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 d'obtention du diplôme de Master en Informatique.
Option : Administration et Sécurité des Réseaux.

Thème

Etude et mise en place d'une politique de sécurité sur une infrastructure de virtualisation

Cas ou niveau: Entreprise Sonatrach de Bejaia

Réalisé par :
Mlle SAHKI Imane

Devant le jury composé de :

Président	**Mr. SADI Mustapha**	**U. A/Mira Béjaïa**
Examinateur	**Mr. KABYL Kamal**	**U. A/Mira Béjaïa**
Encadrant	**Mr. OUZGGANE Redouane**	**U. A/Mira Béjaïa**
Encadreur de Stage	**Mr. SOUADIH Kamel**	**Entreprise Sonatrach de Bejaia**

Septembre 2023

Remerciements

Au terme de ce travail, je tiens à exprimer ma profonde gratitude et mes sincères remerciements.

Je remercié dieu le tout puissant de m'avoir donné la force, la volonté de donner le meilleur de moi-même et le courage de mener ce travail.

Je tiens en premier lieu à exprimer ma profonde reconnaissance à mon encadreur Mr.**OUZEGGANE Redouane** pour son encadrement, pour ça confiance, son encouragement et ses conseils au cours de mon cursus.

J'exprime aussi ma reconnaissance pour le directeur de la RTC Bejaïa de m'avoir aidé et facilité la tâche à effectuer mon stage.

Je remercié vivement et en particulier mon encadreur de stage Mr **SOUADIH Kamel** pour son encadrement et son orientation avec rigueur tout au long de mon stage inspirant de ma curiosité et de ma passion pour promouvoir la réalisation de ce travail.

Je tiens également à remercier les membres de jurys d'avoir consacrés leurs temps à la lecture et à la correction de ce mémoire.

Je remercié particulièrement mes parents, qui m'ont vraiment soutenu et m'avoir donné tout le courage, dont j'avais énormément besoin cela a produit volonté et confiance en moi, je serai éternellement reconnaissante pour eux.

Dédicace

Je dédie ce modeste travail . . .
A mes chers parents
Sans les quel je ne serais pas là aujourd'hui, eux qui étaient derrière moi à chaque seconde de ma vie dans les bons et les mauvais moments, même si j'écrirais un texte immense à la Victor Hugo je ne les remercierais pas assez, En signe de reconnaissance de l'immense bien que vous ayez fait pour moi concernant mon éducation qui aboutit aujourd'hui à la réalisation de ce travail. Recevez à travers ce dernier, toute ma gratitude et mes profonds sentiments.
Que Dieu tout puissant soit vous accorde santé, bonheur et prospérité Inchallah. Mes chers frères ET ma chère sœur Yanis et Rayane et Sarah

Table des matières

Table des figures

Liste des tableaux

Listes d'abréviation

AD	Active Directory
CDV	Centre données virtualisés
CPU	Central Processing Unit
CIP	Confidentiality and Integrity Protection
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
DRGB	Direction Régionale de Bejaïa
ESXI	Elastic Sky X integrated
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IBM	International Business Machines
IP	Internet Protocol
ISO	International Organization for Standardization
KVM	Kilobyte Virtual Machine
L'OS	Système d'exploitation
LAN	Local Area Network
MAC	Media Access Control
NetBIOS	Network Basic Input Output System
NAS	Network Attached Storage
NAT	Network Address Translation
QoS	Quality of Service
RAM	La mémoire vive (Random Access Memory)
RAID	Redundant Array of Inexpensive Disks
SAN	Storage Area Network

TVMM	Trusted Virtual Monitor Machine
TXT	Trusted Execution Technology
TRC	Région Transport Centre
VLAN	Virtual Local Area Network
VM	Machine Virtuelle
VMM	Virtual Machine Monitor
VSwitch	Virtual Switch
VPN	Virtual Private Network
WAN	Wide Area Network

Introduction général

Depuis quelques années, la virtualisation est un sujet largement abordé dans la presse informatique. Toutes les grandes entreprises et administrations ont au moins analysé les perspectives offertes par la virtualisation.

De nombreuses organisations envisagent de consolider leurs centres de données traditionnels en les virtualisant dans le but de réduire les dépenses. Cette consolidation permet d'optimiser les ratios de consolidation et de réaliser des économies d'échelle. Grâce aux avancées technologiques telles que les processeurs multicœurs et la technologie Hyperthreading, les ratios de consolidation sont aujourd'hui si élevés que la virtualisation est devenue incontournable d'un point de vue opérationnel.

Cependant, de nombreuses organisations se lancent dans la virtualisation sans avoir pleinement conscience des implications que cela peut avoir, en général et surtout dans le contexte des centres de données virtualisés (CDV), en termes de sécurité. En effet, les CDV présentent non seulement les vulnérabilités inhérentes aux centres de données traditionnels, mais également des vulnérabilités propres à leur nature virtuelle. Ainsi, en cherchant à accroître le ratio de consolidation, les organisations risquent involontairement de compromettre l'architecture de sécurité de leur réseau.

Il est donc essentiel que les organisations comprennent parfaitement les répercussions que cette approche peut avoir sur de nombreux aspects de la sécurité des CDV. De plus, elles doivent anticiper les conséquences de leurs décisions à chaque étape de la conception et du déploiement de leur CDV. Ce n'est qu'en prenant toutes ces précautions qu'il sera possible d'atténuer suffisamment les vulnérabilités de l'infrastructure pour résister aux menaces connues. Le travail réalisé dans ce projet est divisé en quatre chapitres :

Chapitre I : Nous allons présenter l'organisme d'accueil de Sonatrach.

Chapitre II : Nous allons aborder quelques notions de généralités sur la virtualisation.

Chapitre III : Sera didié à la sécurité dans la virtualisation.

Chapitre VI : Sera consacré à la partie pratique de mon travail, dans laquelle nous définirons les différentes configurations,réalisation et test.

Enfin : Nous allons résumer ce travail par une petite conclusion générale.

Chapitre 1

Présentation de l'organisme d'accueil

1.1 Introduction

La présentation de l'organisme d'accueil et l'étude de l'existant est une étape très importante qui représente le cadre de travail qui délimite les périmètres de notre projet. Dans ce chapitre, nous allons présenter l'entreprise SONATRACH, citer ses différents départements, en se focalisant sur le centre informatique, dans lequel se déroule notre stage. puis durant ce chapitre, nous allons décrire l'architecture Globale du réseau de SONATRACH, en mettant l'accès sur la virtualisation des serveurs et leur sécurité, ce qui constitue la problématique de notre travail, sur laquelle nous allons proposer notre solution.

1.2 Présentation générale de l'organisme d'accueil

SONATRACH est un Groupe pétrolier et gazier intégré sur toute la chaîne des hydrocarbures. Il détient en totalité ou en majorité absolue, plus de vingt entreprises importantes sur tous les métiers connexes à l'industrie pétrolière tel que le forage, le raffinage... Il possède aussi des participations significatives dans près de 50 entreprises implantées tant en Algérie qu'à l'étranger.

1.3 Historique et missions

L'entreprise Sonatrach est l'acronyme de « Société Nationale pour le Transport et la Commercialisation des Hydrocarbures » est une entreprise publique algérienne qui a été créé le **31 Décembre 1963** par le décret **n°63/491** .

Les statuts ont été modifiés par le décret **n°66/292** du **22 Septembre 1966**, et SONATRACH devient "Société nationale pour la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures ", cela a conduit à une restructuration de l'entreprise dans le cadre d'un schéma directeur approuvé au début de l'année **1981** pour une meilleure efficacité organisationnelle et économique, de ces principes Sonatrach a donné naissance à **17** entreprises : (**NAFTAL, ENIP, ENAC,...etc**).Après sa restructuration en **1982** et sa réorganisation en **1985**, Sonatrach s'est recentrée sur ses métiers de base que constituent les activités suivantes :

— Exploration et recherche des hydraucarbures

— Exploration des gisements d'hydrocarbures.

— Le transport par canalisation.

— La liquéfaction et la transformation de GAZ.

— La commercialisation.

Pour la réalisation de ces objectifs, SONATRACH est divisé en cinq branches différentes, comme représentées sur la figure 1.1 :

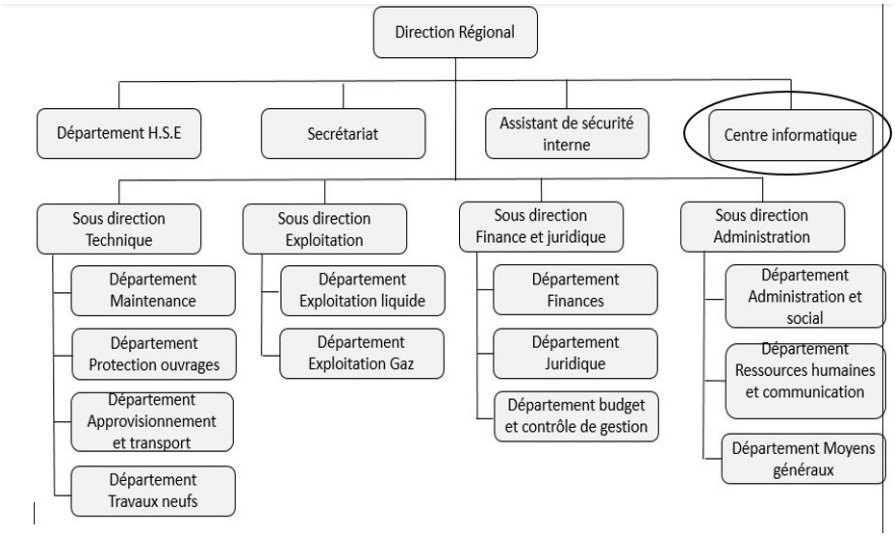

FIGURE 1.1 – Les branches de l'entreprise SONATRACH

À travers cette transformation structurelle et fractionnelle, un schéma de groupes a évolué en constituant des branches d'activités autonomes et leurs filiations. Dans la branche (Activité de transport par canalisation), se trouve la Direction Régionale de Bejaia (DRGB) qui représente l'organisme d'accueil de notre stage.

1.4 Activités de la branche transport par canalisation (TRC)

L'activité de transport par canalisation (TRC) est en charge de l'acheminement des hydrocarbures pétroles brut, gaz et condensat vers les ports pétroliers, les zones de stockages et les pays d'exploitation. Les missions affectées à la branche transport par canalisation sont :

— La gestion et l'exploitation des ouvrages et canalisations de transport d'hydrocarbures.

— La coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation.

— La maintenance, l'entretien et la protection des ouvrages et canalisations.

— L'exécution des révisions générales, des machines tournantes et équipements.

— La gestion de l'interface transport des projets internationaux du groupe ou en Partenariat.

La SONATRACH possède cinq directions régionales de transport des hydrocarbures :

— La direction régionale Est (Skikda).

— La direction régionale Centre (Bejaia).

— La direction régionale Ouest (Arzew).

— La direction régionale de Haoud-El-Hamra.

— La direction régionale d'Ain Amenas.

1.5 Présentation de la direction régionale de Bejaia (DRGB)

La DRGB est l'une des cinq directions chargées du transport, du stockage et de la livraison des hydrocarbures liquides et gazeux. Les hydrocarbures transportés à travers les canalisations gérées et exploitées par la DRGB sont :

— Le GAZ naturel.

— Le pétrole brut.

— Le condensat.

1.6 Structure de la DRGB

Nous illustrons les directions et sous-directions dans le diagramme de la figure 1.2 comme suit :

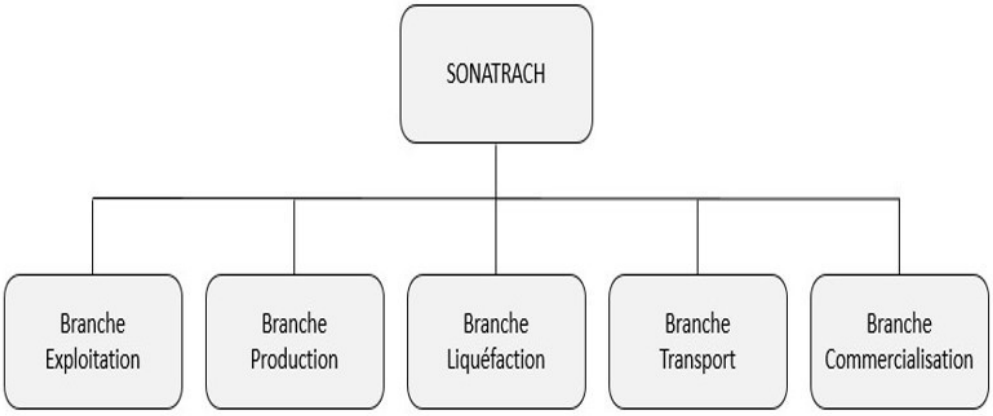

FIGURE 1.2 – Organigramme de la direction régionale de Bejaia (DRGB)

Ci-dessous, une description de quelques départements important de DRGB :

- **Direction régionale :** Elle est dirigée par un directeur régional aidé par des assistants et un Secrétariat.
- **Assistant de sûreté interne :** Sa mission est de protéger et de sauvegarder le patrimoine humain et matériel de la DRGB.
- **Centre informatique :** Il regroupe les moyens d'exploitation et de développement des applications informatiques pour l'ensemble des structures de la DRGB, ainsi que la gestion du réseau informatique interne. Ce centre représente le service de notre stage.
- **Sous-direction technique :** Elle a pour mission d'assurer la maintenance et la protection des ouvrages. Elle est organisée en quatre départements : département maintenance, département protection des ouvrages, département approvisionnement et transport et département des travaux neufs.
- **Sous-direction Exploitation :** Elle est chargée de l'exploitation des installations de la région, et de maintenir le fonctionnement de trois ouvrages en effectuant des réparations en cas de fuite, de sabotage ou de panne pour les stations de pompage. Elle est composée de deux départements : le département exploitation liquide et le département exploitation gaz.

• **Sous-direction Administration :** Elle a pour mission la gestion des ressources humaines et les moyens généraux. Elle est organisée en trois départements : département administration et social, département ressources humaines et communication et département moyens généraux.

• **Sous-direction Finances et Juridique :** Elle a pour mission d'effectuer la gestion financière, le budget et le contrôle de gestion et de prendre en charge les affaires juridiques de la DRGB. Elle est organisée en trois départements : département finances, département juridique, département budget et contrôle de gestion.

1.7 Centre Informatique

L'organisation du centre informatique ne cesse de subir des changements et l'évolution rapide de l'informatique pousse ce dernier à adopter de nouvelles démarches afin de répondre aux nouveaux besoins de l'entreprise.

Pour mener à bien sa mission, le centre informatique est divisé en trois services tels qu'ils sont schématisés dans la figure 1.3 :

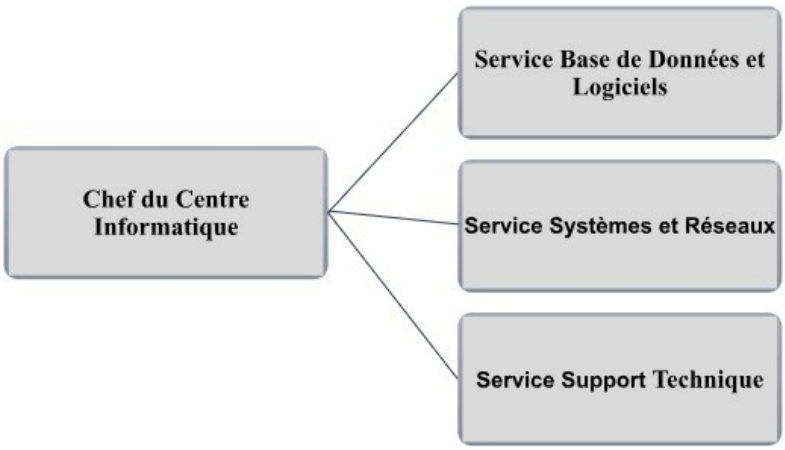

FIGURE 1.3 – Organigramme du centre informatique

1.7.1 Organisation fonctionnelle du Centre Informatique

Chaque service a sa propre fonction, nous allons définir et citer les différentes tâches de chacun ci-dessous :

(a) Service systèmes et réseaux

- **Système**

— Choix des équipements informatiques et logiciels de base.

— Mise en œuvre des solutions matérielles et logicielles retenues.

— Installation et configuration des systèmes.

— Mise en œuvre des nouvelles versions de logiciels.

- **Réseau**

— Assurer le bon fonctionnement et la fiabilité des communications.

— Assurer l'administration du réseau et organiser l'évolution de sa structure.

— Etude et choix de l'architecture du réseau à installer et la participation à sa mise en Place.

— Définition des droits d'accès à l'utilisation du réseau.

— Assurer la surveillance permanente pour détecter les pannes.

— Traitement des incidents survenant sur le réseau.

(b) Service base de données et logiciels

- **Base de données**

— Conception des bases de données, optimisation et suivi des données informatiques.

— Installation, configuration et exploitation du système de gestion de bases de données et ses bases.

— Mise en œuvre et gestion des procédures de sécurité.

— Gestion de la sauvegarde, la restauration et la migration des données.

- **Logiciels**

— Etude et conception des systèmes d'information.

— Développement et maintenance des applications informatiques pour TRC.

— Déploiement des applications et formation des utilisateurs.

(c) Service supports techniques

— Assistance aux utilisateurs en cas de problèmes software et hardware.

— Installation des logiciels de gestion, technique et bureautique.

— Formation aux nouveaux produits installés.

1.8 Étude du réseau de DRGB

Le réseau de la DRGB est constitué de deux parties connectées entre elle (le réseau de l'ancien bâtiment et le réseau du nouveau bâtiment). En effet, il a subi une extension après la construction du nouveau bâtiment.

1.8.1 Les commutateurs utilisés dans le réseau de la DRGB

Le réseau de la DRGB utilise deux types de commutateurs :

Les Commutateurs intelligents

En plus de leur fonction ils peuvent faire le routage. Dans le réseau de la DRGB, on trouve trois exemples de ce type qui sont :

— Catalyst Cisco 6509 : La gamme Catalyst 6509 représentée sur la figure 1.4 offre des moyens pour soutenir la capacité de la bande passante du système et des capacités améliorées de gestion des câbles. Elle fournit également des flux d'air d'avant en arrière qui est optimisé pour les conceptions allée chaude et froide dans le

centre de données colocalisées et les déploiements de services. En outre elle offre une protection exceptionnelle des investissements en soutenant plusieurs générations de produits sur le même châssis, réduisant ainsi les coûts totaux de propriété. Le cadre Cisco Catalyst 6509 supporte à la fois la gamme Cisco Catalyst 6500 Supervisor Engine 32 et Cisco Catalyst 6500 Séries Supervisor Engine 720 familles, avec LAN associés, WAN, et des modules de services.

FIGURE 1.4 – Gamme Catalyst Cisco 6509

— Catalyst Cisco 3750 : La gamme Cisco Catalyst 3750 représentée dans la figure 1.5 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco Stack Wise, interconnectant les commutateurs au sein d'une même pile à 32 GBPS qui permet de construire un système unique de commutation à haute disponibilité. En outre, elle est optimisée pour les déploiements Gigabit Ethernet haute densité et comprend un large éventail de commutateurs qui répondent aux exigences en matière d'accès, d'agrégation ou de connectivité dorsale pour de petits réseaux.

FIGURE 1.5 – Gamme Catalyst Cisco 3750

Les Commutateurs non intelligents

Ce type de commutateurs ne permet pas de faire le routage. Le réseau de la DRGB contient le type suivant :

— Catalyst Cisco 3550 : C'est une gamme de commutateurs CISCO empilables, il fournit une haute disponibilité et des fonctionnalités avancées de qualité de service et de la sécurité afin d'améliorer l'exploitation de réseau Figure 1.6.

FIGURE 1.6 – Gamme Catalyst Cisco 3550

1.8.2 Étude de la sécurité de la DRGB

• **Serveur antivirus :** Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programme modifiant ou supprimant des fichiers, que ce soit des documents infectés de l'utilisateur ou des fichiers nécessaires au bon fonctionnement de l'ordinateur. Un antivirus vérifie les fichiers et courriers électroniques, les secteurs de boot (pour détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clés USB, CD, DVD etc.), les données qui transitent sur les éventuels réseaux (dont Internet) etc.

• **Serveur filtrage Web :** Permet d'interdire l'accès à des sites au contenu répréhensible ou plus simplement de bloquer les bannières publicitaires. Les règles de filtrage sont mises à jour automatiquement dans l'établissement à partir d'une base de données. Les sites filtrés sont classés par catégories (adultes, piratages, publicités) modifiables, ainsi c'est l'établissement qui maîtrise sa politique de filtrage.

• **Serveur reporting :** C'est un outil complet et de rapport facile à utiliser qui permet d'évaluer l'utilisation de l'Internet par des employés de l'entreprise, identifier tous les problèmes possibles avec accès à l'Internet ou à la consommation de la bande passante réseau en générant des rapports détaillés, des résumés ou des graphiques. Il est utilisé pour montrer comment la connexion Internet est utilisée et pour affiner les stratégies de filtrage afin de maximiser les ressources du réseau.

• **Firewall juniperssg 550 :** Représente une nouvelle classe de dispositif de sécurité construite à cet effet qui offre un parfait mélange de haute performance, de sécurité et de connectivité LAN/WAN pour les déploiements de bureau régional et de leurs branches. Avec un réseau éprouvé et la protection au niveau application, le SSG 550 peut être mis en œuvre comme dispositif de sécurité autonome pour arrêter les vers, les logiciels espions, cheval de trois, les logiciels malveillants et

autres attaques émergentes (Figure 1.7).

FIGURE 1.7 – Firewall Juniper ssg 550

Firewall Juniper ssg 550 représenté dans la figure 1.7 contient un ensemble de règles structurées en trois zones qui se présentent comme suit :

- **La zone trust :** C'est la zone la plus confiante, car elle autorise le trafic sortant et interdit le trafic entrant et c'est pour cela que la RTC lui a confiée son réseau LAN.
- **La zone untrust :**

C'est une zone qui autorise de trafic entrant et interdit le trafic sortant.

- **La DMZ (Demilitarized Zone) :**

C'est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet derrière le pare-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (DNS, HTTP, DHCP). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et, pour certains, depuis le réseau externe. Le but est ainsi d'éviter toute connexion directe au réseau interne.

1.9 Architecture globale du réseau de SONATRACH

La description de l'architecture globale du réseau de SONATRACH est la suivante : Elle est composée d'un modèle hiérarchique en trois couches (cœur, distribution et accès). De plus Elle possède plusieurs sites distants au niveau national. SONATRACH héberge également plusieurs serveurs virtuels dans la couche DMZ (voir la Figure 1.8).

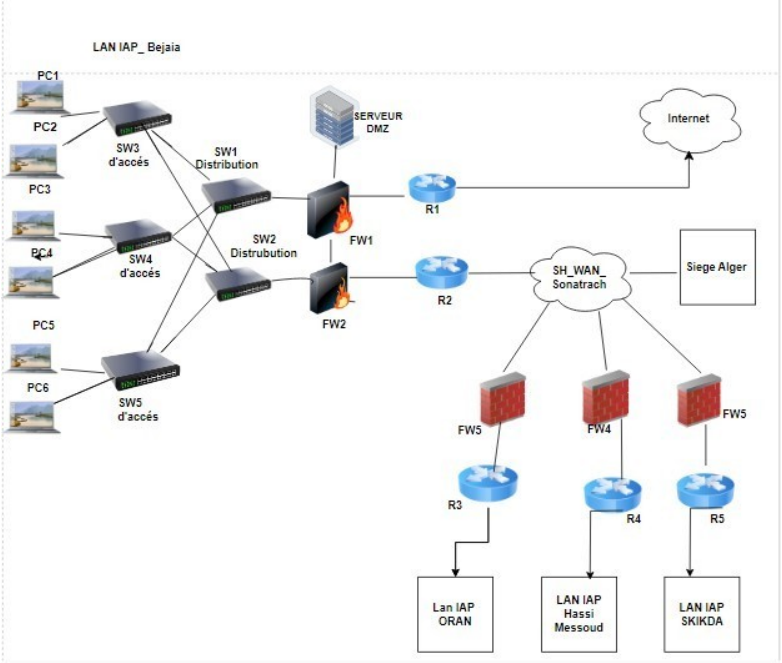

FIGURE 1.8 – Architecteur Réseau WAN

1.10 Analyse du parc informatique

Ce tableau permet de lister les différents équipements et leur appellation.

Périphériques utilisés	Appellation
Commutateur cœur	Cisco Catalyst 9407
Commutateur distribution	Cisco Catalyst 3850
Commutateur accès	Cisco Catalyst 9200 Cisco Catalyst 2960 Cisco Catalyst 3550 Cisco Catalyst 3850
CME (Call Manager Express)	Routeur 2900
ISP (Internet Service Provider)	Cloud PT
Terminal PC	PC bureau DELL, Laptop
Téléphonie IP	IP Phone 7960
Autre devises	Serveurs, imprimantes, Access Point

TABLE 1.1 – Analyse parc informatique

1.11 Problématiques et Solutions

1.11.1 Problématiques

Durant notre étude du réseau DRGB (SONATRACH), nous avons constaté que le Centre Informatique a utilisé plusieurs serveurs virtuels dans la couche DMZ avec une sécurité non renforcée (voir la figure 1.8). Ceci dit que l'aspect sécurité n'as pas été bien pris en considération et ce qui pose un certain nombre de défis en matière des sécurité à savoir :

— L'infrastructure de l'hyperviseur est obsolète ce qui veut dire que la sécurité nécessite une mise niveaux.

— Le problème de chargement des hôtes (les serveurs, les pares-feux...). Lorsque le trafic réseau n'est pas correctement géré, cela peut entrainer une surcharge des ressources du serveur et du pare-feu, des problèmes de performance et de sécurité.

1.11.2 Solutions proposées

Afin de remédier aux problèmes ci-dessus cités, nous avons proposé une solution constituée d'un ensemble de mesures et/ou étapes, comme expliqué ci-dessus :

— 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 détection d'intrusion IDS en l'implémentant dans le firewall pour surveiller le trafic réseau en temps réel pour détecter les activités suspectes et bloquer ces alertes par IPS.

— Nous avons utilisé des VLANs pour sécuriser, optimiser et réduire les coûts du réseau en réduisant la taille des domaines de diffusion et en améliorant les performances.

— Pour renforcer la sécurité du réseau interne de l'entreprise une DMZ a été mise en place et renforcée par la virtualisation, Cette

DMZ sécurise et surveille le noeud externe de manière dédiée, en complément du pare-feu qui protège le reste du réseau.

1.12 Conclusion

Ce chapitre nous a permis de bien comprendre l'architecture globale du réseau de Sonatrach, Par la suite, nous somme focaliser sur la problématique de la sécurisation de la virtualisation des déférents services de la DMZ, et nous avons proposé une solution, adaptée l'architecture de SONATRACH (DRBG), sous forme mesures et étapes à suivre. Vue l'importance de la virtualisation et aussi l'aspect sécurit, les deux prochains chapitres seront consacrés sur ces deux points, respectivement Ce chapitre nous a permis de bien comprendre l'architecture Globale

Chapitre 2

Généralités sur la Virtualisation

2.1 Introduction

La virtualisation joue un rôle essentiel dans les entreprises, car elle vise à gérer plus efficacement leurs infrastructures informatiques, à optimiser l'utilisation des ressources, à réduire les coûts et à faciliter le déploiement de machines virtuelles. Elle contribue ainsi à aider les entreprises à atteindre leurs objectifs commerciaux.

Dans ce chapitre, nous allons aborder la notion de virtualisation en nous concentrant sur son rôle, ainsi que ces différents types couramment utilisés avec une petite différence entre ces deux types d'hyperviseurs.

2.2 Définition de la virtualisation

La virtualisation est une technologie qui permet de créer plusieurs environnements virtuels sécurisés à partir d'un seul système physique. Elle est réalisée à l'aide d'un logiciel appelé hyperviseur, qui divise le système en plusieurs machines virtuelles distinctes. Ces machines virtuelles peuvent utiliser de manière efficace les ressources matérielles disponibles. Les opérateurs ont un contrôle précis sur ces instances virtuelles, ce qui leur permet de gérer les ressources telles que le processeur, la mémoire, le stockage et d'autres éléments [2].

La figure suivante illustre la différence entre une architecture traditionnelle, dans laquelle un seul système d'exploitation qui est exécuté sur une machine physique, et une architecture avec la virtualisation, dans laquelle plusieurs systèmes d'exploitation sont virtualisés sur une machine hôte :

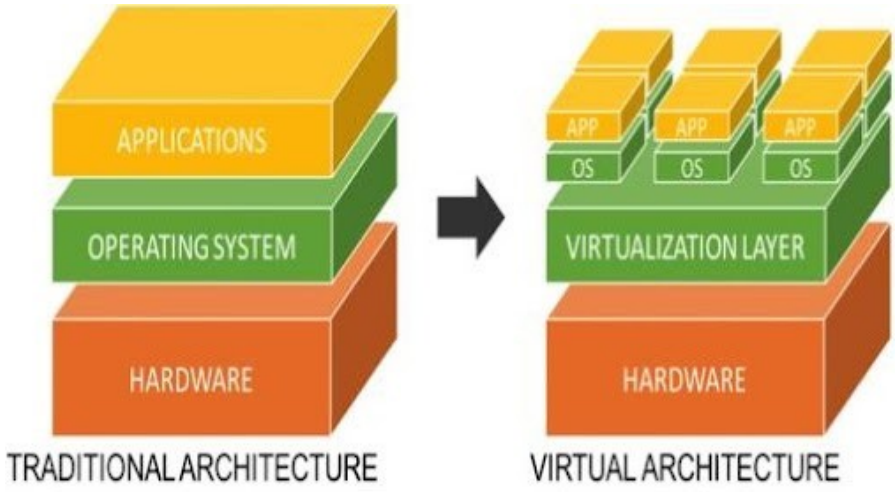

FIGURE 2.1 – Architecture traditionnelle et Architecture avec virtualisation [27]

2.3 Le rôle de la virtualisation

La virtualisation occupe une place essentielle dans le système informatique (postes de travail, serveurs, imprimantes, réseaux, ...) des entreprises, comme expliqué ci-dessous [3] :

a) La virtualisation permet aux utilisateurs de travailler avec des ressources virtualisées grâce à des interfaces standards qui minimisent l'impact sur les utilisateurs lors des changements apportés à l'infrastructure informatique. Les utilisateurs peuvent continuer à utiliser leur interface d'origine et leur manière d'interagir avec les ressources virtuelles reste inchangée, même si la mise en œuvre des ressources sous-jacentes change.

b) La virtualisation permet de simplifier la représentation, l'accès et

la gestion des ressources informatiques, comme l'infrastructure, les systèmes et les logiciels, tout en offrant des interfaces standardisées pour entrées et sorties.

c) La technologie de virtualisation permet de minimiser le couplage entre l'utilisateur et une implémentation spécifique de ressource, réduisant ainsi sa dépendance. Les administrateurs système peuvent ainsi minimiser l'impact sur les utilisateurs lors de la maintenance et de la mise à niveau des ressources informatiques.

2.4 Types courants de technologie de virtualisation

Dans ce qui suit, nous allons voir de types principaux de virtualisation, à savoir virtualisation des infrastructures et virtualisation logicielle :

2.4.1 Virtualisation des infrastructures

La virtualisation des infrastructures est un concept essentiel pour les opérations des centres de données, qui englobe la virtualisation du réseau, du stockage et du système de fichiers [4] .

a) **La virtualisation du réseau :** consiste à intégrer les ressources matérielles et logicielles du réseau afin de fournir des connexions réseau virtuelles aux utilisateurs. On peut distinguer deux formes de virtualisation du réseau : la virtualisation du réseau local et la virtualisation du réseau étendu.

b) **La virtualisation du stockage :** implique la création d'une vue logique abstraite des périphériques de stockage physiques. Elle se décline principalement en deux formes : la virtualisation du stockage basée sur les périphériques de stockage et la virtualisation du stockage basée sur le réseau.

c) **Le RAID (Redundant Array of Inexpensive Disks) :** est un exemple courant de virtualisation du stockage basée sur les périphériques de stockage. Cette technologie combine plusieurs disques physiques dans une baie de disques, utilisant des disques peu coûteux, afin de fournir un espace de stockage unifié, à hautes performances et résistant aux pannes.

d) **Le NAS (Network Attached Storage) et le SAN (Storage Area Network) :** sont des exemples représentatifs de la virtualisation du stockage basée sur le réseau.

2.4.2 Virtualisation logicielle

La virtualisation logicielle inclut la virtualisation des logiciels en plus de la virtualisation des infrastructures et des systèmes. Elle englobe des concepts de virtualisation intégrés aux programmes et aux langages de programmation utilisés par les utilisateurs. Les formes les plus couramment reconnues de cette technologie dans l'industrie comprennent la virtualisation des applications et la virtualisation des langages de haut niveau [5] :

• La virtualisation des applications permet de créer un environnement d'exécution virtuel dédié au programme en séparant le programme d'application du système d'exploitation. Cet environnement inclut le fichier exécutable de l'application ainsi que l'environnement d'exécution requis. Les composants du programme sont transmis par le serveur de virtualisation des applications au client qui les intègre ensuite dans son environnement d'exécution virtuel en temps réel.

• Lorsque l'utilisateur ferme l'application, toutes les données et modifications associées sont téléchargées vers un serveur centralisé de gestion. Cette approche permet aux utilisateurs d'utiliser leurs applications sur différents appareils sans être limités à un seul terminal.

FIGURE 2.2 – la virtualisation logicielle [28]

2.5 Les caractéristiques de la virtualisation

La virtualisation possède de multiples caractéristiques que nous allons aborder [6] :

1. **Partitionnement :** la technologie de virtualisation permet de diviser les ressources disponibles en plusieurs partitions, ce qui permet l'allocation des ressources et des applications sous forme virtuelle entre plusieurs utilisateurs ou organisations.
2. **Isolation :**la virtualisation permet de créer des versions virtuelles de ressources physiques ou de stockage uniques tout en maintenant toutes les versions virtuelles isolées les unes des autres. Cela permet de limiter les impacts en cas de crash d'une machine virtuelle sur les autres. Les données d'une machine virtuelle ne sont pas partagées avec les autres ensembles de machines virtuelles fonctionnant sur la même plate-forme.
3. **Évolutivité :**la capacité d'augmenter et de réduire les ressources en fonction des demandes des clients est un élément clé de la virtualisation et permet la croissance efficace d'une entreprise.
4. **Flexibilité :**la technologie de virtualisation offre la caractéris-

tique de flexibilité, qui permet la disponibilité des ressources ou des applications pour plusieurs clients ou organisations en même temps.

5. **Sécurité :** la virtualisation offre un haut niveau de sécurité et de protection pour les machines invitées en utilisant des pares-feux et un cryptage pour assurer la sécurité des données et des applications. Elle protège la machine hôte de tout dommage ou dommage autorisé par les machines invitées.

2.6 Différence entre le cloud-computing et la virtualisation

La virtualisation crée une instance virtuelle pour chaque ressource ou application à partir d'un seul système matériel, tandis que le cloud-computing est une configuration informatique qui permet aux organisations ou aux individus d'accéder aux ressources matérielles, logicielles, de stockage et d'infrastructure réseau à tout moment et n'importe où. Bien que la virtualisation soit à la base du cloud-computing, il ne s'agit pas de la même chose. Voyons la différence entre eux [7] :

Virtualisation	**Cloud-computing**
La virtualisation est un processus de création de plusieurs copies de matériel et de logiciels sur la même machine.	Le cloud-computing est l'accès à la demande aux ressources matérielles et logiciels
Il est très simple de mettre en place un logiciel de virtualisation	La mise en place d'un environnement cloud est une tache compliquée
Les utilisateurs doivent disposer d'une authentification appropriée avant d'accéder aux ressources virtuelles.	Tout utilisateur peut accéder aux ressources du cloud n'importe où et n'importe quand.
La virtualisation est plus rentable que le cloud-computing	Le cloud-computing peut être plus coûteux que la virtualisation.

TABLE 2.1 – la différence entre la virtualisation et cloud-computing

2.7 Types de virtualisation

La virtualisation facilite la mise en œuvre du cloud-computing par les utilisateurs. Il permet la création de formes virtuelles de matériel, de logiciels, de serveurs et de système d'exploitation. Par conséquent, la virtualisation peut être divisée en les types suivants :

2.7.1 Virtualisation matérielle

La virtualisation matérielle permet de créer des versions virtuelles de ressources matérielles physiques qui peuvent être partagées entre

plusieurs utilisateurs ou organisations. Une machine virtuelle est créée sur le système d'exploitation existant plutôt que d'utiliser la ressource matérielle physique d'un utilisateur. L'hyperviseur ou le gestionnaire de machines virtuelles surveille les programmes, contrôle la mémoire et le matériel, permettant d'installer différents systèmes d'exploitation et d'y exécuter diverses applications, tout en gérant les ressources physiques partagées entre le fournisseur de cloud et les utilisateurs [8].

a) **Le fonctionnement de la virtualisation matérielle** La virtualisation matérielle crée une couche d'abstraction entre le logiciel et le matériel via un hyperviseur ou un gestionnaire de machines virtuelles (VMM). Installé sur la machine hôte, ce VMM autorise les logiciels invités à opérer sur des ressources virtuelles telles que des processeurs virtuels, plutôt que sur le matériel réel [9]. Cette virtualisation bénéficie aux logiciels invités, incluant les systèmes d'exploitation. Deux types d'hyperviseurs existent [10] :

➤ **L'hyperviseur de type 1 :** appelé hyperviseur bare-metal ou natif, est une couche logicielle qui s'exécute directement sur le matériel de l'ordinateur hôte. Il gère les ressources matérielles et contrôle les systèmes d'exploitation invités. Ce type d'hyperviseur est qualifié de "bare-metal" car aucune autre couche logicielle ou système d'exploitation n'interfère entre le serveur physique et son matériel sous-jacent. C'est une forme fondamentale d'hyperviseur, assurant une efficacité opérationnelle et des performances optimales. Les fournisseurs renommés de ce type d'hyperviseur incluent VMware ESXi, KVM, Oracle VM et Citrix Hypervisor.

➤ **L'hyperviseur de type 2 :** appelé hyperviseur hébergé, s'exécute au sein du système d'exploitation d'un hôte physique. Ce type d'hyperviseur comporte une couche logicielle qui repose sur le matériel. Il agit comme une interface de gestion pour les machines virtuelles, éliminant le besoin d'une autre application pour

la création et la gestion des VM. Parmi les fournisseurs renommés de type-2 figurent Oracle VM VirtualBox, VMware Workstation Pro et Windows Virtual PC.

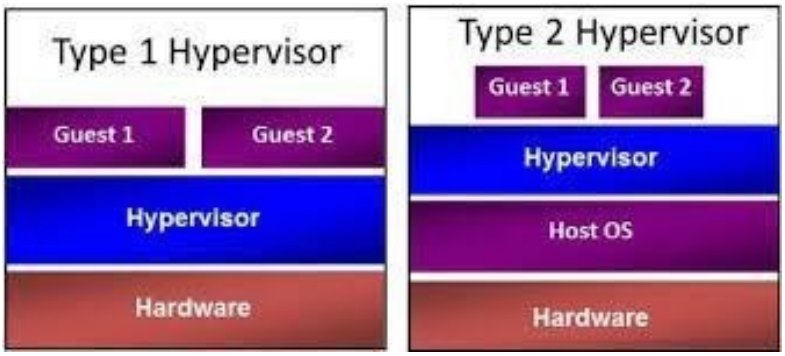

FIGURE 2.3 – types d'hyperviseur [29]

b) **Types de virtualisation matérielle** La virtualisation matérielle peut être globalement divisée en trois types [5] :

➤ **La virtualisation complète :** La virtualisation complète est une méthode de virtualisation matérielle qui isole un environnement pour exécuter un système d'exploitation invité. Cette approche simule entièrement le matériel sous-jacent, permettant au système d'exploitation invité de fonctionner sans conscience de la virtualisation. Chaque serveur invité peut ainsi opérer avec son propre système d'exploitation, sans nécessiter de modifications, et accéder à l'ensemble des logiciels compatibles avec le matériel physique. Cela offre une solution économique en créant un environnement similaire à un serveur physique pour les systèmes d'exploitation invités non altérés.

➤ **La paravirtualisation :** La paravirtualisation se distingue de la virtualisation complète en employant une version altérée du système d'exploitation invité au sein de la machine virtuelle. Contrairement à la virtualisation complète, le système d'exploitation invité reconnaît sa condition d'invité et interagit avec le

système d'exploitation hôte à travers des hyperappels, évitant les instructions directes au matériel. Pour la paravirtualisation, les systèmes d'exploitation invités doivent être adaptables via une API pour les ajustements nécessaires. Les hyperappels sont utilisés pour des opérations noyau telles que la gestion de la mémoire et des threads. Cette approche a pour but de réduire le temps requis pour des opérations complexes dans un environnement virtuel.

➤ **La virtualisation assistée par matériel :** La virtualisation assistée par matériel exploite les ressources matérielles de l'ordinateur pour créer et gérer des machines virtuelles. Contrairement à la virtualisation logicielle, elle utilise le matériel pour mettre en œuvre les fonctions de virtualisation, ce qui diminue la charge système. Cela permet à l'hôte d'accueillir un grand nombre de machines virtuelles et d'améliorer les performances. L'hyperviseur communique avec le processeur pour créer et maintenir les machines virtuelles. Cette approche a été initialement développée par IBM en 1972.

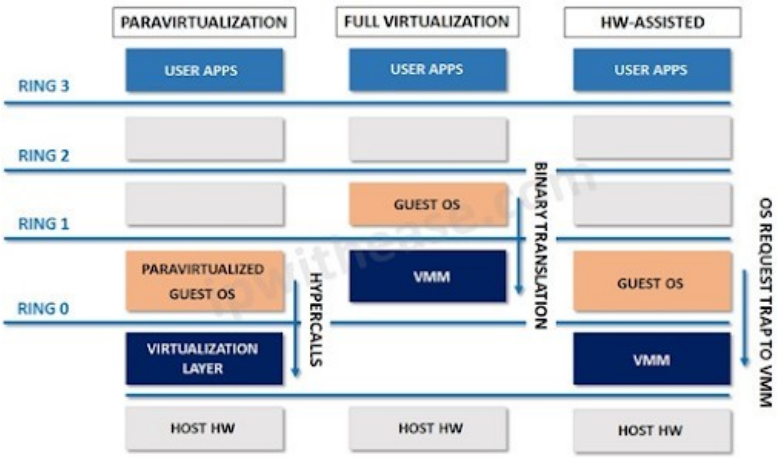

FIGURE 2.4 – Les types de la virtualisation complète [30]

2.7.2 Virtualisation logicielle

Le logiciel virtuel limite les fonctions du matériel physique pour exécuter plusieurs machines virtuelles sur une seule machine physique, il existe trois types de virtualisation logicielle [5] :

a) **Virtualisation du système d'exploitation :** La virtualisation du système d'exploitation implique l'exécution de multiples systèmes d'exploitation sur des ressources matérielles partagées. Cette réalisation repose sur un logiciel créant des environnements virtuels où chaque système d'exploitation fonctionne séparément et efficacement, sans interférence mutuelle. Fondamentalement, cette approche permet à plusieurs systèmes d'exploitation de tourner simultanément sur une seule machine physique, en utilisant les mêmes ressources matérielles.

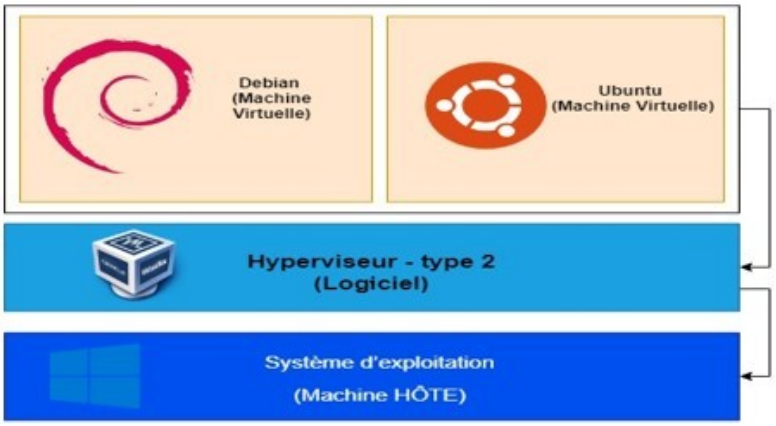

FIGURE 2.5 – virtualisation du système d'exploitation [31]

b) **Virtualisation des applications :** La virtualisation des applications comprend l'hébergement d'applications individuelles dans un environnement virtuel distinct du système d'exploitation natif. Cette technologie encapsule le programme informatique dans le système d'exploitation .

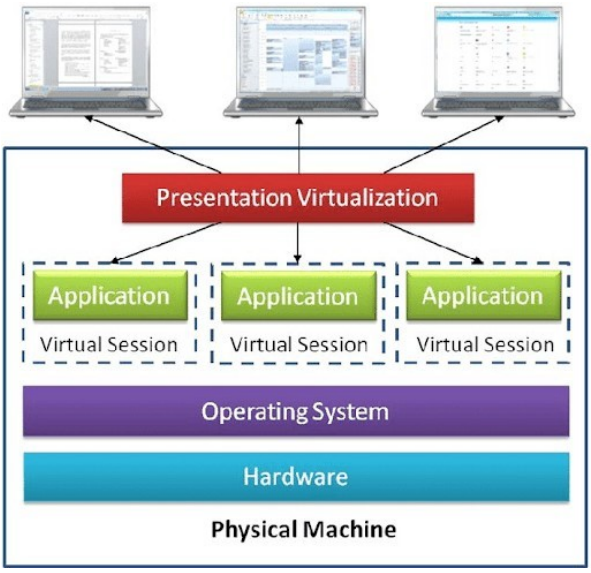

FIGURE 2.6 – le concept de virtualisation assisté par matériel [32]

c) **Virtualisation des services :** La virtualisation des services implique la reproduction de composants inaccessibles lors des tests en raison de leur développement, de blocages, de restrictions ou de tiers les possédant, voire pendant leur maintenance. En créant des répliques virtuelles de ces composants, cette approche réduit la dépendance envers ceux nécessaires pour les tests, ce qui économise du temps et de l'argent en évitant l'utilisation de ressources physiques spécifiques. En somme, la virtualisation des services permet d'accéder aux éléments requis par le biais d'une simulation.

2.7.3 Virtualisation de serveur

La virtualisation de Serveur implique la création de versions virtuelles de diverses ressources ou systèmes. Dans la virtualisation de serveur, un serveur physique est segmenté en plusieurs serveurs virtuels au moyen d'un logiciel dédié. Cela permet aux administrateurs de créer des environnements virtuels isolés qui fonctionnent indépendamment, sans interférence mutuelle. Ces environnements sont nommés serveurs privés virtuels, invités, instances, conteneurs ou émulations. L'applica-

tion d'un hyperviseur partitionne le logiciel et le matériel pour exécuter la virtualisation du serveur. Trois approches distinctes de virtualisation de serveur existent [11] :

a) **Modèle de machine virtuelle :** Le modèle de machine virtuelle repose sur le concept hôte-invité pour permettre la virtualisation matérielle, permettant à chaque invité de fonctionner dans un environnement virtuel. L'administrateur peut créer plusieurs machines virtuelles, chacune avec un système d'exploitation différent. Chaque machine invitée opère indépendamment, ignorant l'OS hôte et l'environnement virtuel. Un hyperviseur maintient la coordination entre l'hôte et les invités, en communiquant avec le CPU et en gérant les ressources de l'hôte.

b) **Machine para-virtuelle :** Le modèle de machine para-virtuelle ressemble au concept hôte-invité, mais avec la particularité que les invités sont conscients de leur utilisation de matériel virtuel. L'hyperviseur peut modifier le système d'exploitation invité, appelé portage, pour faire fonctionner des machines virtuelles avec divers systèmes d'exploitation. Les serveurs invités anticipent les demandes de ressources de chaque machine virtuelle, réduisant le besoin de coordonner les ressources entre l'hôte et les machines virtuelles. Ce modèle permet une communication directe entre le système d'exploitation invité modifier et l'hyperviseur, améliorant ainsi les performances du système.

c) **Virtualisation au niveau du système d'exploitation :** La virtualisation de niveau du système d'exploitation évite le modèle hôte-invité, où le système d'exploitation hôte assume les rôles d'hyperviseur, incluant la virtualisation et l'allocation des ressources physiques. Les fonctions d'un hyperviseur entièrement virtualisé sont gérées par le système d'exploitation hôte.

2.7.4 Virtualisation du stockage

La virtualisation du stockage consiste à regrouper physiquement plusieurs périphériques de stockage pour créer un pool de stockage unique, qui est ensuite divisé en plusieurs espaces de stockage logiques attribués à chaque client. Les espaces de stockage logiques fonctionnent comme des espaces physiques, mais les données sont stockées dans le cloud pour plus de sécurité. Cette approche offre une vue centralisée de l'espace de stockage, en extrayant les ressources physiques des utilisateurs. Ces ressources peuvent provenir de différents fournisseurs et réseaux. Les utilisateurs reçoivent des copies virtuelles des ressources de stockage, sans savoir où leurs données sont réellement situées sur le serveur. L'accès se fait via des chemins logiques. Pour illustrer le concept de la virtualisation du stockage, vous pouvez vous référer à la Figure suivante [12] :

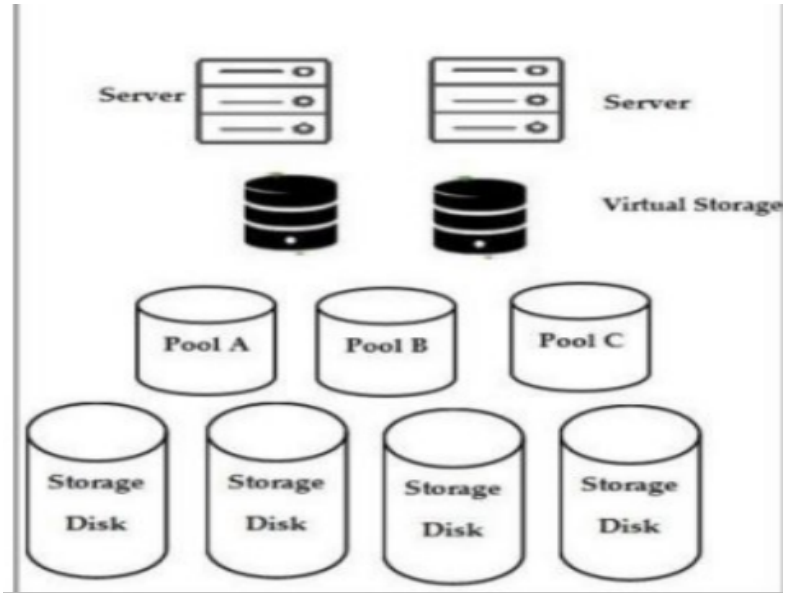

FIGURE 2.7 – Le concept de virtualisation de stockage [33]

La virtualisation du stockage peut se réaliser à deux niveaux : le niveau des blocs et le niveau des fichiers. Les deux approches offrent un stockage virtuel pour les données, avec des méthodes différentes. Le niveau des blocs stocke les données en blocs, tandis que le niveau des fichiers les organise en fichiers et dossiers. La virtualisation au niveau des blocs implique la création de volumes bruts avec un système d'exploitation, tandis que celle au niveau des fichiers gère les fichiers et dossiers via des périphériques de stockage. Bien que la virtualisation au niveau des blocs soit plus souple, celle au niveau des fichiers est plus simple et économique. Il existe plusieurs façons d'appliquer le stockage à un environnement virtualisé, donc voici les principales méthodes :

➢ **Virtualisation du stockage basée sur l'hôte**
➢ **Virtualisation du stockage basée sur la baie de stockage**
➢ **Virtualisation du stockage basée sur le réseau.**

2.7.5 Virtualisation du système d'exploitation

La virtualisation du système d'exploitation implique de diviser le système d'exploitation en plusieurs partitions où les ressources du noyau hôte sont partagées avec chaque instance. Différentes versions du système d'exploitation peuvent s'exécuter à l'intérieur de la machine hôte, permettant ainsi l'exécution de diverses applications. Cette forme de virtualisation opère au niveau de la couche du système d'exploitation. Le noyau du système d'exploitation hôte crée des instances pour différents utilisateurs, appelées conteneurs ou moteurs de virtualisation. Il agit en tant que noyau pour toutes les instances virtuelles, fournissant les fonctionnalités du système d'exploitation. Cependant, si un problème survient dans le noyau, toutes les instances sont impactées, car elles partagent le même noyau. Il existe deux types de virtualisation du système d'exploitation [13] :

a) **Virtualisation Linux :** La virtualisation Linux consiste à installer, exécuter et entretenir une ou plusieurs machines virtuelles au sein d'un système d'exploitation Linux. Cette approche permet

de partager et de répartir les ressources du système d'exploitation entre différentes machines virtuelles et processus en cours d'exécution. Chaque machine virtuelle fonctionne indépendamment tout en partageant les ressources disponibles. L'objectif de la virtualisation Linux est d'appliquer cette technique sur un système Linux, en isolant des applications spécifiques, du code de programme et des tests. Cela permet d'optimiser l'utilisation des ressources matérielles, contribuant ainsi à la réduction des coûts énergétiques et de maintenance. Parmi les solutions populaires de virtualisation Linux, on trouve Xen, KVM, VirtualBox et VMware.

b) **Virtualisation Windows :** La virtualisation Windows est conçue pour réaliser la virtualisation sur un système qui exécute le système d'exploitation Windows. Diverses machines virtuelles sont installées sur le système. Chacun d'eux partage les ressources du système d'exploitation Windows.

2.8 Conclusion

Dans ce chapitre nous venons de voir que la virtualisation est une technologie essentielle qui offre une meilleure utilisation des ressources, assure leur flexibilité, une consolidation des serveurs, une amélioration de la disponibilité et une simplification de la gestion des infrastructures. Elle continue d'évoluer et de jouer un rôle important dans l'optimisation des infrastructures informatiques. En ce qui concerne l'aspect sécurité, principalement dans la virtualisation, elle sera traitée dans le chapitre suivant.

Chapitre 3

La Sécurité dans la virtualisation

3.1 Introduction

La sécurité informatique, en générale, permet de renforcer la protection des ressources matérielles et logicielles. L'objectif de ce chapitre est de préciser l'importance de la sécurité spécifique à la virtualisation, et comment sécuriser les ressources virtuelles.

3.2 Sécurité de l'hyperviseur

La sécurité dans la virtualisation concerne principalement lé sécurité des de l'hyperviseur. Dans ce qui suit, nous allons détailler cet aspect, en présentant l'évolution de ce domaine, les risques, les vulnérabilités ainsi que quelques solutions utilisées dans ce type de sécurité [14].

3.2.1 Évolution et sécurité de l'hyperviseur

Les technologies de virtualisation ont connu une croissance importante depuis les années 2000, avec de nouveaux usages tels que la virtualisation des postes de travail, des applications d'entreprise, du stockage et l'émergence du cloud-computing. La virtualisation permet des économies d'espace, d'énergie et de budget en réduisant le nombre de serveurs utilisés grâce à la mutualisation et à l'optimisation de leur

utilisation. Elle améliore également la sécurité, la fiabilité et la disponibilité des systèmes informatiques, et est de plus en plus adoptée par les grandes entreprises (PME et PMI). L'hyperviseur améliore la sécurité du point de vue informatique, suivant les critères suivants [14] :

a) **Disponibilité :** L'hyperviseur est une technologie qui repose sur le matériel et permet de créer des machines virtuelles. En cas de défaillance de la machine, il suffit d'avoir un équipement compatible avec le produit de virtualisation pour créer une machine virtuelle équivalente.

b) **Intégrité :** Avec l'utilisation du stockage partagé de type SAN, l'hyperviseur permet la synchronisation de la réplication.

c) **Confidentialité :** L'hyperviseur permet de créer des environnements isolés au sein d'un hôte, ce qui permet de travailler sur le réseau local sans nécessiter physiquement de carte réseau.

3.2.2 Hyperviseur et ses risques

L'utilisation de l'hyperviseur engendre de nouveaux risques, tels que les attaques entre machines virtuelles, la fuite d'informations d'une machine virtuelle et la prise de contrôle du système hôte. Ces risques sont liés aux avancées technologiques des hyperviseurs [14] :

a) **Risque de compromission des systèmes :** La compromission d'un système invité par un acteur malveillant, que ce soit depuis un autre système invité ou depuis la couche d'abstraction, entraîne un risque de fuite d'informations et de perturbations du système, pouvant aller jusqu'à l'indisponibilité d'un service. Il est donc crucial de maintenir à jour toutes les composantes matérielles, le système d'exploitation hôte et les systèmes d'exploitation invités avec les correctifs de sécurité nécessaires pour prévenir de tels risques.

b) **Accroissement du risque d'indisponibilité :** La panne d'une ressource commune peut entraîner l'indisponibilité simultanée de

plusieurs systèmes et potentiellement de tous les services hébergés sur la même machine.

c) **Fuite d'information par manque de cloisonnement :** La virtualisation implique le partage de ressources entre les instances, ce qui rend difficile la gestion des échanges internes et la prévention des fuites d'informations. Dans une architecture virtualisée, les machines virtuelles partagent une carte réseau unique (figure 3.1), ce qui rend difficile le cloisonnement des flux de données. En cas de compromission, les différents flux d'information peuvent se mélangent.

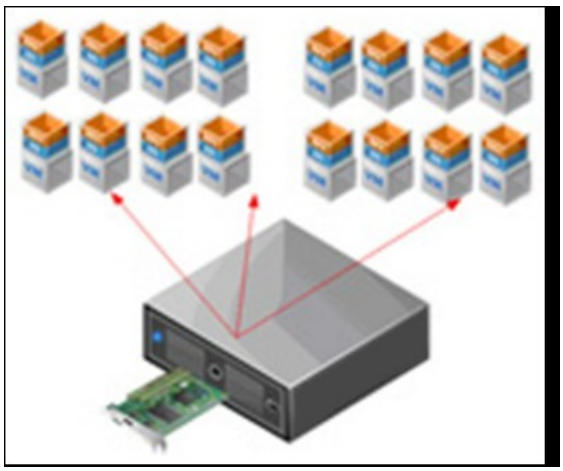

FIGURE 3.1 – Partage de la carte réseau [14]

d) **Complexification de l'administration :** La virtualisation complexifie l'administration en introduisant de nouvelles opérations telles que la mise en place de quotas sur les ressources partagées et la gestion de l'ajout de disques ou de périphériques de stockage réseau entre les machines virtuelles. De plus, la gestion de ces aspects peut être difficile car ils sont souvent gérés par des personnes différentes.

e) **Complexification de la supervision :** Les opérations de supervision peuvent être complexes en raison de l'incompatibilité entre le cloisonnement nécessaire des machines virtuelles et la

nécessité d'avoir une vision d'ensemble pour la supervision. Par conséquent, il devient difficile de tracer, de bout en bout, un événement ou une action.

f) **Prolifération non souhaitée des données et des systèmes :** Les systèmes invités sont moins adhérents aux équipements, ce qui signifie qu'un système peut être reproduit à l'identique sur plusieurs machines. Cela rend la localisation précise des données plus complexe et augmente les risques de copie non maîtrisée, avec les conséquences graves que cela peut entraîner, comme la modification ou le vol d'informations.

3.2.3 Vulnérabilités et attaques sur les hyperviseurs

Les hyperviseurs permettent de gérer des machines virtuelles sur un serveur physique et que les vulnérabilités peuvent causer des failles de sécurité dans la machine virtuelle ou le système hôte. Les attaques peuvent prendre différentes formes telles que [15] :

a) **Les attaques d'accès :** Les attaques d'accès visent à entrer illégalement dans un système et menacent la confidentialité des données. Les pirates utilisent différentes techniques telles que le sniffing, les chevaux de Troie, l'ingénierie sociale ou le craquage de mot de passe. Pour éviter ces attaques, il est essentiel de mettre en place des mesures de prévention adéquates.

b) **Attaques de modification :** Les attaques de modification visent à changer les informations dans un système. Elles prennent la forme de virus, de vers ou de chevaux de Troie qui altèrent des informations systèmes ou leur affichage. Elles peuvent détruire des données, perturber le fonctionnement du système et ralentir le réseau.

c) **Attaques par saturation :** Les attaques de saturation inondent un site web avec de multiples messages de diverses sources, provoquant son dysfonctionnement et facilitant l'intrusion du pirate.

Les techniques courantes sont le "flooding", qui envoie d'énormes paquets IP jusqu'à la déconnexion de la cible, et le "smurf", qui sature une station via des requêtes ping. Ces attaques génèrent d'énormes volumes de données, atteignant plusieurs giga-octets.

d) **Attaques par répudiation :** Les attaques par répudiation altèrent ou nient des informations, remettant en question leur source. L'usurpation d'identité par courriel en est un exemple. Le chiffrement est recommandé pour contrer ces attaques. La sécurité informatique est essentielle pour éviter pertes financières et interruptions. La préservation de l'intégrité et de la confidentialité des données est cruciale, dans les domaines physique et virtuel (comme la virtualisation et le cloud).

3.3 La sécurité informatique

La sécurité informatique englobe les méthodes visant protéger les données et les systèmes contre les accès non autorisé, assurant leur utilisation en accord avec les décisions de l'organisation ou des utilisateurs, sans perturbations [14].

3.3.1 Les piliers de la sécurité informatique

La sécurité des systèmes d'informations cible les piliers suivants [14] :

- **La confidentialité :** permet de garantir que les informations ne soient accessibles qu'aux personnes autorisées.
- **L'intégrité :** Permet de garantir que les informations ne soient pas modifiées ou altérées par des personnes non autorisées.
- **La disponibilité :** permet d'assurer le bon fonctionnement et l'accès aux services et ressources dans les délais prévus.
- **L'authentification :** est un élément essentiel pour gérer l'accès aux espaces de travail pertinents et maintenir la confiance dans les relations d' change en identifiant les utilisateurs de manière fiable.

• **La traçabilité :** permet de collecter et de sauvegarder les informations sur les tentatives d'accès, ce qui facilite leur utilisation ultérieure.

3.3.2 Les attaques informatiques

1. **Définition d'une attaque informatique**

   Une attaque informatique se réfère à l'exploitation d'une vulnérabilité présente dans un système informatique (système d' ;exploitation, logiciel ou même une erreur de l'utilisateur) dans le but de réaliser des actions inconnues de l'opérateur du système et généralement nuisibles.

   Les motivations des attaques peuvent être de différentes sortes [16] :

   — Obtenir un accès au système
   — Voler des informations, tels que des secrets industriels ou des propriétés
   — Intellectuelles
   — Glaner des informations personnelles sur un utilisateur
   — Récupérer des données bancaires
   — S'informer sur l'organisation ou l'entreprise ciblée.
   — Troubler le bon fonctionnement d'un service.
   — Utiliser le système de l'utilisateur comme « rebond » pour une attaque.
   — Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur Lequel il est situé possède une bande passante élevée.

2. **Les techniques d'attaques**

   Tout ordinateur connecté à un réseau est vulnérable à des attaques, même en cas d'incidents, Les attaques courantes [16] :

a. Le Spam et le Phishing

Le Spam, envoi massif d'e-mails non sollicités, vise la publicité peu coûteuse mais peut aussi servir au phishing, trompant les destinataires pour obtenir des informations personnelles via des e-mails frauduleux se faisant passer pour des institutions légitimes.

b. Le Spyware (logiciel espion)

Un programme non divulgué, installé par une société de marketing, collecte nos habitudes sans consentement, provoquant des préjudices tels que la divulgation non autorisée d'informations, la surcharge des ressources du système, et l'affichage de publicités ciblées basées sur les données collectées.

c. Le virus

Les virus informatiques, programmes malveillants, infectent des logiciels légitimes (hôtes) sur d'autres ordinateurs, entraînant des perturbations variables. Ils se propagent via réseaux, cédéroms, clés USB, etc. Classés par mode d'infection, types de virus incluent sont :

- **Les vers informatiques :**sont des virus qui sont capables de se répandre à travers un réseau en exploitant des vulnérabilités de sécurité.
- **Les chevaux de Troie :** sont des logiciels malveillants dissimulés dans des programmes authentiques, paraissant légitimes mais contenant des fonctionnalités nuisibles. Ils infectent les ordinateurs pour espionner, voler des données et créer des accès non autorisés.
- **Les bombes logiques :** sont des virus qui peuvent se déclencher suite à des événements spécifiques tels que la date du système ou l'activation à distance.

3.3.3 Les mécanisemes de sécurité

Il existe plusieurs mesures pour protéger les données dans les systèmes informatiques et d'en détecter les tentatives d'intrusions. En voici quelques-unes [16] :

a) **Pare-feu (Firewall)**

Un pare-feu est un système de défense informatique qui protège un ordinateur ou réseau contre les intrusions extérieures, en filtrant les données échangées avec au moins deux interfaces réseau, une pour le réseau à protéger et une pour l'externe (comme Internet). Il utilise des règles prédéfinies pour autoriser, bloquer ou rejeter les connexions. Les politiques de sécurité peuvent autoriser uniquement les communications autorisées ou empêcher les échanges interdits. Les pare-feu, logiciels ou matériels, agissent comme intermédiaires sécurisant le trafic. Les pares-feux personnels, pour un ordinateur, contrôlent l'accès réseau des applications et bloquent les attaques telles que les chevaux de Troie [17].

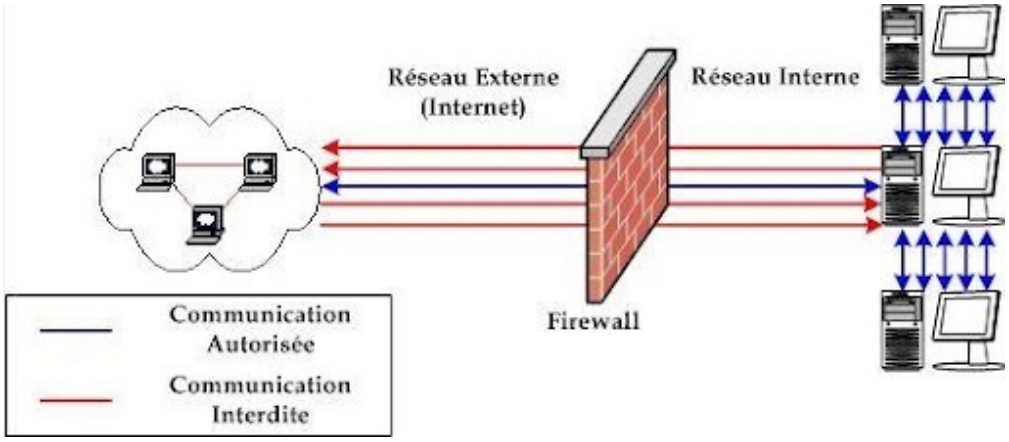

FIGURE 3.2 – principe de par feu [37]

b) **DMZ (Zone démilitarisée)**

Une zone démilitarisée (DMZ) est un sous-réseau isolé du réseau local et d'Internet, utilisant un pare-feu. Elle héberge des serveurs accessibles en ligne (comme web ou messagerie) sans menacer la sécurité. Le pare-feu sécurise la DMZ et bloque l'accès au réseau local, limitant l'impact d'une compromission aux machines de la DMZ plutôt qu'au réseau local [18].

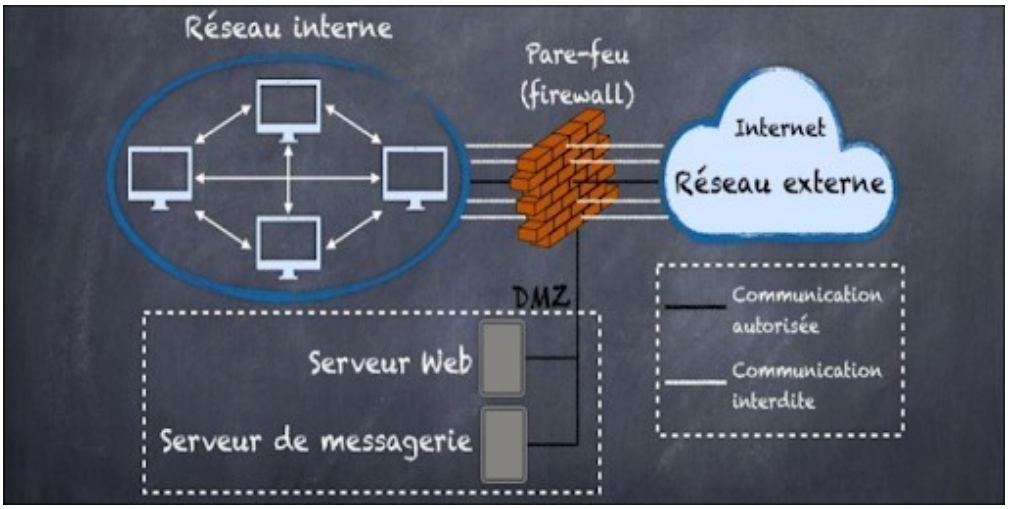

FIGURE 3.3 – Zone démilitarisée [38]

c) **Système de prévention et de Détection d'intrusions (IDS et IPS)**

Un système de détection d'intrusions (IDS) surveille et signale les activités anormales, sans les bloquer, contrairement à un système de prévention d'intrusions (IPS). Ils sont adaptés aux couches réseau (NIDS/NIPS) et système d'exploitation (HIDS/HIPS) pour sécuriser les réseaux et les hôtes [19].

d) **Les réseaux locaux virtuels (VLAN)**

Les réseaux locaux virtuels 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 [20].

3.3.4 Solutions pour quelques attaques informatiques

Nous allons proposer des solutions pour contrer chaque attaque citée précédemment comme le montre le tableau ci-dessous [14] :

Attaque	**Solution**
Ver, Virus, Spyware, Chevaux de Troie	Antivirus+ logiciels anti Spam et anti Trojan
Spam, Phishing	— Ne pas cliquer directement sur le lien contenu dans le mail, mais ouvrir plutôt le navigateur et saisir l'URL d'accès au service. — Méfiance des formulaires demandant des informations bancaires sur le net. — S'assurer que le navigateur est en mode sécurisé — S'assurer que l'adresse dans la barre du navigateur commence par HTTPS et qu'un petit cadenas est affiché dans la barre d'état au bas du navigateur

TABLE 3.1 – les solutions proposées pour quelque attaque

3.4 Conclusion

Dans ce chapitre nous venons de voir que la sécurité de la virtualisation (sécurité des hyperviseurs) dans les entreprises vise à protéger les environnements virtualisés en assurant la confidentialité, l'intégrité, la disponibilité et l'isolation des systèmes et des données. Le prochain chapitre portera sur des Test et Mise en œuvre de la Solution proposée au niveau du chapitre I.

Chapitre 4

Test et Mise en œuvre de la Solution

4.1 Introduction

Dans ce chapitre, nous allons expliquer comment installer tous les outils nécessaires pour configurer notre environnement logiciel et mettre en place notre solution proposée. Cette étape est essentielle pour la simulation de notre architecture réseau. Ce chapitre est le cœur de ce mémoire et il est illustré par des captures d'écran pour faciliter la compréhension des étapes d'installation et de 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

Nous avons opté pour l'utilisation de VMware Workstation version 16.0.0 pour simuler notre réseau. Ce logiciel permet de créer des machines virtuelles connectées à un réseau local avec une adresse IP différente, tout en étant exécutées sur la même machine physique [21].

FIGURE 4.1 – VMware Workstation 16 professionnel [34]

4.2.2 ESXI version 7.0.1

ESXi est un hyperviseur 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. ESXi dispose de son propre système d'exploitation et fournit une interface pour gérer les machines virtuelles qu'il exécute. La décision a été prise 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 installée dans l'entreprise [22].

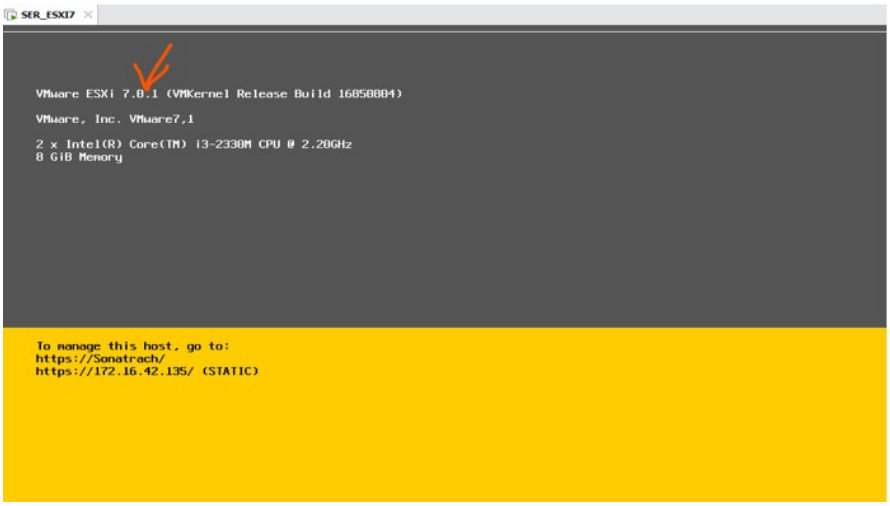

FIGURE 4.2 – ESXi.

4.2.3 Kali linux

Kali Linux est une distribution Linux basée sur Debian largement utilisée par les professionnels de la sécurité, les testeurs d'intrusion et les hackers éthiques. C'est un système d'exploitation libre et open-source qui est spécialement conçu pour la forensique numérique, les tests d'intrusion et l'audit de sécurité. L'objectif de Kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information [23].

FIGURE 4.3 – Kali Linux [35].

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 [24].

4.2.5 Windows server 2022

Windows Server 2022 est un système d'exploitation serveur développé par Microsoft. Il s'agit de la dernière version de la plate-forme Windows Server, conçue pour répondre aux besoins des entreprises et des organisations en matière de gestion de serveurs, de stockage, de réseautage et d'autres services informatiques [25].

4.2.6 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, et il est largement utilisé dans les environnements d'entreprise pour renforcer la sécurité du réseau [26].

FIGURE 4.4 – Snort [36]

4.3 Architecture proposée

La mise à niveau est une opération visant à améliorer une structure existante en ajoutant un ou plusieurs composants. Dans notre cas, nous effectuerons des mises à niveau à la fois au niveau logiciel et matériel.

Au niveau logiciel, nous mettrons en place VMware ESXi, qui nous permettra de virtualiser les différents serveurs. Cela nous permettra de réduire le nombre initial de serveurs et d'optimiser l'infrastructure. De plus, nous utiliserons le pare-feu pfsense pour segmenter et sécuriser les communications internes et externes de notre infrastructure de virtualisation. Nous établirons également une connexion trunk reliant la couche physique et le pare-feu, permettant ainsi la détection et la prévention des intrusions grâce à un système IPS/IDS.

Au niveau matériel, nous réduirons le nombre de serveurs afin de rendre le centre de données moins encombrant et de réduire la consommation d'énergie. Cette mise à niveau matérielle contribuera à une gestion plus efficace des ressources et à une meilleure utilisation de l'espace physique.

Après l'intégration de la solution de virtualisation et de sécurité VMware ESXi et pfsense, voici comment sera l'architecture réseau de Sonatrach :

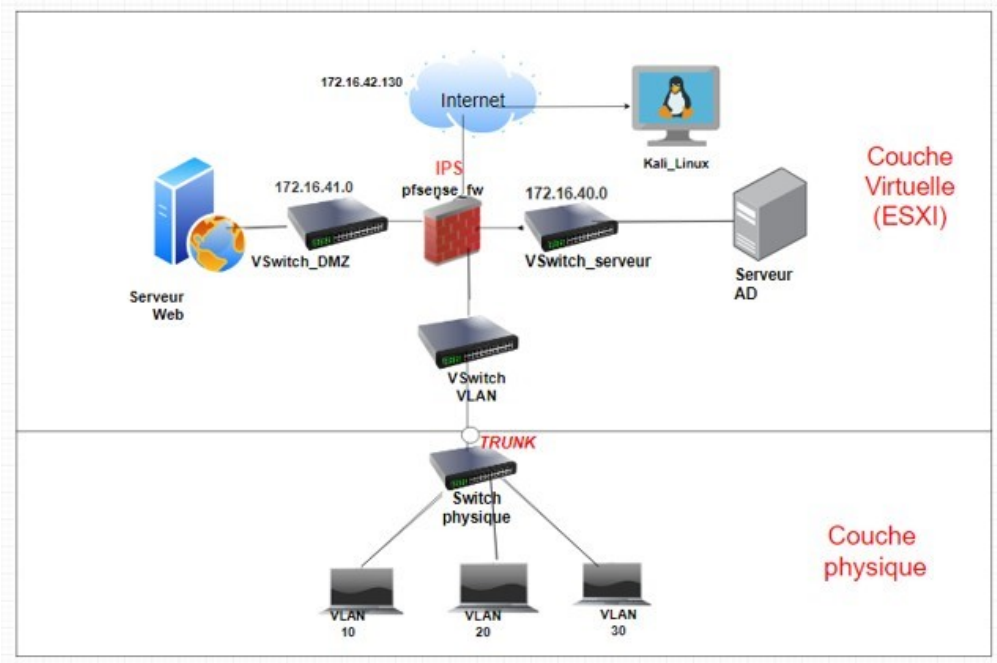

FIGURE 4.5 – Architecture de la solution proposée

4.3.1 Tableau d'adressage des équipements

Equipment Virtuelle	**Interface**	**Adresse IP**	**Masque**
FW-Sonatrach	DMZ	172.16.41.1	/24
	Serveurs	172.16.40.1	/24
	Wan	DHCP	/
	Vlan 10	172.16.10.1	/24
	Vlan 20	172.16.20.1	/24
	Vlan 30	172.16.30.1	/24
Serveur AD	Serveurs	172.16.40.100	/24
Serveur Web	DMZ	172.16.41.100	/24
Client	Serveurs	172.16.10.10	/24

TABLE 4.1 – Tableau d'adressage des équipements

4.3.2 Tableau d'adressage des VLANS

Nom VLAN	**Id VLAN**	**Adresse sous RX**	Passerelle Virtuelle
Service RH	10	172.16.10.0/30	172.16.10.250
Service HSE	20	172.16.20.0/30	172.16.20.250
Service INFO	30	172.16.30.0/30	172.16.30.250

TABLE 4.2 – Tableau d'adressage des Vlans

4.3.3 Tableau d'adressage des cartes réseaux ESXi

Switch virtuel	**Groupe de port**	**Adresse Réseaux**	**Nic physique**
Vswitch0	Mangement	172.16.42.0/24	Vmnic 0
Vswitch0	Internet	DHCP	Vmnic 0
Vswitch1	Serveurs	172.16.40.0/24	Vmnic 1
Vswitch2	DMZ	172.16.41.0/24	Vmnic 2
Vswitch3	Lan vlan	172.16.0.0/24	Vmnic 3

TABLE 4.3 – Tableau d'adressage des cartes réseaux ESXi

4.4 Création et paramétrage des cartes réseau physiques VMnet sur VMWare Workstation

— On lance le programme VMWare Workstation puis le menu Édit → Virtual Network Editor de VMWare Workstation.

— On doit cliquer sur Change Settings pour que Virtual Network Editor obtienne les droits administrateurs. Pour ajouter un nouveau réseau virtuel :

✓ On Clique sur Add Network (exemple VMnet6 ici)

✓ On Coche Host-only

✓ Subnet IP : on choisit un sous-réseau

✓Cliquez sur OK pour finir

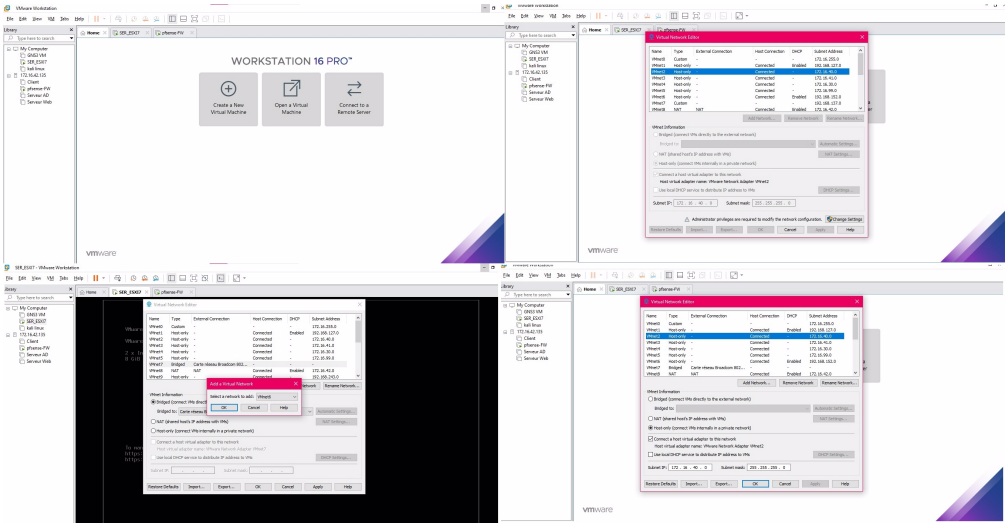

FIGURE 4.6 – Ajouter une carte réseau

On a créer 4 Cartes réseau comme on l'a vu dans la figure précédente et dans le tableau des réseaux :

— VMnet2 pour les Serveurs

— VMnet3 pour La DMZ

— VMnet4 pour les LAN-Vlan

— VMnet8 pour la connexion internet

4.5 Installation de ESXI

On a Choisi la version de notre ESXI ici, on travaille avec la version 7.0.1 On Clique sur New Virtual Machine → Custom après, on choisit la version de notre ESXI puis charger notre Image ISO de ESXI préalablement télécharger du site de VMWare dans les étapes à suivre :

— On va donner un nom à notre VM (c'est SER-ESXI7 ici) Sélectionner le nombre processeurs que l'on veut dédier à notre ESXI, la RAM (ici, c'est 8 Go) est la taille de l'espace de sauvegarde.

— Avant de démarrer notre ESXI, on configure les paramètres de la VM dont l'ajout de nos VMnets, puis sur finish.

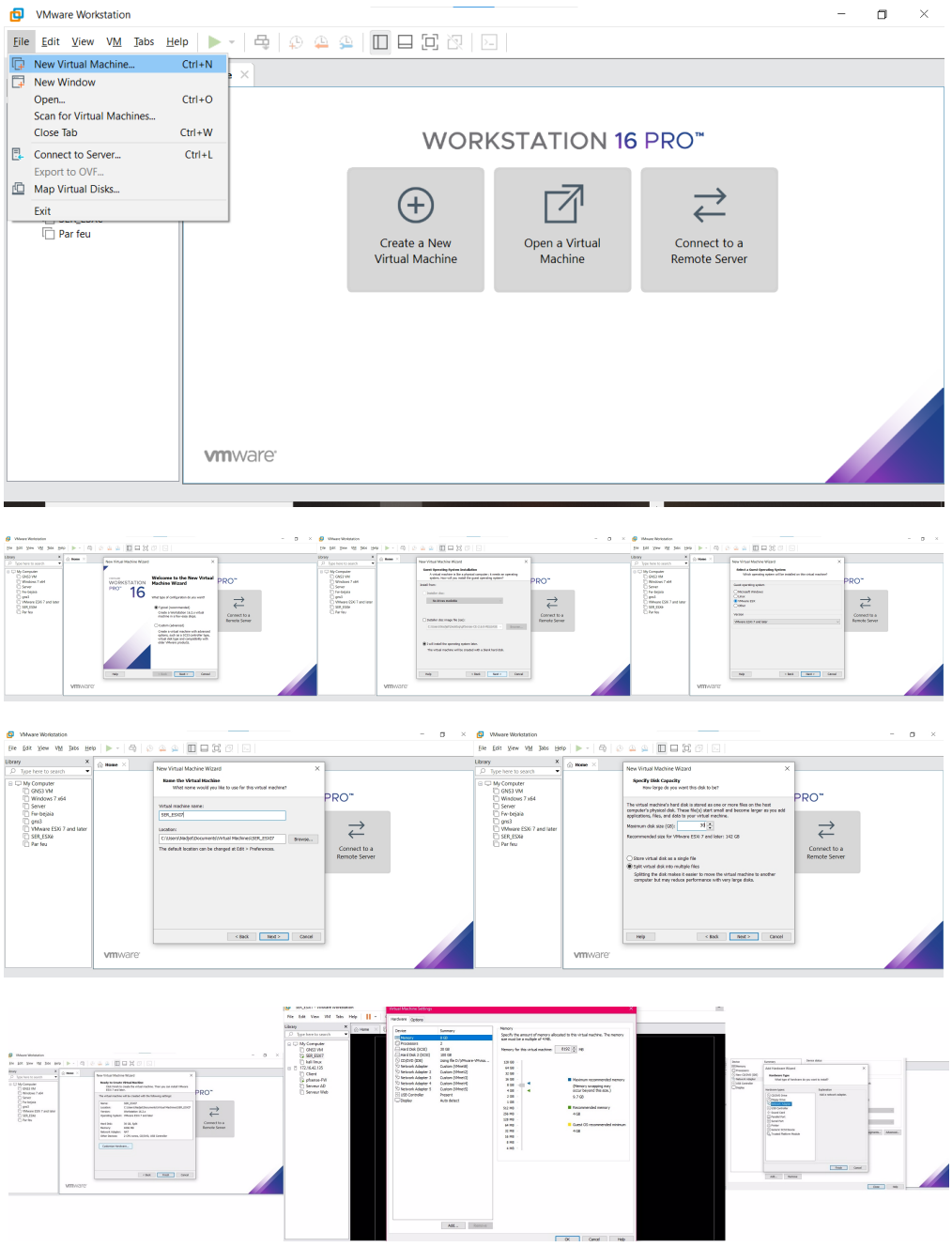

FIGURE 4.7 – Création machine virtuelle SER-ESXI7

— On Démarre la VM, après le chargement de l'ISO

— On clique sur F2 pour accéder au paramètre, nous avons entré notre mot de passe de (ASR**2023) → Configure

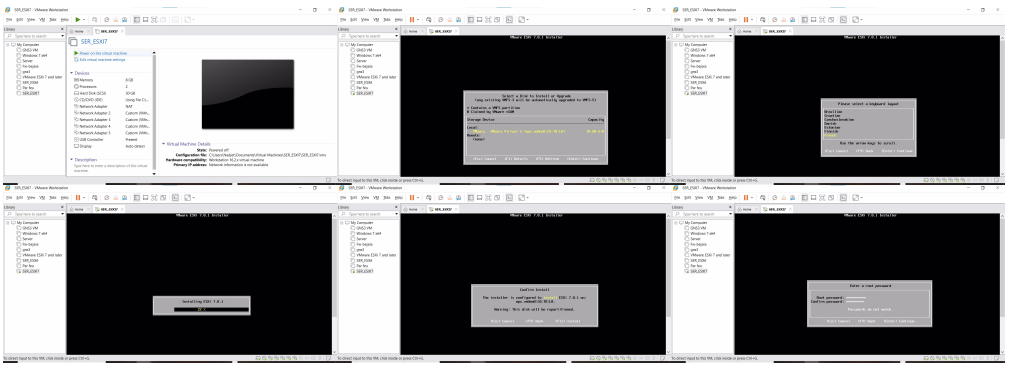

FIGURE 4.8 – Installation ESXI

— On configure le Management Network → IPv4 Configuration → Set Statique IPv4 adresse and network configuration.

— IPv6 Configuration → espace (pour choisir disable IPv6).

— DNS Configuration → host Name (Sonatrach. Local).

— Renseigner l'adresse IP, Masque et la Passerelle en adéquation avec le sous-réseau du VMnet management créé au tout début Cliquez sur OK puis sur Yes pour redémarrer Configure Management Network.

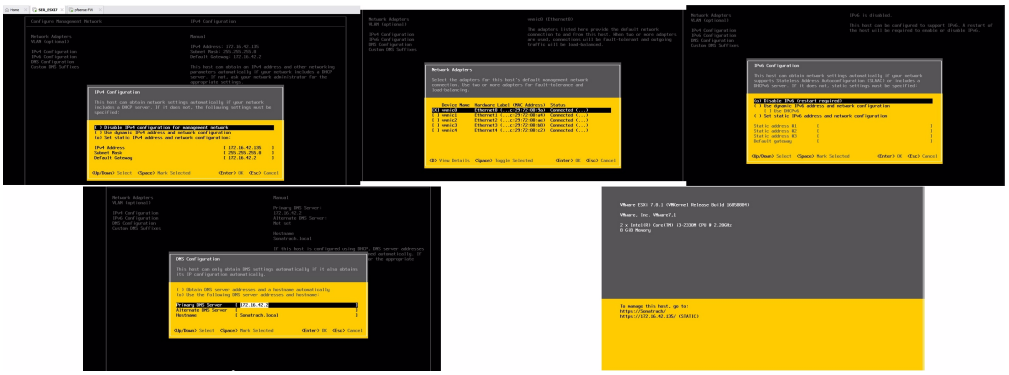

FIGURE 4.9 – Configuration de ESXi

4.5.1 Création des commutateurs virtuelle vSwitchs

— Sur l'interface graphique de notre ESXI (ça veut dire dans le navigateur) on doit donner l'adresse de notre SER-ESXI7 (ici, c'est https ://172.16.42.135) → après saisir le nom et le mot de passe

— Un commutateur virtuel, également appelé vSwitch ou commutateur réseau virtuel, est un commutateur basé sur un logiciel qui fonctionne dans un environnement virtualisé. Il permet aux machines virtuelles (VM) de communiquer entre elles et avec le réseau physique.

— Un vSwitch crée des connexions de réseau virtuel entre les machines virtuelles et le réseau physique. Il permet également des configurations de réseau avancées, telles que le marquage VLAN, le façonnage du trafic et l'isolation de réseau.

— On va cliquer sur une mise en réseau → commutateur virtuel, on clique sur ajouter un commutateur virtuel standard, une fenêtre va apparaitre (regarder la figure 4.10) on donne un nom à notre VSwitch (exemple ici VSwitch1) et on clique sur ajouter.

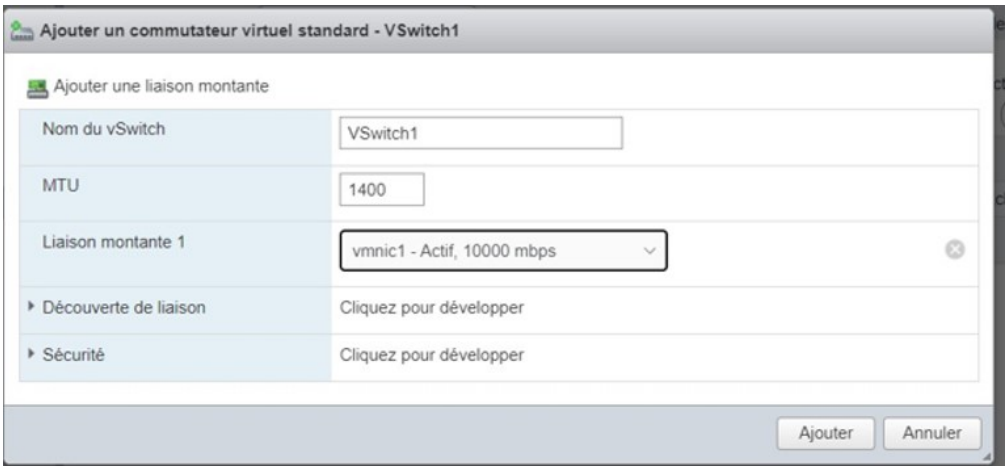

FIGURE 4.10 – Création de premier Commutateurs virtuels

— Voici tous les commutateurs virtuels que l'on a créés, le vSwitch0 c'est le commutateur par défaut de l'ESXI (pour le management de notre ESXI).

FIGURE 4.11 – Création des commutateurs virtuels

4.5.2 Création des groupes de port

— Un réseau ou groupe de ports est connecté à un VSwitch, qui lui-même se connecte à une interface réseau physique. Les groupes de ports compartimentent une partie des ports du Switch.

— Ajout d'un groupe de port On clique sur ajouter un groupe de ports, dans la fenêtre suivante, on donne un nom à notre groupe de ports (ici le nom est Serveurs) et puis on lui affecte le vSwitch adéquat et on laisse tous les autres paramètres par défaut (regarder la figure 4.12).

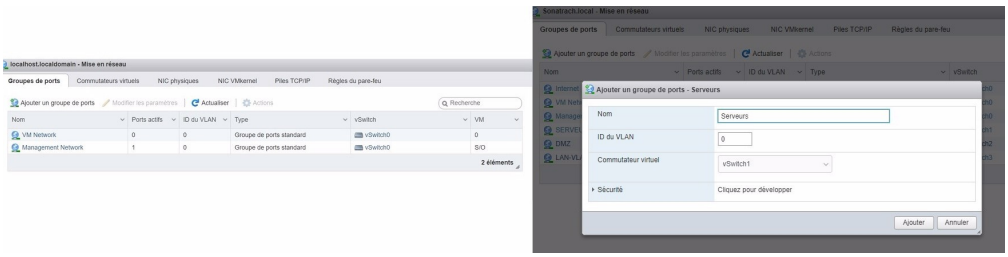

FIGURE 4.12 – Ajout de groupe de port

— Voici Les groupes de port de notre ESXI que on a créer (regarder la figure 4.13)

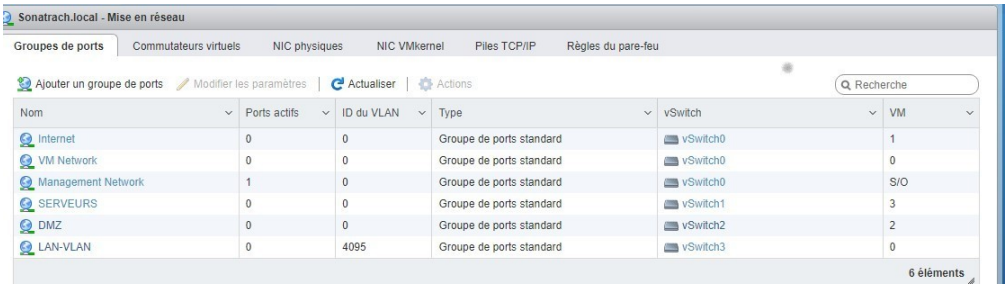

FIGURE 4.13 – Groupes de ports crées.

— Une fois le vSwitch et le groupe de ports créés et configurés, on passe à la création machine virtuelle (VM)

4.5.3 Création d'une machine virtuelle

— Sur notre ESXI, on clique sur le bouton machine virtuelle. Puis, on clique sur créer une machine virtuelle, Ensuite, nous cliquons sur suivant dans la première fenêtre qui apparaît et nous entrons le nom VM, et sélectionnez le système d'exploitation que nous voulons installer sur la VM.

— On clique une dernière fois sur Suivant et l'on arrive sur le résumé de notre machine, on clique sur Terminer. On met notre VM sous tension et l'on procède à l'installation de l'OS.

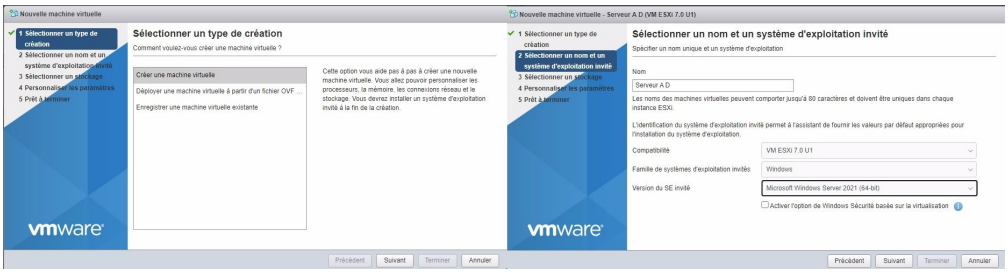

FIGURE 4.14 – création de la machine virtuelle Serveur AD

— Ensuite, nous choisissons l'emplacement de stockage(datastore) où nous voulons installer notre VM et nous arrivons à l'écran avec lequel nous configurons le matériel De la VM. Configuration minimale recommandée Pour notre système d'exploitation. Sur le lecteur de DVD, sélectionnez dans la liste déroulante" Fichier ISO Banque de données", l'écran suivant apparaître afin que vous puissiez choisir l'ISO à utiliser avant le téléchargement.

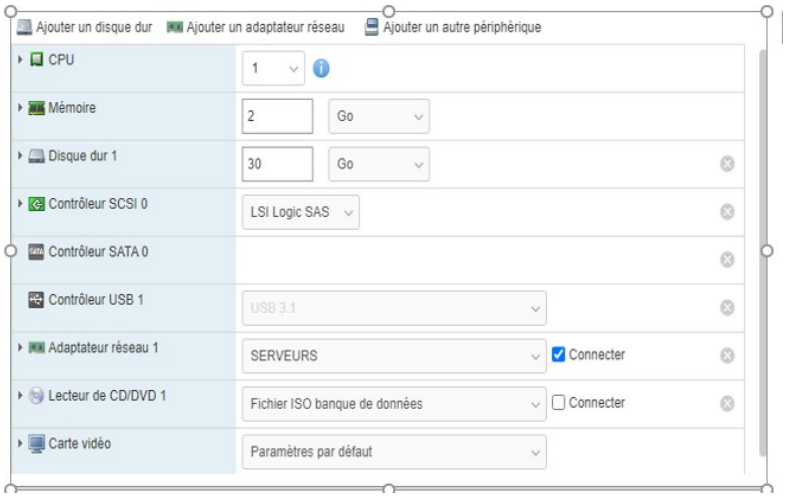

FIGURE 4.15 – Configuration de la machine virtuelle.

FIGURE 4.16 – Informations de la machine Serveur AD

— Pour les trois autres machines virtuelles (Client et pare-feu et serveur web) nous avons suivi la même méthode pour les créer. La figure 4.17 illustre les trois machines virtuelles crées.

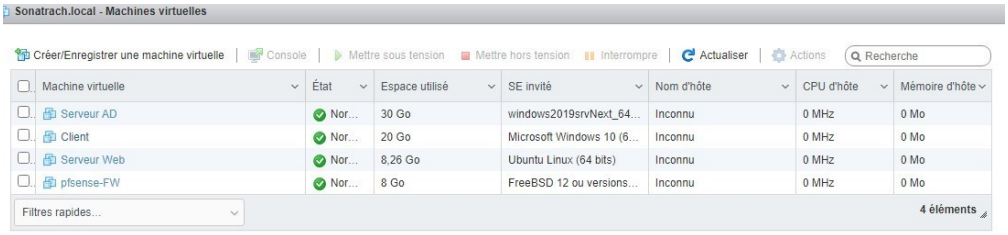

FIGURE 4.17 – les Quatre machines virtuelles crées

4.6 Installation de pfsense

Pour commencer, il faut disposer d'une image iso de Pfsense version 2.6.0 Basé sur FreeBSD, cette image est disponible sur https ://Pfsense.org/dowlnload. On utilise une machine virtuelle disposant de cartes réseaux une reliée au réseau local et l'autre branchée au réseau WAN et une treizième pour la zone DMZ et quatrième pour les serveurs. Cette capture montre l'ajout des quatre cartes réseaux que nous allons utiliser.

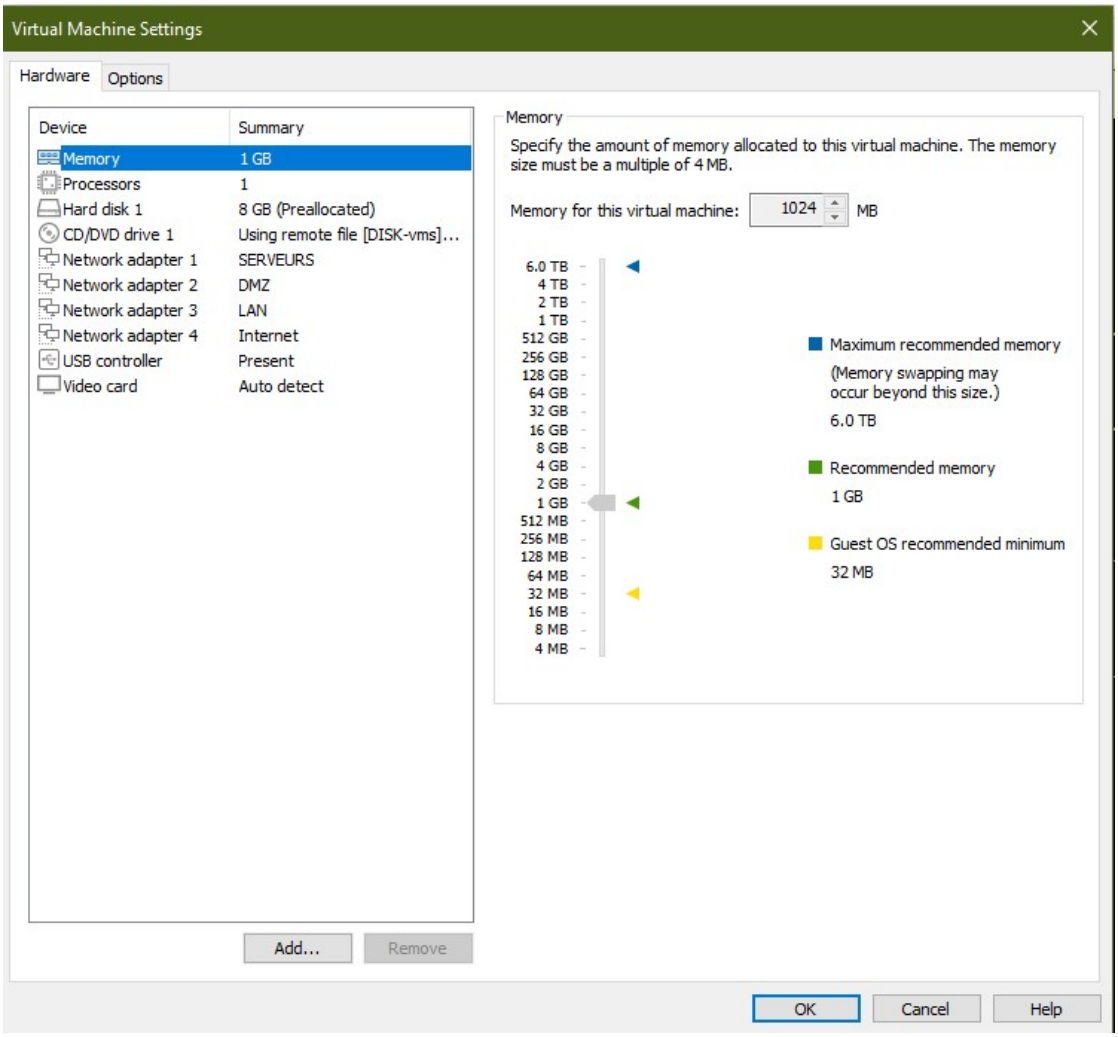

FIGURE 4.18 – Configuration des cartes réseau de pfsense

- Pour aboutir à une installation complète et correcte de pfsense nous allons suivre les étapes dans les trois prochaines captures.

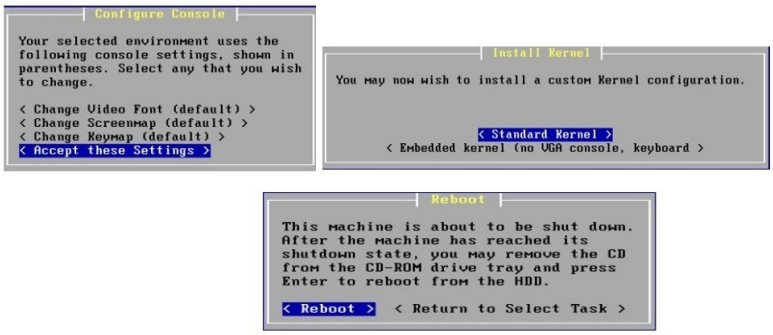

FIGURE 4.19 – Installation de par feu

4.6.1 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 4.20).

FIGURE 4.20 – Les quatre interfaces sur pfsence

L'interface graphique de notre pare-feu pfSense est accessible depuis la machine client.

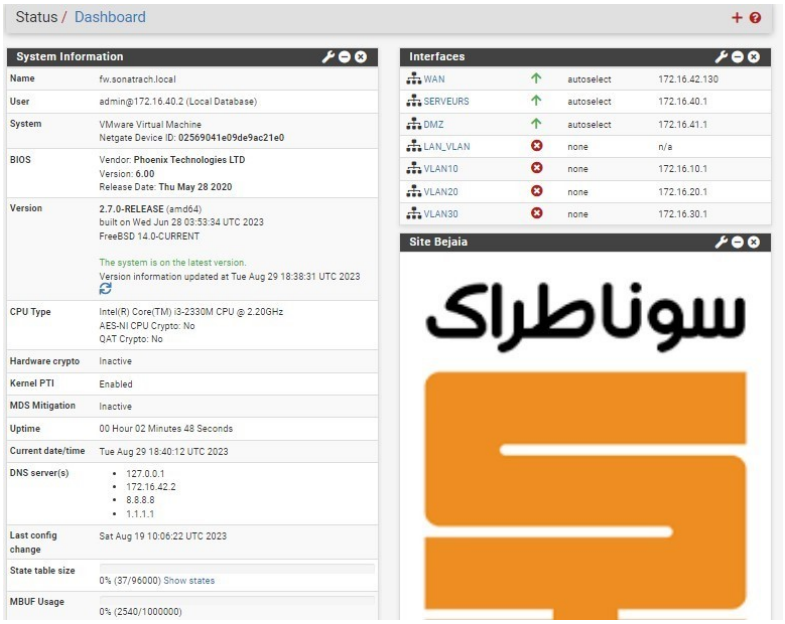

FIGURE 4.21 – l'interface graphique de parefeu.

4.6.2 Ajout des interfaces sur pfsense

La (figure 4.22) montre les quatre interfaces ajoutées :

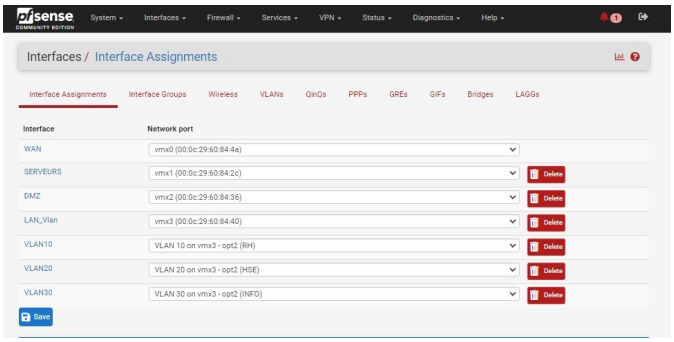

FIGURE 4.22 – Ajout des interfaces de pare feu.

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

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

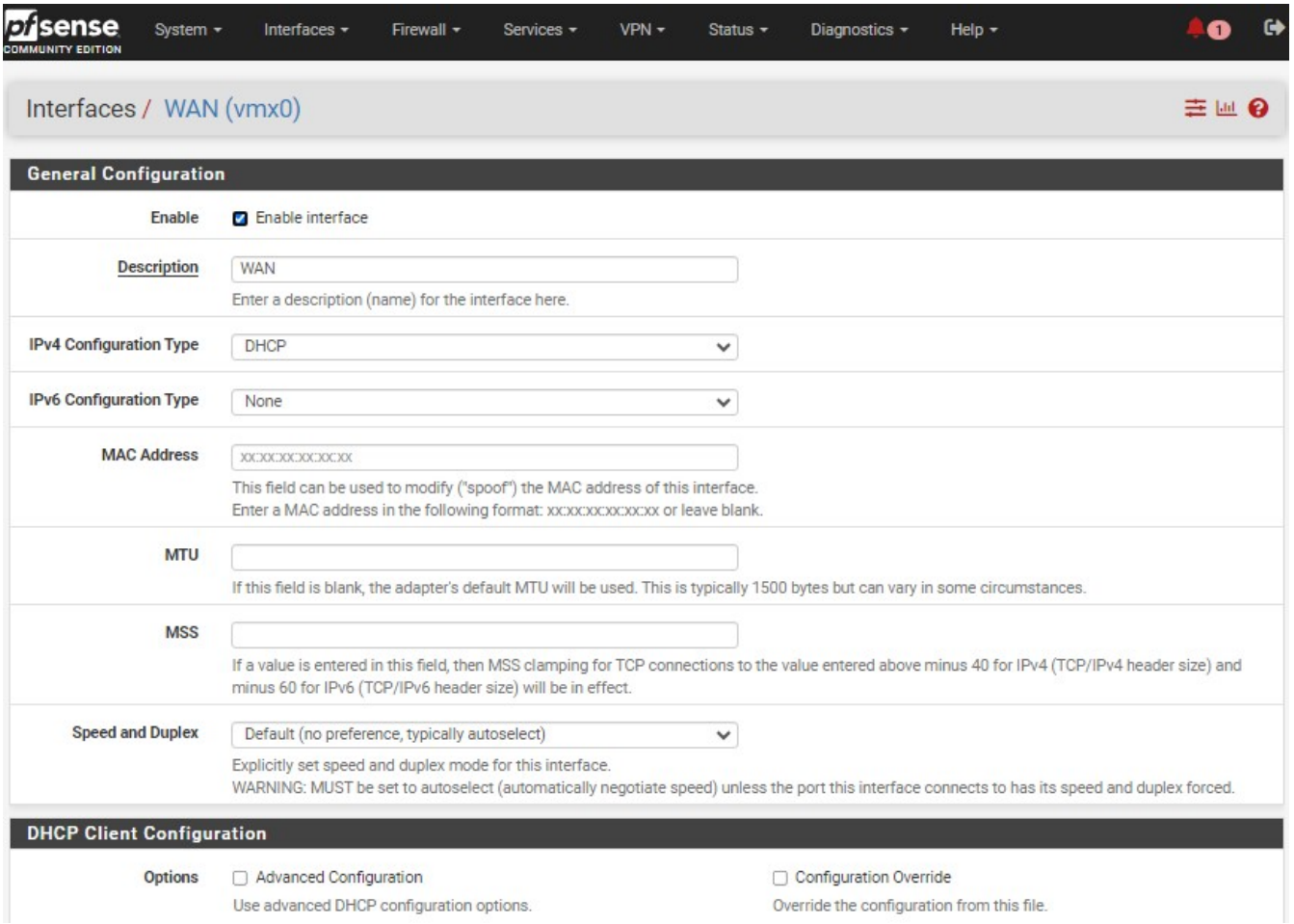

FIGURE 4.23 – La configuration de l'interface LAN.

(b) Pour l'interface du réseau LAN nous n'avons pas choisi une adresse IP.

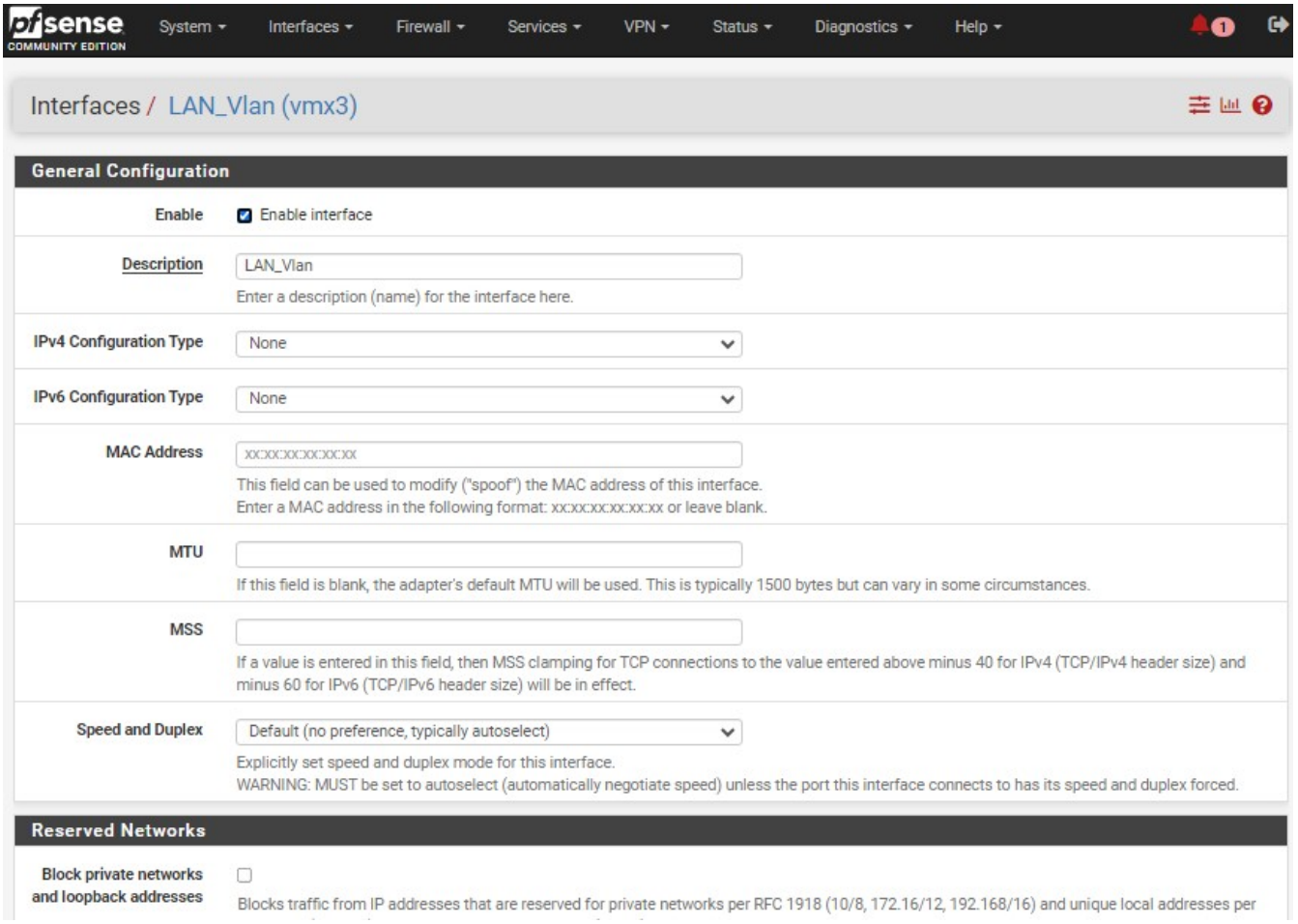

FIGURE 4.24 – La configuration de l'interface LAN.

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

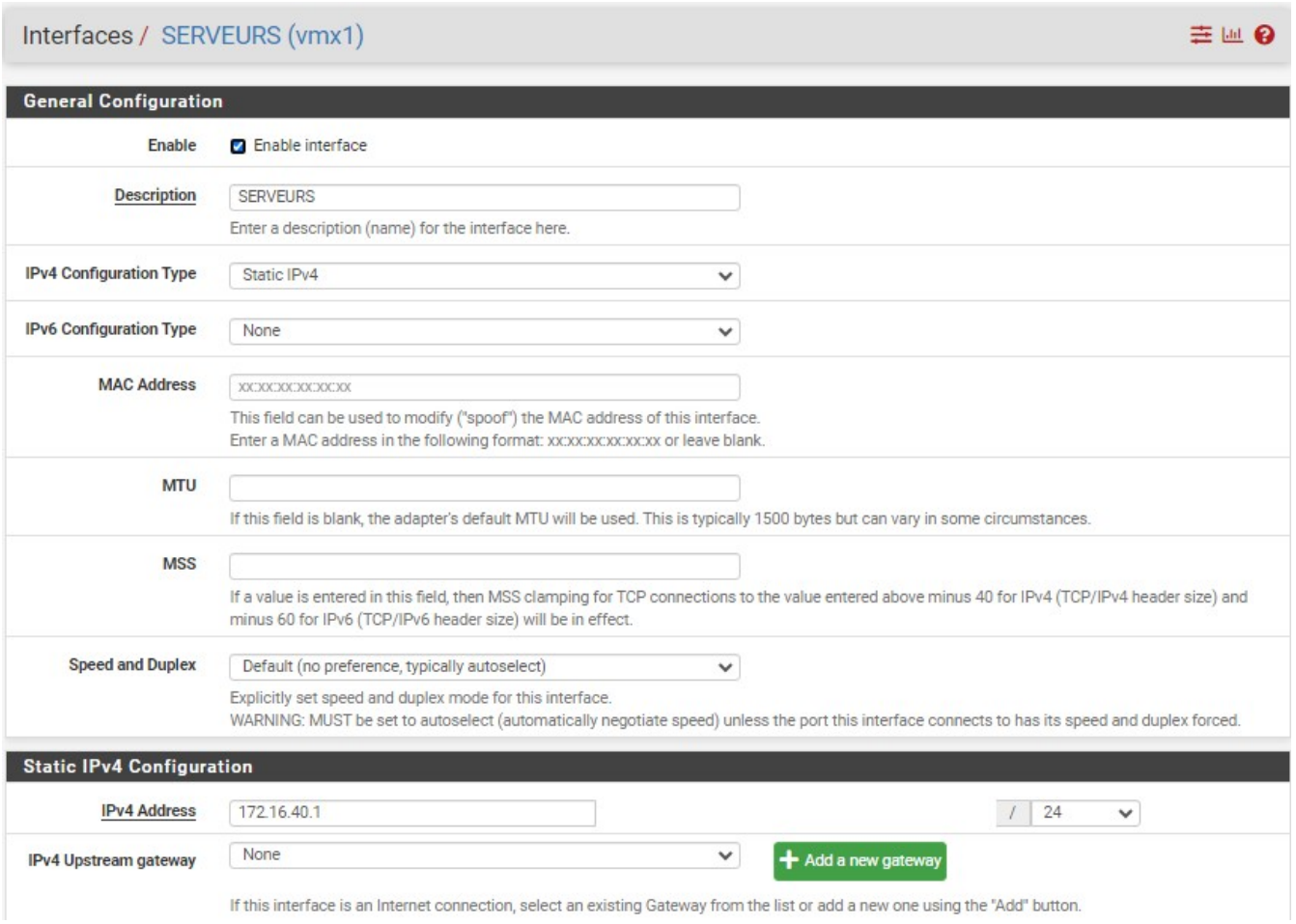

FIGURE 4.25 – La configuration de l'interface Serveurs

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

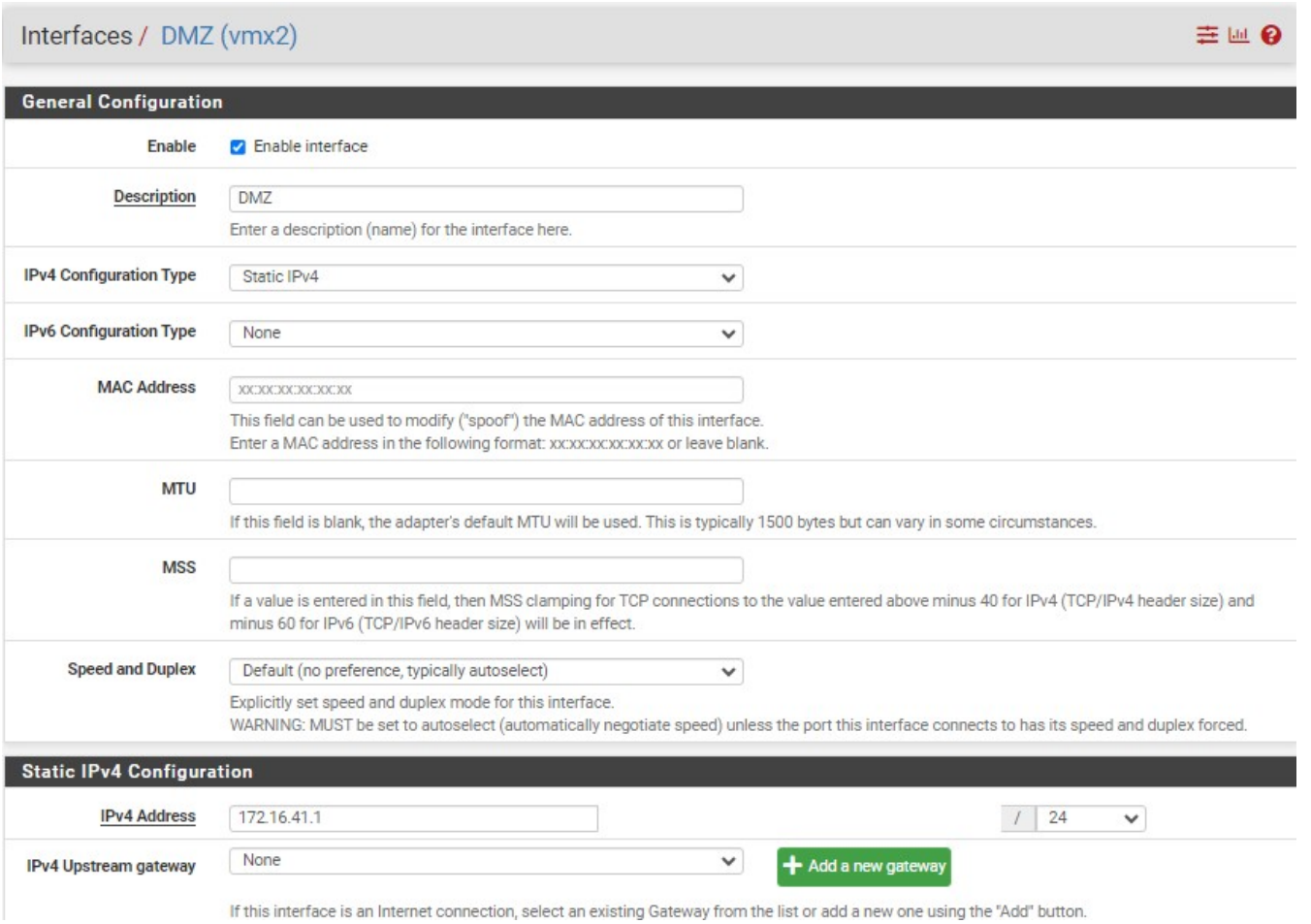

FIGURE 4.26 – La configuration de l'interface DMZ.

(e) Pour l'interface du sous réseau Vlan 10 nous avons choisi l'adresse IP static, le masque de sous Réseau et la passerelle par défaut.

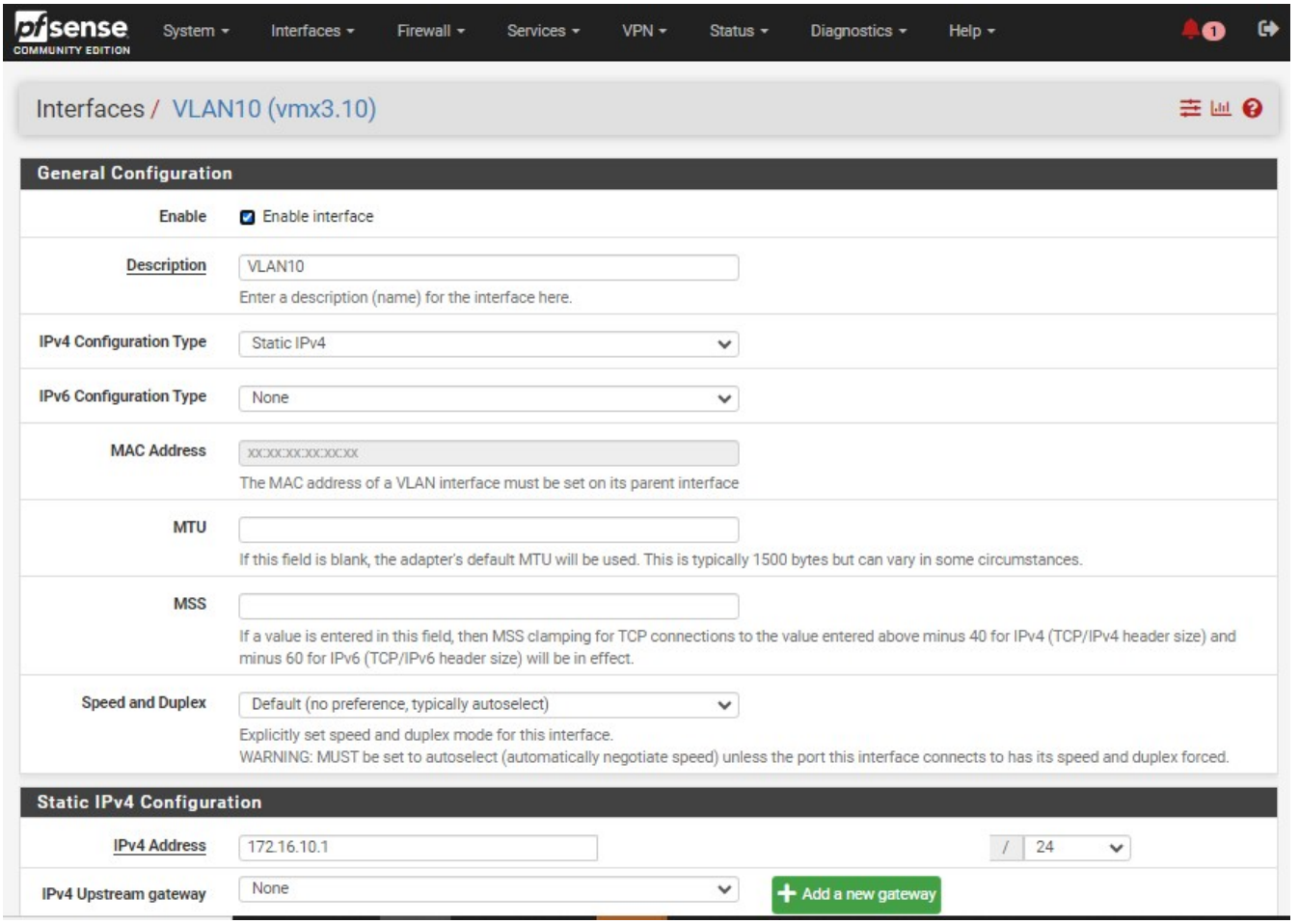

FIGURE 4.27 – La configuration de l'interface LAN-VLAN 10

(f) Pour l'interface du sous réseau Vlan 20 nous avons choisi l'adresse IP static, le masque de sous Réseau et la passerelle par défaut.

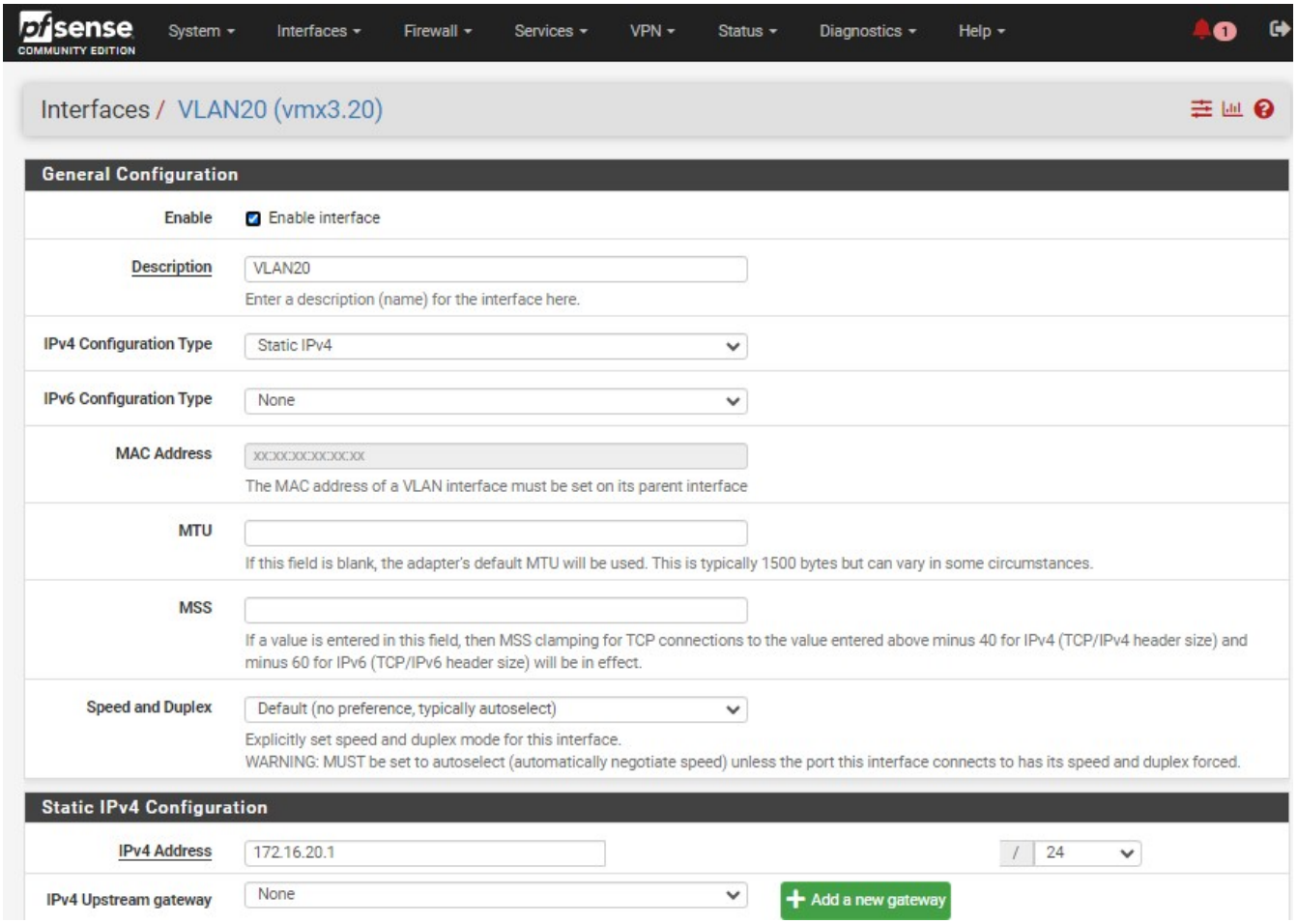

FIGURE 4.28 – La configuration de l'interface LAN-VLAN 20

(g) Pour l'interface du sous réseau Vlan 30 nous avons choisi l'adresse IP static, le masque de sous Réseau et la passerelle par défaut.

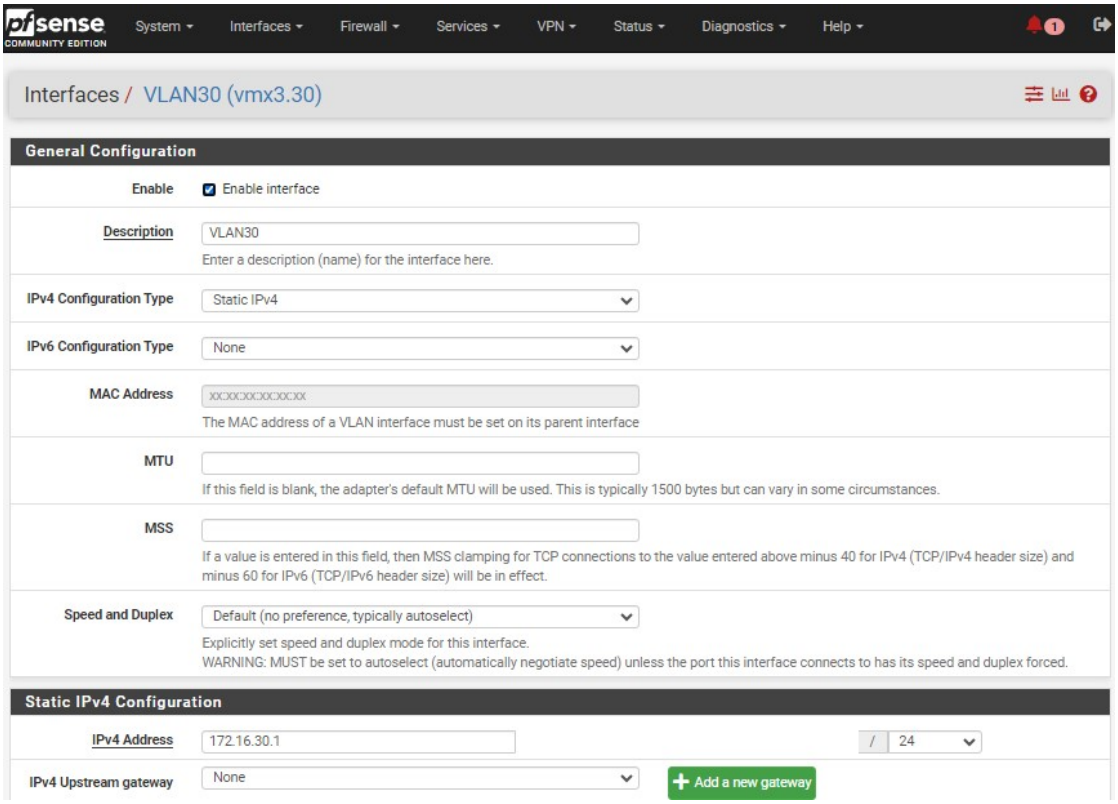

FIGURE 4.29 – La configurationde l'interface LAN-VLAN 30

— 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 4.30 représente la réussite de l'activation de la route par défaut vers Internet.

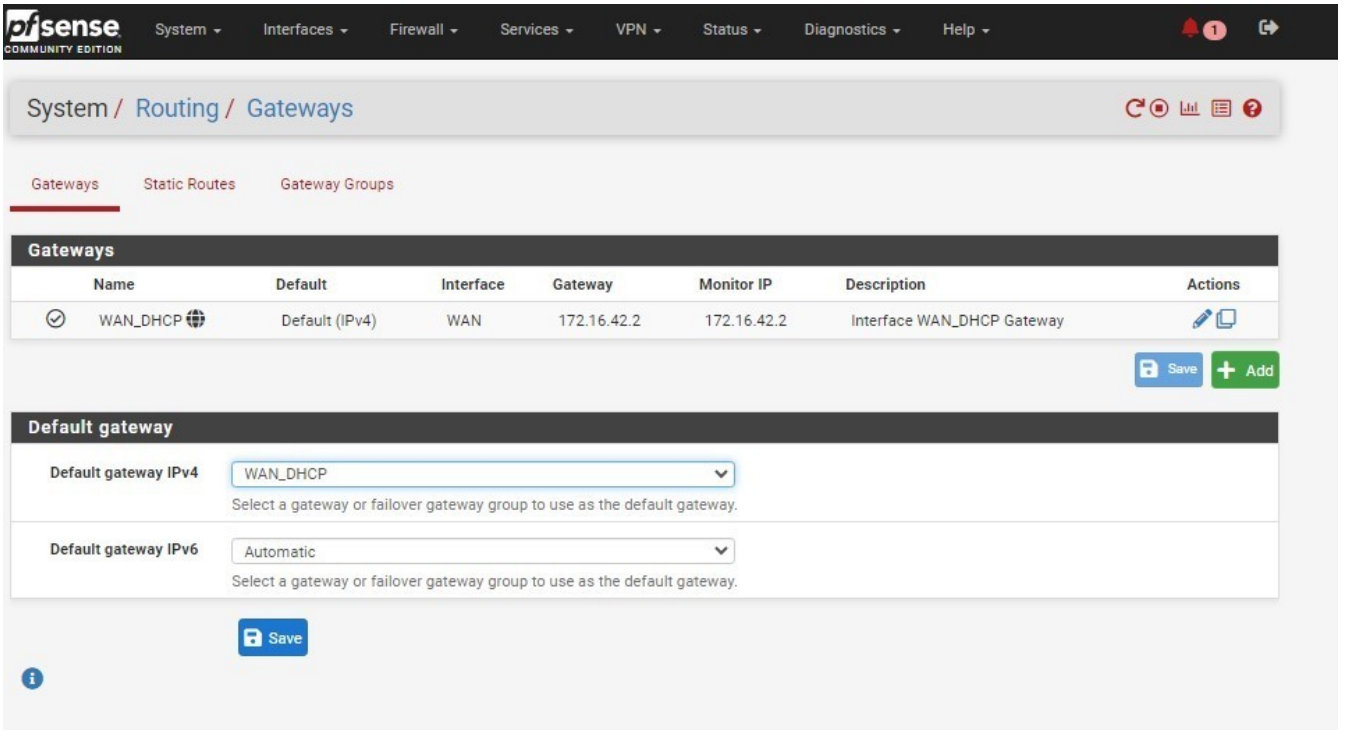

FIGURE 4.30 – Routageactivé.

— Après nous avons créé 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 :

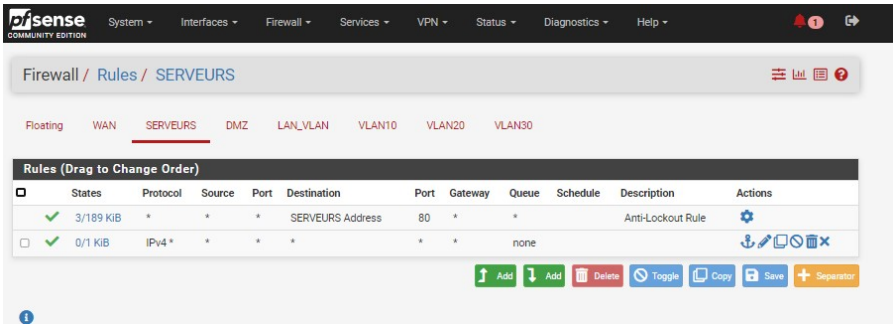

FIGURE 4.31 – Le réseau Serveurs

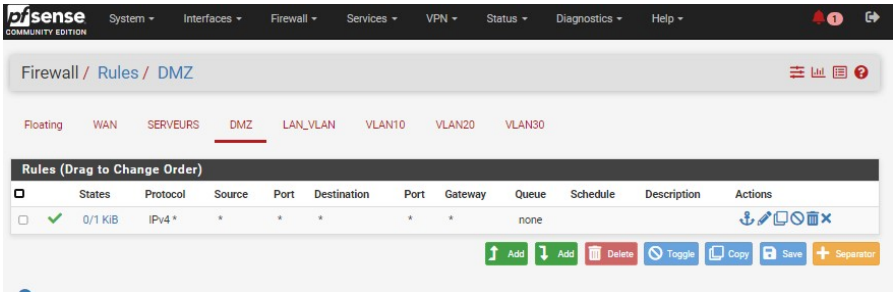

FIGURE 4.32 – Le réseau DMZ

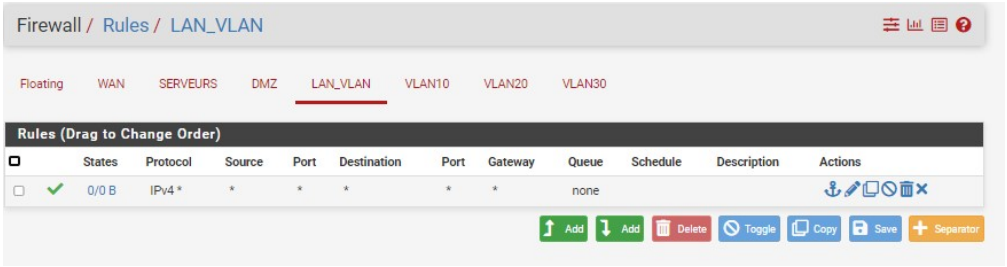

FIGURE 4.33 – Le réseau LAN

4.6.3 Installation de logiciel Snort sur pfsense

— Pour installer Snort sur un pare-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 Package disponibles et cliquer sur "installer".

— La figure 4.34 représente le package Snort recherché.

— La figure 4.35 représente que l'installation du logiciel Snort a été effectuée avec succès.

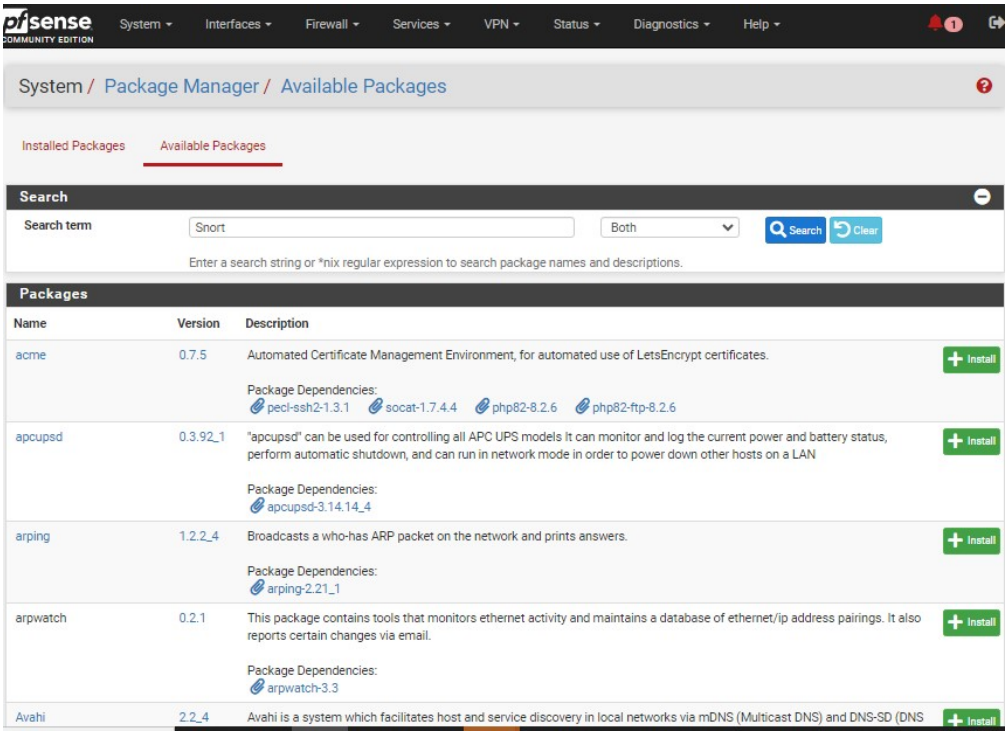

FIGURE 4.34 – Le package de Snort

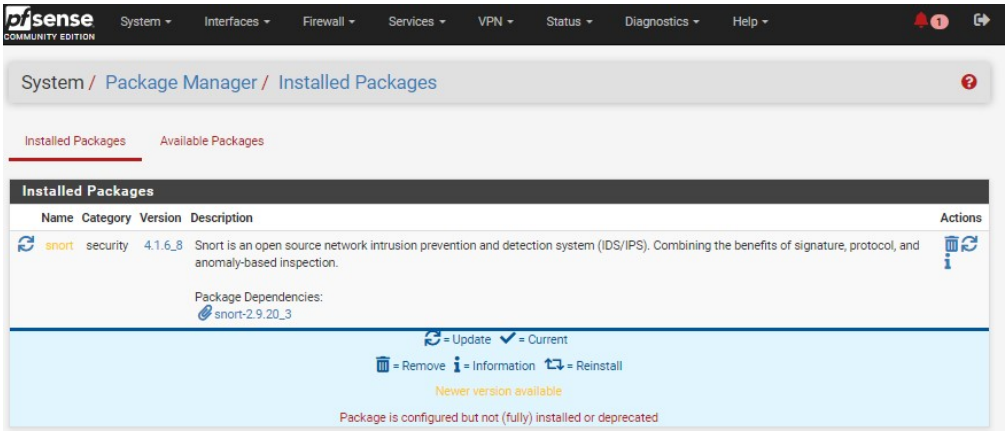

FIGURE 4.35 – Installation réussie de Snort-

4.6.4 Les configurations globales de Snort

Après l'installation, accéder aux paramètres de Snort en cliquant sur "Global Settings" Puis "Snort" pour cocher tous les packagent nécessaires et gratuits. La figure 4.36 représente l'interface des paramètres de logiciel Snort

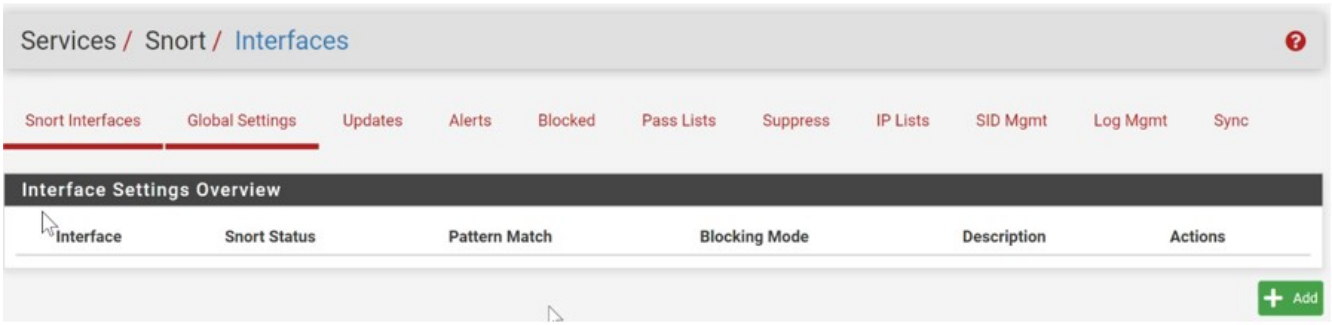

FIGURE 4.36 – Interface des Paramètres de Snort

Les figures ci-dessous représentent les packages nécessaires :

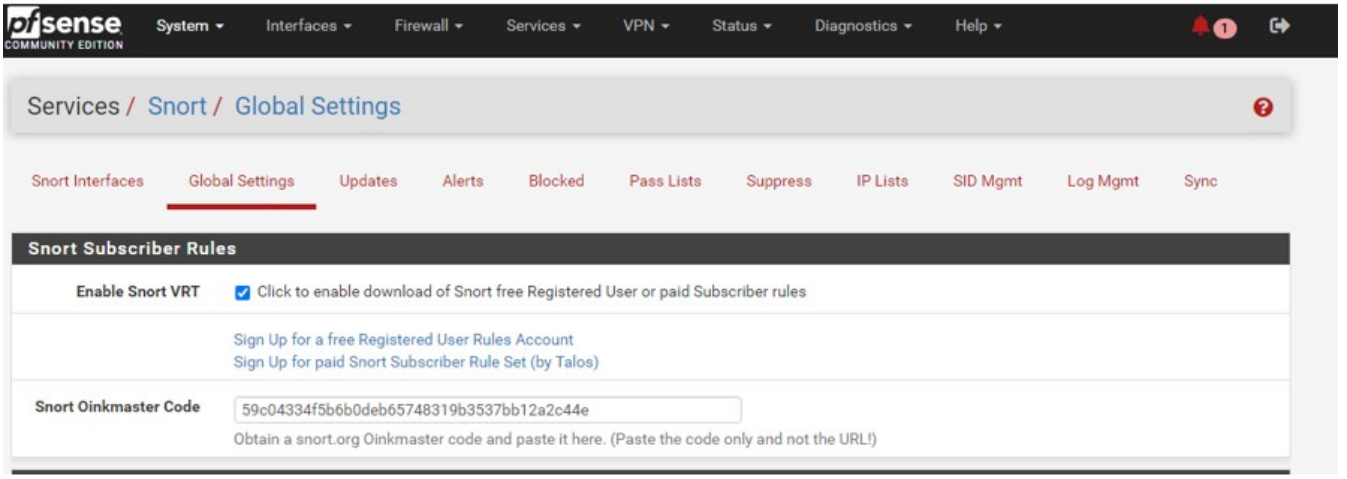

FIGURE 4.37 – Le package de la signature.

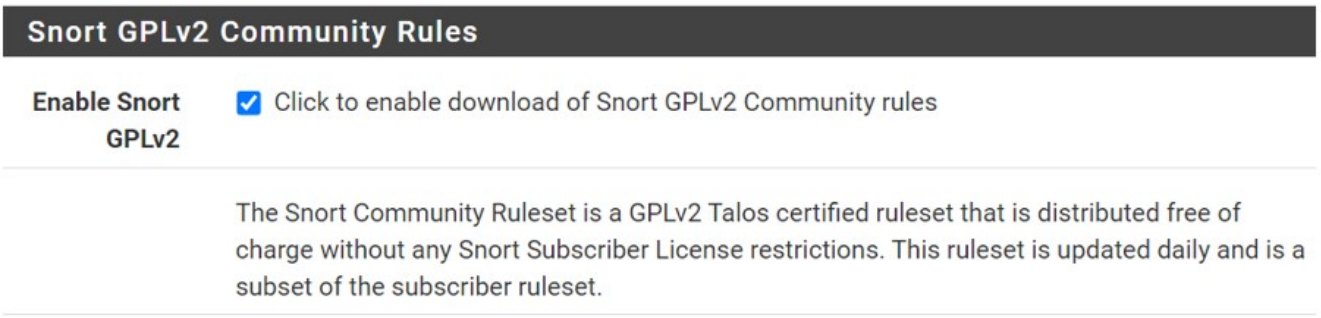

FIGURE 4.38 – La licence GPLv2 de Snort.

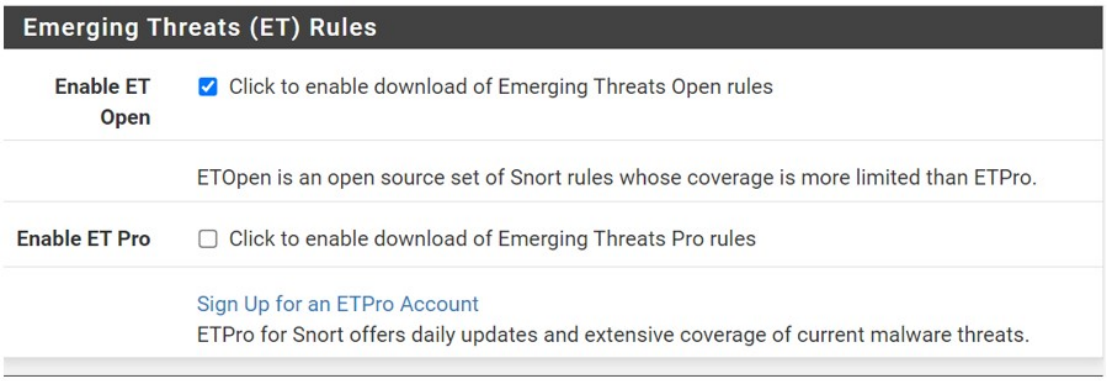

FIGURE 4.39 – Les règles de détection d'intrusion.

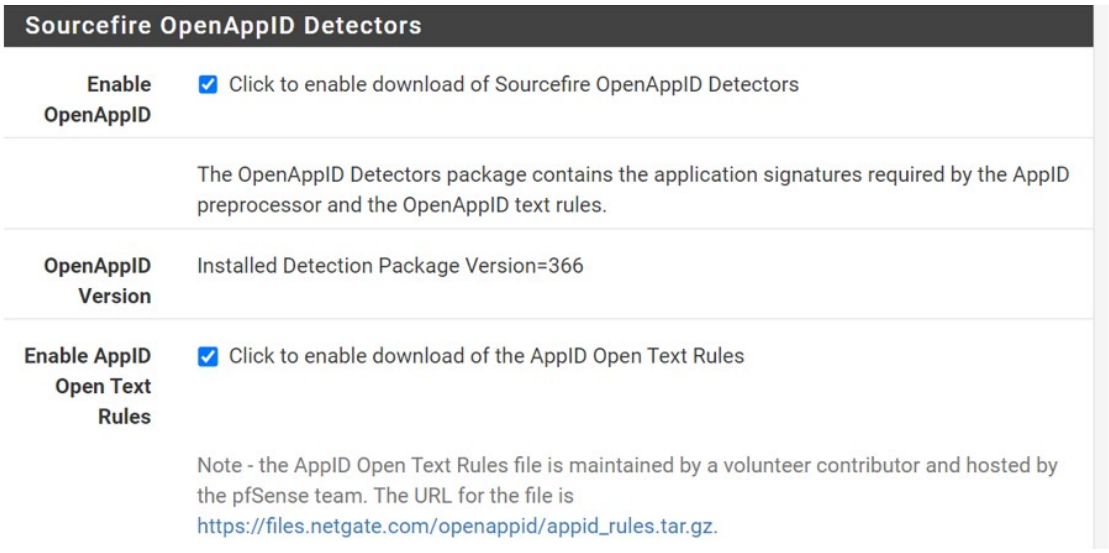

FIGURE 4.40 – Les règles de détection d'intrusion.

Les mises à jour 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 4.41) les mises se feront automatiquement.

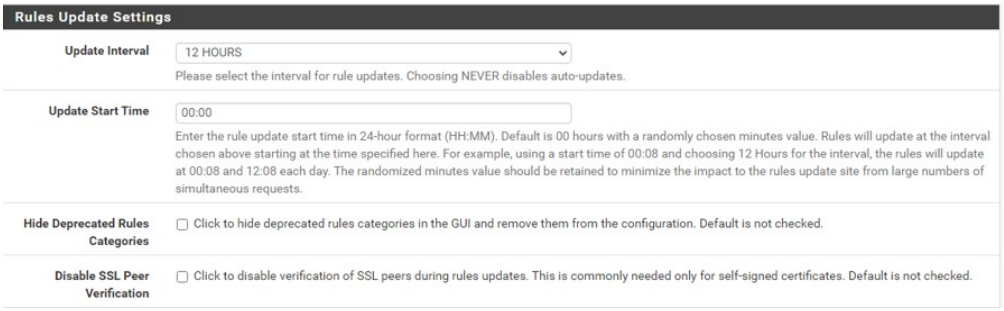

FIGURE 4.41 – Paramètres de mise jour des règles.

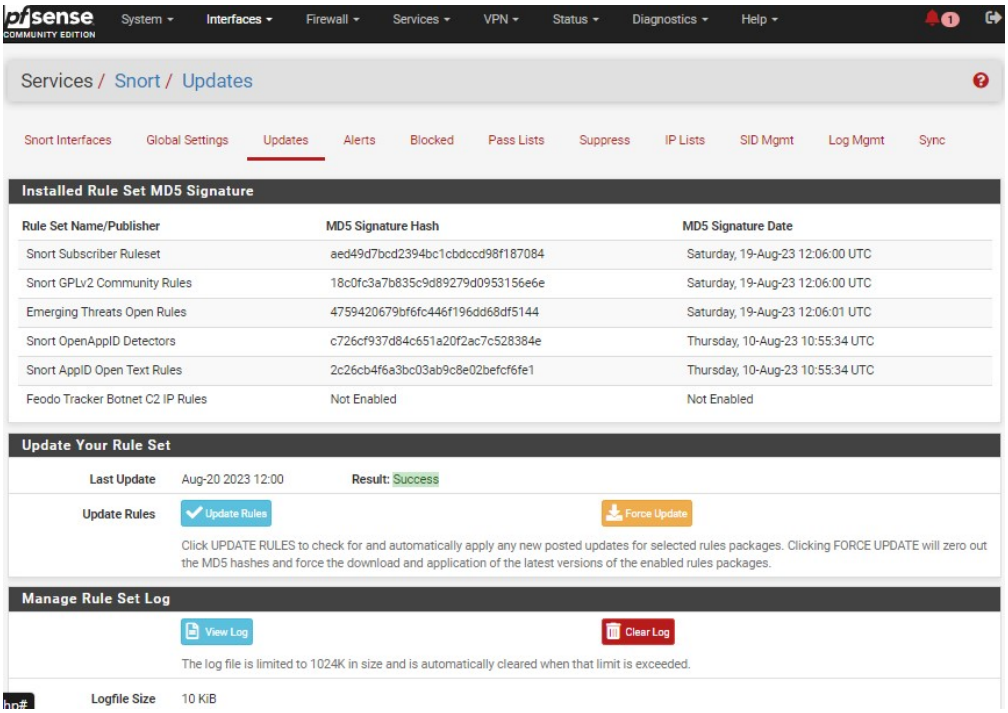

FIGURE 4.42 – Les mises jour effectuer par Snort

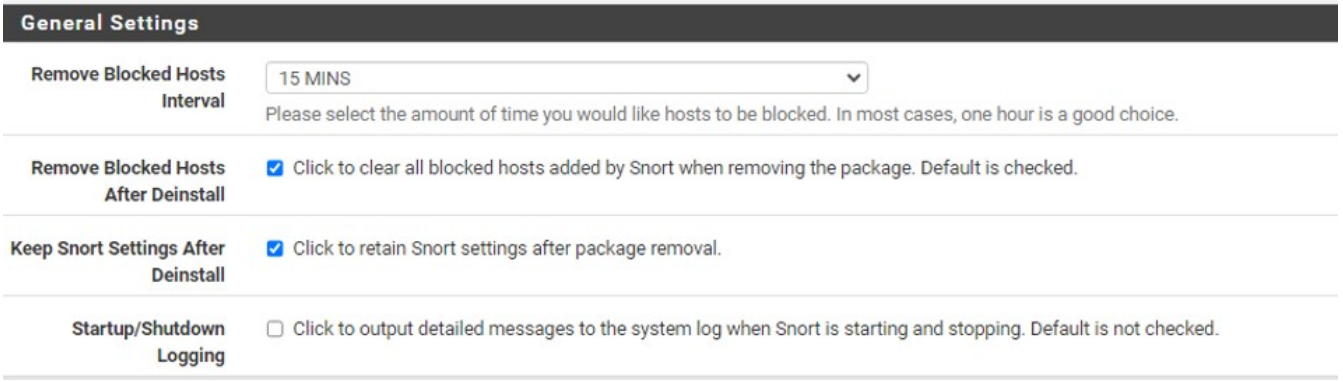

FIGURE 4.43 – Contrôle du temps de blocage.

4.6.5 Configuration de l'interface Snort

Nous avons choisi l'interface WAN pour appliquer les détections d'intrusions (Snort).

La figure 4.44 illustre les étapes de configurations.

Les deux figures 4.45 et 4.46 représentent les packages utilisés pour la détection des intrusions.

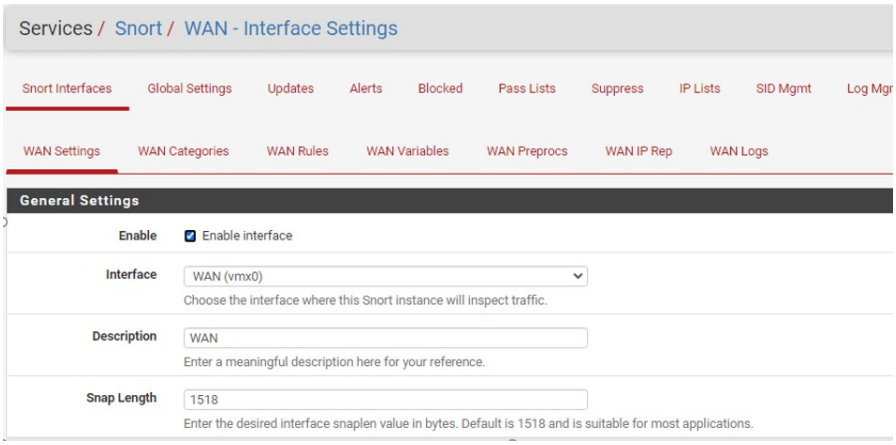

FIGURE 4.44 – L'interface Snort

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

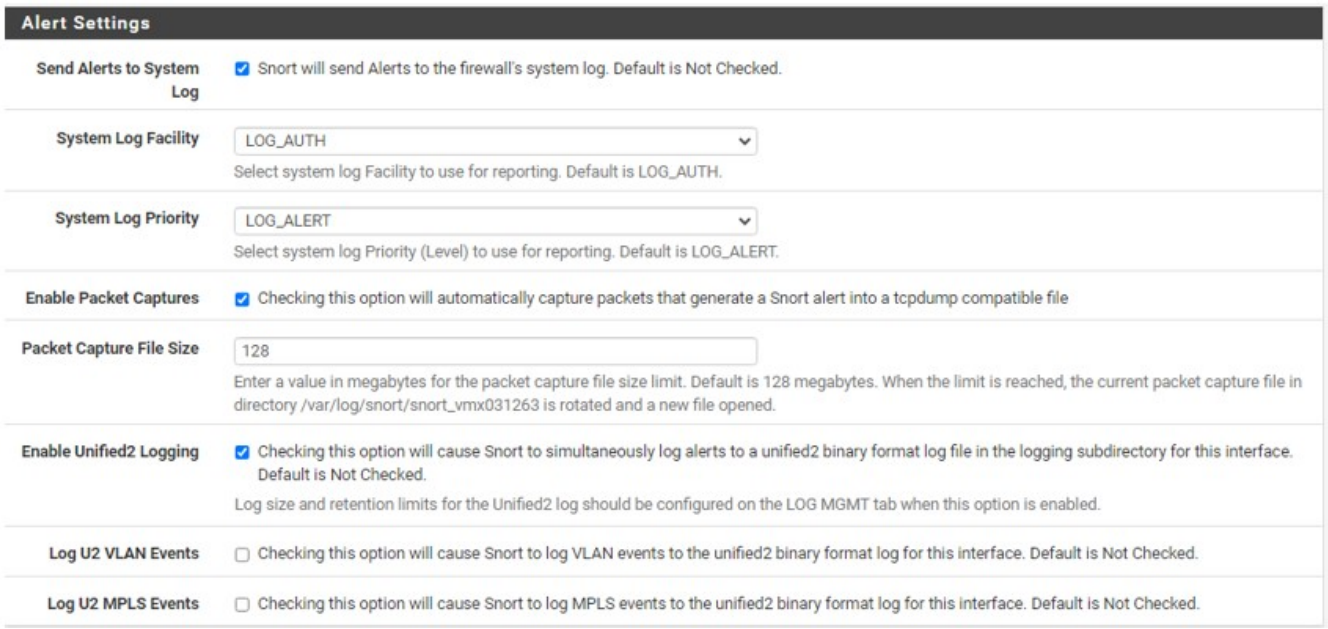

FIGURE 4.45 – Activation des alertes

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

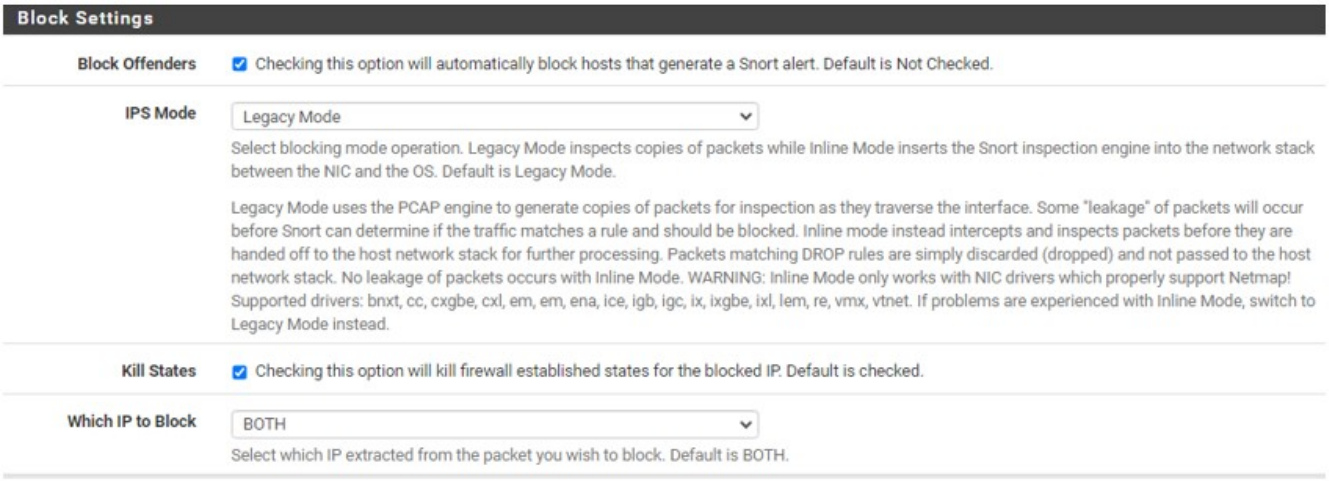

FIGURE 4.46 – Blackage des hôtes

4.6.6 Activation de l'interface Snort

C'est selon les mises à jour que nous avons effectué :

Les étapes pour activer l'interface Snort sont illustrer dans les deux figures 4.47 et 4.48.

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

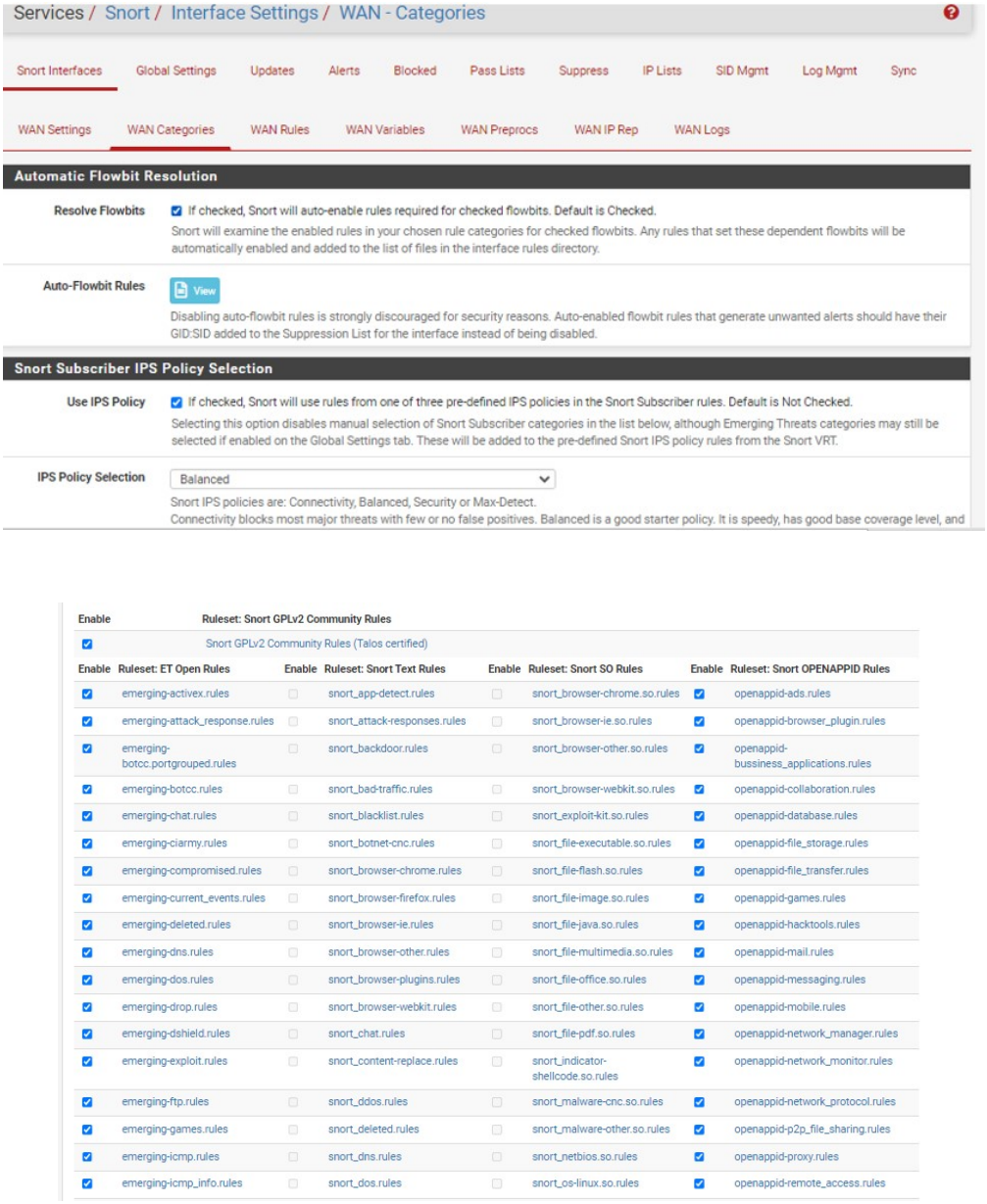

FIGURE 4.47 – Activation de Snort

Allumage de l'interface Snort.

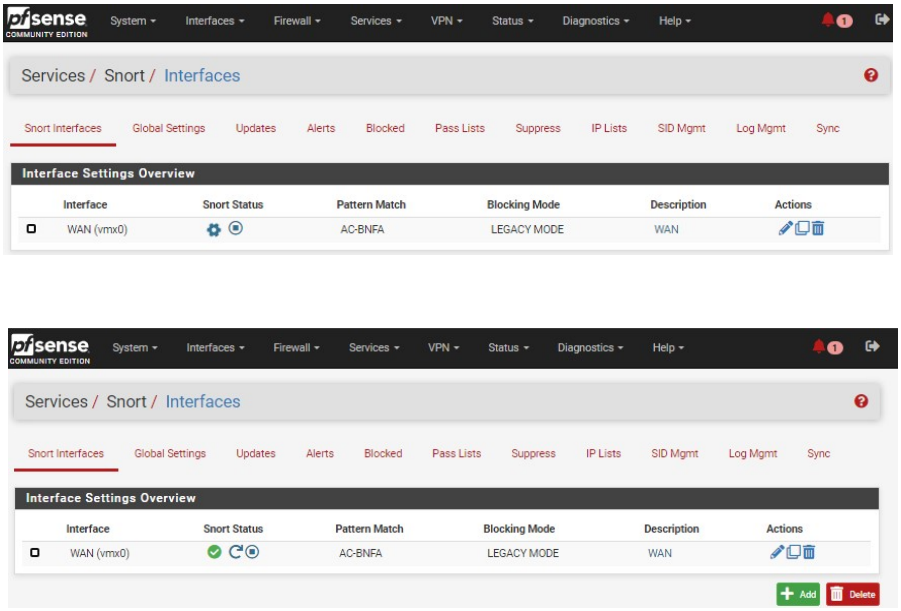

FIGURE 4.48 – Interface en action

Ouvrir les ports pour recevoir les alertes comme illustrer dans la figure 4.49.

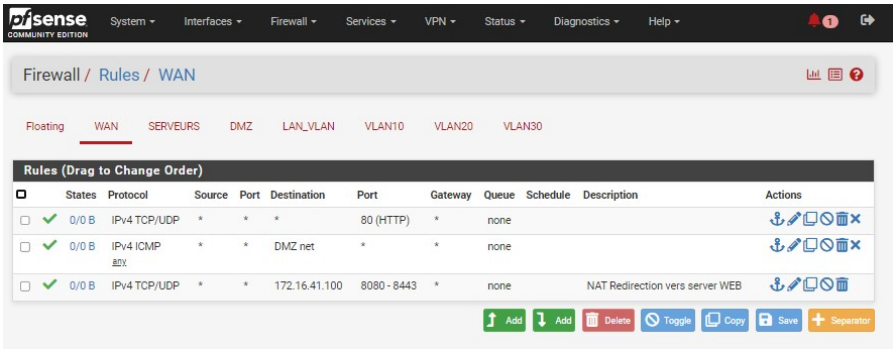

FIGURE 4.49 – Ouverture des ports

4.7 Les serveurs

4.7.1 Installation d'Active Directory

Active Directory de Microsoft gère les ressources réseau sous Windows et peut être déployé dans VMWare en tant que machine virtuelle pour des services d'annuaire centralisés. Il centralise l'authentification des utilisateurs, la gestion des comptes, groupes, politiques de sécurité, et la gestion des ressources réseau.

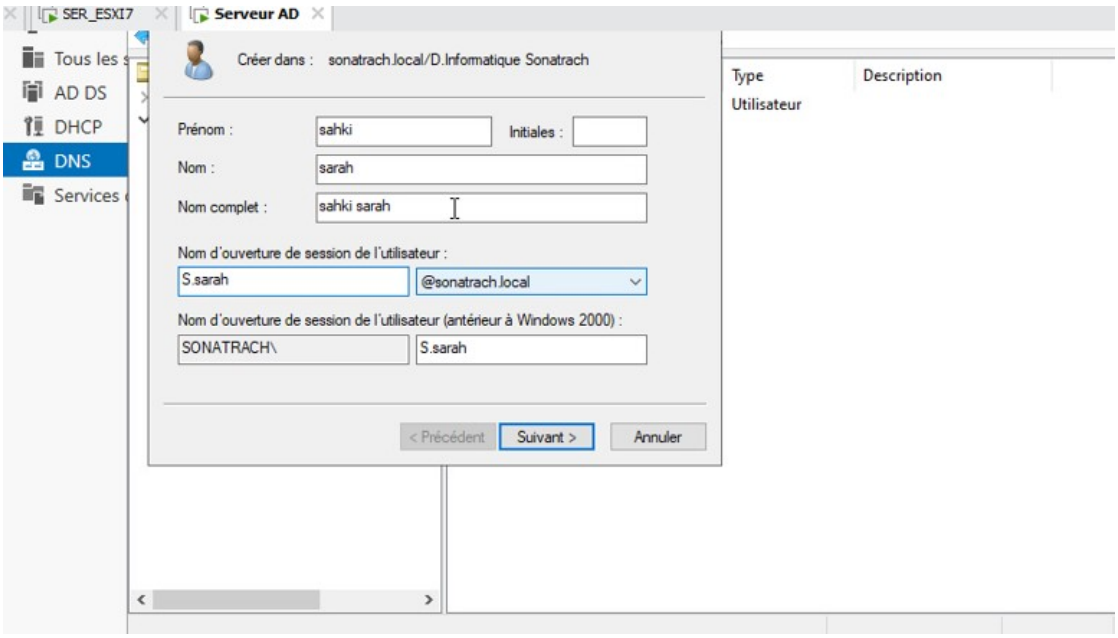

FIGURE 4.50 – les étapes d'installation Serveur AD

L'utilisation d'Active Directory dans VMWare permet de simplifier la gestion des ressources et des utilisateurs à travers l'infrastructure virtuelle. Pour ajouter Active Directory, il est nécessaire de passer par l'assistant de gestion des rôles. Il suffit de cocher la case "Serveur AD DS" et "Serveur DNS " puis on clique sur Ajouter des fonctionnalités, puis continuez l'assistant en cliquant sur Suivant.

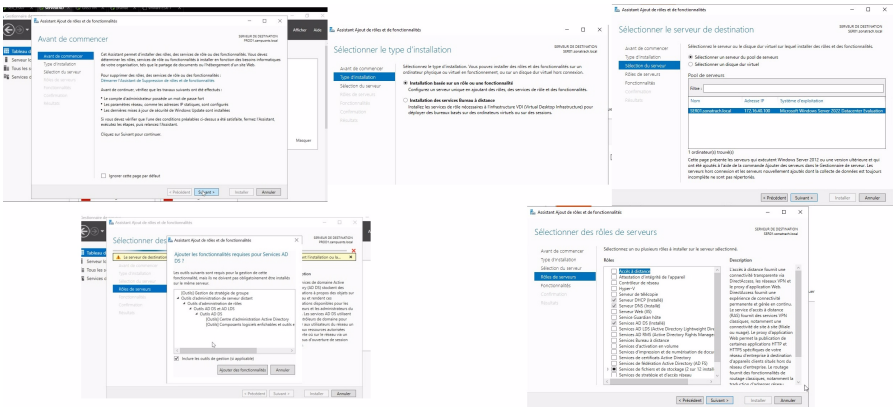

FIGURE 4.51 – Ajout des fonctionnalités de serveur AD

Dans les prochaines étapes, les fonctionnalités obligatoires ont été prés cochés. En cliquant sur "Suivant", tous Les paramètres par défaut sont conservés. Ensuite, en cliquant sur "Installer", l'assistant procède à l'installation Des services Active Directory Domain Services.

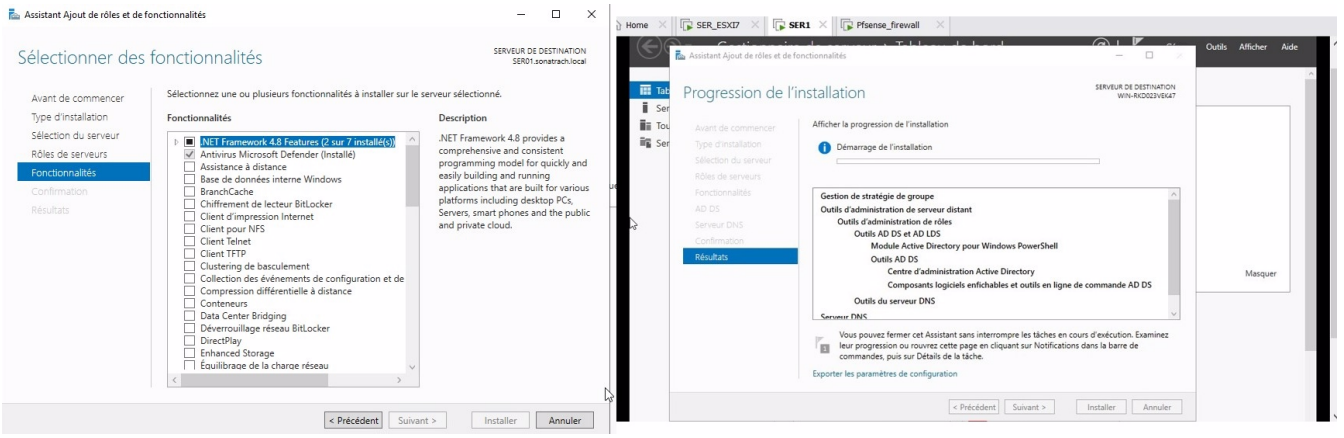

FIGURE 4.52 – Installation des services de serveur AD

Pour transformer cet ordinateur en contrôleur de domaine, il est nécessaire de suivre des étapes supplémentaires. En cliquant sur "Promouvoir ce serveur en contrôleur de domaine", L'assistant de Configuration des Services de domaine Active Directory se lance, on ajoute une forêt et on lui donne un nom de domaine.

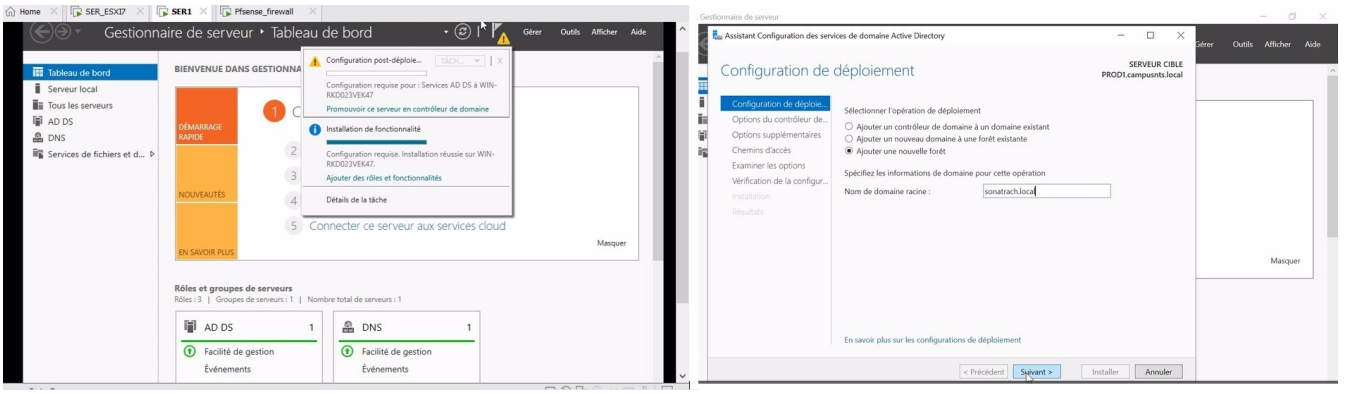

FIGURE 4.53 – Ajout d'une forêt

Ensuite, nous définissons le niveau fonctionnel de la forêt et du domaine, ainsi que le mot de passe. Ensuite, nous cliquons sur "Suivant".

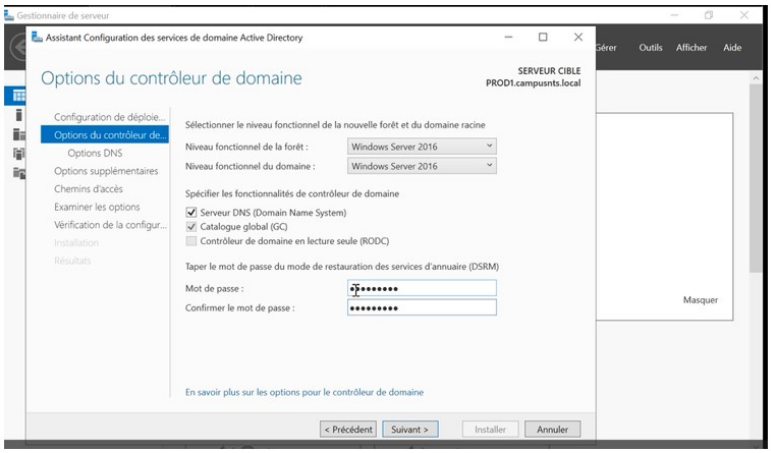

FIGURE 4.54 – Ajout mot de passe pour le forêt

Dans toutes les étapes suivantes, on laisse les paramètres par défaut en cliquant sur suivant. Ici le nom NetBIOS de notre domaine est ensuite déterminé, on peut éventuellement le changer.

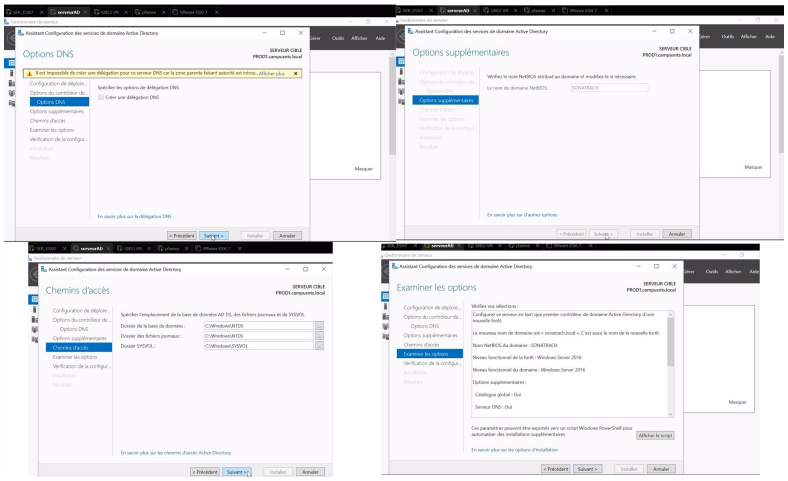

FIGURE 4.55 – Ajout un nom NetBIOS

Le dernier écran récapitule notre configuration, puis nous cliquons sur "Installer" pour finaliser le processus. Une fois cette tape terminée,

l'installation est achevée.

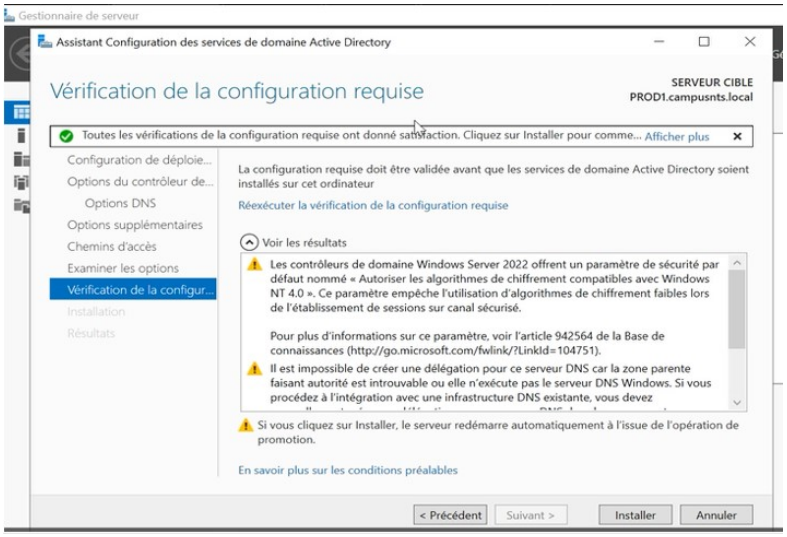

FIGURE 4.56 – vérification de la configure requise

a) **Création des utilisateurs, unité d'organisation et groupe :** Ouvrir la console Utilisateurs et ordinateurs Active Directory. Faire un clic droit sur le domaine, aller sur Nouveau et l'on clique sur Unités d'organisation

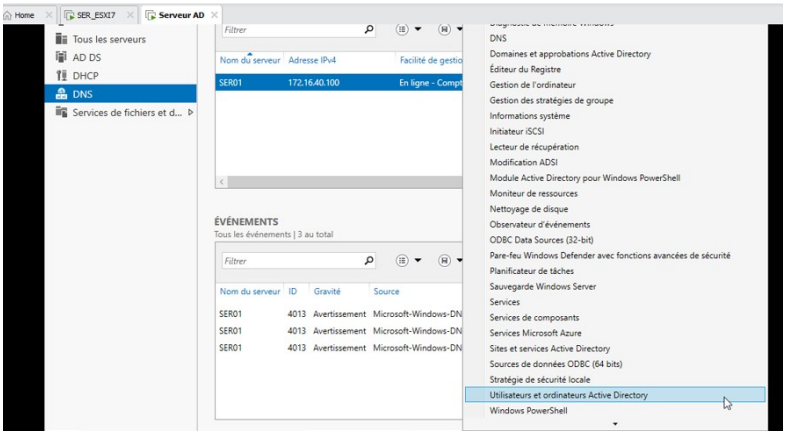

FIGURE 4.57 – Ajout utilisateurs et ordinateurs AD

Nous commençons par attribuer un nom à notre unité d'organisation, puis nous cliquons sur "OK". Dans ce cas, nous avons créé une unité d'organisation appelée (département informatique Sonatrach). À l'intérieur de cette unité, nous avons également créé une autre unité appelée "user" (utilisateurs), comprenant les utilisateur Sarah (cette dernière étant créée dans une autre unité)

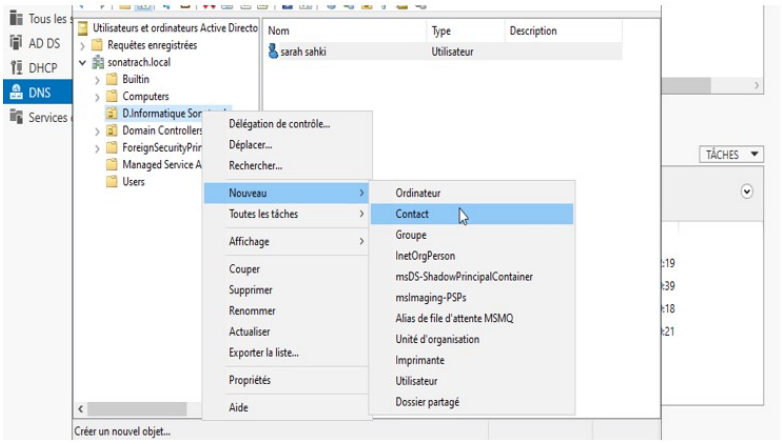

FIGURE 4.58 – Création d'utilisateur pour l'unité d'organisation

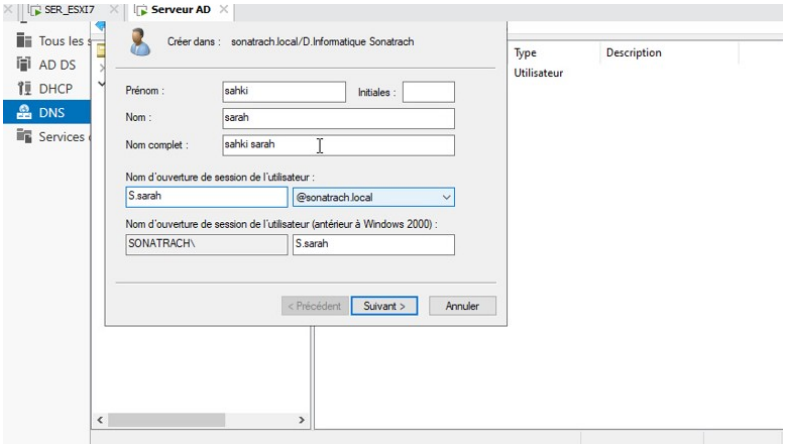

FIGURE 4.59 – Création d'utilisateur pour l'unité d'organisation

Clique droite sur user nouveau utilisateur, on entre le nom, prénom et l'identifiant de l'utilisateur qui est associé au domaine S. imane @Sonatrach.local puis on clique sur suivant on (par la suite, on va ajouter cet utilisateur autant qu'administrateur de notre système depuis la machine client)

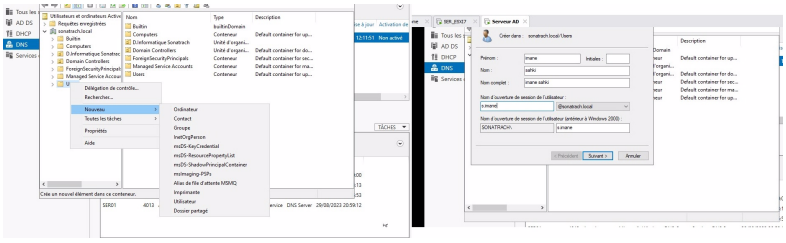

FIGURE 4.60 – Création d'utilisateur et l'associé a notre domaine

On choisit un mot de passe pour notre utilisateur et l'on choisit si le mot de passe reste fixe ou bien l'utilisateur pourra le changer puis on clique sur suivant et puis sur terminer pour ajouter notre utilisateur

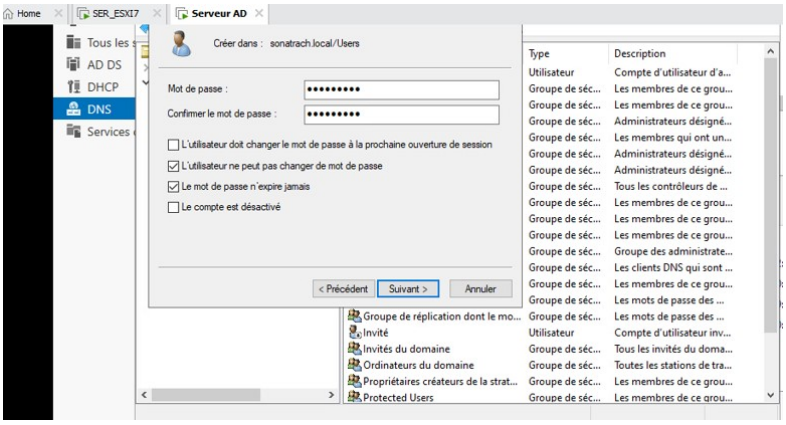

FIGURE 4.61 – Ajout mot de passe à notre utilisateur

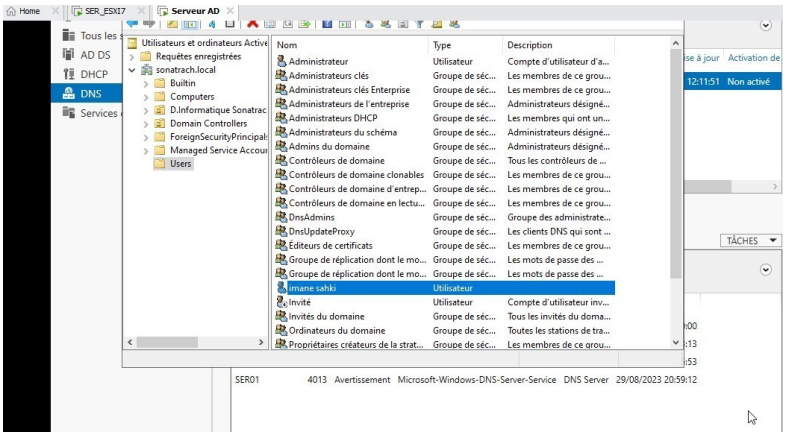

FIGURE 4.62 – Le nouvel utilisateur crée

Ajouter client au domaine en tant qu'admin associé à un utilisateur : Lorsque nous cliquons sur "Identifier" sur le réseau, une fenêtre s'affiche, nous permettant de sélectionner les cases qui indiquent que notre ordinateur est connecté à un réseau d'entreprise et que notre entreprise possède un nom de domaine. Nous saisissons l'identifiant de notre utilisateur, préalablement créé dans l'Active Directory, ainsi que son mot de passe. L'utilisateur est ensuite associé à la machine "client"

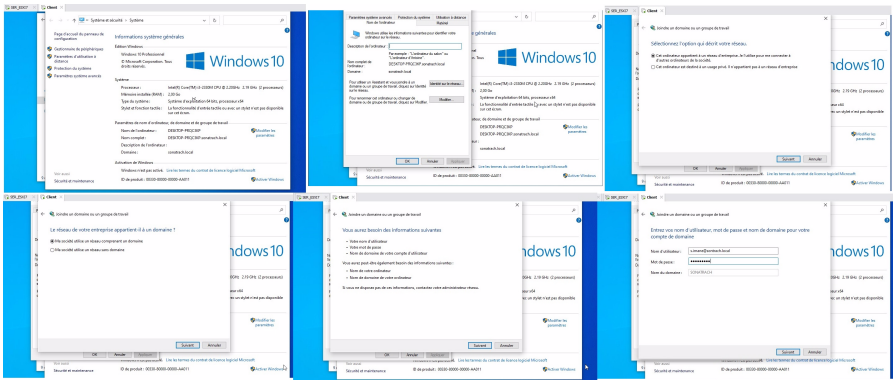

FIGURE 4.63 – Ajout client au domaine

Après cela ont saisi le nom de notre domaine, s'authentifier pour autoriser se connecter au domaine

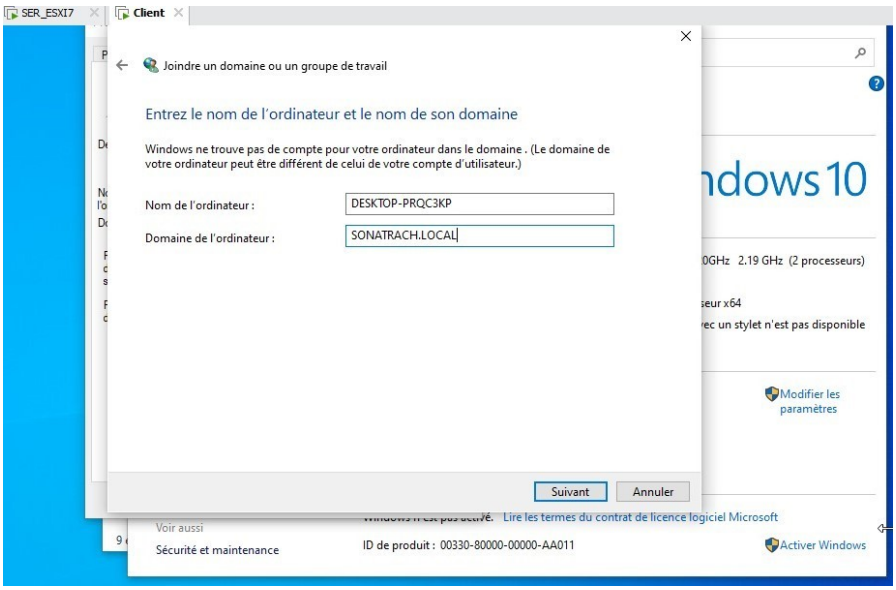

FIGURE 4.64 – Saisir le nom de notre domaine

Nous activons le compte de l'utilisateur du domaine sur cet ordinateur (client) et le sélectionnons comme administrateur. Ensuite, nous cliquons sur "Suivant", puissur "Terminer", et redémarrons notre machine pour appliquer les configurations

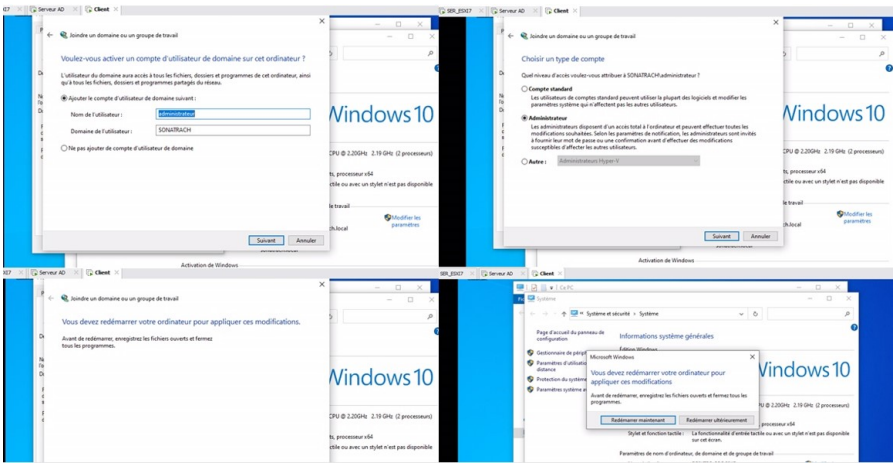

FIGURE 4.65 – Activation de compte administrateur

4.7.2 Installation de Serveurs web

La figure 4.66 illustre les étapes d'installation apache2 sur de serveur web.

La f igure 4.66 illustre les étapes d'installation apache2 sur de serveur web.

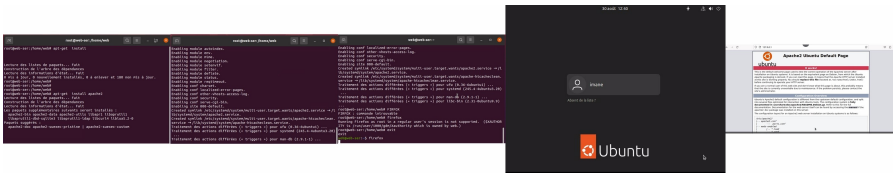

FIGURE 4.66 – les étapes d'installation serveur web

4.8 Installation de Kali linux

La figure 4.67 illustre les étapes d'installation de kali linux.

FIGURE 4.67 – Installation de kali linux

4.9 Installation Client Windows 10

La figure 4.68 illustre les étapes d'installation Client Windows 10

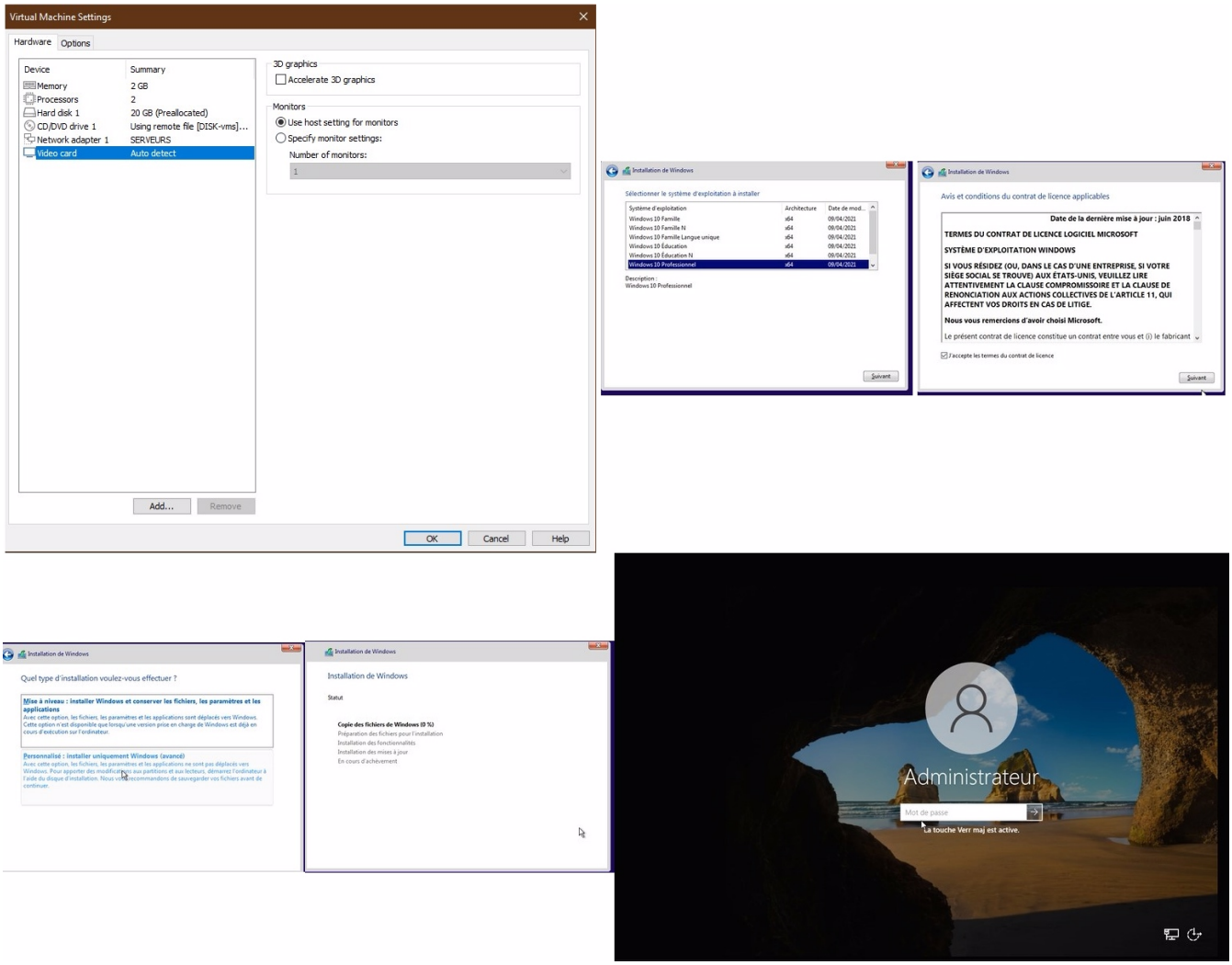

FIGURE 4.68 – Installation de kali linux

4.10 Analyse des résultats de la solution proposée

4.10.1 Test de ping

La figure 4.69 représente un test de connectivité vers internet après avoir autorisé le Trafic réseau.

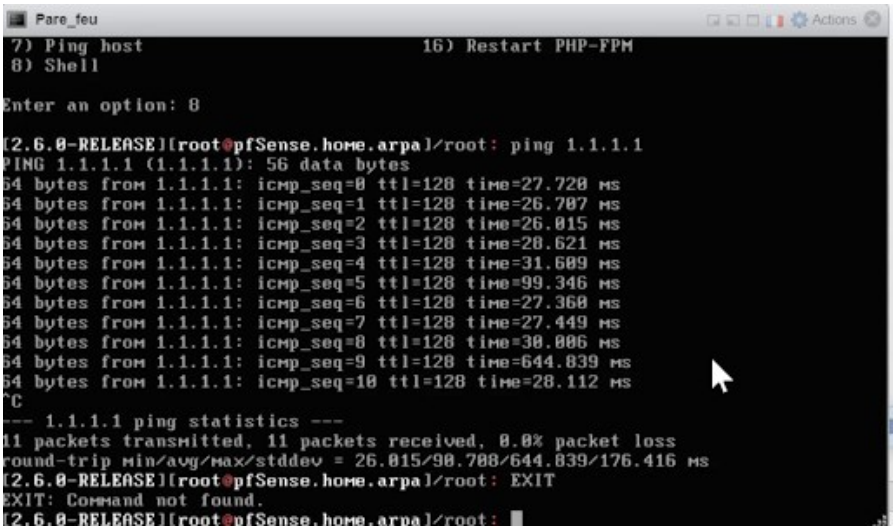

FIGURE 4.69 – Test de connectivité vers l'extérieur (internet)

La figure 4.70 représente :

✓ Un Test de connectivité Client vers le serveur AD

✓ Un Test de DNS

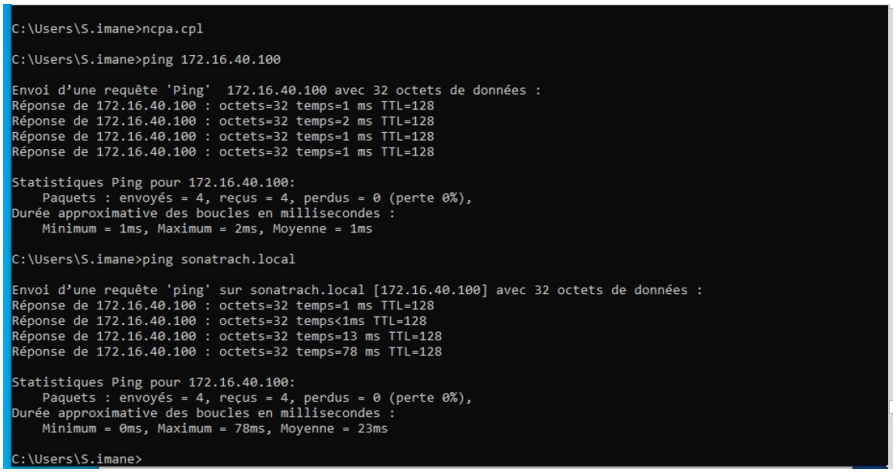

FIGURE 4.70 – Test connectivité Client vers serveur AD

La figure 4.71 représente : Après avoir effectué un test de ping vers le domaine Sonatrach. Local, une fenêtre s'affiche indiquant qu'il existe une connexion vers le domaine de serveur AD.

FIGURE 4.71 – Connexion vers le domaine de serveur AD

La figure 4.72 représente : Affichage de la connectivité vers le Client
La figure 4.72 représente : Affichage de la connectivité vers le Client

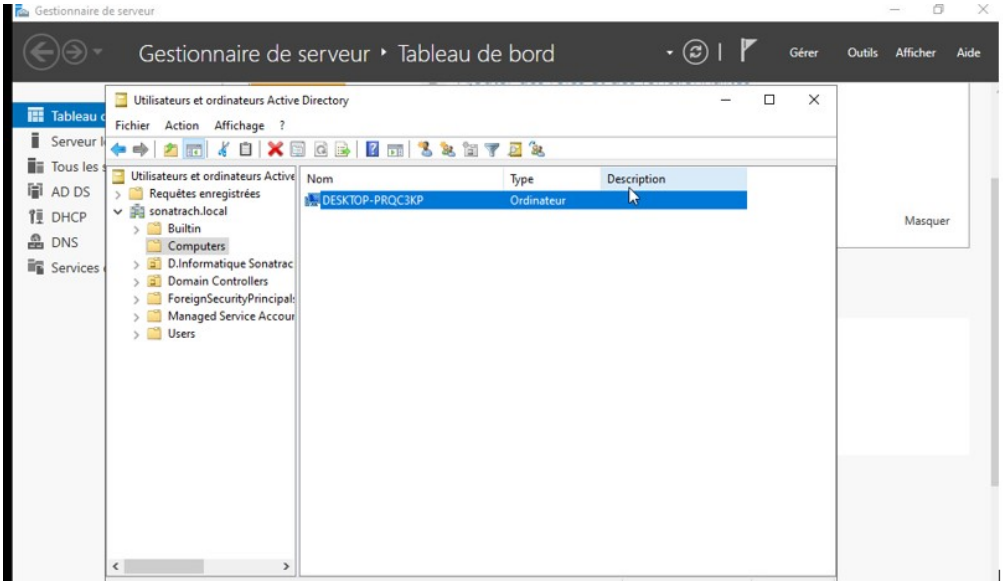

FIGURE 4.72 – Affichage de connectivité vers le Client

4.10.2 Test de détection d'intrusion

La figure 4.73 représente l'interface de Kali Linux.

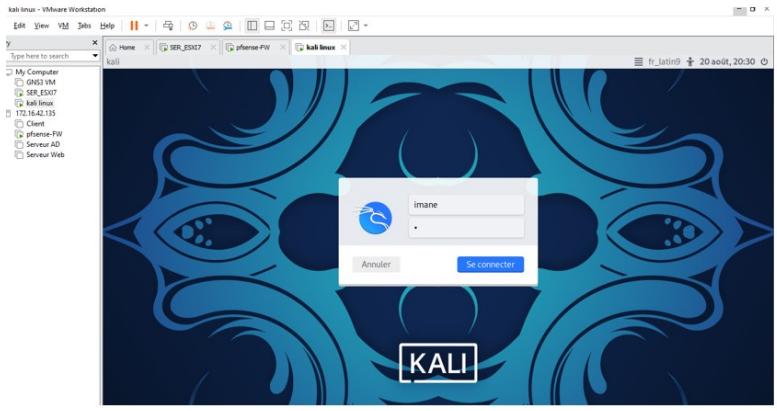

FIGURE 4.73 – L'interface de Kali Linux

Kali Linux demande une adresse 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 la Vmnet8) ce qui lui permet de communiquer avec le firewall.

La figure 4.74 représente la demande de connexion de Kali Linux vers le firewall

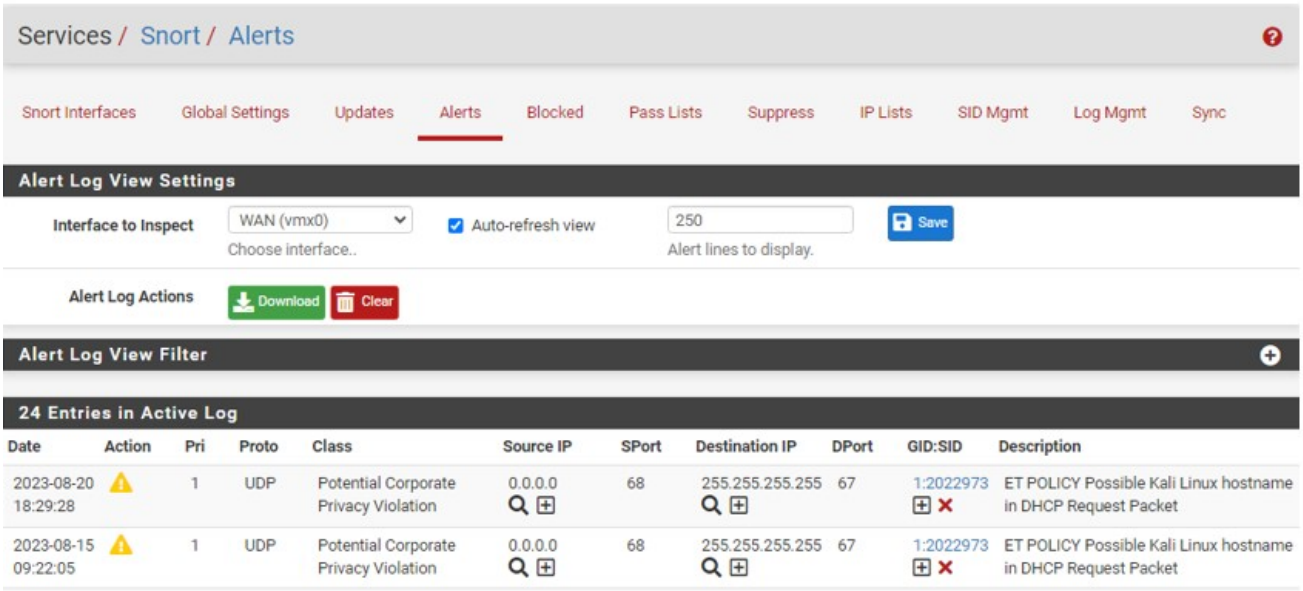

FIGURE 4.74 – La demande de connexion de Kali Linux vers le firewall

La f igure 4.75 représente un test de connectivité du Kali- Linux vers internet.

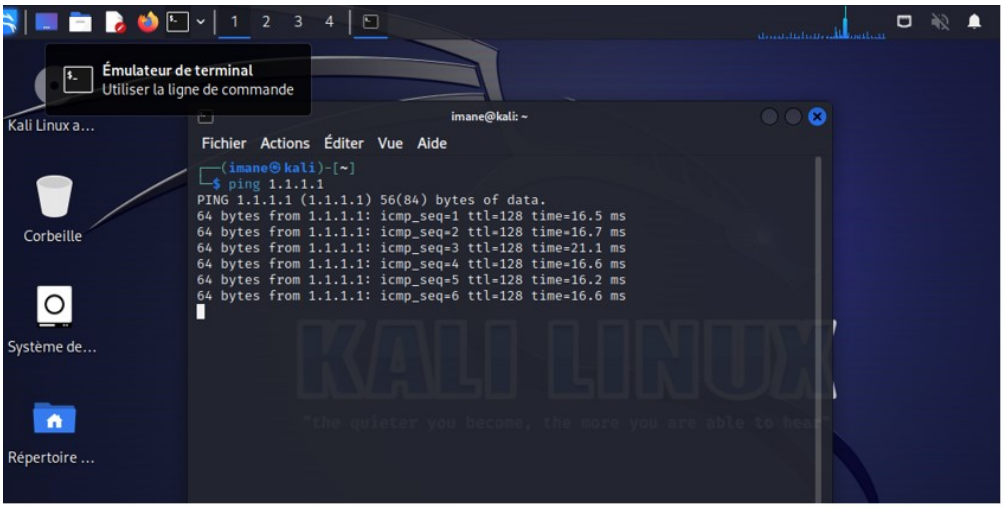

FIGURE 4.75 – Test de connectivité du Kali vers internet

La figure 4.76 illustre comment lancer un scan partir de la commande nmap.

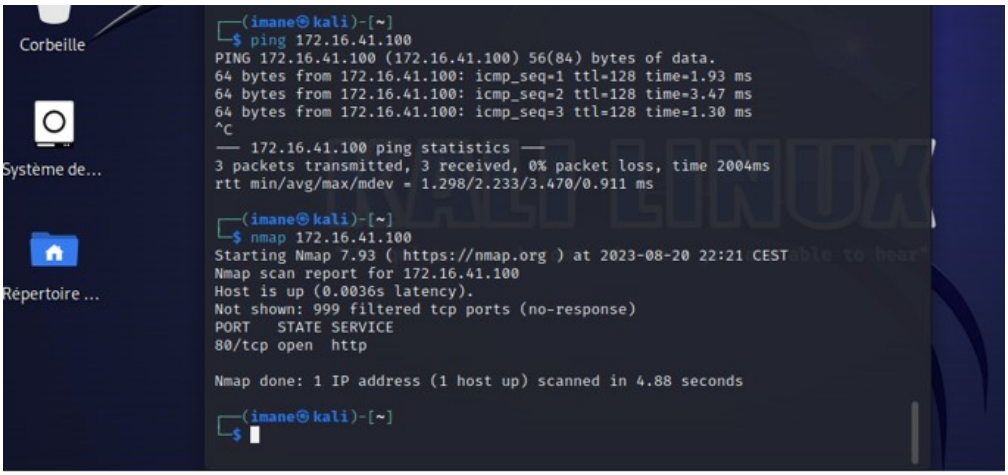

FIGURE 4.76 – Lancement de scan

Après l'attaque effectuée avec la machine Kali, le firewall reçoit les alertes.

La figure 4.77 représente les attaques effectuées.

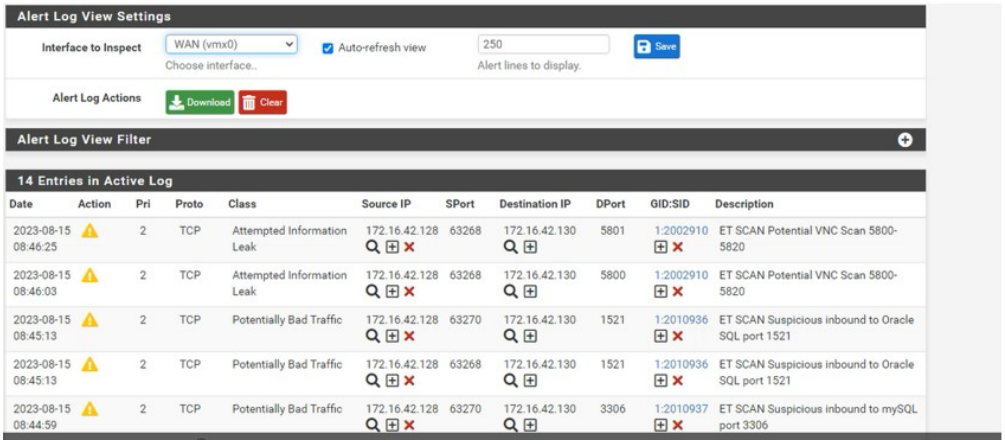

FIGURE 4.77 – Les attaques effectuées

Les attaques vont être détecté et bloquer par notre Snort.

La f igure 4.78 représente comment détecter une attaque.

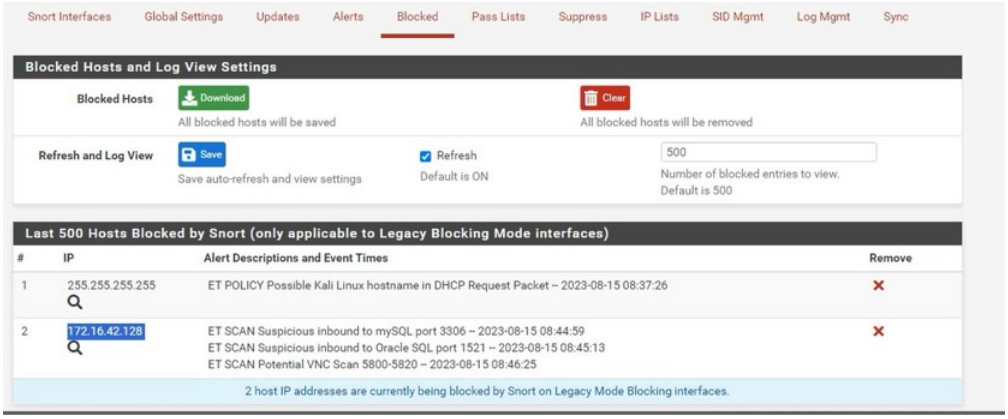

FIGURE 4.78 – La détection et blocage d'attaques

4.11 Conclusion

Dans ce chapitre, nous avons amélioré le réseau de Sonatrach pour le rendre plus sûr et plus à jour. Nous avons décrit les étapes suivies, ainsi que toutes les installations et configurations nécessaires pour mettre en place un système de prévention d'intrusion dans un firewall. Nous avons utilisé ESXi pour segmenter et surveiller le trafic réseau, et nous avons réalisé des tests à la fin du chapitre pour montrer le fonctionnement de Snort dans la détection des attaques

Bibliographie

[1]- Aissani, Djamil. “Cas d’entreprise Sonatrach Bejaia, Mémoire.” Université de Béjaia, 2019/2020.
https ://lamos.org/docs/Encadrement_Aissani_2019_Juillet.pdf

[2]- Red Hat, Inc. “Comprendre la virtualisation.” Consulté en Avril 2023.
https ://www.redhat.com/fr/topics/virtualization

[3]- appvizer. “Qu’est-ce que la virtualisation ?” Consulté en Mai 2023.
https ://www.appvizer.fr/magazine/services-informatiques/virtualisation/qu-est-ce-que-la-virtualisation

[4]- Free Work. “Technologies de virtualisation : l’essentiel à connaitre.” Consulté en Mars 2023.
https ://www.free-work.com/fr/tech-it/blog/actualites-informatiques/technologies-de-virtualisation-lessentiel-a-connaitre

[5]- Data Flair. “Software Virtualization – How it Works, Types, Advantages.” Consulté en Avril 2023.
https ://data-flair.training/blogs/software-virtualization/

[6]- Geeks for Geeks. “Characteristics of Virtualization.” Consulté en Mai 2023.
https ://www.geeksforgeeks.org/characteristics-of-virtualization

[7]- napsis. “Virtualisation et Cloud Computing, quelles différences ?” Consulté en Mai 2023.
https ://www.napsis.fr/cloud-lexique/virtualisation/

[8]- GLOBAL ENGEENERING. “Six types de virtualisation.”.
https ://global-engineering.ma/ ?p=1012

[9]- Citrix. “What is hardware virtualisation ?” Consulté le 28/04/2023.
https ://www.citrix.com/solutions/vdi-and-daas/what-is-hardware-virtualization

[10]- Red Hat. “Un hyperviseur, qu’est-ce que c’est ?” Consulté le 20/03/2023.
https ://www.redhat.com/fr/topics/virtualization/what-is-a-hypervisor

[11]- Server Watch. “What is Server Virtualization ? How It Works, Types, and Example.” Consulté le 2/08/2023.
https ://www.serverwatch.com/virtualization/server-virtualization/

[12]- SYSBLOG, ’La virtualisation du stockage’, URL :
https ://sysblog.informatique.univ-paris-diderot.fr/2020/03/13/$_{t}rashed-3/$

[13]- Wiki Ubuntu Fr, ’Virtualisation de systèmes d’exploitation’, URL :
http ://doc.ubuntu-fr.org/virtualisation Consulté le : 13 mai 2022

[14]- Wikipédia, ’Sécurité des systèmes d’information’, URL :
https ://fr.wikipedia.org/wiki/S

[15]-, ’Type d’attaques’, URL :
https ://www.academia.edu/15633432/Type$_{d}attaquesConsultle$: 13$juin$2022

[16]- A, CYBERUNIVERSITY, ’Attaques informatiques : Tout savoir sur les différentes menaces’, URL :
https ://www.cyberuniversity.com/ Consulté le : 5 avril 2022

[17]- SYloe, ’Firewall (pare-feu)’, URL :
https ://www.syloe.com/glossaire/firewall-pare-feu/ Consulté le : juin 2022

[18]- HUAWEI, ’c’est quoi une DMZ ?’, URL :
https ://forum.huawei.com/enterprise/fr/c-est-quoi-une-dmz/thread/1075341-100371 Consulté le : 10 mai 2023

[19]- JUNIPER NETWORKS, ’Qu’est-ce que la détection et la prévention d’intrusion (IDS/IPS) ?’, URL :
https ://www.juniper.net/fr/fr/research-topics/what-is-ids-ips.html Consulté le : 11 mars 2023

[20]- IBM, 'Réseaux locaux virtuels (VLAN)', URL :
https ://www.ibm.com/docs/fr/POWER8/p8hb1/p8hb1$_v ios_c oncepts_n etwork$
$_v lan.htmConsultle$: $5mars2020$

[21]- Techopedia, 'VMware Workstation', URL :
https ://www.techopedia.com/definition/25690/vmware-workstation Consulté le : juin 2018

[22] - Techtarget, 'ESXi (VMware)', URL :
https ://www.lemagit.fr/definition/ESXi-VMware
Consulté 2007-2023

[23] Kali Linux, URL :
https ://fr.wikipedia.org/wiki/Kali$_L inux, Consultle28juin$ 202307 :
23.

[24]- Wikipédia, *pfSense*, URL :
https ://fr.wikipedia.org/wiki/PfSense, Consulté le 16 février 2022 à 10 :00.

[25]- Wikipédia,Windows Server 2022, URL :
{https ://fr.wikipedia.org/wiki/Windows$_S erver_2$022, $Consultle2juin202314$:
29.

[26]- Wikipédia, Snort, URL :
https ://fr.wikipedia.org/wiki/Snort, Consulté le 19 février 2023 à 19 :25.

[27]- https ://www.weodeo.com/wp-content/uploads/2022/02/architecture-virtuelle.png

[28]https ://techvidvan.com/tutorials/wp-content/uploads/sites/2/2021/10/cloud-computing-software-virtualization.webp

[29]- https ://qph.cf2.quoracdn.net/main-qimg-cabc4e29cca70b9592eb3edbc3ec559a.webp

[30]- https ://i1.wp.com/ipwithease.com/wp-content/uploads/2019/12/Full-virtualization-vs-Para-virtualization-vs-Hardware-assisted-virtualization.jpg ?resize=700 2C451ssl=1

[31]-https ://linuxhaiti.files.wordpress.com/2020/01/3aad9-virtualisation os.jpg

[32]-https ://www.researchgate.net/publication/280095977 /figure/fig13/AS :667718931980288@1536208007331/Application-virtualization.png

[33]- https ://www.researchgate.net/publication/339749891/figure/fig6/AS : 866155510108161@1583518974393/Storage-Virtualization-Architecture.jpg

[34]- https ://www.virtualhome.blog/wpcontent/uploads/2019/12/vmware-workstation*logo.png*

[35]- https ://images.techhive.com/images/article/2016/02/kali-linux-logo-100645937-orig.jpg ?auto=webpquality=85,70

[36]-https ://www.datasecuritybreach.fr/wp-content/uploads/2014/02/Snort.gif

[37]- https ://www.frameip.com/wp-content/uploads/firewall-attaque-outils-defenses-piratage-vpn.jpg

[38]-https ://www.ionos.fr/digitalguide/fileadmin/DigitalGuide/Screenshots/dmz-network-diagram-2.png

Résumé

Le mémoire de fin d'études porte sur « Etude et mise en place d'une politique de sécurité sur une infrastructure de virtualisation ». L'entreprise Sonatrach de Bejaia a été confrontée à des problèmes de sécurité liés à son infrastructure informatique. Pour résoudre ces problèmes, nous avons choisi d'utiliser l'hyperviseur de type 1, VMware ESXi. Au sein de cet environnement, nous avons intégré un pare-feu pour segmenter le réseau et limiter l'accès non autorisé aux données et aux ressources de l'entreprise. Nous avons recommandé l'ajout d'un système de détection d'intrusion (IDS) intégré au pare-feu pour surveiller le trafic réseau et repérer les activités suspectes. Cette approche détaillée a permis de mettre en avant les aspects de sécurité de manière approfondie et de proposer des solutions appropriées pour garantir la protection de l'infrastructure de virtualisation de l'entreprise..

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

Abstract

The end-of-studies dissertation focuses on ""Study and implementation of a security policy on a virtualization infrastructure"". The Sonatrach company in Bejaia has faced security problems related to its IT infrastructure. To solve these problems, we chose to use the type 1 hypervisor, VMware ESXi. Within this environment, we have integrated a firewall to segment the network and limit unauthorized access to corporate data and resources. We recommended adding an intrusion detection system (IDS) built into the firewall to monitor network traffic and spot suspicious activity. This detailed approach made it possible to highlight security aspects in depth and to propose appropriate solutions to guarantee the protection of the company's virtualization infrastructure.

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