de prévention d'intrusion (IDS/IPS) est devenue nécessaire.

Le but de notre projet est de mettre en place un système de détection et de prévention d'intrusion (IDS/IPS) sous le pare-feu Pfsense. Ce système permettra de détecter et de bloquer les attaques malveillantes en surveillant le trafic réseau pour assurer une sécurité plus fiable.

Dans Le premier chapitre **généralités sur les réseaux informatique** nous avons étudié les déférentes généralité sur les réseaux informatiques.

Dans le deuxième chapitre, nous abordons la sécurité informatique les différentes attaques ainsi que les mécanismes de sécurité mis-en-place.

Le troisième chapitres est consacré pour l'**étude de l'existant** ce chapitres c'est une présentation de l'entreprises Cevital est les modèles des équipements utilisés. Ce sont des informations internes de l'entreprise.

Le quatrième chapitre **Les système de détection et de prévention d'intrusion** est consacrés à l'étude des systèmes de détection d'intrusion etle système de prévention d'intrusion, leur architecture méthodes, avantages et une comparaison entre IDS et IPS.

Le dernier chapitre **Conception et réalisation** consiste à la mise en place des deux systèmes de sécurité dans la première partie étude et analyse des besoins nous allons citer les pare-feu est les logiciels utilisé comme GNS3 et VMware linux est Windows ainsi que le pare-feu pfsense. Et dans la deuxième partie la Mise en œuvre de la configuration nous allons présenter leurs manipulations : installations, configurations (tests et résultats).

Chapitre 1

Généralités sur les réseaux informatiques

Introduction

Les réseaux représentent un ensemble inter-connecté d'éléments ou de dispositifs qui communiquent entre eux. Autrefois, les communications entre machines se limitaient essentiellement au transfert de données. Aujourd'hui, les réseaux ont évolué pour permettre le partage de diverses ressources, incluant non seulement des données informatiques, mais aussi des contenus multimédias tels que la voix et la vidéo.

Dans ce premier chapitre, nous explorons les fondamentaux théoriques des réseaux informatiques. Pour ce faire, nous commençons par discuter des différents types de réseaux informatiques, puis nous examinons en détail les différentes couches du modèle OSI. Enfin, nous abordons les protocoles de communication responsables du routage des données entre les réseaux, ainsi que les équipements essentiels impliqués dans ce processus.

1.1 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipements (finaux et intermédiaire) inter connectés qui permettent le partage des ressources et des informations entre différents utilisateurs à travers des moyens de transmission de données, tels que des câbles, des fibres optiques ou des liaisons sans fil et a travers des protocoles de communication afin de faciliter l'échange d'informations et de services.

1.2 Classification des réseaux informatiques

Les réseaux peuvent être dévissée en plusieurs types :selon leur étendue ,architecture et leur topologie :

1.2.1 Classification selon l'étendue géographique

Il existe quatre types de réseaux pour cette classification :

1.2.1.1 PAN(Personnal Area Network)

Un réseau personnel (PAN) est un réseau de proximité inter-connectant les outils de plusieurs poste de travail.

1.2.1.2 LAN(Local Area Network)

Un réseau local (LAN) est un réseau qui peut relier deux ordinateurs d'une maison ou plusieurs appareils au sein dune entreprise.Mais également des réseaux dans des institution publique comme les administrations,peut s'étendre de quelques mètres à quelques kilomètres [1].

1.2.1.3 MAN(Metropolitan Area Network)

le réseau (Man) est un réseau de communication a large bande qui relie plusieurs LAN.Ce réseau Couvre une zone géographique métropolitaine, telle qu'une ville par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local [1].

1.2.1.4 WAN(Wide Area Network)

Un réseau étendu (WAN) couvre des vaste zones géographique a l'échelle d'un pays ou de la planète entière.Les WAN utilisent souvent des technologies de télécommunication telles que des lignes louées, des fibres optiques et des satellites pour connecter des sites distants.

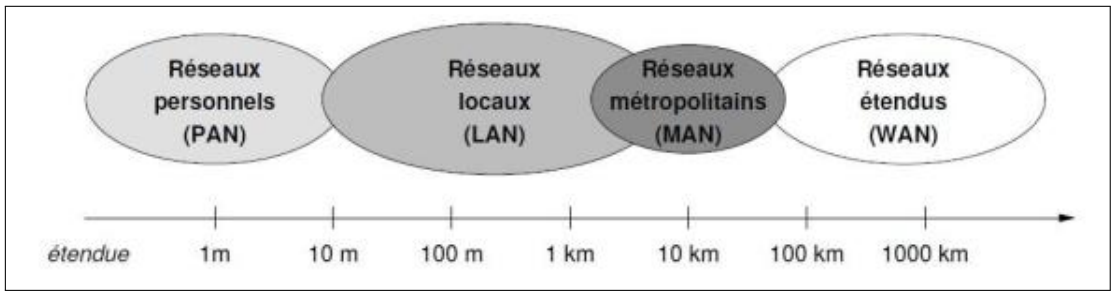

FIGURE 1.1 – Types des réseaux

1.2.2 Classification selon l'architecture des réseaux

On distingue généralement deux types de réseaux :

1.2.2.1 Réseau poste à poste (peer to peer)

Un réseau poste a poste fait référence à un modèle de communication et de partage de ressources où les participants d'un réseau ont des capacités égales et peuvent agir à la fois en tant que clients et en tant que serveurs. Les réseaux poste à poste sont souvent utilisés pour le partage de fichiers, la diffusion en continu de médias [2].

1.2.2.2 Réseau client / serveur

Le réseau client /serveur est un modèle de communication où les dispositifs ou les ordinateurs d'un réseau sont divisés en deux catégories principales : les clients et les serveurs. Dans ce modèle, les clients font des demandes auprès des serveurs, qui répondent en fournissant les services ou les ressources demandées. Ce modèle est couramment utilisé dans les environnements informatiques professionnels et d'entreprise.

Les avantages de réseau client/serveur

— C'est une architecture extensible et permet de déceler facilement les pannes, lorsque plusieurs ordinateurs présentent le même problème, c'est souvent le serveur qui est mis en cause.

— Sécurité renforcée :les serveurs peuvent mettre en oeuvre des politique de sécurité centralisées,telles que l'authentification des utilisateurs [2].

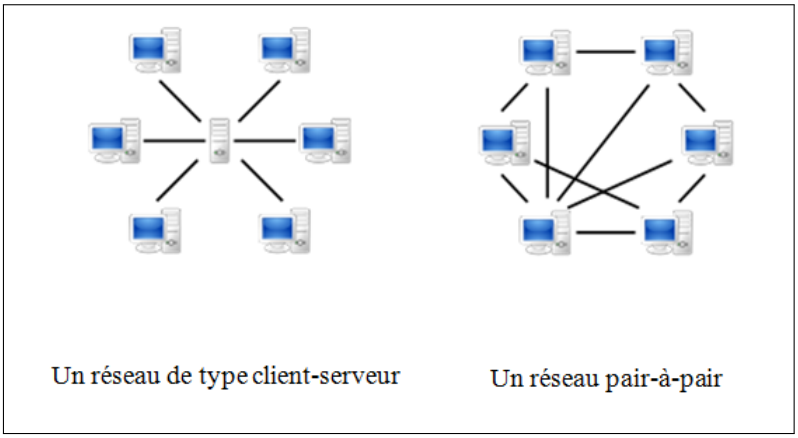

FIGURE 1.2 – Les architectures des réseaux

1.2.3 les Topologies des réseaux

Une topologie de réseau informatique définissant les liaisons entre les équipements du réseau et une hiérarchie éventuelle entre eux. On distingue deux types de topologie qui sont différentes à l'utilisation :

1.2.3.1 La Topologie logique

la topologie logique représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

1.2.3.2 La Topologie physique

La topologie physique indique comment les différentes stations sont raccordées physiquement (câblage) [3].
Cette topologie peut se partager en plusieurs groupes :

— **Topologie en bus**
La topologie en bus est l'organisation la plus simple d'un réseau tous les ordinateurs sont relies à une même ligne de transmission par l'intermédiaire de câble ou les données sont transmises sur un bus partage par plusieurs stations de travail.Lorsqu'une station émet des données, toutes les autres stations connectées au bus les reçoivent, mais seule la station destinataire copie le message. Ce type de topologie est utilisé dans des réseaux comme Ethernet.

— **Topologie en étoile**
La topologie en étoile est un arrangement physique dans lequel chaque périphérique du réseau est connecté à un concentrateur central. Les périphériques ne sont pas directement connectés les uns aux autres, mais ils communiquent via le Hub. Si un périphérique échoue, cela n'affecte pas le reste du réseau, à l'exception du périphérique défaillant.

— **Topologie en anneau**
La topologie d'anneau est un type de configuration de réseau où les périphériques sont connectés de manière circulaire, formant ainsi une boucle fermée.

— **Topologie en arbre**
Une topologie en arbre ou topologie arborescente ou hiérarchique peut être considérée comme une collection de réseaux en étoile disposés en hiérarchie. Ce réseau est divisé en niveaux. Le sommet, de haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur.

— **Topologie en maillé**
La topologie en maillé est une topologie de réseau qualifiant les réseaux (filaires ou non) dont tous les hôtes sont connectés pair à pair sans hiérarchie centrale, formant ainsi une structure en forme de filet.

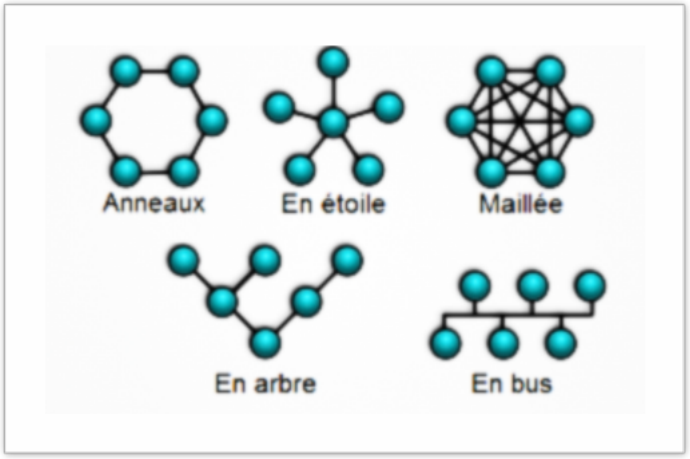

FIGURE 1.3 – Les Topologie des réseaux

1.3 les équipements d'interconnexion

1.3.1 Le commutateur(switch)

Un switch est un équipement réseau de couche deux du modèle OSI qui agissent au niveau de la couche de liaison des données,permet de connecter plusieurs appareils au sein d'un même réseau Ethernet. Le switch est chargé d'analyser les trames qui arrivent sur les ports d'entrée et les envoie uniquement à l'appareil auquel elles sont destinées, cela permet une communication plus rapide et plus efficace entre les appareil sur le réseau.

1.3.2 Le routeur

Un routeur est un équipement de couche trois du modèle OSI. un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, selon un ensemble de règles formant la table de routage.

1.3.3 Le concentrateur(Hub)

Un Hub est un élément matériel permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. Lorsqu'un paquet est reçu sur un port, celui-ci est envoyé aux autres ports afin que tous les segments du réseau local puissent accéder à tous les paquets. Le hub sert comme point de connexion commun pour les périphériques d'un réseau.

1.3.4 Le Pare-feu(firewall)

Un pare-feu est un appareil de sécurité de réseau informatique qui surveille et protège un réseau du trafic indésirable. Cette unité matérielle-logicielle dédiée fonctionne en bloquant ou en autorisant sélectivement les paquets de données. Il est généralement destiné à aider à prévenir les activités malveillantes et à empêcher quiconque, à l'intérieur comme à l'extérieur d'un réseau privé, de se livrer à des activités Web non autorisées [4].

1.3.5 Le pont(Bridge)

le pont est un équipement qui permet de raccorder différents segments d'un réseau local. Plus précisément, il stocke et transfert les paquets de données entrantes (les trames) aux multiples segments qu'il relie, après les avoir filtrés à l'aide de leurs adresses MAC. Le but du pont est surtout de diviser les grands réseaux en sections plus petites pour ensuite gérer le flux de données entre ces diverses parties [5]

1.3.6 Les répéteurs

Les répéteurs sont des équipements qui permettant d'étendre la distance de câblage d'un réseau local. Leur rôle consiste à amplifier et à répéter les signaux qui leurs parviennent.

1.4 Les supports de transmission

Les supports de transmission permettent d'interconnecter les périphériques composants le réseau. il existe deux types de transmission qui permet de faire circuler les données. Certain des supports les plus couramment utilisé sont :

1.4.1 Câbles réseaux

Les câbles de réseau, également appelés câbles Ethernet sont des câbles utilisés pour connecter différents périphériques réseau entre eux afin de permettre la transmission de données. Ces câbles sont utilisés dans les réseaux locaux (LAN), les réseaux étendus (WAN) et d'autres types de réseaux .

1.4.1.1 Câbles en cuivre

Les câble en cuivre transporte des signaux électriques. Il en existe de deux types : le câble coaxial et la paire torsadée.

1.4.1.2 Le câble coaxial

Le câble coaxial offre la meilleure bande passante, est moins sensible aux perturbations et peu couvrir une plus grande distance que la paire torsadée.

1.4.1.3 Le câble a paire torsadée

Le câble à paire torsadée peut transporter des signaux numérique et analogique.Il a un très faible diamètre. C'est ce qui favorise les nombreuses perturbations et l'affaiblissement très important des signaux. Du coup, son usage est limité sur des courtes distances.

1.4.1.4 Câble en fibre optique

La fibre optique est un type de câble utilisé pour transmettre des informations à grande vitesse sur de longues distances. Contrairement aux câbles traditionnels en cuivre, qui utilisent des signaux électriques, la fibre optique utilise la lumière pour transporter les données [6].
Il existe deux types de câble en fibre optique : monomode et multimode :

- **Fibre Monomode :** Les fibres monomodes ont un cœur optique de faible diamètre et sont les plus complexes à réaliser, mais offrent une très grande bande passante (10 GHz/km) et les meilleurs débits.
- **Fibre Multimode :** La fibre multimode a un cœur de grand diamètre par rapport à la fibre monomode. Elle permet le passage de plusieurs longueurs d'ondes lumineuses.

1.4.2 Supports sans fils

les réseaux sans fil, telle que le wifi, utilise des ondes radio pour transmettre les données, ils offrent une grandes flexibilité et permettre la connectivité sans avoir besoin des câbles physique. On distingue plusieurs types comme infrarouge , onde radio .

1.5 Les modèles de communications

Il existe de deux types de modèles communication OSI et TCP/IP :

1.5.1 Modèle OSI (Open System Interconnection)

Ce modèle définit une architecture de référence permettant la communication entre différents systèmes hétérogènes et d'assurer la compatibilité entre une variété d'appareils et de technologies. Les tâches à effectuer sont structurées en sept niveaux appelés couches[7].

Couche	Fonction
7-Application	Fournit une interface pour les logiciels applicatifs afin d'accéder au réseau et d'échanger des données de manière significative pour l'utilisateur final.
6-Présentation	S'occupe de la traduction, de la compression et du chiffrement des données pour garantir une communication compréhensible entre les applications.
5-Session	Établit, maintient et termine les sessions de communication entre les applications, permettant la synchronisation et la gestion des dialogues.
4-Transport	S'occupe de la transmission des données de manière fiable et efficace entre les appareils finaux.
3-Réseau	Responsable du routage des données à travers différents réseaux pour atteindre la destination souhaitée.
2-Liaison de données	Elle gère la transmission fiable des données à travers un réseau physique et assure l'intégrité des données et la correction des erreurs.
1-Physique	Cette couche concerne les aspects physiques de la communication, comme les câbles et les signaux électriques.

TABLE 1.1 – Les différentes couches utiliser dans le modèle OSI

1.5.2 Modèle TCP/IP

est un ensemble de protocoles de communication qui se compose de quatre couches principales : [7]

Couche	Fonction
4-Application	Cette couche est la plus haute du modèle TCP/IP et gère les applications nécessitant une communication réseau, telles que les clients de messagerie ou les sites internet. Les protocoles courants incluent HTTP, SMTP, FTP, etc.
3-Transport	Similaire à la couche transport du modèle OSI, cette couche fragmente et reconstitue les données pour les transmettre entre la couche application et la couche Internet. Les protocoles TCP et UDP sont utilisés à ce niveau.
2-Internet	Équivalente à la couche réseau du modèle OSI, cette couche joue un rôle crucial dans l'acheminement des données à travers différents réseaux. Le protocole IP (IPv4, IPv6) est central à cette couche.
1-Accès Réseau	Cette couche combine la liaison de données et la couche physique du modèle OSI. Elle gère la transmission physique des données sur le réseau, incluant les aspects matériels comme les câbles et les cartes réseau.

TABLE 1.2 – Les différentes couches utilisées dans le modèle TCP/IP

— Grâce à TCP/IP, chaque application peut transmettre et échanger des données sur n'importe quel réseau, quel que soit l'emplacement du destinataire.Le protocole IP garantit que les paquets de données atteignent leur destination, tandis que le TCP contrôle le transfert de données et assure la connectivité entre les flux de données et les applications. La principale différence entre TCP/IP et OSI est le nombre de couches, dont certaines sont fusionnées.

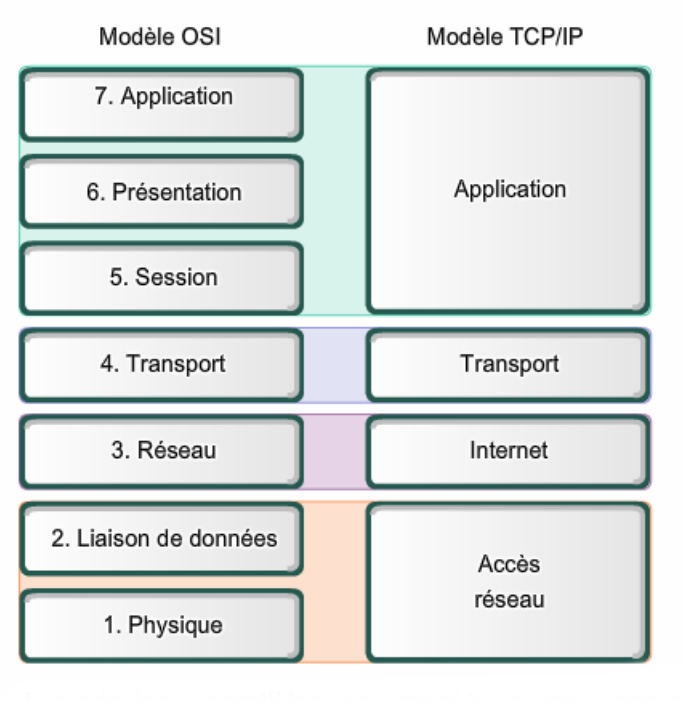

FIGURE 1.4 – Le modèle OSI et le modèle TCP/IP

1.6 Les protocoles réseaux

un protocole réseau est un ensemble de règles et de procédures de communication utilisées d'une part et d'autre par toutes les stations qui échangent des données sur le réseau

Il existe de nombreux protocoles réseaux, mais ils n'ont pas tous, ni le même rôle, ni la même façon de procéder. Certains protocoles réseaux fonctionnent au niveau de plusieurs couches du modèle OSI, d'autres peuvent être spécialisés dans la réalisation d'une tâche correspondant à une seule couche du modèle OSI.

1.6.1 Protocole TCP(Transmission Control Protocol)

Le protocole TCP est un protocole de couche 4 de modelé OSI est un protocole fiable orienté connexion de bout en bout pour assurer la transmission des données. Certaines des principales fonctionnalités de TCP sont la détection d'erreur, le démarrage lent, le contrôle de flux et le contrôle de congestion. TCP est un mécanisme de transport fiable.

1.6.2 Protocole UDP(User Datagram Protocol)

UDP est un protocole de communication sans connexion utilisé pour le transport de paquets sur les réseaux et principalement utilisé pour établir des connexions à faible latence et à tolérance de perte entre les applications sur l'internet.

La différence entre TCP et UDP :

- TCP est un protocole orienté connexion et offre une transmission fiable des données.
- UDP est un protocole sans connexion et non fiable.
- TCP a un overhead plus élevé en raison de ses fonctionnalités de contrôle de flux.
- UDP a un overhead plus faible car il n'inclut pas de mécanismes de contrôle de flux ou de congestion [8]

1.6.3 Protocole DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP permet d'attribuer et de configurer automatiquement les adresses IP ,les masques de sous-réseau et les passerelles par défaut des appareils sur un réseaux

1.6.4 Protocole DNS (Domain Name System)

C'est un protocole qui permet aux utilisateurs d'accéder aux ressources réseau en utilisant des noms de domaine conviviaux plutôt que des adresses IP numériques difficiles à mémoriser. Il facilite également la flexibilité en permettant aux administrateurs réseau de déplacer des services entre des adresses IP sans perturber les utilisateurs .

1.6.5 Protocole FTP(File Transfer Protocol)

Le protocole de transfert de fichiers ,permet de partager des fichiers entre des hôtes locaux et distants et fonctionne sur TCP. Pour les transferts de fichiers, FTP crée deux connexions TCP : une connexion de contrôle et une connexion de données. Les connexions de contrôle sont utilisées pour transférer des informations de contrôle, telles que des mots de passe, des commandes pour récupérer et stocker des fichiers, etc., et les connexions de données sont utilisées pour transférer des fichiers réels [9].

1.6.6 Protocole ARP(Adresse Résolution Protocol)

est un protocole utilisé pour associer une adresse IP à une adresse MAC sur un réseau informatique. Plus précisément, il permet de faire le lien entre une adresse IP d'une carte réseau et une adresse matérielle. Il fonction entre la couche réseau (couche 3 du modèle OSI) et la couche de liaison (couche 2 du modèle OSI).

1.6.7 protocole RIP(Routing Information Protocol)

Le protocoles RIP permet aux routeurs de partager des information sur les réseaux auxquels ils sont connectés.Le protocoles RIP utilise une approche de routage à vecteur de distances, ou les routeurs échangent périodiquement des mise à jour de routage pour maintenir une table de routage a jour. Cela permet aux routeurs de prendre des décisions de routage et déterminer les meilleure chemins pour acheminer les paquets de données.

1.6.8 Protocole ICMP(Internet Control Message Protocol)

Le protocole ICMP Permet d'informer d'une erreur réseau (message d'erreur)ou de formuler une demande d'état a un système.Les messages ICMP sont capsulés dans un datagramme IP.Le protocole ICMP ne fiabilise pas IP .c'est un protocole d'information.

1.6.9 Protocole SNMP(Simple Network Management Protocol)

Le protocole SNMP est un protocole de couche application utilisé pour surveiller et gérer les périphériques réseau connectés via une adresse IP.

1.6.10 Protocole SMTP(Simple Mail Transfer Protocol)

Le protocole(SMTP) est un protocole de communication utilisé pour envoyer et recevoir des messages électroniques sur Internet. Il est généralement utilisé avec POP3 ou Internet Message Access Protocol pour enregistrer les messages dans une boîte aux lettres du serveur et les télécharger périodiquement à partir du serveur pour l'utilisateur.Il agis au niveau de la couche application.

1.6.11 Protocoles 802.3 et 802.11

Les protocoles 802.3 et 802.11 sont des normes définies par l'Institute of Electrical and Electronics Engineers (IEEE) pour les réseaux locaux.

Le protocole 802.3 est une norme pour les réseaux Ethernet câblés qui définit les spécifications pour la transmission de données sur des réseaux a haute débit a l'aide de câbles physique. D'autre part , le protocole 802.11 est une norme de réseau sans fil qui définit les spécifications pour la transmission de données sur des réseaux à l'aide d'onde radio.

1.7 Les réseaux Locaux Virtuel

1.7.1 Définition d'un VLAN

Un Vlan est un réseau local permet de regrouper un ensemble de stations de travail de façon logique et non physique, les Vlans sont distribué sur des équipements de niveau 2 du modèle OSI (couche liaison). Plusieurs VLAN peuvent être définit sur un même commutateur,

cependant ce dernier peut avoir plusieurs domaines de diffusion, ce qui veut dire qu'un broadcast envoyé par une machine d'un vlan sera diffusé uniquement vers toutes les autres machines du même Vlan.

1.7.2 Avantages des VLANS

Si la technologie des VLANs est très répondue de nos jours, c'est bien pour de nombreux avantages. Les principaux avantages sont :.

-Sécurité : les terminaux qui se trouvent dans un certain VLAN sont séparés du trafic de données des autres VLANs du réseau, ce qui permet de protéger les données sensibles ou a grande importances et d'éviter les risques de violation de confidentialité.

-Réduction du coût : des économies sont réalisées grâce à une diminution des mises à niveau du réseau en éliminant le besoin d'équipements réseau coûteux supplémentaires.

-Meilleures performances : la diffusion du réseau peut être gérée et contrôlée en créant de nombreux VLAN, ce qui augmente invariablement le nombre de domaines de diffusion tout en diminuant leur taille.

-Flexibilité : l'ajout, le déplacement et la modification du réseau est facilement réalisé en configurant simplement un port approprié le VLAN et en affectant les hôtes au même VLAN.

-Dépannage facile : En regroupant les utilisateurs de notre réseau et des ressources dans différents VLAN, des problèmes émanant dans le réseau peut être facilement identifié et corrigé par simple groupe de traçage auquel ces hôtes appartiennent.

1.7.3 Protocole VTP(Vlan Trunking Protocol)

Le VTP est un protocole utilisé pour configurer et distribuer automatiquement les informations de VLAN sur un réseau de commutateurs, simplifiant ainsi la gestion des vlan en permettant une configuration centralisée.

1.7.4 Protocole STP (Spanning Tree Protocol)

STP est un protocole de gestion de liens conçu pour empêcher les boucles de commutation dans les réseaux Ethernet en désactivant les liens redondants, assurant ainsi une topologie sans boucle et une meilleure faiblit du réseau.

1.8 L'adressage IP(internet protocol)

Chaque ordinateur dans un réseau possède une adresse unique sur 32 bits. Plus précisément, chaque interface dispose d'une adresse IP particulière À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le cheminement (ou le routage) des paquets entre les différents réseaux. Ces groupes ont été baptisés classes d'adresses IP. Classes (A, B, C, D ou E) selon la valeur de son premier octet.

1.8.1 Définition d'une adresse IPv4

Une adresse IPv4 est une adresse IP dans la version 4 du protocole IP (IPv4). Cette adresse permet d'identifier chaque machine connectée sur un réseau informatique utilisant le protocole IP version 4.

Cette adresse est composée de quatre octets, chacun ayant leur valeur décimale comprise entre 0 et 255, séparés par des points. Exp : 212.85.150.133.

1.8.2 Les masques de sous-réseaux

Le masque de sous-réseau est un outil fondamental pour la gestion et la configuration des réseaux IP et définir les limites des sous-réseaux et optimiser l'utilisation des ressources réseau. Il permet de contrôler le flux de données, de segmenter les réseaux pour des raisons de sécurité ou de performances, et de permettre une gestion efficace de l'adressage IP.

Classe	Adresse	Masque
Classe A	0.0.0.0 à 127.255.255.255	255.0.0.0
Classe B	128.0.0.0 à 191.255.255.255	255.255.0.0
Classe C	192.0.0.0 à 223.255.255.255	255.255.255.0
Classe D(multicast)	224.0.0.0 à 239.255.255.255	255.255.255.255
Classe E(réservée)	240.0.0.0 à 255.255.255.255	255.255.255.255

TABLE 1.3 – Les adresses IP

— Un sous-réseau est une subdivision d'un réseau IP plus grand en parties plus petites et distinctes. Cette subdivision permet de mieux organiser et gérer les adresses IP au sein du réseau, ainsi que de contrôler le trafic et améliorer la sécurité.

1.8.3 Le routage IP

Le routage IP fait référence à la manière dont les paquets de données IP sont acheminés de leur source à leur destination à travers un réseau. Cela implique l'utilisation de routeurs pour diriger les paquets vers le bon réseau en se basant sur des tables de routage en peut distinguer deux types de routage, routage statique routage dynamique.

1.8.3.1 Routage statique :

Le routage statique est une méthode de configuration des tables de routage dans un réseau informatique où les chemins de transfert des données entre les réseaux sont configurés manuellement par un administrateur réseau.

1.8.3.2 Routage dynamique :

Le routage dynamique utilise des algorithmes et des protocoles pour calculer et mettre à jour les routes automatiquement . il existe de types de routage dynamique :

le routage a état des lien : est utilisé par des protocoles tel que OSPF

le routage a vecteur de distances : est utilisé par des protocoles tels que RIP.

Conclusion

Dans ce chapitre,nous avons présenté les principes de bases des réseaux informatiques (architectures, types, topologies...), aussi nous avons cité les modèles générale de communication (OSI, TCP/IP) en détails. Puis nous avons défini les différents protocoles existants dans un réseau informatique.
Pour compléter les informations, nous avons présenté les éléments du réseau qui servent au transfert d'informations (Switch, hub, routeur,...).

Le développement de ce dernier a posé des conflits majeurs aux utilisateurs qui restent confrontés à une augmentation et à une complexité croissante d'intrusions et attaques informatiques dans leurs réseaux. Cependant, dans le chapitre 2, nous allons étudier les différentes attaques et les moyens misent à la disposition pour sécuriser les données informatiques.

Chapitre 2

Généralités sur la sécurité informatique

Introduction

L'évolution fulgurante des réseaux informatiques et d'internet dans ces dernières années a modifié le paysage économique ainsi que les différents modes de communication et d'échanges. Attirée par une flexibilité de services et de nouvelles niches économiques, la majorité des organismes privés et gouvernementaux utilisent les ressources d'Internet aussi bien pour interconnecter des sites distants que pour proposer des services en ligne.

Ce chapitre, va présenter les définitions nécessaires pour comprendre ce qui est une sécurité informatique et quels sont ses objectifs et ses domaines, il va entamer les politiques de sécurité,. Puis il aborde la notion de gestion des risques ainsi présente les différentes attaques de sécurité.

2.1 Sécurité informatique

2.1.1 Définition

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains pour protéger l'intégrité et la confidentialité des informations stockées dans un système informatique. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles Caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la Sécurité.

2.1.2 Objectif de la sécurité informatique

La sécurité de l'information s'articule autour de trois principes clés : la confidentialité,l'intégrité et la disponibilité :

- **Disponibilité** : exiger que les informations sur le système soient disponibles pour le personnel autorisé.
- **Confidentialité** : exiger que les informations soient lues que par le personnel autorisé.
- **Intégrité** : Empêcher la modification des informations par des utilisateurs non autorisés Empêcher la modification non autorisée ou involontaire des informations par des utilisateurs autorisés.

2.2 La politique de sécurité

Une politique de sécurité définit un certain nombre de règles, de procédures et une bonne pratique permettant d'assurer un niveau de sécurité conforme au besoin de l'organisation. Elle définit l'intégralité de la stratégie de sécurité informatique de l'entreprise.
Elle permit de maximiser cette dernière afin de mettre à disposition des équipes concernées les moyens nécessaires pour contrer les principaux risques auxquels elles sont confrontées.

La politique de sécurité permit de transcrire le travail effectué pour comprendre le risque et leur impact en des mesures opérationnelles de sécurité. Sa spécification facilite le choix et la mise en œuvre des mesures de sécurité Elle donne de la cohérence à la gestion et contribue à adopter, vis-à-vis des risques, une attitude pro-active et réactive [10].

2.3 Les types de politique de sécurité

Il existe plusieurs types de politique de sécurité :

2.3.1 La sécurité du réseau

Les sécurités du réseau sont utilisées pour éviter que des utilisateurs malveillants entrent dans vos réseaux. Cela permit de garantir la disponibilité, la fiabilité et l'intégrité du réseau. Ces types de la sécurité sont nécessaires pour empêcher les pirates d'accéder aux données de réseau.

2.3.2 La sécurité de point d'extrémité et sécurité en nuage

La sécurité des points d'extrémité ou la protection des points d'extrémité est le processus qui consiste à défendre les points d'extrémité, les appareils qui se connectent à un réseau, comme les ordinateurs portables et les Smartphones, contre les attaques. La sécurité des points de terminaison peut également consister à bloquer le comportement dangereux de l'utilisateur qui pourrait compromettre le dispositif de point de terminaison ou l'infecter avec un logiciel malveillant. La sécurité en nuage protège les utilisateurs contre les menaces, peu importe d'où ils accèdent à Internet, et elle sécurise les données et les applications dans le nuage. La sécurité en nuage peut également aider à Bloquer les menaces plus rapidement.et Permettre de mieux protéger le nuage.

2.3.3 La sécurité des applications

Avec la sécurité des applications, les applications sont particulièrement codées lors de l'ouvrage pour être aussi protégées afin qu'elle ne soit pas fragiles aux effractions.

2.4 Les menaces informatiques

La menace est toute couse potentielle d'incident. Tout ordinateur connecter à un réseau est potentiellement vulnérable à une attaque. Elles désignent l'exploitation d'une faiblesse de sécurité par un attaquant, que ce soit interne ou externe a l'entreprise.

2.4.1 Les types de menaces

il existe deux types de menaces :

2.4.1.1 Menaces accidentelles

Ce sont des risques provoqués par des erreurs ou des mauvaises pratiques involontaires des utilisateurs, ces menaces peuvent inclure des actions telle que des erreurs de manipulation, des suppressions involontaires des données.

2.4.1.2 Menaces intentionnelles

Les menaces intentionnelles en sécurité informatique font référence aux attaques planifiées et exécutées par des individus ou des groupes dans le but de compromettre des systèmes informatiques, voler des données sensibles. les cybercriminels utilisent ces méthodes intentionnelles pour exploiter les vulnérabilités des systèmes et des utilisateurs, mettant en péril la sécurité informatiques des données.

2.5 Attaque informatique

L'attaque informatique est toute tentative d'accès non autorisé à un ordinateur, un système informatique ou un réseau informatique dans le but de causer des dommages. Les attaques informatiques visent à désactiver, perturber, détruire ou contrôler des systèmes informatiques ou à modifier, bloquer, supprimer, manipuler ou voler les données contenues dans ces systèmes.

2.5.1 Les types d'attaques informatiques

2.5.1.1 Les attaques directes

c'est la plus simple des attaques. Le hacker attaque directement sa victime a partir son ordinateur [11].

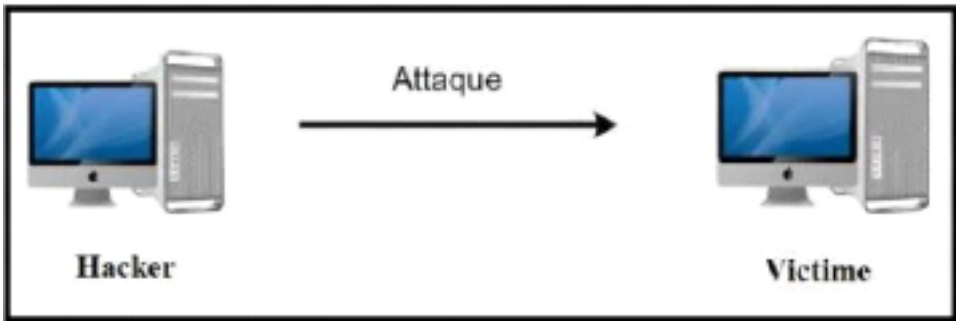

FIGURE 2.1 – Attaque directe

2.5.1.2 Les attaques indirectes par rebond

cette attaque est très prisée des hacker En effet, le rebond a deux avantages :

— Masquer l'identité (l'adresse IP) du hacker
— Éventuellement, utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante...) pour attaquer.

Le principe en lui-même, est simple : Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime [11].

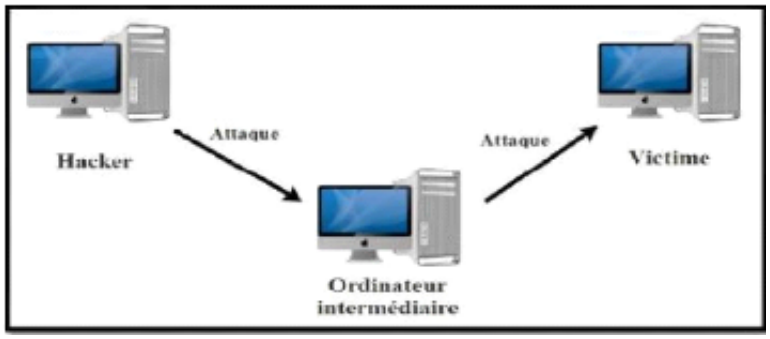

FIGURE 2.2 – Attaque indirecte par rebond

2.5.1.3 Les attaques indirectes par réponse

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinatrice victime [11].

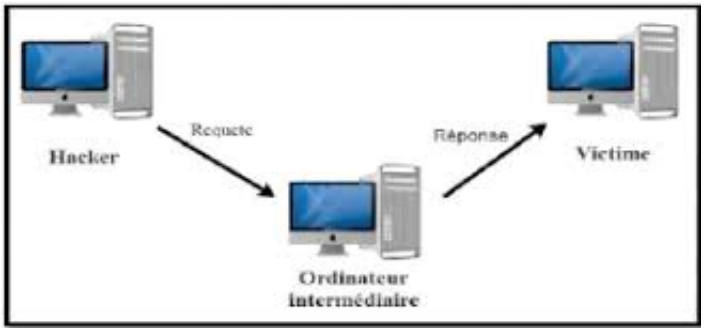

FIGURE 2.3 – Attaque indirecte par réponse

2.5.2 Les technique d'attaques

Les attaques sont regroupées en deux catégories :

2.5.2.1 Attaque des réseaux

Ce type d'attaque se base principalement sur des failles liées aux protocoles ou à leur implémentation.

— **IP spoofing**

L'usurpation d'adresse IP est une attaque qui consiste à falsifier les adresses IP sources afin de masquer l'identité de l'appareil de l'attaquant. Les pirates peuvent utiliser cette astuce pour cacher leur identité et commettre des crimes tels que le

phishing, la distribution de logiciels malveillants, le spam, etc. Ils peuvent également utiliser cette méthode pour accéder à des sites Web restreints et voler des informations sensibles.

— **Attaques DNS**

Le DNS Spoofing (Domain Name Service Spoofing) ou usurpation de DNS consiste à injecter de fausses données DNS dans le cache d'un résolveur DNS, ce qui provoque le renvoi par ce dernier d'une adresse IP incorrecte pour un domaine pour rediriger un utilisateur ciblé vers un site Web malveillant contrôlé par l'attaquant.

— **Attaques DHCP**

Il s'agit d'une attaque par déni de service (DoS) sur les serveurs DHCP où l'attaquant diffuse des demandes DHCP falsifiées et tente de louer toutes les adresses DHCP disponibles dans la portée DHCP.

En conséquence, l'utilisateur légitime n'est pas en mesure d'obtenir ou de renouveler une adresse IP demandée via DHCP, ce qui fait échouer l'accès au réseau.

— **Attaque ARP**

Attaque ARP (Address Resolution Protocol) est un type d'attaque dans le quel un acteur malveillant envoie des messages ARP falsifiés sur un réseau local. Un développeur malveillant pourrait exposer des vulnérabilités et s'infiltrer sur votre réseau à votre insu dans l'espoir d'accéder à des données importantes.

— **Attaque VLAN**

Une attaque VLAN est une tentative malveillante visant à compromettre ou à exploiter les réseaux virtuels configurés au sein d'un réseau local.

2.5.2.2 Principales attaques des périphériques finaux

Virus

Un virus informatique est une application malveillante ou un logiciel utilisé pour exercer une activité destructrice sur un appareil ou un réseau local.

L'activité malveillante du code peut endommager le système de fichiers local, voler des données, interrompre des services, télécharger des logiciels malveillants supplémentaires ou toute autre action codée dans le programme par l'auteur du logiciel malveillant.

De nombreux virus se font passer pour des programmes légitimes afin d'inciter les utilisateurs à les exécuter sur leur appareil, délivrant ainsi la charge utile du virus informatique [12].

Ver

Un ver informatique est un logiciel malveillant qui se propage sur un réseau pour infecter un maximum de systèmes. Il permet d'espionner l'activité d'un poste, de détruire ou de corrompre des données, d'ouvrir une porte dérobée aux hackers. Le ver est également employé pour réaliser une attaque par déni de service. C'est-à-dire qu'il sature un réseau ou un site Web ciblé afin pour le rendre inaccessible [13]

Déni de service

Le déni de service (ou DoS : Denial of Service) est une attaque qui vise à rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs. Les serveurs de messagerie peuvent être victimes de ces attaques,et se réfère à une attaque qui émane d'une seule source. .
Une attaque DOS fonctionne en submergeant un serveur ou un réseau avec un trafic illégitime, de sorte que les demandes légitimes ne puissent pas être traitées. Cela peut être accompli en utilisant une multitude de techniques, telles que l'envoi de paquets inutiles, la surcharge du réseau ou l'exploitation de vulnérabilités dans le logiciel [14].

Sniffer

Le sniffing est une technique qui consiste à analyser le trafic réseau, pour récolter illégalement des informations secrètes ils peuvent être exploités de manière malveillante par des pirates informatiques pour espionner le trafic, intercepter des données sensibles telles que des mots de passe, et mener des attaques [15]

Intrusion

Accès non autorisé à un système informatique ou à un réseau, obtenu en contournant ou en désamorçant les dispositifs de sécurité en place.

Cheval de Troie

Un cheval de Troie est un type de programme malveillant se faisant passer bien souvent pour un logiciel authentique. Les chevaux de Troie peuvent être utilisés par des cybercriminels et des pirates informatiques pour accéder aux systèmes des utilisateurs. Une fois activés, les chevaux de Troie peuvent permettre aux cybercriminels de vous espionner, de dérober vos données sensibles et d'accéder à votre système à l'aide d'un backdoor [16]

2.6 Les dispositifs de protections

2.6.1 Antivirus

Un logiciel de sécurité comprenant plusieurs couches de protection qui permettent de détecter, bloquer et supprimer des virus. Il utilise pour cela de nombreuses techniques, parmi

lesquelles : - Le contrôle général du système de l'ordinateur - La surveillance des lecteurs de supports amovibles

2.6.2 Les mécanismes de chiffrement

IL existe plusieurs types des mécanisme de chiffrement

2.6.2.1 Le chiffrement symétrique

Chiffrement à clé secrète, utilise une seule clé pour chiffrer et déchiffrer les données. Vous devez partager cette clé avec le destinataire. Disons que vous voulez dire "Je t'aime maman", que vous écriviez votre e-mail, puis que vous fixiez une clé secrète pour le chiffrer. Lorsque votre maman recevra le message, elle devra entrer la clé secrète pour déchiffrer l'email [17].

2.6.2.2 Le chiffrement asymétrique

Le chiffrement asymétrique a pour principale caractéristique de nécessiter deux clés pour le décodage d'un fichier (par exemple), au lieu d'une seule habituellement. Deuxièmement, une clé privée utilisée pour déchiffrer les données [17].

2.7 Contrôles d'accès

Le contrôle d'accès est un ensemble de règles de la sécurité qui détermine qui est autorisé à accéder à certaines données, applications et ressources, et dans quelles circonstances.

2.7.1 Le contrôle d'accès physique

le contrôle d'accès physique se réfère aux méthodes et technologies utilisées pour réguler et restreindre l'accès aux infrastructures physiques . L'objectif est de garantir que seules les personnes autorisées peuvent entrer dans un espace donné.
Ce contrôle peut être mis en œuvre de différentes manières, en utilisant diverses technologies et méthodes, telles que :

2.7.1.1 Lecteurs de badges et Carte d'accès

Un lecteur de badge est un appareil qui lit et scanne les badges ou cartes d'accès de votre entreprise, pour ainsi, permettre de gérer les flux entrants et sortants au sein de vos locaux.

2.7.1.2 Systèmes de reconnaissance biométrique

Les systèmes de contrôle biométrique utilisent des caractéristiques physiques uniques des individus, telles que les empreintes digitales, la reconnaissance faciale, la reconnaissance de l'iris ou la reconnaissance de la voix, pour vérifier leur identité et leur accorder l'accès aux zones autorisées.

2.7.1.3 Systèmes de vidéosurveillance

Les caméras de surveillance sont utilisées pour surveiller et enregistrer les activités dans les zones sensibles de l'entreprise,surveiller les points d'entrée et de sortie, ainsi que les zones sensibles, permettant une vérification visuelle de l'identité des personnes et facilitant la détection des intrusions.

2.7.1.4 Systèmes de verrouillage et de protection

Il s'agit de l'utilisation de portes verrouillées, de portes blindées et d'autres dispositifs physiques pour empêcher l'accès non autorisé aux zones sensibles.

2.7.1.5 Systèmes d'alarme

Des systèmes d'alarme peuvent être intégrés au contrôle d'accès pour détecter et signaler toute tentative d'accès non autorisé.

2.7.2 Le contrôle d'accès logique

le contrôle d'accès logique est axé sur la gestion des autorisations et des permissions numériques.réfère aux méthodes et aux systèmes utilisés pour réguler l'accès aux données, aux systèmes informatiques et aux applications. les organisations peuvent sécuriser leurs données, protéger leurs systèmes informatiques contre les accès non autorisés, et garantir la confidentialité, l'intégrité et la disponibilité de leurs informations numériques.

2.8 Le contrôle d'accès administratif (Protocole AAA)

Le contrôle d'accès administratif est un cadre de sécurité qui contrôle l'accès aux ressources informatiques, applique des politiques et audite l'utilisation. L'AAA et ses processus combinés jouent un rôle majeur dans la gestion et la cybersécurité du réseau en sélectionnant les utilisateurs et en assurant le suivi de leur activité pendant qu'ils sont connectés.

2.8.1 L'authentification

L'authentification permettant de vérifier les identités présumée des utilisateurs. Lorsqu'il existe une seule preuve de l'identité (mot de passe par exemple) on parle d'authentification simple. Lorsque l'authentification nécessite plusieurs facteurs, on parle alors d'authentification forte.

2.8.2 L'autorisation

Attribue des droits différenciés pour autoriser les utilisateurs à utiliser des services spécifiques.

2.8.3 Comptabilité

il s'agit des informations récoltées pendant toute la durée de la session, après identification de l'utilisateur.

2.9 Les listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées au trafic circulant via une interface de routeur.Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions précises. Les ACL permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.

Les listes d'accès filtrent le trafic réseau en commandant aux interfaces d'un routeur d'acheminer ou de bloquer des paquets routés. Le routeur examine chaque paquet afin de déterminer s'il doit l'acheminer ou le rejeter en fonction des conditions précisées dans la liste de contrôle d'accès. Certaines conditions dans une ACL sont des adresses source et de destination, des protocoles et des numéros de port de couche supérieure.

2.9.1 Listes de contrôle d'accès standard

Les listes d'accès standard vérifient l'adresse d'origine des paquets IP qui sont routés. Selon le résultat de la comparaison, l'acheminement est autorisé ou refusé pour un ensemble de protocoles complet en fonction des adresses réseau, de sous-réseau et d'hôte.

2.9.2 Listes de contrôle d'accès étendues

Les listes d'accès étendues sont utilisées plus souvent que les listes d'accès standard car elles fournissent une plus grande gamme de contrôle. Les listes d'accès étendues vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port. Cela donne une plus grande souplesse pour décrire ce que vérifie la liste de contrôle d'accès. L'accès d'un paquet peut être autorisé ou refusé selon son emplacement d'origine et sa destination, mais aussi selon son type de protocole et les adresses de ses ports. Une liste de contrôle d'accès étendue peut autoriser le trafic de messagerie issu de l'interface Fa0/0 vers des destinations S0/0 données tout en refusant des transferts de fichiers et des navigations sur le Web. Lorsque des paquets sont éliminés, certains protocoles envoient un paquet d'écho à l'émetteur, pour lui indiquer que la destination était inaccessible.

2.10 Pare-feu

Un pare-feu(firewall) est une structure située entre l'utilisateur et le monde extérieur afin de protéger le réseau interne des intrus. Dans la plupart des cas, les intrus proviennent du réseau global Internet et des milliers de réseaux distants qu'il interconnecte. Un pare-feu réseau

est constitué de plusieurs machines différentes qui travaillent ensemble pour empêcher l'accès indésirable et non autorisé.

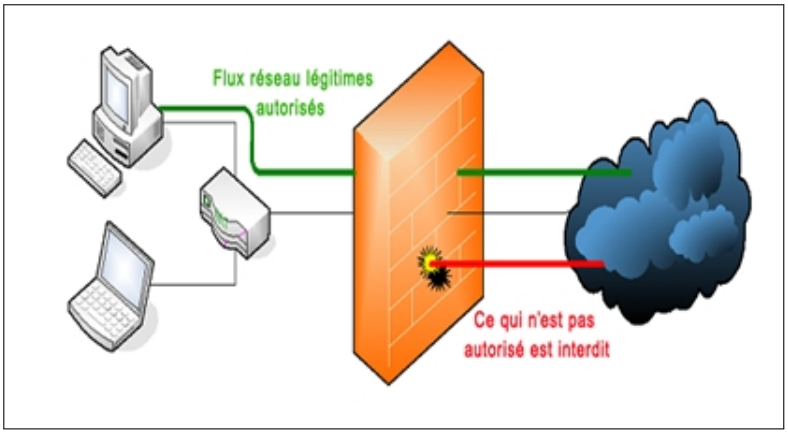

FIGURE 2.4 – Parfeu(Firewall)

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

— D'autoriser la connexion (allow) ;
— De bloquer la connexion (deny) ;
— De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité.

2.11 DMZ

Une DMZ ou zone démilitarisée est un réseau périmétrique qui protège et ajoute une couche de sécurité supplémentaire au réseau local interne d'une organisation contre le trafic non fiable. L'objectif final d'un réseau de zone démilitarisé est de permettre à une organisation d'accéder à des réseaux non fiables, tels qu'Internet, tout en s'assurant que son réseau privé ou son LAN reste sécurisé [18]

Conclusion

Dans ce chapitre nous avons vue en premier lieu les principes de la sécurité, les objectif fixés par la sécurité, ainsi que les menaces et différents attaquants qui veulent faire intrusion dans le réseau, En deuxième lieu nous avons présenté quelques solutions qui permettent d'assurer une politique de sécurité efficace tel que le firewall, le chiffrement DMZ contrôle d'accès. Dans le prochain chapitre, nous allons présenter l'organisme d'accueil de l'entreprise Cevital .

Chapitre 3

Étude de l'existant

Introduction

Ce chapitre est consacré à l'étude de l'existant au sein de l'entreprise Cevital. Nous examinerons en détail les équipements, l'infrastructure et l'architecture organisationnelle actuellement en place. Cette analyse est essentielle pour comprendre les fondations opérationnelles de Cevital et identifier les points d'amélioration potentiels.

3.1 Présentation de l'entreprise et de son historique

Cevital agro-industrie est une des filiales du groupe Cevital, elle fait partie des entreprises algériennes qui ont vu le jour dès l'entrée de notre pays en économie de marché. Elle a été créée par des fonds privés en 1998, elle a pour actionnaires principaux, Mr ISSAD REBRAB et ses enfants. Le siège social de Cevital est sis à Garidi Kouba (Alger), le complexe qui a fait l'objet de notre cas d'étude est situé au nouveau quai de l'arrière port de Bejaïa.

Cevital contribue largement au développement de l'industrie agroalimentaire nationale, elle offre des produits de haute qualité aux consommateurs mais aussi aux industriels et cela grâce à ses prix compétitifs, son savoir-faire, la modernité de ses unités de production, le contrôle strict en ce qui concerne la qualité mais aussi et surtout un réseau de distribution très développé.

Elle couvre les besoins nationaux et a permis de faire passer l'Algérie du stade d'importateur à celui d'exportateur pour les huiles, les margarines et le sucre. Leader en Afrique et dans le Bassin Méditerranéen dans l'industrie du sucre et de l'huile végétale ; Ses produits se vendent dans plusieurs pays, notamment en Europe, au Maghreb, au Moyen Orient et en Afrique de l'Ouest.

3.1.1 Organisme du Cevital

L'entreprise CEVITAL est constituée de différentes directions. On cite :

- **La direction des finances et comptabilité :**
  le rôle de cette direction est de préparer et mettre à jour les budgets, de tenir la comptabilité et préparer les états comptables et financiers et de pratiquer le contrôle de gestion.
- **La direction commerciale :**
  elle a en charge de commercialiser toutes les gammes des produits, le développement du fichier client de l'entreprise et de la gestion de la relation client.
- **La direction des ressources humaines :**
  cette direction a pour mission d'assurer un support administratif à l'ensemble du personnel de CEVITAL, de piloter les activités du social et d'assister à la direction générale ainsi que tous les managers sur tous les aspects de la gestion des ressources humaines.

— **La direction industrielle** :
elle est chargée de l'évolution industrielle des sites de production et définit, avec la direction générale, les objectifs et le budget de chaque site. Elle analyse les dysfonctionnements sur chaque site (équipements, organisations, etc.) et recherche des solutions techniques ou humaines pour améliorer en permanence la productivité, la qualité des produits et des conditions de travail. Elle anticipe aussi les besoins en matériels et supervise leurs achats.

— **La direction des systèmes d'informations :**
elle assure la mise en place des moyens des technologies de l'information nécessaire pour supporter et améliorer l'activité, la stratégie et la performance de l'entreprise. Elle doit ainsi veiller à la cohérence des moyens d'informatique de communication mis à la disposition des utilisateurs, à leurs mises à niveau, à leurs maîtrises techniques, disponibilité et opérationnalité permanente en toute sécurité.

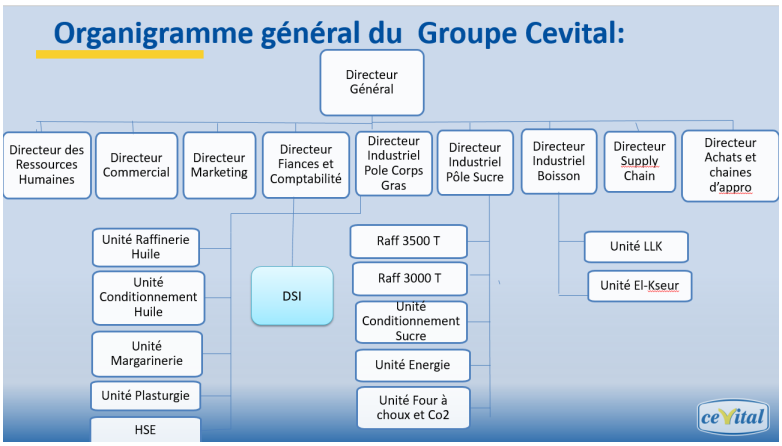

FIGURE 3.1 – Organigramme général du Groupe Cevital

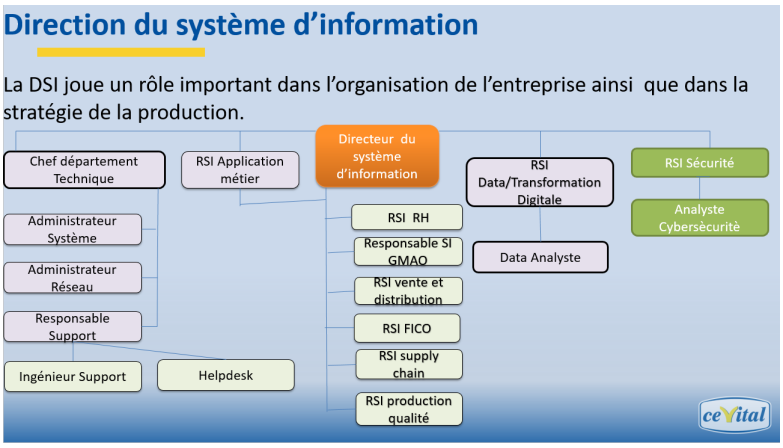

FIGURE 3.2 – Direction du système d'information

Les quatre règles d'or (IRIS) à respecter :

Initiative : Le collaborateur anticipe les problèmes potentiels, et propose des solutions innovantes grâce à sa connaissance métier.

Respect : Un principe prime entre collaborateurs, et avec les partenaires internes et externes.
Intégrité : Une valeur fondamentale, les collaborateurs par leurs actes doivent adopter une éthique professionnelle irréprochable.
Solidarité : Les collaborateurs doivent s'entraider mutuellement, et partager leur expérience et savoir.

Infrastructure de l'entreprise

Cevital Agro-industrie dispose de plusieurs unités de production ultra modernes qui se présentent comme suit :
- Deux raffineries de sucre.
- Une unité de sucre liquide.
- Une raffinerie d'huile.
- Une margarine-rie.
- Une unité de conditionnement d'eau minérale (se situe à Tizi-Ouzou).
- Une unité de fabrication et de conditionnement de boissons rafraîchissantes (site El-Kseur).
- Une conserverie.
- Silos portuaires.
- Unité de trituration

3.1.2 Situation géographique

Cevital agro-industrie est le plus grand complexe privé en Algérie, il s'étend sur une superficie de 45000 m^2 avec un siège social situé à Béjaïa, au nouveau quai du port, à proximité de la route nationale 26 soit à 280 km d'Alger, ce qui fait que cet emplacement géographique lui est bénéfique, car elle se trouve pas loin de l'aéroport, du port de Bejaia, et dela zone industrielle d'Akbou ce qui lui permet de posséder un quai privé.

Le groupe possède également des installations et des bureaux dans d'autres villes algériennes telles qu'Alger, Oran, Tizi-Ouzou et Constantine. Le complexe qui a fait l'objet de notre cas d'étude est situé au nouveau quai de l'arrière-port de Bejaïa.a également étendu ses activités à l'étranger, avec des bureaux et des installations dans plusieurs pays, notamment la France, les Émirats Arabes Unis, le Portugal, l'Italie, les États- Unis, l'Espagne et le Brésil.
Ces filiales étrangères sont principalement axées sur la distribution et la commercialisation de produits Cevital dans ces pays.

3.2 Équipements informatique

3.2.1 Modèles et nombres des équipements

<table>
<tr><td colspan="2" rowspan="2">Équipement</td><td colspan="3">Le hardware</td><td rowspan="2">Le software</td></tr>
<tr><td>Nombre</td><td colspan="2">Marque</td></tr>
<tr><td colspan="2" rowspan="2">Ordinateurs personnels</td><td rowspan="2">1400</td><td colspan="2">80% HP</td><td rowspan="2">Windows10 22H2

Windows 11 22H2</td></tr>
<tr><td colspan="2">15% Lenovo</td></tr>
<tr><td colspan="2">Imprimantes</td><td>150</td><td colspan="2">90% Canon</td><td rowspan="6"></td></tr>
<tr><td rowspan="4">Téléphones</td><td>Numériques</td><td rowspan="4">700</td><td rowspan="4">Alcatel-Lucent</td><td>4019,4029,4039</td></tr>
<tr><td>Analogiques</td><td>/</td></tr>
<tr><td>IP</td><td>4018,4028,8028s</td></tr>
<tr><td>Dect</td><td>8232s</td></tr>
<tr><td colspan="2">Routeur</td><td>02</td><td colspan="2">Cisco</td></tr>
<tr><td colspan="2">Switch</td><td>55</td><td colspan="2">Cisco</td></tr>
<tr><td rowspan="2">Serveur</td><td>Physique</td><td>40</td><td colspan="2" rowspan="2">HP</td><td rowspan="5"></td></tr>
<tr><td>Virtuelle</td><td>22</td></tr>
<tr><td colspan="2">Pare-feu</td><td>04</td><td colspan="2">Fortinet</td></tr>
<tr><td colspan="2">Point d'accès</td><td>26</td><td colspan="2">Ruckus, zoneFlex R500</td></tr>
<tr><td colspan="2">PDA</td><td>———</td><td colspan="2">Motorola</td></tr>
<tr><td colspan="2">Cameras</td><td>473</td><td colspan="2">Samsung, pelco, dahua</td></tr>
</table>

TABLE 3.1 – Modèles et nombre des équipements

3.2.2 Nombre et modèles des switchs

Modèle	Nombre
C9200-L-48P-4G	03
WS-C2960X-48FPS-L	06
WS-C2960X-24PS-L	06
WS-C2960X-24PS-L V03	04
WS-C2960X-24PS-L V06	02
WS-C2960-48PST-L	03
WS-C2960-48TC-L	07
WS-C2960-24TC-L	03
WS-C2960-24TC-S	01
WS-C2960-24PC-L	03
WS-C2960C-12PC-L V05	02
WS-C2960-24LT-L	02
WS-C2960C-12PC	02
WS-C2960-8TC-L	01
C2950-I6K2L2Q4-M	01
WS-C2950G-12-EI	02
WS-C3850-24S	02
C6807-XL	02
Nexus 3048	03

TABLE 3.2 – Nombre et modèles des switch

Serveurs :

Cevital possède 62 serveurs dont 40 sont physique tandis que 22 sont logiques, parmi eux :

-Serveur WSUS pour les mises à jour des machines.

-Sage x3 pour la facturation et comptabilité.

-Coswin pour la gestion des stocks et maintenance

-Kelio pour le suivi des pointages.

-Skeeper pour la traçabilité.

-2 Exchange comme serveurs de messagerie.

-GLPI présente la plateforme pour recevoir les tickets des utilisateurs au cas de problèmes informatique.

Codification des équipements de Cevital

-CEVWKS 1XXX : ordinateur de bureau

-CEVLAP 1XXX : ordinateur portable

-CEVSRV 1XXX : serveur

-CEVSWC 13XX : switch

-CEVAP 1XXX : point d'accès wifi

-CEVFW 1XXX : pare feu

-CEVRTR 1XXX : Routeur.

3.2.3 Vlans de l'entreprise

Direction	Vlans
DRH	VLAN10
Direction des Appro	VLAN11
DSI	VLAN12
Raff Huile	VLAN13
Raff sucre 3000T	VLAN14
Division utilités	VLAN15
Supply-chain	VLAN16
Unité margarinerie	VLAN17
Printer	VLAN18
Téléphone	VLAN20
Voice	VLAN21
Direction R D	VLAN22
Performance industriel	VLAN23
Unité Cdt Huile	VLAN24
Management switch	VLAN 25
DFC	VLAN26
Commercial	VLAN27
Direction générale	VLAN28
Direction qualité et management système	VLAN29
Raff sucre 3500T	VLAN30
Cdt sucre	VLAN31
Caméra	VLAN32
Projets	VLAN33
Trituration	VLAN36

TABLE 3.3 – Vlans de l'entreprise

3.3 Réseaux internes de l'entreprise

Cevital dispose d'un réseau informatique assez vaste, lui permettant de relier de manière efficace ses blocs administratifs et ses unités de productions, l'architecture repose sur un modèle hiérarchique en couches, composé principalement de la couche cœur du réseau, la couche distribution ainsi que la couche d'accès, l'entreprise s'est dotée d'une redondance matérielle ce qui lui assure la haute disponibilité du réseau informatique même en cas de panne afin de garantir la continuité des services, tous les périphériques réseaux de l'entreprise sont de marque CISCO, les liaisons d'interconnexion entre les différents périphériques réseaux sont en fibre optique à

hauteur de 95% , le reste en câble en cuivre a paires torsadés.
En matière de sécurité, l'entreprise se dotes de quatre Firewalls de marque Fortinet, deux utilisés pour la sécurisation du réseau interne de l'entreprise, deux autres pour sécuriser tout trafic réseau depuis et vers le réseau extérieur de l'entreprise.

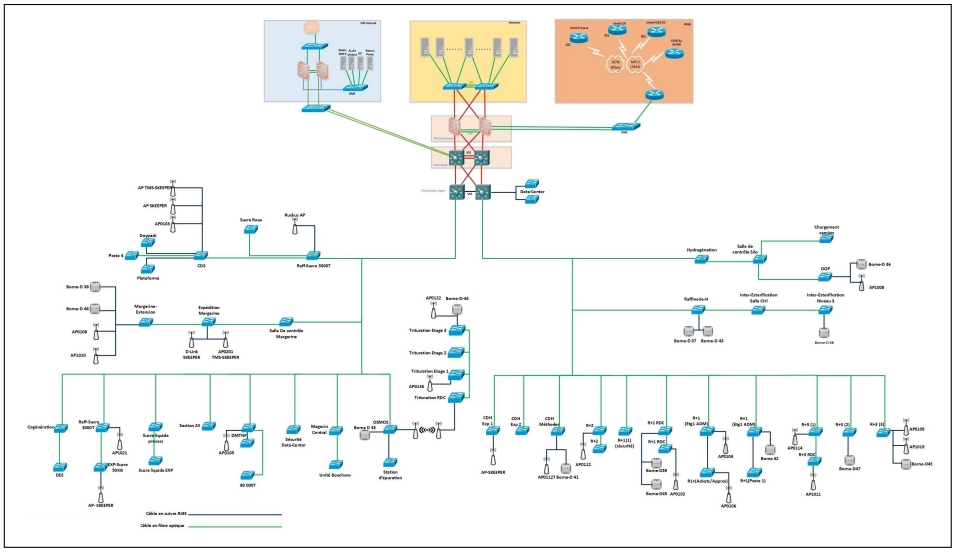

FIGURE 3.3 – Architecture du réseaux informatique CEVITAL

3.4 Problématique

Étant donné que la sécurité du réseau informatique de Cevital présente un enjeu majeur sur la continuité de ses objectifs industriels, par quel moyen pourrions nous détecter, voir de bloquer les attaques qui pourraient toucher et nuire au réseau de l'entreprise ?

3.5 Propositions

1. Évaluer les risques auxquels l'entreprise Cevital est exposée en l'absence d'un système de sécurité pour la détection et la prévention d'intrusions sur son réseau informatique.
2. Analyser les solutions techniques existantes pour la sécurité informatique, en prenant en compte les spécificités de l'entreprise Cevital.
3. Concevoir et proposer un système de sécurité pour la détection et la prévention d'intrusions sur le réseau informatique de l'entreprise Cevital, adapté à ses besoins spécifiques.
4. Évaluer les coûts et les avantages de chaque solution proposée pour aider l'entreprise Cevital à choisir la solution la plus adaptée à ses besoins et à son budget.
5. Proposer des recommandations pour la mise en place effective du système de sécurité choisi, en tenant compte des contraintes de coûts et de facilité d'utilisation.

3.6 Solution

Pour faire face à ces problèmes de sécurité informatique dans le réseau d'entreprise Cevital, nous avons constaté des anomalies relatives à la sécurité de leur réseau, à savoir le manque d'un mécanisme de détection et de prévention d'intrusion. pour cela nous avons mis en place un système de détection et de prévention d'intrusion

Conclusion

Dans ce chapitre,nous avons vue l'étude de l'existant de l'entreprise cevital, architecture ainsi que les différents équipements. Mais malgré toutes les techniques utilisées pour empêcher les attaques Internet, un système n'est jamais totalement sûr. De ce fait des systèmes de détection et de prévention d'intrusion sont mis en place.
Dans le prochain chapitre, nous allons présenter les systèmes de détection et de prévention d'intrusion(IDS,IPS).

Chapitre 4

Systèmes de détection et de prévention d'intrusion

Introduction

Les réseaux informatiques sont de plus en plus susceptibles d'être la cible de dérèglements divers, à l'encontre de leur sécurité, tels que les congestions, les accès malveillants et les attaques.A cet effet, il devient inéluctable de munir ces systèmes d'outils et de mécanismes capables d'inhiber ces dérèglements. Afin de détecter toute tentative de violation de la politique de sécurité, une surveillance permanente ou régulière des systèmes peut être mise en place : ce sont les Systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion(IPS).
Les systèmes de détection d'intrusions ainsi que les systèmes de préventions d'intrusion sont devenus très largement déployés dans les systèmes d'informations et ils ont gagné une place importante dans la conception de la stratégie de sécurité.

4.1 Système de détection d'intrusion (IDS)

Un système de détection d'intrusion (IDS - Intrusion Detection System) est un outil de sécurité informatique qui surveille le trafic réseau pour détecter les tentatives d'accès non autorisées,les attaques de sécurité et les activités malveillantes connues[19].

4.1.1 Types de système détection d'intrusion

Il existe trois types principaux de systèmes de détection d'intrusion (IDS) :

4.1.1.1 Systèmes de détection d'intrusion réseau(NIDS)

Les NIDS (Network Intrusion Detection System) sont des IDS utilisés pour protéger un réseau .Ils surveillent et analysent le trafic réseau à la recherche de comportements suspects et de véritables menaces avec l'aide de capteurs NIDS. Il examine le contenu et les informations d'en-tête de tous les paquets circulant sur le réseau. [20]

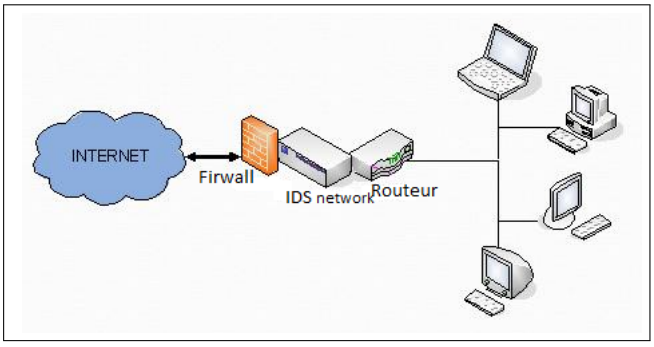

FIGURE 4.1 – Exemple de NIDS

4.1.1.2 Systèmes de détection d'intrusion de type hôte (HIDS)

Les HIDS (Host Intrusion Detection System) sont des IDS dédiés à un matériel ou système d'exploitation. HIDS surveille le trafic sur une seule machine et analyse les journaux systèmes,

les appels, et enfin vérifie l'intégrité des fichiers. Un HIDS a besoin d'un système sain pour vérifier l'intégrité des données. Si le système a été compromis par un pirate, le HIDS ne sera plus efficace .

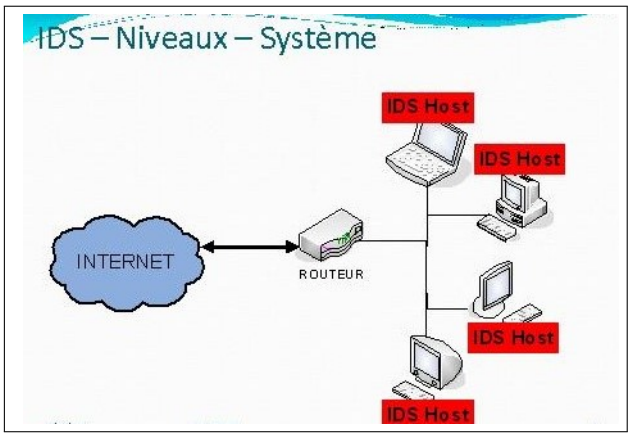

FIGURE 4.2 – Exemple de HIDS

4.1.1.3 Systèmes de détection d'intrusion Hybrides

Un système de détection d'intrusion hybride est une solution de sécurité qui combine plusieurs méthodes de détection d'intrusion(NIDS,HIDS), telles que la surveillance du trafic réseau, l'analyse des activités système et l'inspection du contenu des paquets, pour offrir une protection plus complète contre les menaces informatiques. En intégrant différentes approches, ces systèmes visent à améliorer la précision de la détection et à réduire les faux positifs, offrant ainsi une défense robuste contre les attaques malveillantes.

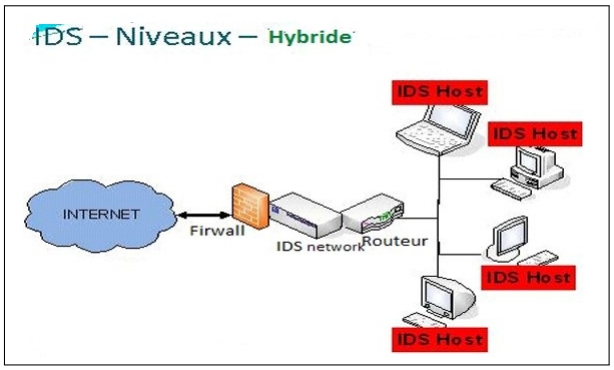

FIGURE 4.3 – Exemple d'Hybride

4.1.2 Comparaison entre les types d'IDS

	Avantages	Inconvénients
NIDS	-Assurer la sécurité contre les attaques puisqu'il est invisible. -Détecter plus facilement les scans grâce aux signatures.	-La probabilité de faux négatifs est élevée et il est difficile de contrôler le réseau entier. -Al'opposé des IDS basés surl'hôte, ils ne voient pas les impacts d'une attaque
HIDS	-Observer les activités sur l'hôte avec précision. -Détecter des attaques impossibles à détecter avec des IDS réseau puisque le trafic est souvent crypté.	-Ils ont moins de facilité à détecter les scans. -Ils sont plus vulnérables aux attaques de type DoS. -Ils consomment beaucoup de ressources CPU.
Hybrides	-moins de faux positifs. -Meilleure corrélation(La corrélation permet de générer de nouvelles alertes à partir de celles existantes). -Possibilité de réaction sur les analyseurs	-Complexité de l'implémentation

TABLE 4.1 – Comparaison entre les types d'IDS

4.1.3 Architecture fonctionnelle des IDS

Dans son fonctionnement, pour arriver à détection une intrusion, les IDS sont découpés en trois grandes parties. La Figure ci-dessous illustre les interactions entre ces trois composants[21].

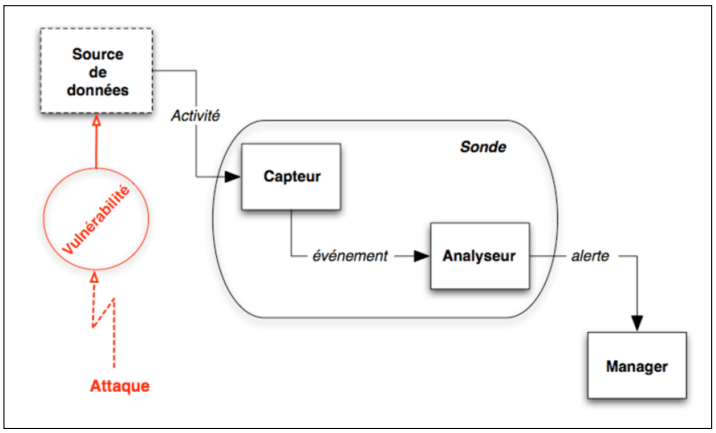

FIGURE 4.4 – Architecture d'un IDS

4.1.3.1 Capteur

Grâce aux capteurs, le système récolte les informations des trafics sur le réseau et le fourni à l'analyseur. Avant de le fournir à ce dernier, ces informations sont soumises à un pré-traitement c'est-à-dire un filtre BPF (Berkeley Paquet Filter) leur est appliqué. Ce filtre correspond à l'affinage des informations que l'IDS cherche à récupérer.

4.1.3.2 Analyseur

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

4.1.3.3 Manager

Le manager collecte les alertes produites par le capteur, les met en forme et les présente à l'administrateur.Le manager est généralement chargé de limiter les effets des attaques et tenter de les arrêter, restaurer le système affecté et identifier les problèmes.

4.1.4 Méthodes de détection des IDS

Il existe deux méthodes de détection d'intrusion (IDS) :

4.1.4.1 Approche par scénario ou par signature

Les systèmes à base de signatures qui consistent à rechercher dans l'activité de l'élément surveillé les signatures (empreintes) d'attaques répertoriées et donc connues. Ce principe de détection d'intrusion est réactif et pose plusieurs contraintes, en effet il ne détecte que les attaques répertoriées dont il possède l'empreinte. De ce fait il nécessite des mises à jour fréquentes. Ce principe de détection implique aussi que les pirates peuvent contourner celui-ci en maquillant leurs attaques, il modifie en fait la signature connue par les IDS et de ce fait l'attaque devient invisible par l'IDS.

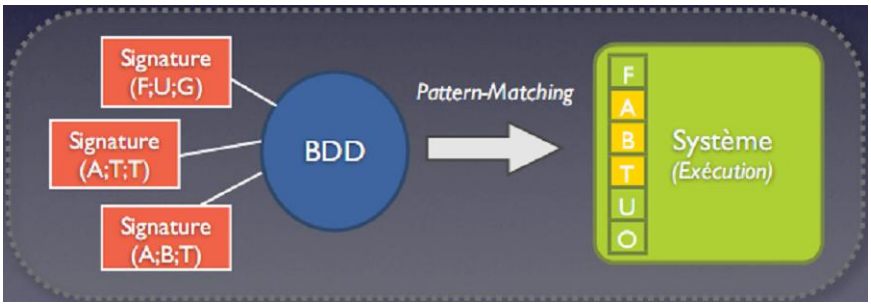

FIGURE 4.5 – Approche par signature

4.1.4.2 L'approche comportementale (Anomaly Detection)

Cette technique consiste à détecter une intrusion en fonction du comportement passé de l'utilisateur. Il faut préalablement dresser un profil utilisateur à partir de ses habitudes et dé-

clencher une alerte lorsque des événements hors profil se produisent.
Cette technique peut être appliquée non seulement à des utilisateurs mais aussi à des applications et services.Il détecte les nouveaux types d'attaques.
Plusieurs paramètres sont possibles : la charge CPU, le volume de données échangées, la durée et l'heure de connexion sur des ressources, la répartition statistique des protocoles et applications utilisés [22].

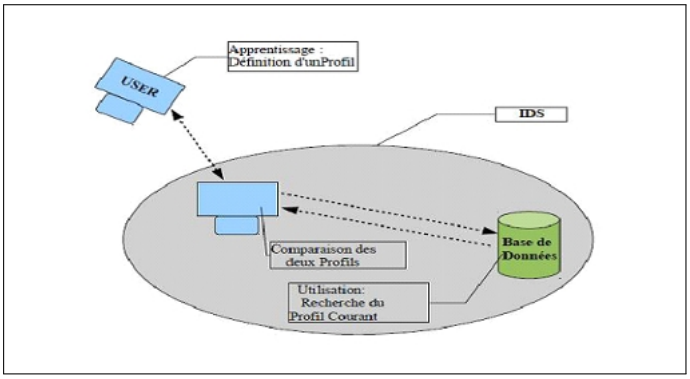

FIGURE 4.6 – illustration de l'approche comportementale

4.1.5 Limite des IDS

— **N-IDS** : Ils sont basés sur une bibliothèque de signatures d'attaques connues,cette bibliothèque devra être mise à jour à chaque nouvelle attaque sera affichée. Si l'attaque ne contient pas la signature d'une attaque spécifique et récente, cette dernière passera au travers des mailles du filet et la sécurité des données et le réseau en général sera menacé[23].

— **H-IDS** : Il génère une alerte si une activité sur l'hôte s'éloigne de la norme, mais si dans un cas exceptionnel une requête justifiée mais non prévue par le système venaient à arriver en masse, cette méthode de protection risquerait de générer des alertes infondées. Dans ce cas les H-IDS ne sont pas fiables car ils ne font que générer des alertes, et ce sera à un administrateur en charge de la sécurité du réseau de dire si telle ou telle requête est valable ou pas[23].

4.1.6 Avantages des IDS

— Effectuer une détection en temps réel.
— Surveille le trafic réseau à la recherche de modèles et d'activités suspectes.
— Offre une détection des menaces et un système d'alerte précoce.
— Permettant aux équipes de sécurité de réagir rapidement aux menaces émergentes avant qu'elles ne s'aggravent.

4.2 Système de prévention d'intrusion(IPS)

Un système de prévention d'intrusion (IPS-Intrusion Prevention System) est un outil de protection et de sécurité informatique contre les intrusions pour détecter et bloquer les activités malveillantes sur un réseau ou un système informatique, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque.
C'est un IDS actif, il empêche toute activité suspecte détectée au sein d'un système. [24]

4.2.1 Types de système de prévention d'intrusion

Il existe trois types d'IPS :

4.2.1.1 Systèmes de prévention d'intrusion réseau(NIPS)

Les NIPS (Network Intrusion Prevention System) sont des IPS permettant de surveiller l'ensemble du réseau pour détecter tout trafic suspect en analysant l'activité des protocoles. Il est installé à des endroits stratégiques pour surveiller l'ensemble du trafic réseau et détecter les menaces [25].

4.2.1.2 Systèmes de prévention d'intrusion de type hôte (HIPS)

Les HIPS (Host-based Intrusion Prevention System) sont des IPS installés sur des hôtes ou des terminaux individuels et surveille leurs activités à la recherche de comportements malveillants [25].

4.2.1.3 Systèmes de prévention des intrusions sans fil(WIPS)

Les WIPS (Wirless Intrusion Prevention System) surveille les protocoles réseau sans fil pour détecter les activités suspectes, comme les utilisateurs non autorisés et les appareils accédant au Wi-Fi de l'entreprise. Si un WIPS détecte une entité inconnue sur un réseau sans fil, il peut terminer la connexion. Un WIPS peut également aider à détecter les appareils mal configurés ou non sécurisés sur un réseau Wi-Fi et à intercepter les attaques potentielles, où un pirate informatique espionne secrètement les communications des utilisateurs [26].

4.2.2 Architecture fonctionnelle 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 [27].

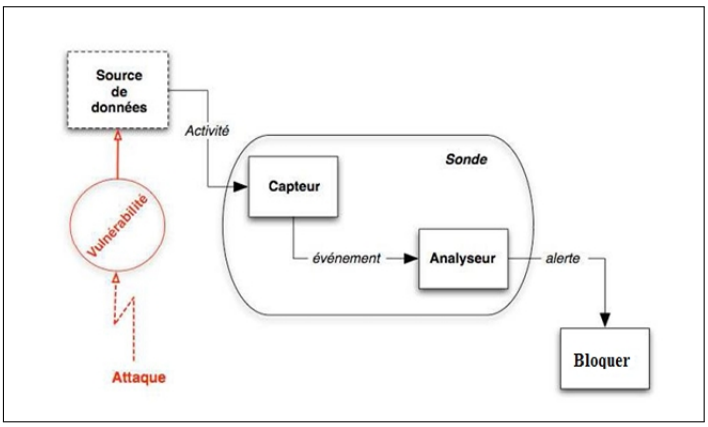

FIGURE 4.7 – Architecture d'un IPS

4.2.3 Avantages des IPS

— il réduit les risques d'incidents de sécurité
— il fournit une protection plus dynamique contre les menaces.
— Protège les systèmes, des comportements dangereux et pas seulement le trafic.
— offre des réponses automatisées aux menaces détectées, réduit la fenêtre d'opportunité pour les attaquants et applique les politiques de sécurité du réseau.

4.2.4 Inconvénients des IPS

— Ils bloquent toute activité qui lui semble suspecte, mais n'étant pas fiable à 100 % ils peuvent donc bloquer incorrectement des applications ou des trafics légitimes.
— IPS peut générer des faux positifs, entraînant des perturbations potentielles du trafic réseau légitime.
— Ils laissent parfois passer certaines attaques sans les repérer, et permettent donc aux pirates d'attaquer un PC.
— Ils sont peu discrets et peuvent être découverts lors de l'attaque d'un pirate une fois qu'il aura découvert l'IPS s'empressera de trouver une faille dans ce dernier pour le détourner et arriver à son but [28].

4.3 Comparaison entre les IDS et les IPS

Bien que les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion (IPS) visent tous les deux à améliorer la sécurité du réseau.

Les IDS (systèmes de détection d'intrusion) sont des outils logiciels conçus pour détecter et surveiller le trafic réseau. Cependant, son rôle s'arrête là. Un outil IDS n'agit point contre les activités malveillantes. Contrairement à un IPS, il n'entreprend aucune action de lui-même. Il nécessite un humain pour analyser les résultats et prendre les décisions sur les mesures à prendre. Entre autres, l'IPS est une extension de l'IDS.

Un IDS envoie juste des alertes aux administrateurs dans la détection d'une menace. En revanche, un IPS prend toutes les dispositions pour protéger au maximum le réseau contre les

dommages [29].

4.4 La différence entre Firewall et IPS

Firewall est un système de contrôle d'accès basé sur des règles statiques autorisant ou refusant certains flux. Il se concentre généralement sur la sécurité au niveau de la couche quatre du modèle OSI ce qui est insuffisant pour les intrusions.
Tandis qu'**IPS** offre une protection plus complète en surveillant l'intégralité des flux de données jusqu'à la couche applicative (couche sept), ce qui leur permet de détecter et de bloquer les menaces

4.5 La différence entre Firewall et IDS

Les pare-feux et les systèmes de détection des intrusions (IDS) sont des outils de cybersécurité qui peuvent à la fois protéger un réseau ou un endpoint. Cependant, leurs objectifs sont très différents les uns des autres.

IDS : Les systèmes de détection des intrusions sont des outils de surveillance passive qui identifient les menaces possibles et envoient des notifications aux analystes des centres d'opérations de sécurité (SOC). De cette manière, les intervenants aux incidents peuvent rapidement examiner et traiter l'événement potentiel.
Pare-feu : Un pare-feu, en revanche, analyse les métadonnées contenues dans les paquets réseau et décide d'autoriser ou d'interdire le trafic entrant ou sortant du réseau en fonction de règles préétablies. Un pare-feu crée essentiellement une barrière qui empêche certains trafics de le traverser.

— Un IDS se concentre sur la détection et la génération d'alertes sur les menaces, tandis qu'un pare-feu inspecte le trafic entrant et sortant, maintenant tout le trafic non autorisé à distance [30].

Conclusion

Ce chapitre nous a permis de découvrir les systèmes de détection d'intrusion et de prévention d'intrusions, leurs architecture,leur types ainsi que leurs fonctionnements.
le chapitre suivant nos renseigne comment réussir la configuration, après installation, du système de détection et de prévention d'intrusion afin de mieux sécuriser le réseau.

Chapitre 5

Conception et réalisation

Introduction

Dans ce dernier chapitre, nous allons implémenter les plates-formes de sécurité PfSense et snort, nous allons voir toutes les configurations nécessaires.
En final, nous allons donner quelques tests que nous avons réalisés en lançant quelques attaques et quelques virus et voir comment ces derniers sont détectés et bloqués.

5.1 Étape de réalisation

Les étapes de notre travail sont :
-Mettre en place un système de détection précoce des tentatives d'intrusion.
-Mettre en œuvre des mécanismes de prévention pour stopper les attaques en cours.
-Étudier et analyser toutes les aspects traités par un système de détection/prévention d'intrusion réseau.
-Étude de cas : snort
-Installation et configuration de snort
-Tests de détection d'intrusion en utilisant des règles -prédéfinies de snort.
-Tests et évaluations de performance d'IDS IPS Snort.

5.2 Outils de travail

5.2.1 Ordinateur personnel

HP probook DESKTOP-5E2006T équipé d'un processeur Intel Core i5 de 8ème génération, 16 Go de RAM et un disque dur SSD. Le système d'exploitation utilisé est Windows 10 en version 64 bits.

5.2.2 VMware

VMware est une société de logiciels spécialisée dans la virtualisation et le cloud computing. La virtualisation consiste à créer une représentation logicielle de quelque chose, un serveur par exemple, afin de pouvoir y accéder et l'utiliser sans se soucier des contraintes liées à son matériel physique. L'infrastructure virtuelle VMware permet aux entreprises de réduire leurs coûts informatiques en étant plus efficaces, plus flexibles et plus réactives. La gestion d'une infrastructure virtuelle permet aux responsables informatiques d'allouer et de gérer dynamiquement des ressources en fonction des besoins.

VMware Workstation Pro est un logiciel hyperviseur de type 2 qui permet un utilisateur de crée et d'exécuter des machines virtuelles sur un système d'exploitation hôte.

VMware Workstation Pro prend en charge une variété de système d'exploitation, notamment Windows, Linux et MacOs. IL comprend également des fonctionnalités telles que la simulation de réseau virtuel, une interface a onglets multiples, la création de clichés instantanés,

la duplication, et bien d'autres.

5.2.3 PfSense

Pour la supervision du trafic réseau au niveau des entreprises ou des sociétés, nous avons choisi PFSENSE comme étant un outil excellent à mettre en place.

Notre choix s'est basé sur les points forts de cet pare-feu notamment sa haute disponibilité (HA) qui permet à l'infrastructure ou bien à un service d'etre joignable il possède une interface graphique qui est facile à configurer et facilite la tâche aux administrateurs réseaux afin d'effectuer toutes les configurations possibles et d'éviter des attaques.

pfSense est une solution open source qui se base sur le système d'exploitation FreeBSD, elle est spécialisée dans les fonctions de pare-feu et de routeur.

En utilisant pfSense, l'environnement de travail bénéficie d'un pare-feu puissant et flexible pour protéger le réseau de Cevital. Il permet de définir des politiques de sécurité adaptées,De détecter les intrusions et de prévenir les attaques en utilisant Snort, et de mettre en place des mécanismes de filtrage et de blocage pour protéger les ressources et les données de l'entreprise. La configuration et les tests réalisés sur pfSense fourniront des résultats précis sur l'efficacité du système IDS/IPS dans la détection et la prévention des intrusions.

5.2.4 Kali Linux

Kali Linux est un système d'exploitation qui permet avant tout de protéger et d'optimiser des ordinateurs et des réseaux et de déchiffrer des mots de passe.
Cette distribution Linux est largement utilisée dans le domaine de la sécurité informatique. Elle est spécialement conçue pour les tests de sécurité et les audits de pénétration. Dans le cadre du projet, Kali Linux est utilisé pour effectuer des tests d'intrusion dans le réseau de Cevital, afin d'évaluer la résistance du système IDS/IPS (Snort) et de détecter d'éventuelles vulnérabilités.

5.2.5 Windows 10

Windows 10 est Une machine virtuelle, utilisée dans l'environnement de travail pour la configuration et les tests des systèmes IDS/IPS. Vous pouvez également utiliser pFsense via un navigateur web sur Windows 10 pour tester la compatibilité et les performances des systèmes IDS/IPS.

En utilisant VMware sur Windows 10 ,il est possible de créer un environnement virtuel complet et réaliste où les machines virtuelles interagissent avec les périphériques réseau simulés. Cela permet une simulation plus précise des conditions réelles et offre une plate-forme de test plus robuste pour les systèmes de sécurité réseau.

5.2.6 Architecture utilisée

en raison des performances de l'ordinateur personnel nous utiliserons une architecture pour simplifier la simulation du réseau de Cevital pour illuster comment que les machines virtuels sont interconnecter virtuellement.

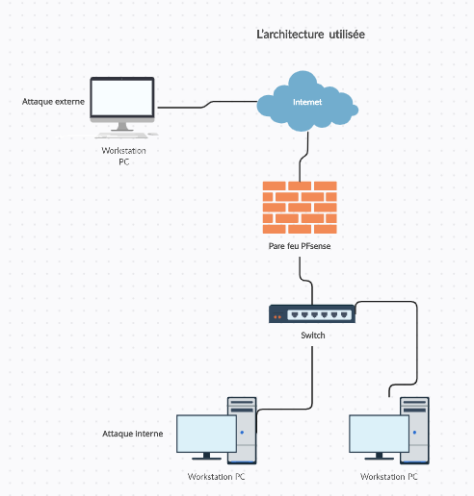

FIGURE 5.1 – Architecture utilisée

5.3 Snort (Système de détection et de prévention d'intrusion)

Snort est un système de détection et de prévention des intrusions (IDS,IPS) open source gratuit qui fournit une analyse du trafic réseau et un enregistrement des paquets de données en temps réel. Snort utilise un langage basé sur des règles qui combine des méthodes d'inspection des anomalies, des protocoles et des signatures pour détecter les activités potentiellement malveillantes.
Le langage de règle SNORT détermine quel trafic réseau doit être collecté et ce qui doit se passer lorsqu'il détecte des paquets malveillants et comme une solution IPS réseau complète qui surveille l'activité réseau et détecte et bloque les vecteurs d'attaque potentiels [31]

Snort offre une grande flexibilité en termes de configuration des règles de détection et de prévention, c'est le système le plus utiliser pour renforcer la sécurité du réseau de l'entreprise.

5.3.1 L'implémentation des IDS et IPS

L'implémentation du système IDS (Intrusion Detection System) et IPS (Intrusion Prevention System) dépend de la configuration et du déploiement de Snort sur le pare-feu pfSense.

5.3.2 Configuration des règles de détection

La configuration des règles de détection de Snort est une étape clé. Il est essentiel d'identifier les signaux d'alerte et les modèles d'attaques informatiques. Il faut ensuite établir des

protocoles d'intervention pour réagir en cas de détection d'activité anormales. Les règles Snort permettent de détecter une grande variété d'attaques comme les dépassements de tampons, les scans,etc.

5.3.3 Intégration avec pfSense

Snort est utilisé en conjonction avec le firewall pfsense pour surveiller les données qui entrent et sortent du réseau. Cette combinaison permet de renforcer la sécurité en appliquant des règles spécifique de détection et de prévention des intrusions.

5.4 Tests de vérification

Une fois configuré, des tests sont effectués pour évaluer l'efficacité de Snort dans la détection des attaques. On peut simuler une attaque pour s'assurer que snort réagit correctement et envoie des alertes adéquates.

En suivant ces étapes, nous nous sommes assurés que Snort était correctement configuré et en cours d'exécution, prêt à détecter et à prévenir les intrusions dans le réseau d'entreprise de Cevital. Les exemples de test vérifieront si Snort peut identifier les attaques internes et externes, afin d'assurer la sécurité des données et des services du réseau.

5.5 Mise en ouvre de la configuration

5.5.1 Installation et Configuration des machines virtuels Vmware

-Accédons au site officiel de www.vmware.com sur google, puis Workstation Pro
-Choisissons le téléchargement sur le système d'exploitation puis cliquer sur Download now

FIGURE 5.2 – Site de Vmware

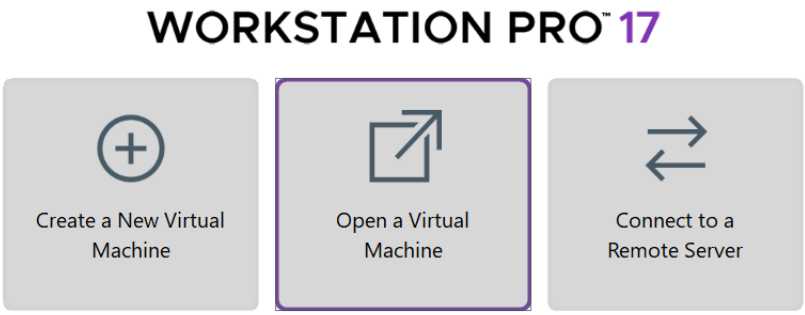

FIGURE 5.3 – Ouvrir une machine virtuel

Une fois télécharger la machine virtuel de Kali Linux nous allons l'implémenter sur VMWARE en clinquant sur "open a new virteul machine " pour faire des attaques malveillantes contre Pfsense et tester la sécurité du réseau

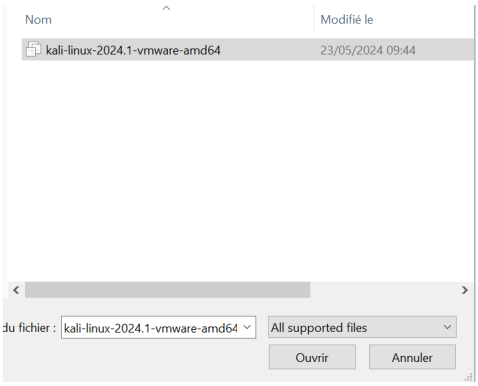

FIGURE 5.4 – Importer la machine Kali Linux

5.5.2 Configuration de pfSense

Nous téléchargeons l'image ISO pfSense a partir du site officiel www.pfsense.org et l'installer sur une machine virtuelle.

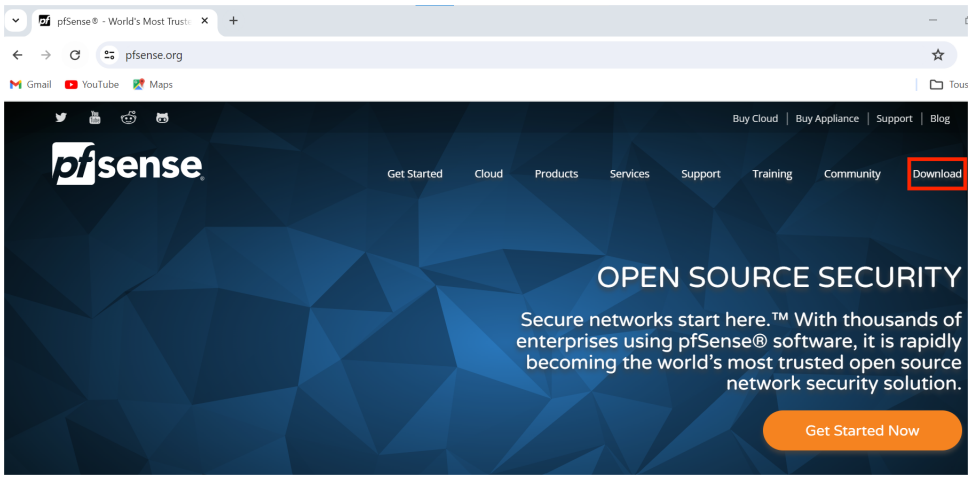

FIGURE 5.5 – Site de PfSense

FIGURE 5.6 – Télécharger PfSense

Nous sélectionnons l'ISO de pfSense que vous avez téléchargée pour l'importer dans VMWARE et l'ouvrir comme une machine virtuel.

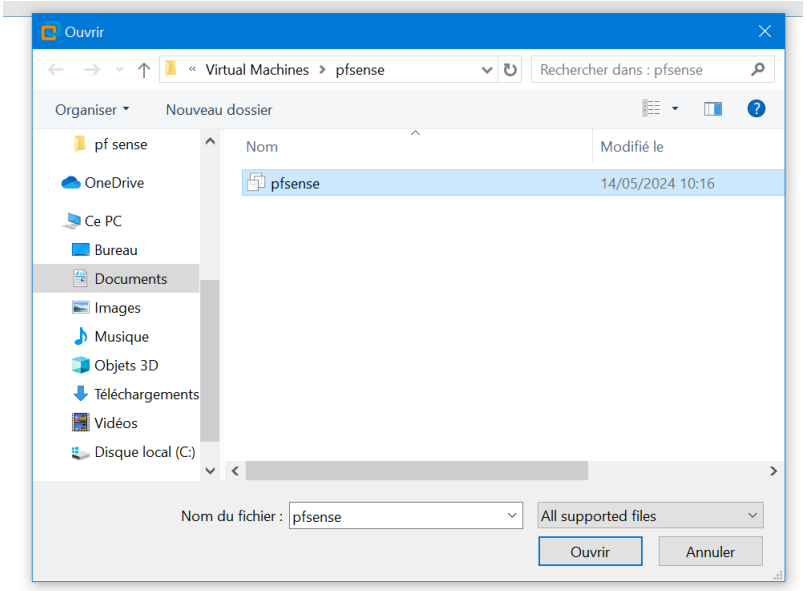

FIGURE 5.7 – Importer Pfsense

5.5.2.1 Configuration initiale de Pfsense

Nous suivons les étapes de configuration initiale jusqu'à ce que nous atteignion l'option "Set Disk Partition" (Définir la partition du disque).

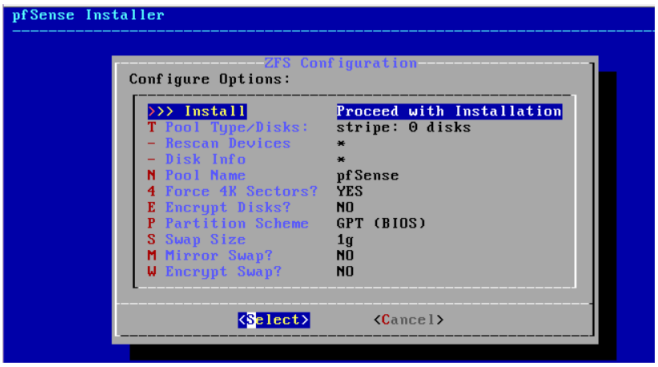

FIGURE 5.8 – Configuration initiale de pfsense étape 1

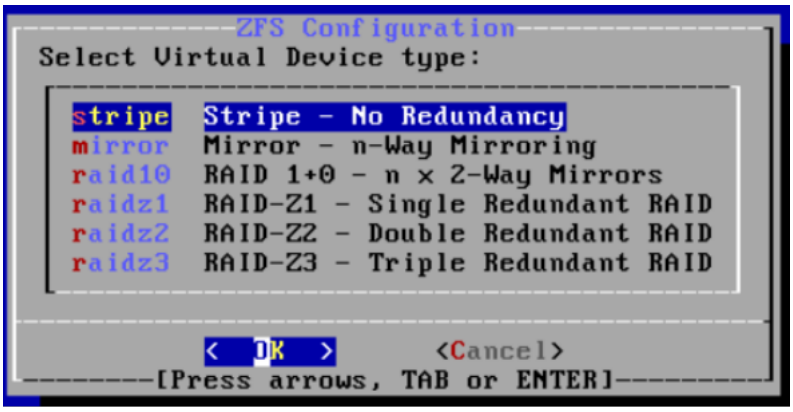

FIGURE 5.9 – Configuration initiale de pfsense étape 2

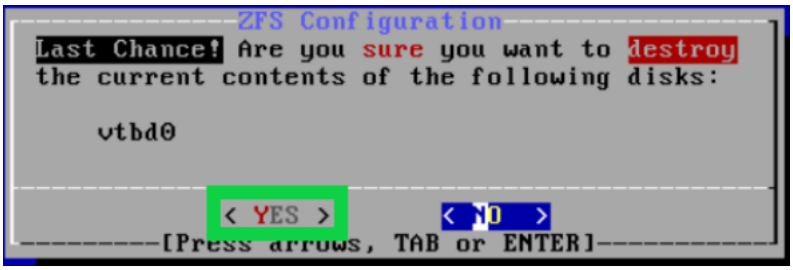

FIGURE 5.10 – Configuration initiale de pfsense étape 3

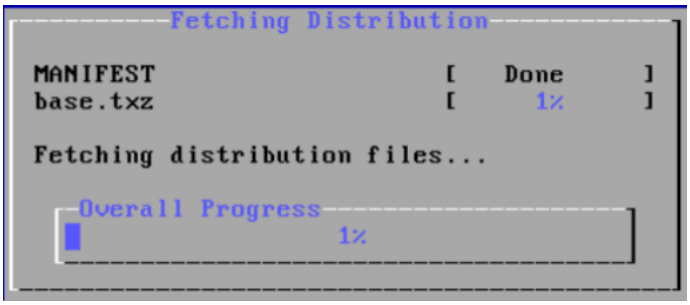

FIGURE 5.11 – Configuration initiale de pfsense étape 4

- Dans l'option "Set Disk Partition", nous sélectionnons "Auto (ZFS)" pour créer automatiquement une partition ZFS sur le disque.

-Nous serons invité à confirmer la création d'une partition ZFS. Appuyez sur "Enter" pour confirmer.
-L'assistant va créer une partition ZFS sur le disque. Une fois terminé, il affichera un résumé des configurations effectuées.
Le système redémarrera pour appliquer les configurations.

5.5.2.2 Configuration des interfaces réseaux de PFsense

Le système démarre et affiche un menu avec plusieurs options. Appuyer sur "2" pour configurer les interfaces réseaux.

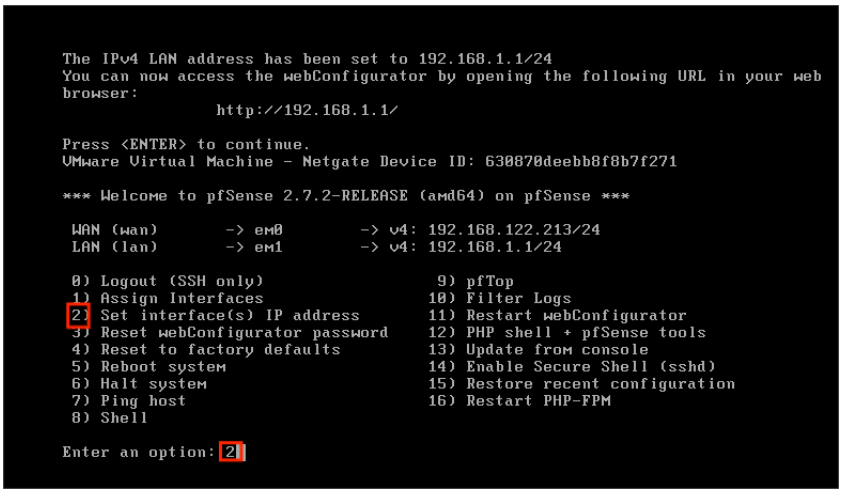

FIGURE 5.12 – Configuration des interfaces réseaux de PFsense étape 1

Nous allons commencer par l'interface WAN donc nous mettons "1"

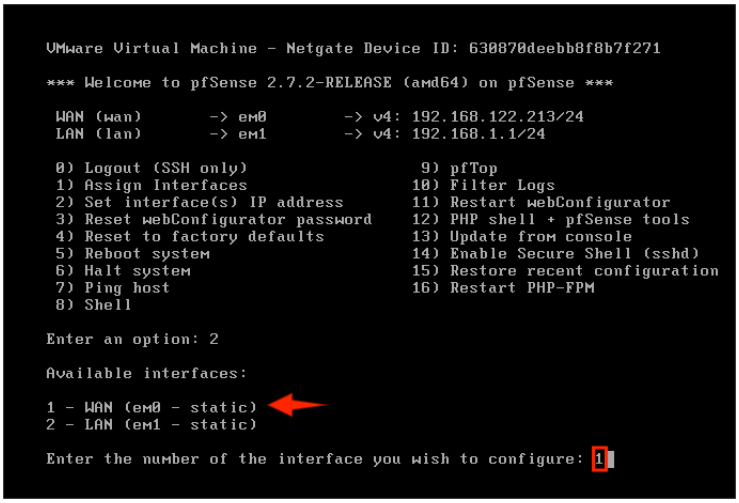

FIGURE 5.13 – Configuration des interfaces réseaux de PFsense étape 2

Pour l'interface Wan nous allons mettre une adresse IP statique

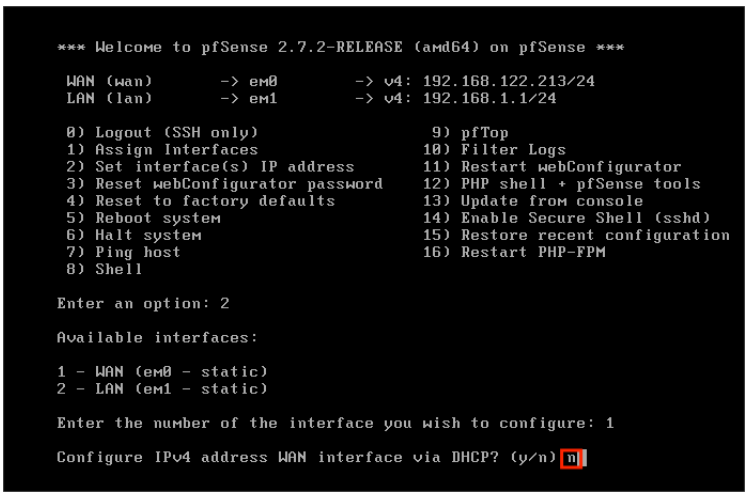

FIGURE 5.14 – Configuration des interfaces réseaux de PFsense étape 3

Pour l'interface WAN nous allons lui configurer :
Une adresse IP : 192.168.80.129/24
Une passerelle par defaut : 192.168.80.2

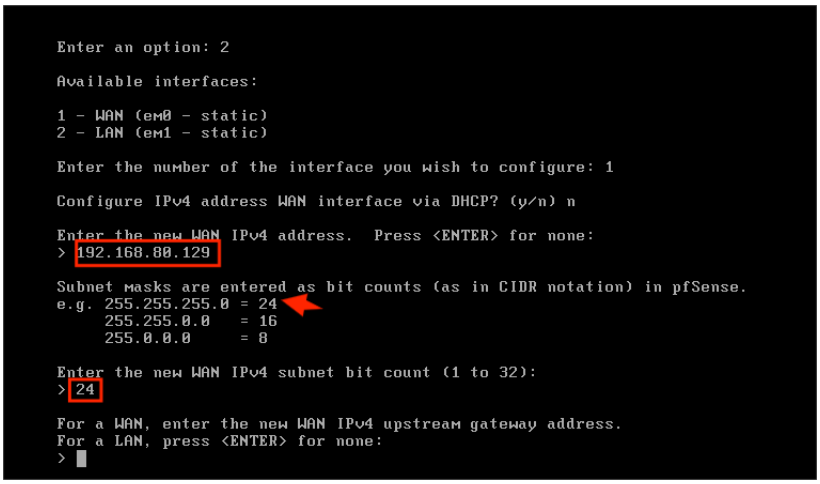

FIGURE 5.15 – Configuration des interfaces réseaux de PFsense étape 4

Une fois la configuration de l'interface WAN est terminer, nous passons à l'interface LAN
Les mêmes étapes de configuration
Pour l'interface LAN nous allons lui attribuer aussi une : Adresse IP : 192.168.1.254/24

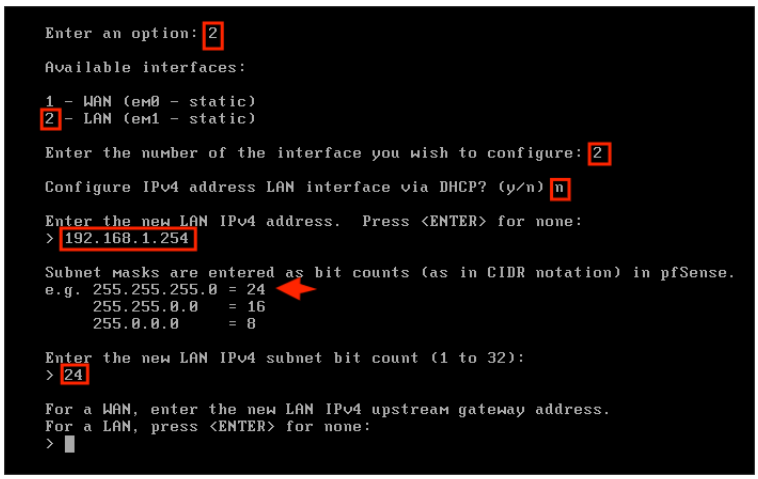

FIGURE 5.16 – Configuration des interfaces réseaux de PFsense étape 5

Cette image montre que les interfaces WAN et LAN sont bien configurer

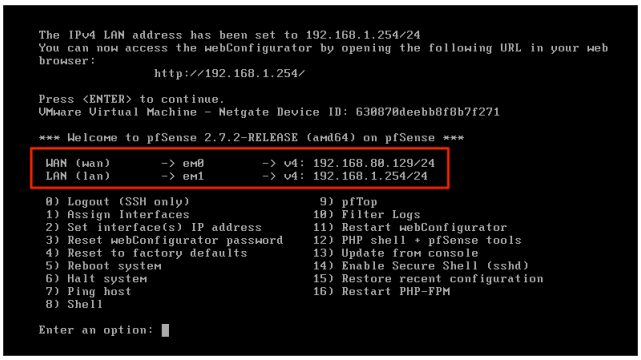

FIGURE 5.17 – Configuration des interfaces réseaux de PFsense étape 6

Une fois que PfSense a redémarré, nous pouvons accéder à son interface Web en ouvrant un navigateur et en saisissant l'adresse IP attribuée à l'interface LAN qui est 192.168.1.254 a partir de là, nous pouvons continuer la configuration de pfSense via l'interface Web.

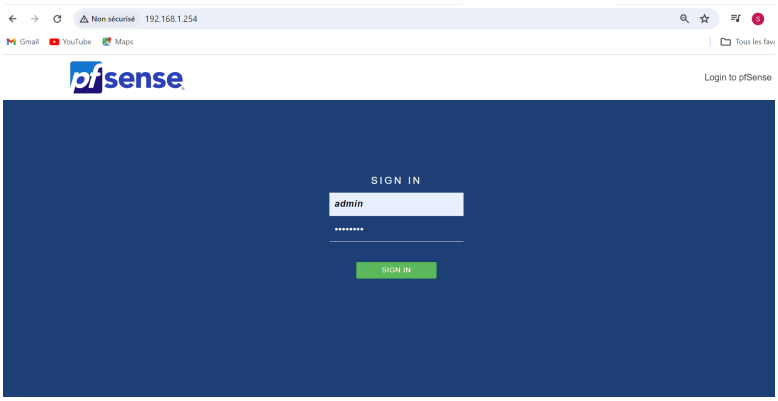

FIGURE 5.18 – Interface web de Pfsense

Et avec les identifiant par défaut (admin) et mots de passe (pfsense) que nous allons avoir accès à l'etape suivante qui est la configuration de PFsense

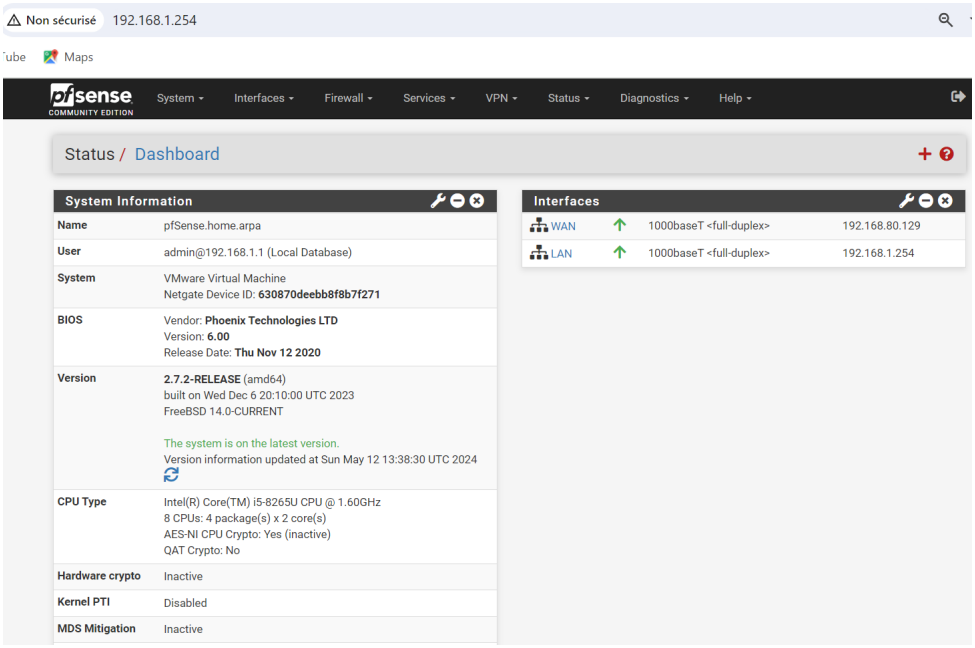

FIGURE 5.19 – Tableau de bord de PfSense

5.5.2.3 Configuration de la topologie

Après avoir installer les différentes appareils virtuels (VMware,Pfsense,Kali Linux),nous allons crée deux réseaux distincts sur cette topologies simplifier le réseau LAN avec l'adresse (192.168.1.0) et le réseau WAN (192.168.80.0).

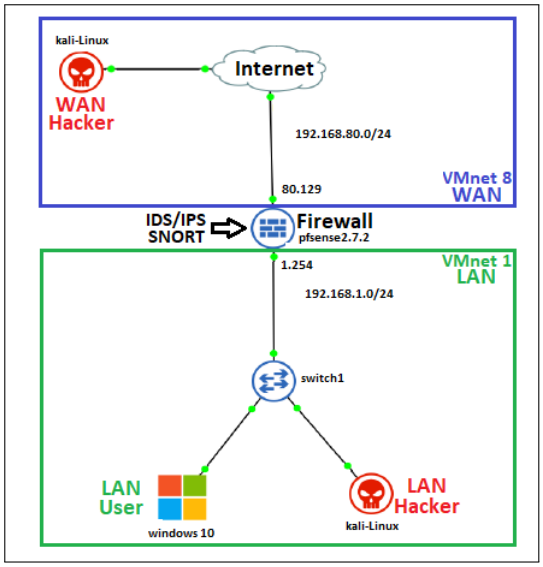

FIGURE 5.20 – Topologie du réseau

5.5.3 Installation et configuration de Snort

Création d'un compte PfSense

-Rendez-vous sur le site Snort.org.
-Cliquez sur Sign up pour créer un nouveau compte.

-Remplissez les informations requises,acceptez les termes et conditions.
-Cliquez sur Create account(créer un compte).

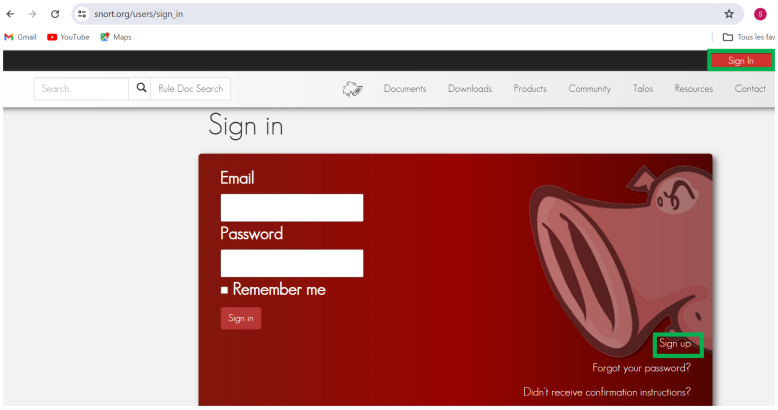

FIGURE 5.21 – Interface web Snort

Installation du Package SNORT

Pour installer le package SNORT faudra se rendre dans **systeme** puis sur **Package Manager**.

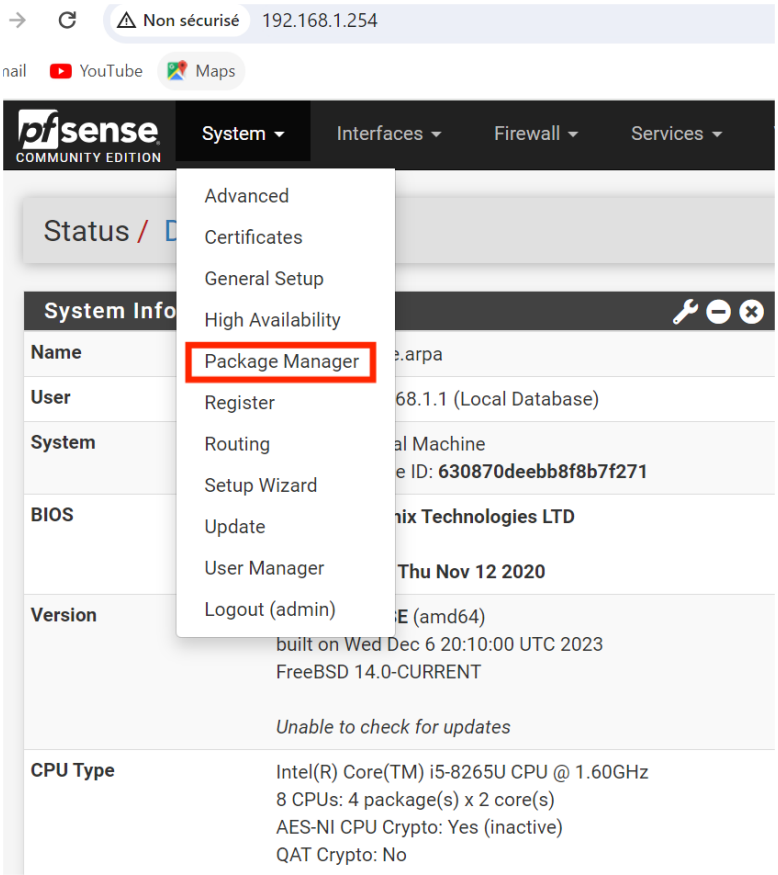

FIGURE 5.22 – Installation du package Snort 1

-D'abord faudra se rendre sur **Available Packages** pour importer et installer le package de Snort.

-Puis on retouvera le package de SNORT bien installe sur **Installed Packeges**.

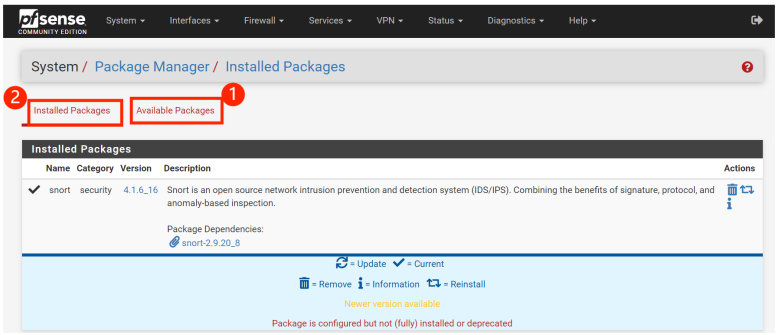

FIGURE 5.23 – Installation du Package Snort 2

-Pour vérifier l'ajout du service SNORT entrez sur le Package SNORT.

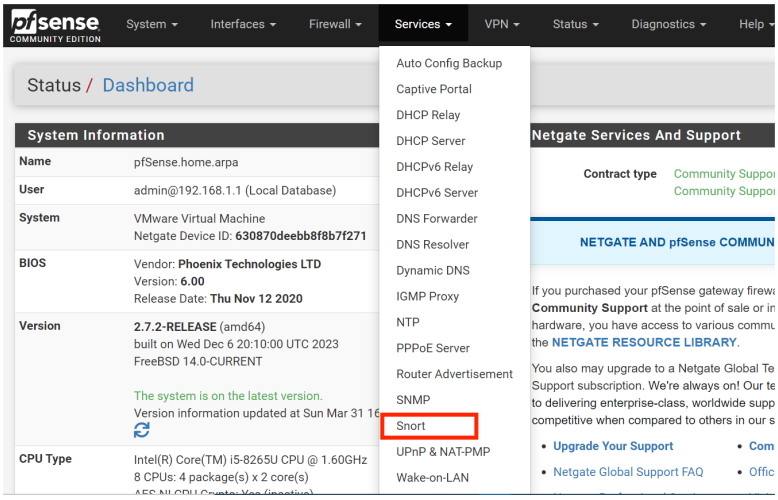

FIGURE 5.24 – L'ajoute du service Snort

Configuration de SNORT

Rendez-vous sur "General Settings" : Cette section nous permet de spécifier le comportement global de Snort, comme l'activation/désactivation des règles, l'activation des fonctionnalités d'IPS (Intrusion Prevention System) ou d'IDS (Intrusion Detection System), la spécification des actions en cas de correspondance de règles, etc.

Nous allons parcourir les différentes sections et configurer les paramètres selon vos besoins.Activer ou désactiver les options en cochant ou en décochant les cases appropriées, et saisir les valeurs requises dans les champs de texte.

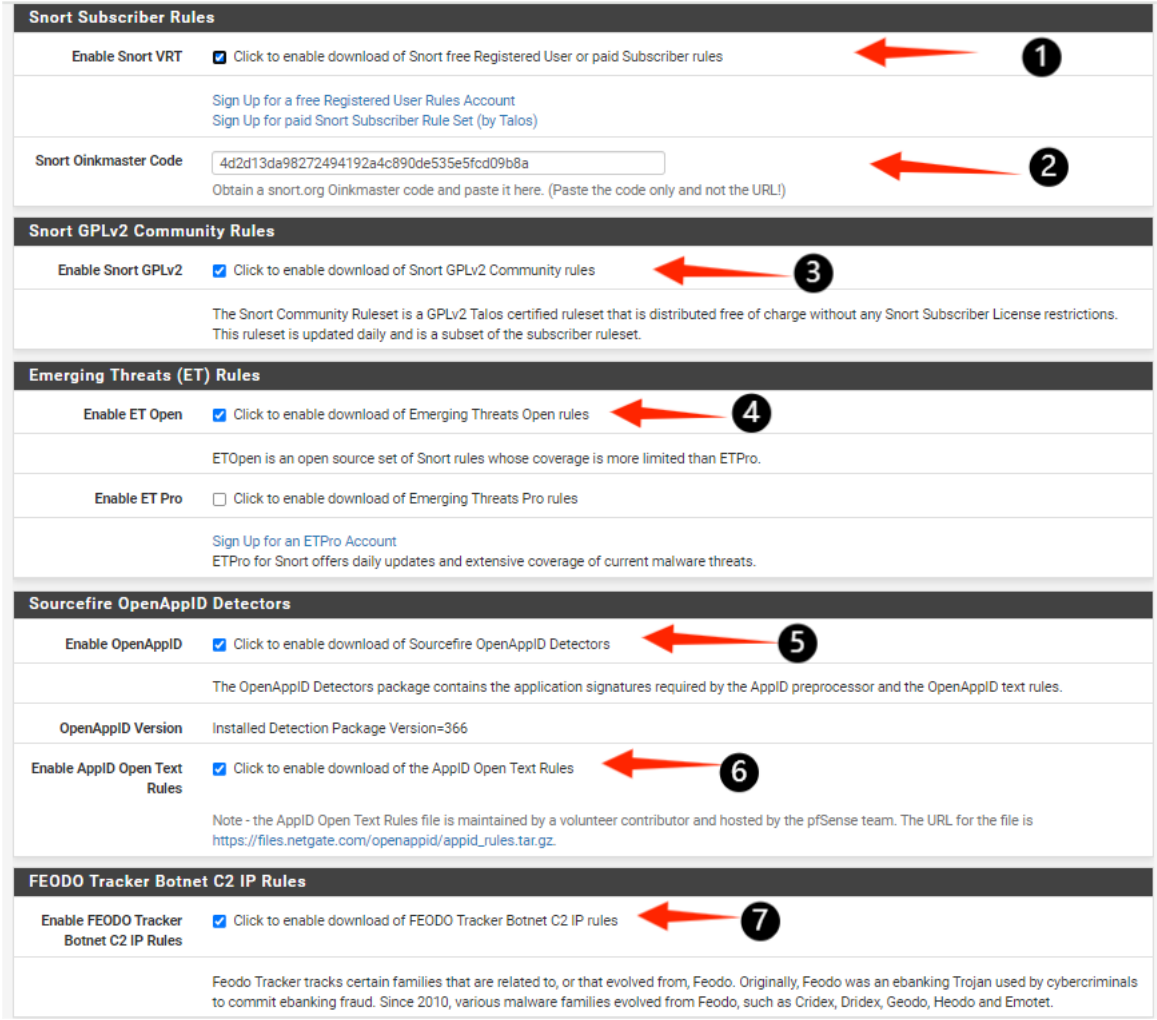

FIGURE 5.25 – Configuration de Snort étape 1

1. Activé pour l'enregistrement de SNORT en ligne
2. Clé API **Snort Oinkmaster Code** à récupérer depuis le site de snort.
3. Activer **Enable snort VRT** (Télécharger les règles gratuites fournies par Snort.
4. Activer **Enable Snort GPLv2** (Télécharger les règles communautaires).
5. Activer **Enable OpenAppID** (OpenAppID est une technologie qui permet d'identifier et de contrôler les applications utilisées sur le réseau en analysant les flux de trafic).
6. Activer **Enable AppID Open Text Rules** (permet d'activer les règles textuelles OpenAppID).
7. Activer **FEODO Tracker Botnet C2 IP Rules** (sont des règles spécifiques dans Snort qui permettent de détecter et bloquer les communications entre des machines infectées par le botnet FEODO et leurs commandes et contrôles (C2).

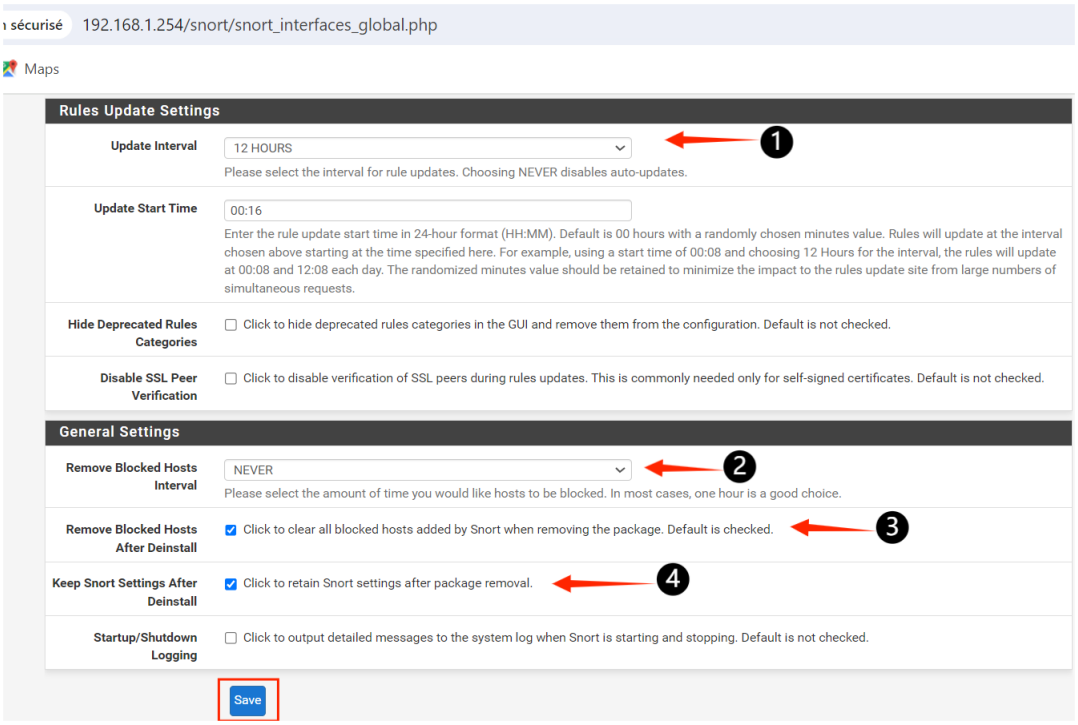

FIGURE 5.26 – Configuration de Snort étape 2

1. Mettre l'intervalle de mise à jour toutes les **12 Heures**.
2. Mettre les hôtes qui seront bloqués sur **1H**.
3. Supprimer tous les hotes ajouter par Snort lors de la désinstallation de package.
4. Garder la configuration de Snort même après la désinstallation.

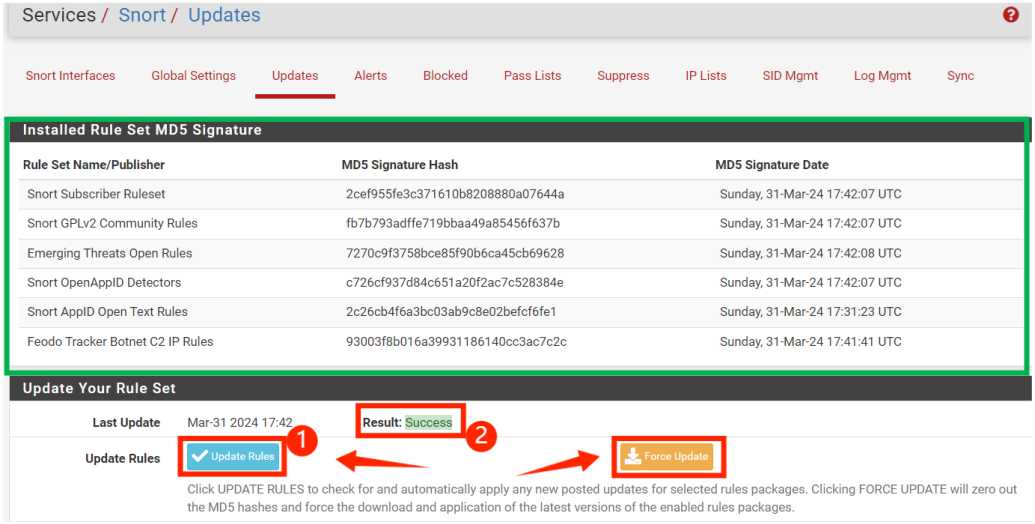

FIGURE 5.27 – Configuration de Snort étape 3

1. Cliquons sur **Uptade rules** pour importer les règles ou bien sur **Force updates** pour forcer l'importation.
   - Les règles importer sont afficher.
2. **Résultat : Success** donc les règles ont était bien importer

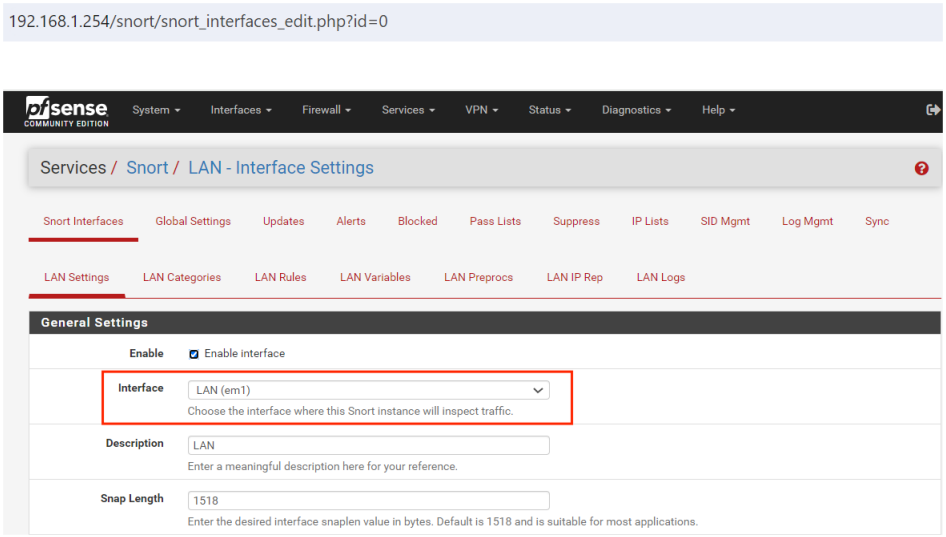

FIGURE 5.28 – Configuration de Snort étape 4

-SNORT puis sur **SNORT INTERFACES** Ajouter une interface de surveillance. LAN

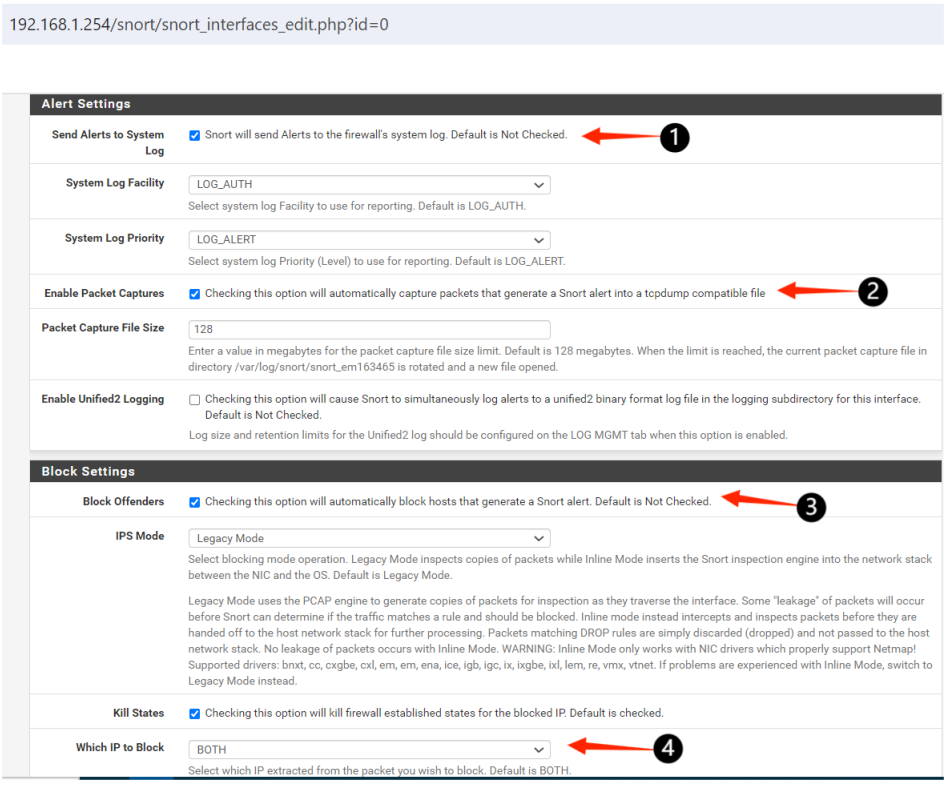

FIGURE 5.29 – Configuration de Snort étape 5

1. Activer «Send alerts to system log».
2. Activer «Enable Packet Captures».
3. Activer **Block Offenders** Bloquer les différentes machines qui peuvent poser problème/ hôtes potentiellement malicieux. Mettre Snort depuis un IDS à un IPS.
4. Activer **Kill states**
   Puis clique sur **Save** pour enregistrer toutes les etapes de configuration .

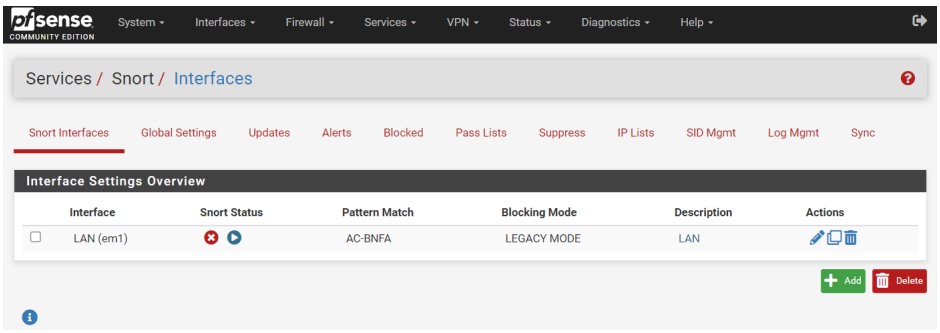

FIGURE 5.30 – Configuration de Snort étape 6

L'interface LAN a était ajouter ,les étapes suivantes explique comment la configurer .

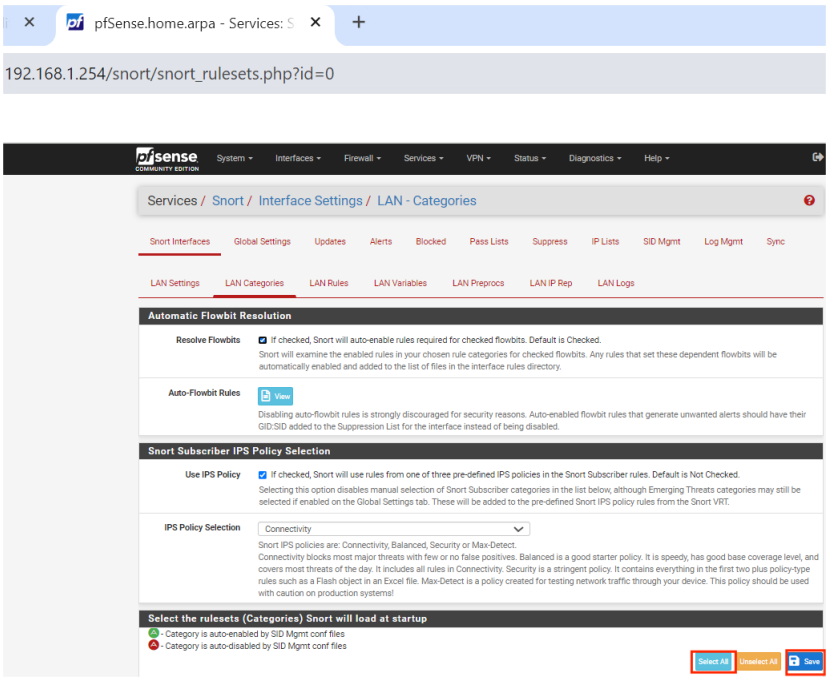

FIGURE 5.31 – Configuration de snort étape 7

Dans :Snort puis **Snort interfaces** /LAN catégories :Activer la fonctionnalité **Use IPS Policy**

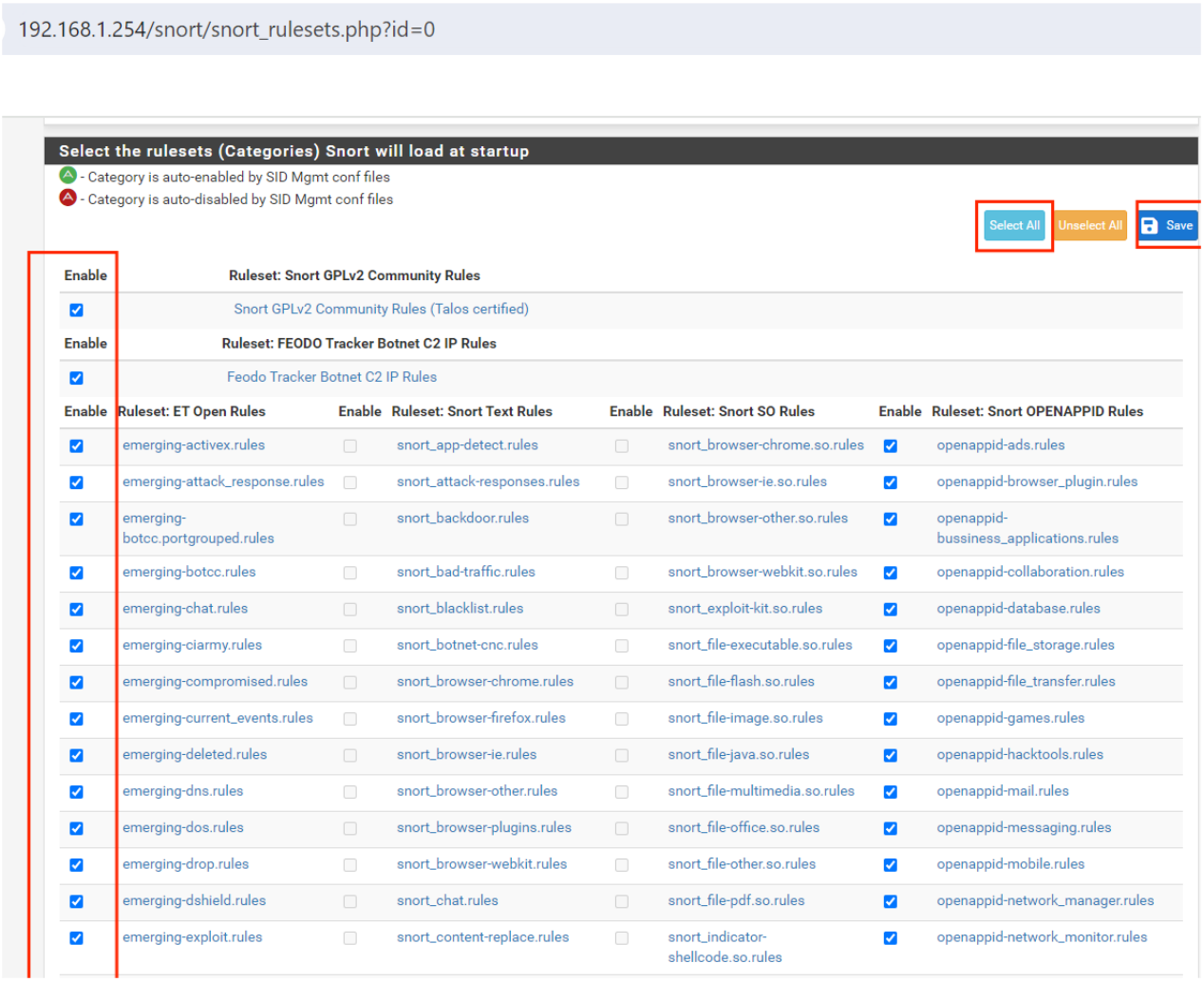

FIGURE 5.32 – Configuration de Snort étape 8

-SNORT / Snort intefaces / LAN categories : Select All. -SNORT / Snort intefaces / LAN RULES : Enable All.

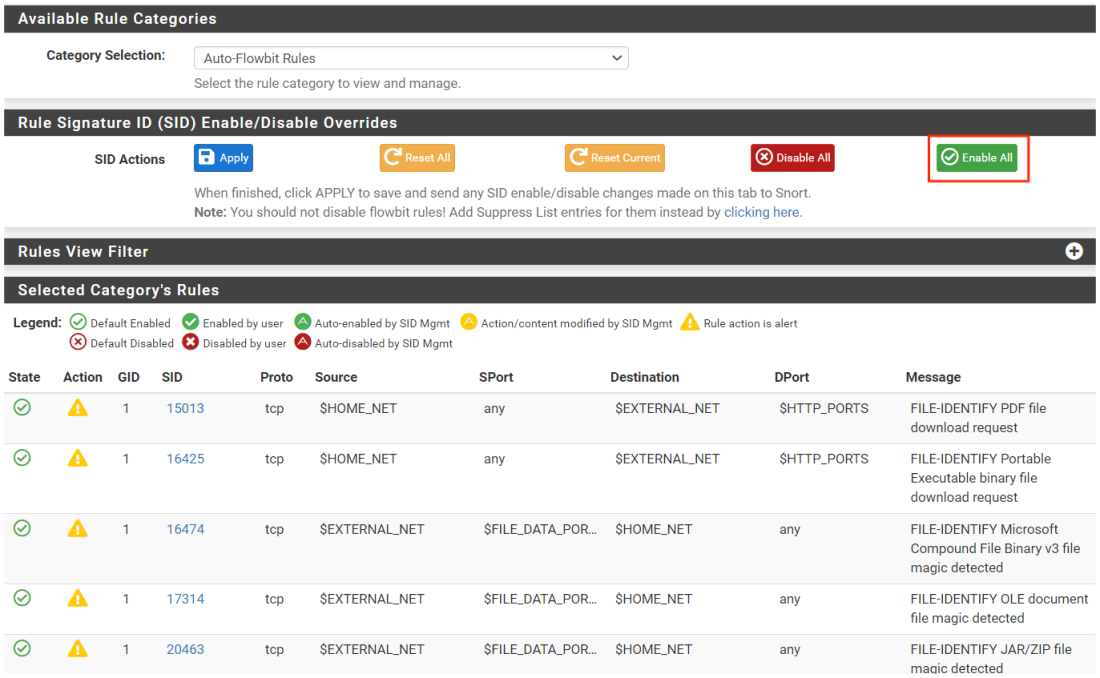

FIGURE 5.33 – Configuration de Snort étape 9

-Clicker sur **Enable all**

-Lancement de la sonde de surveillance de l'interface LAN

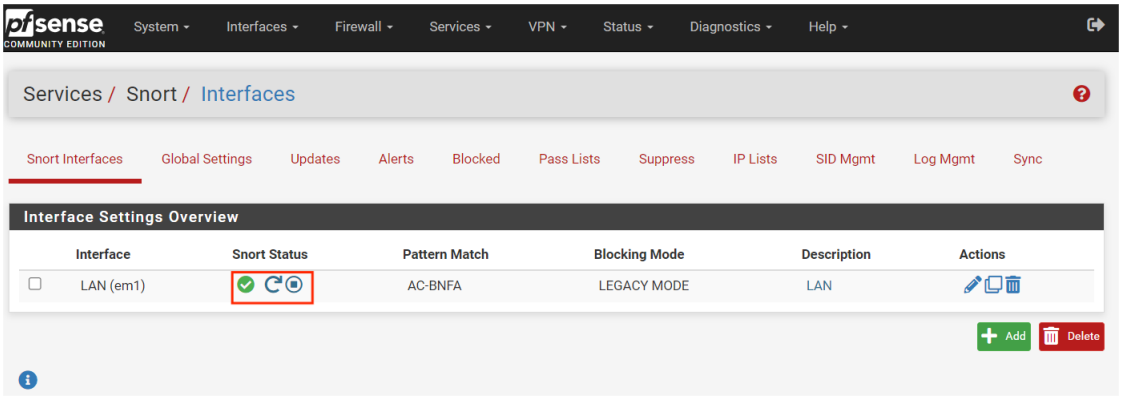

FIGURE 5.34 – Configuration de Snort étape 10

-La sonde de surveillance est activée et fonctionnelle

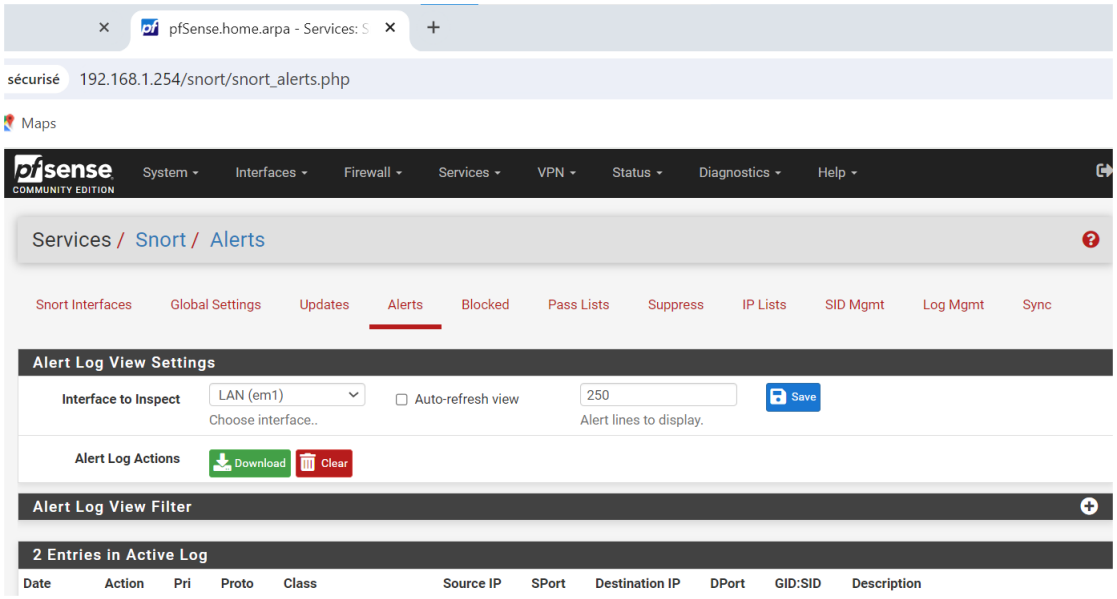

FIGURE 5.35 – Configuration de Snort étape 11

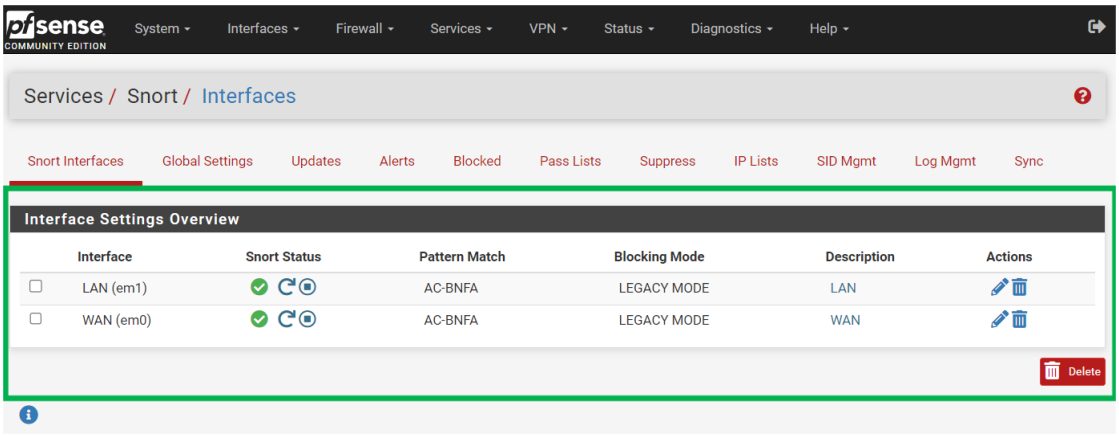

FIGURE 5.36 – Configuration de Snort étape 12

-Les deux sondes de surveillance LAN et WAN sont bien configuré.

— Les règles à appliquer sur l'interface WAN doivent être plus strictes par rapport à l'interface LAN, en raison du nombre de menaces qui peuvent provenir d'Internet tout en respectant les règles spécifiées approprié à la politique de sécurité de l'entreprise.

5.5.4 Tests et vérifications

Dans le cadre de cette étude, Des tests rigoureux ont été réalisés, comprenant des scans de ports, des tentatives d'intrusion et des attaques ciblées. Les résultats ont montré que Snort, configuré et déployé sur pfSense, a réussi à détecter et à bloquer efficacement les attaques, confirmant ainsi son rôle crucial en tant que solution de sécurité réseau fiable.

5.5.5 Réception des alertes sur la sonde LAN

Lors des tests effectués, des alertes ont été reçues sur la sonde LAN de Snort. Ces alertes ont notifié le type d'alerte, qui correspondait à une tentative d'intrusion. L'adresse IP source de l'attaque était identifiée comme étant 1.100, ce qui correspond à l'adresse IP de la machine KALI utilisée pour effectuer les tests. L'adresse IP de destination de l'attaque était répertoriée comme étant 1.254, ce qui correspond à l'adresse IP de l'interface LAN du pare-feu. Cette information permet de suivre précisément l'origine et la cible des attaques détectées par Snort.

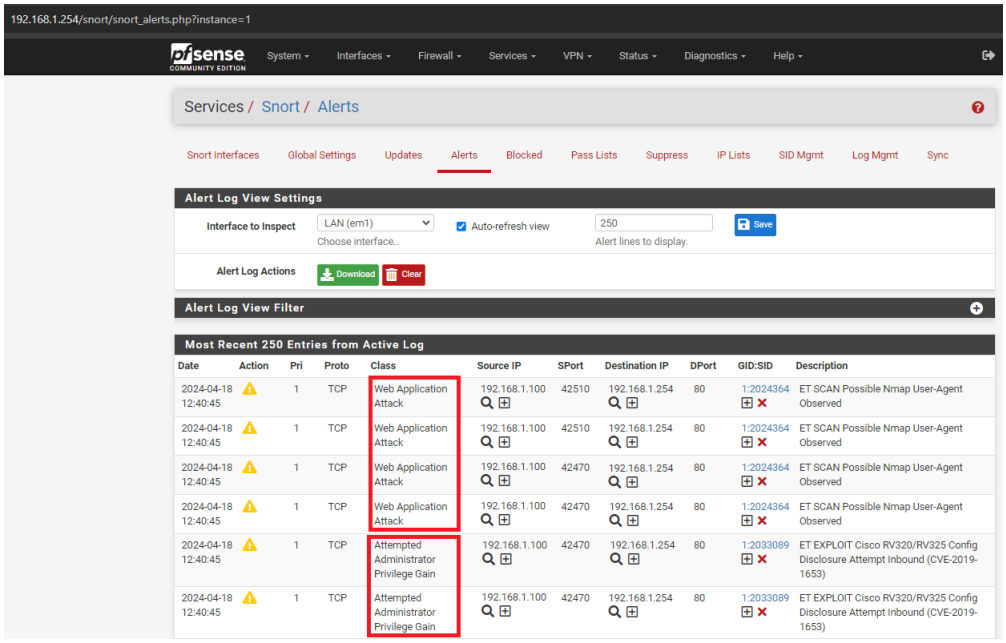

FIGURE 5.37 – Réception des alertes sur la sonde LAN

5.5.6 Réception des alertes sur la sonde WAN

Lors des tests, des alertes ont été reçues sur la sonde WAN de Snort. Ces alertes indiquaient le type d'alerte, qui correspondait à un vol d'informations. L'adresse IP source de l'attaque était identifiée comme étant 80.100, ce qui est l'adresse IP de la machine KALI lorsqu'elle est connectée au réseau WAN. L'adresse IP de destination de l'attaque était répertoriée comme étant 80.129, correspondant à l'adresse IP de l'interface WAN du pare-feu. Ces informations permettent d'identifier précisément la nature de l'attaque, ainsi que les adresses IP sources et de destination impliquées dans l'événement détecté par Snort sur la sonde WAN.

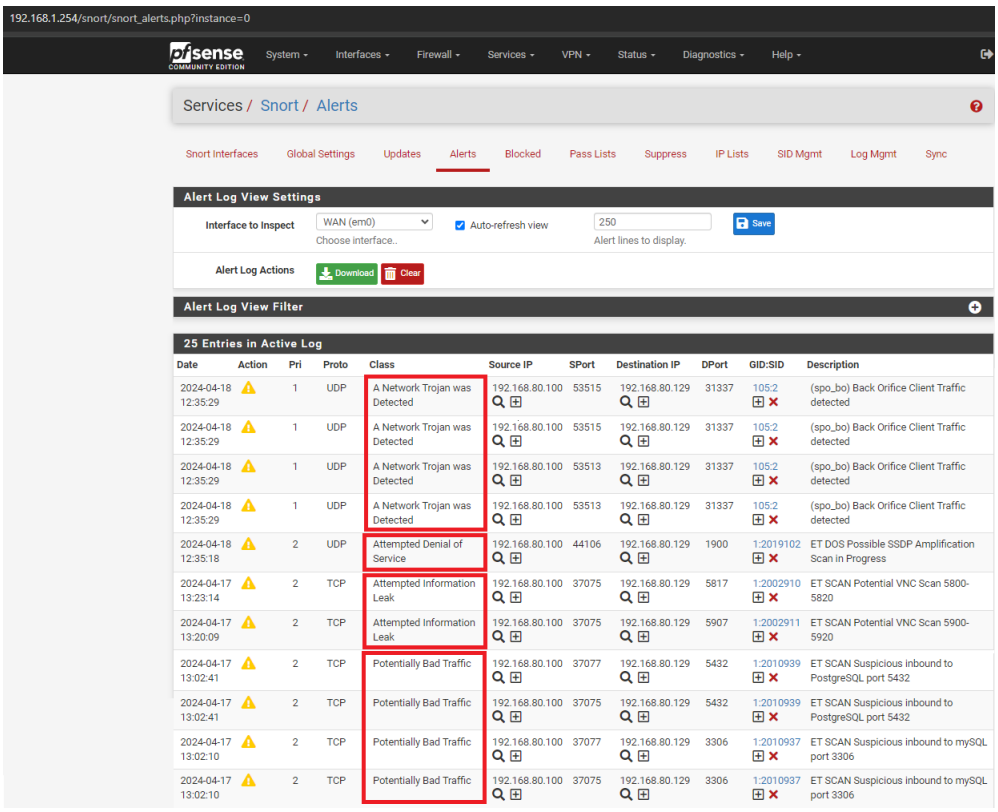

FIGURE 5.38 – Réception des alertes sur la sonde WAN

5.5.7 Blocage d'une attaque sur le par-feu du coté WAN

Deux attaques ont été détectées par Snort sur le côté WAN du pare-feu. Grâce à sa fonctionnalité de détection avancée, Snort a identifié les attaques et le pare-feu a réagi en conséquence pour bloquer ces activités malveillantes. En conséquence, les attaques ont été empêchées de pénétrer dans le réseau protégé par le pare-feu, renforçant ainsi la sécurité du système. Cette réponse proactive du pare-feu démontre son efficacité dans la détection et le blocage des attaques, contribuant ainsi à la protection globale du réseau.

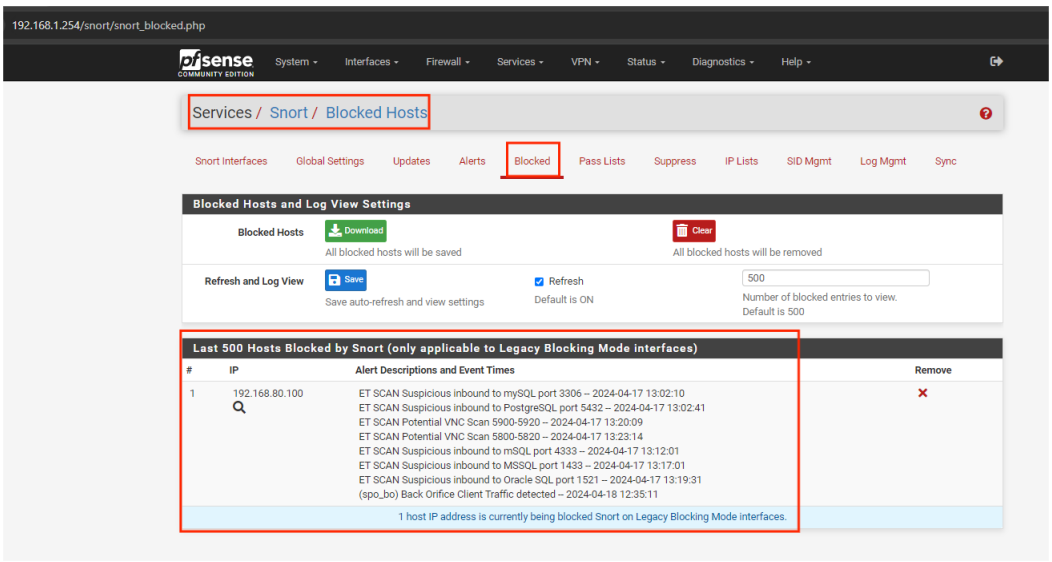

FIGURE 5.39 – Blocage d'une premier attaque sur le parefeu du cote WAN

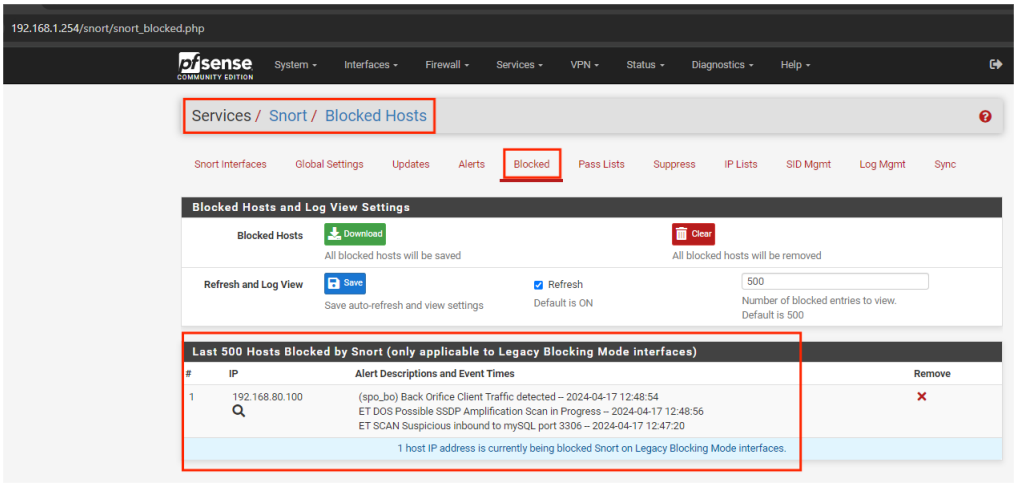

FIGURE 5.40 – Blocage d'une deuxième attaque sur le parefeu du cote WAN

Conclusion

Dans ce chapitre, nous avons présenté des outils importants pour la détection et la prévention d'intrusion. À savoir PfSense et Snort. Nous avons donné toutes les étapes d'installation et configuration de ces outils.
Enfin, nous avons procédé à plusieurs tests visant à évaluer la sécurité du réseau.

Conclusion générale

Nous voici arrivés au terme de notre recherche, encadrée par les quelques lignes et méthodologie présentes dans ce projet, portant sur la mise en place d'un système de détection et de prévention des intrusions au sein de l'entreprise Cevital.

Ce projet nous a permis d'approfondir nos connaissances, notamment en termes de configuration. De plus, nous avons enrichi notre savoir dans le domaine de la sécurité des réseaux grâce à l'implémentation d'un système de détection et de prévention des intrusions.

Cette recherche nous a conduits à découvrir l'une des mesures de sécurité essentielles à déployer pour assurer la protection d'un réseau informatique. Nous avons présenté l'aspect théorique de la sécurité des réseaux informatiques et toutes les notions qui s' rapportent. L'aspect pratique, quant à lui, a porté sur l'implémentation de la solution proposée, suivi de divers tests d'évaluation réalisés pour garantir le succès de la démarche de configuration.

La recherche souligne l'importance d'une surveillance et de mises à jour régulières du système pour rester en avance sur les menaces en constante évolution.

Dans l'ensemble, l'étude démontre l'importance d'investir dans un système de sécurité robuste pour les organisations afin de protéger leurs opérations et leurs actifs.

La mise en place d'un système de sécurité pour la détection et la prévention des intrusions est cruciale pour protéger les biens et les informations. Une solution bien conçue, intégrant pare-feu, détection d'intrusion et contrôle d'accès, offre une défense fiable. La recherche souligne l'importance de la surveillance et des mises à jour régulières pour rester efficace contre les menaces. Ce mémoire approfondit les connaissances théoriques et pratiques en sécurité informatique. En conclusion, investir dans une sécurité robuste est essentiel pour protéger les opérations et les actifs des organisations.

Références

[1] « https ://www.weodeo.com/digitalisation/reseau-informatique-comment-ca-marche, »

[2] « https ://community.fs.com/fr/article/client-server-and-peer-to-peer-networks.html, »

[3] « https ://fr.scribd.com/document/478026505/CHAPITRE-1-Generalites-sur-les-reseaux-informatique, »

[4] « https ://www.kaspersky.fr/resource center/definitions/firewall, »

[5] « https ://www.freelance-informatique.fr/actualites/reseau-informatique-equipements, »

[6] « https ://www.compufirst.com/compufirst-lab/reseau-et-telecom/qu-est-ce-qu-une-fibre-optique/main.do ?appTreeId=45685, »

[7] « A.KHIRDDINE(Réseau de Terrain)[Université A/Mira de Béjaïa], »

[8] « https ://waytolearnx.com/2017/12/difference-entre-les-protocoles-tcp-et-udp.html, »

[9] « https ://www.manageengine.com/fr/network-monitoring/network-protocols.html, »

[10] « Ghernaouti, S. (2022). Politique de sécurité. Dans S. Ghernaouti, Cybersécurité (pp. 89-122), »

[11] « https ://www.securiteinfo.com/attaques/hacking/typesattaques.shtml, »

[12] « https ://www.proofpoint.com/fr/threat-reference/computer-virus, »

[13] « https ://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1445234-ver-informatique-definition-concrete-et-illustree/, »

[14] « https ://www.altospam.com/glossaire/deni-de-service-ddos/, »

[15] D. Massicilia, « Test d'intrusion interne avec une mise en place d'une solution de sécurité, » 2015.

[16] « https ://www.kaspersky.fr/resource-center/threats/trojans, »

[17] « https ://blog.mailfence.com/fr/difference-chiffrement-symetrique-asymetrique/, »

[18] « https ://www.fortinet.com/fr/resources/cyberglossary/what-is-dmz, »

[19] « https ://www.fortinet.com/fr/resources/cyberglossary/intrusion-detection-system, »

[20] « https ://spanning.com/blog/nids-hids-intrusion-detection-systems/, »

[21] « J. Timmis. Artificial immune systems : A novel data analysis technique inspired by the immune network theory. 1999, »

[22] « Abderrahim ESSAIDI. Conception d'une zone démilitarisée (dmz). 2006-2007, »

[23] T. Burgermeister, « Les systèmes de détection d'intrusions, »

[24] « https ://www.proofpoint.com/fr/threatreference/intrusion-prevention-system-ips, »

[25] « LABEDInes.Proposition d'un système immunitaire artificiel pour la détection D'intrusions. 2005-2006, »

[26] « https ://www.ibm.com/fr-fr/topics/intrusion-prevention-system, »

[27] « Osman SALEM. La protection des réseaux contre les attaques dos., »

[28] « CHIKHAsma. Sécurité d'une application web à l'aide d'un systéme de détection d'intrusions comportementale. 2011-2012, »

[29] « https ://www.lebigdata.fr/ips-intrusion-prevention-system, »

[30] « https ://www.fortinet.com/fr/resources/cyberglossary/intrusion-detection-system , »

[31] « https ://www.fortinet.com/fr/resources/cyberglossary/snort, »

Résumé

La sécurité informatique joue un rôle crucial dans le fonctionnement des entreprises. Avec l'évolution rapide des technologies, les mécanismes de protection traditionnels deviennent insuffisants, ce qui souligne la nécessité d'implémenter un système de sécurité plus robuste et fiable.

Ce projet présente la mise en place d'un système de sécurité pour la détection et la prévention d'intrusion, La première section, axée sur la théorie, englobe une analyse des réseaux informatiques. Elle approfondit également la sécurité informatique en examinant différents types d'attaques, les menaces et les mécanismes de sécurité. Dans la seconde partie, orientée vers la pratique, l'accent est mis sur la configuration du système de détection et de prévention Snort, sur le pare-feu pfSense.

Cela nous amènera à un état avancé, soulignant l'importance d'un système de sécurité robuste pour la détection et la prévention des intrusions.

Mots clés : Sécurité informatique,Système de sécurité ,Détection d'intrusion,Prévention d'intrusion, Pare-feu,Pfsesnse,Snort,Attaque,Menaces,Configuration .

Abstract

IT security plays a crucial role in the functioning of companies. With the rapid evolution of technologies, traditional protection mechanisms are becoming insufficient, underlining the need to implement a more robust and reliable security system.

This project presents the implementation of a security system for intrusion detection and prevention, The first section, which focuses on theory, includes an analysis of computer networks. It also deepens computer security by examining different types of attacks, threats and security mechanisms. In the second practical part, the focus is on the configuration of the Snort detection and prevention system on the pfSense firewall.

This will bring us to an advanced state, highlighting the importance of a robust security system for intrusion detection and prevention.

Keywords : cybersecurity, Security System, Intrusion detection, Intrusion Prevention, Firewall, Pfsense, Snort,Attack, Threats,Configuration.