République Algérienne Démocratique et Populaire ministère de
l'Enseignement supérieur et de la recherche scientifique

UNIVERSITEM'HAMEDBOUGARA-BOUMERDES

Faculté de Technologie

Mémoire de Fin d'études Master

Réalisé par :

Mouhammou Aya

Boudissa Rofaida

Filière : Télécommunications

Option : Réseaux et télécommunications

Thème :

Conception et déploiement d'une architecture réseau à base de pfsense

Devant le jury :

Mme	**Sedjelmaci**	**Ibticeme**	**MCB**	**UMBB**	**Président**
Mme	**Haroun**	**Radia**	**MAA**	**UMBB**	**Examinateur**
Mme	**MECHID**	**Samira**	**MAA**	**UMBB**	**Rapporteur**

Année Universitaire : 2023/2024

Remerciements

En préambule à ce mémoire, nous exprimons nos sincères remerciements à **ALLAH** pour Nous avoir guidés, soutenus et accordé la patience et le courage nécessaires tout au long de Nos années d'études.

Nous tenons à remercier notre promotrice **Mme Samira MECHID**, pour son encadrement Précieux et son soutien constant tout au long de ce projet. Ses conseils éclairés et sa Disponibilité ont joué un rôle essentiel dans la qualité de notre travail.

Nous tenons aussi à adresser nos sincères remerciements à nos encadreurs **Mr Abdenour HAMDI** pour nous avoir donné l'occasion de travailler sur un Projet aussi excitant et nous avoir fait découvrir le monde du travail.

Nous désirons aussi remercier **Mr Nassim CHABANE** pour nous avoir orientés, aidés, et conseillés.

Un grand merci au chef de département **Mr. Noureddine Messaoudi** et toute l'équipe pédagogique du département de génie électrique.

Nos remerciements s'adressent également aux membres du jury, qui ont consacré leur temps Et leur expertise pour évaluer notre mémoire.

Enfin, nous exprimons notre gratitude envers toutes les personnes qui, de près ou de loin, Nous avons constamment soutenu et encouragés tout au long de ce parcours.

Veuillez accepter nos plus sincères remerciements

merci

Dédicace

Je dédie ce projet

A ma chère mère, Louli Naima,

A mon cher père, Boudissa Slimane,

Qui n'ont jamais cessé, de formuler des prières à mon égard, de me soutenir et de m'épauler pour que je puisse atteindre mes objectifs. Quoi que je fasse ou que je dise, je ne saurai point te remercier comme il se doit.

A mes frères, Ycaine et Ayoub

A mes chères sœur, kaouthar et Aya

Pour ses soutiens moraux et leurs encouragements et attentions. Ils m'ont permis de réaliser que la famille est sacrée. Je vous aime

A mon cher mari Sofian,

Tu as toujours été à mes côtés pour me soutenir et m'encourager.

A ma chère binôme, Mouhammou Aya,

Pour son entente et sa sympathie et sa patience infinie.

A ma chère amie, Meriem,

Qui m'a aidé et supporté dans les moments difficiles.

A toute ma famille,

A tous mes autres amies,

A tous ceux que j'aime et ceux qui m'aiment.

BoudissaRofaida

Dédicace

Tout d'abord je tiens à remercier ALLAH le tout puissant, qui nous a donné la force la patience d'accomplir ce travail.

À celle qui m'a appris mes premières lettres pour que je me tiens ici, à mon paradis, à la prunelle de mes yeux et la source de ma joie et mon bonheur, ma moitié

Maman Rezzoug Zahia.

À celui à qui je parle des étoiles, il m'apportera la lune, ma source de vie et d'amour, à mon support et mon inspirant, mon héro Papa Mouhammou Smail.

À mon puits de secret, ma source d'énergie mes deux adorable sœurs Haoua, Lyna, Maya, Meriem, Neila, Lylia, Amira, Amel, Yamina, Sara, Chaima, Asmaa, Yesmine merci d'avoir été toujours là pour moi.

À mes frères et ma chère sœur Athmane, Chammesseddine etTakoua mes piliers inébranlables, mes compagnons de vie et mes meilleurs amis. À tous les membres de ma grande famille pour leurs prières et encouragements.

A toute ma famille mes chers grands-parents, mes oncles, mes tantines et mes cousins

À ma promotrices Mme MECHID Samira pour sa guidance précieuse et son soutien constant.

À Mr CHABANE Nassim pour son soutien, encouragement et orientation

À mes précieuses amies merci d'avoir toujours été là pour moi, à travers les hauts et les bas, à partager les rires et les larmes.

Sans oublier mon meilleur binôme Rofaida, qui a toujours su me comprendre, m'écouter et me soutenir, avec qui j'ai créé des souvenirs inoubliables.

Je suis profondément reconnaissante envers tous ceux qui ont contribué à ma réussite et qui m'entourent avec amour.

Mouhammou Aya

Table des matières

ملخص

أصبح تعزيز أمن الكمبيوتر ضرورة أساسية نظرا لظهور أشكال مختلفة من هجمات الكمبيوتر اليوم. وشبكات الشركات والمؤسسات والحكومات هي التي تحتاج إلى هذا الأمن أكثر من غيرها لأنها تكون في كثير من الأحيان أهدافًا لهجمات التطفل. تشكل جدران الحماية خط الدفاع الأول لنظام المعلومات ضد التهديدات.

تشكل جدران الحماية خط الدفاع الأول لنظام المعلومات ضد التهديدات السيبرانية. يقومون بتصفية حركة المرور الواردة والصادرة، ومنع الوصول غير المصرح به وحماية الأصول الرقمية.

الهدف من هذا العمل هو تنفيذ جدار حماية مفتوح المصدر من التدخلات الخارجية pfsense"كحل لحماية شبكة LAN" ومنع تسرب بعض المعلومات إلى الخارج.

الكلمات المفتاحية: جدار الحماية، تصفية الحزمة التكوينات,pfSens captive portail .

Résumé

Le renforcement de la sécurité informatique est devenu une nécessité primordiale vu l'apparition des diverses formes d'attaques informatiques de nos jours, ce sont les réseaux d'entreprises, d'institutions, de gouvernements qui ont le plus besoin de cette sécurisation car elles sont fréquemment les cibles des attaques d'intrusion. Les firewalls constituent la première ligne de défense du système d'information contre les menaces, et la première ligne de défense du système d'information contre les cybermenaces. Ils filtrent le trafic entrant et sortant, bloquant les accès non autorisés et protégeant les ressources numériques.

L'objectif de ce travail est la mise en place d'un firewall open source, pfsense comme solution, pour protéger le réseau LAN des intrusions extérieure et empêché la fuite de certaines informations en externe.

Mots-clés : Firewall, pfSense, filtrage des paquets, configuration, portail captif.

Abstract

The need to strengthen security has become an essential necessity, given the emergence the emergence of various forms of computer attack these days, it is the networks of corporate, institutional and government networks are the ones most in need of need this security, as they are frequently the targets of intrusion attacks. attacks. Firewalls are the information system's first line of defense against threats. against threats, and the first line of defense for the information system against cyberthreats. They filter incoming and outgoing traffic blocking

unauthorized access and protecting digital resources. resources.

The objectives of this project is to implement an open source firewall, with pfsense as the solution, to protect the LAN network from external intrusions and prevent the external leakage of certain information.

Keywords: Firewall, pfSense, packet filtering, configuration, captive portail.

Liste des Figures

CHAPITRE I : Généralités sur les réseaux informatiques

CHAPITRE II : La sécurité réseau

CHAPITRE III : Conception et réalisation

Listes des tableaux

CHAPITRE III : Conception et réalisation

Listes des Abréviations

ACL : Access Control List.

AES: Advanced Encryption Standard.

DES: Data Encryption Standard.

DNS: Domain Name System.

DOS: Denial of Service.

DDoS: Distributed Denial of Service.

FTP: File Transfer Protocol.

HTTP: Hypertext Transfer Protocol

IP: Internet Protocol.

IPSEC: Internet Protocol Security.

LACP: Link Aggregation Control Protocol

LAN: Local Area Network

NAT: Network Address Translation

NGFW: Next-Generation Firewall.

NIC: Network Interface Card

OSI: Open Systems Interconnection.

RPC: Remote Procedure Call.

RSA: Rivest Shamir Adleman.

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol.

SSH: Secure Shell

SSL: Secure Sockets Layer.

STP: Spanning Tree Protocol

TCP: Transmission Control Protocol.

TCP/IP: Transmission Control Protocol/Internet Protocol.

VLAN: Virtual LAN

VPC: Virtual Port Channels

VPN: Virtual Private Network

WAN: Wide Area Network

Introduction générale

Les réseaux informatiques sont devenus essentiels à la bonne marche des entreprises. La croissance accélérée de ces réseaux qui sont de plus en plus ouverts sur internet, et à priori bénéfique, mais pose néanmoins un problème important de sécurité. En effet il en résulte un nombre croissant d'attaques qui peuvent engendrer un dysfonctionnement technique et des pertes financières menaçant l'intégrité, la confidentialité et la disponibilité du système d'information.

Les données sensibles du système d'information de l'entreprise sont donc exposées à des actes de malveillance. Les prédateurs et les intrus s'attaquent aux équipements essentiellement par le biais d'accès aux réseaux reliant l'entreprise à l'extérieur. Face à ces menaces les entreprises sont menées à effectuer un audit de sécurité informatique reposant sur une politique de sécurité claire et fiable.

La sécurité d'une entreprise est fondée avant tout sur une gestion des risques décrivant les ressources critiques de l'entreprise, ses objectifs de sécurité, ses vulnérabilités, les probabilités d'occurrence de menaces sur ses ressources vitales, ainsi que leurs impacts sur l'entreprise.

La solution adéquate pour limiter et restreindre cet accès consiste à déployer notre architecture réseau a base du firewall pfsense. Ce firewall est une distribution personnalisée open source gratuite de FreeBSD conçue pour être utilisée comme pare-feu et routeur entièrement gérée par une interface Web facile à utiliser. Le système de progiciel pfSense permet une extensibilité supplémentaire sans ajouter de surcharge ni de vulnérabilités de sécurité potentielles à la distribution de base, allant de la protection d'un seul ordinateur dans de petits réseaux domestiques à des milliers de périphériques réseau dans de grandes entreprises, universités et autres organisations.

Ce travail a été réalisé au sein de la division EXPLORATION SONATRACH dans le but de sécuriser un réseau LAN, composé de plusieurs équipements.

Afin de cerner convenablement notre sujet, l'approche suivante est adoptée :

- Le premier chapitre est consacré aux généralités sur le réseau informatique.
- Le second chapitre quant à lui est dévoilé à la sécurité informatique et quelques définitions théoriques des différentes attaques les plus connues, une présentation de l'audit et ses différents objectifs, ainsi que ces différentes méthodes.

- Le troisième chapitre, représente-la présentation d'EXPLORATION SONATRACH. Ensuite, nous parlerons d'une solution d'amélioration de la sécurité informatique de l'architecture existante, en décrivant les différents équipements de sécurité nécessaires.

Nous terminons notre mémoire par une conclusion générale et quelques perspectives pour des futurs travaux.

Chapitre I :
Généralités sur les réseaux informatiques

I Introduction

Dans l'ère numérique actuelle, les réseaux informatiques sont les artères vitales qui alimentent la circulation incessante des données à travers le monde. Que ce soit pour envoyer un simple courriel, diffuser un film en streaming, ou coordonner des opérations bancaires à l'échelle mondiale, les réseaux informatiques sont omniprésents, et leur importance ne cesse de croître.
Dans ce chapitre, nous plongerons dans les profondeurs de cet univers fascinant. Nous explorerons les fondements théoriques des réseaux, leurs différentes architectures, les protocoles qui régissent leurs communications.

I.1 Définition d'un réseau informatique

Un réseau informatique est un ensemble de dispositifs interconnectés qui échangent des données et des ressources, tels que des fichiers, des imprimantes, ou des applications. Ces dispositifs peuvent être des ordinateurs, des serveurs, des routeurs, des commutateurs, des périphériques mobiles, etc. Les réseaux informatiques permettent la communication et la collaboration entre les utilisateurs, le partage de ressources, ainsi que l'accès à des services et des informations à distance. Ils peuvent être de taille variable, allant des réseaux locaux (LAN) dans une maison ou un bureau, aux vastes réseaux mondiaux tels qu'Internet.

I.2 Types de réseaux informatiques

Les réseaux informatiques se déclinent en une multitude de formes et de tailles, chacune adaptée à des besoins spécifiques. Des réseaux locaux permettant le partage de ressources au sein d'un foyer ou d'une entreprise (réseau LAN), aux vastes infrastructures mondiales interconnectées comme Internet (WAN), la diversité des types de réseaux reflète la diversité des besoins et des usages dans notre monde numérique en constante évolution.

I.2.1 Réseau local LAN

Un réseau LAN, ou Local Area Network, est une infrastructure informatique interconnectant un ensemble de dispositifs informatiques situés dans une zone géographique limitée, telle qu'un bâtiment, un bureau, ou un campus. Il permet aux utilisateurs de partager des ressources telles que des fichiers et des applications, ainsi que de communiquer entre eux via des protocoles de communication définis. Les réseaux LAN sont généralement caractérisés par des débits élevés et des latences faibles, offrant une connectivité rapide et fiable aux utilisateurs locaux. Ils peuvent être déployés à l'aide de diverses technologies de transmission de données, notamment des câbles Ethernet, des commutateurs réseau, et des équipements

sans fil tels que des points d'accès Wi-Fi. Les réseaux LAN sont largement utilisés dans les environnements professionnels pour faciliter la collaboration, le partage de ressources, et l'accès aux services internes.

I.2.2 Réseau étendu (WAN)

Un réseau WAN, ou Wide Area Network, est un type de réseau informatique qui couvre une zone géographique étendue. Contrairement aux réseaux LAN, les réseaux WAN interconnectent des sites distants situés dans différentes régions géographiques.

Les réseaux WAN utilisent une variété de technologies de transmission de données pour permettre la communication entre les sites distants, notamment les liaisons louées, les réseaux à commutation de paquets (comme Internet), les réseaux privés virtuels (VPN) et les connexions par satellite. Ces technologies permettent aux données de voyager sur de longues distances, souvent à travers des réseaux publics ou privés, tout en offrant des débits de transmission élevés et une faible latence.

I.3 Architectures et Caractéristiques des réseaux informatiques

Pour qu'un réseau informatique soit efficace et répondre aux besoins des utilisateurs, il doit satisfaire à plusieurs critères essentiels :

- **Architecture :** La conception du réseau doit être pensée pour répondre aux besoins spécifiques de l'organisation, en tenant compte de la topologie, de la structure et de la hiérarchie des équipements et des protocoles.
- **Speed :** Le réseau doit offrir des performances optimales en termes de vitesse de transmission des données, garantissant ainsi une communication rapide et fluide entre les utilisateurs et les ressources du réseau.
- **Fiabilité :** Le réseau doit fonctionner de manière cohérente et sans interruption pour éviter les temps d'arrêt et les pertes de données, assurant ainsi la continuité des opérations.
- **Disponibilité :** Les utilisateurs doivent pouvoir accéder aux ressources et aux services du réseau à tout moment, quel que soit l'endroit où ils se trouvent, assurant ainsi une connectivité constante.
- **Sécurité :** Le réseau doit protéger les données sensibles contre les accès non autorisés, les attaques malveillantes et les violations de la confidentialité, assurant ainsi l'intégrité et la confidentialité des informations.

- **Coût :** Le coût de mise en place, d'exploitation et de maintenance du réseau doit être raisonnable et justifiable par rapport aux avantages et aux fonctionnalités offerts, assurant ainsi une utilisation efficiente des ressources financières de l'organisation.

On peut ainsi diviser les architectures en deux catégories principales :

I.3.1 Architecture physique

Implique la disposition physique des équipements réseau, tels que les routeurs, les commutateurs et les câbles, pour créer une infrastructure physique. Cette catégorie comprend différents types d'architectures physiques telles que les topologies en étoile, en bus, en anneau, en arbre, etc. Nous allons particulièrement nous concentrer sur la topologie en arbre dans notre mémoire.

Topologie Arbre

Une topologie en arbre, également appelée topologie arborescente ou hiérarchique, peut être conceptualisée comme une assemblée de réseaux en étoile disposés en différentes strates. Ce schéma réseau est organisé selon une hiérarchie de niveaux, où le niveau supérieur est connecté à plusieurs nœuds de niveau inférieur. Ces derniers peuvent, à leur tour, être reliés à plusieurs autres nœuds de niveau inférieur, créant ainsi une structure pyramidale, comme montre la figure suivante :

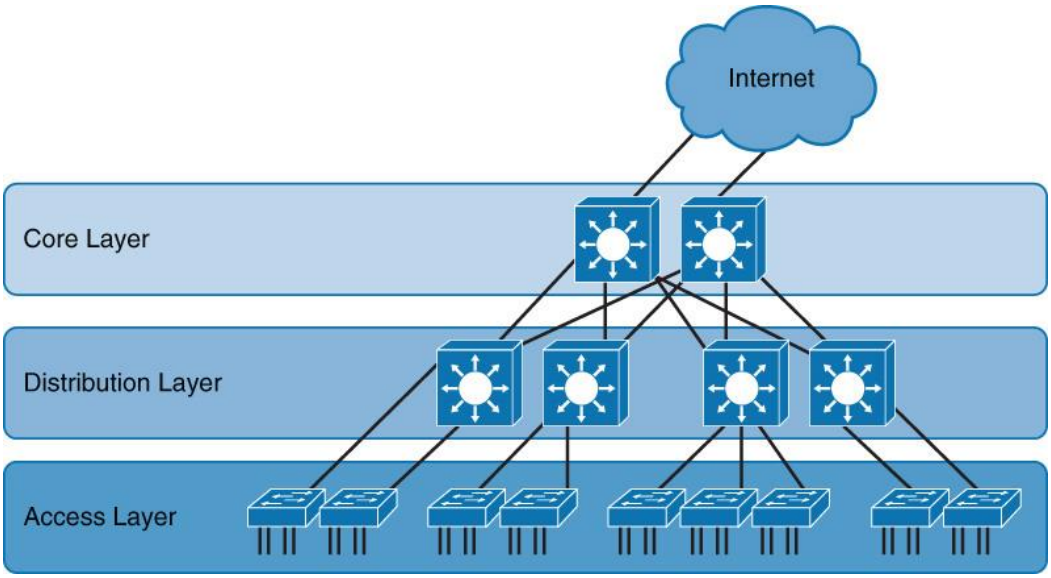

Figure I. 1 Topologie en arbre

Dans cette optique, la conception et la mise en place d'une infrastructure solide et performante se révèlent cruciales pour répondre aux exigences croissantes en matière de

connectivité, de sécurité et de disponibilité. Pour atteindre ces objectifs, les entreprises font souvent appel à des modèles de conception éprouvés, comme le modèle en trois couches comme le montre la figure ci-dessus, qui permet de structurer efficacement les réseaux en fonction de leurs besoins spécifiques.

- Couche Core (Noyau) : Au cœur du réseau, la couche Core assure le transport rapide et fiable des données à travers l'ensemble du réseau d'entreprise. Elle est conçue pour offrir une connectivité haut débit entre les différents sites et réseaux distants, minimisant les temps de latence et fournissant une bande passante élevée pour répondre aux besoins de l'entreprise. La couche Core est hautement disponible, redondante et sécurisée. Dans notre déploiement, nous avons mis en place deux firewalls PFsense en haute disponibilité (HA) pour renforcer la sécurité et la résilience du réseau, assurant ainsi une continuité opérationnelle en cas de défaillance matérielle ou logicielle.
- Couche Distribution : La couche Distribution agit comme une couche d'agrégation entre la couche Core et la couche Access. Dans ce projet, nous avons divisé la couche Distribution en deux parties : les switchs TOR (Top of Rack) et les switchs de Distribution. Les switchs TOR fournissent une connectivité aux équipements d'accès situés dans les racks de serveurs, tandis que les switchs de Distribution agrègent le trafic de plusieurs switchs TOR et assurent la connectivité entre les différents segments du réseau.
- Couche Access (Accès) : En bas du modèle en trois couches, la couche Access fournit la connectivité entre les périphériques finaux, tels que les ordinateurs, les imprimantes et les téléphones IP, et le reste du réseau. La couche Access offre des services tels que la commutation, le VLAN, et la gestion des adresses IP pour permettre aux utilisateurs finaux d'accéder aux ressources réseau de manière sécurisée et efficace. La couche Access est mise en œuvre à l'aide de commutateurs Ethernet, de points d'accès sans fil et d'autres périphériques d'accès réseau. [1]

I.3.2 Architecture logique

Implique la manière dont les données circulent à travers le réseau, définissant les protocoles, les adresses IP et les schémas de routage pour organiser la communication entre les dispositifs. Parmi les éléments clés de l'architecture logique on site les protocoles vPC, etherchannel, NAT, STP, DHCP, DNS, les VLAN et les port Access et trunk.

I.3.2.1 **Protocol VPC (Virtual Port Channels)**

Un canal de port virtuel (VPC) permet aux liens physiquement connectés à deux périphériques Cisco Nexus 7000 ou 9000 différents d'apparaître comme un canal de port unique par un troisième périphérique. Le troisième périphérique peut être un commutateur, un serveur ou tout autre périphérique réseau prenant en charge les canaux de port. Une VPC peut fournir un multi acheminement de couche 2, ce qui vous permet de créer une redondance et d'augmenter la bande passante bissectionnelle en activant plusieurs chemins parallèles entre les nœuds et en autorisant l'équilibrage de charge du trafic. Vous pouvez utiliser uniquement les canaux de port de couche 2 dans le VPC. Vous configurez les canaux de port à l'aide de LACP ou d'une configuration statique sans protocole. [2]

La figure suivante présente la topologie physique et logique du VPC

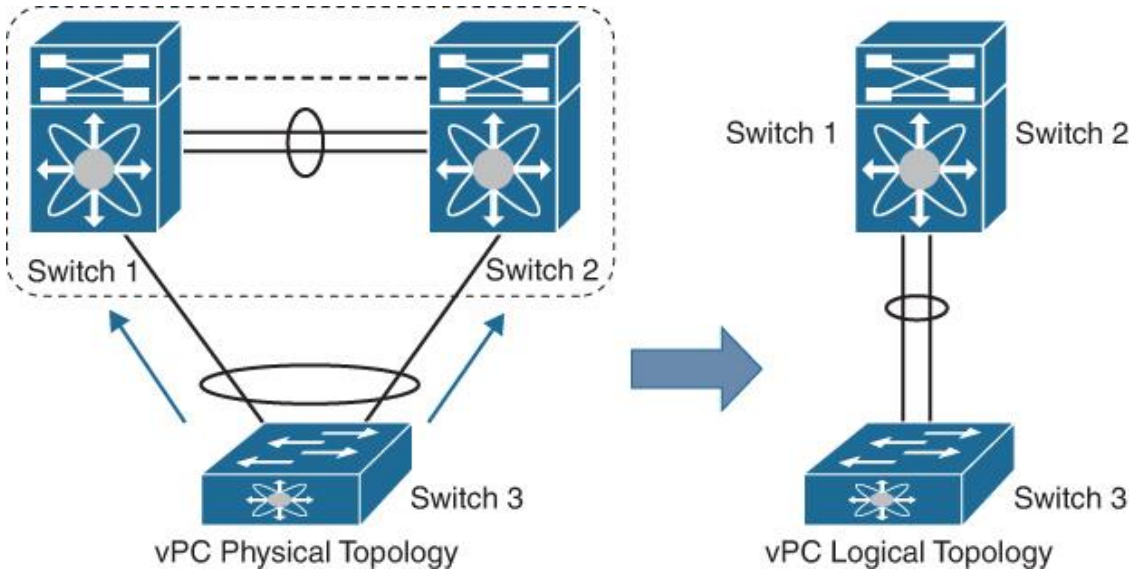

Figure I. *2*: Topologie physique et logique du VPC

Composants VPC

- VPC Domain : C'est le domaine global qui englobe les équipements et Ports sur lesquels on monte le VPC, il se caractérise par un identifiant unique dans le DC.
- VPC Peer switches : Les deux switches qui contiennent le VPC. Un équipement est élu Primary et l'autre est Secondary.

- VPC peer-link : c'est le lien Port-Channel (2 x 10G) qui sert à la synchronisation entre les 2 VPC peers (Identification des Rôles, Flux de multicast et de broadcast, synchro des MACs, HSRP, OSPF …).
- VPC peer-keepalivelink : c'est un lien à part qu'il permet de superviser périodiquement l'état d'une VPC peer (Joignable UP ou non). Il est fortement recommandé qu'il soit dans un Réseau Out-of-Band Management. Aucun trafic DATA ne circule à travers ce lien.
- VPC : c'est le lien Port Channel entre les VPC peers et les autres équipements (Switches, Serveurs...). [3]

La figure suivante présente les composants du VPC

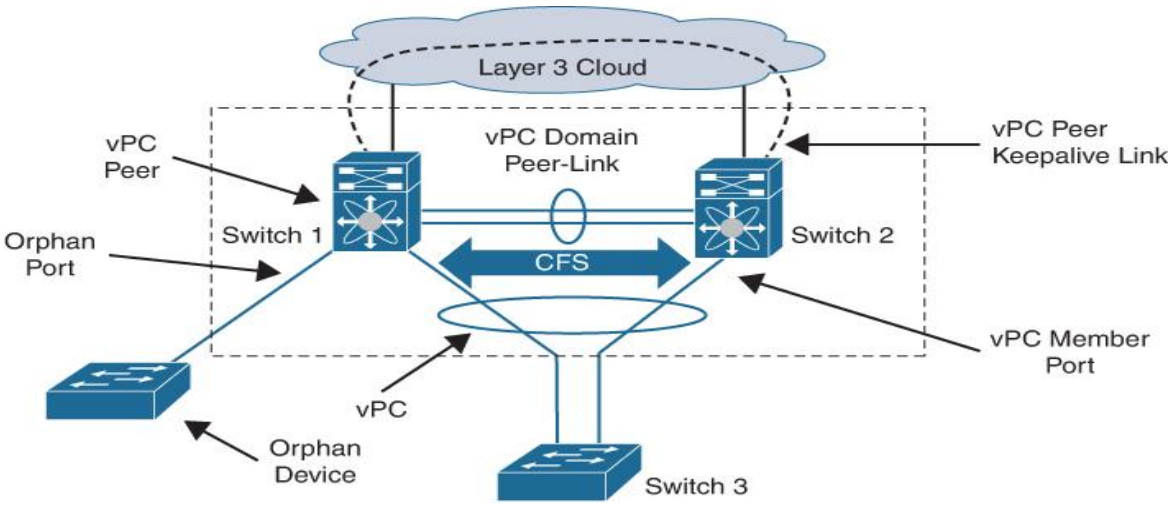

Figure I. *3*: Composants VPC

I.3.2.2 Protocol EtherChannel

Ethernet Port Channels regroupe les liaisons physiques dans un groupe de canaux pour créer une liaison logique unique qui fournit la bande passante globale de 32 liaisons physiques maximum. Ethernet Port Channels relie logiquement plusieurs connexions physiques en une seule connexion logique. La canalisation des ports équilibre également la charge du trafic sur ces interfaces physiques.

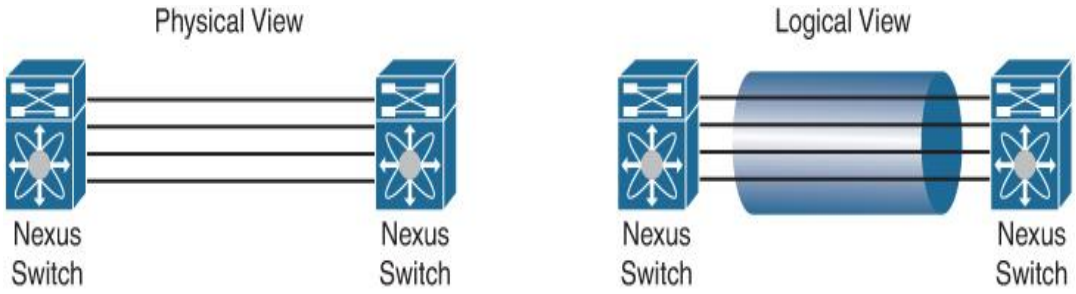

Figure I. *4*: Vues physiques et logiques de l'Ethernet Port Channels

I.3.2.3 Réseau local virtuel VLAN et Routage inter-VLAN

I.3.2.3.1 Réseau local virtuel VLAN

Un VLAN (Virtual Local Area Network ou réseau local virtuel) est un réseau local virtuel qui permet de regrouper plusieurs dispositifs informatiques de manière logique, indépendamment de leur emplacement physique. En d'autres termes, il s'agit de créer des réseaux distincts au sein d'un même réseau physique, facilitant ainsi la gestion, la sécurité et les performances.

Pourquoi utiliser des VLANs ?

Il existe plusieurs raisons pour lesquelles les VLANs sont utilisés :

- Séparation logique :

Les VLANs permettent de séparer les appareils selon leurs fonctions ou départements, même s'ils sont physiquement connectés au même réseau.

- Sécurité :

En isolant les différents départements ou groupes d'utilisateurs, on réduit le risque d'accès non autorisé aux données sensibles et on facilite la mise en place de politiques de sécurité spécifiques pour chaque VLAN.

- Amélioration des performances :

La création de VLANs réduit la congestion du réseau en limitant la diffusion des paquets de données aux seuls appareils concernés. Cela permet d'optimiser les performances du réseau.

- Gestion simplifiée :

Les VLANs simplifient la gestion du réseau en réduisant le nombre de commutateurs physiques nécessaires. Il est également plus facile de déployer et de modifier les

configurations de réseau, comme montre la figure suivante.

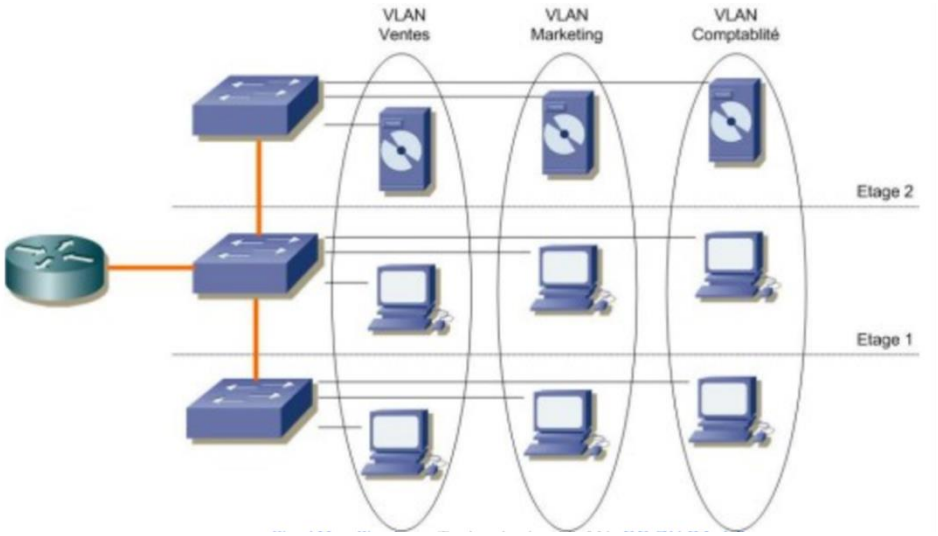

Figure I. 5L'utilisation des VLAN's

I.3.2.3.2 Routage inter-vlan

Le routage inter-VLAN est effectué en connectant différentes interfaces physiques du routeur sur différentes interfaces physiques du commutateur. Les ports du commutateur connectés au routeur ne sont pas en mode trunk mais en mode accès (*access*), chaque interface physique est assignée à un VLAN différent.

Cette méthode requiert autant d'interfaces physiques que vous avez de VLANs, ce qui peut vite devenir gênant. Cette méthode est certainement très peu utilisée et n'est plus implémentée. [4]

I.3.2.4 Types de ports

Les VLANs (réseaux locaux virtuels) permettent de diviser un réseau physique en plusieurs réseaux logiques distincts. Pour que les données circulent correctement entre ces réseaux virtuels, les commutateurs (switches) doivent être configurés avec des réglages spécifiques. Il y a deux types de configurations principales : port Access et port Trunk.

I.3.2.4.1 Port access

Le réglage “Access” est utilisé pour connecter des appareils individuels, tels que des ordinateurs ou des imprimantes, à un VLAN spécifique. Pensez à un bureau où chaque employé est connecté à son propre réseau de département

I.3.2.4.2 Prot trunk

Le réglage “Trunk”, en revanche, est utilisé pour connecter des commutateurs entre eux et permettre la communication entre différents VLANs. Imaginons un immeuble de bureaux avec plusieurs étages, chacun ayant son propre réseau local. Pour permettre aux employés de communiquer entre les étages, il est nécessaire d’établir une connexion entre les réseaux locaux de chaque étage. [5]

I.3.2.5 Protocol de translation d’adresse IP NAT

NAT (Network Address Translation) est un processus de modification des adresses IP et des ports source et de destination. La traduction d'adresses réduit le besoin d'adresses publiques IPv4 et masque les plages d'adresses réseau privées. Le processus est généralement effectué par des routeurs ou des pares-feux.

NAT permet à un seul appareil, tel qu'un routeur, d'agir comme un agent entre Internet (ou réseau public) et un réseau local (ou réseau privé), ce qui signifie qu'une seule adresse IP unique est requise pour représenter un groupe entier d'ordinateurs à quoi que ce soit en dehors de leur réseau. [6]

La figure I.7 présente Network adresse translation.

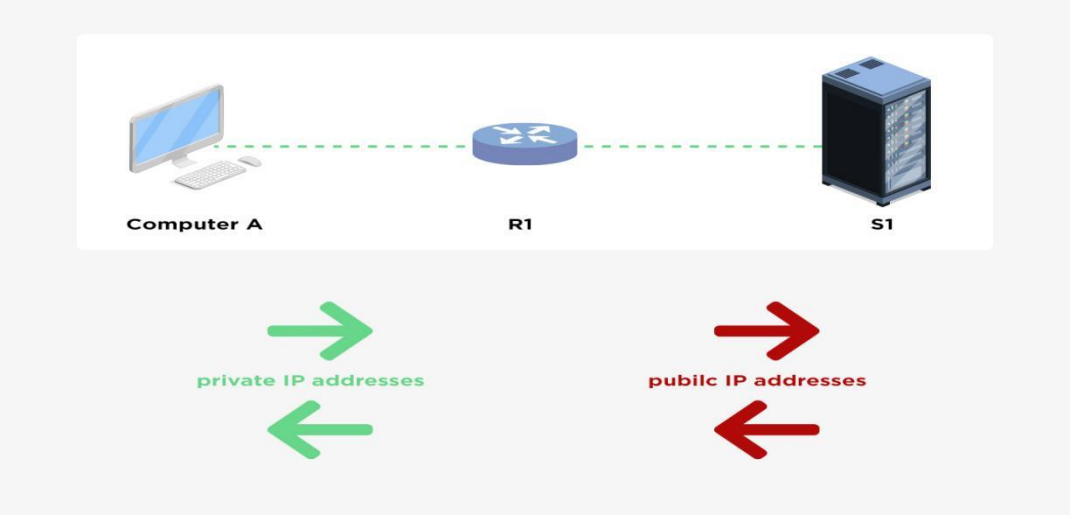

Figure I.*6*: Network address translation (NAT)

I.3.2.6 Protocol STP

Spanning-Tree protocol (STP) est un protocole L2 formalisé IEEE 802.1D qui permet de

garder une topologie physique redondante tout en créant un chemin logique unique.

STP envoie régulièrement des annonces (BPDU) pour élire un commutateur principal (root). [7]

La figure suivante présente le protocole STP.

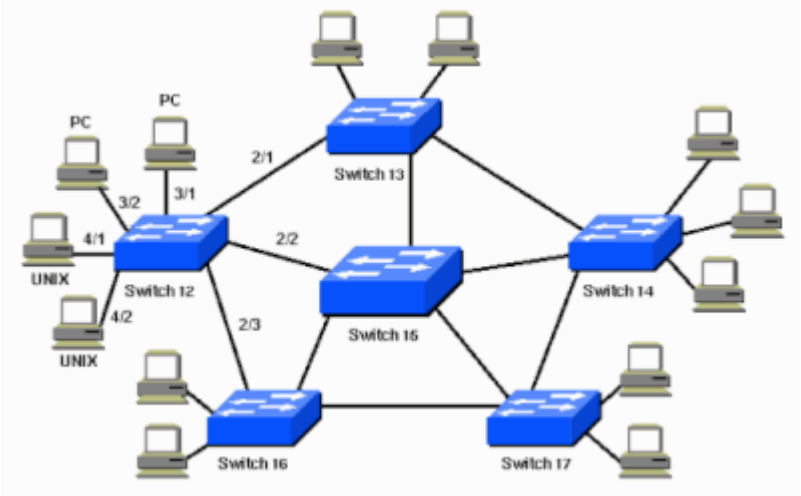

Figure I. *7*: Spanning Tree Protocol

I.3.2.7 Protocol DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) est utilisé pour attribuer dynamiquement des adresses IP (Internet Protocol) à chaque hôte du réseau de votre organisation. Dans cette signification DHCP, un hôte peut faire référence à n'importe quel dispositif qui permet l'accès à un réseau. [8]

La figure suivante présente le protocole DHCP.

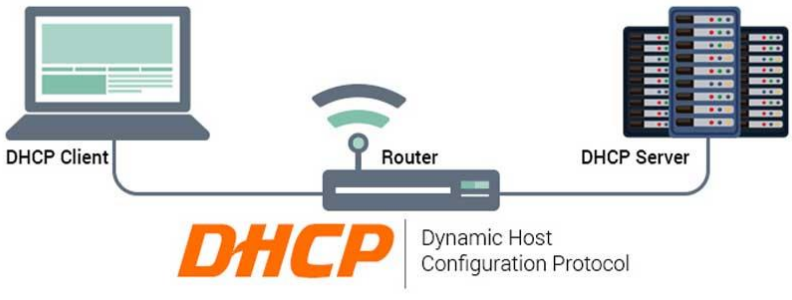

Figure I. *8*:Dynamic Host Configuration Protocol

I.3.2.8 Protocol DNS

Le DNS (Domain Name System, système de nom de domaine) est en quelque sorte le

répertoire téléphonique d'Internet. Les internautes accèdent aux informations en ligne via des noms de domaine (par exemple, nytimes.com ou espn.com), tandis que les navigateurs interagissent par le biais d'adresses IP (Internet Protocol, protocole Internet). Le DNS traduit les noms de domaine en adresses IP afin que les navigateurs puissent charger les ressources web.[9]

La figure suivante présente le protocole DNS.

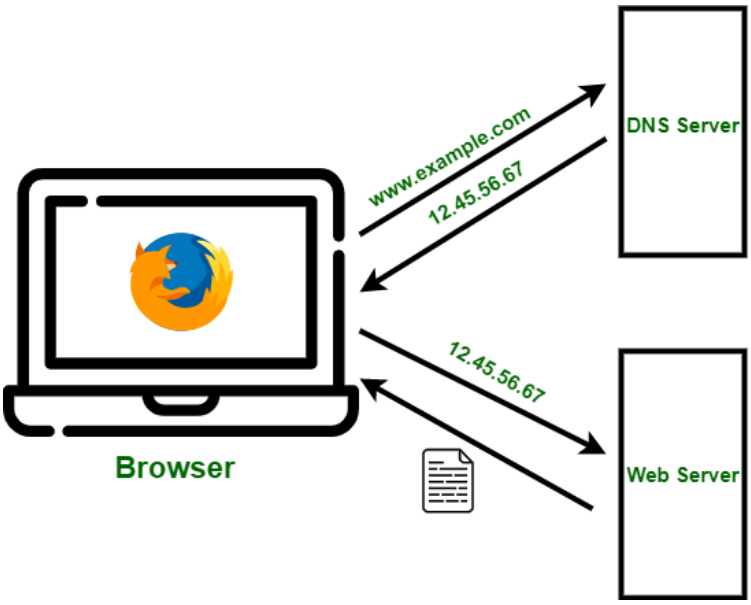

Figure I. *9*: Domain Name System

I.4 Modelés OSI et TCP/IP

Les modèles OSI et TCP/IP sont des cadres conceptuels essentiels pour la compréhension et la mise en œuvre des réseaux informatiques. Voici quelques points clés sur ces deux modèles:

I.4.1 Modèle OSI

Le modèle Open Systems Interconnection (OSI) est un modèle conceptuel créé par l'Organisation internationale de normalisation qui permet à divers systèmes de communication de communiquer à l'aide de protocoles standards, l'OSI fournit une norme permettant à différents systèmes informatiques de communiquer entre eux.

Le modèle OSI peut être considéré comme un langage universel pour la mise en réseau d'ordinateurs. La base du concept est de diviser un système de communication en sept couches abstraites, chacune empilée sur la dernière, comme montre la figure suivante.

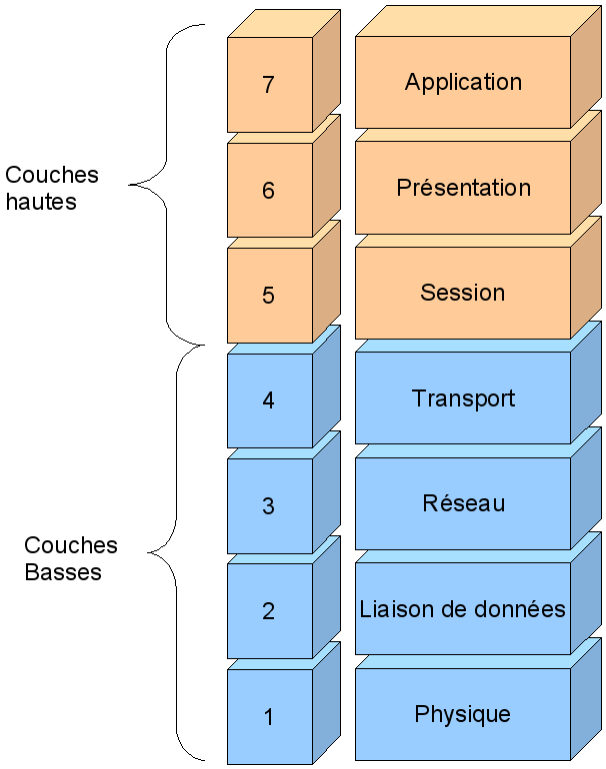

Figure I.*10*: Les 7 couches du modèle OSI

Les 7 couches du modèle OSI sont :

I.4.1.1 Couche Physique

La couche physique est responsable du câble physique ou de la connexion sans fil entre les nœuds réseau. Il définit le connecteur, le câble électrique ou la technologie sans fil reliant les appareils et est responsable de la transmission des données brutes (bits), qui est simplement une série de 0 et 1, tout en prenant en charge le contrôle du débit binaire.

Dans cette couche, on trouve donc des techniques de communication numérique bien connues des utilisateurs comme le Wi-Fi, l'USB, Bluetooth, Ethernet ou ADSL.

I.4.1.2 Couche Liaison de données

La couche de liaison de données établit et met fin à une connexion entre deux nœuds connectés physiquement sur un réseau. Il divise les paquets en cadres et les envoie de la source à la destination.

La coche liaison de données définit les procédures d'exploitation du lien de communication et fournit un cadrage et un séquençage**.**

Par exemple, un switch Ethernet (switch accès) fonctionne sur la couche de liaison de données (couche 2) du modèle OSI pour créer un domaine de diffusion distinct pour chaque port de commutateur, et donne l'accès aux utilisateurs. Le switch Cisco Nexus 9000 (switch TOR) peuvent s'adapter aux sollicitations croissantes de la bande passante tout en consommant peu d'énergie et en offrant un rapport performance exceptionnel et deux modes de fonctionnement, et il donne l'accès au serveur AD pour fournir des informations sur les objets, et les organise et contrôle les accès et la sécurité.

I.4.1.3 Couche Réseau

La couche réseau est chargée de faciliter le transfert de données entre deux réseaux différents. Elle remplit deux fonctions principales :

L'une consiste à briser les segments en paquets de réseau et à réassembler les paquets à l'extrémité de réception.

L'autre est de routage des paquets en découvrant le meilleur chemin à travers un réseau physique.

Dans la couche réseau, Le switch de niveau 3 (switch distribution) prend en charge toutes les fonctions de commutation et possède également des fonctionnalités pour le routage entre VLAN (donne une interface gateway pour le VLAN.)

I.4.1.4 Couche Transport

La couche de transpor**t** prend les données transférées dans la couche de session et la divise en « segments » à l'extrémité de transmission. Il est chargé de réassembler les segments à l'extrémité de réception, en les transformant en données qui peuvent être utilisées par la couche de session.

I.4.1.5 Couche Session

La couche de session crée des canaux de communication, appelés sessions, entre les appareils. Il est responsable de l'ouverture des sessions, de s'assurer qu'ils restent ouverts et fonctionnels pendant le transfert des données et de les fermer à la fin de la communication. La couche de session peut également définir des points de contrôle lors d'un transfert de données.

I.4.1.6 Couche Présentation

La couche de présentation prépare des données pour la couche d'application. Il définit comment deux périphériques doivent coder, chiffrer et comprimer les données afin qu'ils soient reçus correctement à l'autre extrémité. La couche de présentation prend toutes les

données transmises par la couche d'application et la prépare à la transmission sur la couche de session.

I.4.1.7 Couche Application

La couche d'application est utilisée par les logiciels d'utilisation finale tels que les navigateurs Web et les clients de messagerie. Il fournit des protocoles qui permettent aux logiciels d'envoyer et de recevoir des informations et de présenter des données significatives aux utilisateurs.

Quelques exemples de protocoles de couche d'application sont le protocole de transfert hypertexte (HTTP), le protocole de transfert de fichiers (FTP), le protocole de poste (POP), le protocole de transfert de courrier simple (SMTP), le protocole SSH (Secure Shell) et le système de noms de domaine (DNS).[10]

I.4.2 Modèle TCP/IP

Le modèle TCP/IP définit la manière dont les périphériques doivent transmettre des données entre eux et facilite la communication sur les réseaux et les grandes distances. Le modèle décrit la manière dont les données sont échangées et organisées sur les réseaux. Il est divisé en quatre couches, qui définissent les normes en matière d'échange de données et représentent la manière dont les données sont traitées et regroupées lorsqu'elles sont transmises entre des applications, des périphériques et des serveurs.

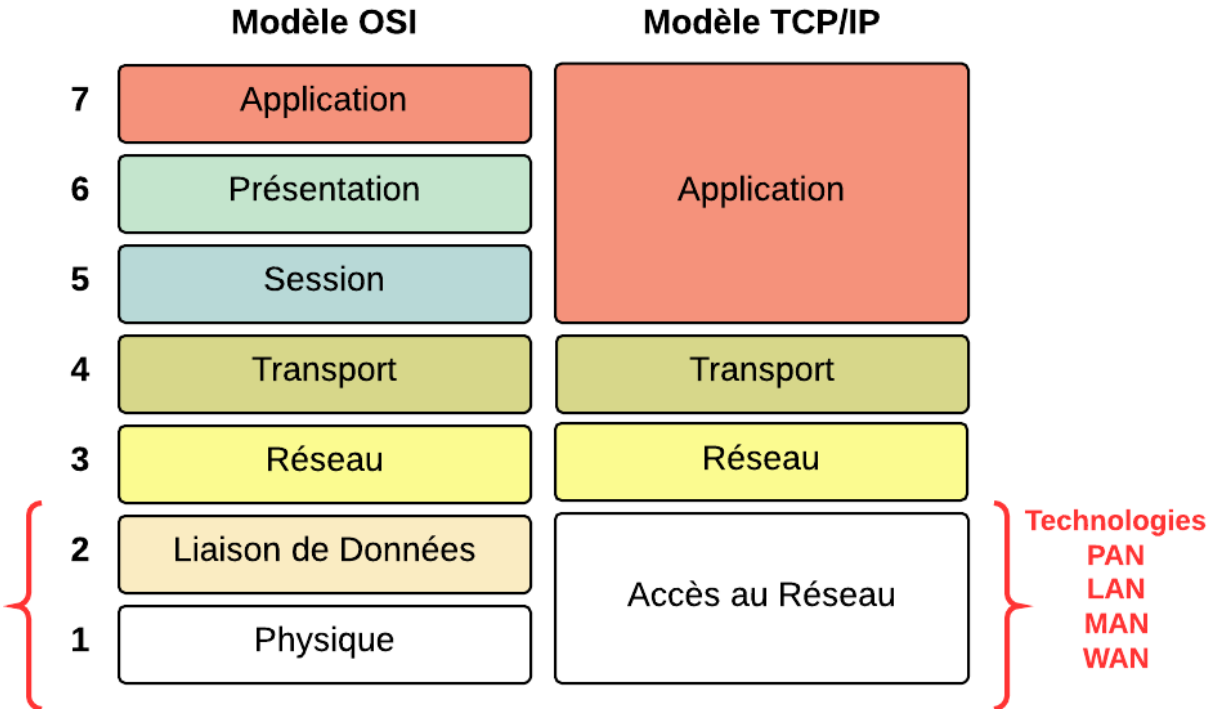

Figure I. ***11*** Modèle OSI & Modèle TCP/IP

Les quatre couches du modèle TCP/IP sont les suivantes :

I.4.2.1 Couche Accès au Réseau

Elle définit la manière dont les données doivent être envoyées, gère l'acte physique d'envoi et de réception des données, et assure la transmission des données entre les applications ou les périphériques sur un réseau. Cela inclut la définition de la manière dont les données doivent être signalées par le matériel et d'autres dispositifs de transmission sur un réseau, tels que le pilote de dispositif d'un ordinateur, un câble Ethernet, une carte d'interface réseau (NIC) ou un réseau sans fil. Elle est également appelée couche de liaison, couche d'accès au réseau, couche d'interface réseau ou couche physique et constitue la combinaison des couches physique et de liaison des données du modèle OSI (Open Systems Interconnection), qui normalise les fonctions de communication des systèmes informatiques et de télécommunications.

I.4.2.2 Couche réseau

Elle permet l'envoi de paquets à partir d'un réseau et contrôle leur mouvement à travers un réseau afin de s'assurer qu'ils atteignent leur destination. Elle offre les fonctions et les procédures de transfert des séquences de données entre les applications et les périphériques sur les réseaux.

I.4.2.3 Couche transport

Elle permet d'établir une connexion de données de qualité et fiable entre l'application ou le périphérique d'origine et sa destination prévue. C'est à ce niveau que les données sont divisées en paquets et numérotées pour créer une séquence. Ainsi, la couche transport détermine la quantité de données à envoyer, leur destination et leur débit. Elle s'assure que les paquets de données sont envoyés sans erreur et en séquence et obtient la confirmation que le périphérique de destination a reçu les paquets de données.

I.4.2.4 Couche application

Elle fait référence aux programmes qui ont besoin de TCP/IP pour les aider à communiquer entre eux. C'est à ce niveau que les utilisateurs interagissent généralement, notamment via les systèmes courriel et les plateformes de messagerie. Elle combine les couches session, présentation et application du modèle OSI. [11]

I.5 Conclusion

Dans ce premier chapitre, nous avons réalisé une analyse approfondie des réseaux

informatiques, en abordant divers aspects tels que la définition des réseaux, les types existants, les architectures, les topologies, les moyens de transmission, les équipements de connexion, ainsi que les modèles tels que l'OSI et TCP/IP, accompagnés de leurs protocoles de communication respectifs. Chaque réseau informatique doit être sécurisé contre les menaces, ce qui sera exploré dans le prochain chapitre où nous traiterons des aspects généraux de la sécurité des réseaux informatiques.

Chapitre II

La sécurité informatique

II Introduction

Avec le développement de l'utilisation d'internet, de plus en plus les entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

Pour cela, la sécurité informatique est devenue un aspect essentiel de notre vie quotidienne. Les attaques sont devenues plus fréquentes et plus sophistiquées, affectant chaque année des millions d'entreprises et de particuliers. La sécurité informatique consiste à protéger les systèmes et réseaux informatiques contre les accès non autorisés, le vol, les dommages et l'exploitation.

Dans ce chapitre, on se concentra sur l'étude de la sécurité des réseaux, en abordant les différentes méthodes d'attaques, les mesures de protection et les architectures de pare-feux. [12][13]

II.1 Sécurité informatique

La sécurité des réseaux est un domaine qui englobe toutes les mesures prises pour protéger l'intégrité d'un réseau informatique et des données qu'il contient. Elle est importante car elle protège les données sensibles des attaques et garantit que le réseau est utilisable et digne de confiance. Ainsi, elle est essentielle pour prévenir les attaques et les tentatives d'hameçonnage, le vol d'informations, les failles de sécurité et la destruction de biens, et elle empêche les cybercriminels d'accéder à des données précieuses et à des informations sensibles. Lorsque des pirates s'emparent de ces données, ils peuvent causer toute une série de problèmes, notamment l'usurpation d'identité, le vol d'actifs et l'atteinte à la réputation. [14]

II.1.1 Objectif de la sécurité informatique

La priorité de la cybersécurité est de préserver l'intégrité des infrastructures informatiques, des flux de communication et des données. En d'autres termes, elle repose sur un ensemble de précautions matérielles et conceptuelles pour éviter l'espionnage.

Voici quelques objectifs spécifiques de la sécurité informatique : [15]

- **La confidentialité**

La confidentialité consiste à s'assurer que les informations diffusées ne sont accessibles

qu'aux personnes qui disposent d'un droit d'accès. Elle constitue un axe important de la sécurité des systèmes d'information.

- **L'intégrité**

La sécurité informatique doit permettre à l'entreprise de garder ses données intactes, et veiller à ce qu'elles ne subissent aucun dommage ou destruction volontaire ou accidentelle.

- **La disponibilité**

La disponibilité est l'une des pierres angulaires de la sécurité informatique. Elle désigne la capacité des collaborateurs à utiliser l'ensemble des données qui leur sont nécessaires pour l'accomplissement d'une tâche de manière sécurisée.

- **La non-répudiation**

La non-répudiation suppose la possibilité de vérifier l'identité de l'expéditeur et du destinataire d'un message transmis dans un cadre professionnel. Cette vérification se fait généralement grâce à la technologie du certificat numérique qui permet de prouver l'identité d'un individu.

- **L'authentification**

L'authentification consiste à s'assurer de l'identité d'un utilisateur puis de déterminer sa légitimité pour accéder à certaines ressources de l'entreprise (données, logiciels, etc.). [16]

Figure II. 1 Les Objectifs de la sécurité informatiques

II.2 Menaces informatiques

Dans le monde numérique d'aujourd'hui, la sécurité informatique est plus importante que

jamais. Les entreprises, les gouvernements et même les particuliers font face à une menace constante des attaques et de violations de données**.**

Les menaces contrées par la sécurité réseau sont :

- Les attaques informatiques.
- Les programmes malveillants

II.2.1 Attaques informatiques

Les attaques informatiques sont des actions malveillantes qui visent à perturber, à voler ou à détruire des informations ou des systèmes informatiques. Ces attaques peuvent prendre de nombreuses formes.

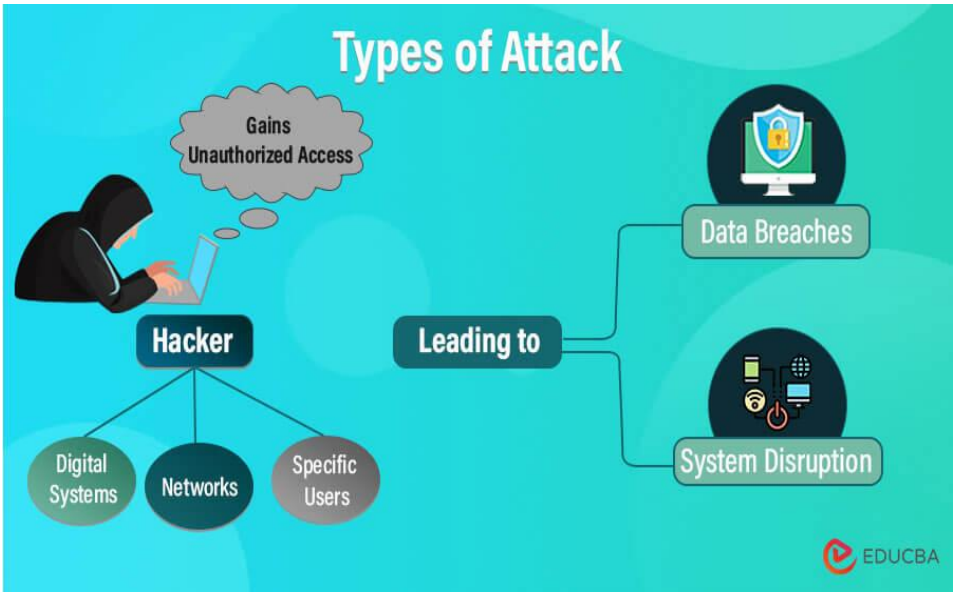

Figure II. 2 Une attaque informatique

Voici quelques-uns des types d'attaques informatiques couramment utilisés :

II.2.1.1 Attaques de reconnaissance

La reconnaissance est la première étape d'un piratage durant laquelle l'attaquant collecte des informations pertinentes à propos de la cible. Cela se fait dans le but d'identifier les différentes vulnérabilités afin de définir les moyens possibles pour l'attaquer. Elle utilise plusieurs outils comme : NMAP, NESSUS, METASPLOIT, SHODAN …

On distingue deux (2) types de reconnaissance :

II.2.1.1.1 Reconnaissance passive

Cela consiste à recueillir des informations sur la cible sans l'interroger directement. Cette collecte d'informations se fait par des recherches à partir de sources accessibles au public sur Internet comme les réseaux sociaux, les moteurs de recherches, etc.

II.2.1.1.2 Reconnaissance active

Contrairement à la reconnaissance passive, cette forme de reconnaissance interagit directement avec la cible. Elle se fait à travers des requêtes qui utilisent par exemple le nom de domaine de l'organisation ou d'autres techniques d'interaction directe. Cette reconnaissance pourrait être détectée par la cible et déclencher une alarme. [17]

II.2.1.2 Ingénierie sociale

L'ingénierie sociale est une technique de fraude qui consiste à manipuler la victime pour l'inciter à divulguer des informations confidentielles.
Voici les différentes techniques d'attaques utilisant l'ingénierie sociale les plus courantes :

- **Phishing ou Hameçonnage**

L'Hameçonnage c'est le moyen le plus répandu de mise en œuvre de l'ingénierie sociale, les pirates informatiques utilisent des courriels, des sites web, les réseaux sociaux et des messages texte trompeurs pour voler des informations personnelles ou organisationnelles sensibles à des victimes sans méfiance.

- **Phishing ciblé ou Spear Phishing**

Cette arnaque par courrier électronique est utilisée pour mener des attaques ciblées contre des particuliers ou des entreprises. Le spear phishing est plus complexe qu'un courriel de phishing de masse, car il nécessite de la part de l'attaquant, des recherches approfondies sur les cibles potentielles et leurs organisations. [18]

II.2.1.3 Attaques d'accès

Ces attaques exploitent les vulnérabilités connues des services d'authentification, services FTP et services Web pour accéder à des comptes Web, des bases de données confidentielles et d'autres informations sensibles. Une attaque par accès permet à une personne d'obtenir un accès non autorisé à des informations qu'elle n'a pas le droit de consulter.[19]

II.2.1.4 Attaques MITM

Une attaque de l'homme du milieu (MITM) est un type de cyberattaque où les attaquants interceptent une conversation ou un transfert de données existant, soit en écoutant, soit en se faisant passer pour un participant légitime. [20]

II.2.1.5 Attaques DOS et DDOS

Une attaque par déni de service (Denial-of-Service, DoS) sature un serveur, rendant ainsi un site Web ou une ressource indisponible. Une attaque par déni de service distribué (Distributed Denial-of-Service, DDoS) est une attaque DoS qui utilise plusieurs ordinateurs ou machines pour saturer une ressource ciblée. Les deux types d'attaques surchargent un serveur ou une application Web dans le but d'en interrompre les services. [21**]**

II.2.1.6 Attaques Hijacking

Aussi appelé "vol de session TCP". C'est une attaque qui cible une session utilisateur dans un réseau sécurisé. La technique utilisée dans ce genre d'attaque est le IP spoofing. L'attaquant emploie la technique de routage des sources des paquets TCP/IP pour insérer des commandes dans une communication active entre deux nœuds dans le réseau. Puis il se déguise en tant qu'utilisateur authentifié.

II.2.1.7 Attaques DNS Spoofing

L'usurpation d'identité du système de noms de domaine (Domain name system (DNS) spoofing**) est** un type de cyberattaque qui utilise des données de serveur DNS falsifiées pour rediriger les utilisateurs vers de faux sites Web. Ces sites malveillants semblent souvent légitimes, mais sont conçus pour installer des logiciels malveillants sur les appareils des utilisateurs, voler des données sensibles ou rediriger le trafic.[22]

II.2.1.8 Attaques DHCP spoofing

DHCP spoofing, également appelée usurpation d'identité DHCP, se produit lorsqu'un acteur malveillant intercepte ou perturbe la communication entre les appareils d'un réseau et le serveur DHCP . Le protocole DHCP (Dynamic Host Configuration Protocol) attribue des adresses IP aux appareils d'un réseau. Lors d'une attaque DHCP, le pirate informatique tente de contrôler ce processus, généralement pour distribuer de fausses adresses IP ou rediriger le trafic réseau. [23]

II.2.1.9 Attaques MAC Flooding

Une attaque par inondation MAC, également connue sous le nom d'attaque par débordement de table MAC, est un type d'attaque de sécurité réseau qui cible les commutateurs réseau. Cela implique de surcharger la table d'adresses MAC d'un commutateur en l'inondant d'une quantité massive de trames Ethernet usurpées, chacune contenant une adresse MAC source unique. [24]

II.2.2 Programmes malveillants

Un malware est un type de logiciel malveillant conçu pour endommager ou désactiver des ordinateurs. Les logiciels malveillants sont souvent diffusés par le biais de pièces jointes de courriels ou de téléchargements qui semblent sûrs, mais qui peuvent être utilisés par des cybercriminels pour gagner de l'argent ou mener des cyberattaques politiques.

La figure suivante présente les types des programmes malveillants.

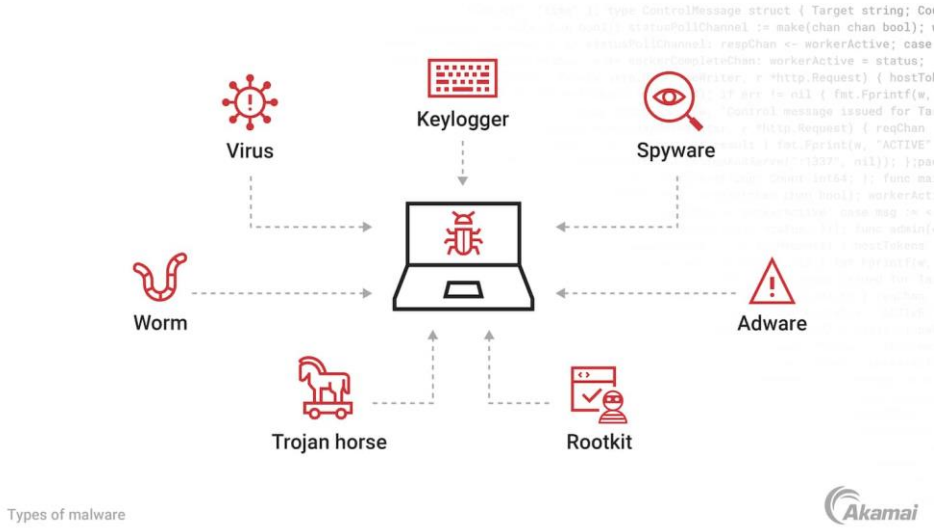

Figure II. 3 Les types des programmes malveillants

Il existe de nombreux types de malwares différents, notamment :

II.2.2.1 Attaques par Virus

Un programme pouvant se dupliquer qui s'attache à un fichier sain et se propage dans tout le système en infectant les fichiers à l'aide d'un code malveillant.

II.2.2.2 Attaques de Cheval de Troie

C'est type de programmes malveillants se faisant passer pour des logiciels authentiques. Les cybercriminels piègent les utilisateurs en téléchargeant des chevaux de Troie dans leur ordinateur pour endommager ou collecter des données.

II.2.2.3 Attaques Spyware

Un programme espion qui enregistre secrètement les actions d'un utilisateur au profit des cybercriminels. Par exemple, un spyware peut enregistrer des coordonnées bancaires.

II.2.2.4 Attaques Ransomware

Un malware qui verrouille les fichiers et les données de l'utilisateur sous menace de les effacer si une rançon n'est pas payée.

II.2.2.5 Attaques Adware

Un logiciel publicitaire qui peut être utilisé pour propager un malware.

II.2.2.6 Attaques Botnets

Des réseaux d'ordinateurs infectés par des malwares que les cybercriminels peuvent utiliser pour effectuer des tâches en ligne sans l'autorisation de l'utilisateur. [25]

II.3 Protocoles de sécurité

Parmi les protocoles de sécurité nous mentionnons les protocoles SSH, SSL/TLS, HTTPS.

- Protocol SSH (Secure Shell)

Le protocole SSH (Secure Shell) est un protocole de communication sécurisé utilisé pour établir des connexions distantes sécurisées entre un client et un serveur à travers un réseau non sécurisé comme Internet. Il assure l'authentification, la confidentialité et l'intégrité des données échangées. SSH permet d'envoyer en toute sécurité des commandes à un ordinateur distant et offre la possibilité de tunnelier les connexions. SSH utilise TCP pour garantir la livraison des paquets dans l'ordre et assurer une connexion fiable, et chiffre les connexions

entre les appareils. [26]

- Protocol SSL/TLS

Le protocole SSL/TLS (Secure Sockets Layer/ Transport Layer Security) est essentiel pour crypter les communications entre un client et un serveur, notamment entre navigateurs Web et sites/applications Web. SSL et son successeur plus sécurisé TLS protègent les données échangées sur Internet, empêchant les attaquants d'intercepter ou modifier les données. Les propriétaires de sites Web doivent implémenter SSL/TLS pour sécuriser les échanges de données sensibles comme les mots de passe et les informations de paiement.SSL/TLS utilise à la fois un cryptage asymétrique et symétrique pour assurer la confidentialité et l'intégrité des données en transit. Pour établir une connexion sécurisée, le client et le serveur s'authentifient mutuellement, et les données sont chiffrées par le protocole SSL du navigateur avant d'être transmises et déchiffrées par le site de destination. Les certificats SSL permettent l'authentification du serveur et le chiffrement des données échangées. [27]

- Protocol HTTPS

Le protocole HTTPS (HyperText Transfer Protocol Secure) est une extension sécurisée du protocole HTTP qui permet de chiffrer les données échangées entre un navigateur web et un serveur distant. Il vise à rendre le web plus sûr en garantissant la confidentialité et l'intégrité des informations des internautes. Il est chiffré afin de renforcer la sécurité du transfert de données. Ceci est particulièrement important lorsque les utilisateurs transmettent des données sensibles. [28]

II.4 Mécanisme de sécurité informatique

Parmi les mécanismes de sécurité utilisés pour protéger les réseaux informatiques contre les menaces externes et internes nous citons ceux qui sont les plus importantes.

II.4.1 Mise à jour régulière des logiciels et des systèmes

Les mises à jour régulières permettent de corriger les failles de sécurité découvertes, d'améliorer la résilience face aux menaces et de maintenir la conformité aux normes de sécurité.

II.4.2 Access par authentification

L’authentification est le processus utilisé par les entreprises pour vérifier que seuls les utilisateurs, services et applications appropriés et dotés des autorisations adéquates peuvent accéder aux ressources de l’organisation. Il s’agit d’un volet important de

la cybersécurité, car la priorité des acteurs malveillants est d'accéder sans autorisation aux systèmes. Pour y parvenir, ceux-ci dérobent les identifiant et mot de passe d'utilisateurs qui disposent d'autorisations d'accès. [29]

II.4.3 Protection par VPN

VPN (réseau privé virtuel) permet de créer un tunnel sécurisé entre deux réseaux distants, permettant ainsi aux utilisateurs d'accéder au réseau à distance de manière sécurisée. Les VPN utilisent des protocoles de cryptage pour sécuriser les communications entre les réseaux.

II.4.4 Protection par cryptographie

Le cryptage implique l'utilisation d'algorithmes complexes pour convertir du texte brut en code illisible, ce qui rend difficile l'accès des personnes non autorisées aux informations sensibles. Il existe deux principaux types de chiffrement : le chiffrement symétrique et asymétrique. Le chiffrement symétrique utilise une clé unique pour chiffrer et déchiffrer les données. Le cryptage asymétrique, quant à lui, utilise une paire de clés, une pour le cryptage et une autre pour le déchiffrement. [30]

II.4.5 Surveillance du réseau

Permet de détecter les activités suspectes et les tentatives d'intrusion. Les outils de surveillance réseau peuvent alerter les administrateurs de réseau en cas d'activité malveillante et permettent d'agir rapidement pour contrer les menaces. [31]

II.4.6 Protection par ACL 's

Les **ACL**, pour **A**ccess **C**ontrol **L**ist, sont des règles appliquées aux trafics transitant via les interfaces du routeur que ce soit en entrée (in) ou en sortie (out). Les ACL filtrent le trafic en demandant aux interfaces d'acheminer ou non les paquets qui y transitent. Pour ce faire, le routeur lit l'en-tête de chaque paquet afin de déterminer s'il doit être acheminé ou non en fonction des conditions définies dans la liste de contrôle d'accès ALS.

Ils nous permettent de :

- Maitriser le réseau en déterminant quel type de trafic sera acheminé ou bloqué.
- Augmenter le niveau de sécurité d'accès réseau de manière basique en accordant ou non l'accès à un segment du réseau.
- Optimiser le réseau à d'autres fins que la sécurité, par exemple pour contrôler la bande-passante, restreindre le contenu des mises à jour de routage ou

identifier et classer le trafic par fonctionnalités de qualité de service (QoS). [32]

II.4.7 Système de détection des intrusions IDS/IPS

- Un système de détection des intrusions (IDS, Intrusion Detection System) surveille le trafic réseau, analyse ce trafic pour identifier des signatures correspondant à des attaques connues et vous avertit en cas d'événement suspect. Dans l'intervalle, le trafic est maintenu.
- Un système de prévention des intrusions (IPS, Intrusion Prevention System) surveille également le trafic, mais en cas d'événement inhabituel, le trafic est interrompu jusqu'à ce que vous examiniez l'incident et décidiez de rétablir le trafic. [33]

II.4.8 Logiciels Antivirus

Le programme informatique présenté sous la forme d'un logiciel antivirus propose une protection efficace de votre système (ordinateur, smartphone, tablette).

Le logiciel antivirus effectue une recherche régulière et automatique des fichiers et du disque dur pour détecter les fichiers malveillants, les éliminer ou les mettre en quarantaine.

Le logiciel antivirus n'est jamais fiable à 100 % mais il constitue une barrière de protection contre les agressions. Il faut savoir qu'un virus peut engendrer la perte de toutes les informations de votre ordinateur et se propager à la totalité des fichiers de votre réseau informatique.

De nombreux logiciels comme BitDefender ou AltoSpam vous protègent contre les logiciels malveillants (malwares) :

- Spams (courriers indésirables),
- Virus reçus en pièce jointe de courriels
- Autre tentative d'attaque (spyware, trojan, ransomware etc.) [34]

II.4.9 Mise en place des firewalls

Un firewall ou pare-feu, est un appareil de sécurité réseau qui surveille le trafic réseau entrant et sortant et autorise ou bloque les paquets de donnés en se basant sur un ensemble de règles de sécurité. Il est chargé de dresser une barrière entre votre réseau interne et le trafic entrant provenant de sources externes (comme Internet) afin de bloquer le trafic malveillant des virus et des pirates. [35]

Un pare-feu est un élément indispensable de toute architecture de sécurité. Il élimine les incertitudes liées aux protections au niveau de l'hôte et les confie à votre appareil de sécurité

réseau. Les pares-feux, et en particulier le Pare-feu de nouvelle génération, se concentrent sur le blocage des logiciels malveillants et des attaques de la couche application. Avec un système de prévention des intrusions (IPS) intégré, ces Pare-feu de nouvelle génération peuvent réagir rapidement et de manière transparente pour détecter les attaques extérieures et y réagir sur l'ensemble du réseau. Ils peuvent définir des politiques pour mieux défendre votre réseau et effectuer des évaluations rapides pour détecter les activités invasives ou suspectes, comme les logiciels malveillants, et les arrêter. [36]

La figure suivante présente un firewall.

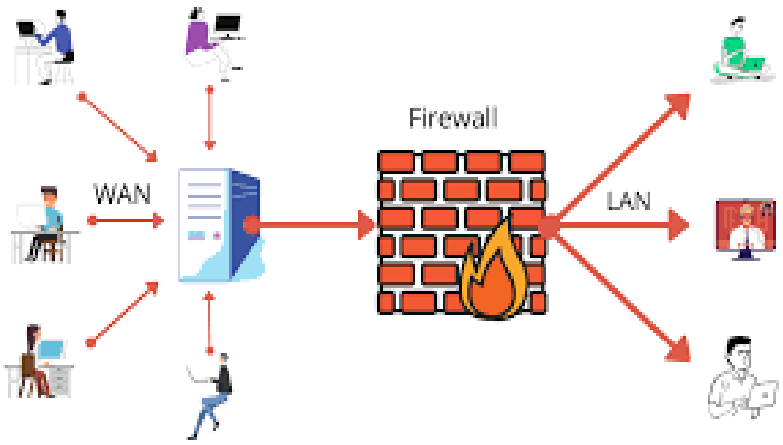

Figure II. 4 Un firewall

II.5 Rôle du firewall dans une entreprise

Les pares-feux jouent un rôle crucial dans les entreprises, en protégeant contre les intrusions et en contrôlant l'accès des utilisateurs par les règles de sécurité

- **Protection contre les intrusions :** Le firewall crée une barrière virtuelle qui protège le réseau contre les attaques externes. En bloquant les connexions non autorisées et en détectant les tentatives d'intrusion, il sécurise le périmètre du réseau et prévient les intrusions potentielles avant qu'elles n'atteignent leur cible.
- **Contrôle d'accès et politique de sécurité :** le firewall permet de mettre en place des politiques de sécurité granulaires pour contrôler l'accès aux ressources réseau. En définissant des règles de filtrage spécifiques, les administrateurs système peuvent

restreindre l'accès aux services et aux applications en fonction des besoins de l'entreprises et des exigences de sécurité.

- **Sécurisation des communications :** En segmentant le réseau en zones de confiance, le firewall peut isoler les différents segments du réseau. Réduisant ainsi les risques de compromission des données sensibles. Il permet également de sécuriser les communications internes en limitant la propagation des attaques entre les différents segments du réseau.
- **Surveillance et réponse aux incidents :** Outre sa fonction de prévention des intrusions, un firewall joue un rôle crucial dans la surveillance du trafic réseau et de la détection d'activités suspectes. En analysant les logs et les alertes générées par l'outil, les équipes de sécurité peuvent identifier rapidement les tentatives d'intrusion et prendre les mesures pour y remédier. [37]

II.6 Types de firewall

Nous trouvons les firewalls à filtrage par paquets, par état d'inspection, firewall proxy, firewall d'application web, Firewalls de nouvelle génération :

II.6.1 Firewalls pare-parquets

Un pare-feu de filtrage des paquets IP permet de créer un ensemble de règles qui interdit ou autorise le trafic sur une connexion réseau. Le pare-feu lui-même n'affecte en rien ce trafic. Un filtre de paquets ne pouvant supprimer que le trafic qui lui est envoyé, l'unité contenant le filtre de paquets doit effectuer un routage des adresses IP ou être la destination du trafic.

Un filtre de paquets contient un ensemble de règles avec des actions d'acceptation ou de refus. Lorsque le filtre des paquets reçoit un paquet d'informations, il le compare à votre ensemble de règles préconfiguré. Dès qu'il rencontre une occurrence, il accepte ou refuse le paquet d'informations. La plupart des filtres de paquets contiennent une règle de "refus global" implicite à la fin du fichier de règles.

Les filtres de paquets autorisent ou refusent généralement le trafic réseau en fonction des éléments suivants :

- Adresses IP de la source et de la destination
- Protocole, tel que TCP, UDP ou ICMP
- Ports de la source et de la destination et codes et types ICMP
- Indicateurs de l'en-tête TCP (le paquet correspond-il à une demande de connexion, etc.)
- Sens (entrant ou sortant)
- Interface physique traversée par le paquet. [38]

La figure suivante présente un pare-feu de filtre de paquets.

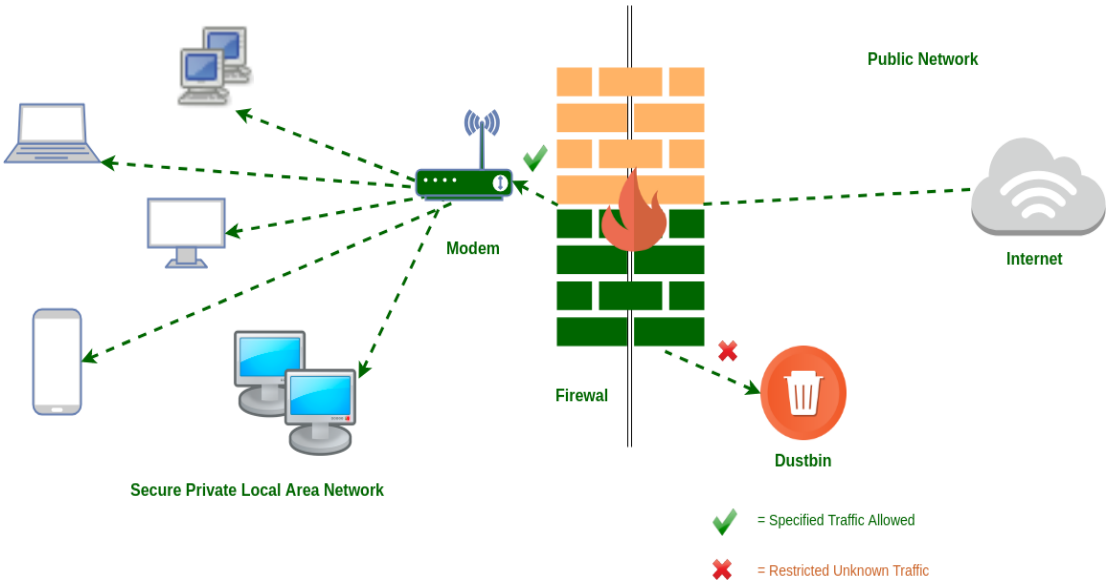

Figure II. 5 Pare-feu de filtre de paquets

II.6.2 Firewalls à inspection d'état

Les firewalls à inspection d'état (Stateful inspection) incluent à la fois la technologie d'inspection des paquets et la vérification de la poignée de main TCP, ce qui les rend supérieurs aux pare-feux pare-paquets ou aux passerelles de niveau circuit. De plus, ces types de pare-feu suivent l'état des connexions établies.

Les stateful firewall peuvent également intégrer des services supplémentaires, tels que le cryptage ou les tunnels. Ils améliorent les performances, car ils empêchent les acteurs malveillants de lire le contenu des communications, rendant ainsi la connexion plus sûre grâce au contrôle d'accès.

Parmi les fonctionnements d'un stateful firewall on mentionne :

- **Inspection dynamique des paquets :**

L'inspection dynamique des paquets est une technologie utilisée par les pare-feux dynamiques pour déterminer les paquets qui peuvent être autorisés à travers le pare-feu.

- **Protocole de contrôle des transports (TCP) :**

Le protocole TCP est l'un des principaux protocoles utilisés par Internet pour envoyer et recevoir des données, ce qui permet l'envoi et la réception simultanés de données. En plus d'aider à transmettre les informations, TCP contient des données qui peuvent entraîner une réinitialisation (RST) de la connexion, l'arrêtant complètement. TCP dicte également le moment auquel la transmission doit prendre fin, par le biais d'une commande FIN (finition).

Il regroupe les données en paquets, et lorsqu'ils arrivent à destination, ces paquets sont réassemblés en données que le récepteur peut comprendre.

- **Échange tripartite :**

L'échange triparti implique la synchronisation des deux côtés du processus de transmission de données pour initier une connexion, puis se reconnaître mutuellement. Dans ce processus, chaque partie transmet des informations à l'autre partie. [39]

La figure suivante présente un firewall a inspection d'état.

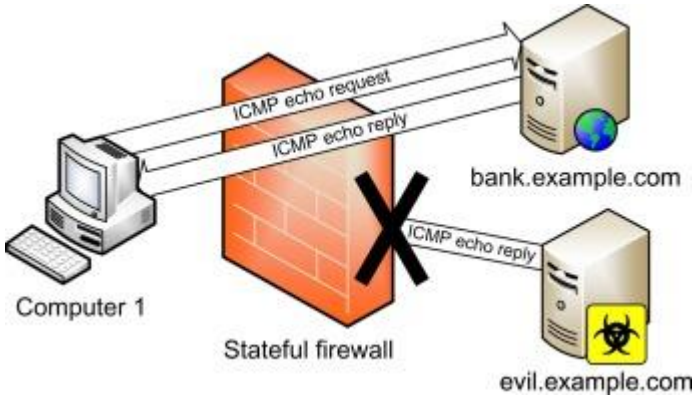

Figure II. 6 Firewall a inspection d'état

II.6.3 Firewalls proxy

Un pare-feu proxy, également appelé pare-feu d'application ou pare-feu de passerelle, limite les applications qu'un réseau peut prendre en charge, ce qui augmente les niveaux de sécurité mais peut affecter la fonctionnalité et la vitesse. Un pare-feu proxy est la forme de pare-feu la plus sécurisée, qui filtre les messages au niveau de la couche application pour protéger les ressources réseau.

Un pare-feu proxy est considéré comme la forme de pare-feu la plus sécurisée car il empêche les réseaux de contacter directement d'autres systèmes. Il possède sa propre adresse IP (Internet Protocol) , ce qui signifie qu'une connexion réseau externe ne peut pas recevoir de paquets directement du réseau.

Un utilisateur tentant d'accéder à un site externe via un pare-feu proxy le ferait via ce processus :

1. L'utilisateur demande l'accès à Internet via un protocole tel que (FTP) ou (HTTP).
2. L'ordinateur de l'utilisateur tente de créer une session entre lui et le serveur, en envoyant un paquet de messages de synchronisation (SYN) depuis son adresse IP vers l'adresse IP du serveur.

3. Le pare-feu proxy intercepte la demande et, si sa politique le permet, répond avec un paquet de messages d'accusé de réception de synchronisation (SYN-ACK) provenant de l'adresse IP du serveur demandé.
4. Lorsque le paquet SYN-ACK est reçu par l'ordinateur de l'utilisateur, il envoie un paquet ACK final à l' adresse IP du serveur. Cela garantit une connexion au proxy mais pas une connexion TCP valide.
5. Le proxy termine la connexion au serveur externe en envoyant un paquet SYN depuis son adresse IP. Lorsqu'il reçoit le paquet SYN-ACK du serveur, il répond par un paquet ACK. Cela garantit une connexion TCP valide entre le proxy et l'ordinateur de l'utilisateur et entre le proxy et le serveur externe.
6. Les demandes effectuées via la connexion client-proxy, puis la connexion proxy-serveur seront analysées pour garantir qu'elles sont correctes et conformes à la politique de l'entreprise jusqu'à ce que l'une ou l'autre des parties mette fin à la connexion. [40]

La figure suivante présente le firewall proxy.

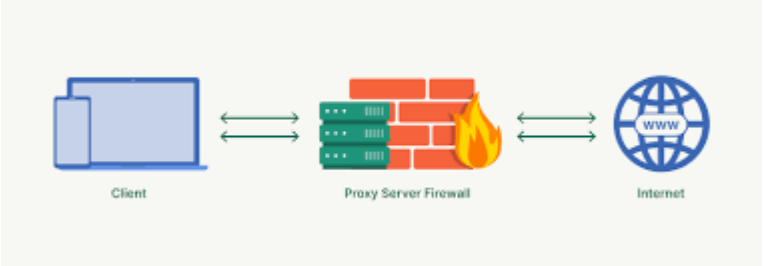

Figure II. 7 Firewall proxy

II.6.4 Firewall d'application Web

Les pares-feux d'applications web permettent de protéger les applications web contre les attaques malveillantes et le trafic Internet indésirable, notamment les robots, les injections et les dénis de service (DoS) au niveau des applications. Le WAF vous aidera à établir et à gérer des règles pour éviter les menaces Internet, notamment les adresses IP, les en-têtes HTTP, le corps HTTP, les chaînes URI, les scripts intersites (XSS), l'injection SQL et d'autres vulnérabilités définies par l'OWASP. Un pare-feu d'application web est déployé pour protéger les applications orientées vers le web et recueillir les journaux d'accès à des fins de conformité et d'analyse.

Voici quelques-unes des principales capacités et caractéristiques des WAF :

- **Routage dynamique du trafic via DNS :** tirez parti des algorithmes de routage de trafic DNS, qui tiennent compte de la latence des utilisateurs à partir de milliers d'emplacements dans le monde pour déterminer les itinéraires à plus faible latence.
- **Haute disponibilité :** lors de la configuration de la fourniture d'applications web, Oracle Cloud Infrastructure WAF offre plusieurs options de configuration à haute disponibilité avec la possibilité d'ajouter plusieurs serveurs d'origine. Ces paramètres peuvent être utilisés dans les cas où les serveurs d'origine primaires sont hors ligne ou ne répondent pas correctement aux contrôles de santé.
- **Méthodes flexibles de gestion des stratégies** : les configurations WAF vous permettent de configurer et de gérer des fonctionnalités pour répondre aux besoins de votre entreprise.
- **Surveillance et reporting :** les WAF offrent aux utilisateurs la possibilité d'accéder aux rapports liés à leur bibliothèque de contenu à des fins de conformité et d'analyse.
- **Escalade :** les informations fournies par les WAF fournissent aux équipes de support la possibilité d'émettre et de faire remonter un ticket en fonction de l'urgence. [41]

La figure suivante présente un firewall d'application web.

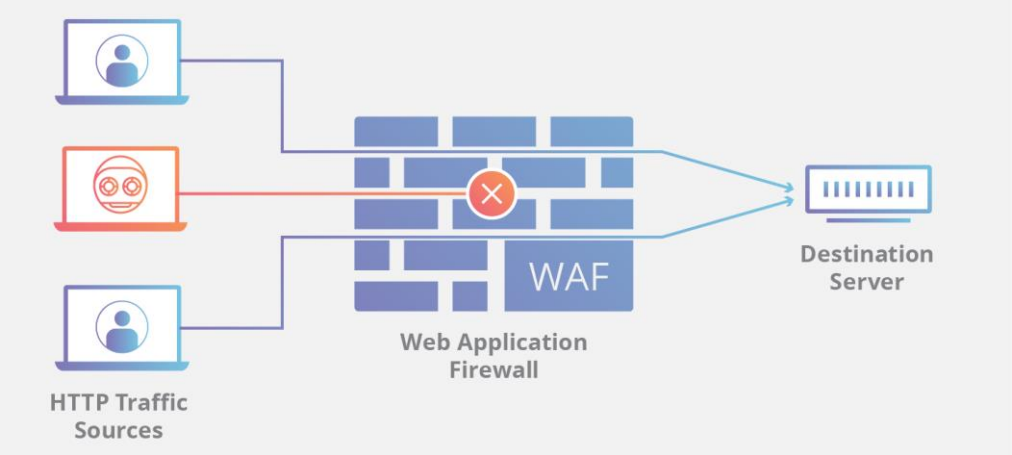

Figure II. 8 Un firewall d'application web

II.6.5 Firewalls de nouvelle génération (NGFW)

Un pare-feu de nouvelle génération (NGFW) est un dispositif de sécurité réseau qui offre des fonctionnalités allant au-delà d'un pare-feu traditionnel avec état. Alors qu'un pare-feu traditionnel fournit généralement une inspection dynamique du trafic réseau entrant et sortant, un pare-feu de nouvelle génération inclut des fonctionnalités supplémentaires telles que la

détection et le contrôle des applications, la prévention intégrée des intrusions et les informations sur les menaces fournies par le cloud.

Un pare-feu de nouvelle génération doit inclure :

- Fonctionnalités de pare-feu standard telles que l'inspection dynamique.
- Prévention intégrée des intrusions.
- Connaissance et contrôle des applications pour voir et bloquer les applications à risque.
- Sources de renseignements sur les menaces.
- Mettre à niveau les chemins pour inclure les futurs flux d'informations.
- Techniques pour faire face à l'évolution des menaces de sécurité. [42]

La figure suivante présente un firewall de nouvelle génération.

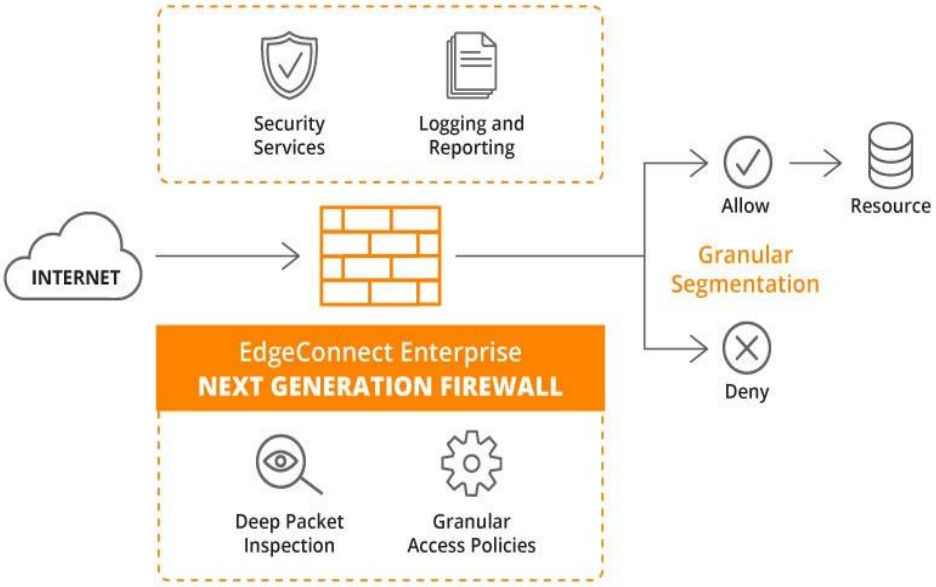

Figure II. 9 Un firewall de nouvelle génération (NGFW)

- Les mécanismes de sécurités fournis par ces types de firewalls sont adaptés pour que les administrateurs peuvent bien gérer et superviser leur environnement, on site :
- **Règle de filtrage simplifier et unifier**

Une règle de filtrage basée sur des règles utilise un ensemble de règles conditionnelles pour filtrer les données en fonction des valeurs des attributs et des actions des règles. [43]

La figure suivante présente un filtrage de firewall.

	Source		Destination		
Protocol	Address	Port	Address	Port	Action
1: tcp,	140.192.37.20,	any,	*.*.*.*,	80,	deny
2: tcp,	140.192.37.*,	any,	*.*.*.*,	80,	accept
3: tcp,	*.*.*.*,	any,	161.120.33.40,	80,	accept
4: tcp,	140.192.37.*,	any,	161.120.33.40,	80,	deny
5: tcp,	140.192.37.30,	any,	*.*.*.*,	21,	deny
6: tcp,	140.192.37.*,	any,	*.*.*.*,	21,	accept
7: tcp,	140.192.37.*,	any,	161.120.33.40,	21,	accept
8: tcp,	*.*.*.*,	any,	*.*.*.*,	any,	deny
9: udp,	140.192.37.*,	any,	161.120.33.40,	53,	accept
10: udp,	*.*.*.*,	any,	161.120.33.40,	53,	accept
11: udp,	140.192.38.*,	any,	161.120.35.*,	any,	accept
12: udp,	*.*.*.*,	any,	*.*.*.*,	any,	deny

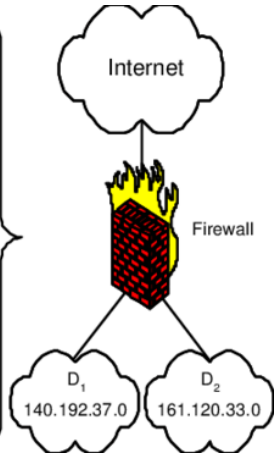

Figure II. 10 Un filtrage de firewall

- **Gestion des utilisateurs par adresses IP ou MAC**

Le filtrage des adresses MAC est plus sécurisé que le filtrage des adresses IP car les adresses MAC changent rarement. Les adresses IP des hôtes changent dans un environnement DHCP, le filtrage des adresses MAC est donc plus fiable pour identifier et filtrer la source et la destination du trafic réseau. [44]

La figure suivante présente la configuration des adresses IP ou MAC.

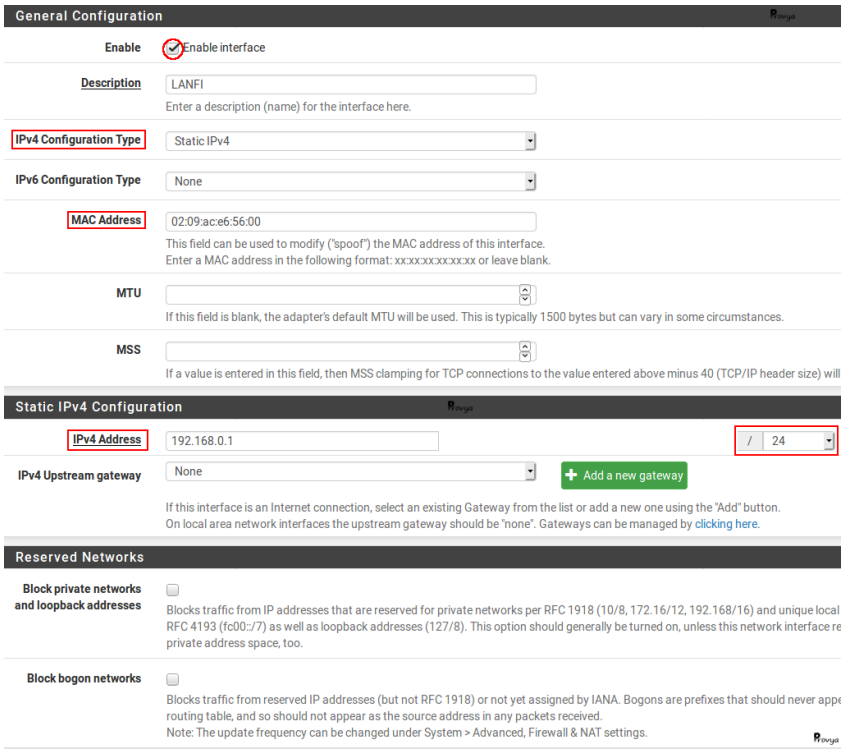

Figure II. 11 Configuration des adresses IP ou MAC

- **Fournir un portail captif**

Le portail captif a pour rôle de rediriger les utilisateurs anonymes du réseau informatique vers une page d'authentification. Ceci afin de restreindre les connexions uniquement aux utilisateurs autorisés.

Le portail captif se révèle particulièrement utile sur le réseau d'entreprise ainsi que les HotSpot, notament sans-fil (Wifi).

Plusieurs options supplémentaires viennent compléter le module d'autentification du portail captif.

Il est ainsi possible de définir :

- Le nombre de connexion simultanée
- La durée maximale d'une connexion
- La redirection d'URL
- Les modes d'authentification
- Le délai d'inactivité [45]

La figure suivante présente la mise en place d'un portail captif sous un firewall.

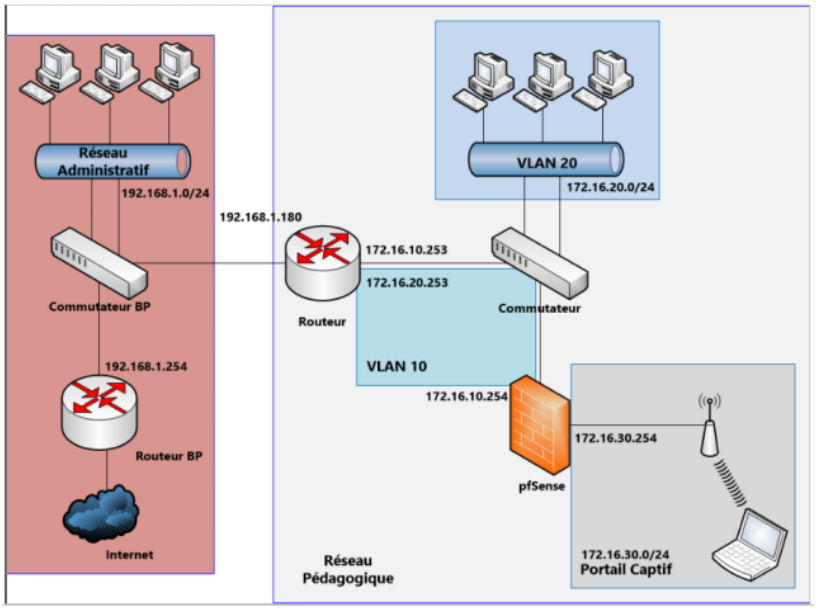

Figure II. 12 Mise en place d'un portail captif sous un firewall

- Parmi les firewalls les plus courantes au monde, nous avons choisi pfsense, alors pourquoi on a choisi pfsense ?

II.7 Définition de Pfsense

Pfsense est un dispositif gratuit, open source on peut l'utiliser comme un pare-feu ou un routeur. Il comprend une liste de fonctionnalités et un système de packages permettant de configurer selon les besoins du réseau. [46]

Pfsense idéal pour la connectivité et la protection réseau des particuliers, des travailleurs à distance, des entreprises et des fournisseurs de services :

- Équipé de nombreuses fonctionnalités de routeur et de pare-feu que l'on trouve généralement uniquement sur les routeurs commerciaux coûteux
- Options de solutions VPN flexibles
- Connu pour sa robustesse et sa stabilité
- Hautement extensible avec des packages tiers pour prendre en charge les listes de blocage, le filtrage de contenu, la prévention des intrusions, le routage basé sur des politiques, etc.
- Facile à installer et à entretenir via l'interface graphique Web
- Disponible pour le déploiement sur site et dans le cloud

- Il permet d'intégrer de nouveaux services tels que l'installation d'un portail captif, la mise en place d'un VPN, DHCP et bien d'autres, [47] comme montre la figure suivante :

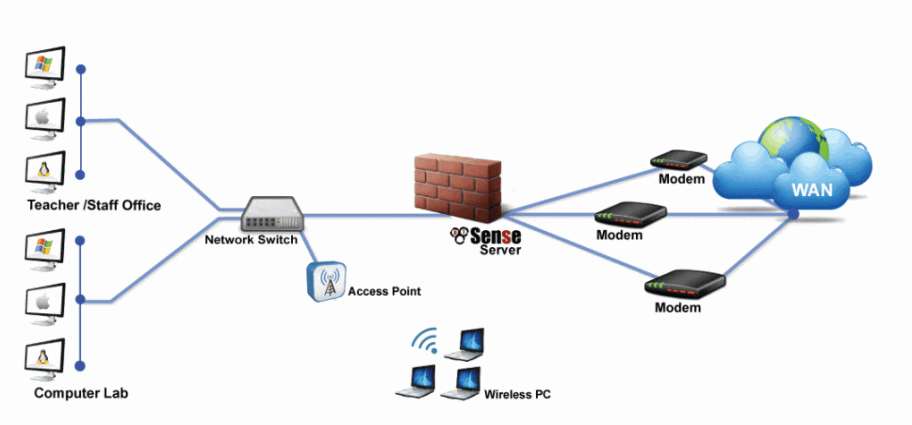

Figure II. 13 La sécurisation d'une infrastructure grâce à pfsense

II.8 Gestion des utilisateurs

Pour la gestion des utilisateurs on a utilisé le serveur Active Directory.

Active Directory :

Active Directory (AD) est un service d'annuaire destiné aux environnements Windows Server. Il s'agit d'une base de données distribuée et hiérarchisée qui partage des informations relatives à l'infrastructure permettant de localiser, de sécuriser, de gérer et d'organiser des ressources ordinateur et réseau ressources dont des fichiers, utilisateurs, groupes, périphériques et appareils réseau.

Pourquoi le choix de Active Directory ?

Mettre en place un Active Directory au sein de son entreprise compte de nombreux avantages :

- La centralisation des données des utilisateurs et des équipements matériels améliore la sécurité du réseau.
- Les administrateurs gèrent les droits d'accès à des utilisateurs ou des groupes plus facilement.
- Les administrateurs ont accès aux mises à jour des applications et des machines pour limiter les failles de vulnérabilité.
- Les entreprises disposent d'une protection contre la perte de données grâce aux réplications au sein même de la structure du contrôleur de domaine.
- Active Directory est compatible avec d'autres annuaires de ressources.

- L’administration des ressources est centralisée : les administrateurs gagnent du temps et peuvent se concentrer sur d’autres missions. [48]

Voici les principaux services qui composent Active Directory :

- Lightweight Directory Services (AD LDS):

Il s'agit d'un service d'annuaire LDAP. Il ne fournit qu'un sous-ensemble des fonctionnalités d'AD DS, ce qui le rend plus polyvalent en termes de lieu d'exécution.

- Services de certificats. :

Ce dernier permet de créer, gérer et partager des certificats de chiffrement, qui permettent aux utilisateurs d'échanger des informations en toute sécurité sur Internet.

- Active Directory Federation Services (ADFS):

Il s'agit d'une solution d'authentification unique (SSO) pour AD. Elle offre aux employés la possibilité d'accéder à plusieurs applications avec un seul ensemble d'informations d'identification, simplifiant ainsi l'expérience utilisateur.

- Services de gestion des droits (AD RMS) :

Cet ensemble d'outils aide à la gestion des technologies de sécurité qui aideront les organisations à sécuriser leurs données. Ces technologies comprennent le cryptage, les certificats et l'authentification. Elles couvrent une gamme d'applications et de types de contenu, tels que les courriels et les documents Word. [49]

La figure suivante montre comment le serveur Active directory géré les utilisateurs.

Figure II. 14 Active Directory

II.9 Conclusion

Au cours de ce chapitre, nous avons pris connaissance des différents aspects liés à la sécurité des réseaux informatiques, nous avons découvert les attaques qui menacent cette dernière et comment se protéger afin de réduire les intrusions et attaques des pirates. Nous avons étudié

les différents types de pare-feu, leurs fonctions et leurs avantages. Nous avons étudié également Active Directory. La sécurité des systèmes informatiques est vitale pour le bon fonctionnement des systèmes d'information. Il est donc nécessaire d'assurer sa protection. Dans le chapitre suivant, nous débuterons la mise en place du pare-feu pfsense.

Chapitre III Conception et réalisation

III Introduction

Dans ce chapitre, nous étudierons la mise en œuvre d'un modèle de réseau pour Sonatrach à l'aide d'EVE-NG, nous verrons comment l'utilisation de Pfsense peut contribuer à améliorer la défense contre les attaques externes, en mettant en évidence les fonctionnalités avancées de ce pare-feu open source, et nous discuterons de la configuration, de l'architecture et des implications pratiques de cette solution pour assurer la sécurité et l'efficacité du réseau de l'entreprise. Nous examinerons également les avantages de Pfsense en termes de flexibilité et de personnalisation des politiques de sécurité, ainsi que sa capacité à fournir une surveillance en temps réel et une journalisation des événements pour détecter et contrer les tentatives d'intrusion ou d'activités malveillantes.

III.1 Présentation de l'organisme d'accueil

La division d'exploration issue de la restauration de l'entreprise nationale SONATRACH octobre1972.D'une direction exploration c'est des divisions les plus importantes de la SONATRACH vu les succès des travaux de recherche et d'exploitation effectues dans le domaine minier Algérie pour cela SONATRACH investi 24 % de ces bénéficier dans l'exploitation.

Elle est composée de dix districts ont pour mission conduire et de développement des activités de prospection et de recherche d'hydrocarbures englobant la production, L'ingénierie pétrolier et le forage.

III.2 Organigramme de l'entreprise

La figure suivante montre l'organigramme de l'entreprise « EXPLORATION SONATRACH »

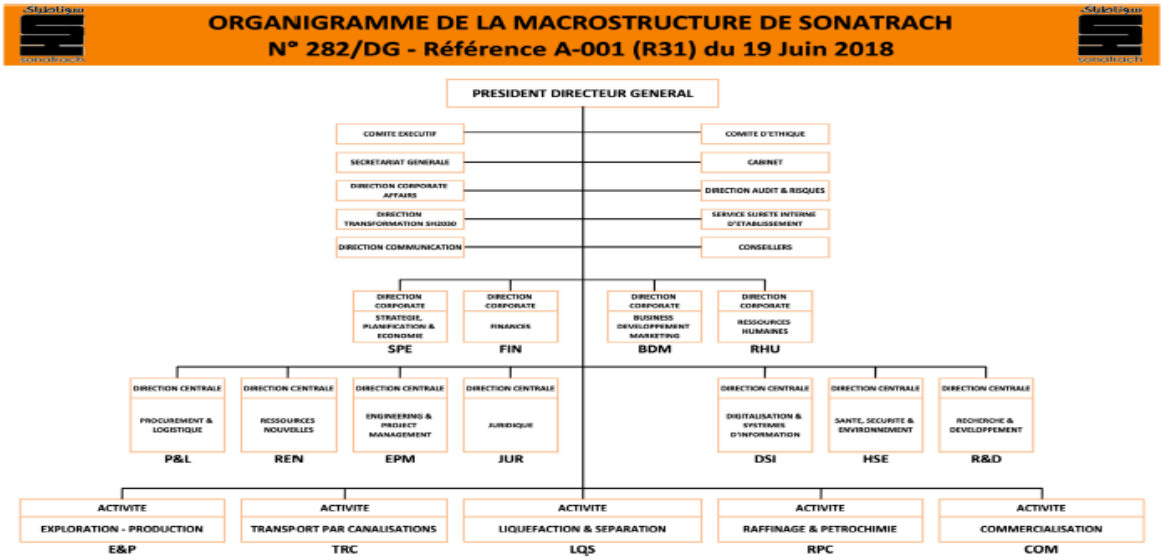

Figure III 1 L'organigramme de l'entreprise

III.3 Les missions de la division exploration de Boumerdes

La division exploration été rune des divisions opérationnels de l'activité amont de l'entreprise SONATRACH et pour missions principales de :

- Conduire et de développer les activités de prospection et de recherche des Hydrocarbures.
- Participer avec les autres Divisions aux appels d'offres d'exploration en Algérie et à l'étranger.
- Participer à l'évaluation des offres de partenariats sur des projets d'exploration en Algérie et à l'‘étranger.
- La mise en œuvre de la stratégie de l'entreprise en matière d'exploration.
- Préparer, établir et recommander les programmes techniques d'exploration et leur suivi.
- Gérer et suivre les contrats en propre et en association.
- Développer et conduire les travaux d'analyse en matière de géologie et de géophysique.
- Développer l'expertise dans le domaine de I ‘exploration.

III.4 Présentation du projet

Le thème intitulé « Conception et déploiement d'une architecture réseau à base de pfsense », vise à sécuriser le réseau de la division Exploration de Boumerdès en mettant en place un firewall logiciel.

Le projet consiste à faire une étude pour une mise en place d'un type de Firewall « pfsense » pour la sécurisation du réseau LAN de l'entreprise.

III.5 Architecture déployée

Dans ce qui suit, nous allons fournir des directives concernant la configuration et la mise en place d'un réseau LAN sécurisé dans le but de comprendre le déploiement des solutions de sécurité Pfsense. L'infrastructure est composée de deux départements (finance et technique) qui auront des comptes dans le gestionnaire des utilisateurs (Active Directory). Ces comptes seront interconnectés via une communication de niveau 3 passant par le pare-feu Pfsense. Ainsi, pour qu'un utilisateur puisse accéder au réseau, il devra disposer d'un compte dans l'Active Directory et être membre du domaine de l'entreprise. Cela permettra la gestion et la supervision des utilisateurs, ainsi que la limitation de leurs accès au réseau.

Les équipements déployés dans cette architecture (Figure III.1) sont les suivants :

- 2 commutateurs d'accès Cisco (ACC_1 et ACC_2) pour connecter les utilisateurs des deux départements.
- 2 commutateurs Cisco Nexus (TOR_1 et TOR_2) pour interconnecter la partie serveurs au LAN (connectés en VPC).
- 2 commutateurs de distribution (DEST_1 et DEST_2) Cisco pour connecter les deux parties serveur et accès au pare-feu.
- 2 pare-feu Pfsense en haute disponibilité pour la sécurité du réseau.
- 3 PC (Windows 10) pour les utilisateurs du département technique et 3 autres PC (Windows 10) pour les utilisateurs du département finance.
- 1 serveur Windows pour l'intégration de l'Active Directory.

La figure III.2 présente la topologie déployée :

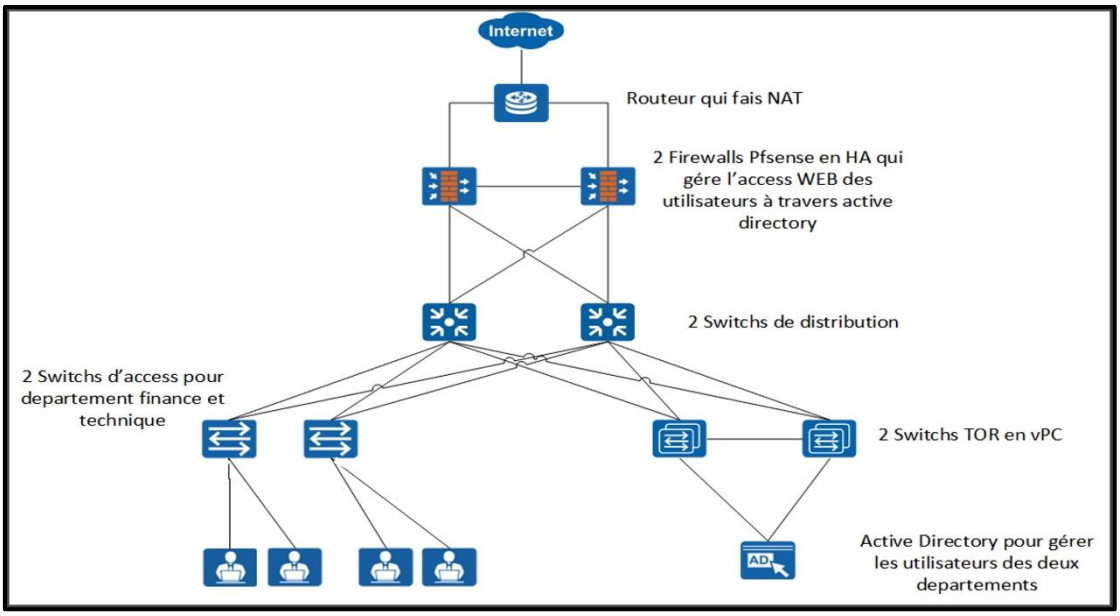

Figure III 2Architecture de l'entreprise

III.6 Planification des Ports

Le tableau suivant montre la planification et la répartition des équipements.

Equipements	Ports	Description	Types de ports	Paramètres de Vlans
ACC_1	G0/0	TO_DST02_P03	Trunk	Native = 1 Allowpass vlan 10,30
	G0/1	TO_DST01_P03	Trunk	Native = 1 Allowpass vlan 10,30
	G0/2	TO_WIN15	Access	Vlan 10
	G0/3	TO_WIN14	Access	Vlan 10
ACC_2	G0/0	TO_DST02_P02	Trunk	Native = 1 Allowpass vlan 20,30
	G0/1	TO_DST01_P02	Trunk	Native = 1 Allowpass vlan 20,30

	G1/0	TO_WIN18	Access	Vlan 20
	G0/3	TO_WIN17	Access	Vlan 20
DEST_1	G0/0	TO_FW02_P02	Trunk	Natrive = 1 Vlan 10,20,30
	G0/1	TO_FW01_P04		Natrive = 1 Vlan 10,20,30
	G0/2	TO_ACC02_P01		Natrive = 1 Vlan 20,30
	G0/3	TO_ACC01_P01		Natrive = 1 Vlan 10,30
	G1/0	TO_TOR01_P02	Etherchannel Trunk	Natrive = 1 Vlan 10,20,30
	G1/1	TO_TOR02_P02		Natrive = 1 Vlan 10,20,30
DEST_2	G0/0	TO_FW02_P04	Trunk	Natrive = 1 Vlan 10,20,30
	G0/1	TO_FW01_P02		Natrive = 1 Vlan 10,20,30
	G0/2	TO_ACC02_P00		Natrive =

				1 Vlan 20,30
	G0/3	TO_ACC01_P00		Natrive = 1 Vlan 10,30
	G1/0	TO_TOR01_P03	Etherchannel Trunk	Natrive = 1 Vlan 10,20,30
	G1/1	TO_TOR02_P03		Natrive = 1 Vlan 10,20,30
TOR_1	E1/1	TO_AD	Etherchanel Trunk	
	E1/2	TO_DST01_P1_0	Etherchanel Trunk	Natrive = 1 Vlan 10,20,30
	E1/3	TO_DST02_P1_0	Etherchanel Trunk	
	E1/5	VPC_PEER_LINK	Etherchanel Trunk	
	E1/6			
	E1/7	VPC_PEER_KEEPALIVE	Access	Vlan 23
TOR_2	E1/1	TO_AD	Etherchanel Trunk	
	E1/2	TO_DST01_P1_1	Etherchanel Trunk	Natrive = 1 Vlan 10,20,30
	E1/3	TO_DST02_P1_1	Etherchanel Trunk	
	E1/5	VPC_PEER_LINK	Etherchanel Trunk	
	E1/6			
	E1/7	VPC_PEER_KEEPALIVE	Access	Vlan 23

Tableau III 1 Planification et répartition des équipements

III.7 Planification des adresses IPs

Le tableau suivant décrit les adresses IP de chaque équipement

Equipements	Interfaces	Address IP	Remarques
TOR_1	Vlan23	10.10.10.1/30	VPCInterconnection
TOR_2	Vlan23	10.10.10.2/30	
Pfsense_1	Vtnet0	10.1.1.1/30	HA Peer link
Pfsense_2	Vtnet0	10.1.1.2/30	
Pfsense_HA	Vlan 10	172.16.10.254/24	Floating IP addresses
	Vlan 20	172.16.20.254/24	
	Vlan 30	172.16.30.254/24	
Pfsense_1	Vtnet 3	172.16.5.21/24	WAN Interfaces
Pfsense_2	Vtnet 3	172.16.6.17/24	
NAT_ROUTER	G0/1	172.16.6.18/24	TO Pfsense
	G0/2	172.16.5.22/24	
	G0/0	192.168.1.186/24	NAT adresse

Tableau III 2 Planification des adresses IPs

III.8 Planification des Vlans

Le tableau suivant montre la planification des Vlans dans ce projet.

VLAN	Description
10	Departement Finance
20	Departement Technique
23	VPCpeerlink
30	Active Directory

Tableau III 3 Planification des Vlans

III.9 Etapes et procédure de la configuration

Pour réaliser notre architecture avec succès, voici une approche étape par étape :

III.9.1 Etapes de Configuration

1. Configurer la connectivité entre les différents équipements
2. Installation de l'AD.
3. Installation des firewalls Pfsense.
4. Configuration de système HA dans les firewalls.

5. Application des règles de sécurité.
6. Configuration duvPC pour les switchs TOR.
7. Configuration du NAT dans le router.
8. Configuration des utilisateurs dans l'Active Directory.
9. Intégration de l'active directory avec les firewalls et les PC.
10. Test de connexion multiple.

III.9.2 Procédure de la Configuration

Pour configurer les switchs accès, les switchs destribution, les switchs TOR et le routeur on passe par les étapes suivantes :

Étape 1 : Configuration de switches d'accès

Dans cette partie nous configurons les switches d'accès pour donner l'accès au réseau pour les utilisateurs des départements, nous configurons les VLANs nécessaires avec les types de ports déjà décrit dans le tableau

Nommer et ajouter levlan 10 au niveau du switch ACC_1

```
Switch> enable.
Switch# Configure terminal.
Switch(config)#hostname ACC_1
ACC_1(config)#vlan 10
ACC_1(config-vlan) #Description Departement_Finance
```

Figure III 3Switch accès 1 : création des vlans

Nommer et ajouter le vlan 20 au niveau du switch ACC_2

```
Switch> enable.
Switch# Configure terminal.
Switch(config)#hostname ACC_2
ACC_2(config)#vlan 20
ACC_2(config-vlan) #Description Departement_TECH
```

Figure III 4 Switch accès 2 : création des vlans

Configurez le type d'interface de liaison Downlink et Uplink sur lesswitches ACC_1 et le switch ACC_2 et les VLAN autorisés pour l'interface.

Remarque :

Les port downlink sont les ports connectésaux utilisateurs, et uplink qui se dirige vers l'internet

- Configuration des ports accès du switch ACC_1 :

```
ACC_1(config)#interface range g0/2-3
ACC_1(config-if-range) #switchport mode access
ACC_1(config-if-range) #switchport access vlan10
ACC_1(config-if-range) #exit
```

Figure III 5Switch accès 1 : configuration des liens accès

- Configuration des ports Access de switch ACC_2 :

```
ACC_2(config)#interface g0/3
ACC_2(config-if) #switchport mode access
ACC_2(config-if) #switchport access vlan20
ACC_2(config-if) #exit
ACC_2(config)#interface g1/3
ACC_2(config-if) #switchport mode access
ACC_2(config-if) #switchport access vlan20
ACC_2(config-if) #exit
```

Figure III 6Switch accès 2 : configuration des liens accès

- Configuration des ports trunk de switch ACC_1 :

```
ACC_1(config)#interface range g0/0-1
ACC_1(config-if-range) #switchport trunk encapsulation dot1Q
ACC_1(config-if-range) #switchport mode trunk
ACC_1(config-if-range) #switchport allowed vlan 10
ACC_1(config-if-range) #exit
```

Figure III 7Switch accès 1 : configuration des liens trunk

- Configuration des ports trunk de switch ACC_2 :

```
ACC_2(config)#interface range g0/0-1
ACC_2(config-if-range) #switchport trunk encapsulation dot1Q
ACC_2(config-if-range) #switchport mode trunk
ACC_2(config-if-range) #switchport allowed vlan 20
ACC_2(config-if-range) #exit
```

Figure III 8Switch accès 2 : configuration des liens trunk

- Vérification du la configuration dans le switch ACC_1 :

```
ACC_1#show running-config
```

Figure III 9 ACC_1 : La commande de vérification de la configuration

La figure suivante montre la configuration de switch ACC_1 :

Figure III 10 Vérification de la configuration de switch ACC_1

- Vérification du la configuration dans le switch ACC_2 :

```
ACC_2#show running-config
```

Figure III 11ACC_2 : La commande de vérification de la configuration

La figure suivante montre la configuration de switch ACC_2 :

```
!
interface GigabitEthernet0/0
 switchport trunk allowed vlan 20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet0/2
 negotiation auto
!
interface GigabitEthernet0/3
 switchport access vlan 20
 switchport mode access
 negotiation auto
!
interface GigabitEthernet1/0
 switchport access vlan 20
 switchport mode access
 negotiation auto
!
```

Figure III 12Vérification de la configuration de switch ACC_2

Étape 2 : Configuration des switches de distribution

Création de vlan 10, vlan 20 et vlan 30 au niveau du switch DESTRIBUTION 1

```
Switch> enable.
Switch# Configure terminal.
Switch(config)#hostname DESTRIBUTION 1
DESTRIBUTION 1 (config)#VLAN 10
DESTRIBUTION 1 (config-VLAN) # name Departement_Finance
DESTRIBUTION 1 (config-VLAN) # exit
DESTRIBUTION 1 (config)#VLAN 20
DESTRIBUTION 1 (config-VLAN) #name Departement_TECH
DESTRIBUTION 1 (config)#VLAN 30
DESTRIBUTION 1 (config-VLAN) #name AD
```

Figure III 13Switch destribution 1 : création des vlans

Création de vlan 10, vlan 20 et vlan 30au niveau du switch DESTRIBUTION 2

```
Switch> enable.
Switch# Configure terminal.
```

```
Switch(config)#hostname DESTRIBUTION 2
DESTRIBUTION 2 (config)#VLAN 10
DESTRIBUTION 2 (config-VLAN) # name Departement_Finance
DESTRIBUTION 2 (config-VLAN) # exit
DESTRIBUTION 2 (config)#VLAN 20
DESTRIBUTION 2 (config-VLAN) # name Departement_TECH
DESTRIBUTION 2 (config)#VLAN 30
DESTRIBUTION 2 (config-VLAN) #name AD
```

Figure III 14Switch destribution 2 : création des vlans

- Vérification du la configuration dans le switch DESTRIBUTION 1 :

```
DESTRIBUTION 1#show running-config
```

La figure suivante montre la configuration de switch DESTRBUTION1

```
!
interface Port-channel12
 switchport trunk allowed vlan 10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/0
 switchport trunk allowed vlan 10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
```

```
!
interface GigabitEthernet0/3
 switchport trunk allowed vlan 10,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet1/0
 switchport trunk allowed vlan 10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
 channel-group 12 mode active
!
interface GigabitEthernet1/1
 switchport trunk allowed vlan 10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
```

Figure III 15 Vérification de la configuration de switch destribution1

- Vérification du la configuration dans le switch DESTRIBUTION 2 :

```
DESTRIBUTION 2#show running-config
```

Figure III 16 vérification de configuration

La figure suivante montre la configuration de switch DESTRIBUTION 2 :

```
!
interface Port-channel13
 switchport trunk allowed vlan 10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/0
 switchport trunk allowed vlan 10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
```

```
!
interface GigabitEthernet0/3
 switchport trunk allowed vlan 10,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
!
interface GigabitEthernet1/0
 switchport trunk allowed vlan 10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
 channel-group 13 mode active
!
interface GigabitEthernet1/1
 switchport trunk allowed vlan 10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 negotiation auto
 channel-group 13 mode active
!
```

Figure III 17 Vérification de la configuration de switch destribution 2

Étape 3 : Configuration du vPC dans les switches TOR

Création de vlan 10, vlan 20 et vlan 30 au niveau du switch TOR 1

```
Switch> enable.
Switch# Configure terminal.
Switch(config)#hostname TOR 1
TOR 1 (config)#VLAN 10
TOR 1 (config-VLAN) #name Departement_Finance
TOR 1 (config-VLAN) # exit
TOR 1 (config)#VLAN 20
TOR 1 (config-VLAN) # name Departement_TECH
TOR 1 (config)#VLAN 23
TOR 1 (config-VLAN) # name Keepalive
TOR 1 (config)#VLAN 30
TOR 1 (config-VLAN) # Description AD
```

Figure III 18 Switch TOR1 : création des vlans

Création de vlan 10, vlan 20 et vlan 30 au niveau du switch TOR 2

```
Switch> enable.
Switch# Configure terminal.
Switch(config)#hostname TOR 2
TOR 2 (config)#VLAN 10
TOR 2 (config-VLAN) #name Departement_Finance
TOR 2 (config-VLAN) # exit
TOR 2 (config)#VLAN 20
TOR 2 (config-VLAN) # name Departement_TECH
TOR 1 (config)#VLAN 23
TOR 1 (config-VLAN) # name Keepalive
TOR 2 (config)#VLAN 30
TOR 2 (config-VLAN) #name AD
```

Figure III 19 Switch TOR2 : création des vlans

Activation des protocoles Nécessaires dans les deux switches :

```
TOR 1(config)#FeaturevPC
TOR 1(config)#Feature lacp
TOR 1(config)#Feature interface-vlan
```

Figure III 20Switch TOR1: Activation des Features

```
TOR 2(config)#FeaturevPC
TOR 2(config)#Feature lacp
TOR 2(config)#Feature interface-vlan
```

Figure III 21Switch TOR2: Activation des Features

- Sur le premier commutateur, nous **c**réons le VLAN 23 avec une adresse IP à l'interface VLAN et en faisons un membre de l'instance VRF créée à cet effet. Nous complétons la configuration en attribuant Ethernet 1/7 au VLAN 23 :

```
TOR 1 (config)#VLAN 23
TOR 1 (config-VLAN) # name keepalive
TOR 1(config-vrf) #vrf context keepalive
TOR 1(config-vrf) #interface Ethernet 1/7
TOR 1(config-if) #switchport mode access
TOR 1(config-if) #switchport access vlan23
TOR 1(config-if) #exit
TOR 1(config)#interface vlan 23
TOR 1(config-if) #ip address 10.10.10.1/30
TOR 1(config-if) #no shutdown
TOR 1(config-if) #vrf member keepalive
TOR 1(config-if) #ip address 10.10.10.1/30
TOR 1(config-if) #no shutdown
```

Figure III 22Switch TOR1: Configuration de VRF

Nous suivons les mêmes étapes de configuration sur notre commutateur Nexus secondaire :

```
TOR 2(config)#VLAN 23
TOR 2(config-VLAN) # name keepalive
TOR 2(config-vrf) #vrf context keepalive
TOR 2(config-vrf) #interface Ethernet 1/7
TOR 2(config-if) #switchport mode access
TOR 2(config-if) #switchport access vlan23
TOR 2(config-if) #exit
TOR 2(config)#interface vlan 23
TOR 2(config-if) #ip address 10.10.10.2/30
TOR 2(config-if) #no shutdown
TOR 2(config-if) #vrf member keepalive
TOR 2(config-if) #ip address 10.10.10.2/30
TOR 2(config-if) #no shutdown
```

Figure III 23Switch TOR2: Configuration de VRF

Le test de connectivité ping entre les liens Peer Keepalive est réussi :

```
TOR 1 #ping 10.10.10.2 vrfkeepalive
```

Figure III 24Switch TOR1 : Test de la connectivité entre les liens peerkeepalive

Établir le lien Keepalive entre homologues vPC :

```
TOR1(config)#vpc domain 10
TOR1(config-vpc-domain)   #peer-keepalive   destination   10.10.10.2   sources
10.10.10.1 vrfkeepalive
```

Figure III 25 Switch TOR1 : Etablissement de lien keepalive entre homloguesvPC

Nous suivons les mêmes étapes de configuration sur notre commutateur Nexus secondaire :

```
TOR2(config)#vpc domain 10
TOR2(config-vpc-domain)   #peer-keepalive   destination   10.10.10.1   source
10.10.10.2 vrfkeepalive
```

Figure III 26Switch TOR2 : Etablissement de lien keepalive entre homloguesVpc

Configurer le vPC Peer-Link :

```
TOR 1(config)# int e1/5-6
TOR 1(config-if) # channel-group23 mode active
TOR 1(config-if-range) #ex
TOR 1(config)#int port-channel 23
TOR 1(config-if) #switchport mode trunk
TOR 1(config-if) #switchport trunk allowed vlan 10,20,30
TOR 1(config-if) #vpc peer-link
TOR 1(config-if) #spanning-tree port type network
```

Figure III 27 Switch TOR1: Configuration deVpcPerr-Link

Une configuration identique suit pour notre switch secondaire :

```
TOR 2(config)# int e1/5-6
TOR 2(config-if) # channel-group23 mode active
TOR 2(config-if-range) #ex
```

```
TOR 2(config)#int port-channel 23
TOR 2(config-if) #switchport mode trunk
TOR 2(config-if) #switchport trunk allowed vlan 10,20,30
TOR 2(config-if) #vpc peer-link
TOR 2(config-if) #spanning-tree port type network
```

Figure III 28 Switch TOR2: Configuration deVpcPerr-Link

Nous pouvons effectuer une vérification finale sur notre vPC à l'aide de la commande show vpc :

```
TOR 1 #show vpc
```

Figure III 29 Switch TOR1 : Vérification de la configuration

Les figures III29 et III30 montrent la configuration de VPC :

```
TOR 1# sh vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : failed
Type-2 inconsistency reason       : SVI type-2 configuration incompatible
vPC role                          : primary
Number of vPCs configured         : 3
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Disabled

vPC Peer-link status
---------------------------------------------------------------------
id    Port   Status Active vlans
--    ----   ------ --------------------------------------------------
1     Po23   up     10,20,30
```

Figure III 30TOR1 : Vérification de la configuration de VPC

```
vPC Peer-link status
---------------------------------------------------------------------
id    Port   Status Active vlans
--    ----   ------ --------------------------------------------------
1     Po23   up     10,20,30


vPC status
----------------------------------------------------------------------------
Id    Port          Status Consistency Reason                Active vlans
--    ------------  ------ ----------- ------                ---------------
11    Po11          up     success     success               10,20,30


12    Po12          up     success     success               10,20,30


13    Po13          up     success     success               10,20,30



Please check "show vpc consistency-parameters vpc <vpc-num>" for the
consistency reason of down vpc and for type-2 consistency reasons for
any vpc.

TOR 1#
```

Figure III 31TOR1 : Vérification de la configuration de VPC (suite)

Vérification du vPC sur l'homologue secondaire :

```
TOR 2 #show vpc
```

Figure III 32 Switch TOR2 : Vérification de la configuration

La figurent III31et III32 montrent la vérification de la configuration de VPC :

```
TOR 2# sh vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 10
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : failed
Type-2 inconsistency reason       : SVI type-2 configuration incompatible
vPC role                          : secondary
Number of vPCs configured         : 3
Peer Gateway                      : Disabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Disabled

vPC Peer-link status
--------------------------------------------------------------------
id    Port   Status Active vlans
--    ----   ------ --------------------------------------------------
1     Po23   up     10,20,30
```

Figure III 33TOR2 : Vérification de la configuration de VPC

```
vPC Peer-link status
--------------------------------------------------------------------
id    Port   Status Active vlans
--    ----   ------ --------------------------------------------------
1     Po23   up     10,20,30


vPC status
----------------------------------------------------------------------------
Id    Port          Status Consistency Reason                Active vlans
--    ------------  ------ ----------- ------                ---------------
11    Po11          up     success     success               10,20,30


12    Po12          up     success     success               10,20,30


13    Po13          up     success     success               10,20,30



Please check "show vpc consistency-parameters vpc <vpc-num>" for the
consistency reason of down vpc and for type-2 consistency reasons for
any vpc.

TOR 2#
```

Figure III 34TOR 2 ; Vérification de la configuration de VPC (suite)

Nous sauvegardons la configuration à l'aide de la commande :

```
TOR 1 #copy running-config startup-config.
```

Figure III 35 Switch TOR1 : Sauvegarder la configuration

Sauvegarde de la configuration dans l'homologue secondaire :

```
TOR 2 #copy running-config startup-config.
```

Figure III 36Switch TOR2 : Sauvegarder la configuration

III.10 Installation de pfsense

Pfsense choisira le mode de démarrage

On clique sur start pour démarrer l'installation de Pfsense. La fenêtre suivante s'affiche.

On choisit le 1er choix, comme montre la figure suivante :

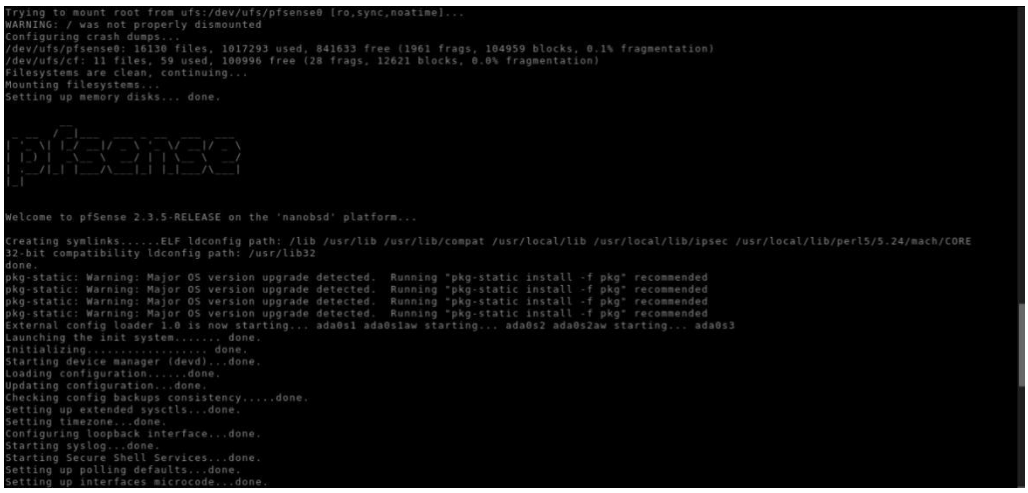

Figure III 37 Pfsense-installation : mode de démarrage

Assignation des interfaces :

On voit bien nos quatre interfaces réseaux (WAN, LAN, OPT1 et OPT2), comme montre la figure suivante :

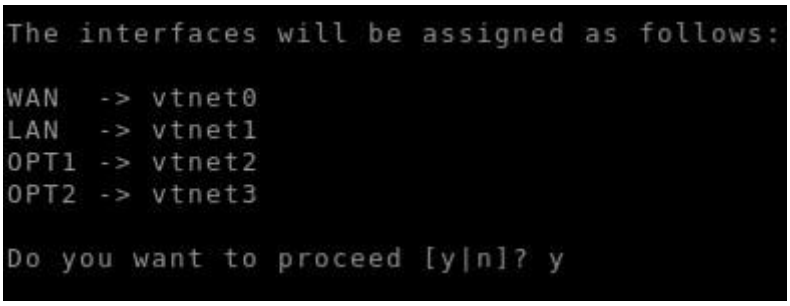

Figure III 38Pfsense : assignation des interfaces réseaux

Installation se termine ici :

L'attribution d'une IP adresses concernant le LAN est attribué statiquement par défaut qui est 192.168.1.1 pour la gestion des firewalls, comme montre la figure suivante :

Figure III 39 Pfsense : Installation terminé

1. Pour accéder à l'interface web de configuration de PfSense, on utilise l'adresse IP de l'interface LAN : http://192.168.1.1. La page suivante s'affiche :

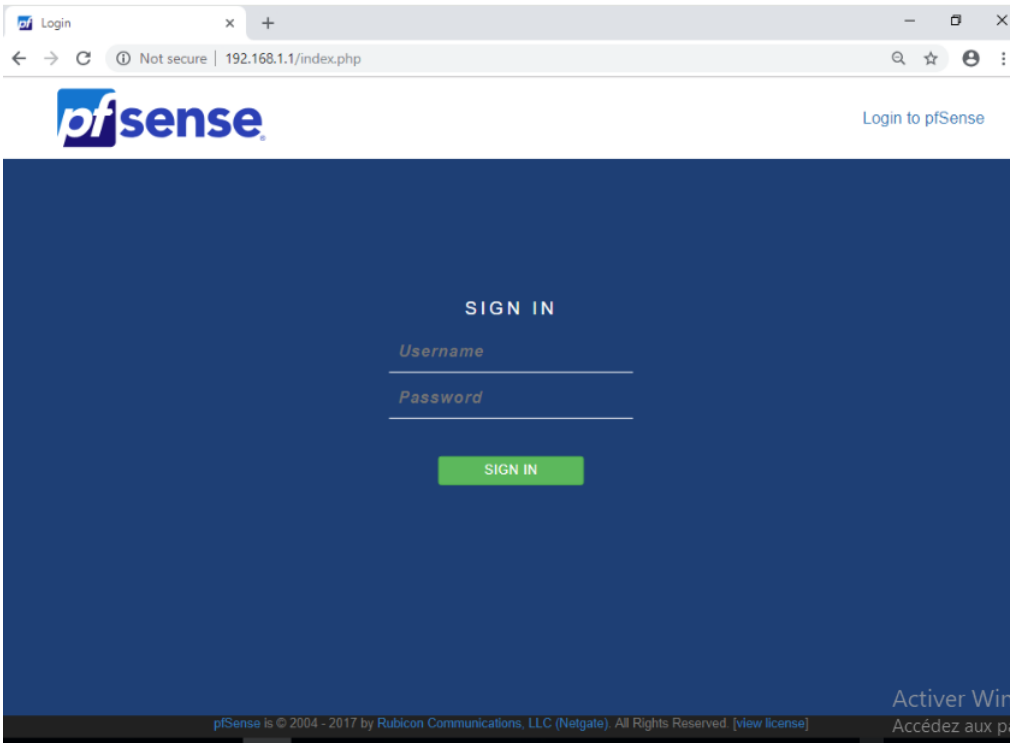

Figure III 40 Page d'identification de pfsense

Les identifiants par défaut de pfsense sont les suivants :

- Username : admin
- Password : pfsense

Après une connexion réussie, vous serez envoyé au tableau de bord Pfsense.

III.11 Configuration des interfaces physiques de pfsense

Une interface physique correspond à une carte réseau du serveur pfsense.

Ces interfaces sont nommées en fonction de leur driver. Par exemple : vtnet0, vtnet1, vtnet3, etc. Elles sont identifiées par leur adresse MAC.

Lors de l'installation de pfsense, il est proposé de configurer les interfaces. Ce sont des interfaces logiques. Elles sont créées, configurées et associées aux interfaces physiques.

Ainsi, dans le cas d'un pfsense disposant de deux interfaces (une interface LAN et une interface WAN), on pourrait avoir l'association suivante :

WAN [interface logique] = vtnet0 [port réseau]

LAN [interface logique] = vtnet1 [port réseau]

Il est également possible de retrouver cette association depuis le menu Interfaces >Assignements : [50]

❖ La configuration de l'interface WAN :

Les étapes de la configuration :

1. Accéder à Interfaces | WAN.
2. Cocher Activer l'interface.
3. Choisirle type de configuration d'adresse par statique IPv4.
4. Laisser le reste des paramètres par défaut.[51]

   La figure suivante montre la configuration de WAN :

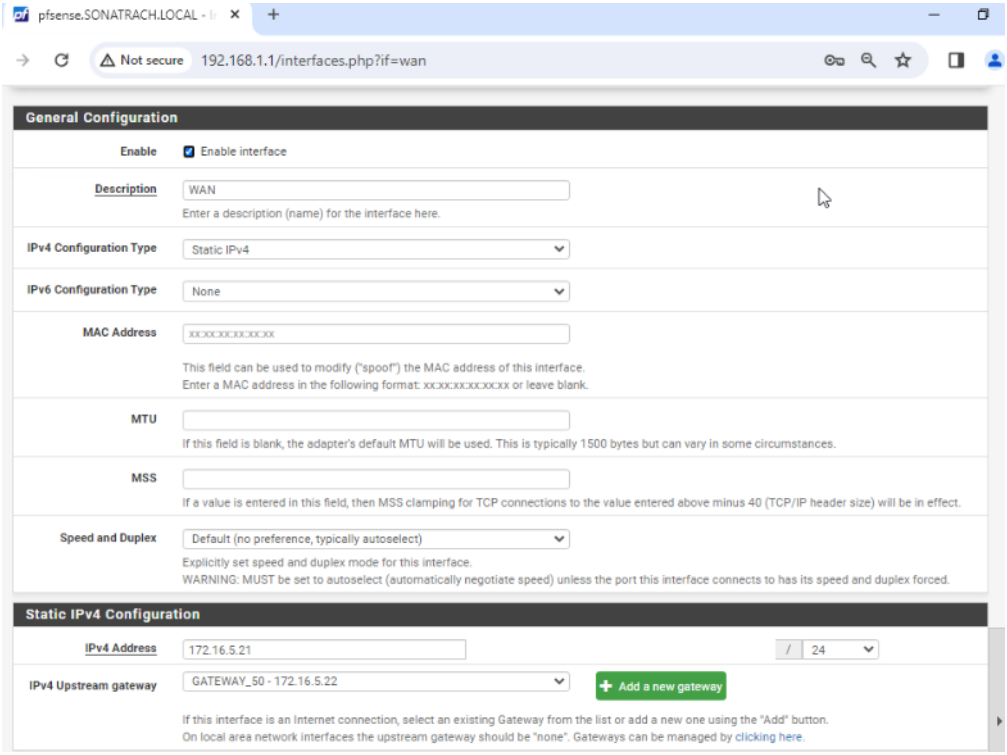

Figure III 41 Configuration de l'interface WAN

- Pfsense 1 (active) :

De même les interfaces seront configurées comme suit dans le firewall 1, comme montre la figure suivante :

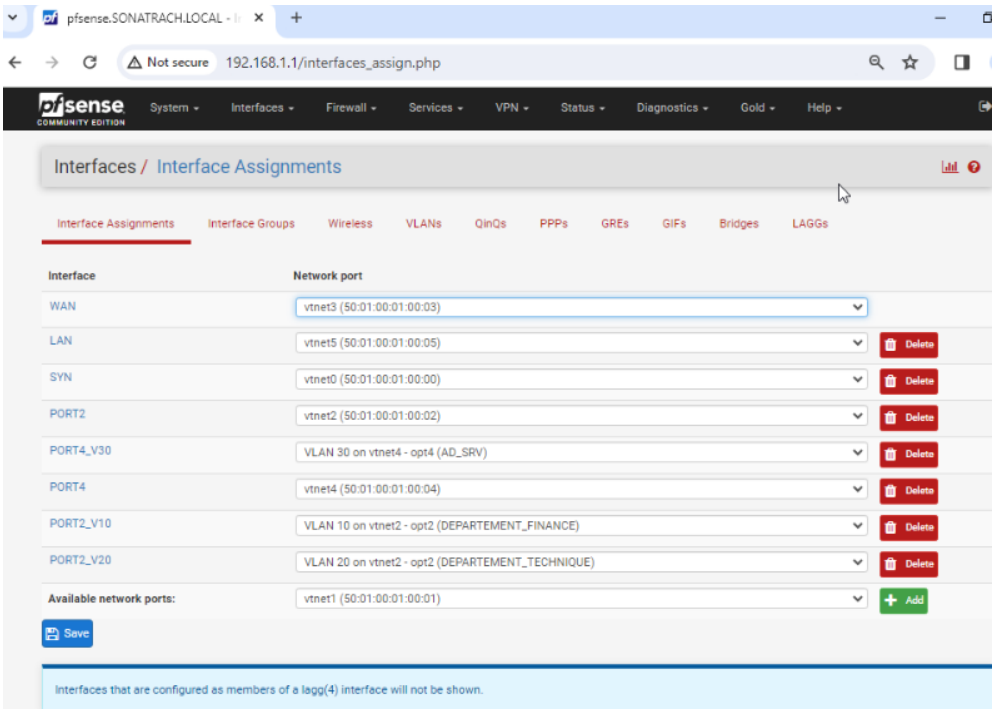

Figure III 42 Configuration des interfaces de pfsense1

- Pfsense 2 (passive) :

De même les interfaces seront configurées comme suit dans le firewall 2.

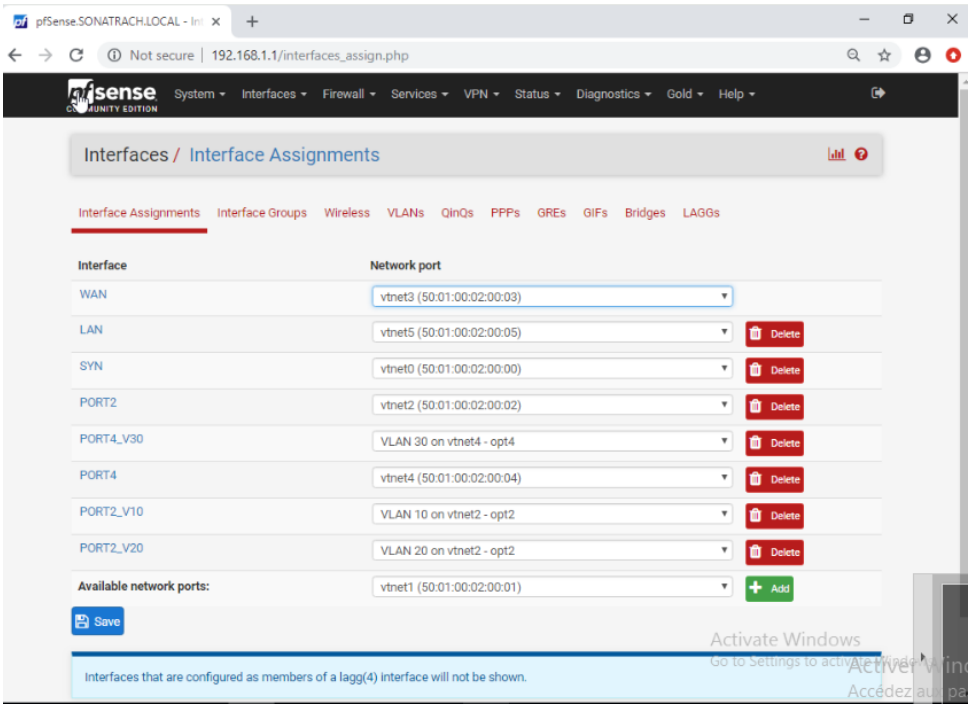

Figure III 43 Configuration des interfaces de Pfsense 2

III.12 Configuration de la haute disponibilité

Pour configurer la haute-disponibilité, il faut préciser le firewall maitre du secondaire, pour que le firewall primaire synchronise ces données et configuration au secondaire ; Pour cela, nous configurons les paramètres de synchronisation comme le montre la figure suivante :

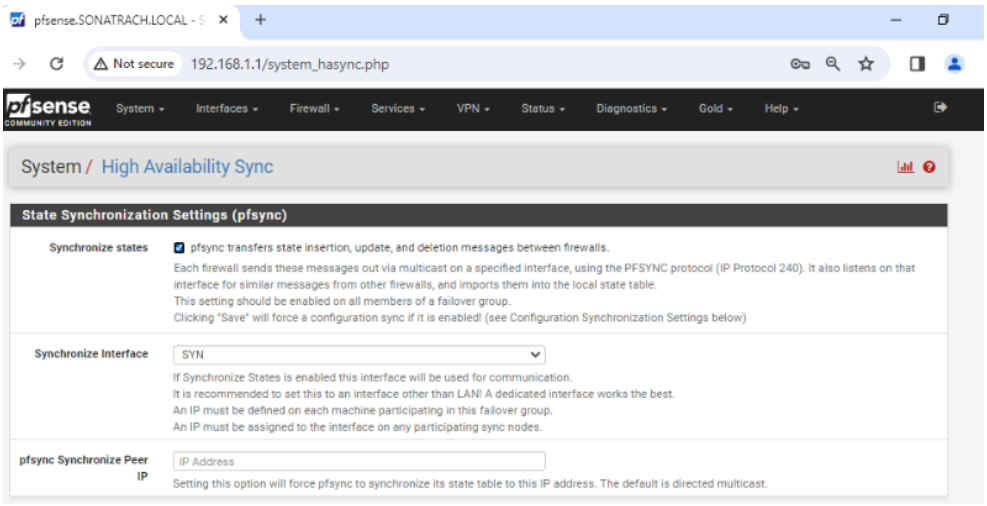

Figure III 44 La configuration de pfsync

La figure III.35 montre l'activation du paramètre de synchronisation (synchronize states) via l'interface SYN.

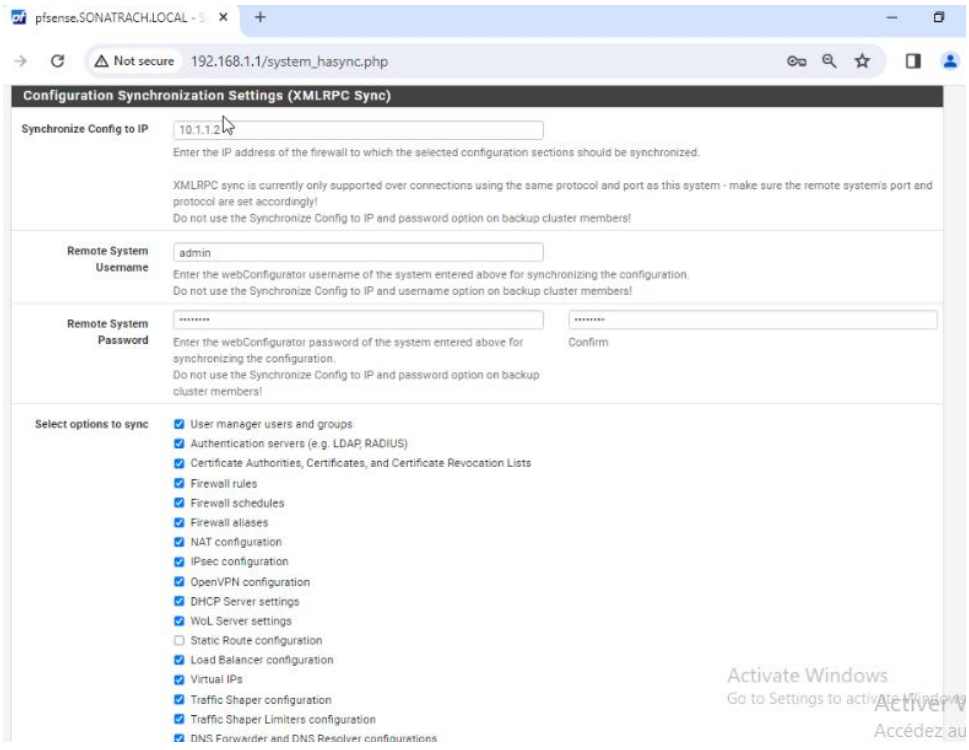

Figure III 45 La configuration de XMLRPC Sync

La figure III.36 montre l'adresse avec qui le firewall active va synchroniser ces données avec le compte d'utilisateur admin et les paramètres qui vont être synchroniser.

Remarque : le paramètre statique route IP est décocher, car les route par défaut du firewall 1 et du firewall 2 ne sont pas identique.

III.13 La configuration des interfaces virtuelles

Ces interfaces sont créées lors de l'activation de certains services (VLAN, WAN...).

La configuration d'un serveurVLAN entraîne automatiquement la création d'une interface virtuelle associée à cette instance serveurVLAN. L'interface virtuelle sera nommée port4_vlan30, port2_vlan20, etc...

Cette interface n'est pas configurable en l'état : ce n'est qu'un port réseau. Il est nécessaire de l'associer à une interface logique afin de pouvoir lui associer des règles de firewall ou de NAT spécifiques. [50]

Lorsque nous procédons à cette association, nous obtenons l'exemple suivant :

- La configuration de l'interface virtuelle WAN est démontrer dans la figure III.11

1. Accéder à Pare-feu | IP virtuelles.
2. Cliquer sur le bouton "plus" pour ajouter une nouvelle adresse IP virtuelle.
3. Choisir Autre comme Type.
4. Sélectionner le WAN comme interface.
5. Spécifierl'adresseIP.
6. Ajouter une description [52]

La figure suivante montre la configuration de l'interface virtuelle WAN :

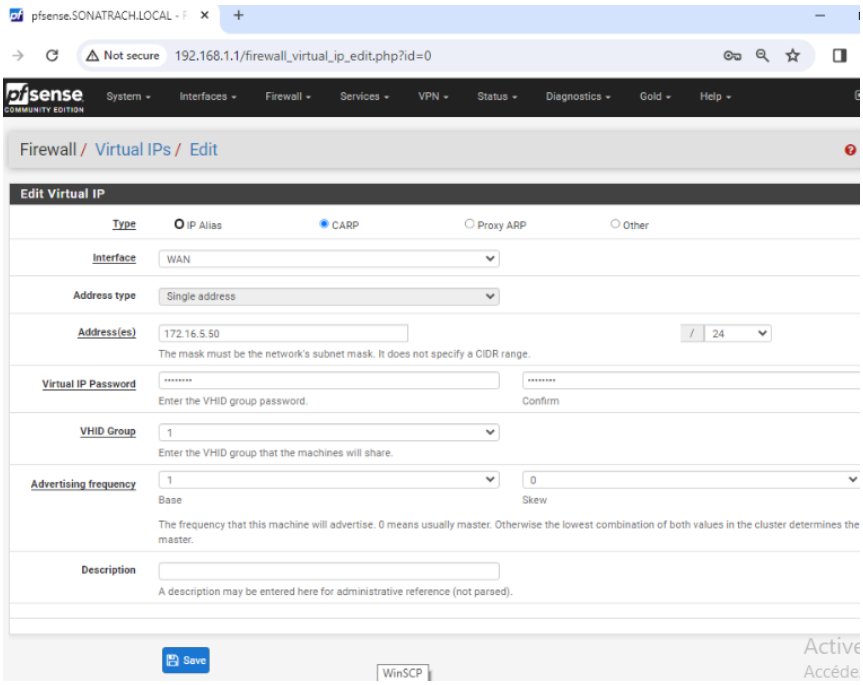

Figure III 46La configuration de l'interface virtuelle WAN

De la même façon, la création d'un VLAN entraîne la création d'une interface virtuelle (qui sera nommée WAN, port4_vlan30, port2_vlan10, port2_vlan20, etc.), cmme montre la figure suivante :

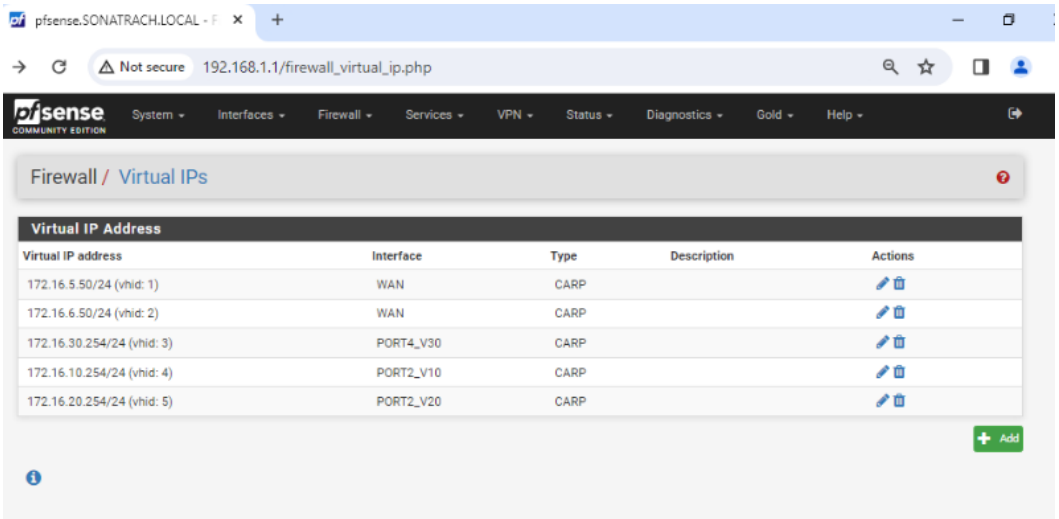

Figure III 47La configuration des interfaces virtuelles sur pfsense 1

- Après la synchronisation réussit la même configuration est appliquée sur Pfsense 2 :

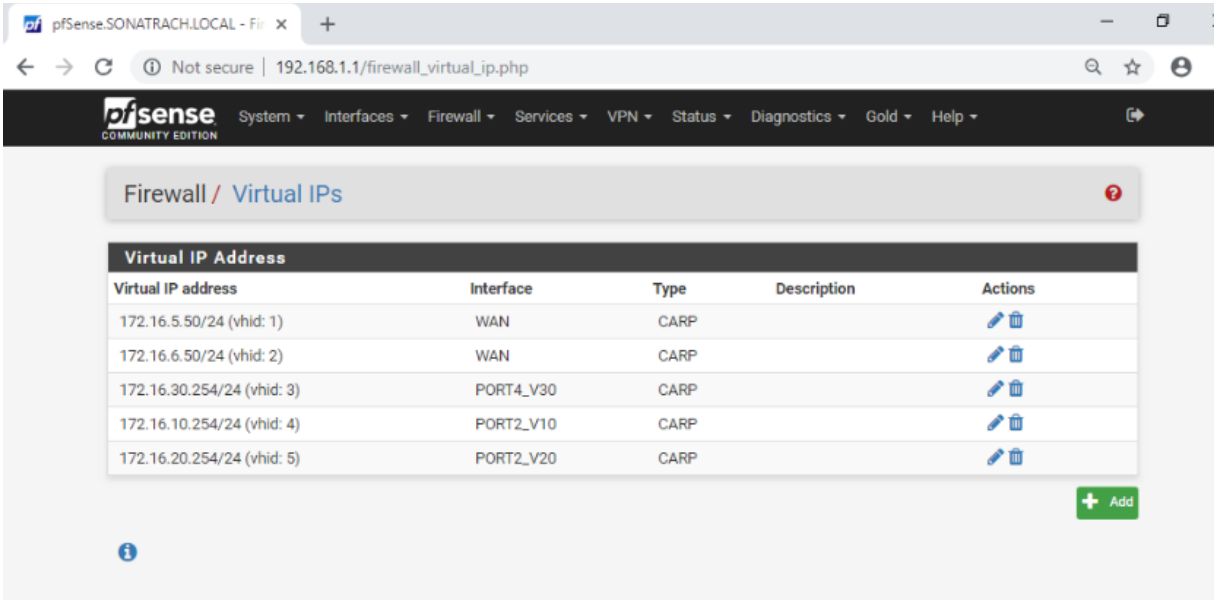

Figure III 48 La configuration des interfaces virtuelles sur pfsense 2

- Tableau de bord de pfSense :

Le tableau de bord de pfSense est une interface utilisateur graphique qui permet de surveiller et de gérer les performances et les activités du système de sécurité réseau pfSense.

La figure suivante montre le tableau de bord :

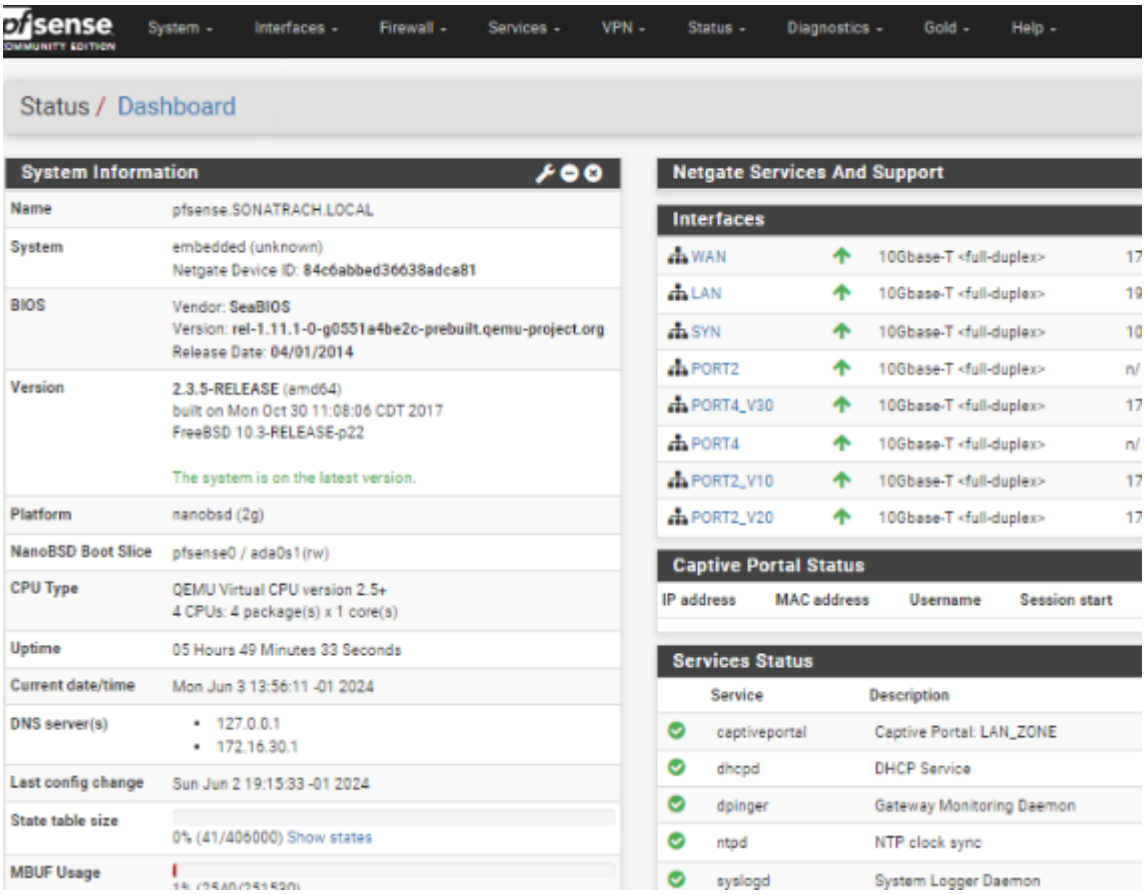

Figure III 49 Tableau de bord de pfsense1

- À la fin de la configuration, nous obtiendrons un menu textuel comme on peut le voir sur la figure suivante :

Cette figure représente le menu textuel pfsense1 :

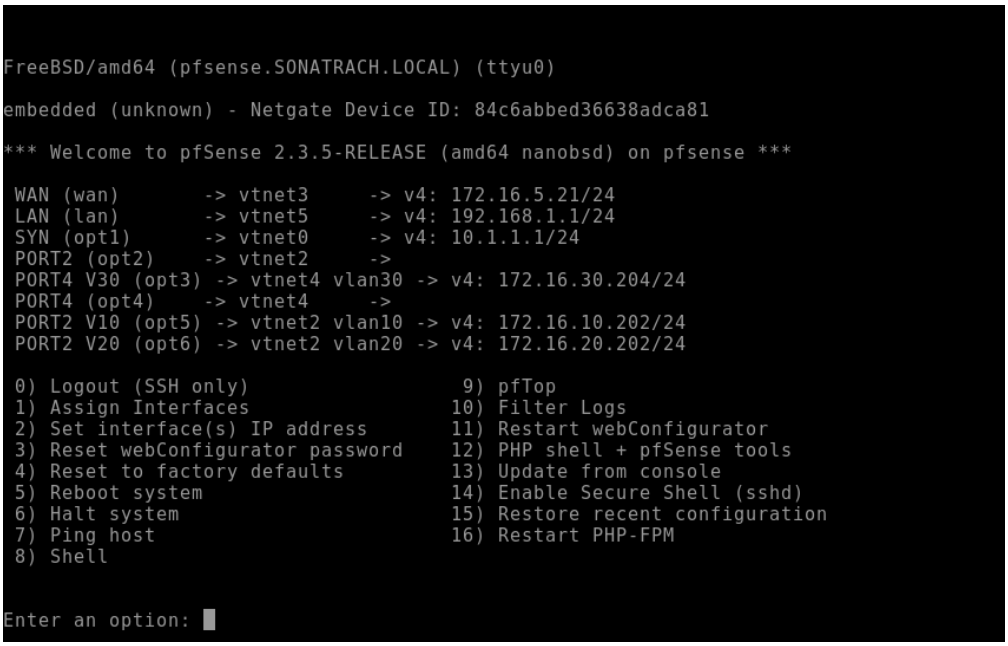

Figure III 50 Menu textuel pfsense1

Cette figure représente le menu textuel pfsense2 :

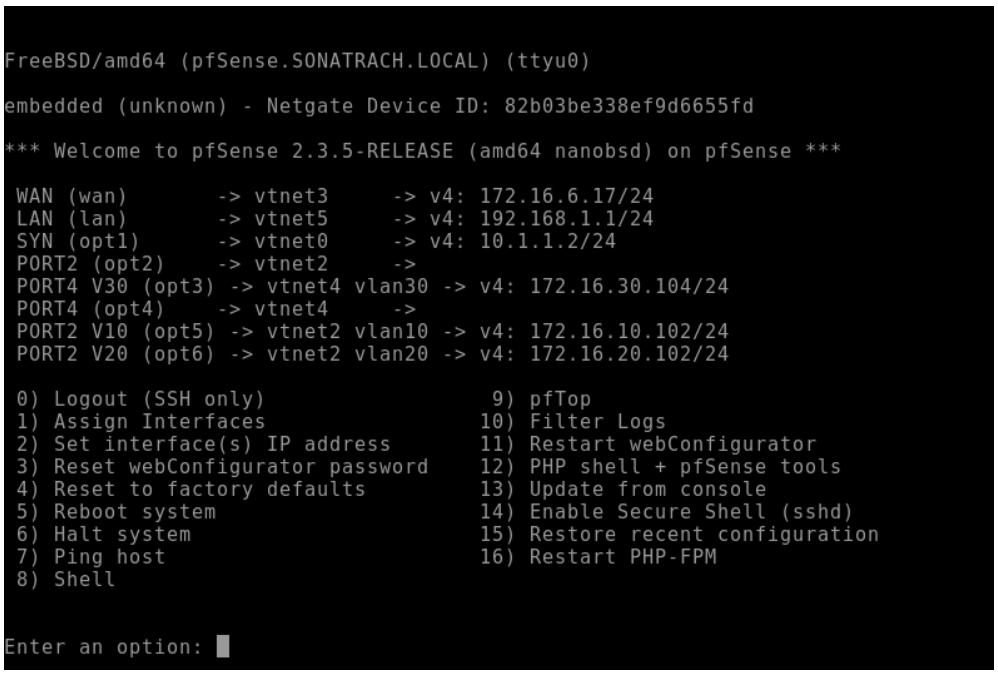

Figure III 51 Menu textuel pfsense2

III.14 Configuration des règles

- ❖ Règles de pare-feu ajoutées sur l'interface WAN :

Des règles de filtrages ont été mis en place comme suit.

Entrerdans Firewall \ Rules \ WAN \ Add.

- **Les étapes de configuration :**

La figure III51 et III.52 montre les étapes de configuration dans l'interface graphique du Pfsense

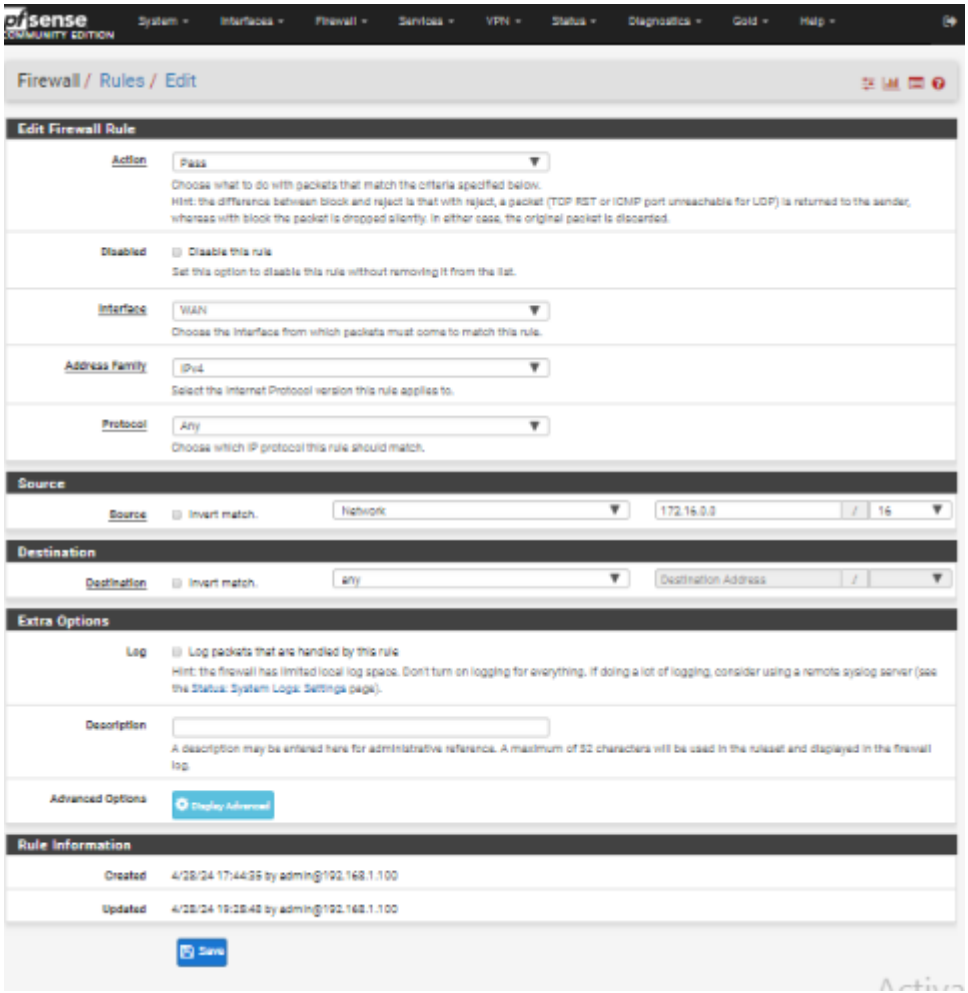

Figure III 52 Les étapes de la configuration des règles de l'interfaces WAN

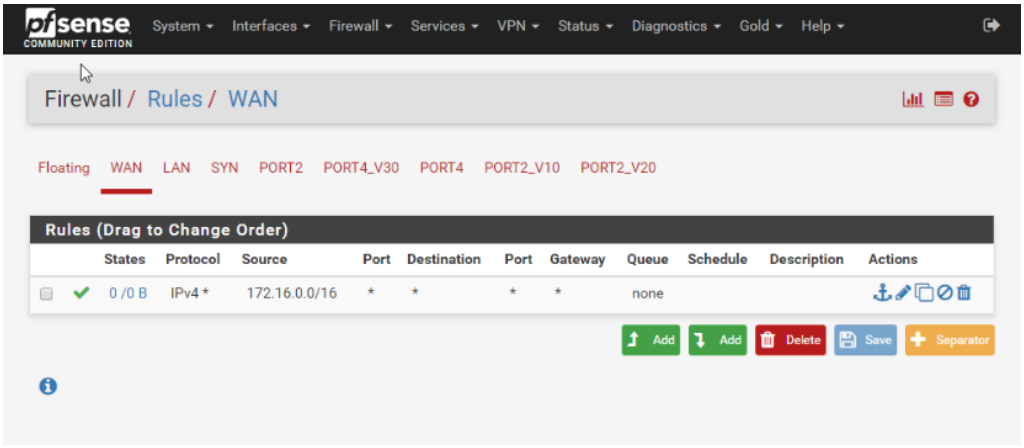

Figure III 53 Les règles configurées pour le WAN

Règle:

-Action: Autoriser (Pass)

-Interface: WAN

-Address family: IPv4

-Protocole : Any

Source :

-Source : Network

-Plage de port source : 172.16.0.0

-Destination

-Destination : Any

Save

Voici les étapes de la configuration des règles qui ont été mises en place pour le WAN :

- ❖ Règles de pare-feu ajoutées sur l'interface SYN

Pour mettre en place des règles de filtrages. Accéder à Firewall \ Rules \ LAN \ Add

La figure suivante montre les règles qui ont été mises en place pour le SYN :

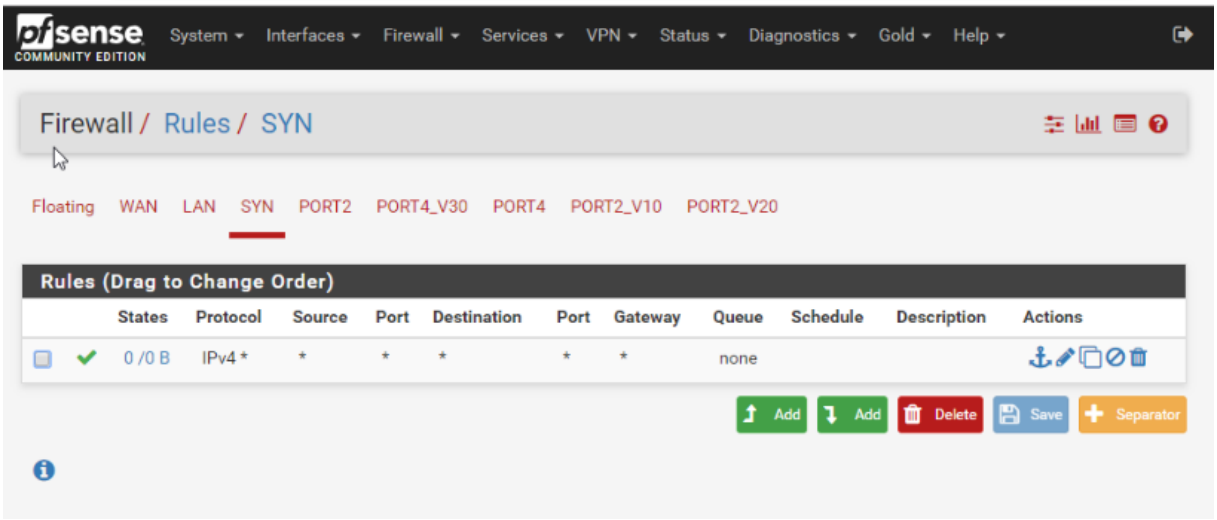

Figure III 54 Les règles configurées pour le SYN

- ❖ Règles de pare-feu ajoutées sur l'interface PORT4_V30

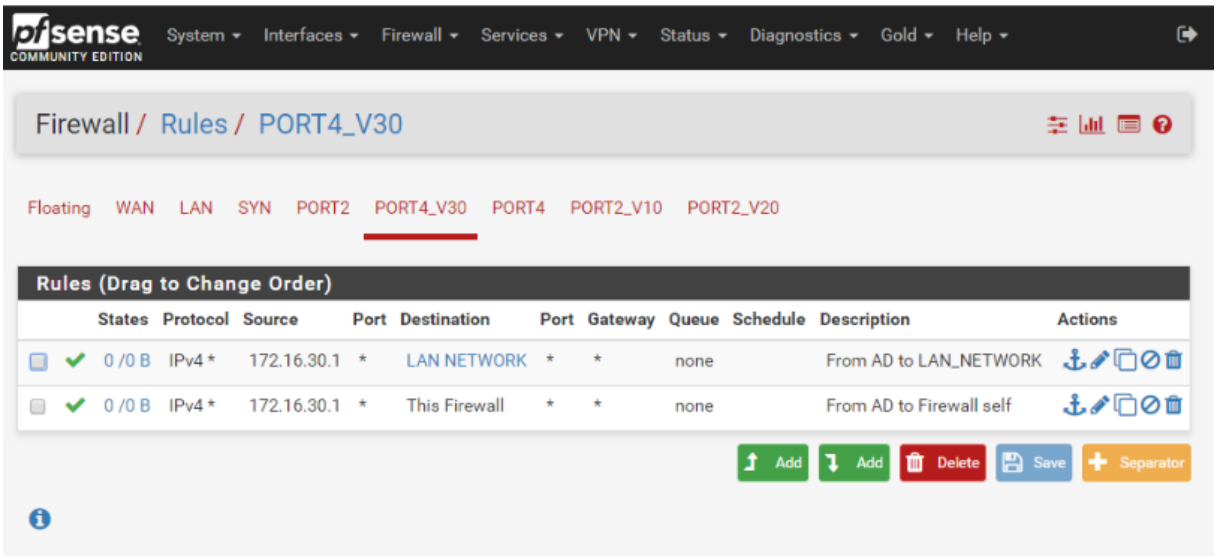

Figure III 55 Les règles configurées pour le PORT4_V30

- Règles de pare-feu ajoutées sur l'interface PORT4_V10

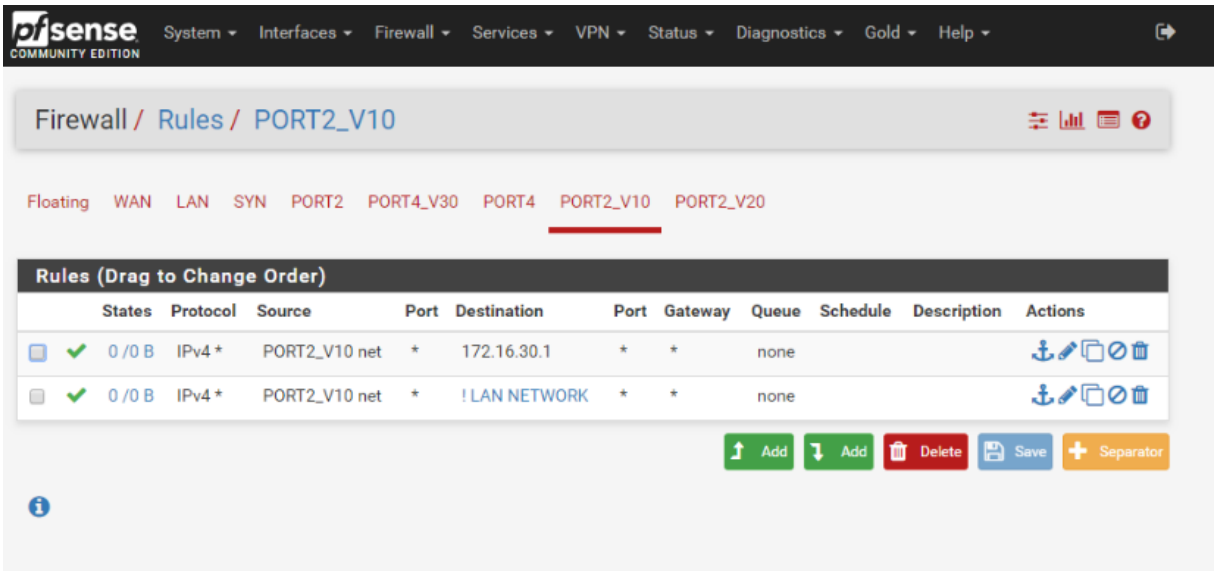

Figure III 56 Les règles configurées pour le PORT4_V10

- Règles de pare-feu ajoutées sur l'interface PORT4_V20

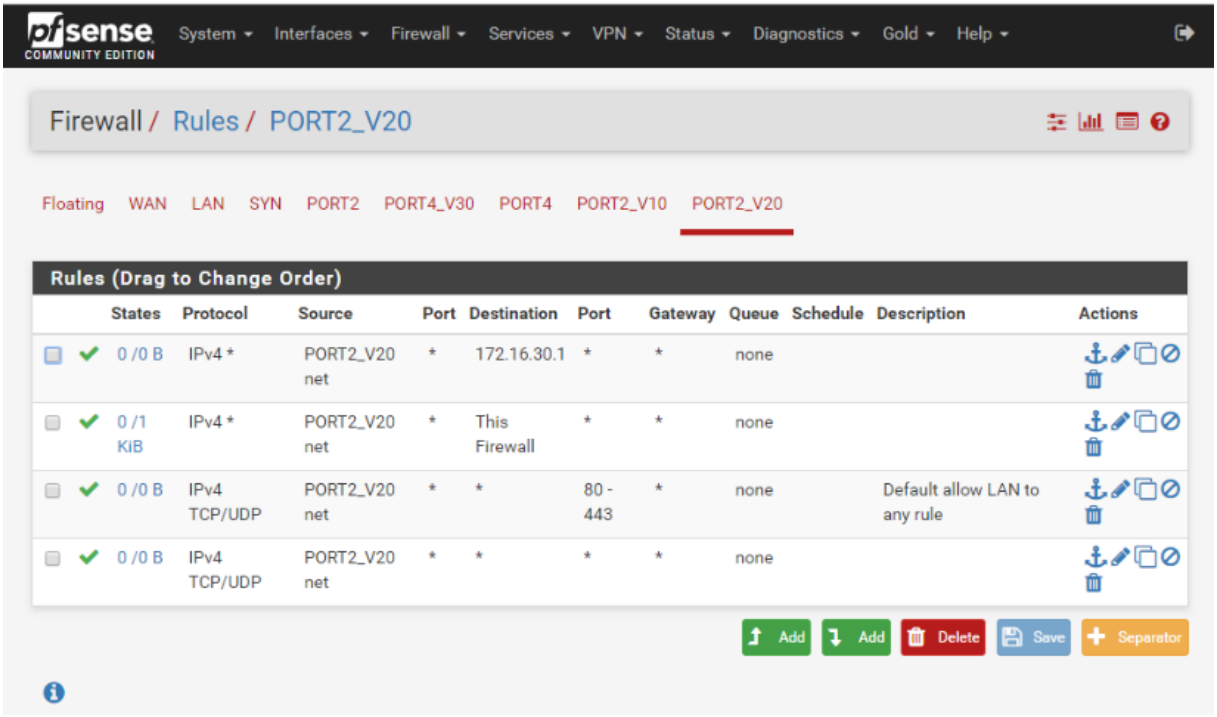

Figure III 57 Les règles configurées pour le PORT4_V20

III.15 Configuration des règles avec les alias

Sous pfSense, un alias permet de définir un groupe de ports réseaux, d'hôtes ou de sous-réseaux. Ces alias peuvent ensuite être utilisés dans les règles de filtrage, les règles de redirection de ports, les règles de NAT, etc. Utiliser des alias est une bonne pratique pour disposer de règles claires, courtes, simples et lisibles sur notre firewall.

- Les alias sont configurables depuis le menu Firewall >Aliases :
  La figure suivante montre la figure suivante :

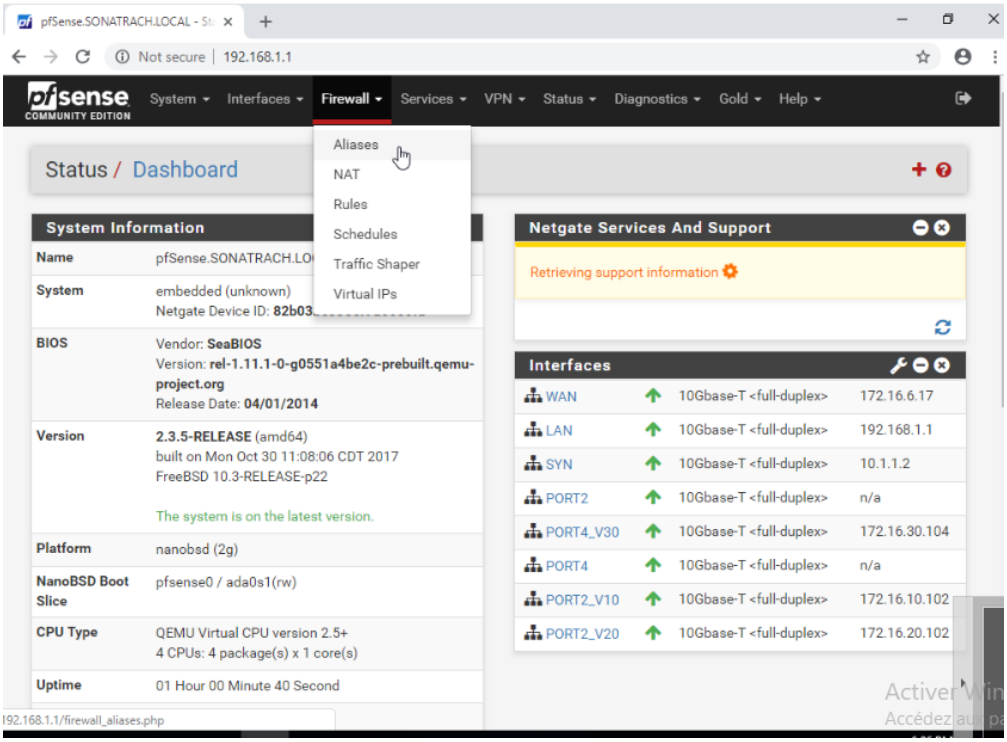

Figure III 58Accéder au Alias

- Depuis l'onglet "IP" on ajoute le type d'alias « Network », comme montre les figure III58 et III59 :

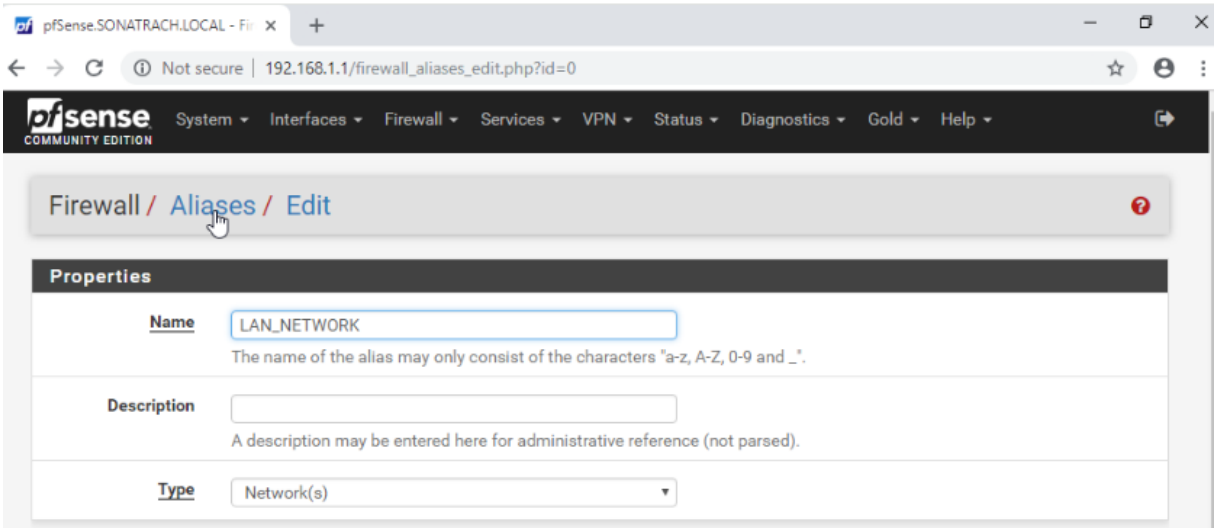

Figure III 59 Configuration de LAN-NETWORK

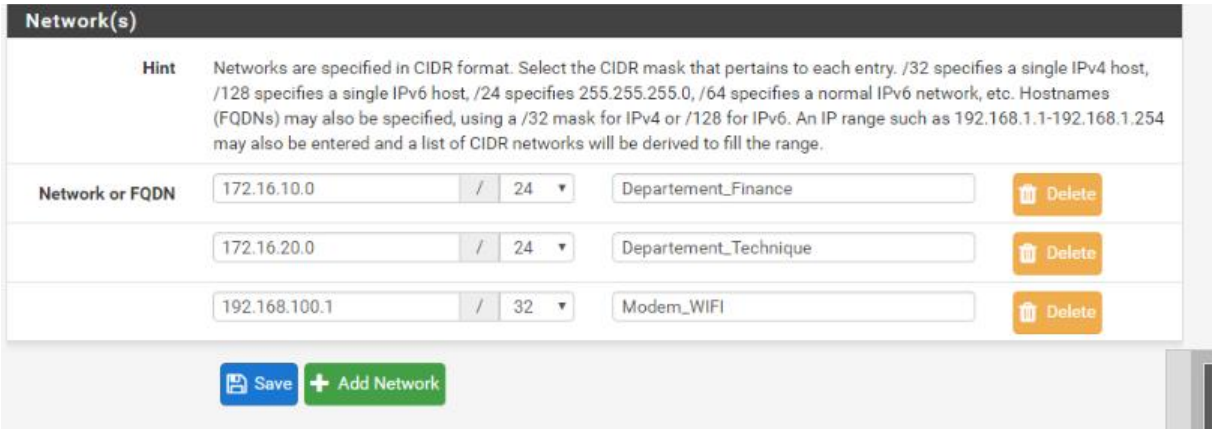

Figure III 60 Configure de network

- On clique sur « save » pour enregistrer la configuration.

III.16 Configuration du NAT au routeur

Pour interconnecter un réseau privé (réseau d'entreprise), en IPv4, il faut se passer du NAT. Voici donc la configuration essentielle afin de permettre un accès à Internet :

```
Router> enable
Router# Configure terminal
Routerconfig) # interface GigabitEthernet 0/0
Router(config-if) #ip address 192.168.1.186 255.255.255.0
Router (config_if) #no shudown
Router (config_if) #exit
Routerconfig) # interface GigabitEthernet 0/1
Router (config-if) #ip address 172.16.6.18 255.255.255.0
Router (config_if) #no shudown
Router (config_if) #exit
Routerconfig) # interface GigabitEthernet 0/3
Router (config-if) #ip address 172.16.5.22 255.255.255.0
Router (config_if) #no shudown
Router (config_if) #exit
```

Figure III 61 Configuration de NAT au routeur

- Vérification du la configuration dans le routeur :

```
Routeur#show running-config
```

Figure III 62 Vérification de la configuration de routeur

La figure suivante présente la configuration de NAT dans le routeur :

```
!
interface GigabitEthernet0/0
 ip address 192.168.1.186 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 shutdown
 duplex auto
 speed auto
 media-type rj45
 nat64 enable
!
interface GigabitEthernet0/1
 ip address 172.16.6.18 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 shutdown
 duplex auto
 speed auto
 media-type rj45
 nat64 enable
!
interface GigabitEthernet0/2
 ip address 172.16.5.22 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 shutdown
 duplex auto
 speed auto
 media-type rj45
 nat64 enable
!
```

Figure III 63 Vérification de configuration de routeur

III.17 Installation et configuration des services nécessaires de Windows Server 2019

Pour installer et configurer le serveur, procédez comme suit:

- **Installation et configuration de Active Directory et DNS :**

Pour configurer un Active Directory sur une machine Windows Server 2019, vous devez exécuter les étapes suivantes :

1. Lancez le programme Gestionnaire de serveur, comme montre la figure suivante :

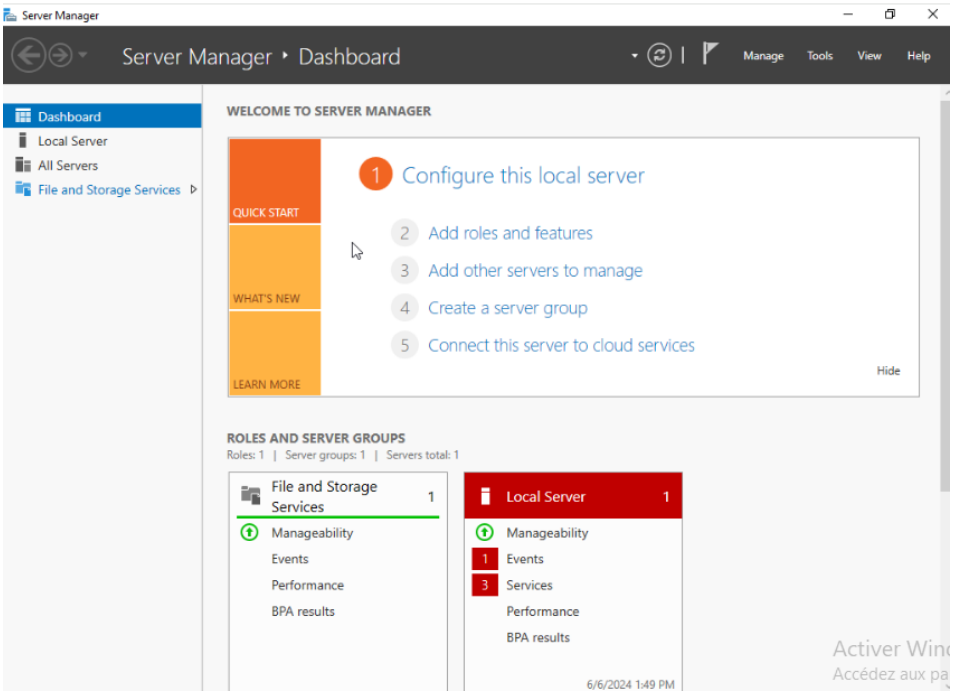

Figure III 64Interface de serveur manager

2. Recherchez « Manage » en haut à droite de la barre de menu. Cliquez dessus, puis sélectionnez « AddRoles and Features ». Une fenêtre pop-up s'ouvrira immédiatement. Cette fenêtre contextuelle est l'assistant d'installation qui vous guide dans la configuration des rôles et des fonctionnalités, comme montre la figure suivante :

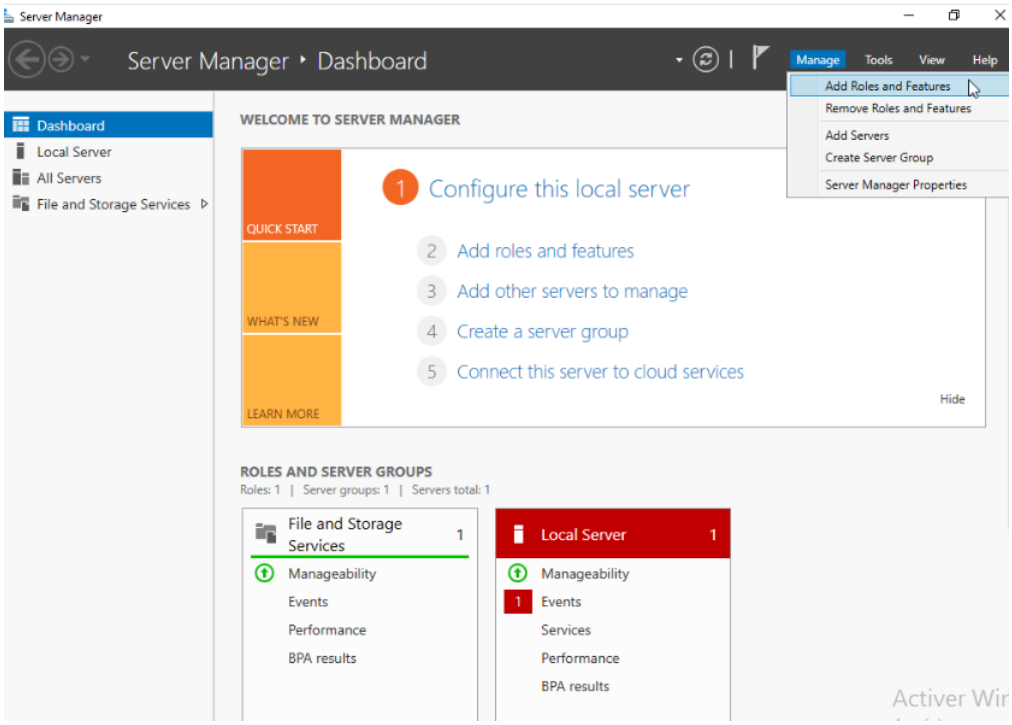

Figure III 65 Interface de serveur manger : configurer les rôles et les fonctionnalités

3. Sur le côté gauche de la fenêtre, vous verrez une liste de tous les points de contrôle que vous rencontrez au cours de cette étape. Cliquez sur “Next", comme montre la figure suivante :

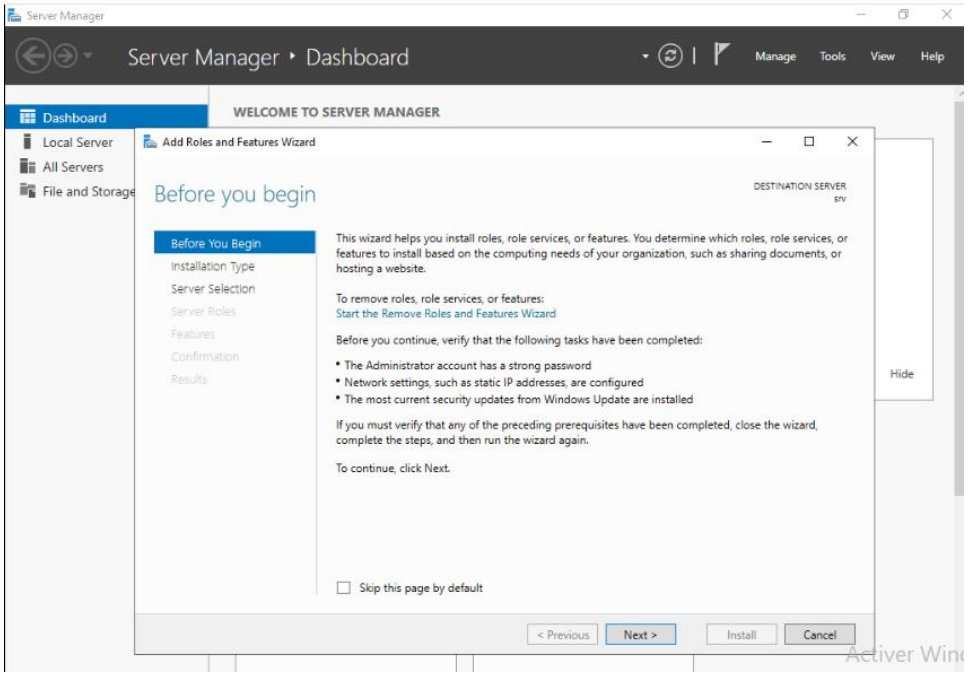

Figure III 66La liste de tous les ponts de contrôle

4. Sélectionnez le type d’installation :

Au point de contrôle « Installation Type », sélectionnez le bouton radio « Role-based or

feature based installation », puis cliquez sur « Next », comme montre la figure suivante :

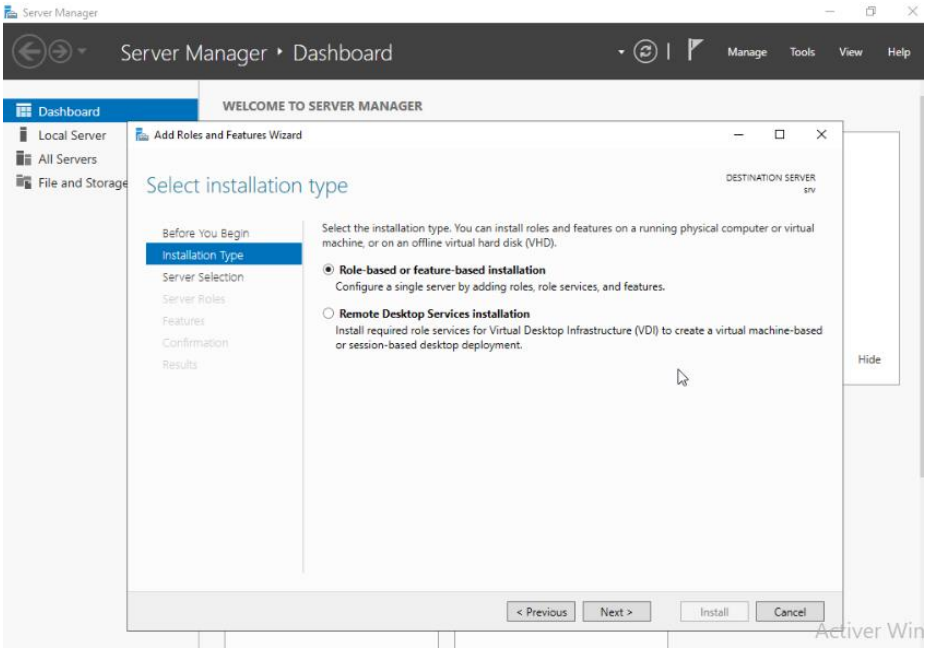

Figure III 67Sélectionne de type d'installation

5. Configurez votre sélection de serveur et vos rôles :

Au point de contrôle « checkpoint, select », sélectionnez le bouton radio « Select a server from the server pool ». Ceci répertorie un serveur installé sur votre machine . Veuillez cliquer une fois sur le serveur souhaité pour le sélectionner et cliquez sur « Next », comme montre la figure suivante :

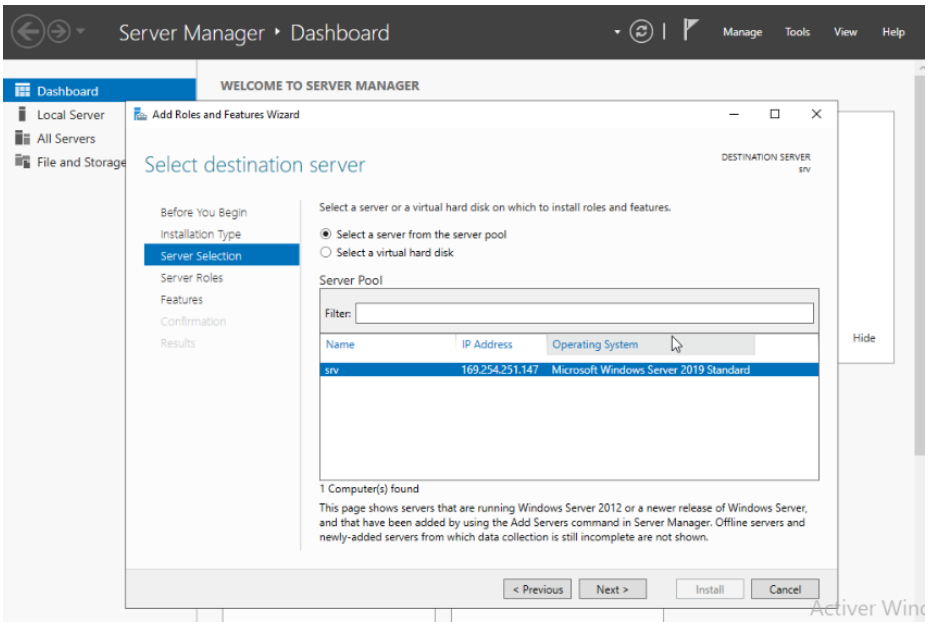

Figure III 68 Configuration de serveur

6. Au point de contrôle « Select Server Roles », sélectionnez le rôle du serveur. Au

centre de la fenêtre se trouve une liste de tous les rôles que vous pouvez attribuer à votre machine serveur. Recherchez « Active Directory Domain Services» et « DNS Server », comme montre la figure suivante :

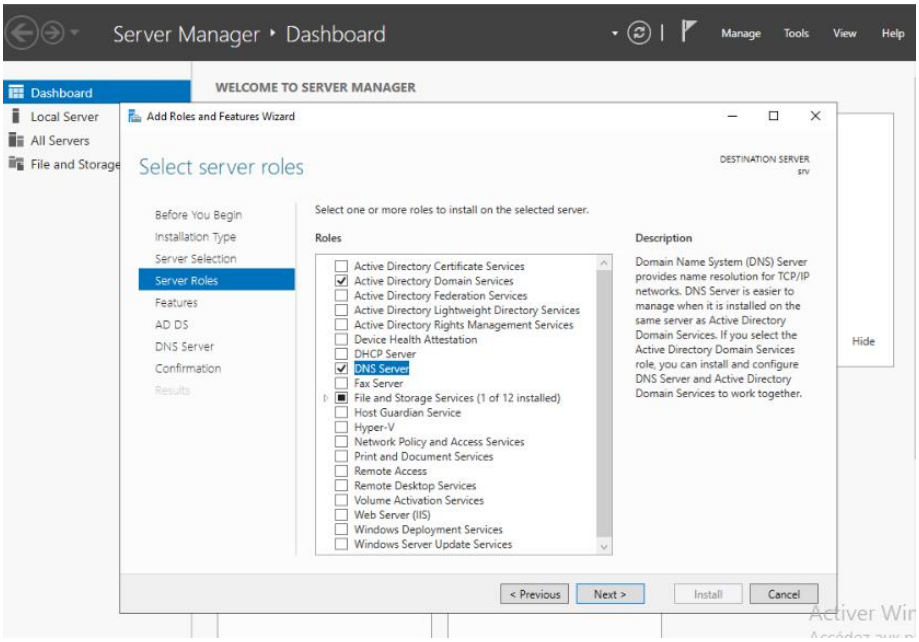

Figure III 69 Sélectionne les rôles de serveurs

7. Ajouter des fonctionnalités :

Une fenêtre contextuelle s'affichera. C'est le point de contrôle pour l'ajout de nouvelles fonctionnalités. Naviguez sur le bouton « Addfeatures » en bas de la fenêtre et une liste des fonctionnalités disponibles s'affichera :

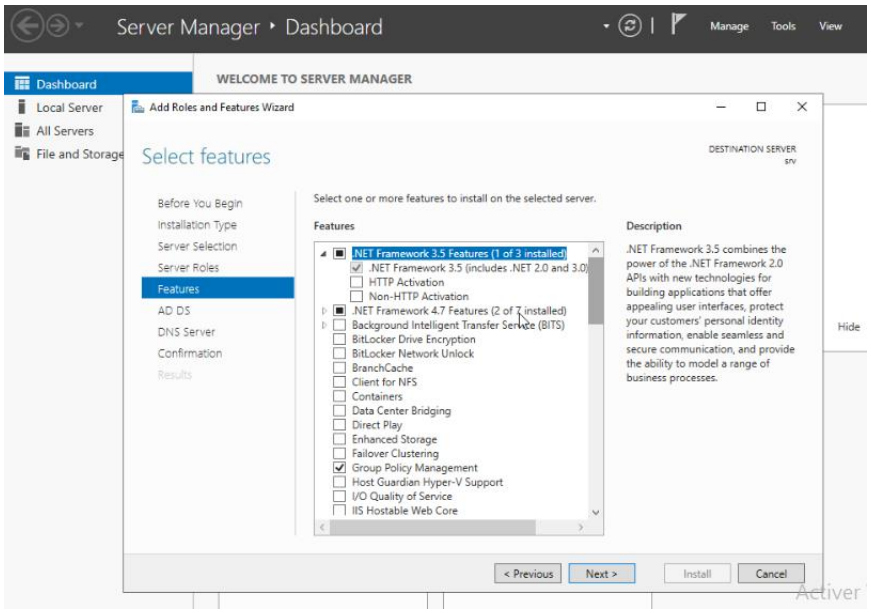

Figure III 70 Sélectionne des fonctionnalités

1. Ensuite, cliquez simplement sur « Next » sans apporter de modifications aux autres paramètres, comme montre la figure suivante :

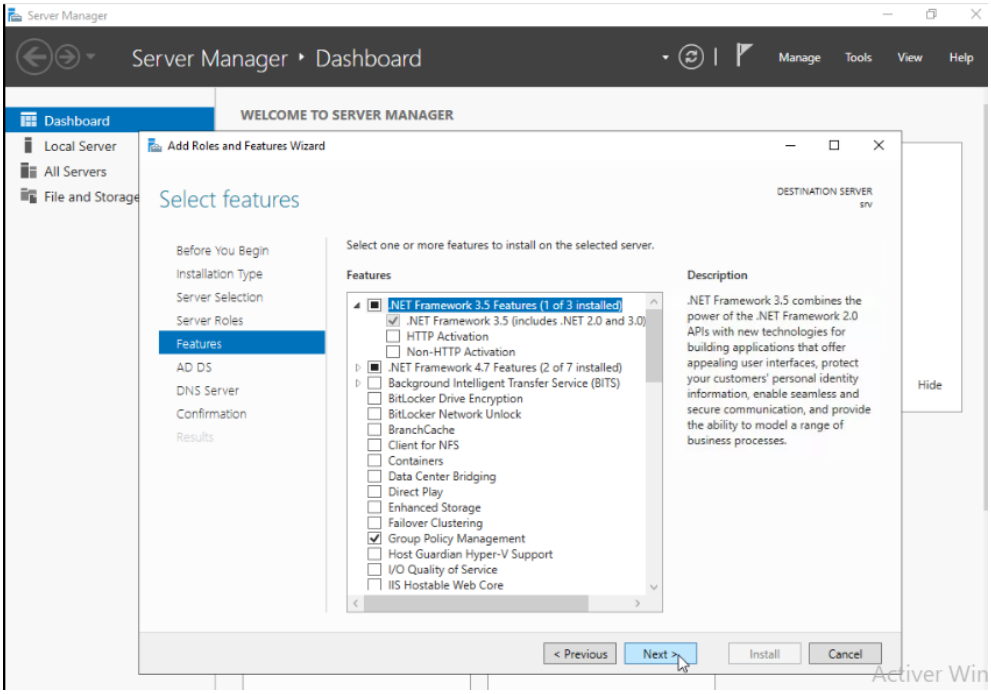

Figure III 71 La suite des étapes

1. Vous serez redirigé vers la fonctionnalité d'ajout de « Active Directory Domain Services et « DNS Server » une fois l'étape précédente terminée. Dans la fenêtre de l'assistant d'installation, cliquez sur « Next » comme montre la figure suivante :

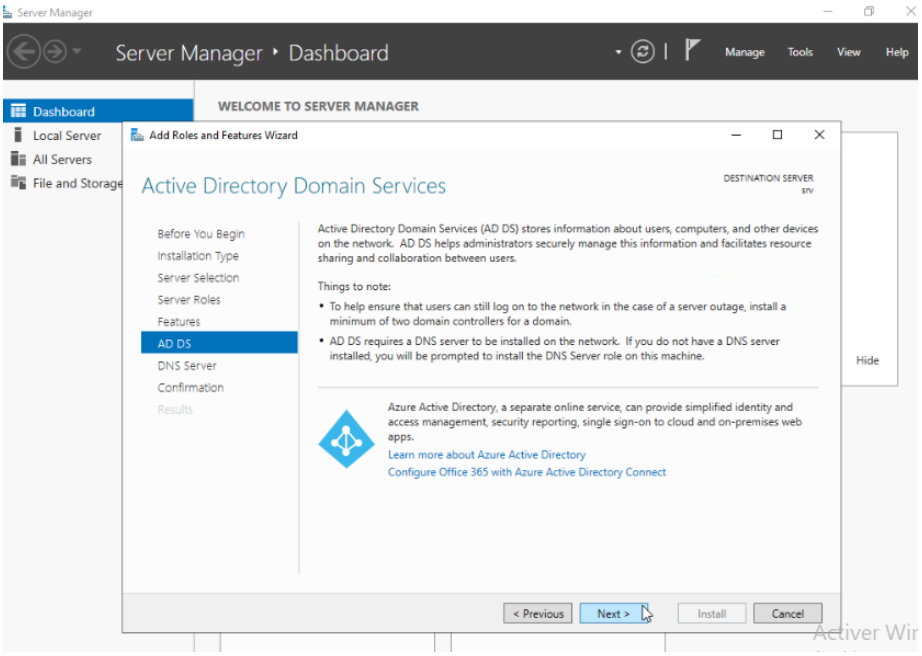

Figure III 72 Redirigé de services de Active Directory

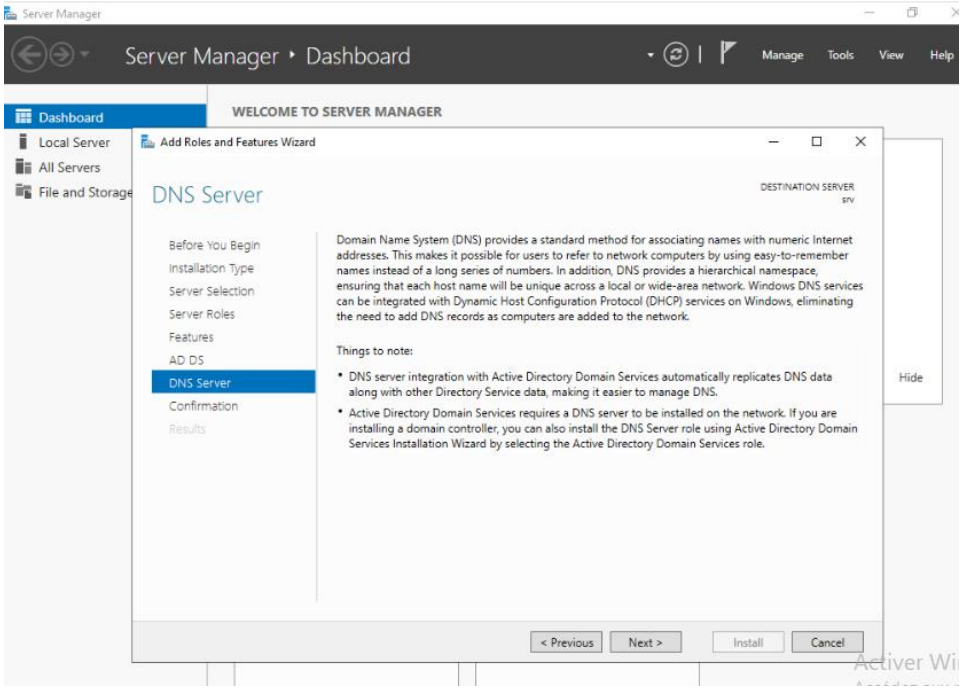

Figure III 73Redirigé de DNS Server

1. Cliquez sur le bouton « Install », une fois que vous êtes satisfait de vos sélections au point de contrôle « Confirmation » comme montre la figure suivante :

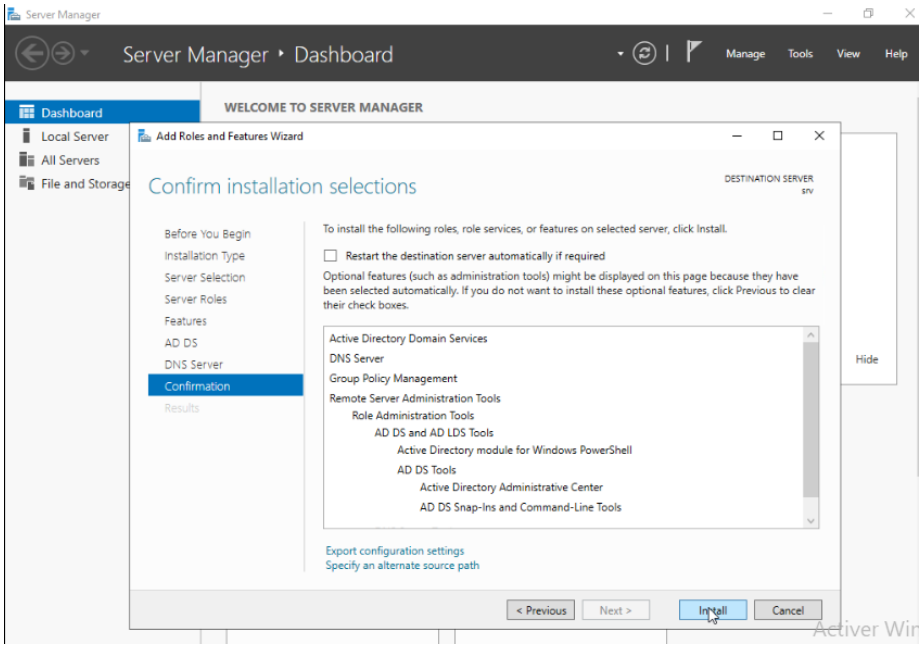

Figure III 74 Confirmer l'installation de DNS Server

2. L'assistant commencera alors l'installation. Le moment de l'installation dépend de la

configuration matérielle de votre ordinateur et des fonctionnalités que vous avez choisi d'installer. Veuillez-vous assurer de ne pas interrompre l'installation. Une fois l'installation terminée, cliquez sur le bouton « Close ». [53]

La figure suivante presente la progression de l'installation :

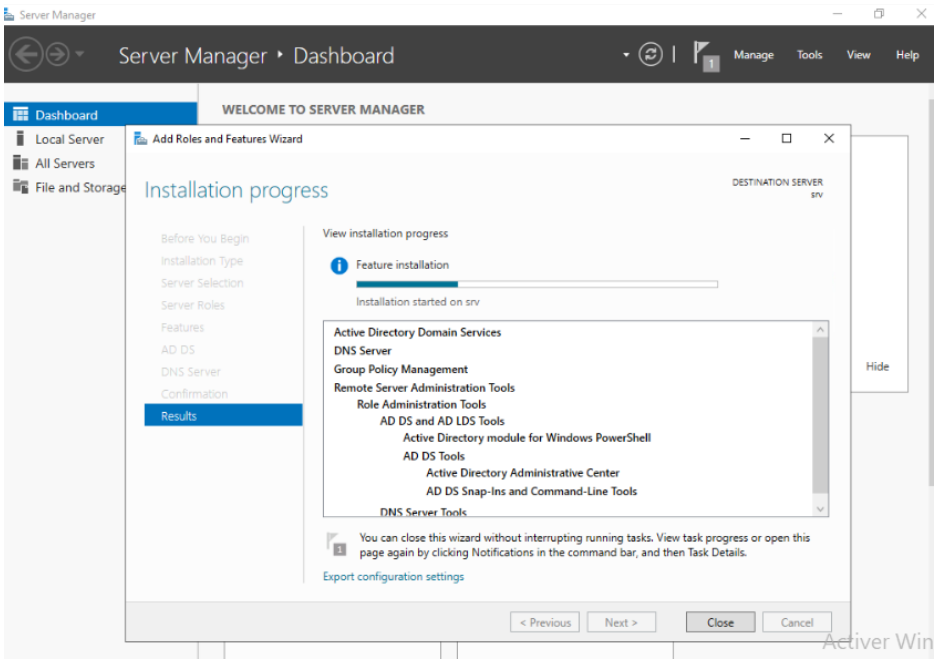

Figure III 75 Progression de l'installation

- **Création des comptes utilisateur et d'un groupe dans une unité d'organisation dans Active Directory**

Création d'une unité d'organisation :

- Ouvrir Active Directory Users and Computers (utilisateur et ordinateur active directory), comme montre la figure suivante :

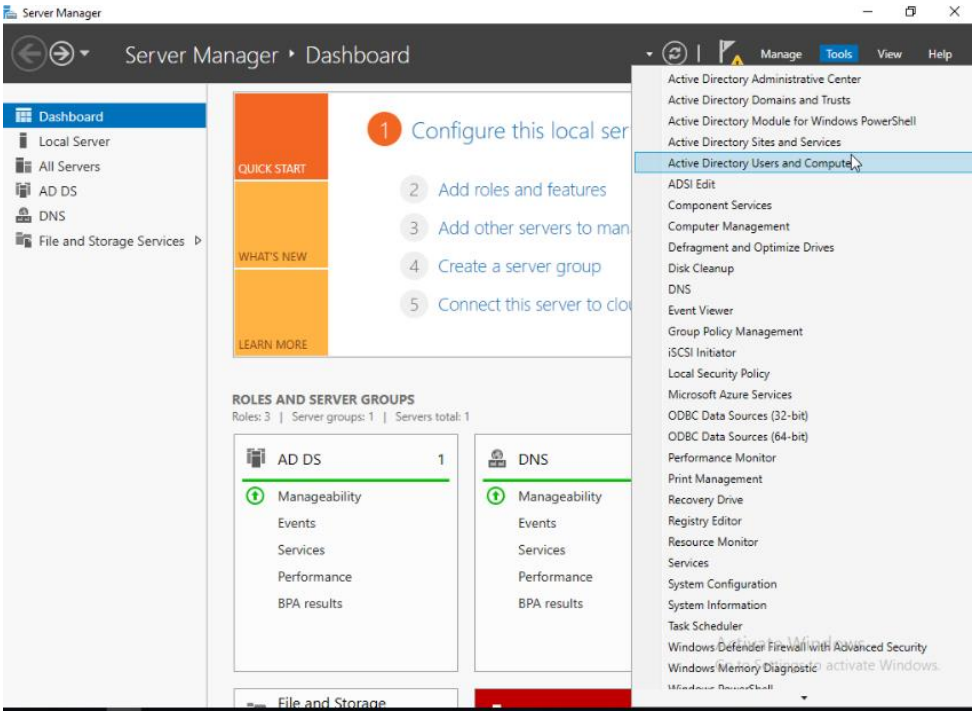

Figure III 76Allez vers Active Directory Users and computers

- Ensuite, on clique avec le botton droit et créer un New Folder « SONATRACH.LOCAL »

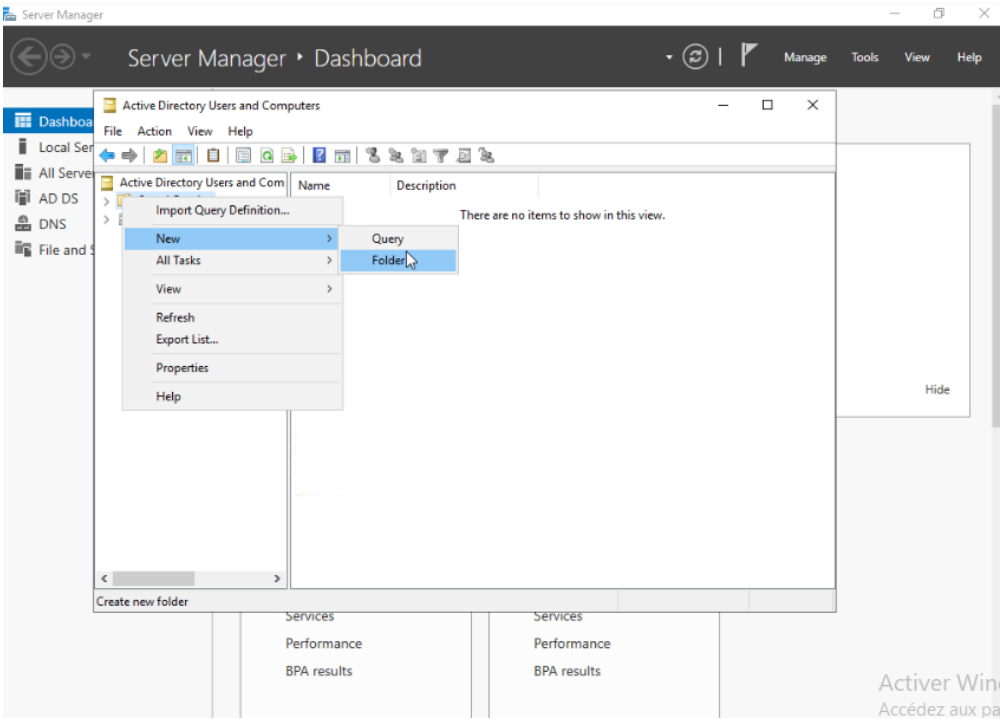

Figure III 77Crier new folder SONATRACH.LOCAL

- Ensuite, on créer une unité d'organisation (Organizational Unit) clic droit sur SONATRACH.LOCAL « new » Organizational Unit, comme montre la figure suivante :

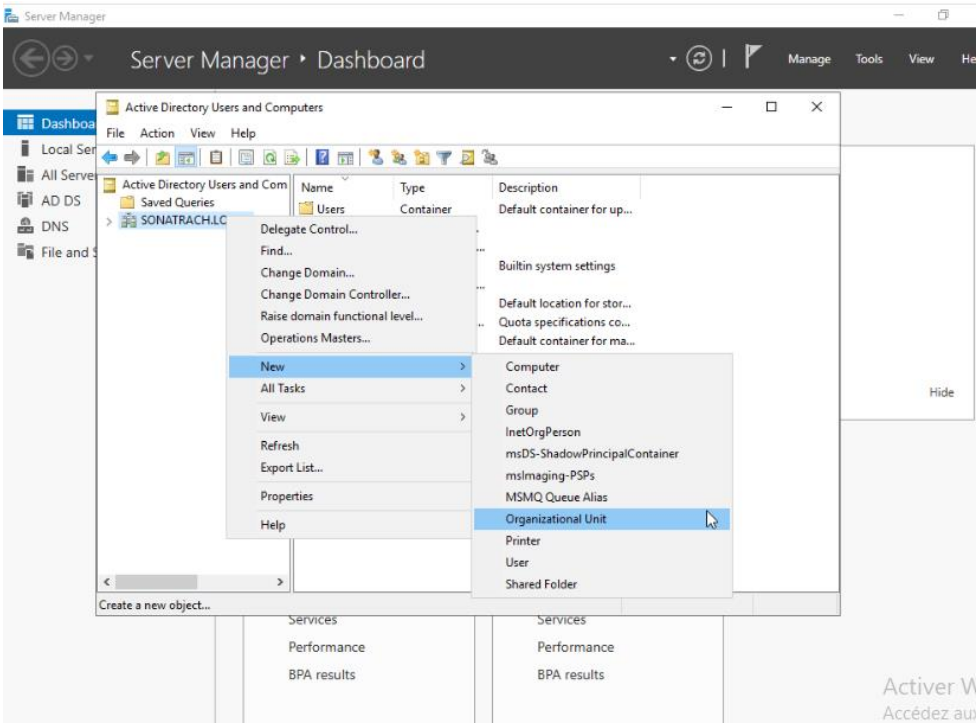

Figure III 78Créer une unité d'organisation

- Ensuite, on a nommé cette organisation « SONATRACH »

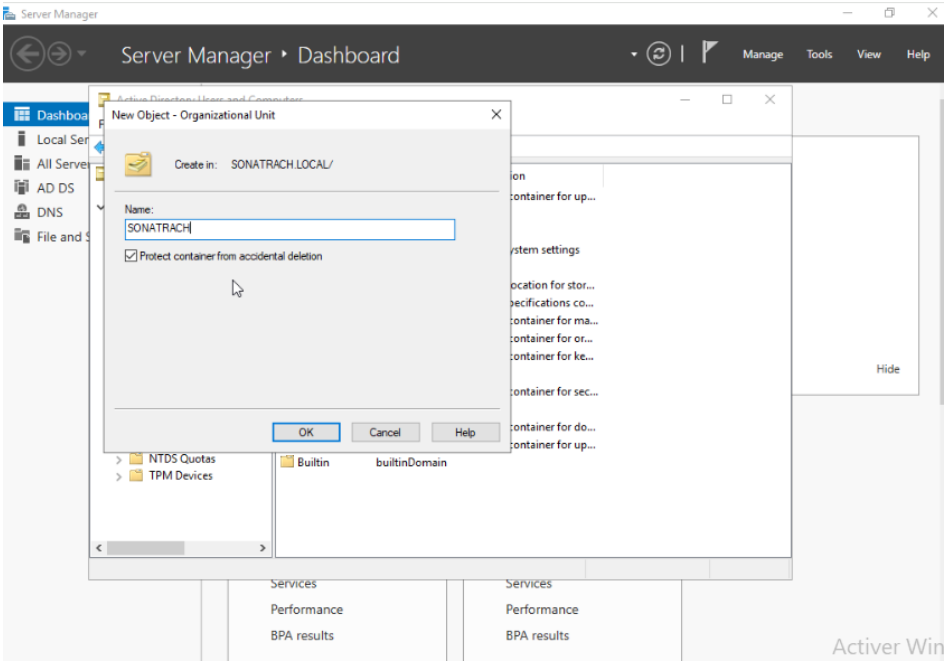

Figure III 79 Nommer l'organisation SONATRACH

- Ensuite, dans l'organisation SONATRACH on ajoute pfsense, et on créer une autre organisation « Departement Finance », comme montre la figure suivante :

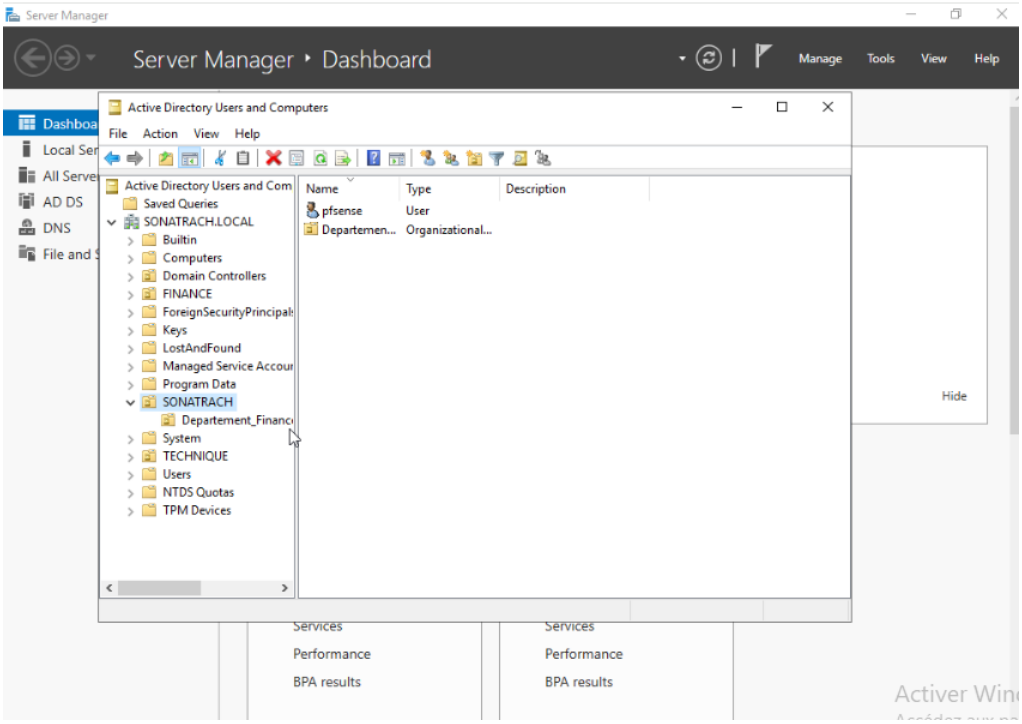

Figure III 80Ajoute de pfsense et departement finance au SONATRACH

- Ensuite, dans le departement finance on crée un utilisateur

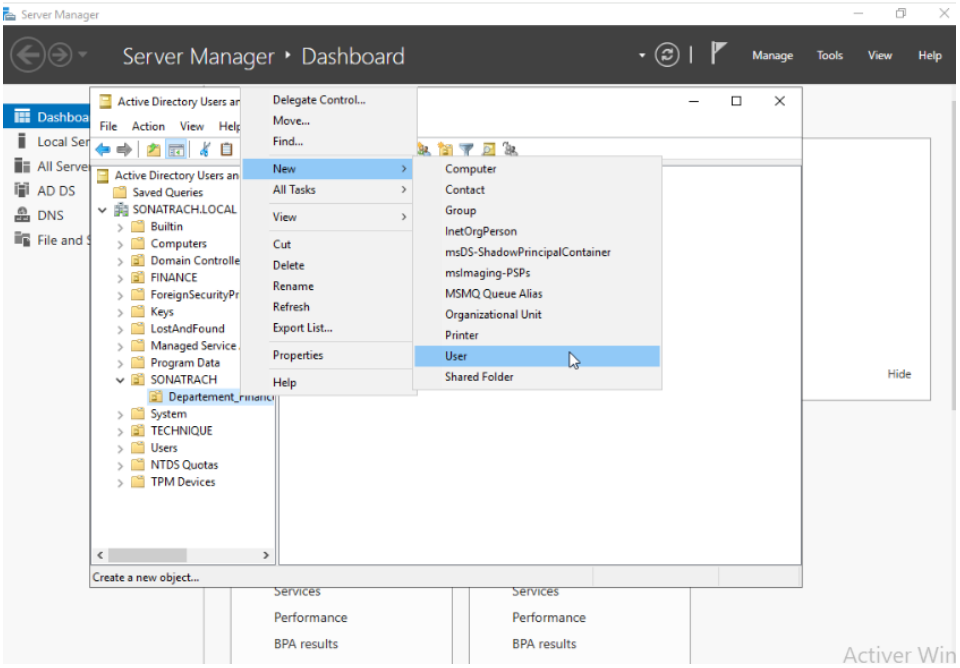

Figure III 81 Création d'un utilisateur

- Indiquer un prénom, nom, nom complet un nom d'ouverture de session choisissez un nom de domaine disponible dans le menu déroulant ensuite cliquer sur « Next », comme montre la figure suivante :

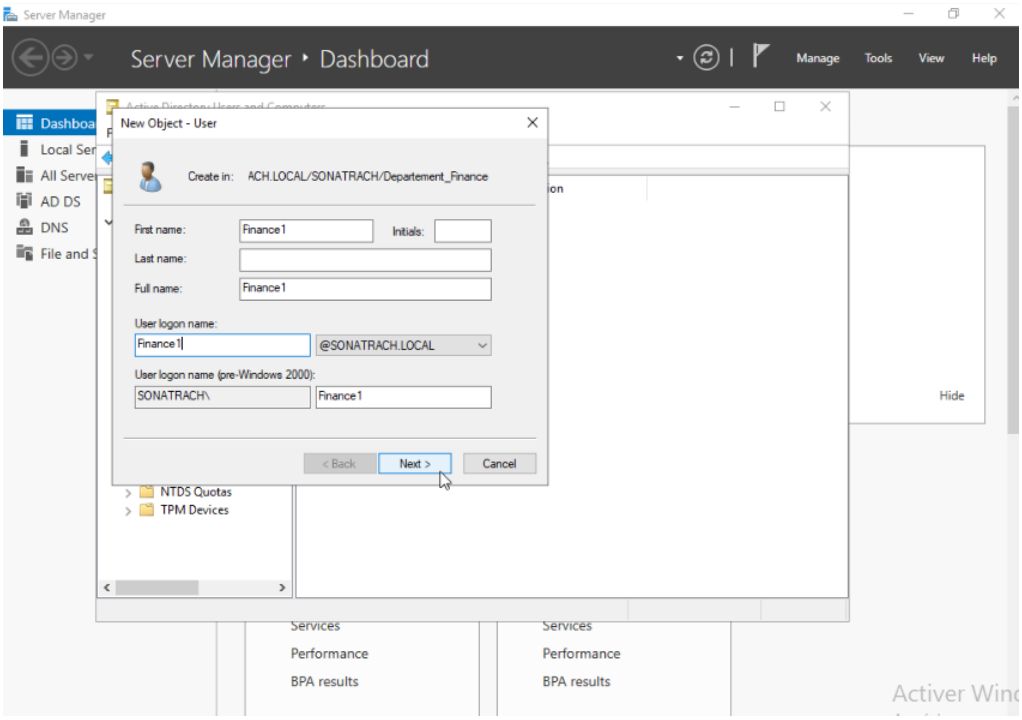

Figure III 82Création d'utilisateur

- Choisissez un mot de passe cocher la case « user must change password at next login », ensuite cliquersur « Next », comme montre la figure suivante :

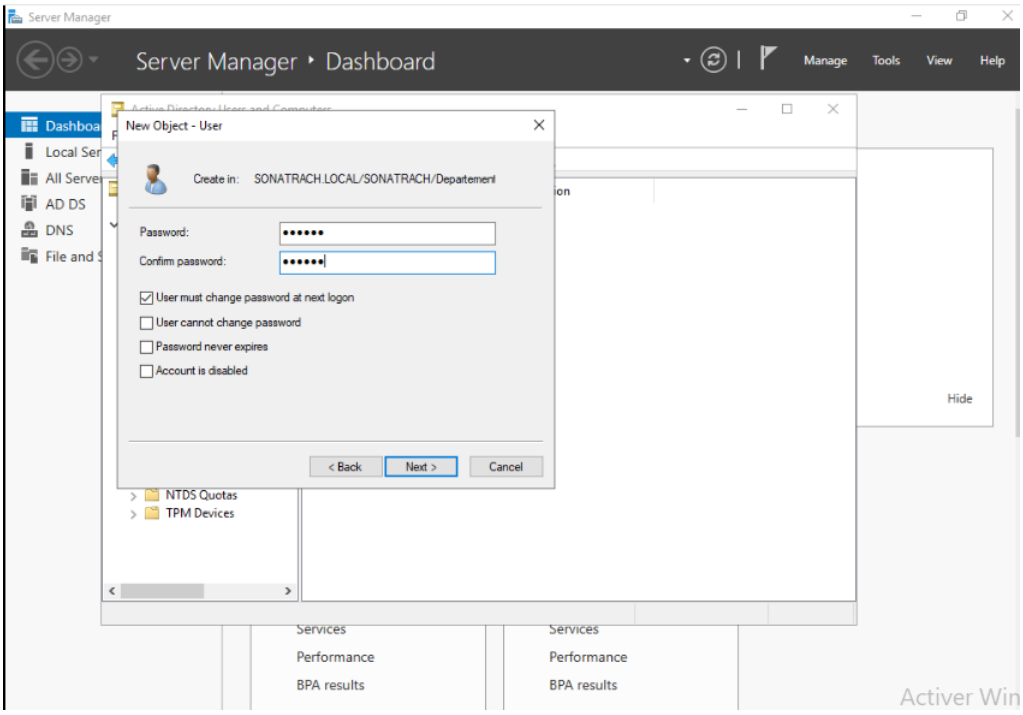

Figure III 83 Configuration de mot de passe

- Ensuite, on clique sur « Finish »
- L'utilisateur « finance1 » créé est affiché dans le volet droit comme le montre la figure

suivante :

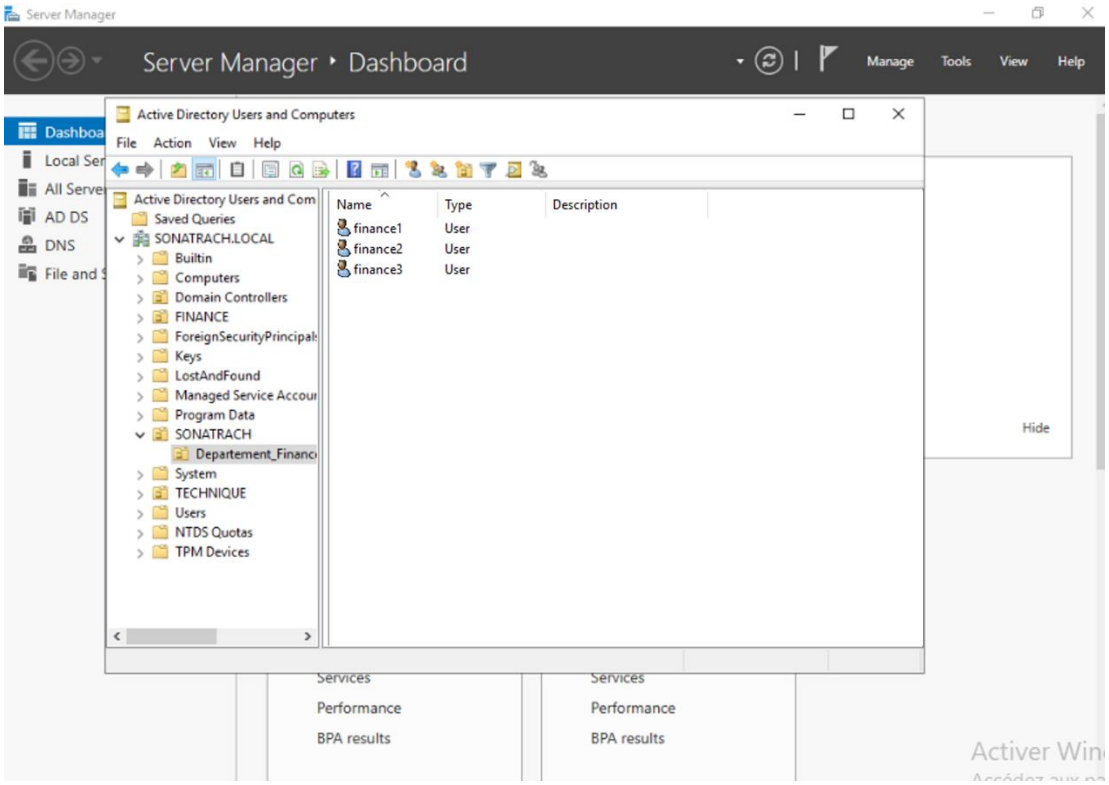

Figure III 84 Fenêtrée des utilisateurs crées

Ainsi pour les utilisateurs admin 2 admin, 3 et finance 2, finance 3.

❖ Configuration de nom de domaine :

- Dans Tools, choisis DNS, comme montre la figure suivante :

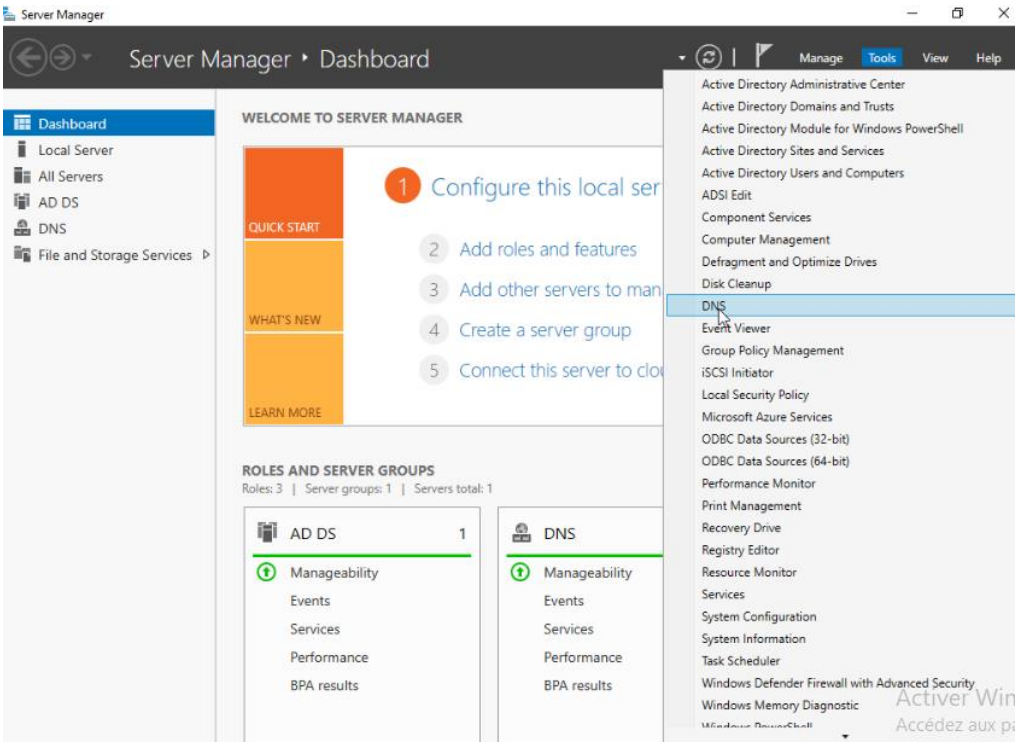

Figure III 85 Allez au DNS

La figure III83 présente :

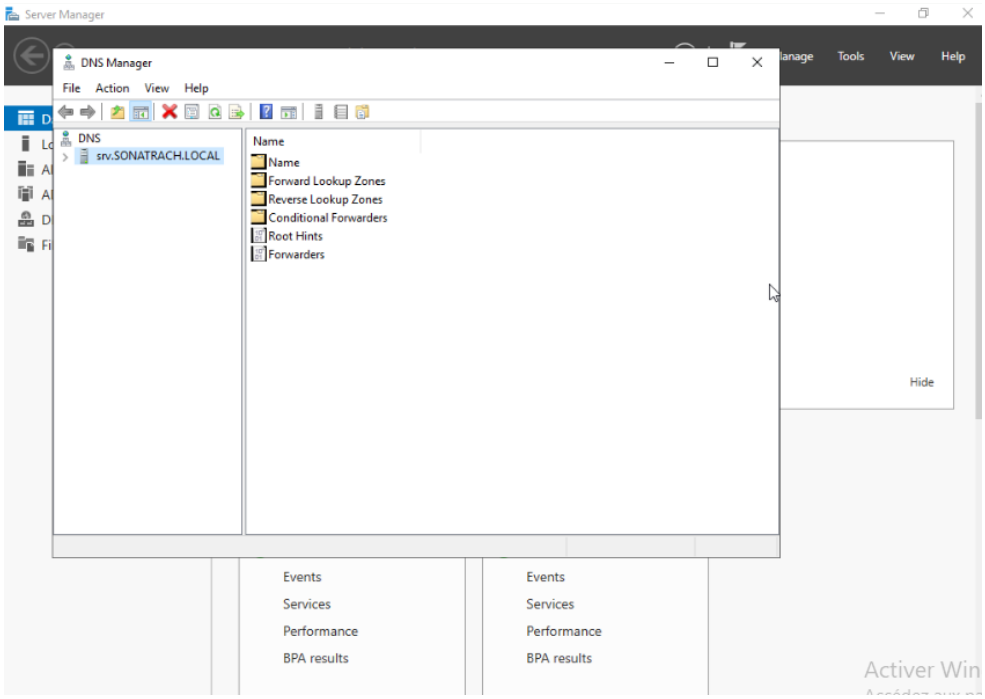

Figure III 86 DNS manager

- Ensuite cliquez avec le bouton droit sur « svr. SONATRAC.LOCAL », et cliquez sur « properties », comme montre la figure suivante :

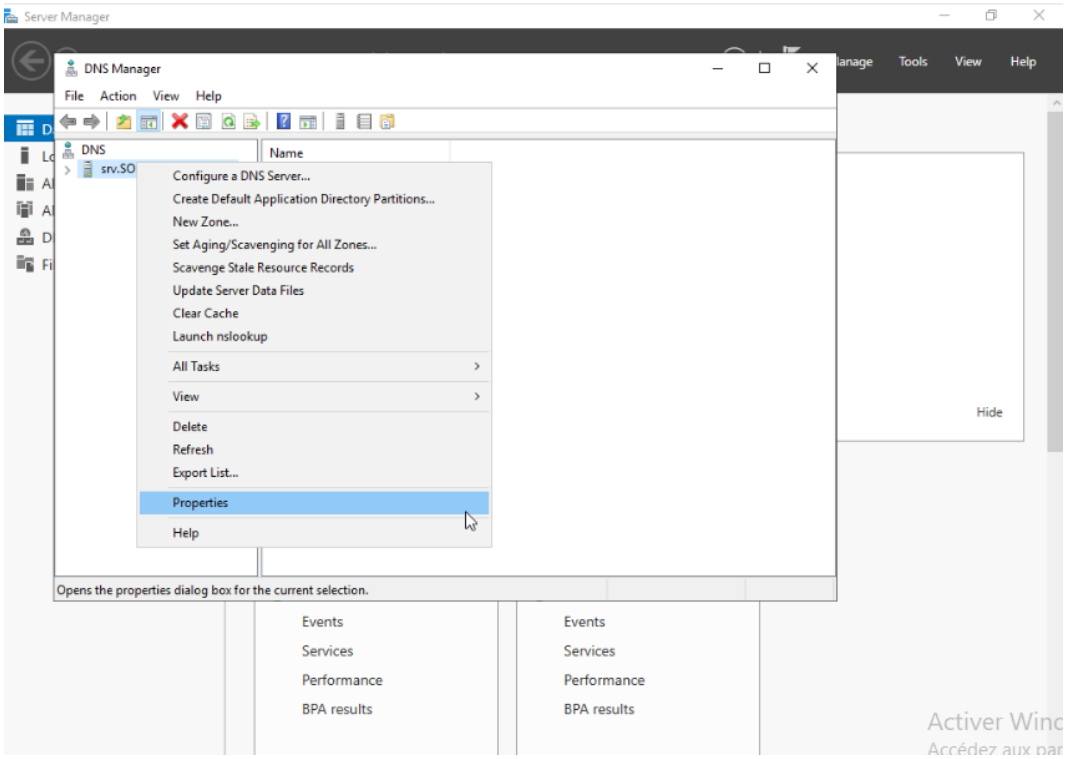

Figure III 87 DNS manager : propreties

- Sur cette icone « Interfaces », on trouve la destination DNS c'est tous les adresses IP, comme montre la figure suivante :

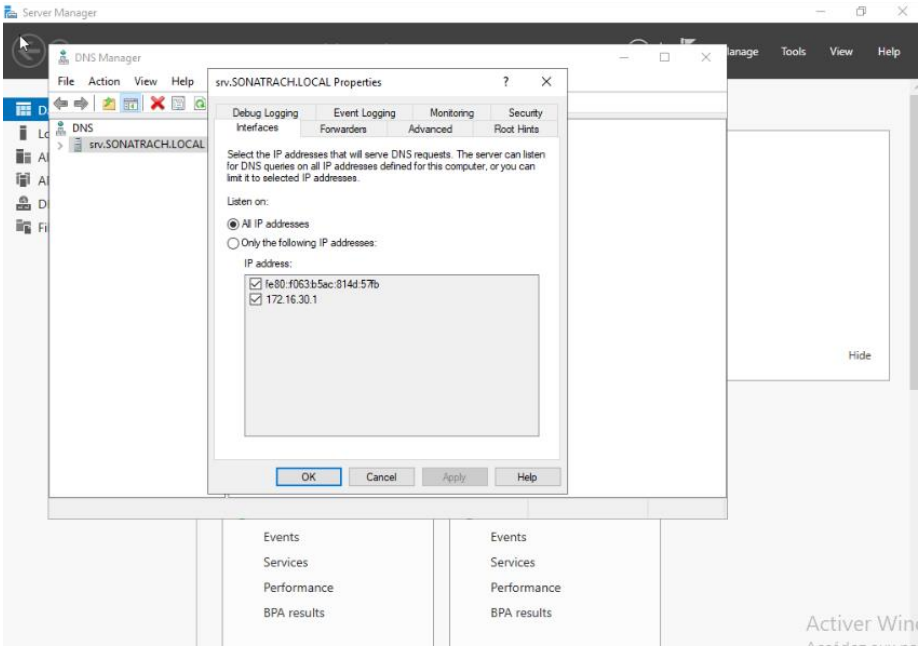

Figure III 88La destination de DNS

- Forwarders de DNS : 192.168.100.1, comme montre la figure suivante :

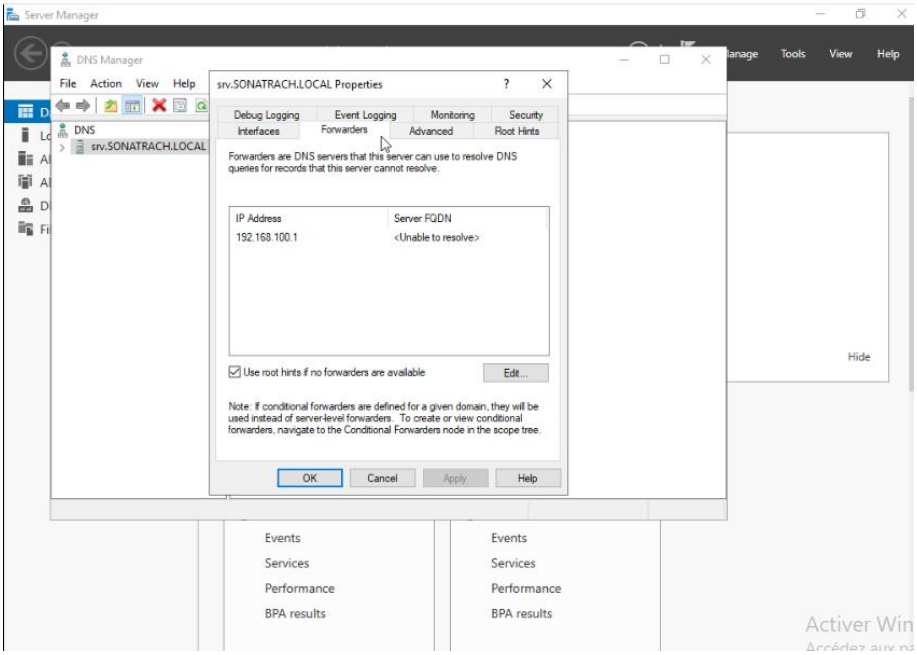

Figure III 89srv SONATRACH.LOCAL: Forwards

- Roothints :

  Lorsque le serveur DNS local ne parvient pas à résoudre une requête à l'aide de son cache ou de sa base de données, il envoie une requête à l'un des serveurs DNS racine sur Internet. Le serveur racine répondra avec une référence contenant les adresses des serveurs DNS faisant autorité pour le domaine de premier niveau (tel que .com ou .net) dans la requête d'origine. Il est recommandé d'effacer tous ces roothints.

  La figure III 88 présente les roots hints dans le folder SONATRACH.LOCAL :

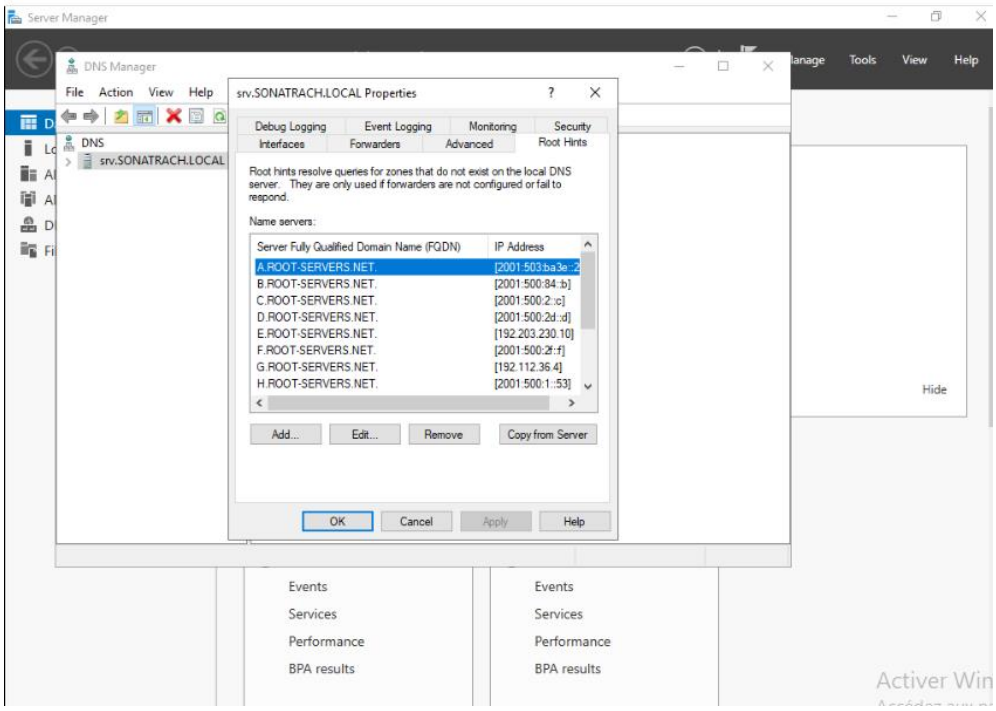

Figure III 90srvSONATRACH.LOCAL : Root Hint

Pour les raisons de la sécurité on supprime les roots hint, comme montre la figure suivante :

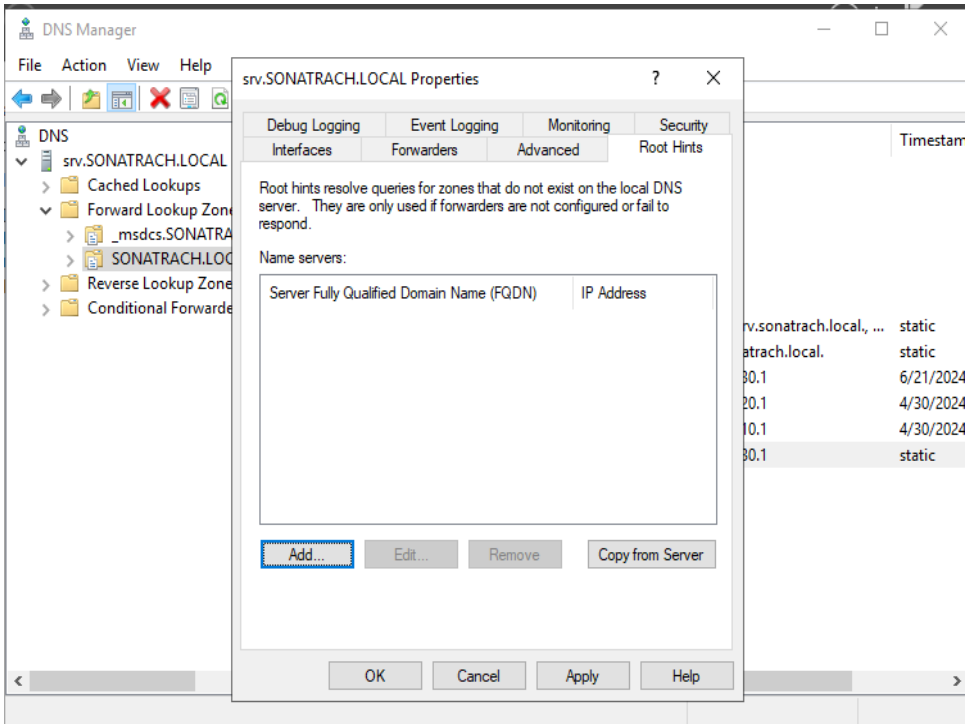

Figure III 91 Suppression des roots hints

Ajouter les PCs et le firewall au domaine de l'AD

❖ Dans le premier PC, on fait les configurations selon les étapes suivantes :

- Ouvrir l'explorateur Windows.

- Faire un clic droit sur Ce PC et cliquer sur Propriétés, comme montre la figure suivante :

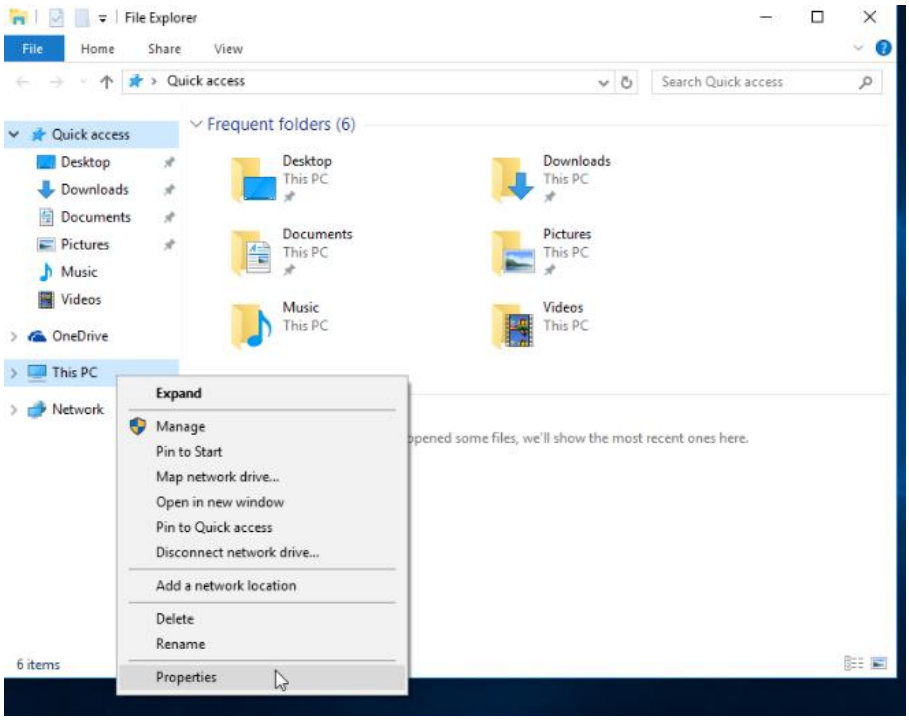

Figure III 92 Allez aux propriétés

- Cliquer sur Modifier les paramétrés
- Cliquer sur Modifier, comme montre la figure suivante :

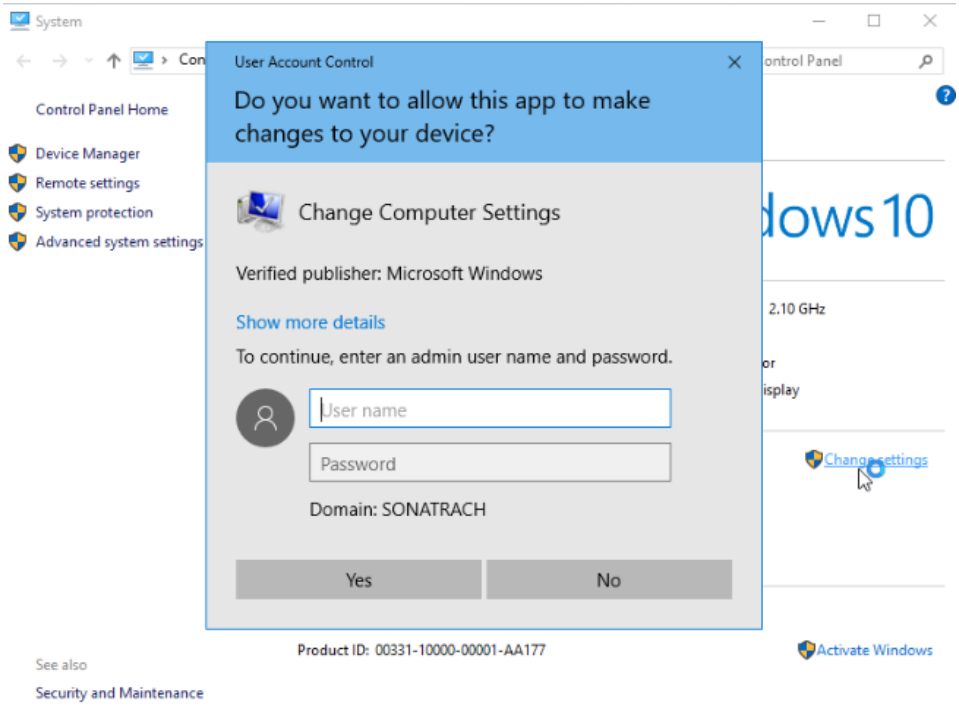

Figure III 93Modification des paramètres

- Entrer le nom de domaine et cliquer sur OK .
- Saisir les identifiants d'un compte Administrateur du domaine et valider.
- Valider le message de Bienvenu dans le domaine.
- Redémarrer l'ordinateur [54], comme montre la figure suivante :

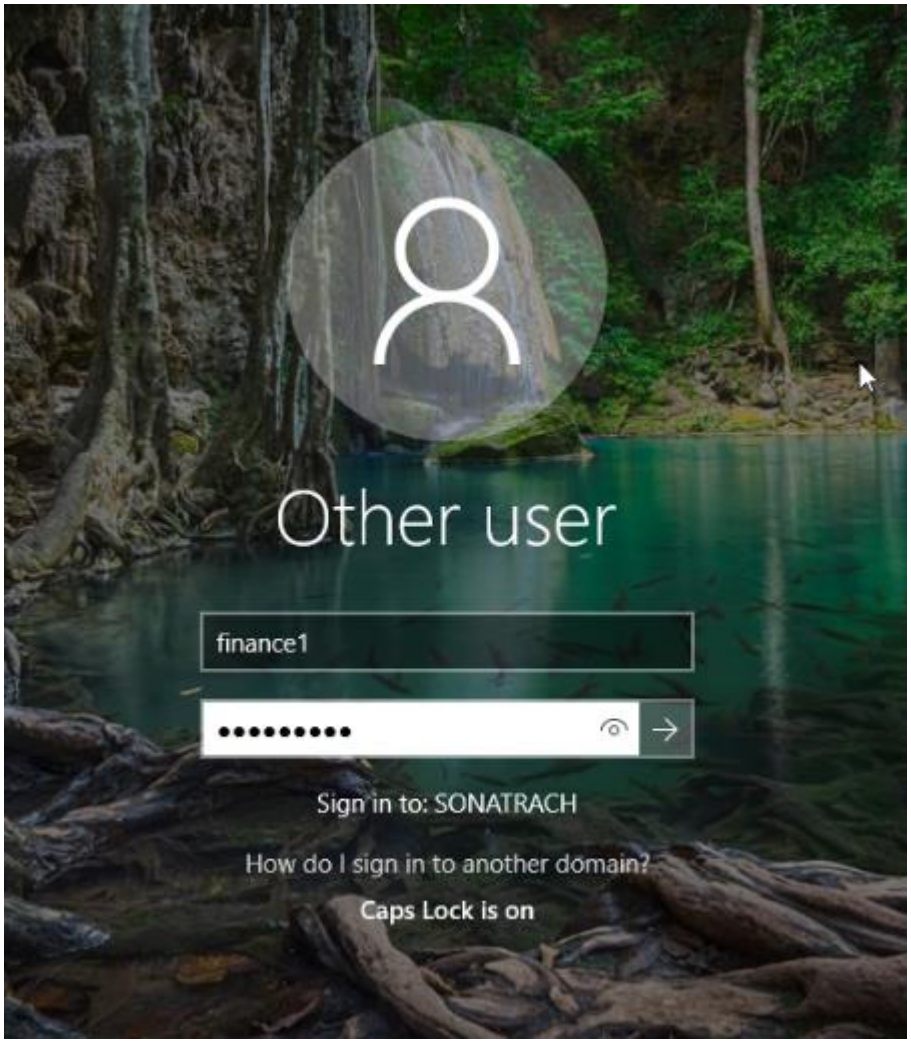

Figure III 94Identifier l'utilisateur

- **Remarque :**

  De la même façon on a ajouté tous les PCs au domaine.

III.18 Synchronisation de pfsense avec Active Directory

1. Cliquez sur le bouton "System" puis "User Manager" qui permet de gérer les utilisateurs et les groupes pfSense, ainsi que de configurer un serveur

d'authentification, comme montre la figure suivante :

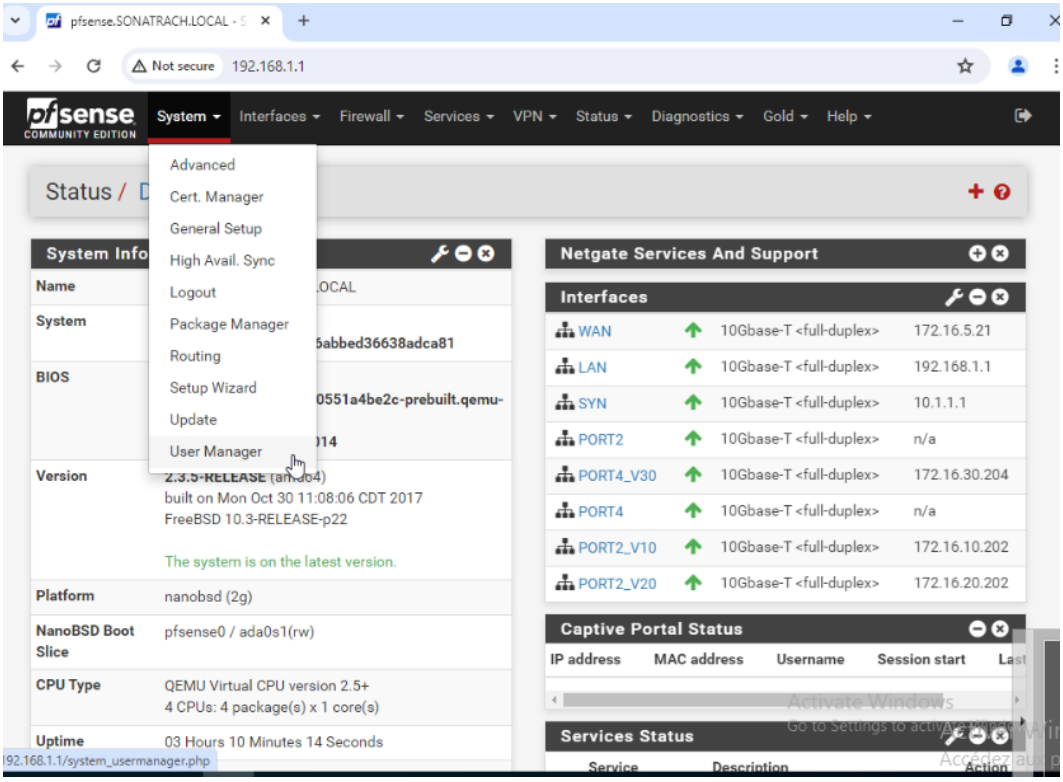

Figure III 95 Aller à l'user manager

1. Cliquez ensuite sur "Authentication Servers", comme montre la figure suivante :

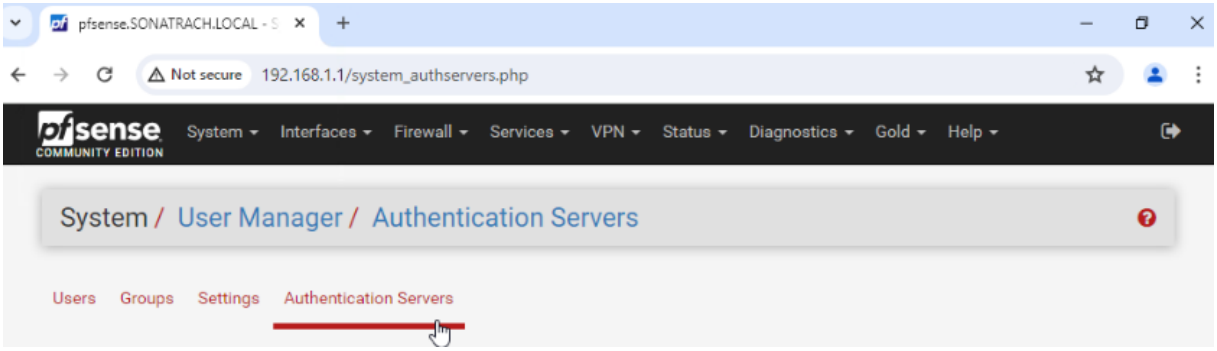

Figure III 96Aller au Authentication Servers

2. Les trois copies d'écran qui suivent font partie de la même page de configuration. Tous les paramètres n'ont pas besoin d'être modifiés, voyons cela ensemble.

- Descriptive name: Active Directory
- Type: LDAP
- Hostname or IP address : 172.16.30.1

La figure présente la configuration des paramètres de la configuration :

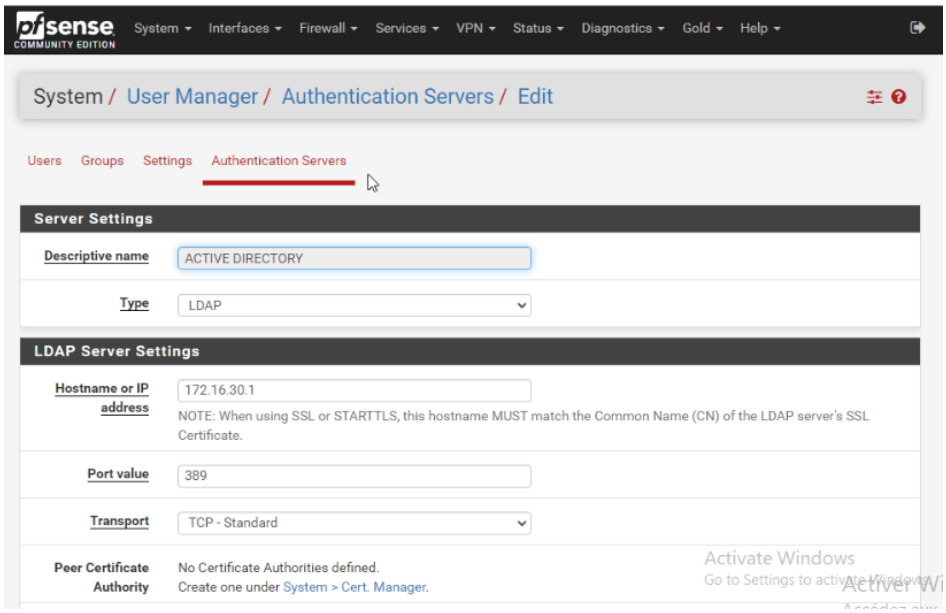

Figure III 97 Configuration des paramètres

1. Copiez ensuite la valeur retournée dans le champ "Bindcredentials" de la confpfSense, puis sur le champ juste à droite indiquez le mot de passe associé à ce compte. D'ailleurs, je suis surpris que le mot de passe s'affiche en clair !!! comme montre la figure suivante :

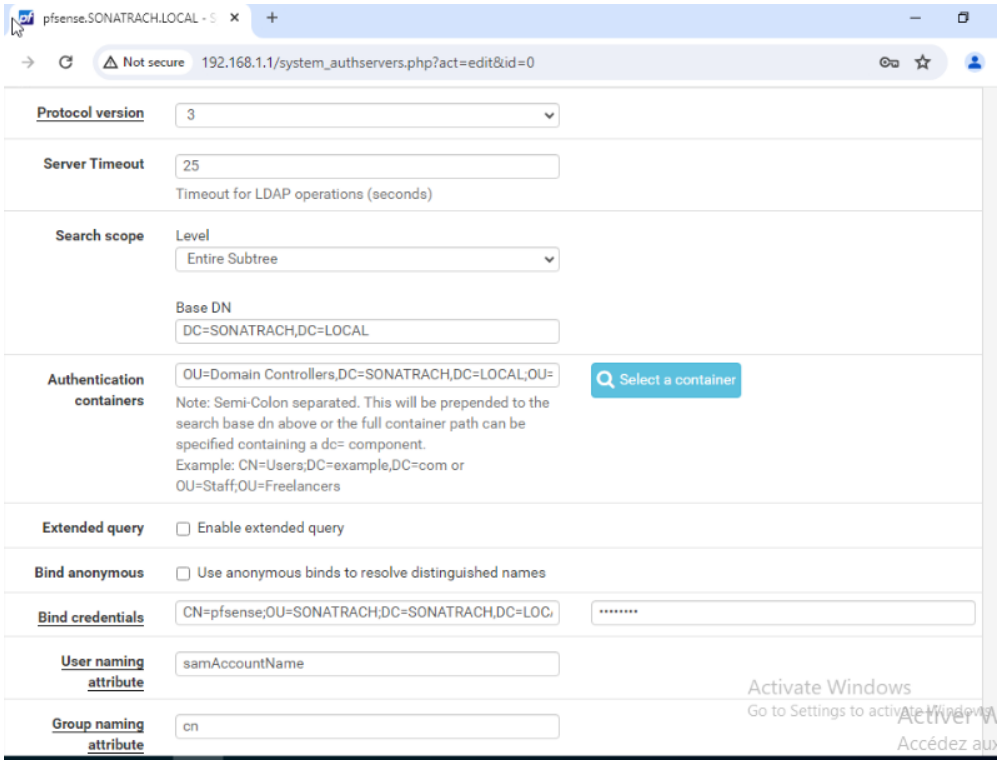

Figure III 98 Configuration des champ "Bind credentials"

2. Enfin, Vous pouvez seulement indiquer "group" à la place de "posixGroup", et veillez à ne pas cocher l'option "LDAP Server uses RFC 2307 style group membership" sinon pfSense ne pourra pas récupérer le nom du groupe auquel appartient votre utilisateur.
3. Sauvegardez la configuration avec le bouton "Save ». [55]

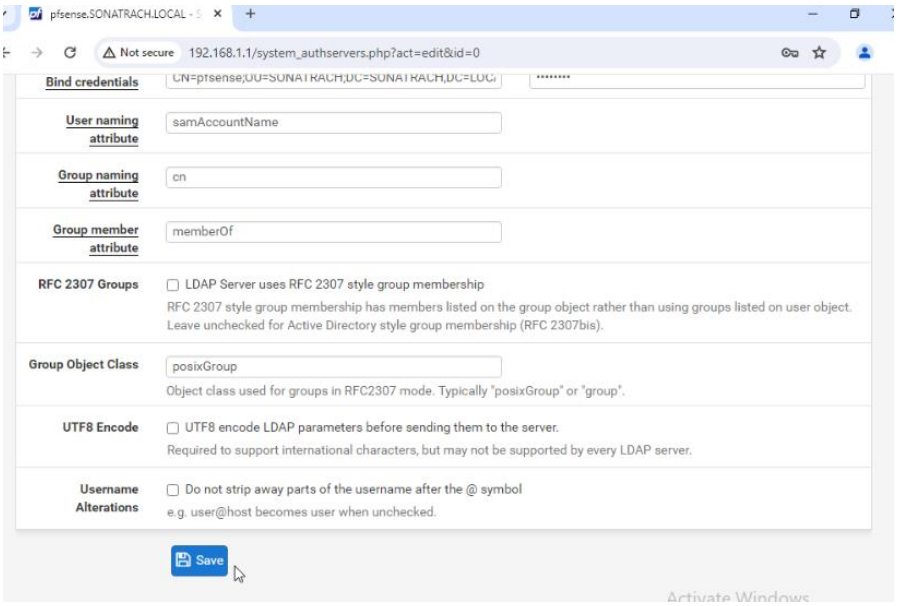

Figure III 99 Indiquer le groupe

- Résulta attendus :

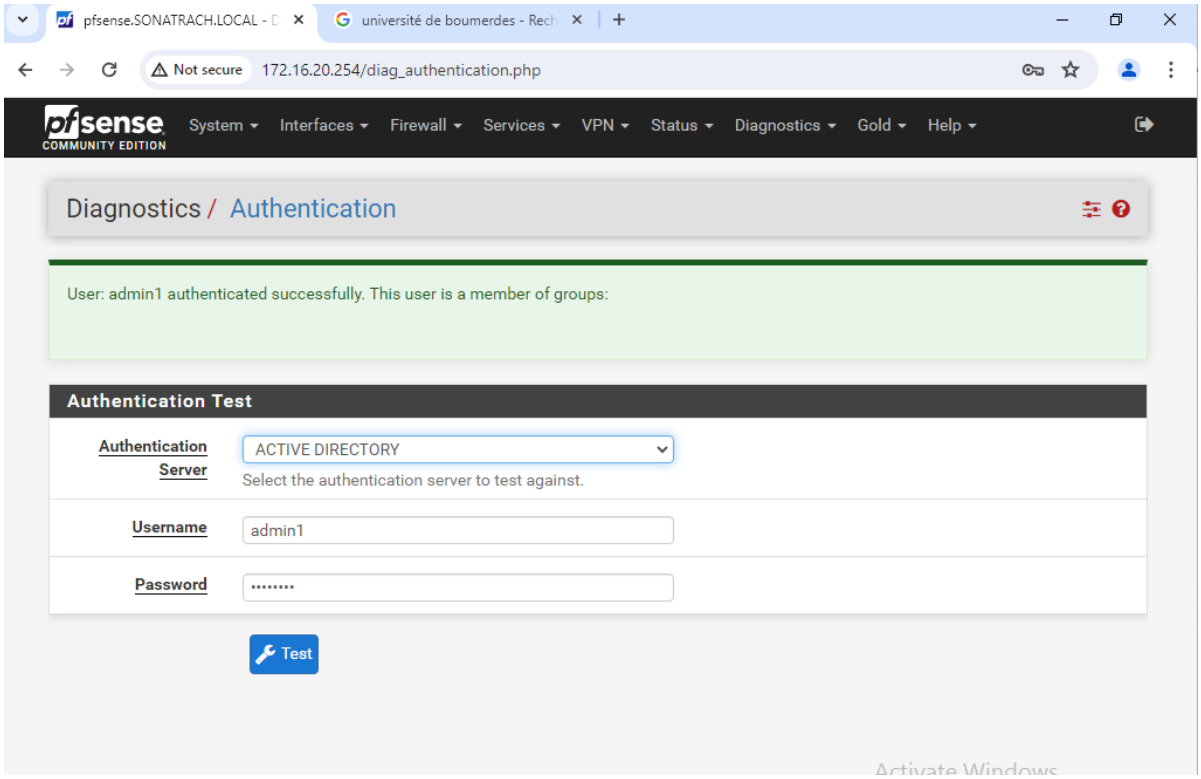

Figure III 100 Résulta de l'authentification de pfsense avec Active Directory

III.19 Configuration du portail captive

1. Accédez au menu Pfsense Services et sélectionnez l'option Portail Captif, comme montre la figure suivante :

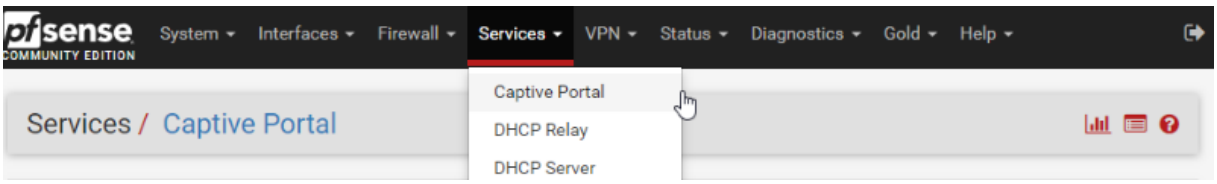

Figure III 101 Ajoute portal captive

1. Sur l'écran du portail Captive, cliquez sur "add" pour ajouter une nouvelle zone, comme montre la figure suivante :
2. Configurer la zone ainsi créée :
   - Activer la zone :

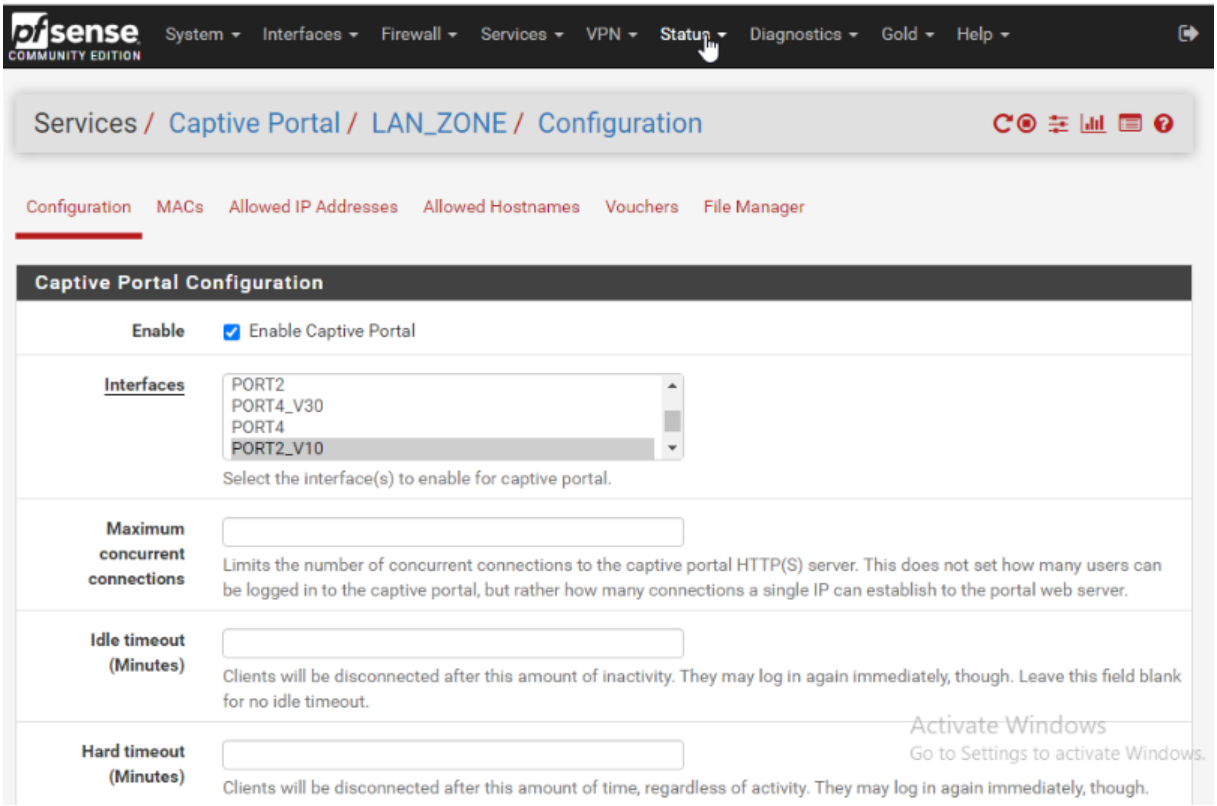

Figure III 102 Active la zone de captive portal

- Sur la zone d'authentification, effectuez la configuration suivante :

Méthode d'authentification : local user manager, comme montre la figure suivante :

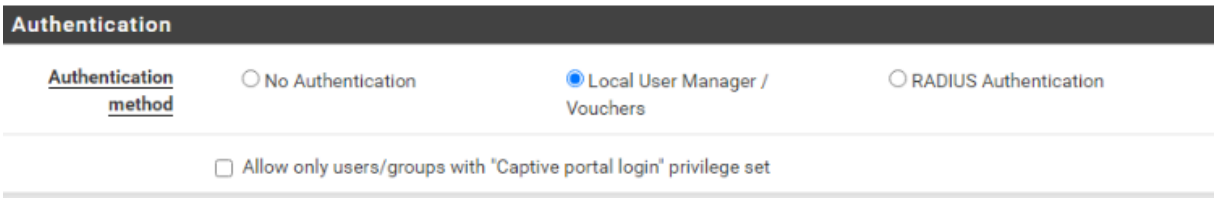

Figure III 103 Authentification de captive portal

3. Cliquez sur le bouton Enregistrer pour terminer la configuration pfsense Captive Portal.

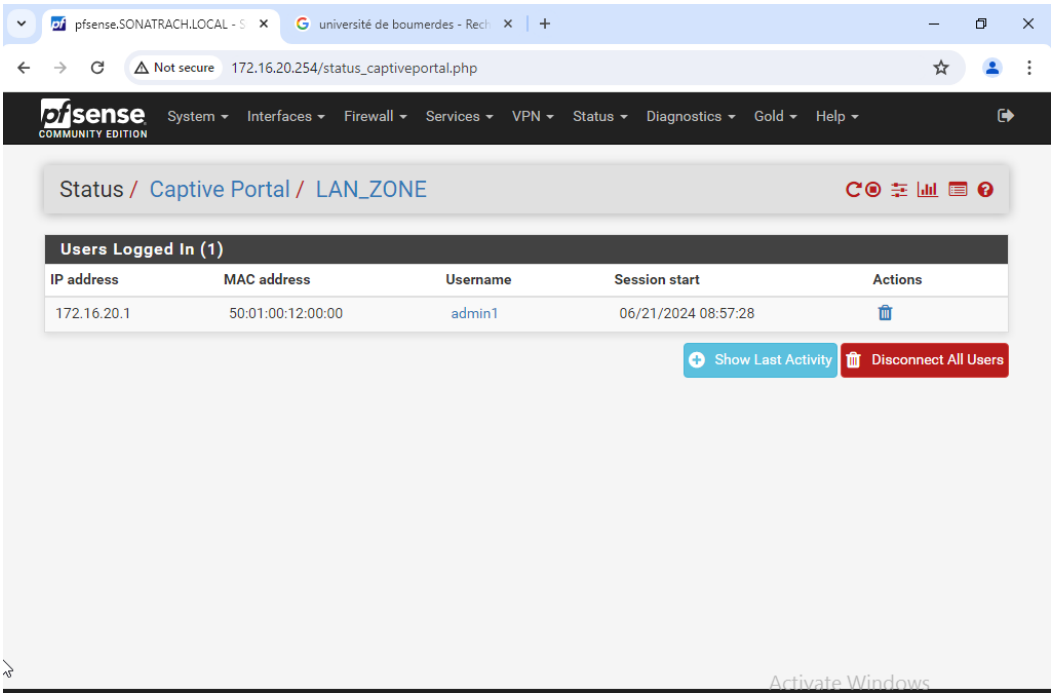

Figure III 104Configuration de portail captive

III.20 Test et validation

Pour vérifier que notre travail est bien fait on va :

1-Confirmer que l'utilisateur est dans le domaine « SONATRACH.LOCAL », comme montre la figure suivante :

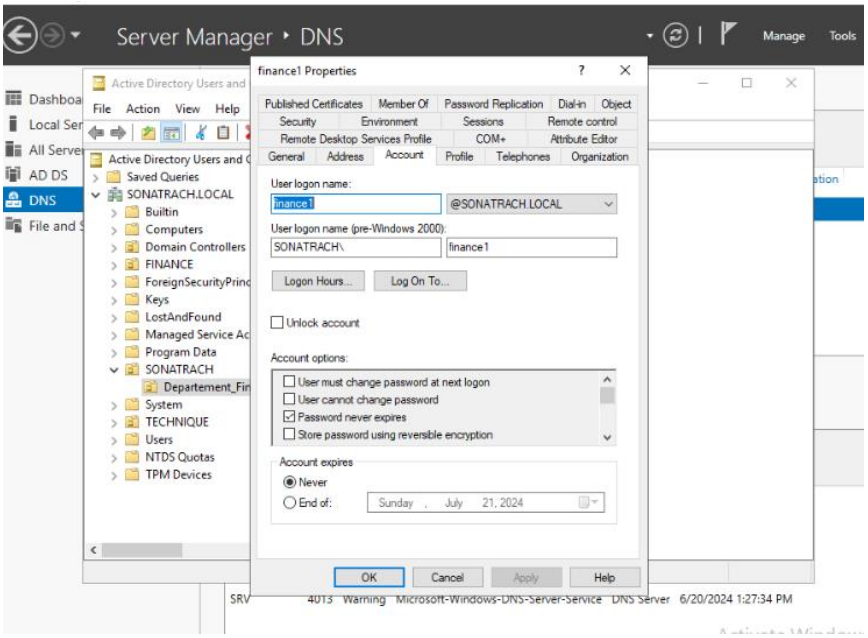

Figure III 105 Confirmer que l'utilisateur est dans le domaine

2-On va aller au l'utilisateur « finance1 », et identifier notre utilisateur, comme montre la figure suivante :

On remarque que l'utilisateur et dans le domaine : SONATRAC.LOCAL :

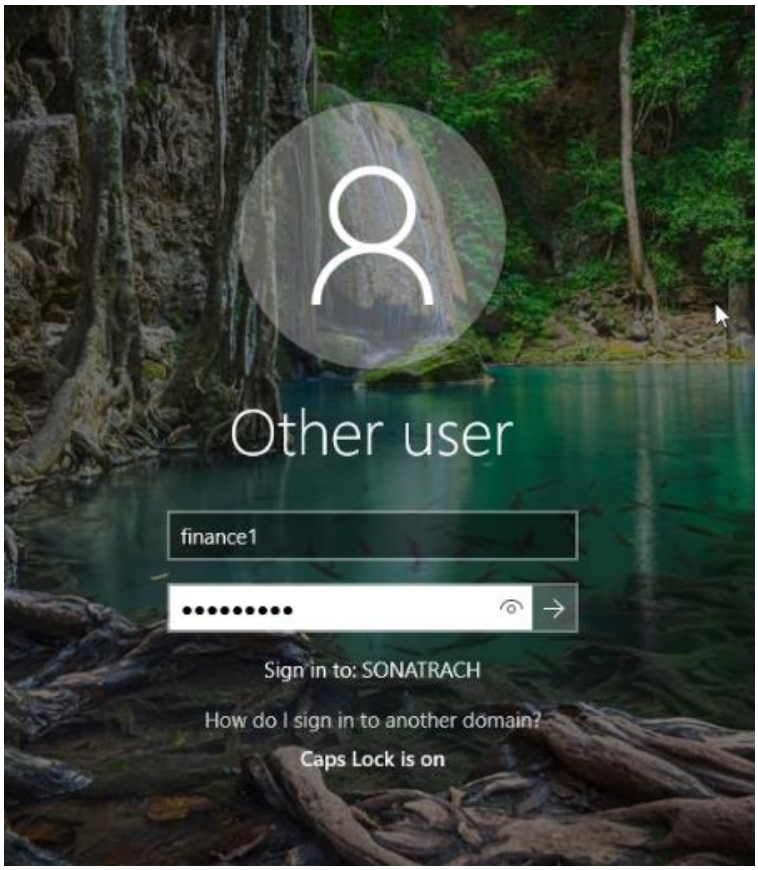

Figure III 106Identification de l'utilisateur finance1

3-On va aller à un site web :

Pour pouvoir accéder au site web, on va identifier le captive portail par le username et le password configuré dans l'Active Directory :

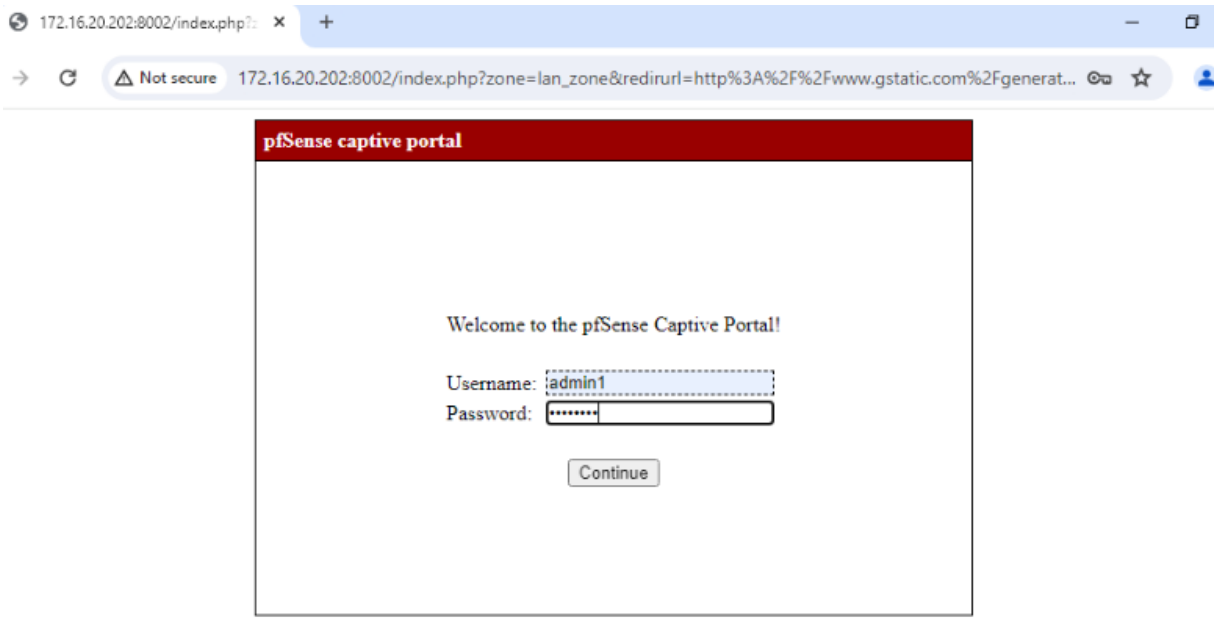

Figure III 107 Identifier le caotive portail

4- On va tester un site :

On prend comme exemple le site de « Université de Boumerdes », comme montre les figures III103 et III104 :

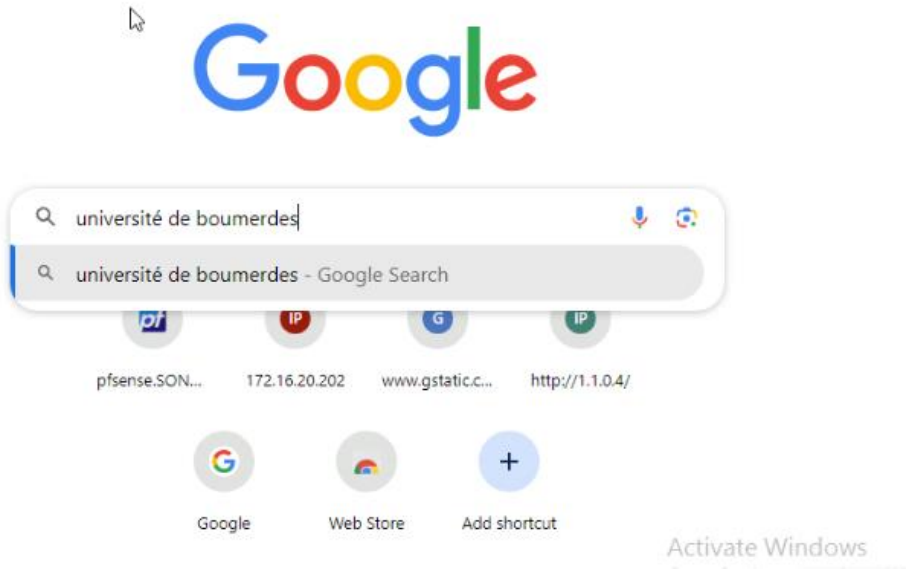

Figure III 108 Tester le site « Université de Boumerdes »

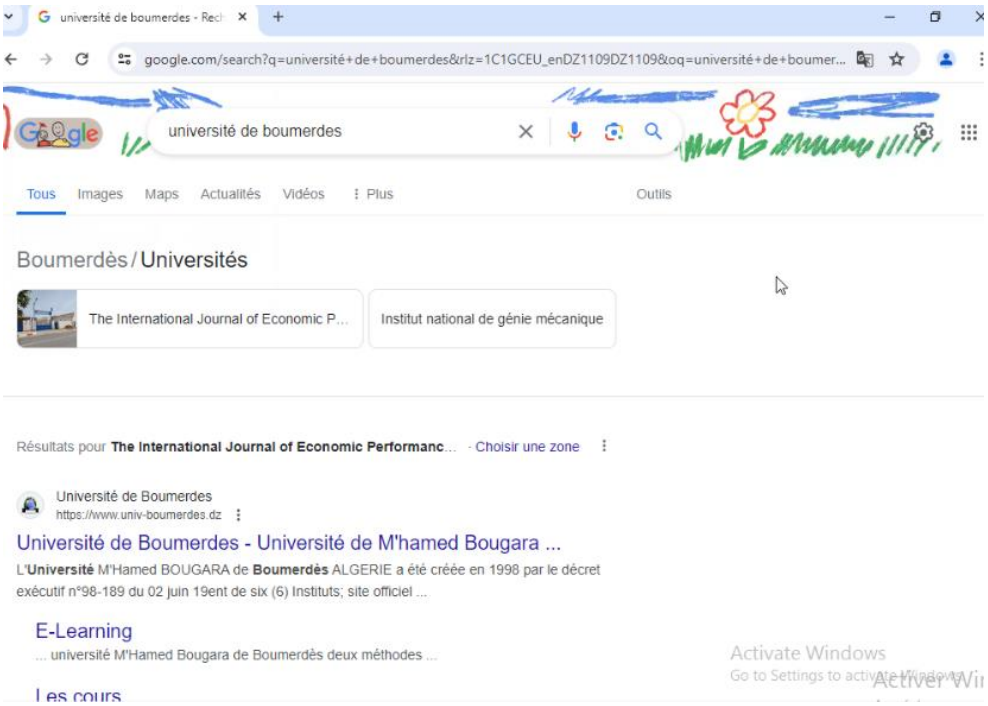

Figure III 109 Accéder au site

5-On a fait un deuxième test : le site de SONATRACH comme montre la figure suivante :

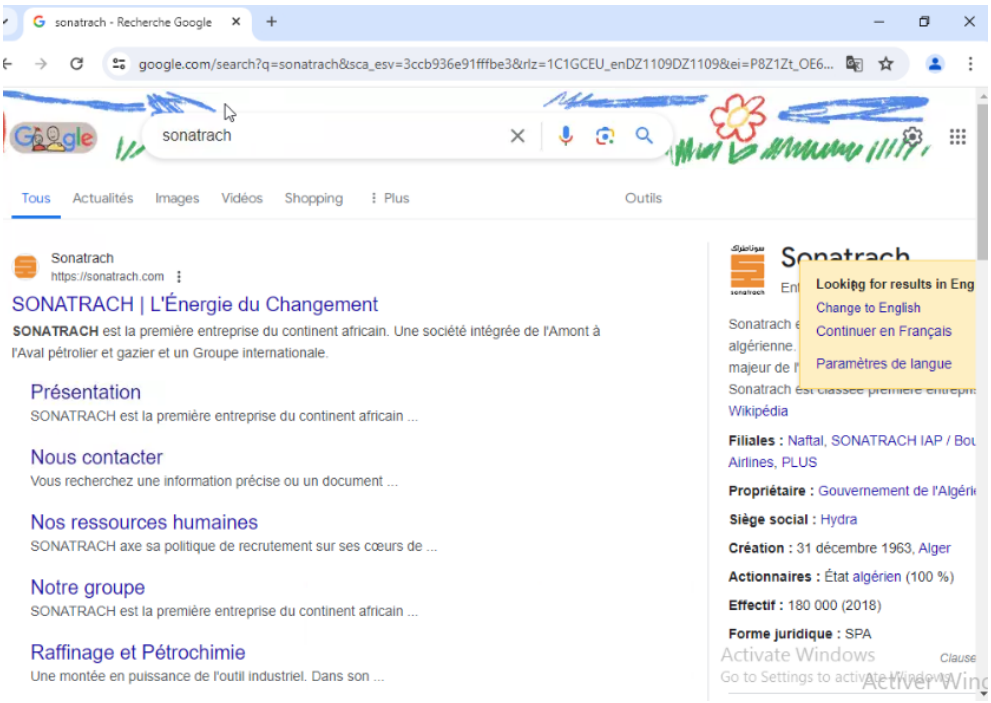

Figure III 110 Accéder au site SONATRACH

6- Enfin, dans pfsense/ captive portail, on trouve que l'utilisateur est en ligne.

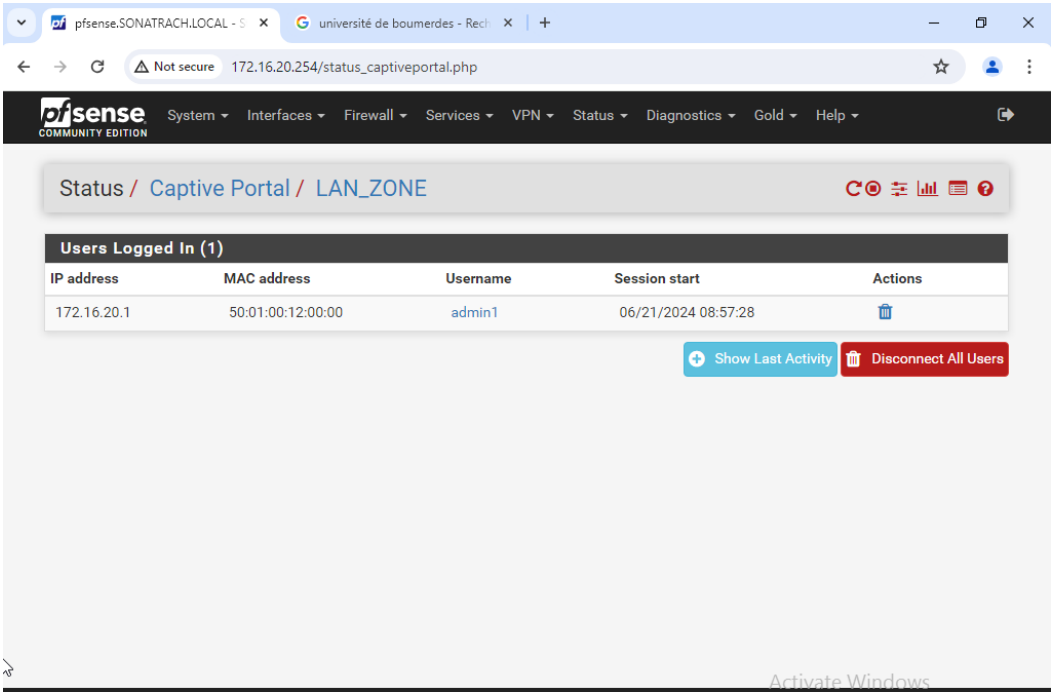

Figure III 111 Captive portail : L'utilisateur admin1 est enligné

III.21 Conclusion

En conclusion, l'intégration du firewall PfSense dans le schéma de réseau de l'entreprise s'avère être une solution efficace pour assurer la sécurité externe. En utilisant les fonctionnalités avancées de PfSense, telles que la gestion des règles de pare-feu, la détection d'intrusion et la protection contre les attaques DDoS, les rules, l'entreprise peut renforcer sa défense contre les menaces extérieures.

L'utilisation de PfSense offre également une grande flexibilité pour la configuration des politiques de sécurité, permettant ainsi une adaptation aux besoins spécifiques de l'entreprise. De plus, la surveillance en temps réel et la journalisation des événements fournis par PfSense offrent une visibilité accrue sur le trafic entrant et sortant, facilitant ainsi la détection précoce des tentatives d'intrusion ou d'activités suspectes.

En somme, l'intégration du firewall PfSense dans le schéma de réseau de l'entreprise constitue un élément essentiel pour renforcer la sécurité externe et protéger les actifs informatiques de l'entreprise contre les menaces en ligne.

Conclusion générale

Au terme de notre projet de fin d'études, nous avons réalisé une analyse approfondie de la sécurité des réseaux informatiques au sein de la division Exploration de Boumerdès.

Il est démontré au cours de ce travail la faisabilité de la mise en place d'un pare-feu à l'aide de l'outil Pfsense de manière à pouvoir mettre en place une politique de sécurité efficace du réseau informatique. Le problème était de savoir s'il est possible de surveiller les activités des différents utilisateurs en les forçant à s'authentifier, de superviser et de vérifier l'état des utilisateurs et filtrer les paquets.

Pour apporter une solution à ces inquiétudes, nous avons analysé les objectifs à atteindre qui sont de disposer d'un système capable de détecter les intrusions réseaux, d'authentifier les utilisateurs tout en contrôlant l'accès aux différentes ressources et de filtrer les accès. Pour atteindre ces objectifs, nous avons examiné les différents éléments constitutifs d'un réseau Informatique, y compris les types de réseaux, les supports de transmission, l'architecture des réseaux et les VLAN. Nous avons pris connaissance des réseaux informatiques, des différents types d'attaques, des techniques de protection des systèmes informatiques, des différents types de pare-feu. Nous avons également étudié Pfsense qui est l'outil retenu pour la mise en place. Pour assurer son efficacité, il a fallu installer et configurer des outils complémentaires comme Active Directory.

Grâce à ce projet, nous avons pu mettre en pratique nos connaissances théoriques dans un contexte concret et contribuer à la sécurité des réseaux informatiques de l'entreprise. Ceci a été une expérience enrichissante.

Comme perspective à ce travail, nous suggérons de mettre en place un Traffic shapper pour partager la bande passante, d'améliorer l'authentification en utilisant le 2FA (Authentification double facteur) et de mettre en place un système permettant de notifier l'administrateur par courrier électronique en cas d'intrusions sur le réseau.

Et pour la perte des donnés, on propose aussi la technologie DLP réseau (Data Loss Prevention réseau), qui veille à ce que les utilisateurs n'envoient pas d'informations sensibles ou critiques en dehors du réseau de l'entreprise. Ce terme décrit les logiciels qui aident un administrateur réseau à contrôler les données que les utilisateurs peuvent transférer.

Webographie

[1]URL : https://cisco.goffinet.org/ccna/ethernet/principes-conception-lan-cisco/#2-mod%C3%A8le-hi%C3%A9rarchique-%C3%A0-trois-couches--3-tier (consulté le 02/03/2024)

[2] URL : https://www.ciscopress.com/articles/article.asp?p=3150966&seqNum=2 (consulté le 02/03/2024)

[3] URL: https://www.chakerbchir.fr/lan-dc/nexus-vpc-virtual-port-channel#:~:text=Les%20composants%20d'une%20architecture,switches%20qui%20contiennEnt%20le%20VPC (consulté le 02/03/2024)

[4] URL : https://www.it-connect.fr/types-darchitectures-de-routage-inter-vlans/ (consulté le 02/03/2024)

[5] URL : https://bouchecousue.com/blog/les-vlans-pour-les-nuls/ (consulté le 03/03/2024)

[6] URL :https://www.manageengine.com/fr/network-configurationmanager/configlets/what-is-nat.html (consulté le 03/03/2024)

[7]URL : https://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco/(consulté le 06/03/2024)

[8]URL : https://www.fortinet.com/fr/resources/cyberglossary/dynamic-host-configuration-protocol dhcp#:~:text=Le%20protocole%20DHCP%20(Dynamic%20Host,l'acc%C3%A8s%20%C3%A0%20un%20r%C3%A9seau. (Consulté le 06/03/2024)

[9] URL : https://www.cloudflare.com/fr-fr/learning/dns/what-is-dns ,(consulté le 15/03/2024)

[10] URL :https://www.malekal.com/la-couche-du-modele-osi-pour-les-nuls/#Qu8217est-ce_le_modele_OSI , (consulté le 15/03/2024)

[11]URL : https://www.fortinet.com/fr/resources/cyberglossary/tcp-ip#:~:text=Le%20mod%C3%A8le%20TCP%2FIP%20est,des%20donn%C3%A9es%20entre%20les%20appareils (consulté le 15/03/2024)

[12]URL : https://web.maths.unsw.edu.au/~lafaye/CCM/secu/secuintro.html, (consulté le 20/03/2024)

[13] URL:https://itmates.fr/introduction-a-la-cybersecurite-episode-1/, (consulté le 20/03/2024)

[14]URL:https://www.lemagit.fr/definition/securite-des-reseaux , (consulté le 20/03/2024)

[15]URL : https://www.formatiques.com/quel-est-lobjectif-de-la-cybersecurite.html , (consulté le 22/03/2024)

[16] URL :https://www.ipi-ecoles.com/securite-informatique/, (consulté le 22/03/2024)

[17] URL : https://techno-skills.com/securite/cyber-securite-ethical-hacking/la-reconnaissance-footprinting/#:~:text=C'est%20quoi%20la%20Reconnaissance,moyens%20possibles%20pour%20l'attaquer , (consulté le 28/03/2024)

[18] URL :https://www.exter.fr/differentes-techniques-dattaques-utilisant-lingenierie-sociale/, (consulté le 02/04/2024)

[19] URL :https://cisco.ofppt.info/ccna1/course/module11/11.2.2.3/11.2.2.3.html , (consulté le 02/04/2024)

[20] URL :https://www.pandasecurity.com/fr/mediacenter/attaque-man-in-the-middle/, (consulté le 04/04/2024)

[21] URL :https://www.fortinet.com/fr/resources/cyberglossary/dos-vs-ddos#:~:text=Une%20attaque%20par%20d%C3%A9ni%20de,pour%20saturer%20une%20ressource%20cibl%C3%A9e., (consulté le 02/04/2024)

[22]URL :https://www.pandasecurity.com/en/mediacenter/dns-spoofing/, (consulté le 02/04/2024)

[23] URL : https://nordvpn.com/fr/cybersecurity/glossary/dhcp-attack/, (consulté le 02/04/2024)

[24] URL : https://www.infosectrain.com/blog/mac-flooding-attack/, (consulté le 02/04/2024)

[25] URL : https://www.skills4all.com/formation-cybersecurite-quels-sont-les-types-de-cybermenaces/ , (consulté le 05/04/2024)

[26] URL :https://www.cloudflare.com/fr-fr/learning/access-management/what-is-ssh/, (consulté le 06/04/2024)

[27] URL :https://www.marche-public.fr/Terminologie/Entrees/Protocole-SSL.htm, (consulté le 06/04/2024)

[28] URL :https://www.cloudflare.com/fr-fr/learning/ssl/what-is-https/, (consulté le 06/04/2024)

[29] URL :

https://support.hpe.com/hpesc/public/docDisplay?docId=sf000094844en_us&docLocale=en_US&page=index.html , (consulté le 15/04/2024)

[30]URL :https://fastercapital.com/fr/contenu/Chiffrement---Securisation-des-donnees---Chiffrement-dans-les-transactions-autorisees.html#Introduction-au-chiffrement-et---son-importance-dans-la-s-curisation-des-donn-es, (consulté le 15/04/2024)

[31]URL : https://cs.univ-batna2.dz/sites/default/files/web/files/securite_des_reseaux_partie_1.pdf, (consulté le 15/04/2024)

[32] URL : : https://www.it-connect.fr/les-listes-de-controle-dacces-acl-avec-cisco/, (consulté le 15/04/2024)

[33] URL : https://www.okta.com/fr/identity-101/ids-vs-ips/, (consulté le 15/04/2024)

[34]URL :https://www.appvizer.fr/services-informatiques/antivirus , (consulté le 15/04/2024)

[35] URL :https://www.forcepoint.com/fr/cyber-edu/firewall, (consulté le 20/04/2024)

[36] URL :] https://www.checkpoint.com/fr/cyber-hub/network-security/what-is-firewall/, (consulté le 20/04/2024)

[37] URL :https://www.certilience.fr/2024/03/maximiser-la-securite-reseau-les-firewalls/, (consulté le 20/04/2024)

[38] URL :https://www.ibm.com/docs/fr/power8?topic=support-ip-packet-filter-firewall, (consulté le 21/04/2024)

[39] URL :https://www.fortinet.com/fr/resources/cyberglossary/stateful-firewall, (consulté le 21/04/2024)

[40] URL :https://www.fortinet.com/resources/cyberglossary/proxy-firewall, (consulté le 21/04/2024)

[41] URL :https://www.oracle.com/dz/security/cloud-security/what-is-waf/#:~:text=Web%20Application%20Firewall)%20%3F-,Pare-feu%20d'applications%20web%2C%20d%C3%A9finition,DoS)%20au%20niveau%20des%20applications, (consulté le 21/04/2024)

[42] URL :https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html, (consulté le 21/04/2024)

[43] :https://fastercapital.com/fr/sujet/comment-modifier-ou-combiner-des-r%C3%A8gles-de-filtrage-pour-cr%C3%A9er-des-strat%C3%A9gies-de-trading-plus-complexes-et-flexibles%C2%A0.html, (consulté le 21/04/2024)

[44] URL :https://docs.sophos.com/nsg/sophos-firewall/19.0/Help/en-

us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/FirewallRules/RulesPoliciesBlockInternetBasedOnMacAddress/index.html, (consulté le 21/04/2024)

[45] URL :https://gplexpert.com/pfsense-securise-systeme-dinformation/, (consulté le 22/04/2024)

[46] URL : https://dspace.univ-eloued.dz/server/api/core/bitstreams/bc8feceb-5b91-4060-85c7-41551a243263/content, (consulté le 22/04/2024)

[47] URL : https://www.netgate.com/, (consulté le 22/04/2024)

[48] URL : https://www.cyber-management-school.com/outils-logiciels-et-technologies/active-directory-quest-ce-que-cest/ , (consulté le 25/04/2024)

[49] : URL :https://www.lebigdata.fr/active-directory-definition-fonctionnement, (consulté le 25/04/2024)

[50] : https://www.provya.net/?d=2015/01/13/13/31/57-pfsense-comprendre-la-gestion-des-interfaces-reseaux (consulté le 02/05/2024)

[51] : https://subscription.packtpub.com/book/cloud-and-networking/9781849514866/1/ch01lvl1sec11/configuring-the-wan-interface (consulté le 02/05/2024)

[52] : https://www.oreilly.com/library/view/pfsense-2-cookbook/9781849514866/ch05s02.html (consulté le 05/05/2024)

[53] : https://infrasos.com/how-to-setup-active-directory-on-windows-server-2022/(consulté le 06/05/2024)

[54] : https://rdr-it.io/joindre-un-ordinateur-a-un-domaine-windows-10-2016/(consulté le 07/05/2024)

[55] :https://www.it-connect.fr/pfsense-2-3-administration-deleguee-avec-utilisateurs-active-directory/#II_Declarer_lannuaire_Active_Directory_sur_pfSense (consulté le 07/05/2024)