République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme de Master en Informatique.
Spécialité : Adminstration et Sécurité des Réseaux.

Thème

Etude et mise en oeuvre d'une solution de détection d'intrusion sur une infrastructure de virtualisation Cas d'étude : Entreprise Portuaire de Bejaia

---

Réalisé par :

Mlle. OUGUERGOUZ Nesrine et Mlle. OUKIL Kahina .

Evalué le 02/07/2023 devant le jury composé de :

Président	**Mr. SIDER Abderrahmane**	**U. A/Mira Béjaïa.**
Examinateur	**Mme. AZOUI Aicha**	**U. A/Mira Béjaïa.**
Encadrant	**Mlle. DJEBBAR Nacera**	**U. A/Mira Béjaïa.**

Année universitaire 2022/2023

Remerciements

Avant d'entamer notre présentation, nous souhaitons exprimer notre gratitude envers Dieu, le Tout-Puissant, de nous avoir donné la force, la persévérance et la patience nécessaires pour surmonter les difficultés et les obstacles rencontrés lors de la réalisation de ce projet. Sa bonté et sa miséricorde nous ont guidés tout au long de ce processus, et nous lui sommes reconnaissantes pour sa grâce.

Nous souhaitons exprimer nos sincères remerciements à toutes les personnes qui ont contribué, de différentes manières, à la réalisation de ce travail. En premier lieu, nous exprimons notre gratitude envers notre encadrante, Mlle DJEBBAR Nacera, d'avoir accepté de nous encadrer. Sa patience et son explications claires ont été une source d'inspiration, et nous sommes honorées d'avoir pu travailler avec elle. Nous la remercions infiniment pour sa disponibilité, son implication et sa réactivité lors de la relecture et ses corrections, malgré son emploi du temps chargé.

Nous tenons également à remercier le personnel de l'organisme d'accueil de l'Entreprise Portuaire de Bejaia (EPB) pour son accueil chaleureux lors de notre stage pratique.

Nous adressons nos remerciements aux membres du jury qui ont accepté la lourde tâche de lire l'intégralité de ce manuscrit et de participer à notre soutenance, en nous accordant de leur temps.

Nous souhaitons également exprimer notre profonde gratitude envers tous les professeurs et enseignants qui nous ont accompagnés tout au long de notre parcours académique.

Enfin, nous voulons exprimer notre sincère reconnaissance à nos chers parents et à nos familles pour leur soutien constant, leurs sacrifices et leurs encouragements qui ont été essentiels pour nous permettre de poursuivre nos études dans les meilleures conditions.

Dédicaces

Nous dédions humblement ce modeste travail :

À nos chers parents, nos frères, nos sœurs et à tous les membres de nos familles pour leur soutien et leurs sacrifices

À tous nos amis avec qui nous avons partagé des moments forts dans notre vie

À tous ceux qui nous ont aidés directement ou indirectement à réaliser ce projet

Enfin, à toutes les personnes que nous aimons et qui nous aiment

NESRINE ET KAHINA

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

APP Developpement	Développement d'applications mobiles
Chroot	Change Root
CRM	Customer Relationship Management
CNA	Compagne Nationale Algerienne de Navigation
CMS	Conversational Monitor System
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
DSI	Direction de Systeme d'Information
ERP	Entreprise Ressource Planning
ESXI	Elastic Sky X integrated
ESX	Elastic Sky X
EPB	Entreprise Portuaire de Bejaia
EPE	Entreprise Publique Economique
FTP	File Transfer Protocol
GED	Gestion Eléctronique De Documents
GPL	General Public Licence
HA	Hosted Architecture
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines
CMS	Conversational Monitor System
IDS	Intrusion detection System
IOB	Input-Output Board
IP	Internet Protocol
IPS	Intrusion prevention system
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
L2TP	Layer 2 tunneling Protocol
MAC	Media Access Control
MAC OS	Macintosh Operating System
NAS	Network Attached Storage
NIST	National Institute of Standards and Technology
OHSAS	Occupational Health and Safety Assessment Series
ONP	Offre National Des pont
OSI	Open Systems Interconnexion
OS	Operating System
PC	Personnel Computer
PPTP	Point-to-Point Tunneling Protocol
SNM	Société Nationale de Manutention

SPA	Société Par Action
SI	Système d'Information
SSD	Solid State Drive
SW	Switch
TCO	Total Cost of Ownership
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VM	Machine Virtuel
VMM	Virtual Machine Monitor
VSwitch	Virtual Switch
VPN	Virtual Private Network
WMAX	Worldwide Interopérabilité for Microware Access
VMFS	Virtual Machine File System
WAN	Wide Area Network
WIFI	Wireless Fidelity
Xfce	XForms Common Environment

Introduction générale

Au fil des années, les entreprises ont de plus en plus adopté la virtualisation pour améliorer leur efficacité opérationnelle, réduire les coûts et offrir des services flexibles à leurs clients. Cependant, les préoccupations relatives à la sécurité et à la confidentialité des données ont empêché certaines entreprises d'adopter certains services.[5][14]

La virtualisation est maintenant une technologie essentielle, offrant une flexibilité accrue et une gestion plus efficace des ressources informatiques. Elle permet de créer des environnements sécurisés pour les applications et les données, offrant ainsi aux entreprises un niveau de contrôle et de personnalisation élevé.

Malgré la mise en place de mesures de sécurité, la protection demeure une préoccupation majeure, en particulier pour les réseaux virtuels. Il est crucial de mettre en place des solutions de sécurité robustes afin de protéger les environnements virtuels contre les cyberattaques[17]. En combinant des mesures telles que le contrôle d'accès, le chiffrement des données, la segmentation du réseau, la surveillance et la détection des intrusions, ainsi que la gestion des correctifs et des vulnérabilités, les entreprises peuvent renforcer la sécurité de leurs environnements et réduire les risques liés à la confidentialité et à la sécurité des données.

Dans ce contexte, la présente recherche se focalise sur l'étude d'une solution de détection d'intrusion sur une infrastructure de virtualisation. Elle est organisée en quatre chapitres et conclue par une conclusion générale :

— **Chapitre 1 :** Fournit une base solide pour la compréhension de l'infrastructure informatique en explorant les différentes solutions de virtualisation et les avantages qu'elles offrent.

— **Chapitre 2 :**Se concentre sur une analyse approfondie des éléments essentiels lié à la sécurité dans les réseaux et dans les environnements virtuels en particulier et les principales précautions à prendre.

— **Chapitre 3 :**Porte sur la présentation de l'organisme d'accueil EBP, en mettant en évidence la problématique liée à l'insuffisance de la sécurité de leur réseau.

— **Chapitre 4 :** Le quatrième et dernier chapitre porte sur la mise en oeuvre de la solution .

— **Conclusion générale :** Nous récapitulerons les points clés de ce mémoire et envisagerons des perspectives pour l'avenir de ce projet.

Chapitre 1

Infrastructure et virtualisation

1.1 Introduction

Ce chapitre offre une base solide pour découvrir de plus près l'infrastructure informatique et ses différents composants en s'appuyant sur la virtualisation qui est la base de notre mémoire. Nous explorons les principes fondamentaux et ses nombreux avantages , tels que la consolidation des ressources et la réduction des coûts.Nous indiquant aussi ses différents types et solutions,en mettant en évidence la VMware utilisée dans la partie réalisation.

1.2 Infrastructure informatique

L'infrastructure informatique d'une entreprise englobe l'ensemble des composants matériels et logiciels inter-connectés qui permettent le fonctionnement de son système informatique.

Cela comprend les serveurs, les ordinateurs, les équipements réseaux, les logiciels,les périphériques ,la virtualsation et autres équipements essentiels [1][2] .

L'infrastructure informatique a pour objectif de connecter tous ces éléments entre eux efficacement et en toute sécurité pour offrir une disponibilité maximale aux collaborateurs [3].

1.2.1 Composants matériels

Cela englobe tout les composants physiques utilisés dans le domaine de l'informatique ce qui inclut [4][5] :

1.2.1.1 Les datacenters

Un centre de données ou datacenter, est une installation qui permet aux entreprises et aux organisations de stocker, traiter et diffuser de grandes quantités de données. Les applications, les services et les données contenues dans un datacenter sont essentiels pour les opérations quotidiennes d'une entreprise, ce qui fait un élément central et un actif critique. les composants d'un datacenter comprennent :

— Les serveurs et les dispositifs de stockage stockent et traitent les données.

— Les équipements réseau permettent aux données de circuler dans le centre de données et d'interagir avec d'autres centres de données.

— Les systèmes de refroidissement maintiennent une température optimale pour les équipements électroniques.

— Les systèmes d'alimentation électrique de secours garantissent que les serveurs et les dispositifs de stockage continuent de fonctionner en cas de panne de courant.

— Les systèmes de sécurité physique protègent les données contre les intrusions et les vols.

— Les systèmes de surveillance permettent aux opératteurs du centre de données de surveiller les équipements et de détecter les problèmes potentiels .

1.2.1.2 Les ordinateurs

L'ordinateur se définit maintenant comme une machine de traitement de l'information, et normalement capable d'acquérir et de conserver des informations, d'effectuer des traitements et restituer les informations stockées.exemple : ordinateur portable , de bureau , de poche..

1.2.1.3 Les périphériques

Il existe différents types de périphériques que l'on classe généralement en 03 types :

— Les périphériques d'entrée comme le clavier.

— Les périphériques de sortie comme l'imprimante.

— Les périphériques d'entrée-sortie comme la clé USB.

1.2.1.4 Les appareils de stockage

Un appareil de stockage est un dispositif utilisé pour stocker des données de manière permanente ou temporaire,comme le disque dur.

1.2.1.5 Les serveurs

Un serveur est un composant clé de l'infrastructure informatique, offrant des services essentiels aux utilisateurs et aux systèmes connectés. Il exécute des opérations en réponse aux requêtes émises par un autre ordinateur appelé "client", C'est pourquoi on parle souvent de la relation "client/serveur".

En théorie, un ordinateur est considéré comme un serveur dès lors qu'il partage des ressources avec une machine cliente [6].

Il existe différents types de serveurs en fonction des services qu'ils fournissent et des tâches qu'ils exécutent. Le tableau ci-dessous résume quelques définitions associé à chaque type de serveur :

Type de Serveur	Explication
Serveur web	Héberge des sites web et les rend accessibles aux utilisateurs via un navigateur.
Serveur de fichiers	Stocke et partage des fichiers au sein d'un réseau pour faciliter l'accès et la gestion centralisée.
Serveur de messagerie	Gère l'envoi, la réception et le stockage des e-mails.
Serveur de base de données	Stocke et gère les données de manière structurée pour les applications.
Serveur de supervision et d'administration	Surveille, contrôle et gère les ressources du réseau.
Serveur de sauvegarde	Effectue des sauvegardes régulières des données pour garantir leur protection.
Serveur d'applications	Fournit un environnement d'exécution pour les applications logicielles.
Serveur d'impressions	Gère les demandes d'impression et contrôle les imprimantes connectées au réseau.
Serveur DNS	Traduit les noms de domaine en adresses IP pour localiser les ressources sur Internet.
Serveur de virtualisation	Crée et gère des machines virtuelles pour consolider les ressources matérielles.
Serveur proxy	Filtre et sécurise les requêtes entre les clients et les serveurs cibles.

TABLE 1.1 – Les types de serveurs[10].

1.2.2 Les réseaux

Les réseaux permettent la connectivité entre les différents appareils et composants de l'infrastructure informatique.

Voici quelques exemples[10][12][20] :

1.2.2.1 Les routeurs

Un routeur est un appareil utilisé pour diriger le trafic réseau entre différents réseaux informatiques. Il permet de connecter plusieurs appareils à un réseau local (LAN) et de les relier à un réseau étendu (WAN) tel qu'Internet.

1.2.2.2 Les commutateurs

Un commutateur, également connu sous le nom de switch, est un appareil réseau qui permet de connecter plusieurs appareils au sein d'un réseau local (LAN).

1.2.2.3 Les câbles

Les câbles sont des conducteurs utilisés pour transmettre des signaux électriques ou optiques d'un appareil à un autre. Voici quelques types courants de câbles :

— Câble Ethernet.

— Câble coaxial.

— Câble à paires torsadées.

1.2.2.4 Les protocoles de communication

Les protocoles de communication sont des règles et des normes qui permettent à différents appareils et systèmes informatiques de communiquer entre eux. Ils définissent la façon dont les données sont échangées et transmises entre les appareils connectés.

Il existe de nombreux protocoles de communication différents, chacun ayant des fonctions et des caractéristiques uniques. Certains des protocoles les plus courants sont TCP/IP, HTTP, FTP, SMTP et POP3.

1.2.3 Composants logiciels

Les logiciels sont des programmes et des applications exécutés sur le matériel informatique pour accomplir des tâches spécifiques. Ils comprennent les systèmes d'exploitation tels que Windows, macOS et Linux, qui servent d'interface entre le matériel et les autres logiciels.

Les applications logicielles, telles que les suites bureautiques, les logiciels de conception graphique, les navigateurs web et les outils de gestion de projet, sont conçues pour des besoins particuliers. Les bases de données, quant à elles, sont essentielles pour le stockage, l'organisation et la gestion des données [7].

Nous presentons ci-dessous quelques exemple[8] :

— **Les systèmes d'exploitation :** tels que Windows, macOS, Linux, fournissent une interface entre les utilisateurs et le matériel.

— **Les applications d'entreprise :**Ce sont les programmes et les applications spécifiques utilisés pour effectuer des tâches et des activités particulières,comme la gestion de base de donnée.

1.2.4 Les dimensions majeures de l'infrastructure informatique

L'infrastructure informatique repose sur différentes dimensions majeures qui sont essentielles à son bon fonctionnement. Chacune de ces dimensions joue un rôle crucial dans la création, la gestion et la sécurisation des systèmes informatiques et des réseaux.

La figure ci-dessous illustre les quatre dimensions clés de l'infrastructure informatique [5] :

FIGURE 1.1 – Les dimensions majeures de l'infrastructure informatique.

1.2.4.1 La dimension Utilisateur

Il s'agit du matériel mis à disposition des collaborateurs, principalement des ordinateurs fixes, des PC et des téléphones mobiles. Ce matériel peut être utilisé à la fois au sein de l'organisation et à distance, notamment dans le cadre du télétravail[12][15].

1.2.4.2 La dimension Cloud

Elle fait référence aux solutions hébergées en dehors de l'organisation. Cela inclut les sauvegardes, les machines virtuelles et la téléphonie unifiée via un Cloud privé ou public. On peut également mentionner les solutions de téléphonie IP et les solutions collaboratives telles que Office 365[12][15[18].

1.2.4.3 La dimension Réseau

Elle englobe les composantes réseau de l'organisation, notamment l'accès à Internet. Elle comprend également les pare-feu, les commutateurs, le réseau sans fil, les logiciels antivirus, ainsi que les outils de gestion du matériel à distance[12][15].

1.2.4.4 La dimension Système local

Certaines organisations préfèrent conserver un système de sauvegarde locale sur leurs propres serveurs en local. Cela leur permet d'avoir un contrôle direct sur leurs sauvegardes et de stocker les données localement plutôt que de les externaliser dans le cloud [25].

1.3 La virtualisation

1.3.1 La définition de la virtualisation

La virtualisation est une technique informatique qui permet de simuler des ressources physiques telles que des ordinateurs , des serveurs, des processeurs, des réseaux et des applications en permettant des environnements virtuels".

Cela permet d'utiliser de manière plus efficace les ressources connues et de répondre à différents besoins tels que le développement de logiciels, les tests, la formation, la consolidation de serveurs ou la gestion de la sécurité informatique.

La virtualisation est donc une technique clé pour améliorer la flexibilité, la résilience, la sécurité et la rentabilité des infrastructures informatiques [5][1][23][24].

1.3.2 Histoire de la virtualisation

A l'heure actuelle, la virtualisation est très connue. On entend parler de virtualisation de serveur, de Virtualbox, du cloud de baremetal, mais aussi de virtualisation de poste de travail, de VDI, et de virtualisation dans les jeux-vidéos avec les émulateurs.

La figure ci-dessus représente l'évolution de la virtualisation en fonction des années :

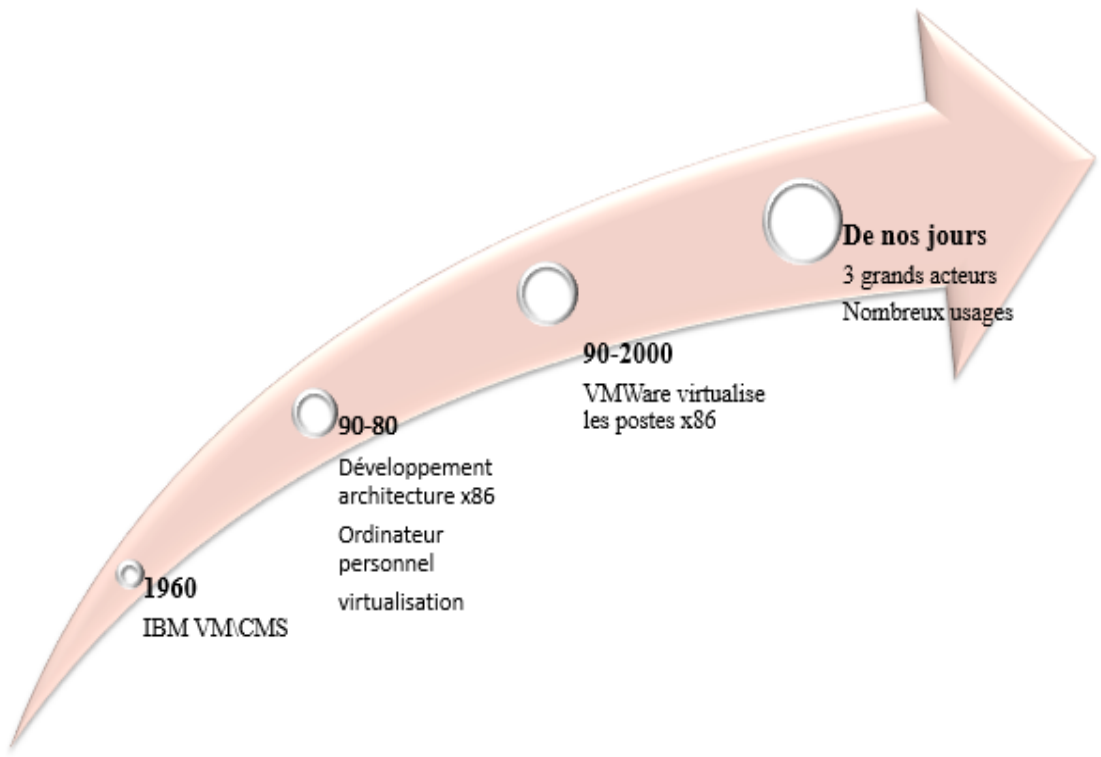

FIGURE 1.2 – Historique de la virtualisation.

1.3.3 Architecture

La virtualisation repose essentiellement sur un système appelé hyperviseur qui peut être un logiciel ou un système d'exploitation .

1.3.3.1 Les hyperviseurs

Un hyperviseur est une couche logicielle qui permet de créer et de gérer des machines virtuelles (VM). Il isole le système d'exploitation hôte et ses ressources des machines virtuelles exécutées sur celui-ci.

Il existe deux types principaux d'hyperviseurs comme le montre la figure ci dessus :

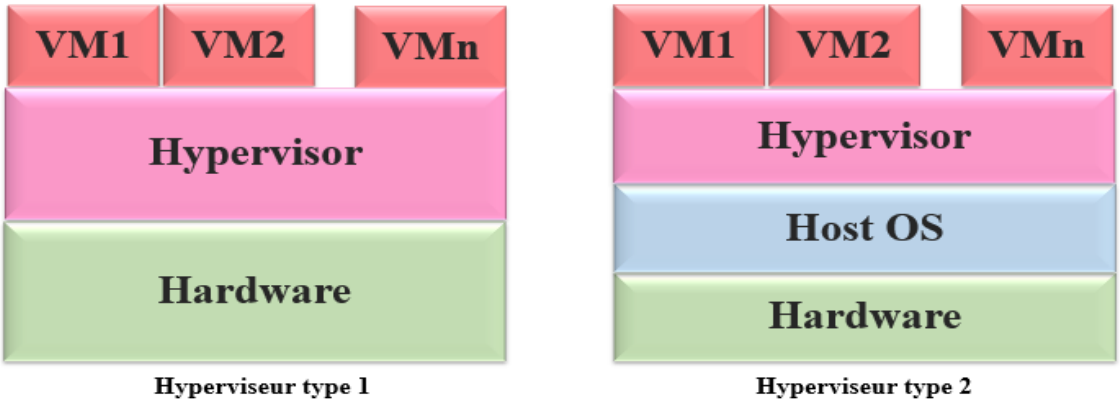

FIGURE 1.3 – Les types d'hyperviseurs.

Le tableau ci-dessous résume les descriptions de chaque type d'hyperviseur et mets en évidence des exemples associé à chacun :

Type d'hyperviseur	**Désignation**	**Description**	**Exemple**
Hyperviseur de type 1	native ou "bare-metal"	L'hyperviseur de type 1 s'installe directement sur la couche matérielle du serveur pour se concentrer sur la gestion des SE invités. Cela permet une utilisation plus efficace des ressources des serveurs et une meilleure performance des VM.	Hyper-V de chez Microsoft, ESXi de chez VMware...
Hyperviseur de type 2	hébergé ou "hosted"	L'hyperviseur de type 2 s'installe et s'exécute sur un SE existant. cela permet une utilisation plus flexible des ressources, mais peut entraîner une perte de performance par rapport a l'hyperviseur de type 1.	VMware Workstation, VirtualBox...

TABLE 1.2 – Les types d'hyperviseurs

1.3.3.2 Machine vertuelle VM

Les machines virtuelles sont des instances isolées qui fonctionnent comme des systèmes informatiques complets. Chaque machine virtuelle a son propre système d'exploitation, ses applications et ses ressources virtuelles attribuées. Elles sont exécutées sur l'hyperviseur et partagent les ressources physiques du serveur hôte [15].

1.3.3.3 Système d'exploitation invité virtuel (OS)

Un système d'exploitation invité virtuel (Guest OS) est le système d'exploitation installé au sein d'une machine virtuelle (VM) dans un environnement de virtualisation. Chaque

machine virtuelle peut exécuter son propre système d'exploitation invité, indépendamment des autres machines virtuelles et du système d'exploitation de l'hôte [5].

1.3.3.4 Commutateur virtuel

Un commutateur virtuel (vSwitch) facilite la communication entre les machines virtuelles en gérant intelligemment les paquets de données. Il peut être intégré dans les logiciels installés ou dans le matériel du serveur ,il consolide les commutateurs physiques en un seul commutateur logique, améliorant ainsi la bande passante et la connectivité [5][15].

1.3.3.5 Stockage virtuel

Le stockage virtuel regroupe les disques physiques provenant de plusieurs périphériques de stockage en réseau, en un seul périphérique de stockage logique tels que des disques durs, des SSD ou des systèmes de stockage en réseau (NAS), géré depuis une console centrale [1][5]. Cette technologie permet une gestion plus efficace des ressources , une allocation flexible de l'espace et offre des avantages en termes de performances, de redondance et de scalabilité [5][1][15].

1.3.4 Le fonctionnement

Le fonctionnement de la virtualisation repose sur trois éléments clés : Le système hôte, l'hyperviseur et le système invité.

— **Système hôte :** Un système hôte est la machine physique qui héberge et exécute les machines virtuelles [16].

— **Hyperviseur :** L'hyperviseur offre une couche d'abstraction entre les machines virtuelles et le matériel physique de l'hôte. Il facilite l'exécution des systèmes invités sur ce dernier, en gérant leur fonctionnement et en assurant leur isolation les uns des autres [16].

— **Système invité :** Le système invité fait référence à l'instance du système d'exploitation qui est exécutée dans l'environnement virtuel du système hôte.Il est également connu sous le nom de machine virtuelle [16].

1.3.5 Les approches de la virtualisation

La virtualisation est une technologie clé dans le domaine du Cloud Computing. Elle permet de créer des environnements virtuels isolés à partir des ressources physiques, ce qui offre une flexibilité et une efficacité accrues dans la gestion des infrastructures informatiques. Voici quelques approches courantes de la virtualisation [13][21] :

1.3.5.1 Les isolateurs ou le cloisonnement

Le cloisonnement est une pratique courante visant à isoler les processus sur un même système d'exploitation. Il améliore la sécurité en créant des conteneurs où les processus sont strictement confinés et ne peuvent pas sortir.

Différentes technologies de cloisonnement existent, allant d'un environnement minimal à une image complète du système. Les systèmes basés sur UNIX, tels que chroot et jail,

offrent des méthodes d'isolation, tandis que Solaris propose des zones plus avancées. Ces technologies maintiennent la même instance du système d'exploitation pour les processus isolés.

Le cloisonnement est également utilisé dans d'autres domaines, comme le sandboxing pour les programmes Java. Bien que la virtualisation soit récente, son concept existe depuis longtemps dans le domaine informatique[18][22].

1.3.6 Les différents types de virtualisation

Le tableau 1.3 représente les deux catégories de la virtualisation, telle que chacune est divisée en 3 types : [5]

Virtualisation des serveurs			
Type	**Description**	**Avantages**	**Inconvénients**
Virtualisation complète	Elle offre une simulation complète de l'ensemble du matériel sous-jacent, permettant à plusieurs systèmes d'exploitation de s'exécuter de manière isolée sur un même ordinateur.	Elle garantit l'intégrité totale de chaque MV et du VMM.	Il est important d'avoir une bonne combinaison de matériel et de logiciel pour une visualisation efficace.
Paravirtualisation	Elle permet de simuler partiellement le matériel sous-jacent, permettant à plusieurs systèmes d'exploitation de s'exécuter de manière isolée sur un même ordinateur.	Les VMs les plus puissantes en entrée/sortie réseau et disque.	Les VMs souffrent d'un manque de rétrocompatibilité, ce qui les rend peu portable.
Virtualisation de L'OS	permet de créer une unique instance du système d'exploitation.	Elle a tendance à être efficace car c'est une installation OS unique pour la gestion et les mises à jour.	Un manque de prise en charge des environnements mixtes comme windows et linux. De plus , elles ne sont pas aussi sécurisées et isolées que d'autres formes de virtualisation.
Virtualisation des ressources			
Type	**Description**	**Avantages**	**Inconvénients**
Virtualisation de stockage	Elle regroupe plusieurs lecteurs de disques physiques en une seule entité.	Offre des solutions de stockage très performantes.	Leur utilisation peut introduire des problèmes de complexité, d'interopérabilité, d'évolutivité.
Virtualisation du réseau	Permet de créer plusieurs réseaux virtuels sur une seule infrastructure physique, simplifiant ainsi la gestion du réseau et réduisant les coûts liés à l'infrastructure réseau.	Utilisation simple de réseau et accès personnalisé à l'essentiel de réseau.	Elle introduit un haut degré de complexité et de surcharge de performance.
Virtualisation d'applications	Elle permet d'exécuter une application serveur sur le bureau de l'utilisateur, la virtualisation bureautique et le streaming applicatif sont inclus dans cette catégorie.	Elle permet de créer des applications préemballées pour l'accès instantané des utilisateurs.	La virtualisation peut être limitée dans sa capacité à virtualiser tous les types de logiciels.

TABLE 1.3 – Types de virtualisation

1.3.7 Solution de la virtualisation

Nous allons vous présenter les principales solutions de virtualisation largement utilisées, notamment QEMU,Xen, KVM et VMware [11][24][25][26].

1.3.7.1 Definition de la QEMU

QEMU est utilisé comme technologie de virtualisation sous-jacente pour des plateformes telles que KVM et VirtualBox. sous licence GNU GPL, est un logiciel de virtualisation complète disponible sur les principales plates-formes telles que Microsoft Windows, GNU/Linux et Mac OS X. Ce qui rend QEMU unique, c'est sa simplicité d'utilisation.

En effet, en tant que projet de virtualisation complète, il suffit d'exécuter un programme sur le système hôte pour créer une nouvelle machine virtuelle avec un système invité. L'un des avantages majeurs de QEMU réside dans sa grande flexibilité, offrant des options de configuration de la machine virtuelle qui peuvent être adaptées selon les besoins spécifiques.

1.3.7.2 Définition de la Xen

Xen, un projet de virtualisation par hyperviseur, est géré par la société XenSource. À l'origine, ce projet était mené au sein de l'Université de Cambridge sous le nom de Xenoserver.

Son objectif initial était de permettre l'hébergement de 100 systèmes invités sur une seule machine physique, tout en offrant des performances optimales. Le nom "Xen" lui-même provient du mot grec "xenos", signifiant "étranger".

1.3.7.3 Définition de la KVM

KVM est un projet de virtualisation complète qui tire parti des instructions de virtualisation des processeurs x86 récents. Sur le plan technique, KVM se compose de deux éléments principaux :Un module noyau ,Un programme utilisateur.

Ainsi, la partie utilisateur de KVM est une adaptation spécifique de QEMU permettant une intégration harmonieuse avec le module noyau, afin de bénéficier pleinement des fonctionnalités de virtualisation offertes par le processeur.

1.3.7.4 Définition de la VMware

VMware est un projet de virtualisation par hyperviseur qui permet de créer et de gérer des machines virtuelles sur des serveurs physiques, offrant ainsi une consolidation des ressources, une flexibilité opérationnelle et une haute disponibilité des applications dans les environnements informatiques.

Elle offre une plateforme complète de virtualisation comprenant des fonctionnalités avancées de stockage, de réseau et de sécurité.

1.4 Conclusion :

Après avoir examiné les différents aspects de la virtualisation et ses nombreuses solutions, nous avons opté pour VMware car elle représente une plateforme complète avec des

fonctionnalités avancées de stockage, réseau et sécurité. Grâce à VMware, nous pouvons consolider les ressources, bénéficier d'une flexibilité opérationnelle et assurer la sécurité de nos environnements virtuels.

Le prochain chapitre portera sur la sécurité dans les réseaux informatiques.

Chapitre 2

Sécurité dans les réseaux informatiques

2.1 Introduction

Ce chapitre vise à fournir un aperçu complet de la sécurité dans les réseaux informatiques. En comprenant les enjeux, les mécanismes de sécurité, les menaces et les méthodes de détection et de prévention des intrusions, nous pourrons mieux appréhender les défis actuels et mettre en place des mesures de sécurité solides pour protéger les réseaux contre les attaques et les violations de sécurité.

2.2 Objectifs de la sécurité

La sécurité des réseaux vise à atteindre trois objectifs fondamentaux :

2.2.1 Confidentialité

La confidentialité des données signifie que seuls les destinataires autorisés et autorisés peuvent accéder aux données et les lire[27][28][29].

2.2.2 Intégrité

L'intégrité des données garantit aux utilisateurs que les informations n'ont pas été altérées lors de leur transmission, de l'origine à la destination. L'intégrité des données garantit aux utilisateurs que les informations n'ont pas été altérées lors de leur transmission, de l'origine à la destination[27][28][29].

2.2.3 Disponibilité

La disponibilité des données garantit aux utilisateurs un accès rapide et fiable aux services de données pour les utilisateurs autorisés. La disponibilité des données garantit aux utilisateurs un accès rapide et fiable aux services de données pour les utilisateurs autorisés[27][28][29].

2.3 Vulnérabilités courantes dans les réseaux

Indépendamment de leur degré de vulnérabilité, tous les systèmes informatiques sont susceptibles de présenter des faiblesses exploitables par des individus malveillants dans le but de causer des préjudices. Une vulnérabilité peut être définie comme une faille ou une fragilité permettant à une personne malintentionnée de porter atteinte au système. Ces vulnérabilités peuvent être regroupées en différentes catégories telles que les vulnérabilités humaines, technologiques, organisationnelles et de mise en œuvre[26][30][32][35].

2.3.1 Vulnérabilités humaines

En raison de la nature humaine, les individus sont intrinsèquement vulnérables. De nombreuses vulnérabilités humaines découlent d'erreurs telles que la négligence, le manque de

compétences ou l'exploitation excessive, comme le dit souvent l'adage "l'erreur est humaine". Étant donné que les systèmes d'information sont composés d'êtres humains, il est essentiel de garantir leur sécurité afin d'assurer un niveau maximal de protection dans le système. Pour garantir la sécurité d'un système d'information, il est crucial de prendre en compte et de protéger les vulnérabilités inhérentes à la nature humaine[26][30][32][35]].

2.3.2 Vulnérabilités technologiques

Les avancées rapides dans le domaine des outils informatiques entraînent quotidiennement la découverte de nouvelles vulnérabilités technologiques. Ces vulnérabilités résultent généralement de négligences humaines lors de la conception et de la mise en œuvre des systèmes. Afin de rester informé des dernières vulnérabilités technologiques, il est possible de s'inscrire aux listes de diffusion proposées par les équipes de réponse aux urgences informatiques (CERT). Ces listes permettent de recevoir des notifications régulières concernant les vulnérabilités récemment découvertes et de prendre les mesures appropriées pour y remédier[26][30][38][40].

2.3.3 Vulnérabilités organisationnelles

Les vulnérabilités d'ordre organisationnel dans un système informatique surviennent en raison de l'absence de documents et de procédures adéquats pour traiter les problèmes de sécurité. Même lorsque ces éléments existent, leur maintenance et leur mise à jour sont souvent négligées[26][27][40][42].

2.3.4 Vulnérabilités mise en œuvre

Les vulnérabilités dans la mise en œuvre d'un projet peuvent être causées par le fait de ne pas prendre en compte certains aspects essentiels lors de sa réalisation[26][27][40][42].

2.4 Conséquences des failles de sécurité dans les réseaux

Les failles de sécurité dans les réseaux peuvent entraîner de graves conséquences pour les entreprises et les utilisateurs. Voici quelques-unes des conséquences les plus courantes :

Conséquences	Description
Perte de données sensibles	Les failles de sécurité peuvent permettre l'accès non autorisé aux données sensibles, entraînant des pertes financières ou des vols d'identité.
Interruption des services	Les failles de sécurité peuvent perturber les services en rendant les systèmes indisponibles, entraînant une perte de productivité pour les utilisateurs.
Attaques par injection	Les failles de sécurité telles que les injections SQL peuvent permettre l'exécution de code malveillant, compromettant l'intégrité et la disponibilité des systèmes.
Réputation endommagée	Les failles de sécurité exposent les entreprises à des risques de réputation négative, de perte de confiance des clients et de partenaires commerciaux.
Coûts financiers élevés	Les failles de sécurité entraînent des coûts importants pour la remédiation, la récupération des données, la mise en place de mesures de sécurité supplémentaires, etc.
Violation de la conformité réglementaire	Les failles de sécurité peuvent entraîner des violations des réglementations de protection des données, exposant les entreprises à des amendes et des sanctions.
Perte de confiance des clients	Les failles de sécurité peuvent entraîner une perte de confiance des clients dans l'entreprise, entraînant une diminution des ventes et des parts de marché.
Perte de propriété intellectuelle	Les failles de sécurité peuvent permettre le vol de secrets commerciaux ou d'informations confidentielles, affectant la compétitivité de l'entreprise.

TABLE 2.1 – Conséquences des failles de sécurité dans les réseaux

2.5 Mécanismes de sécurité

2.5.1 Pare-feu (firewalls)

Les pare-feux sont des systèmes de sécurité qui agissent comme une barrière entre les réseaux internes et externes. Ils filtrent les paquets de données entrants et sortants pour prévenir les attaques et les intrusions. Les pare-feux peuvent être utilisés pour contrôler le trafic entre les systèmes du Cloud et les utilisateurs autorisés [40][42].

2.5.2 Antivirus

antivirus est un logiciel conçu pour détecter, neutraliser et éliminer les logiciels malveillants. Ces logiciels malveillants peuvent exploiter des vulnérabilités de sécurité ou altérer

et supprimer des fichiers, qu'ils s'agissent de documents de l'utilisateur ou de fichiers essentiels au bon fonctionnement de l'ordinateur. L'antivirus effectue des vérifications sur les fichiers, les e-mails, les secteurs de démarrage (pour détecter les virus de démarrage), la mémoire vive de l'ordinateur, les supports amovibles tels que les clés USB, les CD, les DVD, ainsi que les données circulant sur les réseaux potentiels, y compris Internet[28][30].

2.5.3 Mise à jour système

pour se protéger contre les attaques, il est important de maintenir les logiciels à jour afin de corriger les failles potentielles. De plus, en modifiant les options de configuration, on peut détecter les comportements suspects et prévenir certains types d'attaques. Ces mesures simples mais essentielles aident à renforcer la sécurité du système[31][32].

2.5.4 Chiffrement de données

Les données des utilisateurs, qu'elles soit en transit ou au repos, sont vulnérables au vol. C'est pourquoi il est essentiel d'utiliser des techniques pour garantir la confidentialité et la protection de la vie privée des données.

Afin d'améliorer le niveau de sécurité des données dans les réseaux, il est crucial de les chiffrer en utilisant des méthodes d'anonymisation, ainsi que de mettre en place des sauvegardes régulières et des audits [39][40].

2.5.5 Virtual Private Network (VPN)

permettent de créer une connexion privée et chiffrée entre des ordinateurs ou des réseaux distants via Internet. Les VPN fonctionnent selon un système de tunnels privé, qui garantit la confidentialité et l'intégrité des données échangées. Ils sont largement utilisés pour sécuriser les connexions à distances des employés, protéger les données sensibles et contourner les restrictions géographiques [30][31].

2.5.6 Les zones démilitarisées (DMZ)

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur Web, serveur de messagerie, serveur FTP public,...etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de zone démilitarisée (noté DMZ pour Demilitarized zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public [27].

2.5.7 Les réseaux locaux virtuels (VLAN)

Ils permettent de créer des réseaux indépendants du système de câblage, et définissent les domaines de diffusion restreints, ce qui signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations du même VLAN [29].

2.5.8 Systèmes de détection et de prévention d'intrusions (IDS/IPS)

L'utilisation des outils de sécurité qui aident à protéger les réseaux contre les attaques et intrusions. Émettant des alertes lorsqu'ils détectent une activité suspecte ou non autorisée sur un réseau [40].

2.5.9 Protocole de securité

Un protocole est un ensemble de règles et de procédures qui permettent l'émission et la réception de données sur un réseau. Sur Internet, les protocoles utilisés font partie de la suite de protocoles TCP/IP. Cependant, la plupart de ces protocoles ne garantissent pas la sécurité des données lors de leur transmission sur le réseau. Afin de remédier à cela, des protocoles sécurisés ont été développés pour encapsuler les messages dans des paquets de données chiffrées. Certains de ces protocoles sécurisés sont [21][24] :

— SSL/TLS (Secure Sockets Layer/Transport Layer Security)

— SSH (Secure Shell)

— IPsec (Internet Protocol Security)

— S/MIME (Secure/Multipurpose Internet Mail Extensions)

— HTTPS (Hypertext Transfer Protocol Secure)

2.6 Menaces et attaques courantes dans les réseaux

2.6.1 Types d'attaques courantes

Les attaques sur un réseau visent à compromettre des informations sensibles dans le but de nuire à une entreprise. Elles peuvent avoir quatre objectifs : l'interruption, l'interception, la modification et la fabrication. Voici quelques types d'attaques courantes dans un réseau informatique résumées dans le tableau ci-dessous[25][26] :

Type d'attaque	Description
Déni de service (DoS)	Tentative de submerger un réseau ou un système avec un trafic excessif, rendant les services indisponibles aux utilisateurs légitimes.
Déni de service distribué (DDoS)	Attaque DoS impliquant de multiples sources pour inonder les cibles, rendant la défense plus difficile.
Usurpation d'identité (Spoofing)	Falsification de l'adresse IP ou d'autres données pour se faire passer pour une autre entité et tromper les systèmes de sécurité.
Injection	Injection de code malveillant, tel que SQL, dans des applications ou des bases de données pour compromettre la sécurité et accéder à des informations sensibles.
Phishing	Techniques de social engineering pour tromper les utilisateurs et obtenir des informations confidentielles telles que des identifiants de connexion.
Ransomware	Chiffrement des données d'un système ou d'un réseau avec demande de rançon en échange de la clé de déchiffrement.
Interception de données (Man-in-the-Middle)	Positionnement d'un attaquant entre les communications légitimes pour intercepter et manipuler les données échangées.
Force brute	Tentative d'accéder à un système en essayant différentes combinaisons de mots de passe jusqu'à ce que le bon soit trouvé.
Exploits de vulnérabilités	Exploitation de failles de sécurité connues dans les logiciels ou les systèmes pour un accès non autorisé ou la prise de contrôle.
Phishing d'hameçonnage (Spear Phishing)	Forme ciblée de phishing utilisant des informations spécifiques sur la victime pour rendre les attaques plus crédibles et persuasives.

TABLE 2.2 – Les types d'attaques.

2.6.2 Conséquences des attaques sur la sécurité des réseaux

Les attaques sur la sécurité des réseaux peuvent avoir de graves conséquences pour les entreprises et les utilisateurs. Voici quelques-unes des conséquences les plus courantes[28][32][39][40].

— **Perte de données :**Les attaques peuvent entraîner la perte, la corruption ou le vol de données sensibles, ce qui peut avoir un impact financier et juridique important pour les entreprises et les individus concernés.

— **Interruption des services :** Les attaques de déni de service peuvent rendre les services indisponibles, perturbant les activités commerciales, l'expérience utilisateur et entraînant des pertes financières.

— **Impact sur la réputation :** Les attaques réussies peuvent nuire à la réputation d'une entreprise, susciter la méfiance des clients et des partenaires, et entraîner une perte de

confiance.

— **Vol d'identité :** Les attaques de phishing et d'usurpation d'identité peuvent permettre aux attaquants d'obtenir des informations personnelles et financières, entraînant des fraudes et des vols d'identité.

— **Perturbation des opérations commerciales :** Les attaques peuvent entraîner des interruptions dans les opérations quotidiennes, provoquant des retards, des pertes de productivité et des coûts supplémentaires pour rétablir la normalité.

— **Coûts financiers élevés :** Les entreprises peuvent être confrontées à des coûts importants pour la remédiation des attaques, la récupération des données, la mise en place de mesures de sécurité renforcées et la gestion des conséquences légales

— **Violation de la confidentialité :** Les attaques réussies peuvent compromettre la confidentialité des données, exposant des informations sensibles telles que des secrets commerciaux, des informations personnelles ou des données médicales.

— **Rupture de conformité réglementaire :** Les attaques peuvent conduire à des violations de réglementations de protection des données, entraînant des amendes, des litiges et des sanctions légales.

2.7 Systèmes de détection et de prévention d'intrusion

2.7.1 Systèmes de détection d'intrusion IDS

Est un système qui surveille et analyse le trafic réseau ou les activités système à la recherche de comportement suspects ou d'activités malveillantes. Les organisation, entreprises et autres structures utilisent ce dernier pour pouvoir protéger leur système contre les menaces venant de l'intérieur ou de l'extérieur d'un réseau d'objets [36][42]. Il existe différents types :

— **système de détection d'intrusion réseau (NIDS) :** Est un dispositif qui surveille de manière passive le flux de données circulant sur un réseau et détecte en temps réel les intrusions. En d'autres termes, un NIDS écoute l'ensemble du trafic réseau, analyse les paquets de données et génère des alertes si certains paquets semblent représenter une menace[26][27][40].

— **Un système de détection d'intrusion de type hôte (HIDS) :** Est couramment déployé sur des machines sensibles qui sont potentiellement ciblées par des attaques et qui stockent des données confidentielles pour l'entreprise[21][28][25].

— **Un système de détection d'intrusion de type hybride :** Combine les informations provenant à la fois d'un système HIDS et d'un NIDS. Il est généralement utilisé dans des environnements décentralisés et permet de regrouper les informations provenant de différentes sondes placées sur le réseau[21][29][25].

2.7.1.1 Tâches

Un système de détection d'intrusion (IDS) permet de repérer les anomalies dans le trafic réseau en effectuant les actions suivantes[29][30] :

— Détecter les tentatives de découverte du réseau.

— Dans certains cas, déterminer si une attaque a réussi ou non.

— Identifier les attaques de déni de service.
— Évaluer le niveau d'infection du système informatique et les zones du réseau touchées.
— Repérer les machines infectées.
— Générer des alertes centralisées pour toutes les attaques détectées.
— Réagir aux attaques et corriger les problèmes éventuels.

2.7.1.2 Outils

Sur le marché, il existe une variété de systèmes de détection d'intrusion (IDS) avec des fonctionnalités différentes[29][30] :

— ISS RealSecure
— Enterasys DRAGON
— SNORT

2.7.1.3 Méthodes de détection d'intrusion

La détection d'intrusion consiste à surveiller en permanence le réseau à la recherche de signes d'activités malveillantes. Elle peut être réalisée de différentes manières, telles que [26][40][42] :

— **Surveillance des journaux :** Surveillance des journaux : Examiner les journaux d'événements du réseau pour détecter des modèles d'activité suspects, tels que des tentatives de connexion échouées, des accès non autorisés ou des changements inattendus dans les configurations.
— **Analyse du trafic réseau :** Examiner le trafic réseau en temps réel pour détecter des anomalies ou des schémas de trafic inhabituels. Des techniques telles que l'analyse comportementale peuvent être utilisées pour identifier les comportements anormaux qui pourraient indiquer une intrusion.
— **Utilisation de systèmes de détection d'intrusion (IDS) :** Les IDS sont des outils spécialisés conçus pour détecter les activités malveillantes sur le réseau. Ils analysent le trafic réseau à la recherche de signatures d'attaques connues ou de comportements suspects. Lorsqu'une intrusion est détectée, une alerte est générée pour que des mesures appropriées puissent être prises.

2.7.2 Systèmes de prévention d'intrusion IPS

Est un système de prévention d'intrusion qui va au-delà de la simple détection d'intrusion fournie par un IDS. un IPS est capable de prendre des mesures actives pour empêcher les attaques informatiques [29][40].
La différence entre un IDS (réseau) et un IPS (réseau) tient principalement en 2 caractéristiques :

— Un système de détection d'intrusion (IDS) fonctionne traditionnellement en mode d'écoute passive sur le réseau, agissant comme un "sniffer" pour détecter les intrusions. En revanche, un système de prévention d'intrusion (IPS) se positionne en mode de coupure, lui permettant d'intervenir activement sur le réseau pour empêcher les intrusions détectées[25][26].

— L'un des avantages de l'IPS est sa capacité à bloquer immédiatement les intrusions, indépendamment du protocole de transport utilisé, sans nécessiter de reconfiguration d'un équipement tiers. En effet, l'IPS est intrinsèquement doté de techniques de filtrage de paquets et de moyens de blocage, lui permettant de prendre des mesures de protection sans délai[25][26].

2.7.2.1 Méthode de prévention d'intrusion

La prévention d'intrusion vise à bloquer ou à atténuer les attaques avant qu'elles ne compromettent la sécurité du réseau. Voici quelques-unes des méthodes couramment utilisées pour prévenir les intrusions :

— **Utilisation de pare-feu :** Les pare-feu sont des dispositifs de sécurité qui contrôlent le flux du trafic réseau en fonction de règles prédéfinies. Ils peuvent bloquer le trafic malveillant, limiter les connexions non autorisées et fournir une protection de base contre les attaques.

— **Utilisation de systèmes de prévention d'intrusion (IPS) :** Les IPS vont au-delà de la simple détection en prenant des mesures actives pour bloquer les attaques en temps réel. Ils surveillent le trafic réseau et peuvent bloquer, réécrire ou rejeter les paquets de données suspects.

— **Utilisation de listes de contrôle d'accès (ACL) :** Les ACL sont utilisées pour définir des règles de contrôle d'accès spécifiques qui permettent ou refusent le trafic en fonction de critères tels que l'adresse IP, le port ou le protocole. Elles permettent de restreindre l'accès non autorisé aux ressources réseau.

2.7.3 Gestion des incidents de sécurité

La gestion des incidents de sécurité consiste à planifier et à mettre en œuvre des processus pour faire face aux incidents de sécurité lorsqu'ils se produisent. Cela inclut généralement les étapes suivantes[29][32][41] :

— **Détection et évaluation de l'incident :** Identifier et confirmer la présence d'une intrusion ou d'une activité suspecte. Évaluer l'impact et la gravité de l'incident sur le réseau.

— **Réponse et mitigation :** Prendre des mesures immédiates pour atténuer les effets de l'incident et empêcher toute escalade ou propagation. Cela peut inclure l'isolation des systèmes compromis, le blocage des adresses IP suspectes ou la réinitialisation des identifiants d'accès.

— **Investigation et analyse :** Mener une enquête approfondie pour comprendre l'origine et la nature de l'incident. Collecter des preuves, analyser les journaux et les traces numériques pour identifier les techniques d'attaque utilisées et les failles de sécurité exploitées.

— **Restauration et prévention :**Restaurer les systèmes affectés à un état sécurisé et normal. Mettre en place des mesures préventives pour éviter de futurs incidents similaires, telles que la mise à jour des logiciels, la sensibilisation à la sécurité et la révision des politiques et des procédures.

2.8 Conclusion

L'objectif de ce chapitre était de sensibiliser à l'importance de la sécurité des réseaux, de mettre en évidence les vulnérabilités et les conséquences des failles , ainsi que de présenter les mécanismes de sécurité et les systèmes de détection et de prévention d'intrusion.

En comprenant ces concepts et en adoptant les bonnes pratiques de sécurité, les organisations peuvent renforcer la protection de leurs réseaux contre les menaces croissantes.

Dans le prochain chapitre nous allons présenter l'EPB notre organisme d'accueil.

Chapitre 3

Présentation du contexte du projet

3.1 Introduction

Le port de Bejaia joue un rôle crucial pour les échanges internationaux en raison de sa position géographique privilégiée. Actuellement il est classé comme premier port d'Algérie en ce qui concerne les marchandises générales et le troisième port pour le transport de produits pétroliers du pays. En outre, il est distingué en tant que premier port du bassin méditerranéen à obtenir la certification des trois systèmes ISO 9001, 2000 pour la qualité, ISO 14000 pour l'environnement et OHSAS 18001 pour l'hygiène, santé et sécurité au travail.

Dans ce chapitre, nous allons nous concentrer sur l'organisme d'accueil et la structure de l'entreprise de Bejaia, ou nous avons effectué notre stage pour le projet actuel. Nous allons étudier le centre informatique de l'EPB, en examinant l'état actuel de l'entreprise et en proposant des améliorations pour le centre informatique.

3.2 Présentation générale de EPB

Le port de Béjaïa est un port d'Algérie, situé dans la région de Kabylie au nord du pays. Il est particulièrement dédié au commerce international et aux hydrocarbures. Compte tenu de sa situation géographique, elle joue un rôle très important dans les transactions internationales.

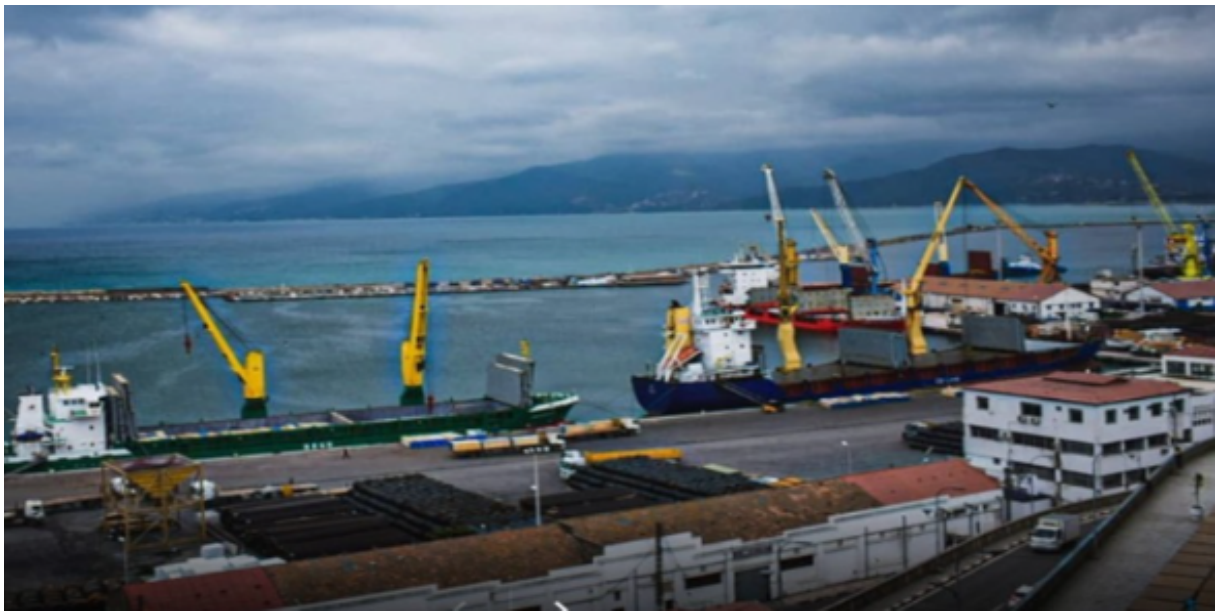

FIGURE 3.1 – Le port de béjaia.

3.3 Direction du système d'information (DSI)

L'EPB est structurée en différentes directions, placées sous la responsabilité d'une Direction Générale chargée de la gestion et du développement de l'entreprise. Chaque partie prenante de l'organisation joue un rôle indéniablement crucial. Cependant, dans le contexte de ce mémoire, notre attention sera exclusivement portée sur la Direction des Systèmes

d'information (DSI). Son rôle consiste à superviser tous les systèmes d'informations et de télécommunication de l'entreprise.

3.3.1 Présentation

Le système d'information (SI) est constitué d'un ensemble organisé de ressources qui permettent la collecte, le stockage, le traitement et la distribution de l'information.

La DSI est une direction de l'entreprise portuaire de Bejaia (EPB) qui est directement rattachée à la direction générale de l'entreprise. Sa mission principale est de mettre en place l'automatisation des différentes activités et processus métiers de l'entreprise portuaire de Bejaia.

3.3.2 Taches

Durant le stage effectué au niveau de la direction nous avons pu analyser et identifier les différentes missions du système d'information comme le montre la figure ci-dessous :

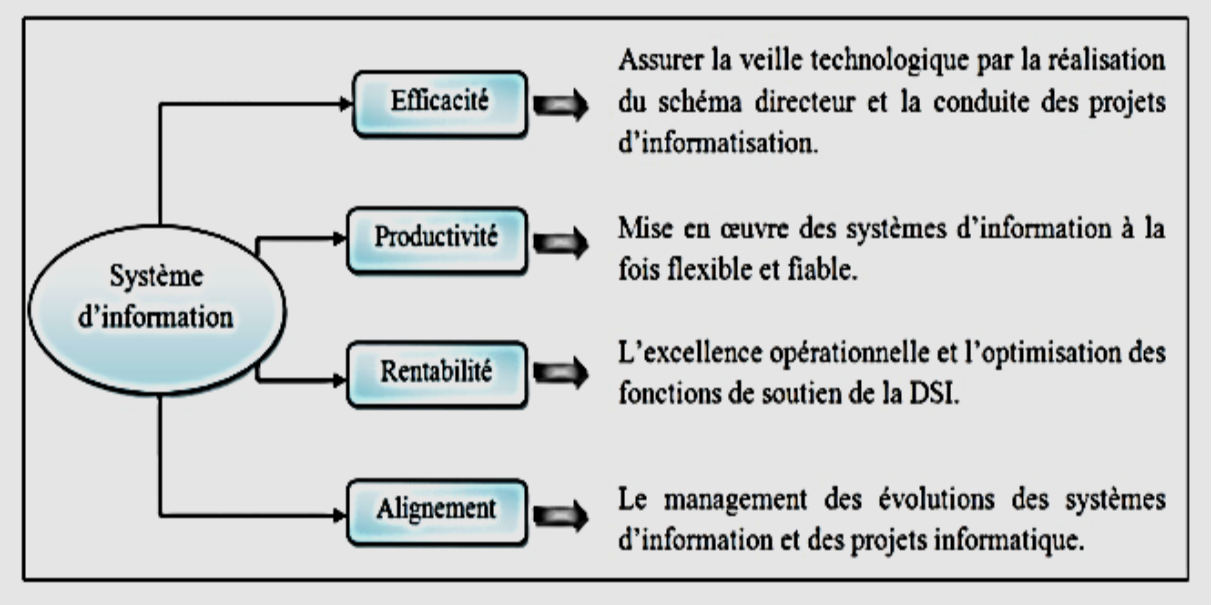

FIGURE 3.2 – Mission du système d'information de l'EPB.
[43]

3.3.3 Organisation

La direction se compose de trois départements comme le montre l'organigramme suivant :

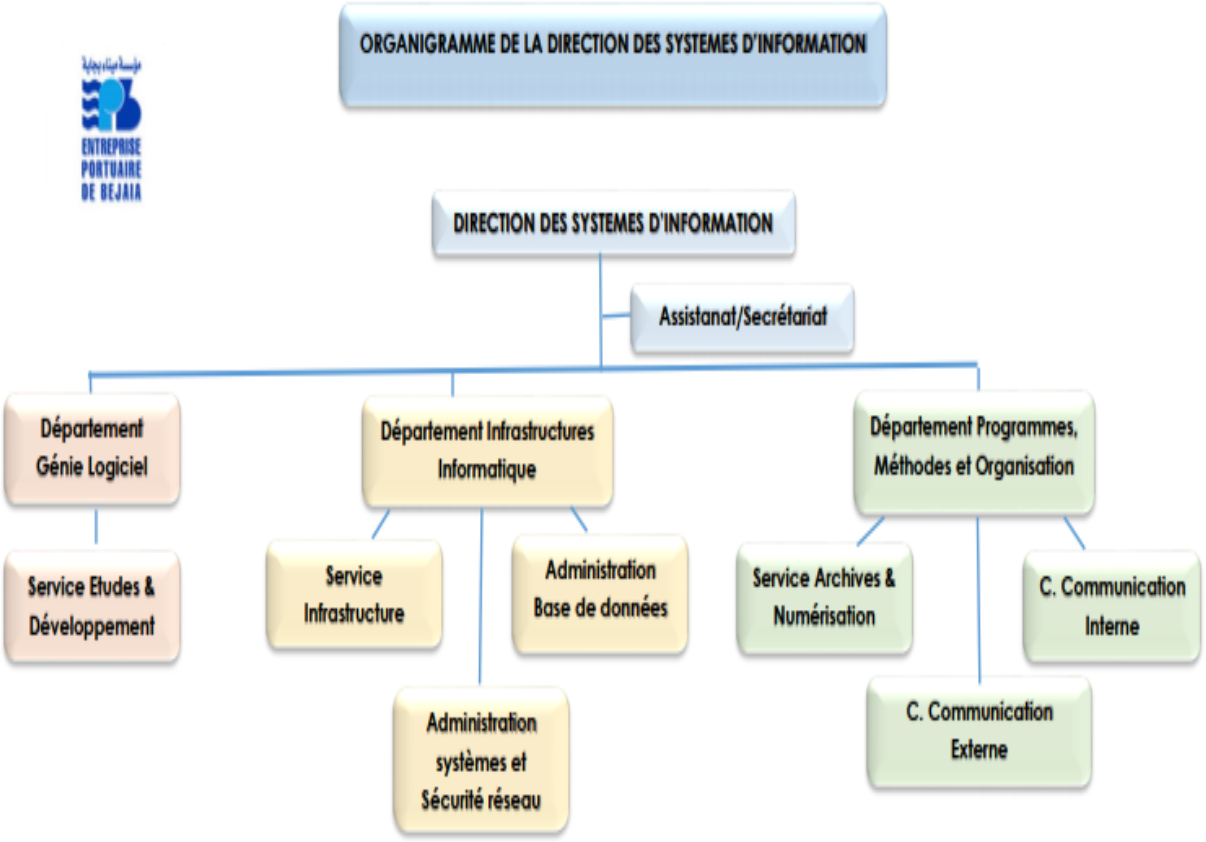

FIGURE 3.3 – Organigramme de la direction du système d'information.
[43]

3.4 Analyse et critique du réseau existant

3.4.1 Infrastructure informatique

L'infrastructure réseau de l'entreprise portuaire de Béjaïa repose sur une architecture complexe permettant de garantir une connectivité fiable et sécurisée. Au cœur de cette infrastructure se trouve la fibre optique, qui constitue le principal support de transmission des données.

La couche département informatique est le socle de la connexion, c'est-à-dire qu'elle assure la gestion et la maintenance de l'ensemble du réseau de l'entreprise portuaire. Elle joue un rôle essentiel dans la planification, la conception, la mise en œuvre et la surveillance de l'infrastructure réseau.

La couche département informatique fournit la connexion internet pour l'ensemble des

autres directions.

Le réseau du port de Bejaia couvre une zone allant du port pétrolier (n°16) aux ports 13 et 18 (parc à bois).

À l'intérieur de la salle machine du réseau local de l'EPB, on trouve principalement deux armoires : Une armoire de brassage et une armoire optique de grande taille.

Ces deux armoires sont utilisées pour connecter les différents sites de l'entreprise au département informatique à l'aide de fibres optiques de type 4 et 12 brins, comme illustré dans la figure(1-6) ci-dessous.

Chaque site dispose d'une armoire de brassage contenant un ou plusieurs convertisseurs de média, ainsi qu'un ou plusieurs commutateurs (Switch) auxquels les différents équipements sont connectés à l'aide de câbles informatiques.

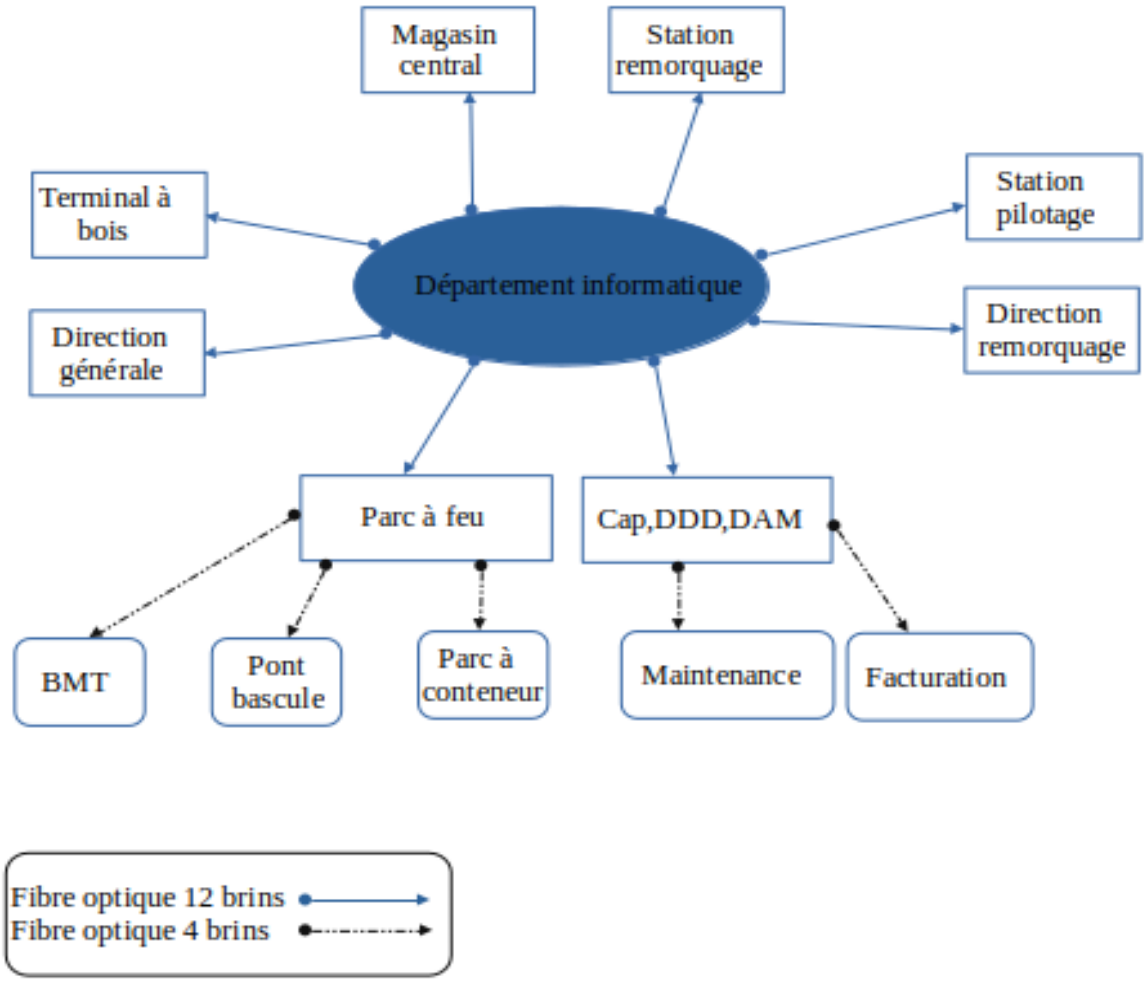

FIGURE 3.4 – Réseau Fibre Optique de l'EPB.
[43]

3.4.2 Architecture du réseau de l'EPB

Le réseau interne de l'EPB facilite l'échange d'informations entre les différents postes de travail, permettant ainsi la connexion externe et l'utilisation d'applications internes essentielles à l'exécution des tâches quotidiennes des employés.

Ce réseau s'étend du port pétrolier (N16) aux ports 13 et 18 du port de Bejaïa (port à bois), comme illustré dans la figure 3-5.

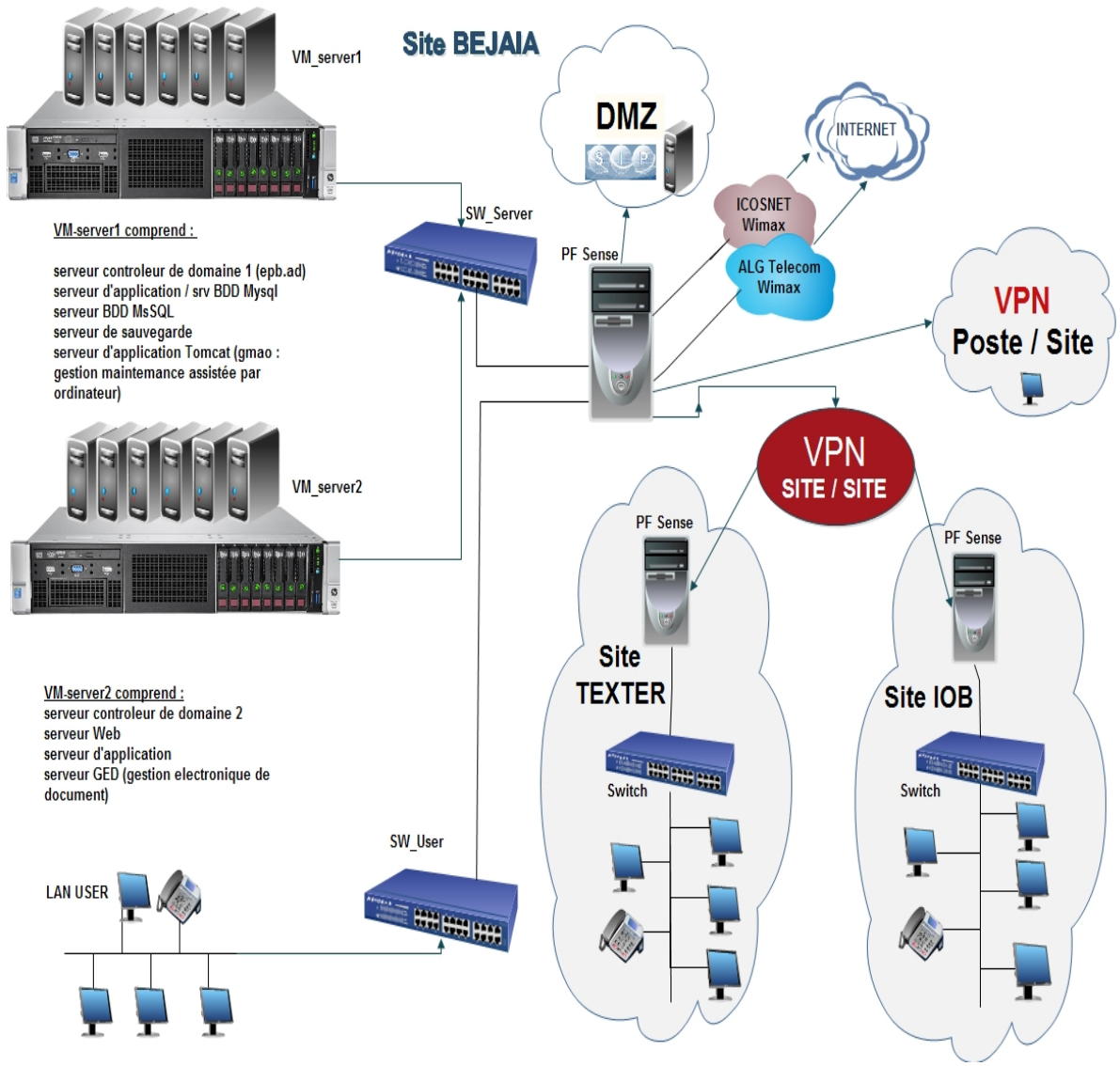

FIGURE 3.5 – Architecture actuelle du réseau local de l'entreprise.
[43]

Dans ce qui suit nous allons donner une explication détallée de l'entreprise portuaire de bejaia qui nous a accueillies.

1. **Connexion Internet**
   L'entreprise portuaire de Béjaïa a deux options de connexion à Internet : Icosnet et Algérie télécom.

Elle privilégie l'accès haut débit sans fil WIMAX pour sa rapidité et sa flexibilité. En utilisant cette solution alternative, elle se connecte sans fil depuis un poste fixe via une antenne-relais appelée station de base. Cette approche garantit une connectivité fiable et efficace.

2. **Sécurité**
   La sécurité est garantie par l'utilisation d'un pare-feu qui applique des stratégies d'accès et des règles de routage pour contrôler l'accès des clients à Internet.
   - **Pfsense (pare- feu)** :La sécurité est assurée par deux serveurs pare-feu virtuels qui contrôlent l'accès au réseau et filtrent les connexions pour minimiser les risques associés à une connexion normale.
   - **DMZ** :Une zone démilitarisée (DMZ) est une zone sécurisée créée pour permettre les échanges entre le réseau interne et le réseau externe.
   - **VPN (Virtuel Private Network)** :Accès à distance vers les diffèrents sites de l'entreprise :site TEXTER(BORDJ BOU ARRERIDJ) et site IOB(IGHIL OUBEROUAK -TALA HAMZA).
3. **Salle machine**
   Cette dernière rassemble tous les serveurs nécessaires dans des armoires de brassages.
   - **Serveur Controleur de domaine 1** : Sous Windows Server 2012,l'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateur utilisant le système Windows.
   - **Serveur de base de données SQL** : Un serveur de base de données répond à des demandes de manipulation de données stockées dans une ou plusieurs bases de données.
   - **Serveur de sauvegarde** : Conçu pour stocker des copies de données importantes en vue de les restaurer en cas de perte ou de panne du système d'origine.
   - **Serveur d'application Tomcat** : est un serveur d'application Java open source utilisé pour exécuter des applications Web basées sur Java.
   - **Serveur Web** :conçu pour stocker, traiter et diffuser des pages Web et d'autres contenus Web à travers Internet ou un réseau privé.
   - **Serveur GED** :gestion électronique de document est un serveur informatique utilisé pour stocker, organiser, gérer et distribuer des documents électroniques.

3.4.3 Problématique

Après notre diagnostic de l'entreprise portuaire bejaia (EPB), nous avons identifié problèmes suivant :

- L'infrastructure de datacenter de l'hyperviseur est obsolète ce qui veut dire que la sécurité nécessite une mise à niveaux.
- Le problème de chargement des hôtes (les serveurs, les pare-feu...). Lorsque le trafic réseau n'est pas correctement géré, cela peut entraîner une surcharge des ressources du serveur et du pare-feu, des problèmes de performance et de sécurité.

3.5 Conclusion

Ce chapitre nous a permis de présenter l'EPB, notre organisme d'accueil, ainsi que d'étudier en détail son réseau existant.

Au cours de cette étude, nous avons identifié des lacunes et des faiblesses dans le réseau.

Nous avons donc opté pour une solution qui vise à renforcer la sécurité, améliorer le contrôle et la gestion des ressources, et répondre aux exigences croissantes en matière de traitement des données et de confidentialité.

Chapitre 4

Mise en oeuvre et réalisation

4.1 Introduction

Dans ce chapitre, nous allons procéder à l'installation de tous les outils nécessaires pour bien configurer notre environnement logiciel et implémenter notre proposition de solution. cette étape est impérative pour la simulation de notre architecture réseau. Ce chapitre constitue le corps principal de ce mémoire et il est illustré par des captures d'écran pour faciliter la compréhension des étapes d'installation et de la configuration.

4.2 Présentation des outils de travail

Pour la réalisation de notre solution nous avons opter pour les outils citer ci-dessous :

4.2.1 VMware Workstation version 17.0.0

Nous avons choisi d'utiliser VMware Workstation version 17.0.0 pour émuler notre réseau. Il permet de créer des machines virtuelles qui peuvent être connectées à un réseau local avec une adresse IP différente, tout en étant sur la même machine physique.

FIGURE 4.1 – VMware.

4.2.2 VMware ESXi Version 7.0.1

ESXi est un huperviseur de type 1 qui s'exécute sur la machine physique et qui est conçu pour les réseaux domestiques et entreprise. Il abstrait les ressources comme le processeur, la mémoire, le stockage et la mise en réseau pour les fournir aux machines virtuelles qu'il exécute. Il dispose de son propre système d'exploitation et fournit une interface pour gérer les machines virtuelles qu'il exécute [2].

Après avoir examiné les options disponibles, nous avons choisi de passer à ESXi 7 pour bénéficier de ses améliorations significatives en termes de performances, de sécurité et de gestion des ressources par rapport à la version 5 précédemment installé dans l'entreprise.

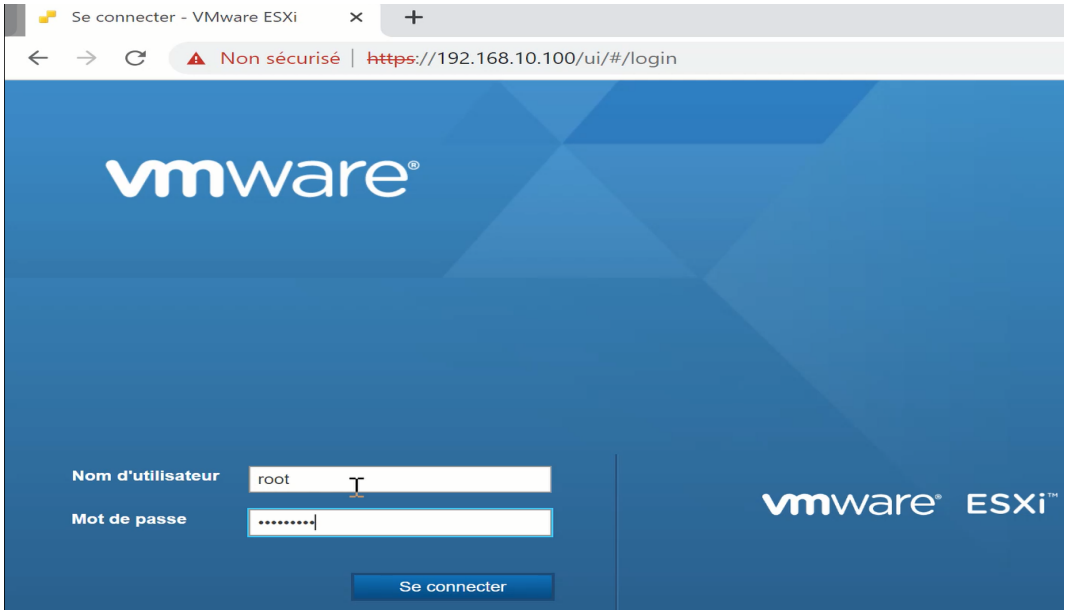

FIGURE 4.2 – ESXi.

4.2.3 Kali Linux

Kali Linux est un système d'exploitation conçu pour les tests de sécurité informatique, basé sur Debian et un successeur de la distribution BackTrack. Il est livré avec des outils préinstallés pour aider les professionnels de la sécurité des systèmes à tester la sécurité des systèmes et des réseaux. Kali Linux est open source et est mis a jour chaque année pour améliorer le contenu et a ajouter de nouvelles fonctionnalités. La première version de Kali Linux a été publié en 2013 et utilise l'environnement de bureau Xfce [47].

FIGURE 4.3 – Kali Linux.

4.2.4 pfsense

pfSense est un système d'exploitation open source gratuit basé sur FreeBSD qui est utilisé comme pare-feu (firewall) et routeur. Il offre des fonctionnalités avancées de sécurité et de réseau, en permettant la configuration et la gestion des règles de pare-feu, la création de réseaux virtuels privés (VPN), la surveillance du trafic réseau, la gestion de la qualité de service (QoS) et bien plus encore. pfSense est souvent utilisé dans les environnements professionnels et domestiques pour renforcer la sécurité du réseau et assurer une gestion avancée des communications.

Voici quelques service réseau offert par le pfsense :

— **Pare-feu (Firewall) :** pfSense permet la configuration de règles de pare-feu.
— **Routage :** pfSense est capable de router le trafic entre différents réseaux locaux ou entre des réseaux locaux et Internet.
— **Réseau privé virtuel (VPN) :** pfSense prend en charge les protocoles VPN tels que OpenVPN, IPsec, PPTP, L2TP, permettant la création de connexions sécurisées entre des réseaux distants ou des utilisateurs distants et le réseau local.
— **Serveur DHCP :** pfSense peut agir en tant que serveur DHCP pour attribuer automatiquement les adresses IP.
— **Serveur DNS :** pfSense peut héberger un serveur DNS, ce qui permet la résolution des noms de domaine localement sans avoir à dépendre d'un serveur DNS externe.
— **Filtrage de contenu :** pfSense permet le filtrage de contenu en appliquant des listes de blocage pour restreindre l'accès à certains sites Web ou à certains types de contenu indésirable

4.2.5 Snort

Snort est un système de détection d'intrusion open source et gratuit qui peut être utilisé pour surveiller le trafic réseau en temps réel et détecter les activités suspectes.

Il utilise des règles pour analyser le trafic réseau et signaler les événements qui correspondent à ces règles.

Snort peut être utilisé pour détecter les attaques de type déni de service, les scans de ports..., il est largement utilisé dans les environnements d'entreprise pour renforcer la sécurité du réseau.

FIGURE 4.4 – Snort.

4.3 Solution proposée

Pour remédier à ces problématiques, nous avons proposé une série de solutions :

— Mettre en place un firewall pour segmenter le réseau et limiter l'accès non autorisé aux données et aux ressources de l'entreprise.

— Mise en place d'un système de prévention d'intrusion en l'implémentant dans le firewall pour la surveillance du trafic réseau et la détection des activités suspectes.

4.3.1 Architecture proposée

Nous avons configuré un pare-feu avec trois interfaces : DMZ, LAN et WAN (Internet). Voici comment chaque interface est utilisée :

— L'interface LAN est connectée à une station de travail, qui est un ensemble de PC. Cette station de travail nous permet d'accéder et de gérer notre pare-feu PFSense.

— La DMZ est utilisée pour renforcer la sécurité de notre réseau. Elle peut être configurée pour héberger des serveurs ou des services sensibles, isolés du reste du réseau tel que chaque machine virtuelle fonctionne de manière indépendante et est séparée des autres machines virtuelles et du système hôte.

— L'interface WAN est connectée à un serveur appelé Kali Linux. Ce serveur est utilisé pour effectuer des attaques externes vers Internet.

Nous avons également ajouté un protocole de détection d'intrusion :IDS(Snort), à notre PFSense. Snort permet de détecter et de bloquer les attaques en temps réel.

Toute cette architecture est installée dans un environnement de virtualisation, ESXi(version 7), qui est un hyperviseur de type 1. L'utilisation d'ESXi nous permet d'exécuter plusieurs machines virtuelles de manière isolée sur un seul serveur physique, offrant ainsi une flexibilité et une sécurité accrues.
Comme l'illustre la figure 4.5 :

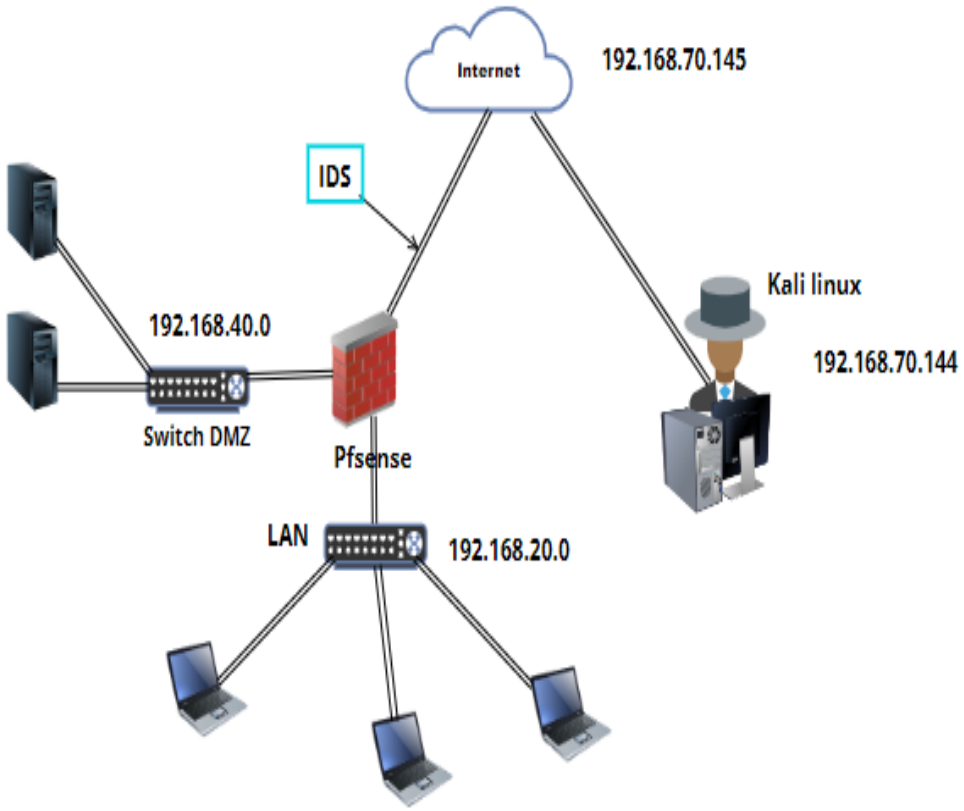

FIGURE 4.5 – Architecture de la solution proposée.

4.3.2 Tableau des équipement

Equipemments	Interfaces	Adresss IP
Firewall	— LAN — Serveur — DMZ — WAN	— 192.168.20.1 — 192.168.30.1 — 192.168.40.1 — DHCP
Serveurs	192.168.30.0/24	192.168.30.100
Client	192.168.20.0/24	DHCP

4.3.3 Tableau de réseaux

switch virtuel	groupe de port	Adresse réseau	Nic physique
Management	Management	192.168.40.0/24	Vmnic0
LAN	LAN	192.168.20.0/24	Vmnic1
Serveurs	Serveurs	192.168.30.0/24	Vmnic2
DMZ	DMZ	192.168.40.0/24	Vmnic3
Internet	Internet	DHCP	Vmnic4

4.4 Les configurations globales sur l'interface de l'ESXi

4.4.1 Création des commutateurs virtuels

Le commutateur virtuel vSwitch est un logiciel qui permet de connecter des machines virtuelles à un réseau physique et contrôle la communication entre le réseau physique et les machines virtuelles en dirigeant les paquets de données vers leurs destinations appropriées.

Pour accéder à la configuration du réseau dans l'interface graphique d'ESXI, vous pouvez suivre ces étapes : "Configurations" puis sur "Réseau"et enfin sur "Commutateurs virtuels". Ensuite vous pouvez suivre les étapes pour créer un nouveau commutateur virtuel. Le vSwitch0 représente le commutateur par défaut de l'ESXi et est utilisé pour le management de ESXi.

— La figure 4.5 représente un exemple d'un commutateur crée.

— La figure 4.6 représente les commutateurs virtuels crées.

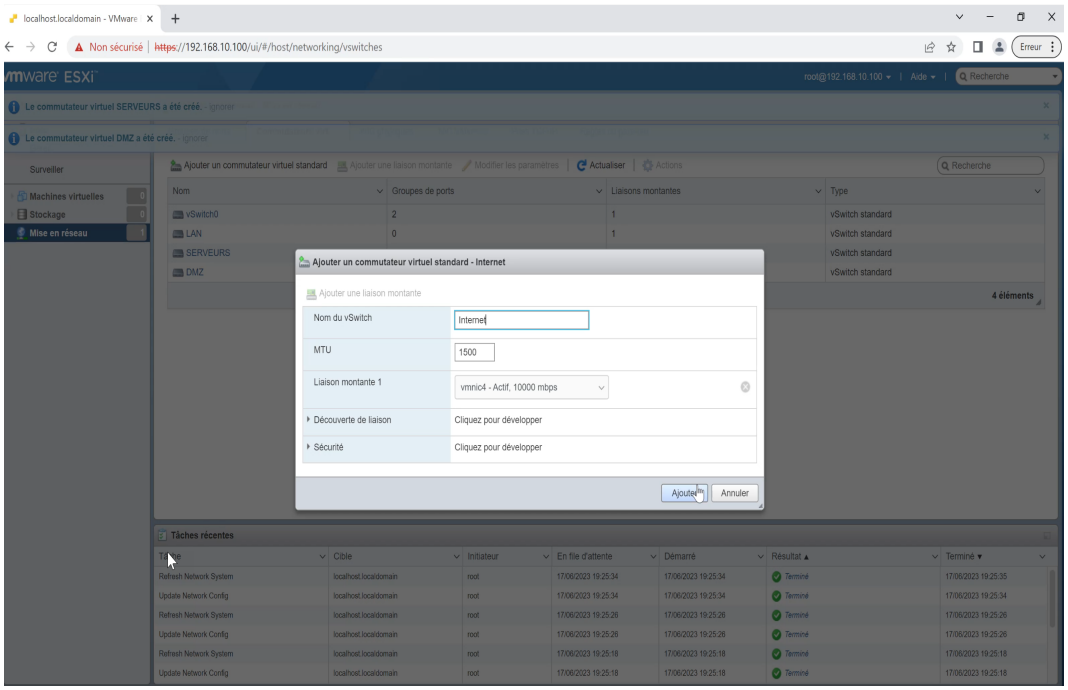

FIGURE 4.6 – Exemple de commutateur Internet.

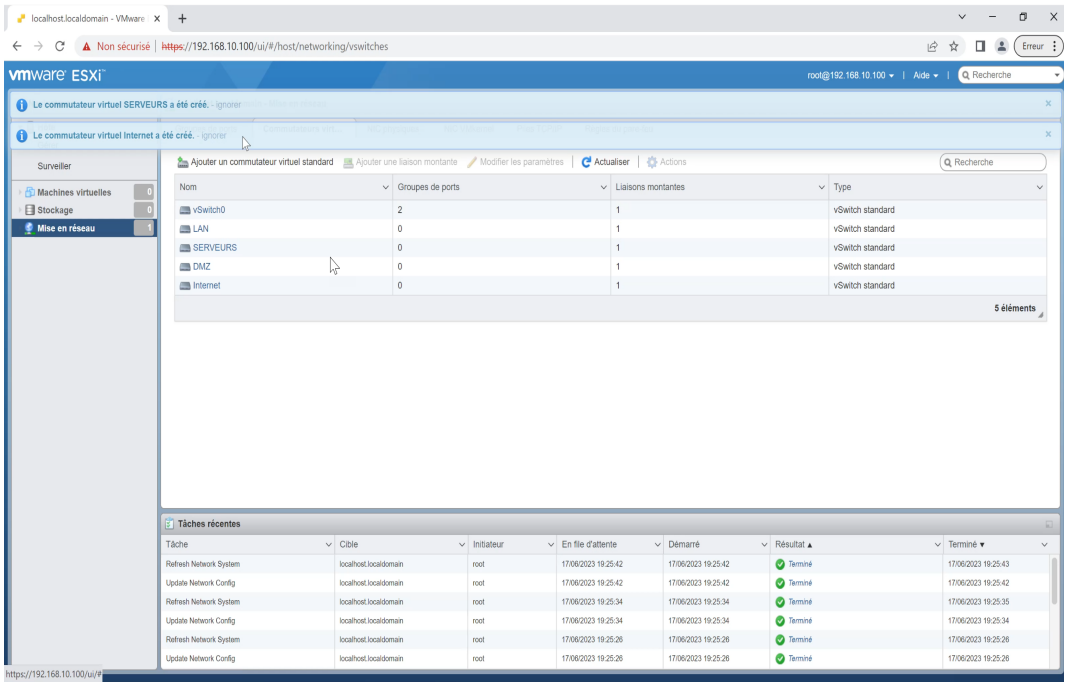

FIGURE 4.7 – Commutateurs virtuels crées.

4.4.2 Création des groupes de ports

Les groupes de ports permettent de compartimenter une partie des ports du vSwitch. Un vSwitch peut avoir plusieurs groupes de ports, chacun est connecté à une interface réseau physique différente.

En divisant les ports du vSwitch, vous pouvez contrôler la façon dont les machines virtuelles sont connectées aux réseaux physiques.

Pour l'ajout d'un groupe de ports vous pouvez cliquer sur "ajouter un groupes de ports" dans la fenêtre de configuration de vSwitch. Ensuite donnez un nom à votre groupe de ports et affectez-le au vSwitch approprié. Les autres paramètres peuvent être laissés par défaut.

— La figure 4.7 représente un exemple d'un port crée.

— La figure 4.8 représente les groupes de ports crées :

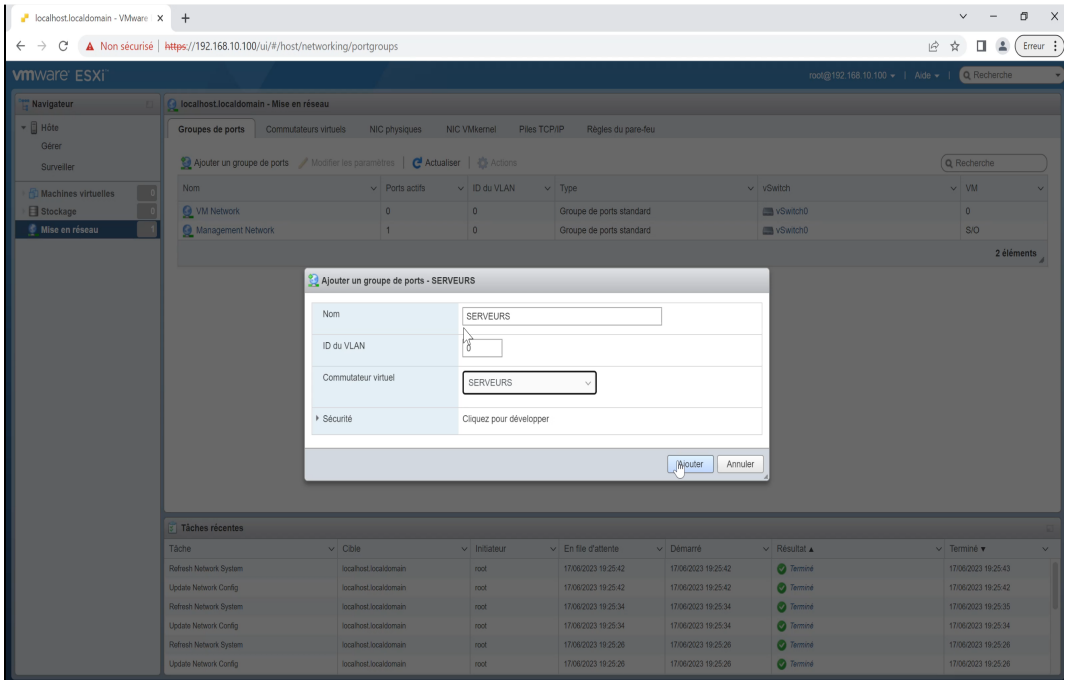

FIGURE 4.8 – Exemple de groupe de port.

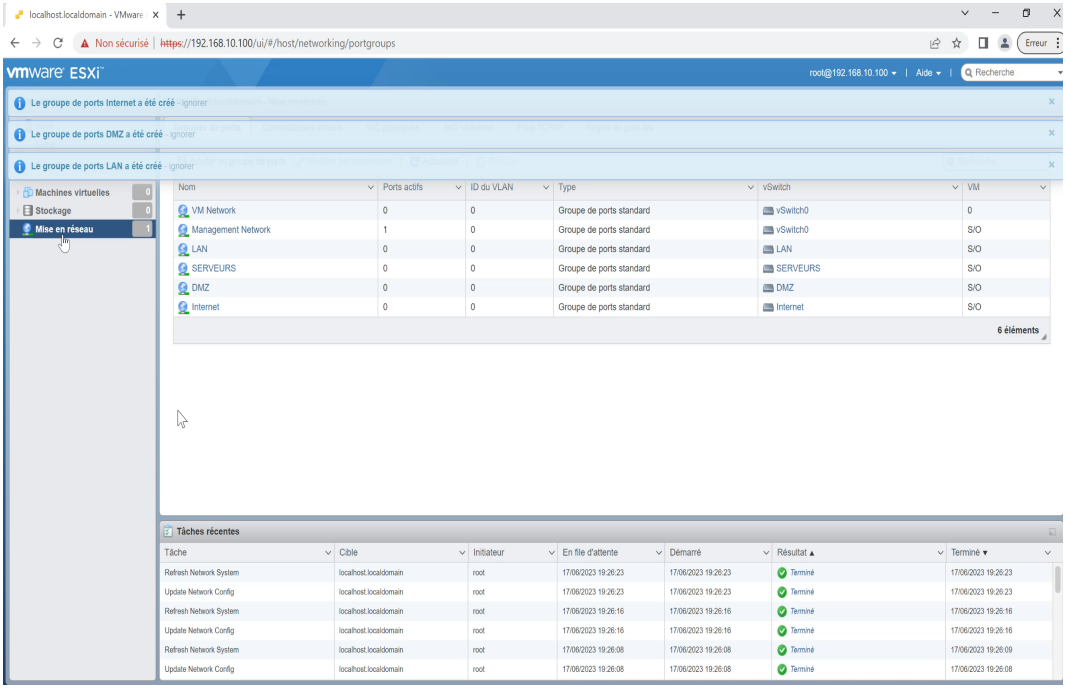

FIGURE 4.9 – Groupes de ports crées.

Après la création et la configuration des vSwitches et les groupes de ports. Nous passons à la création des machines virtuelles.

4.4.3 Création des machines virtuelles

C'est dans la base de données VMsBDD que nous avons créer les trois machines virtuelles.

— La figure 4.9 représente l'interface de la base de données VMsBDD.
— La figure 4.10 représente la machine client1.
— La figure 4.11 représente les différentes configurations effectués pour la machine client1.
— La figure 4.12 représente toute les informations que contient la machine client1.

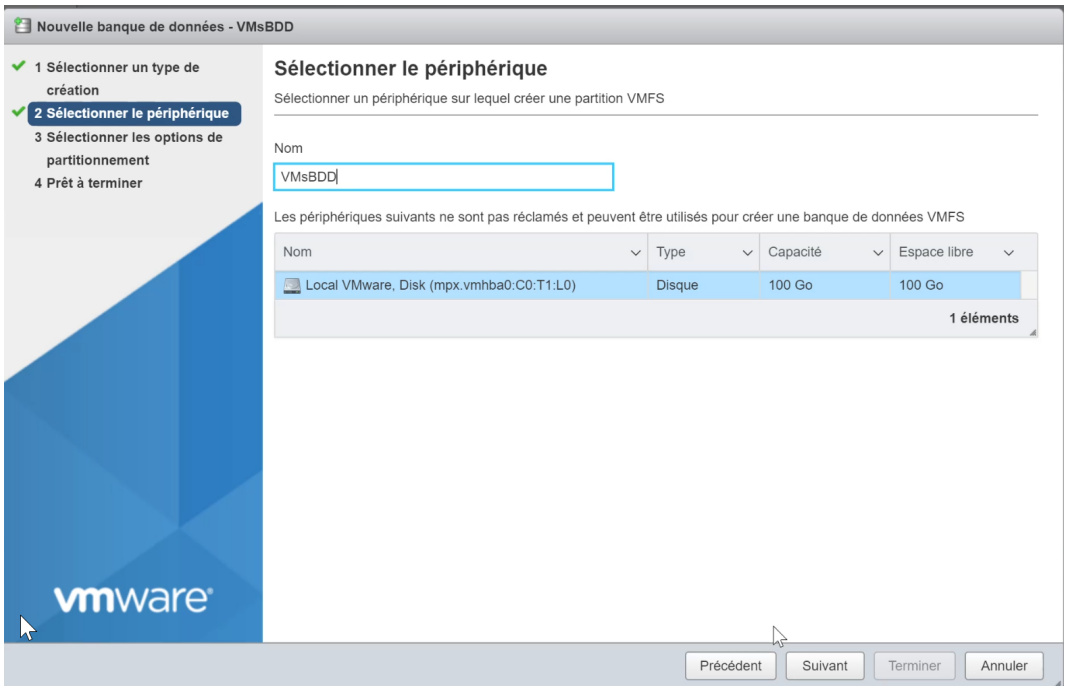

FIGURE 4.10 – Création de la base de données.

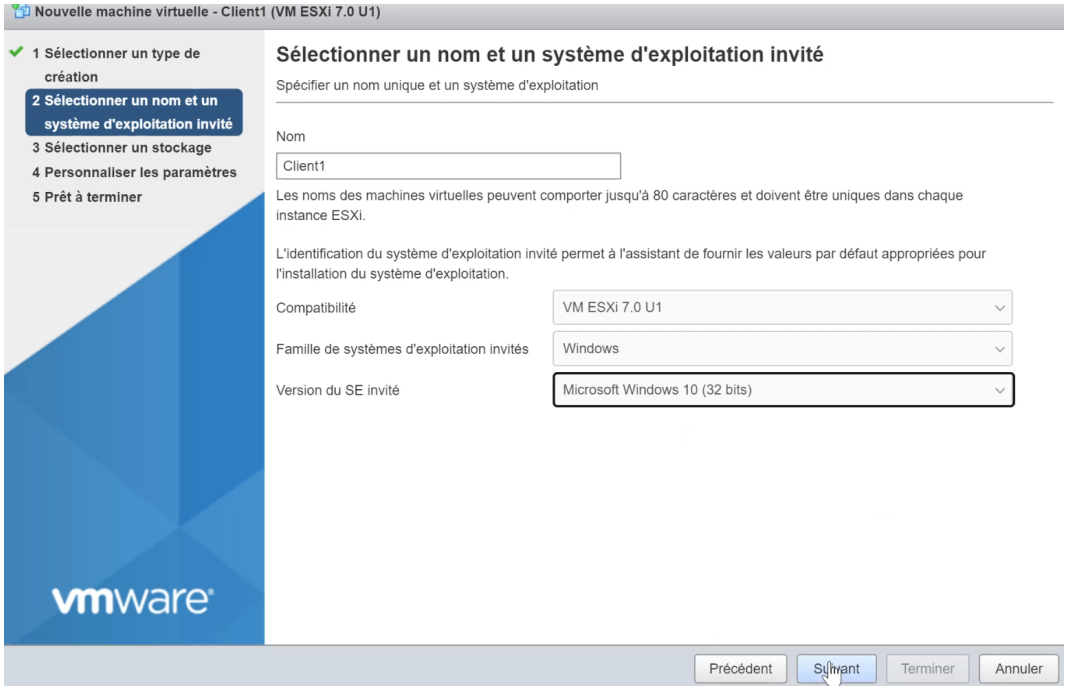

FIGURE 4.11 – Exemple de la machine virtuelle.

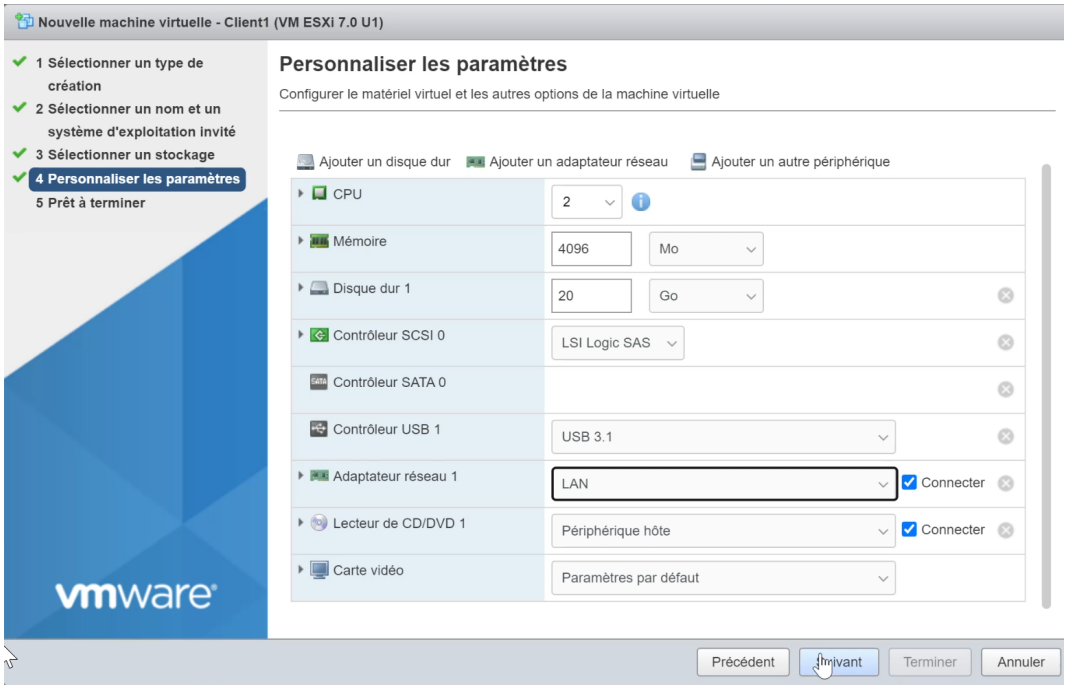

FIGURE 4.12 – Configuration de la machine virtuelle.

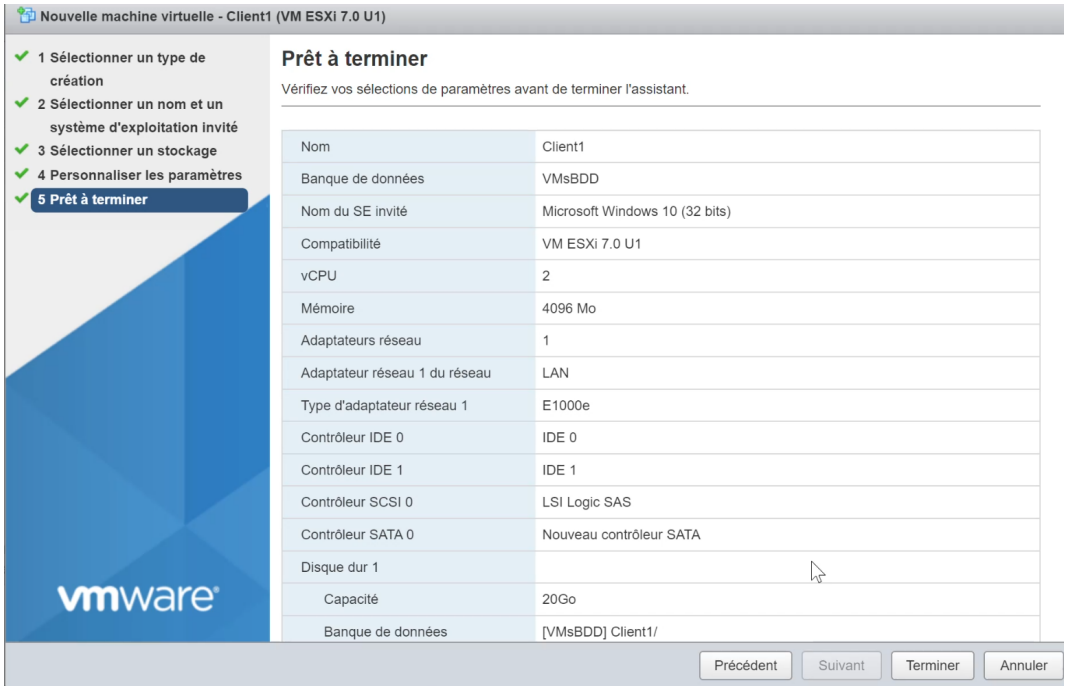

FIGURE 4.13 – Informations de la machine clinet1

Pour les deux autres machines virtuelles (serveurs et pare-feu) nous avons suivi la même méthode pour les créer. La figure 4.13 illustre les trois machines virtuelles crées.

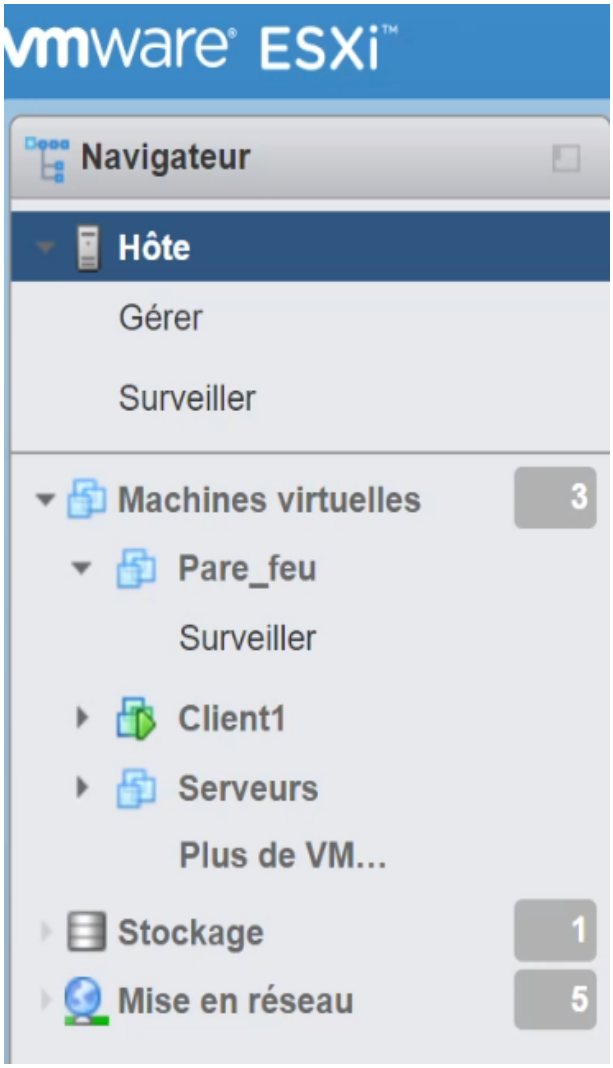

FIGURE 4.14 – les trois machines virtuelles crées.

4.4.4 Paramétrage et configuration de base de pfsence

Dans la ligne de commande nous avons attribué les adresses IP des 4 interfaces du pare-feu, comme illustré dans la figure 4.14.

L'interface graphique de pfsence (pare-feu) est accessible depuis la machine client.

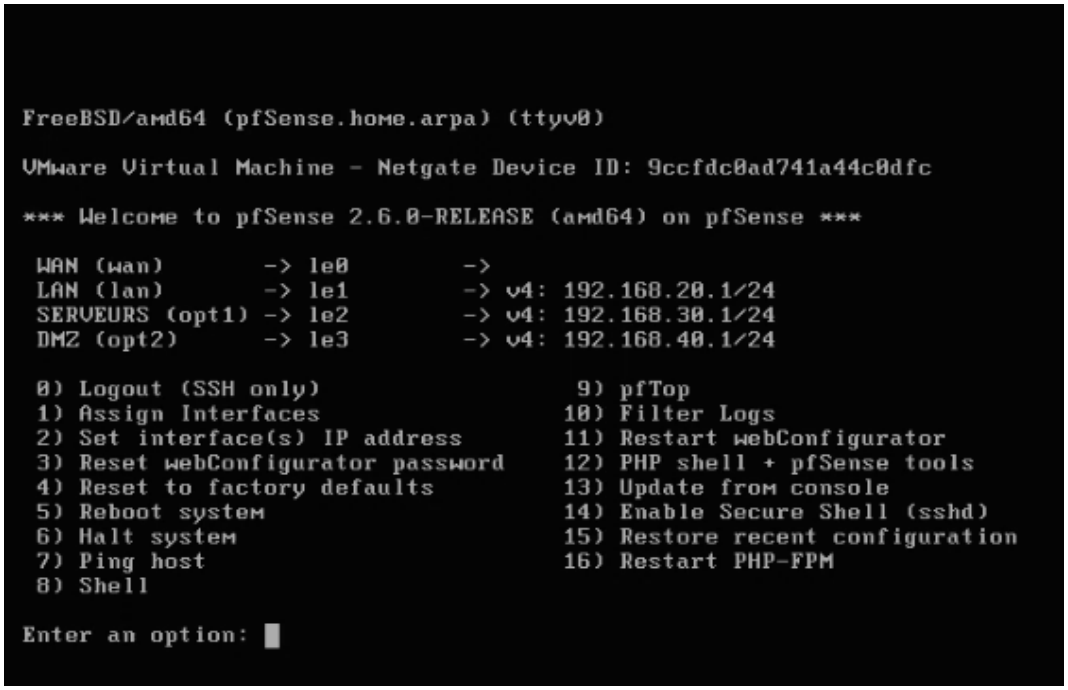

FIGURE 4.15 – Les quatre interfaces sur pfsence.

4.4.4.1 Ajout des 4 interface

La figure 4.15 montre les quatre interface ajoutées

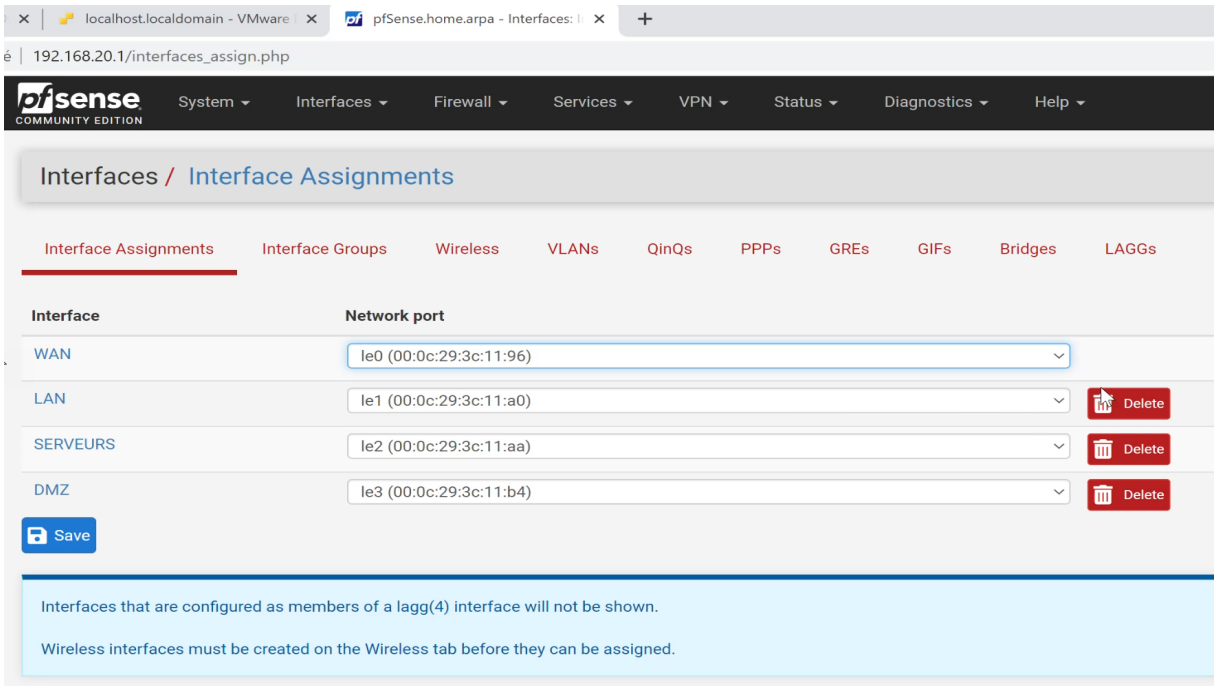

FIGURE 4.16 – Ajout des quatre interfaces.

Après nous avons commencé la configuration de chaque interface comme l'illustrer les 4 figures ci dessous :

(1) Pour l'interface du réseau WAN nous avons choisi l'adresse IP DHCP, le masque de sous réseau et la passerelle par défaut.

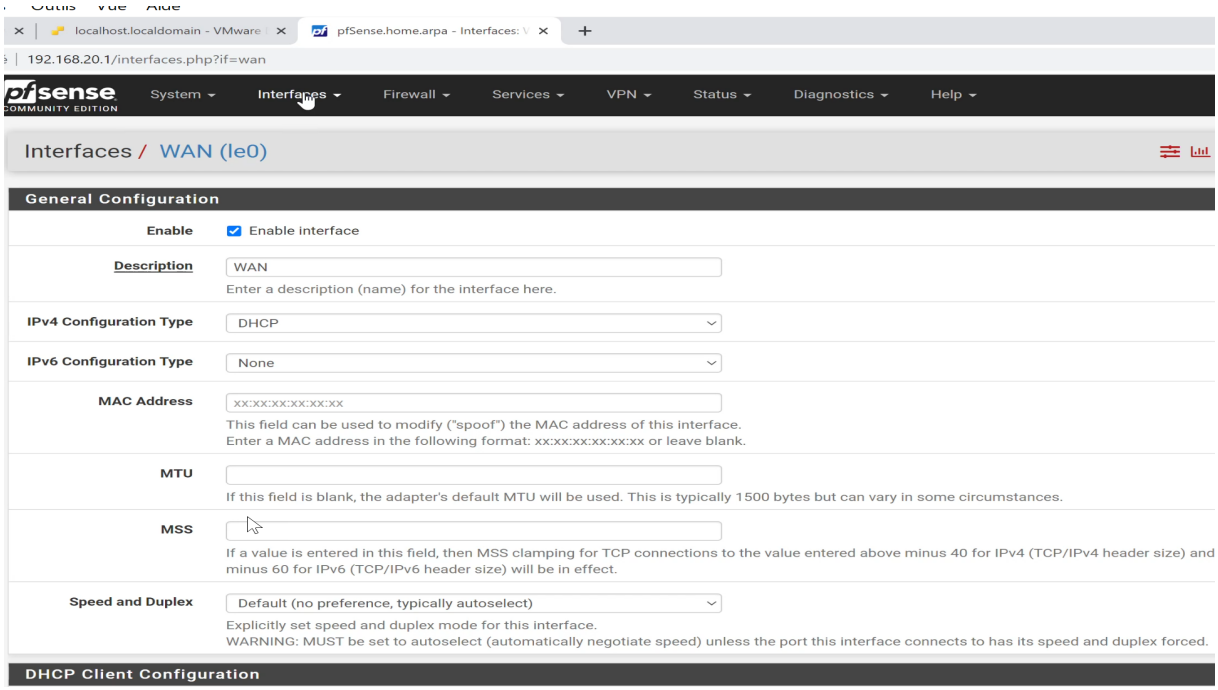

FIGURE 4.17 – La configuration de l'interface WAN.

(2) Pour l'interface du réseau LAN nous avons choisi l'adresse IP static, le masque de sous réseau et la passerelle par défaut .

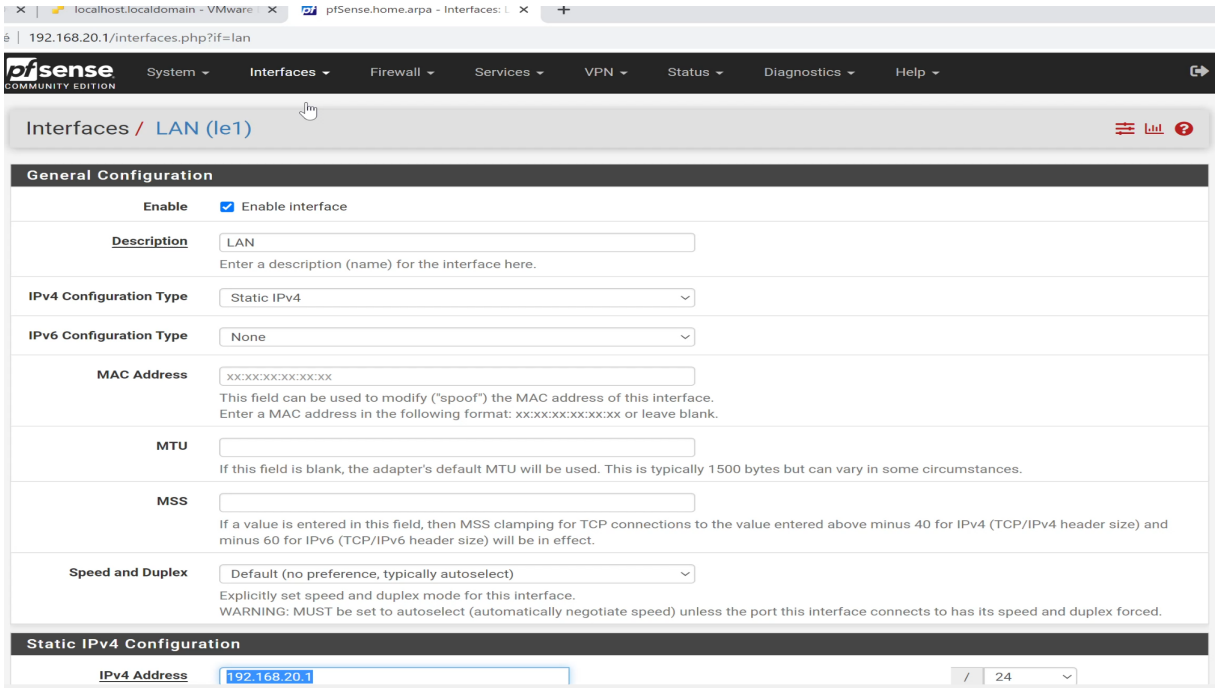

FIGURE 4.18 – La configuration de l'interface LAN.

(3) Pour l'interface du réseau serveurs nous avons choisi l'adresse IP static, le masque de sous réseau et la passerelle par défaut.

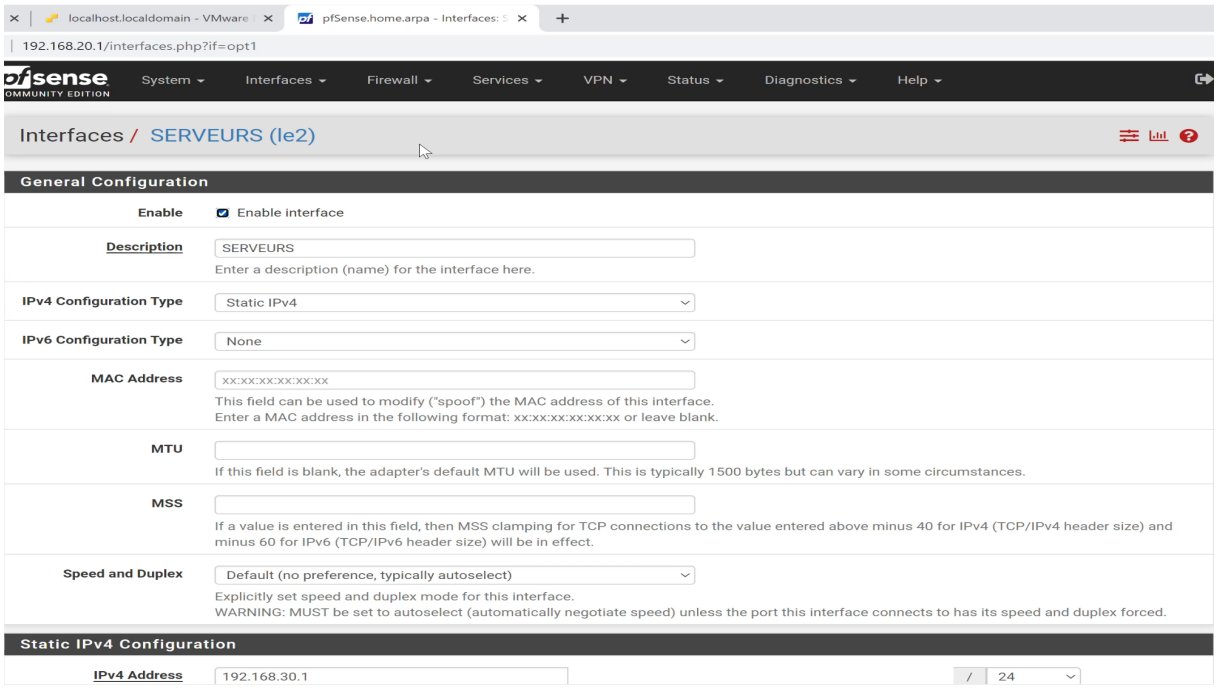

FIGURE 4.19 – La configuration de l'interface Serveurs.

(4) Pour l'interface du réseau DMZ nous avons choisi l'adresse IP static, le masque de sous réseau et la passerelle par défaut.

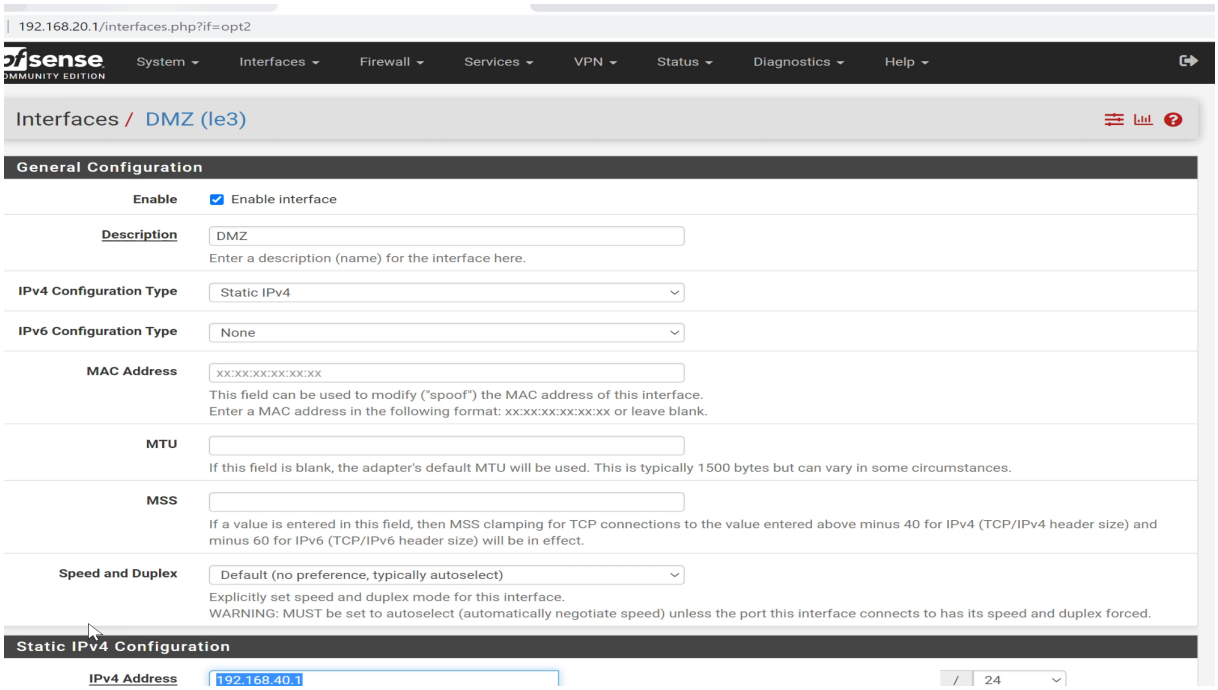

FIGURE 4.20 – La configuration de l'interface DMZ.

Une fois que Snort est installé sur le pare-feu, vous pouvez effectuer le routage en activant la route par défaut vers Internet. Pour cela, accédez à l'onglet "System", puis sélectionnez "Routing" et enfin "Gateways".

La figure 4.20 représente la réussite de l'activation de la route par défaut vers Internet.

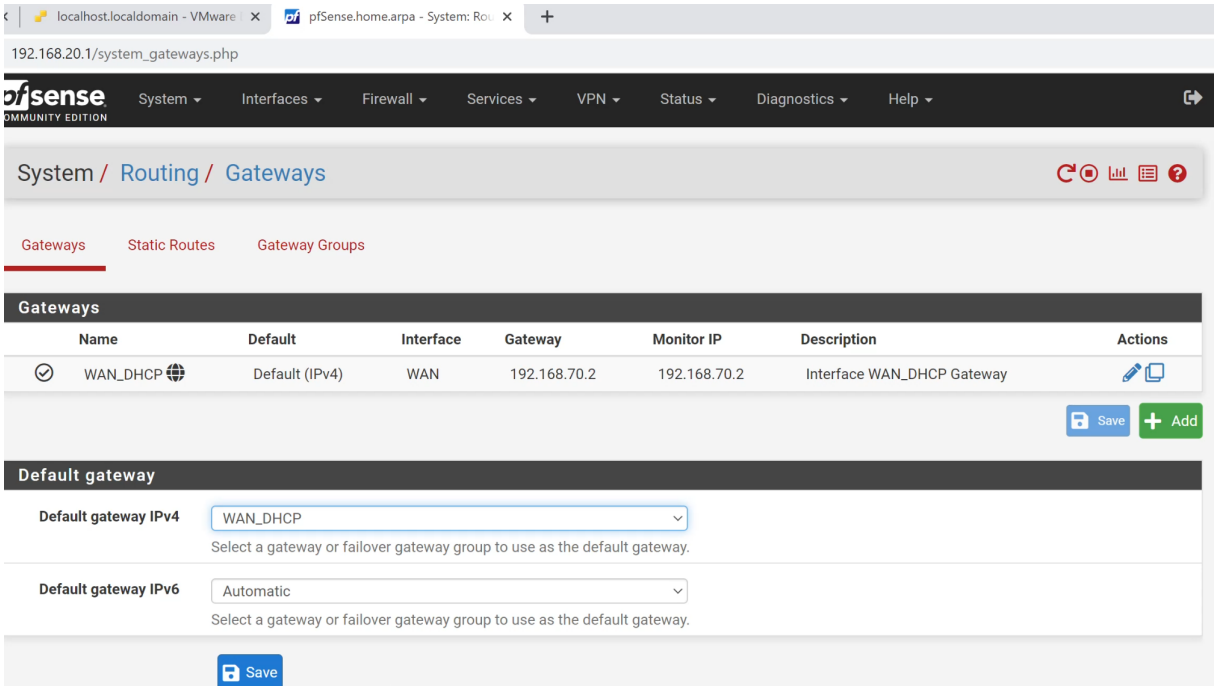

FIGURE 4.21 – Routage activé.

Après nous avons créer des règles de filtrage pour toutes les interfaces afin d'autoriser le trafic réseau. Pour bloquer la connectivité réseau vous pouvez simplement cliquer sur "disable".

Comme illustrer dans les figures ci dessous :

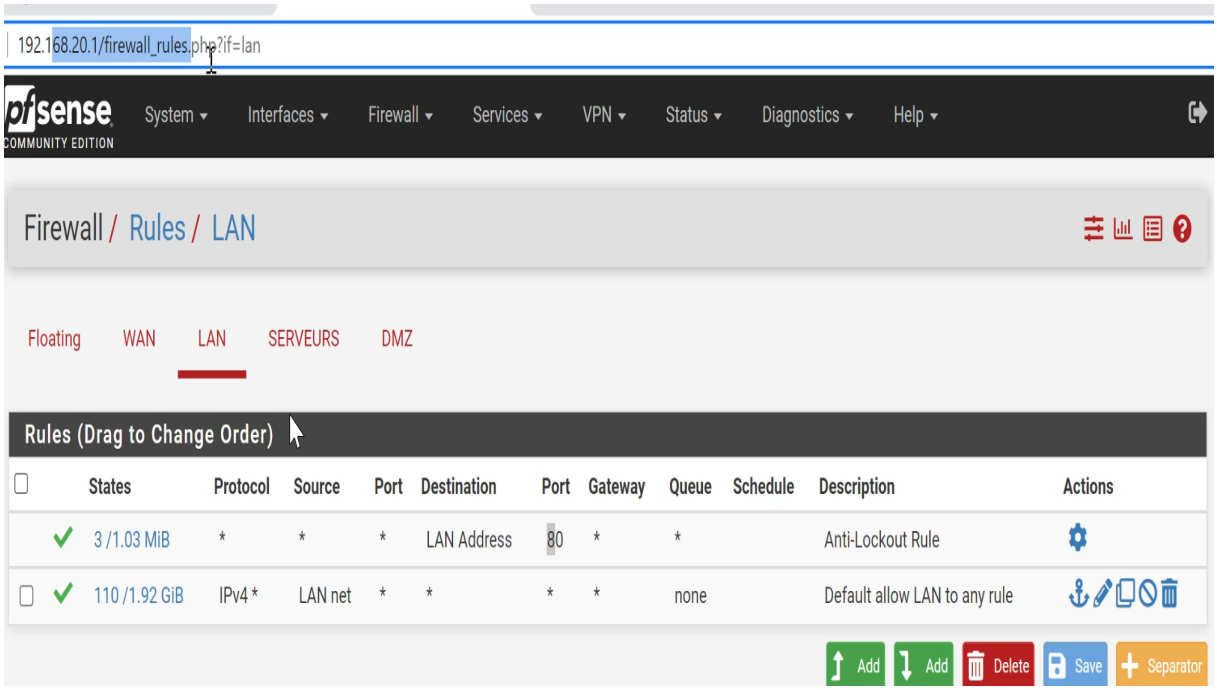

FIGURE 4.22 – Le réseau LAN

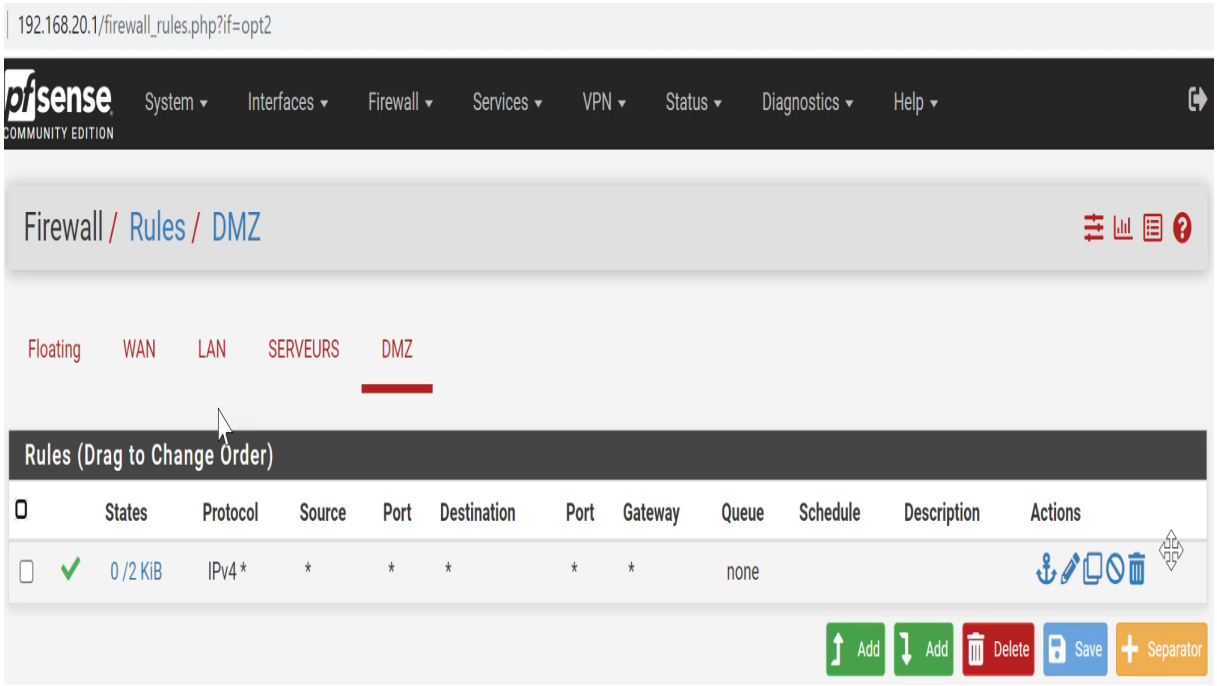

FIGURE 4.23 – Le réseau DMZ

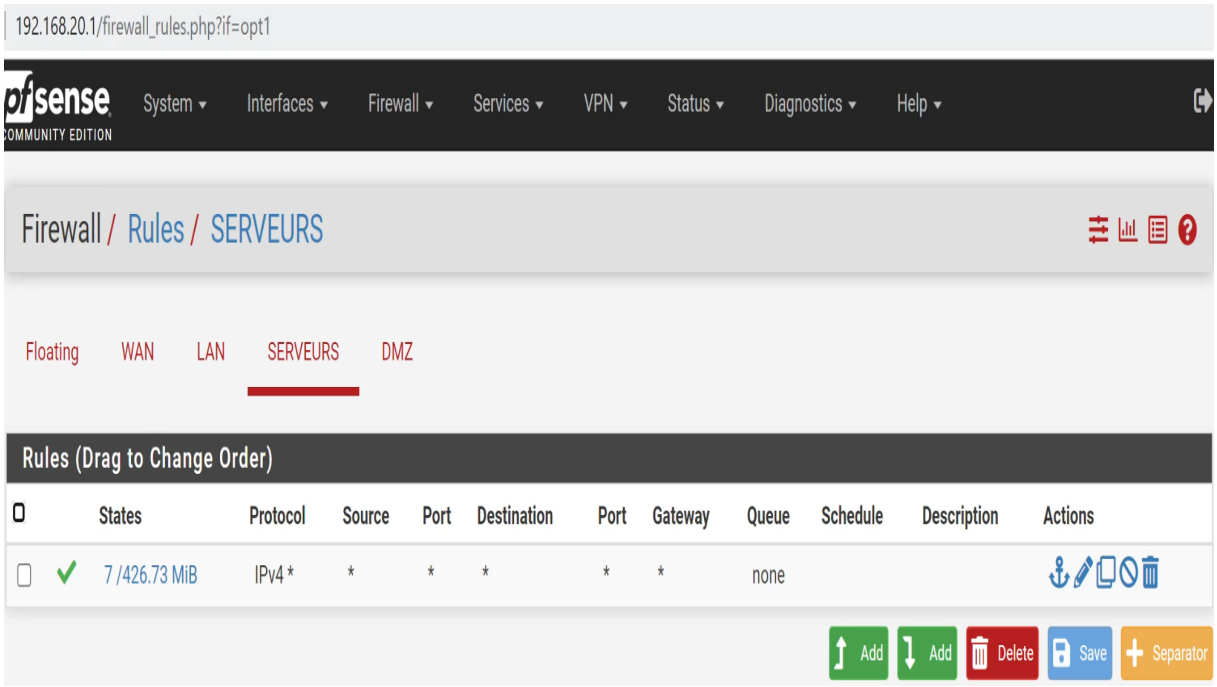

FIGURE 4.24 – Le réseau serveurs

4.4.5 Installation de logiciel Snort sous pfsense

Pour installer Snort sur un par-feu "pfsense" en utilisant le gestionnaire de packages intégré, vous devez accéder à l'onglet "System" de votre pare-feu et sélectionner "Package Manager" dans le menu déroulant. Ensuite vous devez rechercher Snort dans la liste des packages disponibles et cliquer sur "installer".

— La figure 4.24 représente le package Snort recherché.

— La figure 4.25 représente que l'installation du logiciel Snort a été effectuée avec succès.

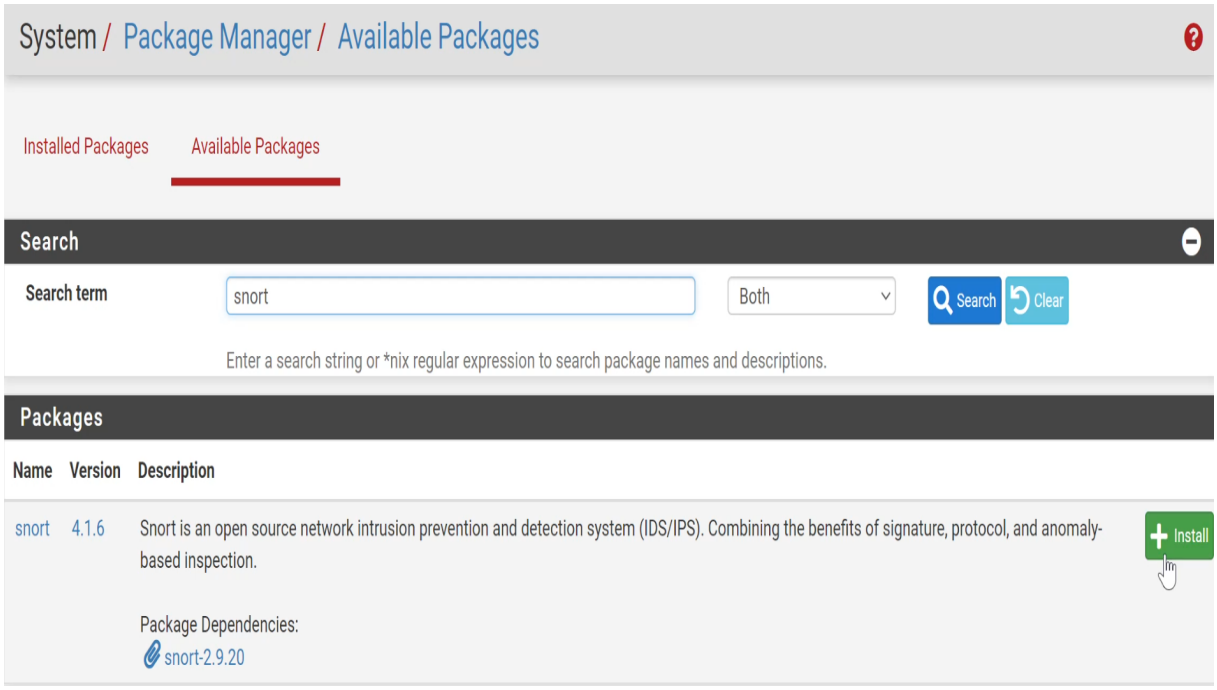

FIGURE 4.25 – Le package de Snort

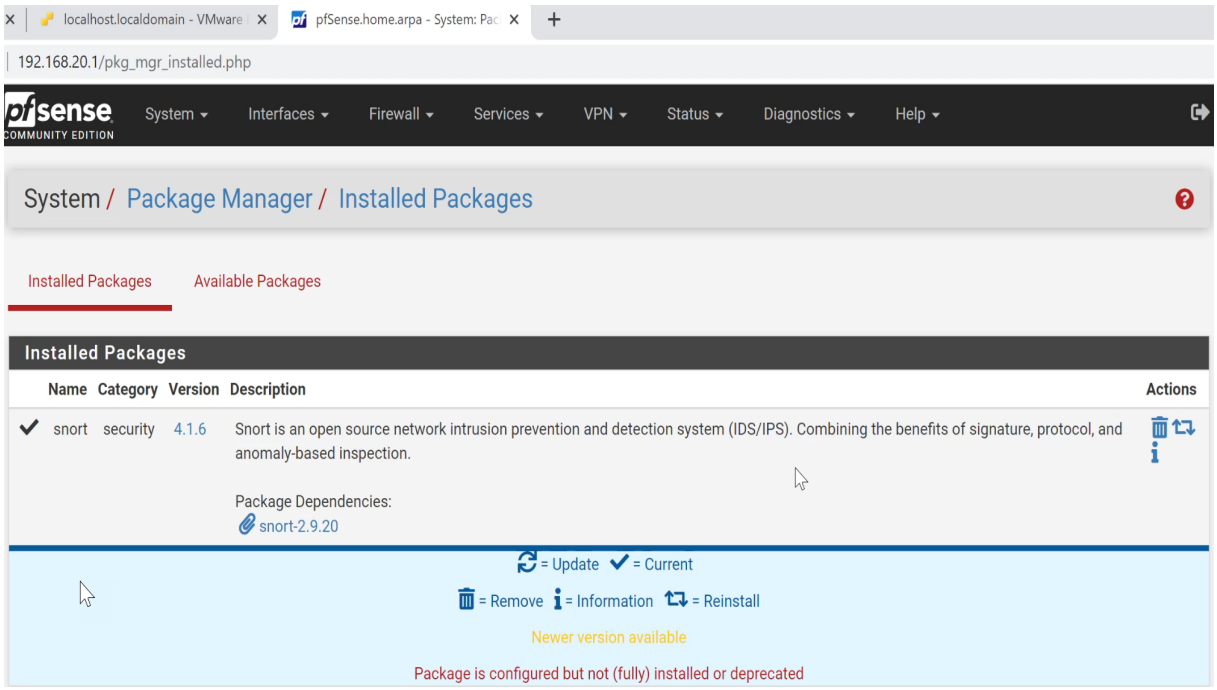

FIGURE 4.26 – Installation réussie de Snort

4.4.5.1 Les configurations globales de Snort

Après l'installation, accéder aux paramètres de Snort en cliquant sur "Global Settings" puis "Snort" pour cocher tout les packages nécessaires et gratuits.

La figure 4.26 représente l'interface des paramètres de logiciel Snort

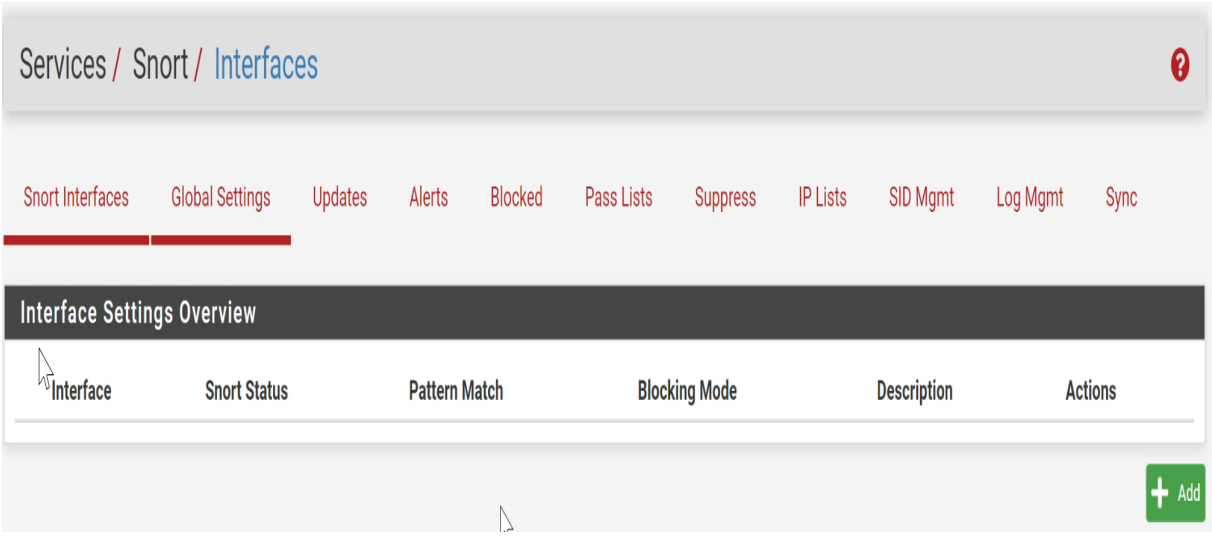

FIGURE 4.27 – Paramètres de Snort

— Les figures ci-dessous représentent les packages nécessaires :

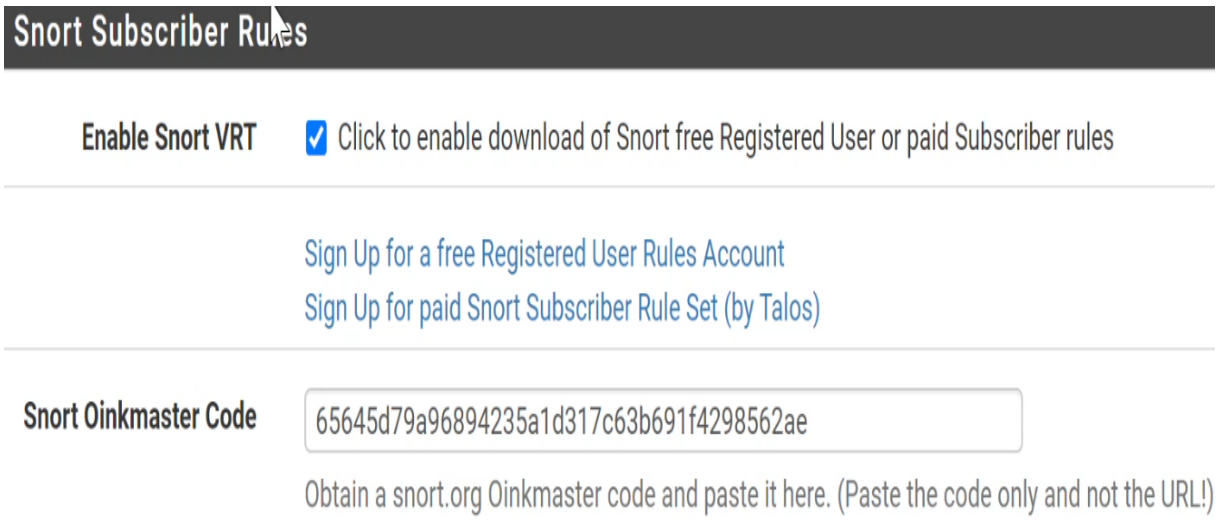

FIGURE 4.28 – Le package de la signature.

FIGURE 4.29 – La licence GPLv2 de Snort.

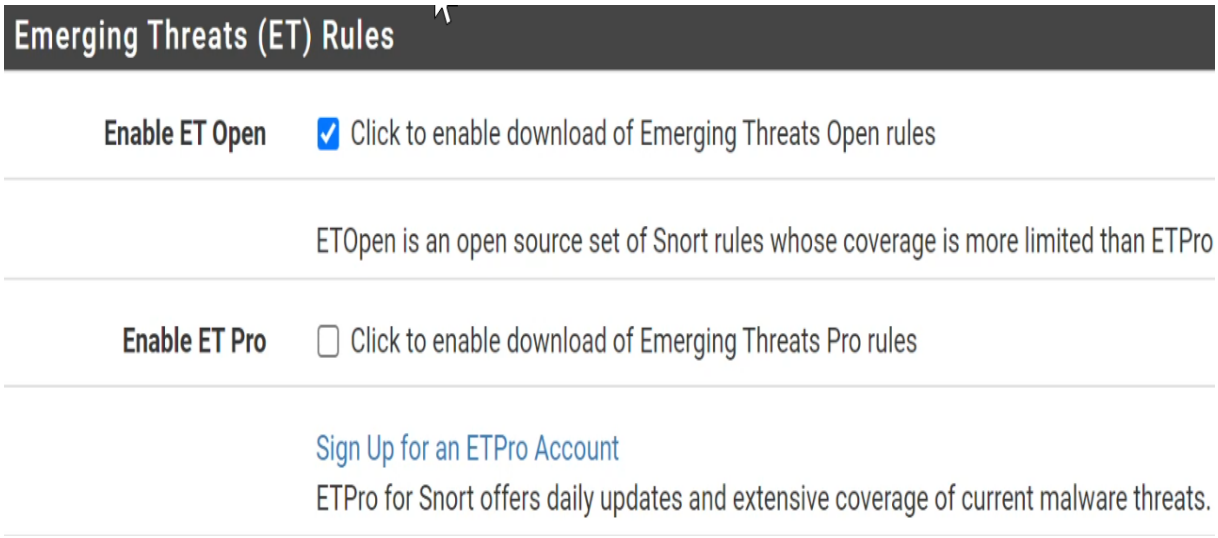

FIGURE 4.30 – Les règles de detèction d'intrusion.

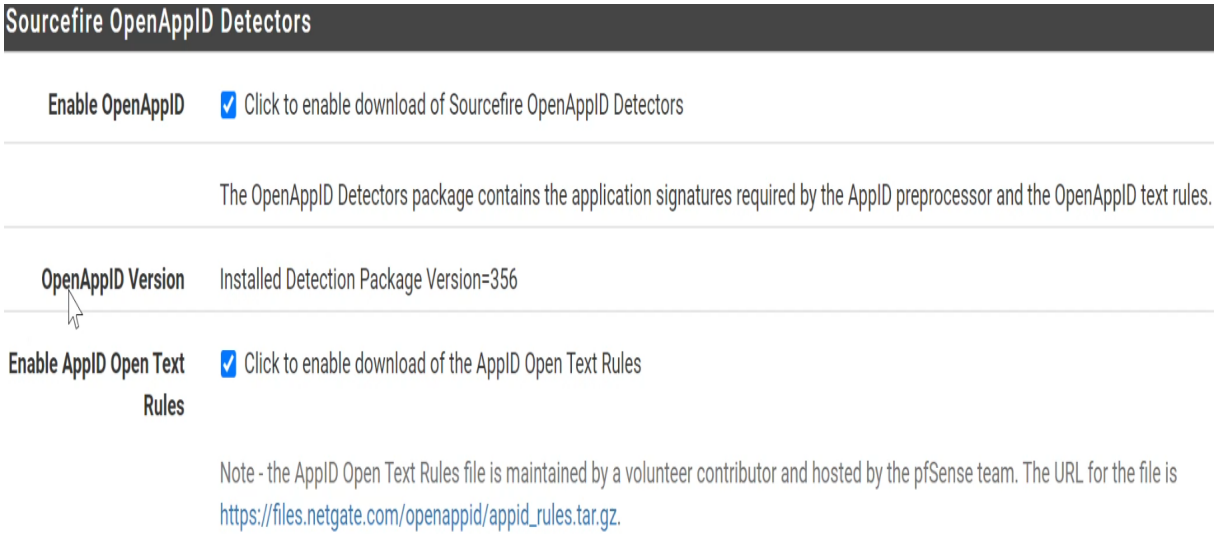

FIGURE 4.31 – Les détecteurs OpenAppID de Sourcefire.

— Les mises à jours de Snort sont essentielles pour maintenir la sécurité de votre système, car elles permettent de garantir que les règles de détection sont à jour et que Snort peut détecter les menaces les plus récentes.
Avec ce package (figure 4.31) les mises se feront automatiquement.

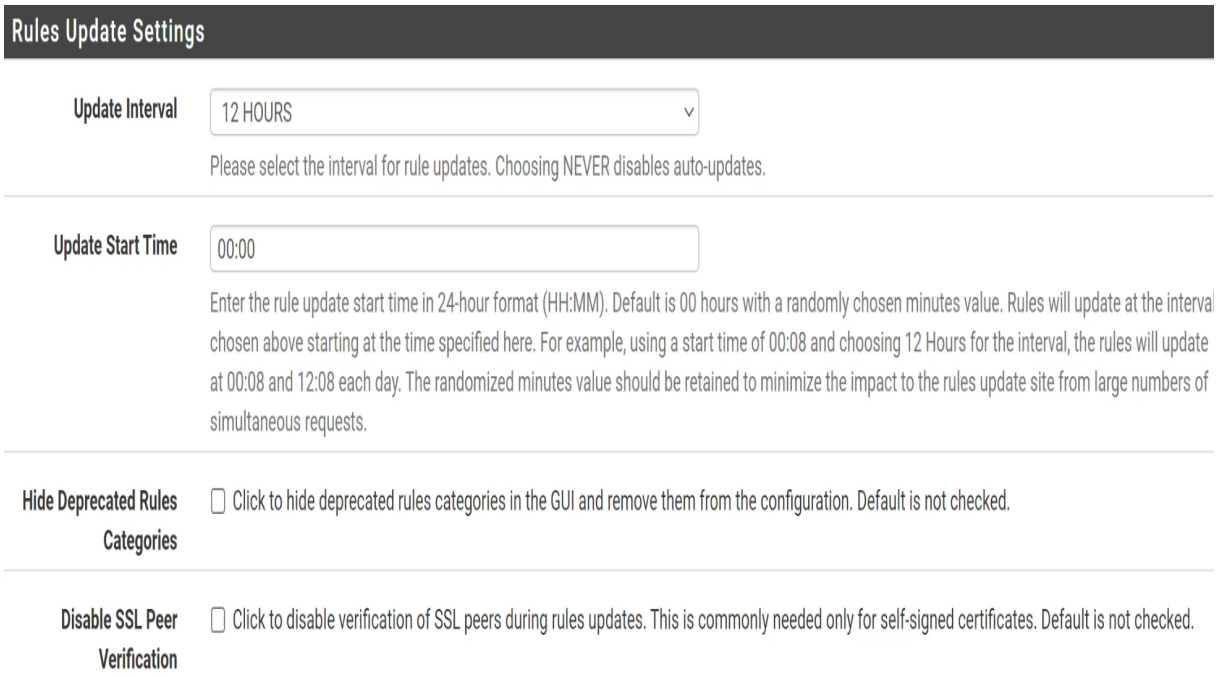

FIGURE 4.32 – Paramètres de mise à jour des règles.

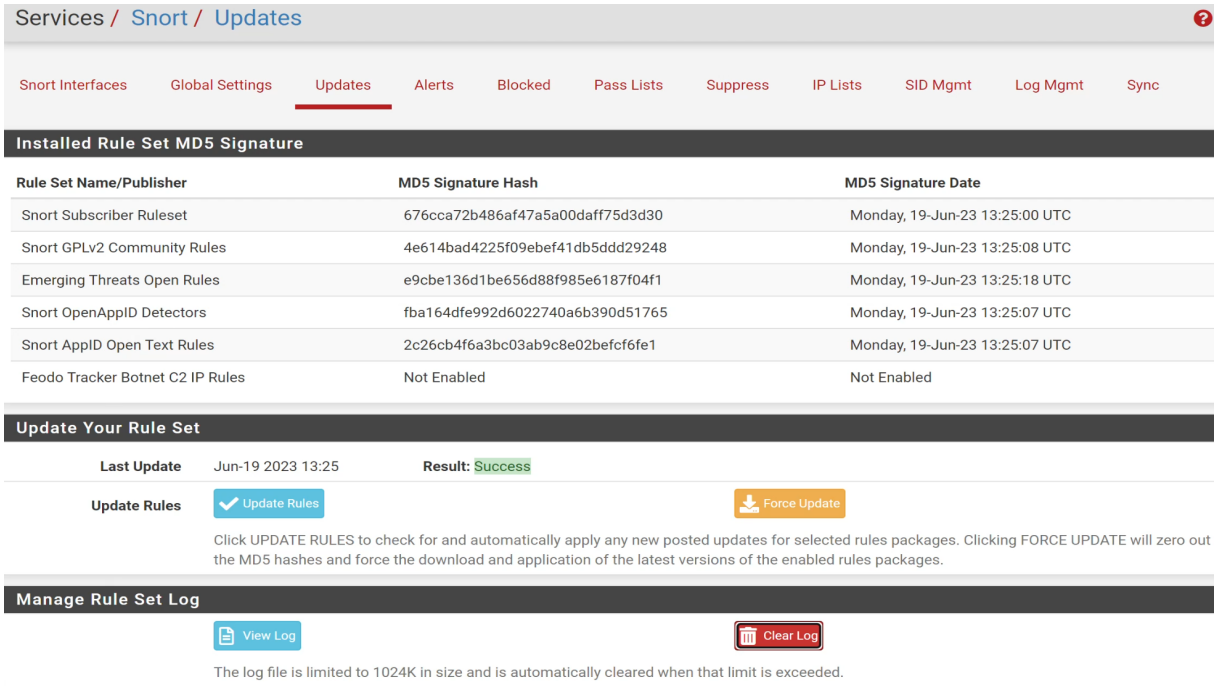

FIGURE 4.33 – Les mises à jour effectuer par Snort

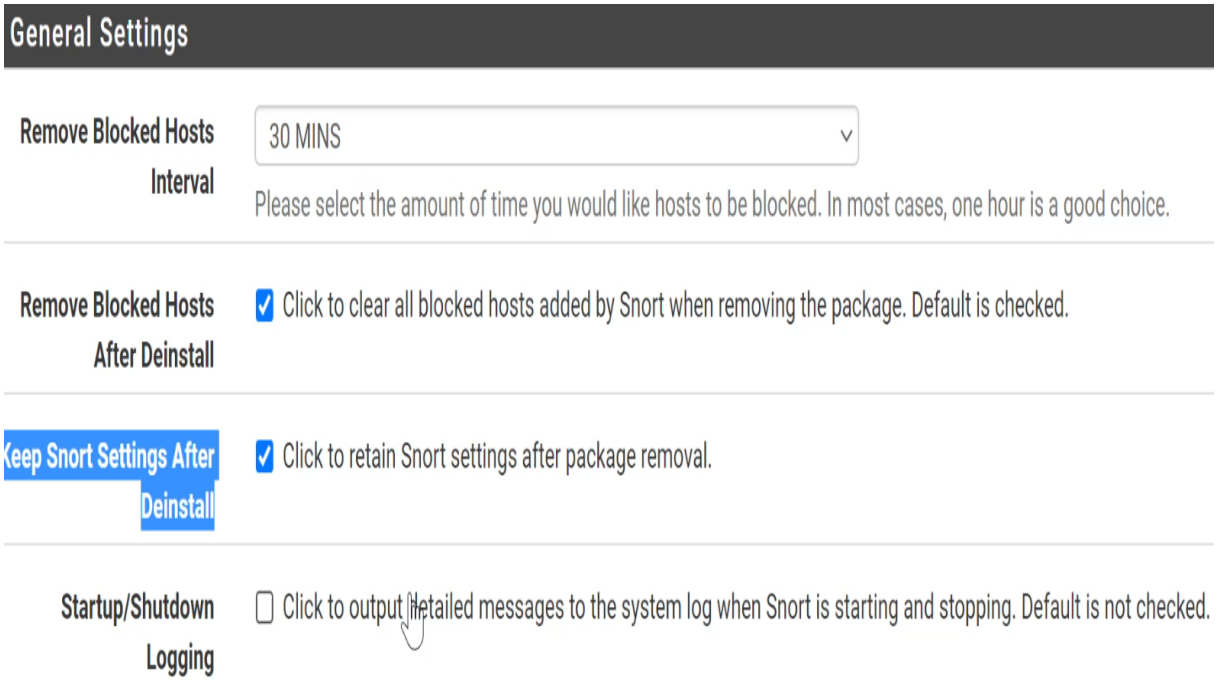

FIGURE 4.34 – Contrôle du temps de blockage.

4.4.5.2 Configuration de l'interface Snort

Nous avons choisi l'interface WAN pour appliquer les détections d'intrusions (Snort). La figure 4.34 illustre les étapes de configurations.

Les deux figures 4.35 et 4.36 représentent les packages utilisés pour la détection des intrusions.

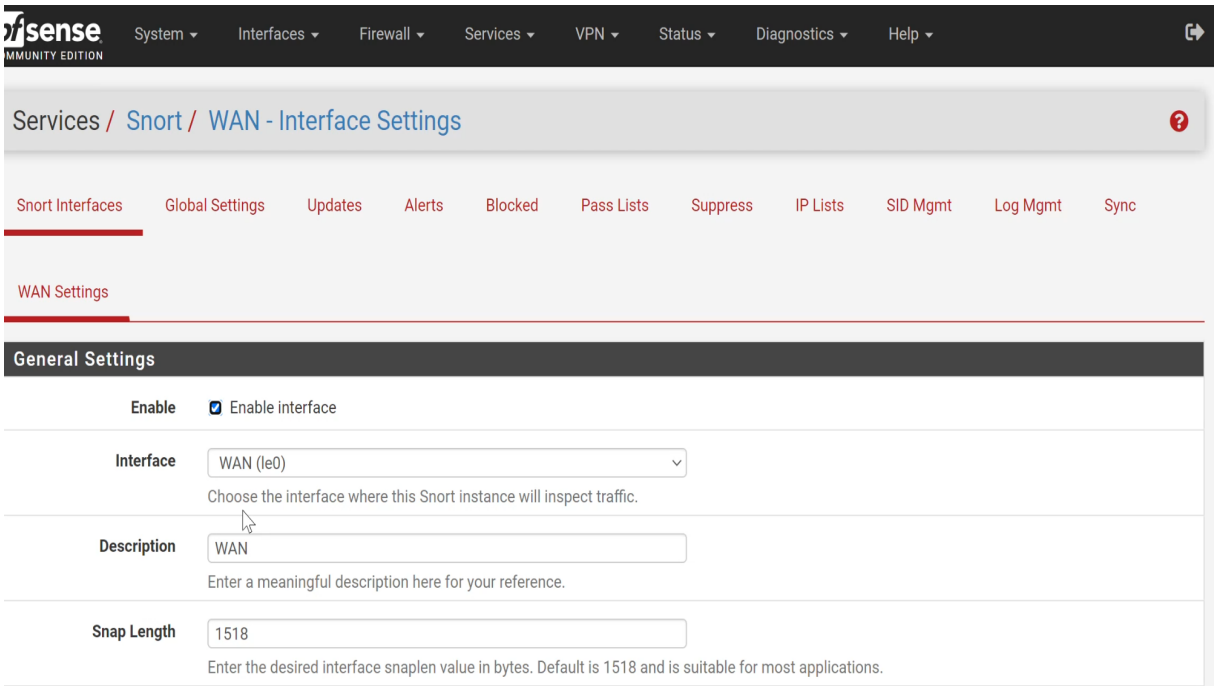

FIGURE 4.35 – L'interface Snort

Alert Settings : Activer les alertes, activer les captures de trafic et enfin envoyer le format en binaire.

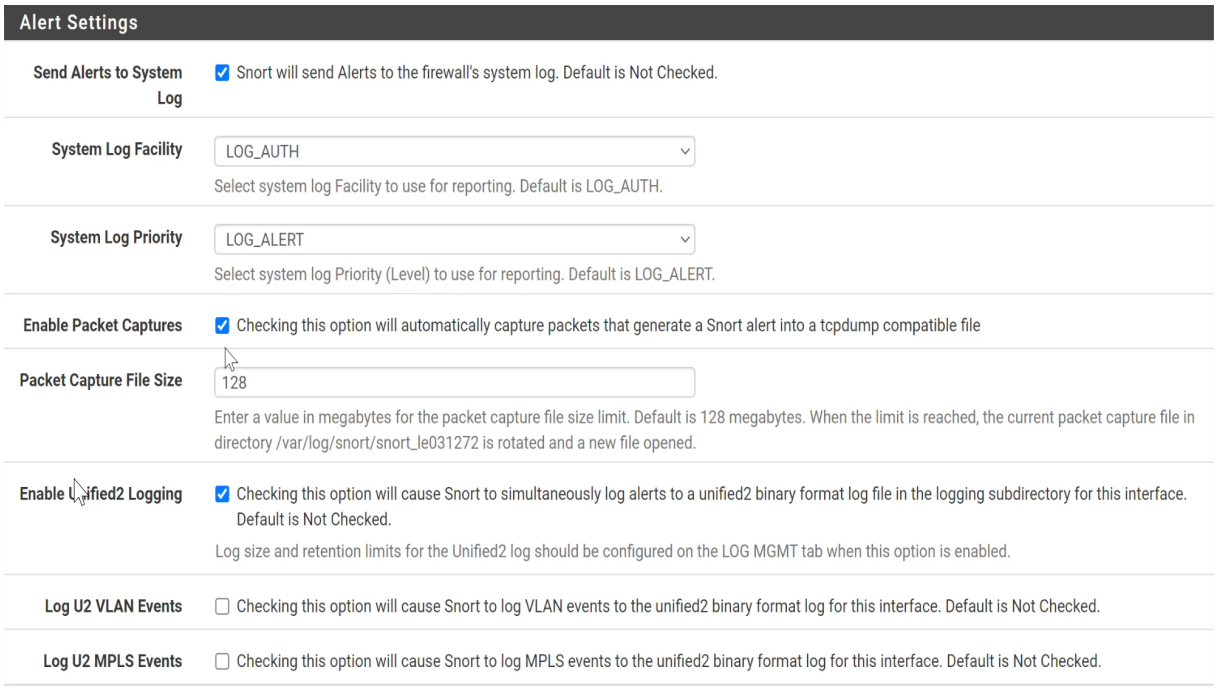

FIGURE 4.36 – Activation des alertes.

— **Block Settings :** Permet de bloquer automatiquement les hôtes qui génèrent une alerte

Snort, assurer que toutes les connexions pour l'adresse IP bloquée sont interrompues.

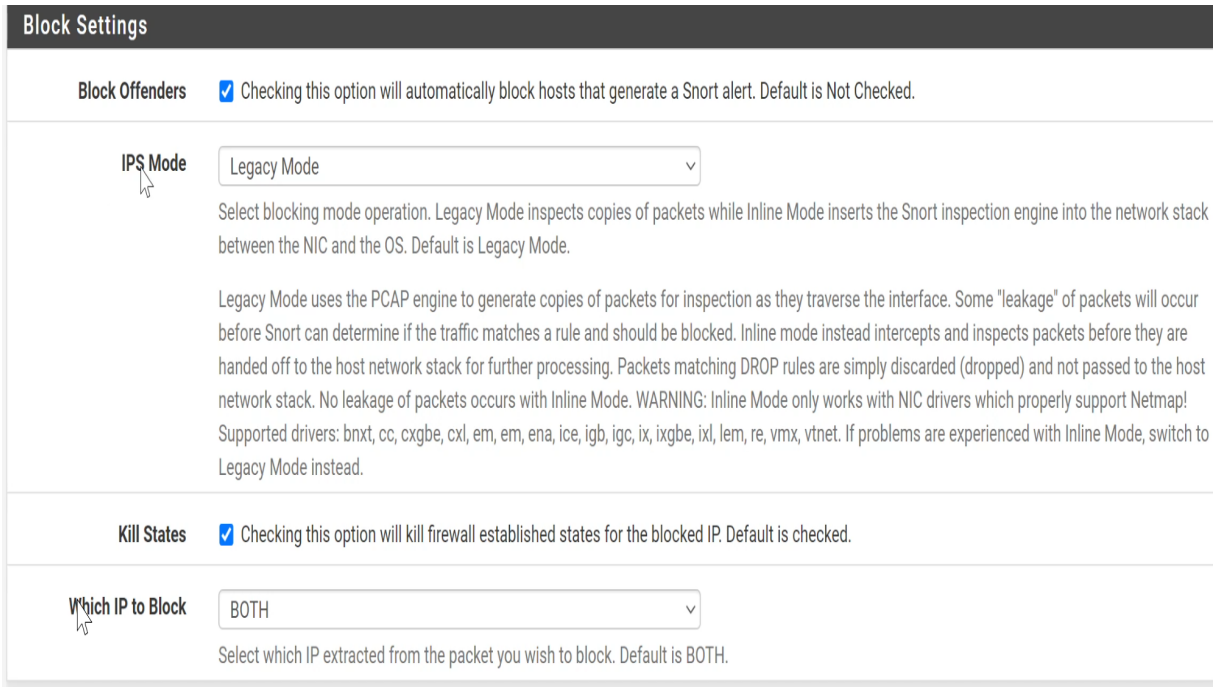

FIGURE 4.37 – Blockage des hôtes.

4.4.5.3 Activation de l'interface Snort

C'est selon les mises à jours que nous avons effectué :
Les étapes pour activer l'interface Snort sont illustrer dans les deux figures 4.37 et 4.38.

Balanced : politique équilibrée de Snort, rapide et elle offre une bonne couverture de base et protège contre la plupart des menaces du jour.

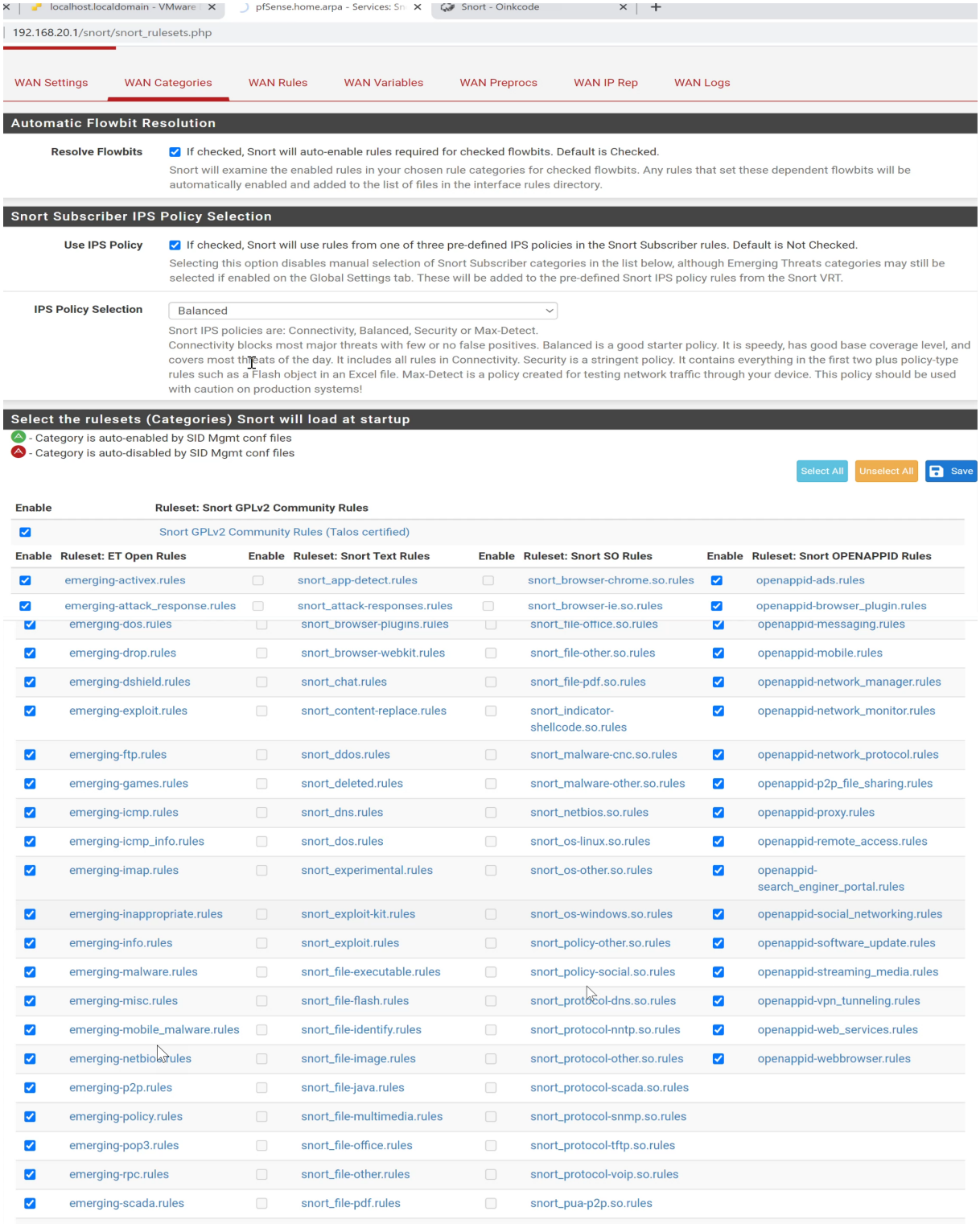

FIGURE 4.38 – Activation de Snort

— Allumage de l'interface Snort.

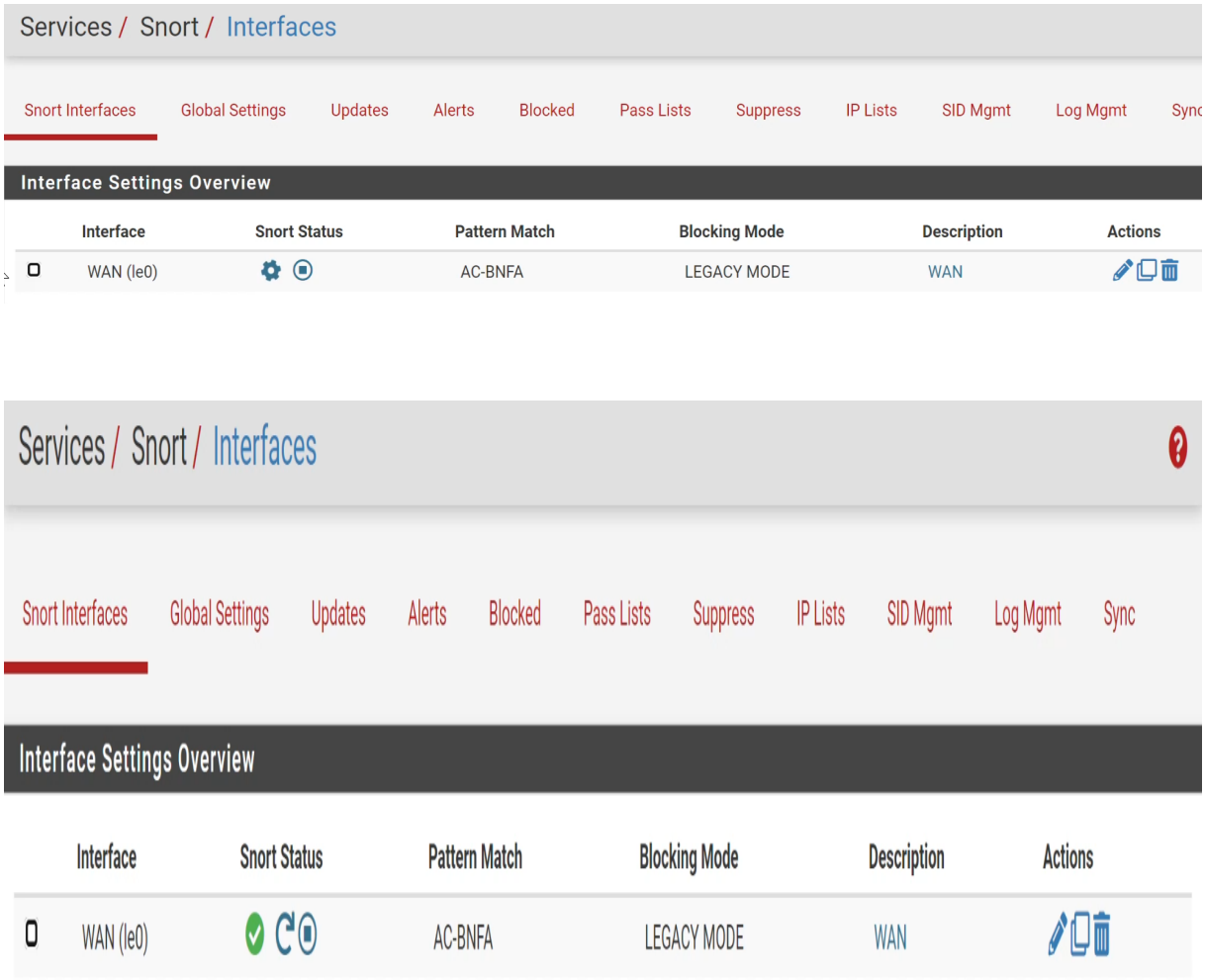

FIGURE 4.39 – Interface en action

— Ouvrir les ports pour recevoir les alertes comme illustrer dans la figure 4.39 .

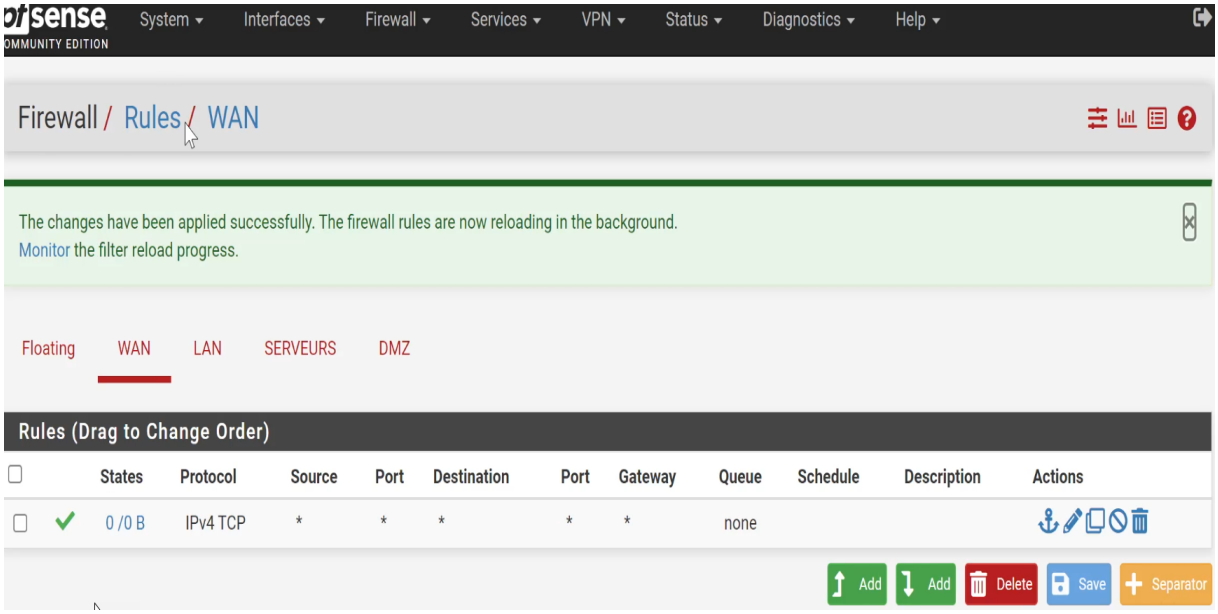

FIGURE 4.40 – Ouverture des ports.

4.5 Analyse des résultats de la solution proposée

4.5.1 test de ping

— La figure 4.40 représente un test de connectivité vers internet après avoir autorisé le trafic réseau.

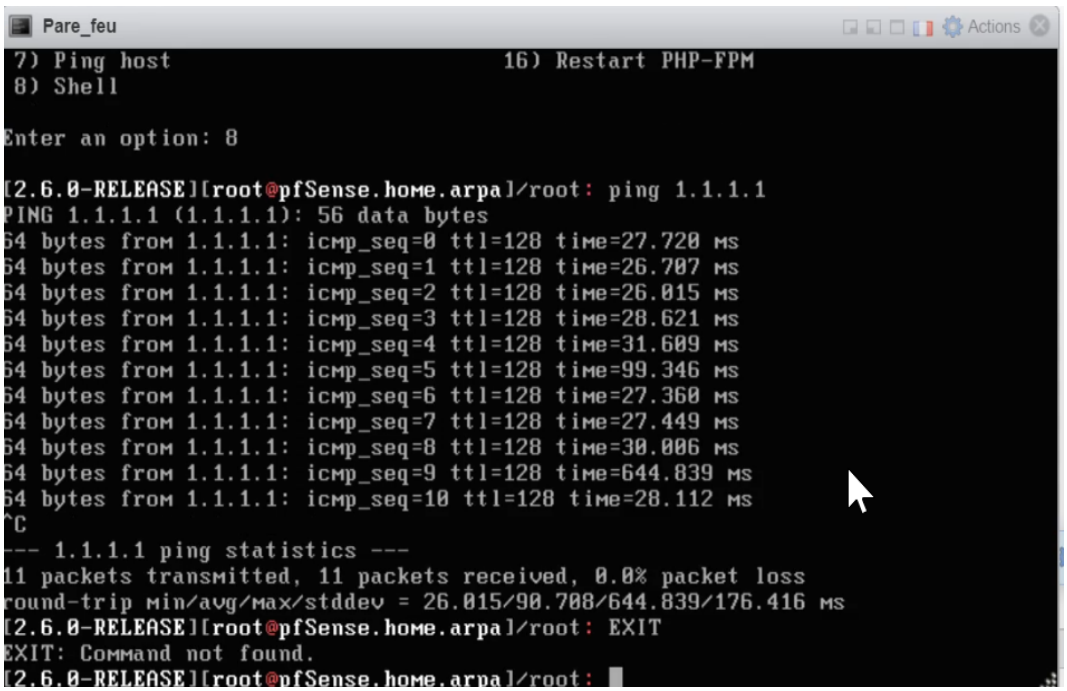

FIGURE 4.41 – Test de connectivité vers l'extérieur (internet)

— La figure 4.41 représente un test de connectivité de la machine client vers internet.

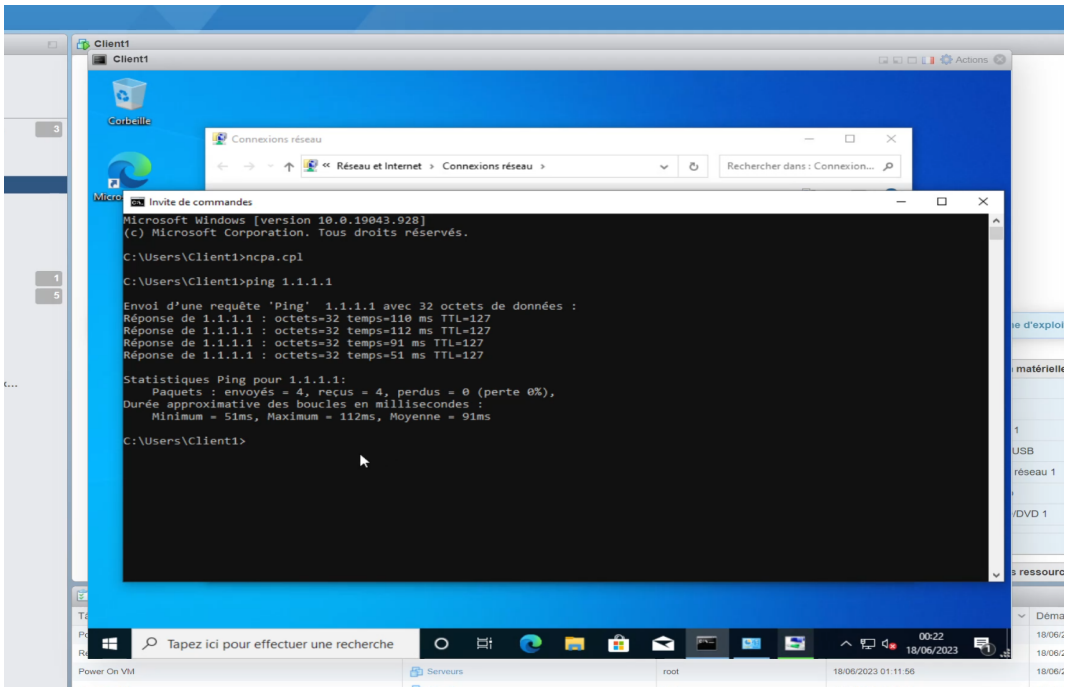

FIGURE 4.42 – Test de connectivité du client vers l'extérieur

— La figure 4.42 représente un test de connectivité de la machine client vers le serveurs.

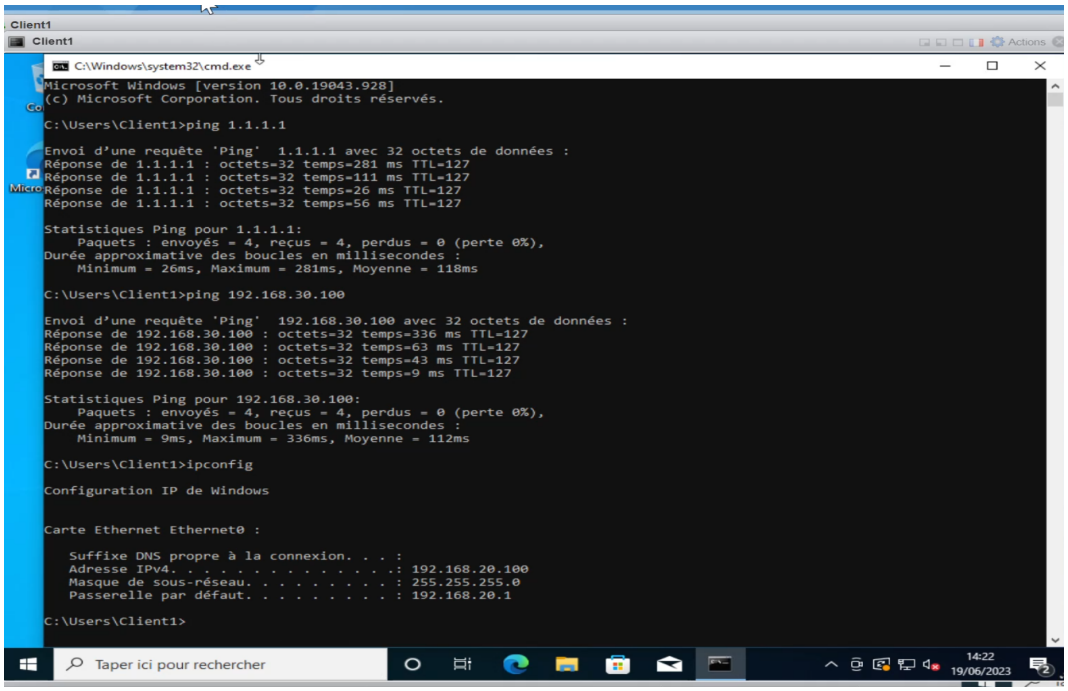

FIGURE 4.43 – Test de connectivité de client vers serveurs

— La figure 4.43 représente la réussite de la connextion du client vers le serveurs.

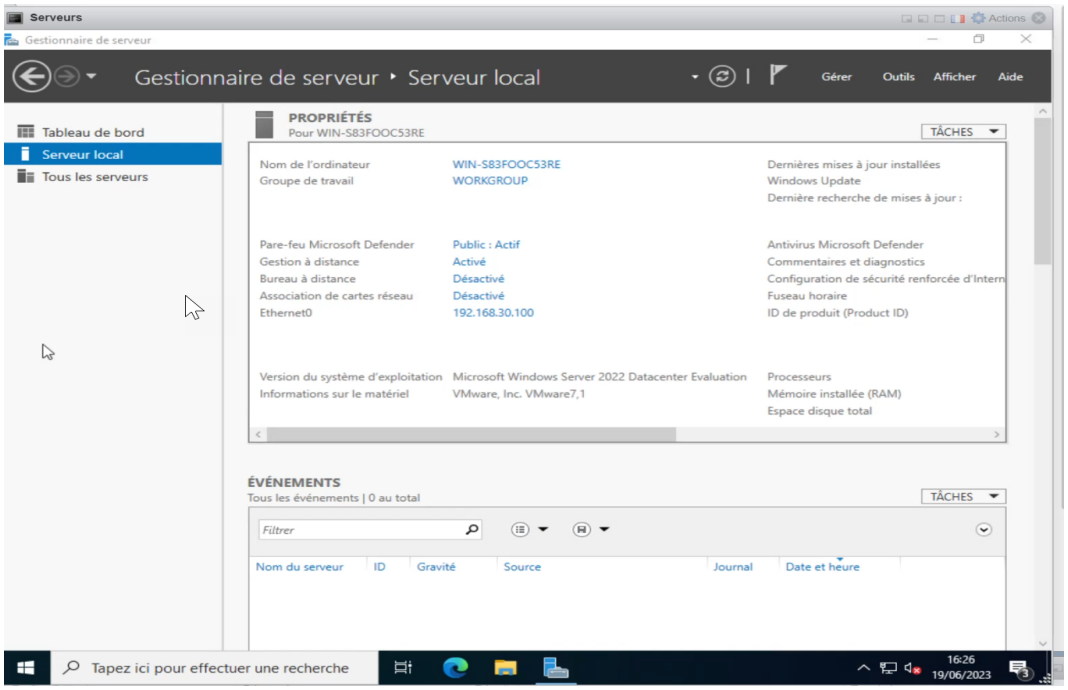

FIGURE 4.44 – Connexion client serveurs

— La figure 4.44 représente un test de connectivité du serveurs vers internet.

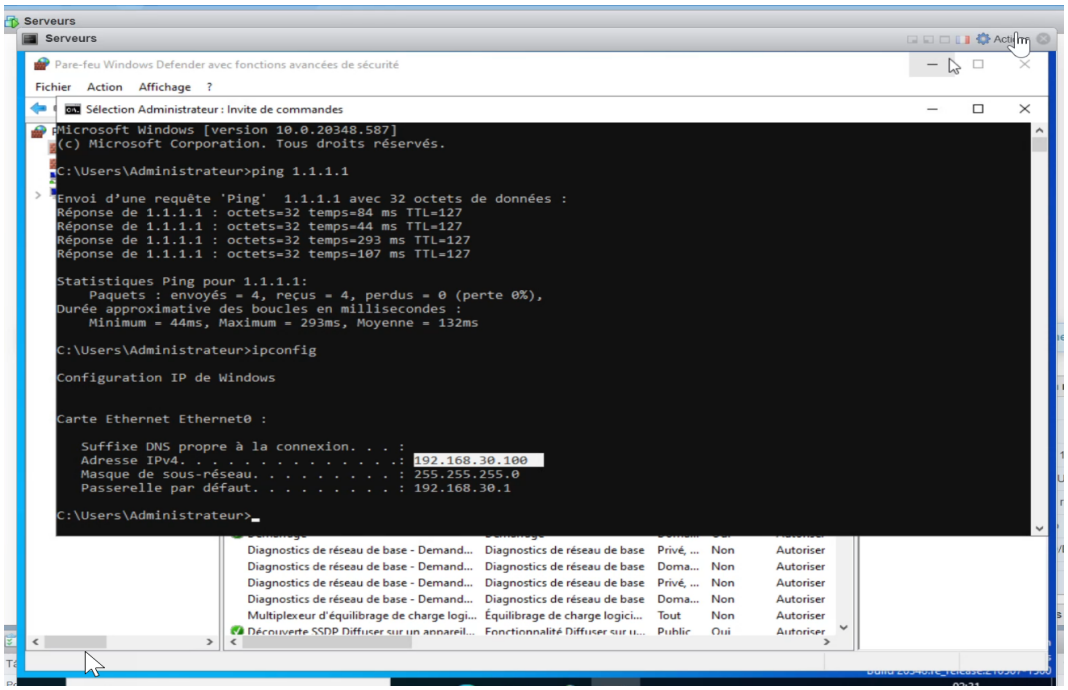

FIGURE 4.45 – Test de connectivité du serveurs vers internet

4.5.2 test de détection d'intrusion

— La figure 4.45 représente l'interface de Kali Linux.

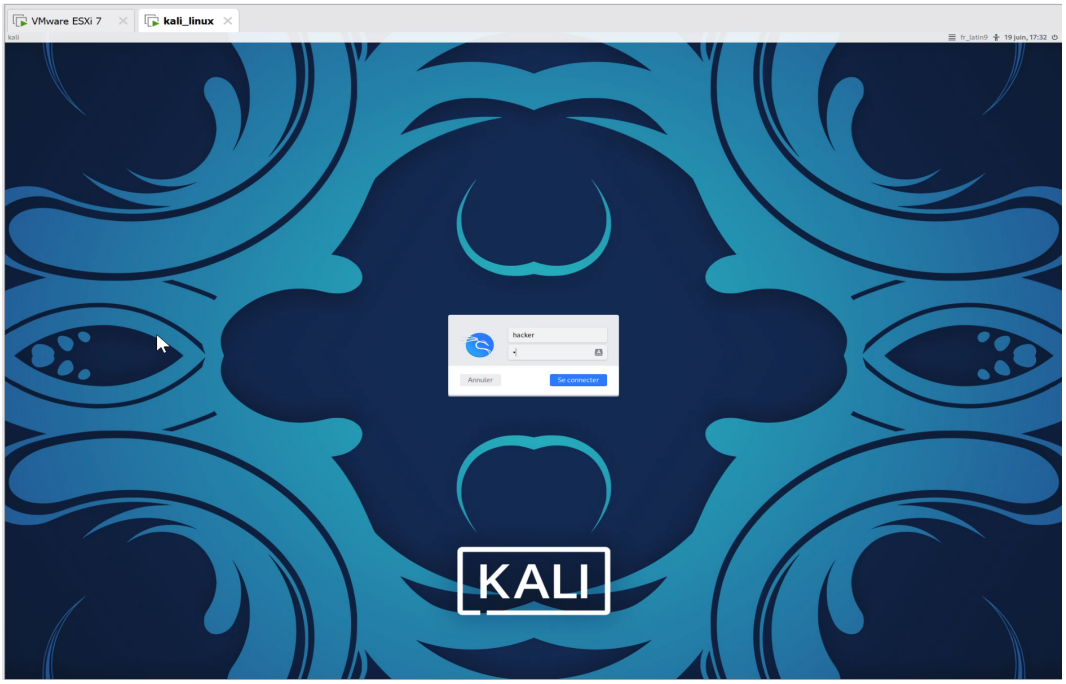

FIGURE 4.46 – L'interface de Kali Linux

— Kali Linux demande une addresse et le firewall va recevoir la demande. Dans ce cas, le serveur DHCP attribue une adresse IP a la machine virtuelle Kali Linux (car il est connecté a la Vmnet8) ce qui lui permet de communiquer avec le firewall.
La figure 4.46 représente la demande de connexion de Kali Linux vers le firewall.

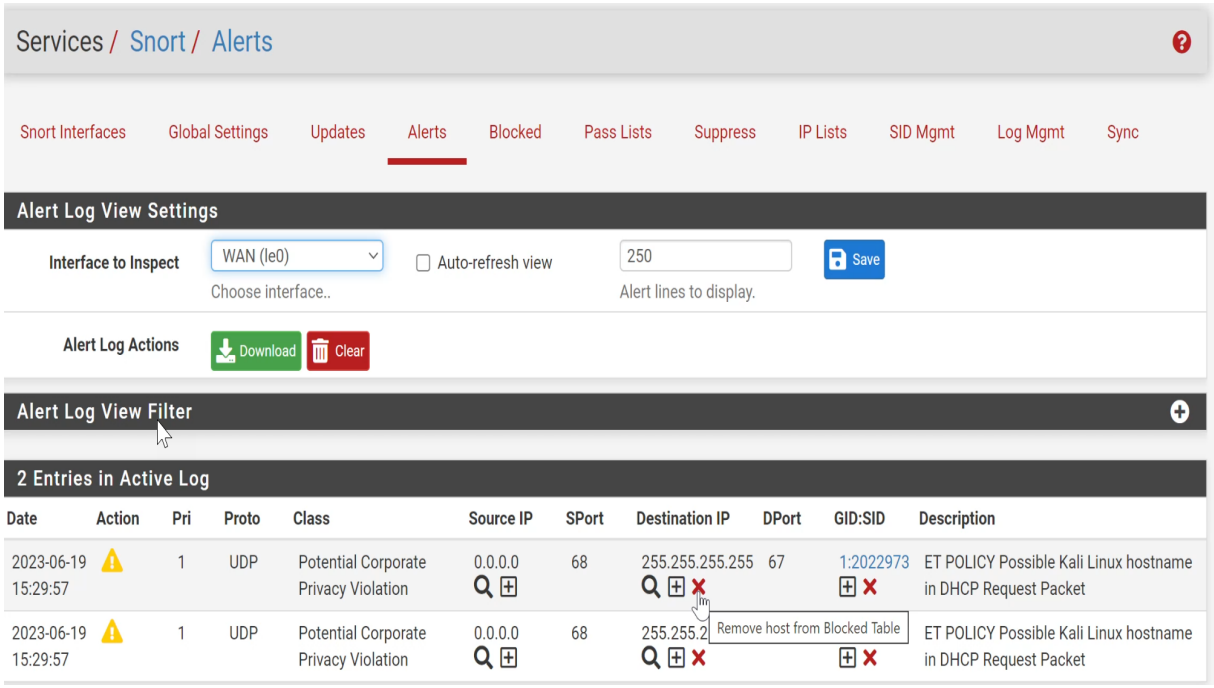

FIGURE 4.47 – La demande de connexion de Kali Linux vers le firewall

— La figure 4.47 représente un test de connectivité du Kali- Linux vers internet.

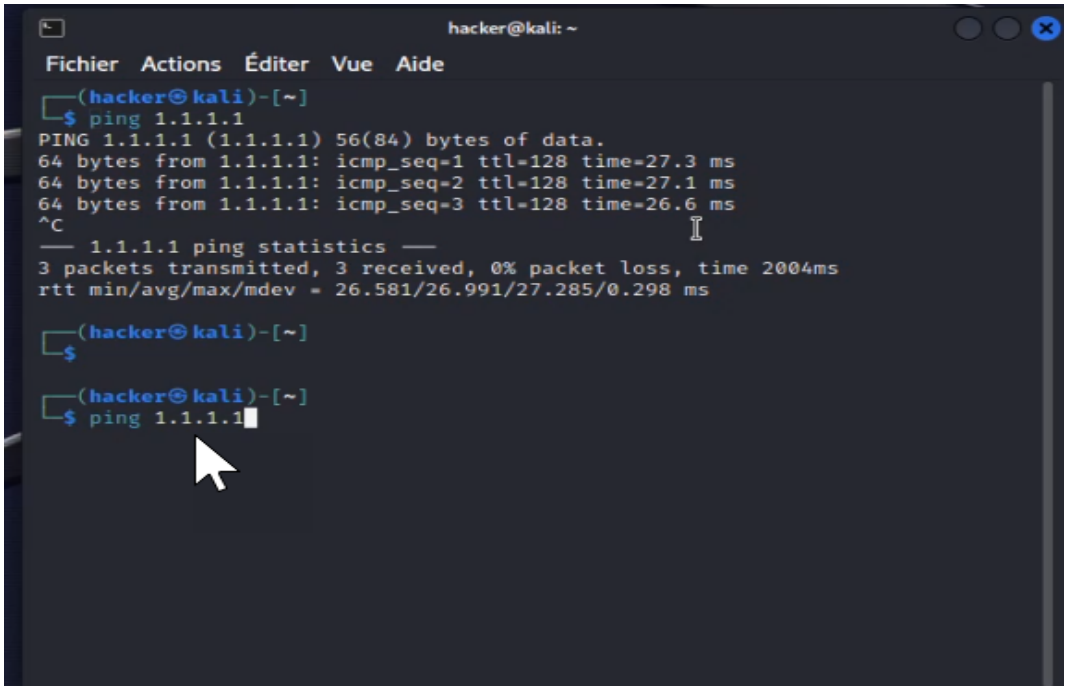

FIGURE 4.48 – Test de connectivité du Kali vers internet

— La figure 4.48 illustre comment lancer un scan a partir de la commande nmap.

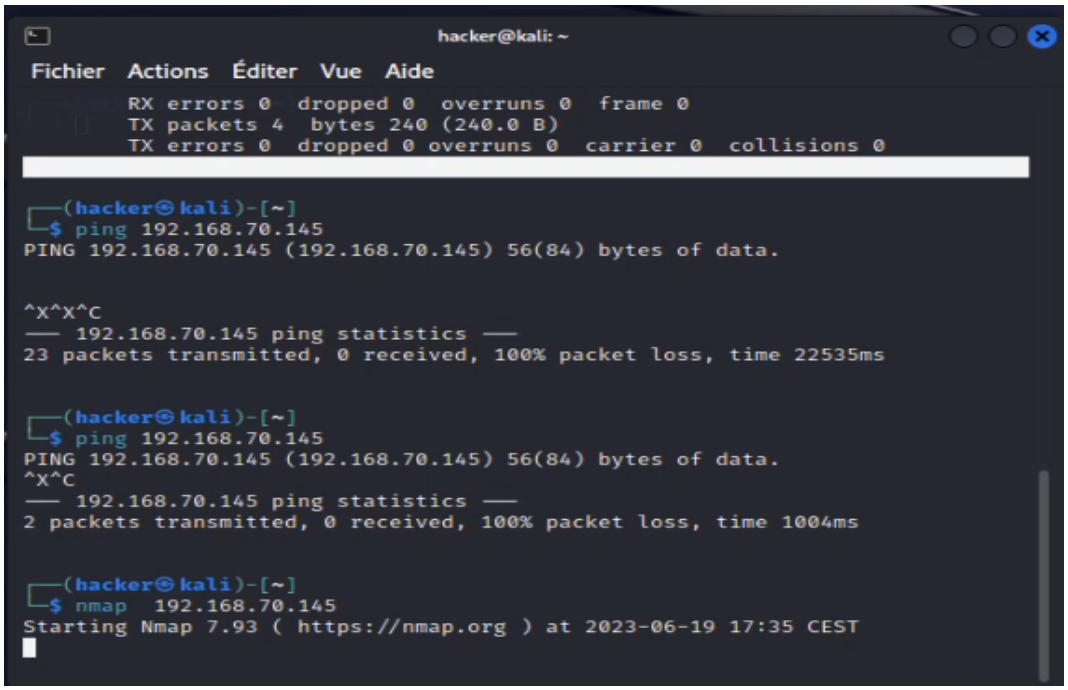

FIGURE 4.49 – Lancement de scan

— Après l'essaye de Kali, le firewall reçoit les alertes.
La figure 4.49 représente les attaques effectuer.

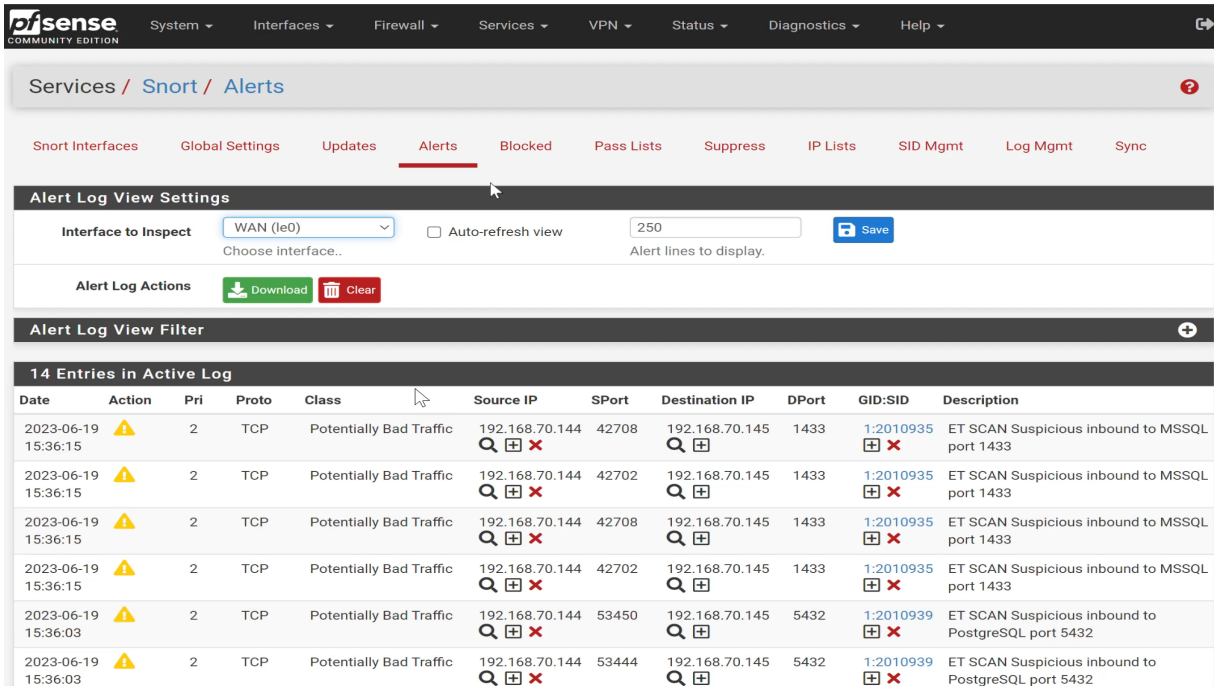

FIGURE 4.50 – Les attaques effectuées

— Les attaques vont être détecter et bloquer par notre Snort.
La figure 4.50 représente comment détecter une attaques.

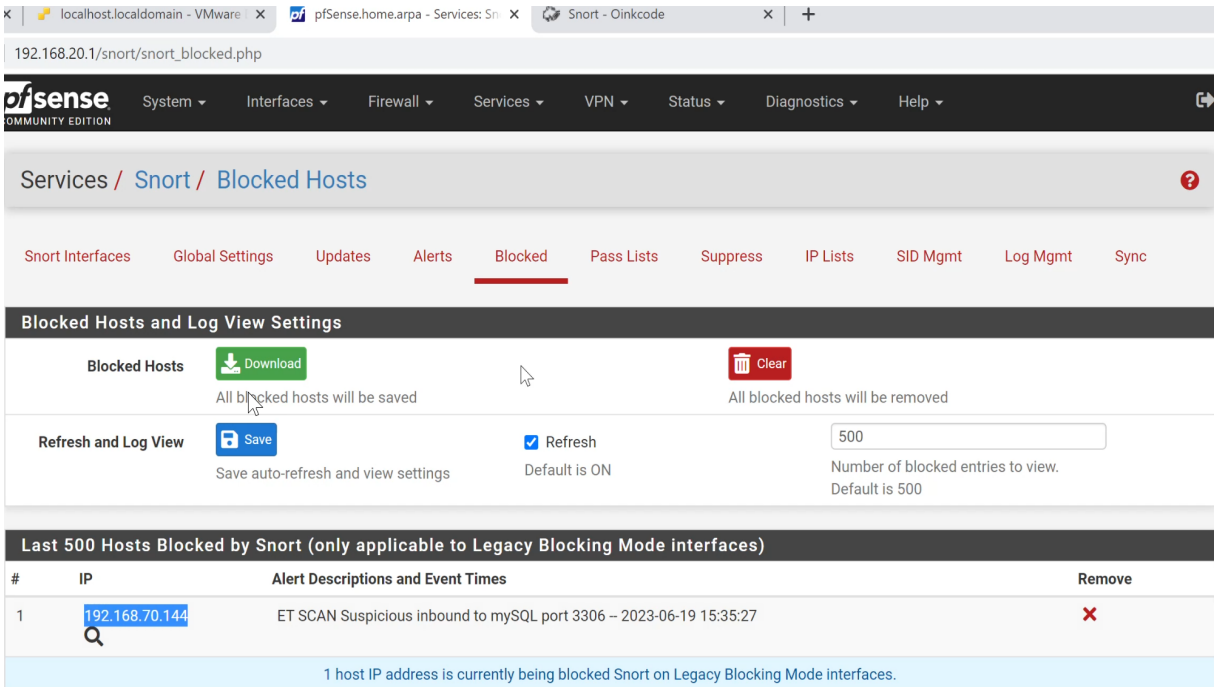

FIGURE 4.51 – La détection et blocage d'attaques

4.6 Conclusion

Dans ce chapitre nous avons apporté des améliorations du réseau de l'EPB pour mettre à jour et renforcer la sécurité de l'entreprise, nous avons décrit les étapes suivies et toute les installations et configurations effectuées pour la mise en place d'un système de prévention d'intrusion en l'implémentant dans un firewall afin de segmenter et surveiller le trafic réseau en utilisant la solution VMware ESXi,certain test sont realisés à la fin du chapitre dans le but de montrer le fonctionnement de snort dans la détection des attaques.

Conclusion générale

En conclusion, ce mémoire a abordé en profondeur l'etude et mise en oeuvre d'une solution de détection d'intrusion sur une infrastructure de virtualisation au niveau de l'EPB. Tout au long de cette étude, plusieurs problèmes ont été identifiés et nécessitent une attention particulière.

Tout d'abord, l'infrastructure de datacenter de l'hyperviseur s'est avérée obsolète, ce qui a mis en évidence le besoin urgent d'une mise à niveau pour garantir la sécurité des systèmes. Les risques liés à une infrastructure obsolète peuvent compromettre la confidentialité, l'intégrité et la disponibilité des données. Ainsi, il est impératif de procéder à une modernisation adéquate afin de renforcer la sécurité de l'ensemble du système.

Le problème identifié concerne le chargement des hôtes, notamment des serveurs et des pare-feu. Une mauvaise gestion du trafic réseau peut entraîner une surcharge des ressources, affectant à la fois les performances et la sécurité du système. Pour résoudre ce problème, il est recommandé de mettre en place un firewall efficace pour segmenter le réseau et limiter l'accès non autorisé aux données et aux ressources de l'entreprise. Cette mesure permettra de renforcer la sécurité globale du système et de prévenir les incidents de sécurité indésirables.

En outre, la mise en place d'un système de detection d'intrusion est une autre solution essentielle pour garantir la sécurité du réseau. En intégrant cette solution au firewall, il sera possible de surveiller le trafic réseau en temps réel, détecter les activités suspectes et réagir rapidement aux éventuelles menaces. Cela renforcera la posture de sécurité globale du système et contribuera à prévenir les intrusions indésirables.

En somme, cette étude a mis en évidence les défis et les enjeux liés à la mise en place d'une solution de détection d'intrusion sur une infrastructure de virtualisation . Les problèmes identifiés ont été abordés en proposant des solutions telles que la modernisation de l'infrastructure, la segmentation du réseau via un firewall et l'implémentation d'un système de detection d'intrusion. En mettant en œuvre ces mesures, il est possible d'établir un environnement de virtualisation sécurisé, assurant la confidentialité, l'intégrité et la disponibilité des données et des ressources de l'entreprise. Cependant, il convient de souligner que la sécurité est un processus continu et qu'il est important de rester vigilant et de mettre à jour régulièrement les mesures de sécurité pour faire face aux menaces émergentes.

Bibliographie

[1] A.MOUMENE ,F.TIGRINE.Virtualisation de la couche infrastructure d'un systeme d'information,cas d'etreprise portuaire d'alger EPAL."Mémoire" .Université de Béjaia.2020/2021

[2] AAhttps ://bluebearsit.com/infrastructure-informatique/ Consulté le 08/06/2023

[3] A.Alnaim,Ahmed M.Alwakeel Eduardo B. Fernandez,A Pattern for an NFV Virtual Machine Environment,"Article",2019

[4] Cours électronique l1 math informatique,R.SOUADIH, 2018 / 2019

[5] Lo, M Massamba.Etude et mise en place s'une solution cloud computing sur une infrastructure de virtualisation,cas d'etude :AISAKAGROUP,"Mémoire",2019.

[6] L. C. Miller, Server virtualization for dummies, John Wiley et Sons inc, New jersey, 2012

[7] D. Barrett, et G. Kipper, Virtualization and Forensics : A Digital Forensic Investigator's Guide to Virtual Environments, Syngress - Elsevier Inc., 2010

[8] K.è Scarfone, M. Souppaya, et P. Hoffman, Guide to Security for Full Virtualization Technologies, NIST Special Publication, 800-125, 2010

[9] A. Newman, A. Patrizio, L. Barrett et A. Goldman, Understanding the Security Implications of Virtualization, Internet.com Security eBook, a division of QuinStreet Inc, 2010

[10] https ://mrproof.blogspot.com/2010/11/securite-informatique-dmz-nat-securite.html consulté le 14/05/2023

[11] https ://https ://www.frameip.com/vpn/consulté le 11/05/2023.

[12] Y.KHERROUBI, K.IDIR .Mise en œuvre d'une sécurité réseau basée sur l'utilisation du pare-feu PfSence Cas : Algérie Télécom de Tizi-Ouzou."mémoire" 22/09/2018

[13] https ://syxperiane.com/infrastructure-informatique/ Consulté le 17/05/2023

[14] Mathieu Caizergues.Point sur la virtualisation."Arcticle".2013

[15] A.Arnaud,P.Alain ,Vitualisation et partage de charge."Mémoire",2014

[16] L. Bonnet Bearstech. Etat de l'art des solutions libres de virtualisation pour une petite entreprise

[17] G. Collier, D. Plassman, et M. Pegah, Virtualization's Next Frontier : Secu-rity."Mémoire", 2007

[18] M. Rosenblum, and T. Garfinkel, Virtual Machine Monitors : Current Technology and Future Trends, IEEE Computer Society."Mémoire", 2005

[19] J. Hoopes, Virtualization for Security, Syngress – Elsevier Inc."Mémoire",2009

[20] J. Sahoo, S. Mohapatra, et R. Lath, Virtualization : A Survey on Concepts, Taxanomy and Associated Security Issues, IEEE Computer Society,"Mémoire", 2010.

[21] D. Barrett, et G. Kipper, Virtualization and Forensics : A Digital Forensic Investiga- tor's Guide to Virtual Environments, Syngress - Elsevier Inc,"Mémoire", 2010

[22] K.è Scarfone, M. Souppaya, et P. Hoffman, Guide to Security for Full Virtualization Technologies, NIST Special Publication, 800-125, 2011

[23] J. Hoopes, Virtualization for Security, Syngress – Elsevier Inc., 2009

[24] https ://wikimemoires.net/2012/08/quest-ce-quun-firewall-fonctionnement-et-types-de-firewall/ consulté le 14/05/2023

[25] D.Mizouza.Optimisation de systeme de detection d'intrusion (IDS) sans le reseau viéculaire V2G à l'aide des regeles d'associations maximales et de la regression logistique ."mémoire".Université de Quebec à trois rivieres .Août 2022

[26] J. Hoopes, Virtualization for Security, Syngress – Elsevier Inc., 2009

[27] A. Newman, A. Patrizio, L. Barrett et A. Goldman, Understanding the Security Implications of Virtualization, Internet.com Security eBook, a division of QuinStreet Inc, 2010

[28] D. Barrett, et G. Kipper, Virtualization and Forensics : A Digital Forensic Investigator's Guide to Virtual Environments, Syngress - Elsevier Inc, 2010

[29] S. Riebach, B. Toedtmann, E. Rathgeb. Combining IDS and Honeynet Methods for Improved Detection and Automatic Isolation of Compromised Systems, Computer Networking Technology Group, Institute for Experimental Mathematics, University Duisburg-Essen, Germany, (2006)

[30] M. Benjamin, Corrélation d'alertes issues d'outils de détection d'intrusions avec prise en compte d'informations sur le système surveillé. Thèse de doctorat, Institut National des Sciences Appliquées de Rennes. Rennes, France, (février 2004)

[31] S. Noel, S. Jajodia, B. O'Berry, M. Jacobs, Efficient Minimum-Cost Network Hardening Via Exploit Dependency Graphs, ACSAC'03 Proceedings of the 19th Annual Computer Security Applications Conference, IEEE Computer Society Washington, DC, USA, ISBN :0769520413, (2003).

[32] K. Ingols, R. Lippmann, K. Piwowarski, Practical Attack Graph Generation for Network Defense, ACSAC'06 Proceedings of the 22nd Annual Computer Security Applications Conference , 121-130, (2006)

[33] V. Paxson, Bro : A System for Detecting Network Intruders in Real-Time, Computer Networks, Proceedings of the 7th USENIX Security Symposium San Antonio, Texas, (janvier 1998)

[34] S. J. Stolfo Lee, W. and K. W. Mok. Adaptive intrusion detection : A data mining approach,. Artificial Intelligence Review 14 (6), 533567. (2000)

[35] D. Dasgupta and F. A. Gonzalez. An intelligent decision support system for intrusion detection and response. International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS), St.Petersburg. Springer-Verlag„ (21-23 mai, 2001)

[36] F.Teng. « Management des données et ordonnancement des tâches sur architectures distribuées ». École Centrale Paris et Manufactures. "Thèse pour l'obtention du grade de Docteur", octobre 2011

[37] H.Bouzayani.Modèle quantitatif pour la détection d'intrusion.Une architec-ture collaborative IDS-HONEYPOT."Mémoire de Maîtrise".Université de Québec en Outaouais,2018

[38] H.Debar, B.Morin, F.Cuppens, F.Autrel, L.Mé, B.Vivinis S.Benferhat, M.Ducassé, R.Ortalo, Détection d'intrusions : corrélation d'alertes. Article de synthèse, Caen, France, 2004.

[39] C.Michel, Langage de description d'attaques pour la détection d'intrusions par corrélation d'événements ou d'alertes en environnement réseau hétérogène, thèse de doctorat de l'Université de Rennes1,16 Décembre 2003

[40] L. Arockiam et N.Veeraragavan Enhancing Data Security during Transit in Public Cloud.Irudayasamy Amalraj."Article",2013.

[41] H.Bouzayani.Modèle quantitatif pour la détection d'intrusion.Une architecture collaborative IDS-HONEYPOT."Mémoire de Maîtrise".Université de Québec en Outaouais,2018

[42] N.Dagrorn.Détection et prévention d'intrusion :présentation et limites."Rapport de recherche,2006

[43] EPB,2020,Documentation de l'entreprise.

[44] https ://www.portdebejaia.dz/download/brochure-epb.pdf

[45] https ://www.portdebejaia.dz/

[46] https ://www.ionos.fr/digitalguide/serveur/configuration/kali-linux/ 20/06/2023

[47] M.Bekono, Y.Fouda, S.Georges . Mise en place d'un environnement reseau virtuel en utilisant GNS3. Institut Africain,Cameroun.2020-2021

[48] K.Scarfone, M. Souppaya, et P. Hoffman, Guide to Security for Full Virtualization Technologies, NIST Special Publication, 800-125, 2011

Résumé

Arrivés au terme de notre mémoire de fin d'études dont le thème est intitulé : «Etude et mise en oeuvre d'une solution de détection d'intrusion sur une infrastructure de virtualisation», on se rend bien compte que ce n'est pas facile d'assurer une sécurité à un réseau et de le protéger contre d'éventuelles intrusions.

L'entreprise portuaire de bejaia, est confrontée à des problèmes liés à son infrastructure informatique,Pour faire face nous avons mis en place une solution utilisant un hyperviseur de type 1, VMware ESXi. Au sein de cet hyperviseur, nous avons intégré un pare-feu pour segmenter le réseau et restreindre l'accès non autorisé aux données et aux ressources de l'entreprise. De plus, nous avons recommandé l'ajout d'un système de détection d'intrusion (IDS) intégré au pare-feu afin de surveiller le trafic réseau et détecter les activités suspectes.

Notre travail a donc permis d'aborder en détail cet aspect de sécurité et de proposer des solutions adaptées pour assurer la protection de l'infrastructure de virtualisation .

Mots clés : virtualisation, infrastructure,sécurité,VMware ESXI,hyperviseur,pare-feu,IDS.

Abstract

At the end of our dissertation entitled : "Study and implementation of an intrusion detection solution on a virtualization infrastructure", we realize that it's not easy to ensure the security of a network and protect it against possible intrusions.

Bejaia port company is facing problems with its IT infrastructure. To deal with them, we have set up a solution using a type 1 hypervisor, VMware ESXi. Within this hypervisor, we integrated a firewall to segment the network and restrict unauthorized access to company data and resources. In addition, we recommended the addition of a firewall-integrated intrusion detection system (IDS) to monitor network traffic and detect suspicious activity.

Our work has therefore enabled us to address this aspect of security in detail, and to propose appropriate solutions for protecting the virtualization infrastructure.

Keywords : virtualization, infrastructure,security,VMware ESXI,hypervisor,firewall,IDS.