République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Université Abderrahmane Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master professionnel en Informatique

Option :Administration et Sécurité des Réseaux

Mise en place d'une architecture réseau sécurisée pour l'entreprise Amimer Energie

Réalisé par :
Mme. BENAMAR Zahra
Mme. BOUDEBBOUZ Nassima

Encadré par :
M. AMROUN Kamal
(U.A/Mira Béjaïa)
M. ELSAKAAN Nadim
(U.A/Mira Béjaïa)

Examiné par :

M.SELLAMI Khaled : U.A/Mira Béjaïa - Examinateur
M.NAFI Mohammed : U.A/Mira Béjaïa - Examinateur

Promotion : 2020/2021

Remerciements

La réalisation de ce projet s'est avéré une tâche ardue et enrichissante qui n'aurait pu être complétée sans le soutien de nombreuses personnes.

En premier lieu, on tiens à exprimer toute notre reconnaissance à nos encadreurs de mémoire, Monsieur Amourn Kamel et Monsieur Elsakaan Nadim qui par leurs paroles, leurs écrits, leurs conseils et leurs critiques a guidé nos réflexions ainsi que par leurs encouragements et surtout pour la confiance inébranlable en nos capacités à réussir et à donner le meilleure de nous-même.

En second lieu, je remercie l'encadreur de stage Madame Semaoun Sarah , responsable de l'etreprise Amimer Energie Seddouk où on a effectuer notre stage pratique dans le but de l'obtention le diplôme de Master en Informatique, mention, Administration et sécurité des réseaux.

Enfin, on aimerais exprimer notre gratitude à nos famille,qui nous ont toujours encouragées dans la poursuite de nos études, ainsi que pour leurs aide,leurs compréhension et leurs soutien.

Dédicace

À mes chers parents,aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'espère que votre bénédiction m'accompagne toujours.Que ce modeste travail soit l'exaucement de vos vœux tantformulés, le fruit de vos innombrables sacrifices, bien que je ne vous en acquitterai jamais assez.Puisse Dieu, le Très Haut, vous accorder santé, bonheur et longue vie et faire en sorte que jamais je ne vous déçoive.

A mes frères Yanis et Simou que j'aime beaucoup et que j'ai trouvé à mes cotés.

A mon chèr ami Massi, cette personne que je porte beaucoup d'amour et de tendresse, je suis très reconnaisant sur ta présence tout au long de ma préparation, je suis tellement chanceux de t'avoir, UN GRAND MERCI.

A ma chère binôme et amie Wissam, ta présence est remarquable tout au long de notre études et notre préparation de mémoire.

A mes amis que je nomme Cylia, Nawel, Alissia, Sissa, Thileli, Malika, Rima, Lydia, Cola.

En témoignage de mon affection fraternelle, de ma profonde tendresse et reconnaissance.

Merci d'être toujours là pour moi.

Benamar Zahra

Dédicace

Afin d'être reconnaissante envers ceux qui m'ont appuyé et encouragé à effectuer ce travail de recherche, je dédie ce mémoire :

A mes très chère mère « noria» malgré son absence mais ses prières sont toujours avec moi, tous les sacrifices consentis et ses précieuse conseils.

A mes précieuses soeurs « Sonia » et « Nacera » et à mon bien-aimé frère « Mokran» pour toute la complicité et l'entente qui nous unissent, pour leur soutien et leur aide tout au long de ce travail.

A mon beau frère « Hakim ».

mon prochain chère neveu .

A ma chère binome « zahra ».

A mes très chères amis «tutuch,zahra,Lydia,Alicia,cylia»

A toute ma famille «cousines et cousins», mes enseignants et mes camarades. A tous ceux qui ont participé à ce travail et m'ont soutenu de prêt ou de loin.

Boudebbouz Nassima

Liste des abréviations

OSI :Open System Inter-connections.

TCP/IP :Transmission Control Protocol/Internet Protocol.

VLAN :Virtuel Local Area Network.

VTP : VLAN Trunking Protocol.

ACL :Access Control List.

DMZ : demilitarized zone.

VM :Virtuel Machine

SSH :Secure Shell.

DHCP :Dynamic Host Configuration Protocol.

DNS :Domain Name System.

AD :Active Directory.

LAN :Local Area Network.

ASCII :American Standard Code for Information Interchange.

IEEE :Institute of Electrical and Electronics Engineers.

PVLAN :Private Virtuel Local Area Network.

VACL :VLAN Access Control List.

MAC :Media Access Control.

VPN :Virtuel Privat Network.

IPSEC :Internet Protocol Security.

HSRP : Hot Standby Router Protocol.

MPLS :MultiProtocol Label Switching.

PKI :Public Key Infrastructure.

AH :

ESP :Stabilisateur Eléctronique Programmé.

NAT :Network Address Translation.

BPDU :Bridge Protocol Data Units.

TCN :

RSTP : Rapid Spanning Tree Protocol.

PAGP :Port Aggregation Protocol.

Table des matières

Table des figures

Liste des tableaux

Introduction générale

De nos jours, la sécurité informatique est quasi-indisponsable pour le bon fonctionnement de n'importe quel réseau informatique. Pour cela, les administrateurs réseau d'entreprise doivent installer des mécanismes de gestion et de sécurité plus robustes de leur réseau.

La sécurité informatique reste une problématique importante, car les effets sont de plus en plus lourds. Notamment avec le développement de l'utilisation d'internet, ce qui l'expose à une multitude de menaces potentielles qui sont de plus en plus ciblées et plus en plus sophistiquées mais le réseau peut également être mis en péril par les menaces intérieur de l'organisme.

Afin d'éviter les risques d'attaques, il faut garantir une sécurité du réseau informatique de l'entreprise et le rendre moins vulnérable. L'objectif de notre projet est de pouvoir mettre un mécanisme de sécurisation des échanges de données dans le réseau local de l'entreprise Amimer Énergie. En plus, il est nécessaire de segmenter le réseau local en plusieurs LAN virtuels(VLAN) pour réduire les domaines de collisions et éviter les congestions. Ce qui permet de renforcer la sécurité au niveau du réseau local.

Pour atteindre ces objectifs, nous avons à notre disposition plusieurs solutions de sécurisation parmi lesquelles, on mettra en place des VLANs comme on va choisir le protocole IPSec qui est le principal outil permettant d'implémenter les VPN ainsi pour bien sécuriser l'architecture proposée pour l'entreprise on appliquera plusieurs protocoles de sécurité (RADIUS, SSH, HSRP, VTP, LACP..) et des configurations qui vont renforcer la sécurité du réseau de l'entreprise et on présentera brièvement dans les chapitres venant.

Pour réaliser ce projet nous avons partitionné notre mémoire en quatre chapitres. Le premier chapitre concerne la présentation des parcs informatique, les modèles de référence, la sécurité informatique et la sécurité des réseaux . Le second chapitre porte sur la présentation de l'organisme d'accueil, l'étude et la critique de l'existant ce qui nous a permis de mieux comprendre le fonctionnement du réseau entreprise. Dans le troisième chapitre nous abordons la réalisation d'une nouvelle architecture à travers le simulateur GNS3. Enfin, dans le quatrième chapitre on passe aux tests pour voir les résultats de nos configurations.

Chapitre 1

Généralités sur les réseaux et la sécurité des VLANs

1.1 Introduction

D'une manière générale, un réseau n'est rien d'autre qu'un ensemble d'objets ou de personnes connectés ou maintenus en liaisons et dont le but est d'échanger des informations ou des biens matériels. Toute au long de ce chapitre,nous nous concentrerons sur des concepts complémentaires en rapport avec l'architecture des réseaux en vue d'élargir nos compétences. Nous serons ainsi en mesure de réaliser un projet de conception d'un réseau d'entreprise avec une vision globale de la mise en réseau.Pour bien organisé notre travail nous allons le diviser en trois parties. Dans la première partie, nous allons définir brièvement les deux parcs informatique matériel dont nous allons citer les différents équipements réseaux les plus courants ainsi le câblage et le logiciel dont nous allons citer les différents logiciel qu'on a utiliser durant notre travail et enfin on passe à la présentation des serveurs utiliser.

Dans la deuxième partie les modèles de référence(OSI et TCP/IP) et la sécurité informatique ensuite pour bien terminer le chapitre nous allons approfondir dans la troisième partie sur la sécurité des réseaux où nous allons commencer par la présentation des VLANs d'une façon détaillée pour bien comprendre ses fonctionnalités et son rôle dans la sécurité des réseaux (VLAN privé, VLAN ACL..) et enfin on passe à définir les ports de sécurité, les VPN et la DMZ.

1.2 Partie 1 : Les parcs informatique et les serveurs utilisés

1.2.1 Le parc matériel

1-Equipements réseau

Voici une liste des équipements réseau les plus courants :

— Routeur
— Commutateur (switch)
— Concentrateur (hub)
— Répéteur
— Pont (bridge)
— Passrele (gateway)
— Modem
— Pare-feu

-Routeur :est un équipement réseau informatique assurant le routage des paquets son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles[1].

Il y a habituellement confusion entre routeur et relais, car dans les réseaux Ethernet les routeurs opèrent au niveau de la couche 3 du modèle OSI .

-Commutateur : Il permet l'interconnexion d'appareils communicants, d'ordinateurs, des serveurs, de périphériques, relie à un même réseau physique [2].

Il existe trois couches du modèle hiérarchique ou on peut trouver les commutateurs :

— La couche cœur : C'est la couche supérieure dont le rôle consiste à relier entre eux les différents segments d'un réseau à savoir : les sites distants, les réseaux

locaux (LANs) ou les étages de l'immeuble d'une société. Cette couche est aussi appelée Backbone.

— La couche distribution : Le rôle de cette couche est de filtrer, de router, d'autoriser ou non les paquets. Cette couche se trouve entre la couche cœur et la couche d'accès c'est-à-dire entre la partie « liaision » et la partie « utilisateur ». La segmentation du réseau commence ici en ajoutant plusieurs switches de niveau 3 qui sont reliés à la fois à la couche cœur et à la couche d'accès.

— La couche accès : Cette couche qui est la dernière du modèle hiérarchique permet de connecter les périphériques des utilisateurs finaux au réseau. À ce niveau, on utilise des switche de niveau 2 car la configuration de ce type de switchés pose moins de contraintes : le besoin en performances n'est plus vraiment une nécessité car chaque switch aura un nombre d'utilisateurs égal à son nombre de ports (moins 1 ou 2 pour le trunk entre la couche d'Access et la couche de distribution). Les traitements restent basiques.

-Concentrateur : permet de concentrer le trafic provenant de différents équipements terminaux. Cela peut se réaliser par une concentration du câblage en un point donné ou par une concentration des données qui arrivent simultanément par plusieurs lignes de communication [3].

-Répéteur : C'est un organe non intelligent, qui répète automatiquement tous les signaux qui lui arrivent et les transitent d'un support vers un autre support. Au même temps, le répéteur régénère les signaux, ce qui permet de prolonger le support physique vers un nouveau support physique. Il doit avoir des propriétés en accord avec le réseau [3].

-Pont : C'est un organe intelligent, capable de reconnaître les adresses des blocs d'information qui transitent sur le support physique. Un pont filtre les trames et laisse passer les blocs destinés au réseau raccordé. En d'autres termes, un pont ne retransmet que les trames dont l'adresse correspond à une machine située sur le réseau raccordé [4].

-Passerelle : C'est un système matériel et logiciel permettant de faire la liaison entre deux réseaux ou deux réseaux de télécommunications, aux caractéristiques différentes. Lorsque l'utilisateur d'un réseau souhaite accéder à un réseau utilisant un protocole différent, la gateway examine la légitimité de sa demande,si celle-ci respecte les conditions fixées par l'administrateur du réseau visé, alors la gateway établit une liaison entre les deux réseaux [4].

-Modem : C'est un périphérique qui permet de se connecter à internet. C'est en quelque sorte la « porte d'accès » à internet. Il se charge de convertir toutes les données numériques en ondes analogiques et, à l'inverse, peut également reconvertir les ondes analogiques en données numériques [4].

Pare-feu : c'est un équipement conçu pour protéger les données d'un réseau. Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur [5].Son Objectif est de :

— Contrôler et Gérer les connexions sortantes à partir du réseau local.
— Protéger le réseau interne des intrusions venant de l'extérieur.
— Surveiller ou tracer le trafic entre le réseau local et Internet.
— Protéger des réseaux à adressage privé.

Il existe deux types de pare-feu qui sont :

1. **Proxy** :Le pare-feu a pour objectif de couper la communication entre un client

et un serveur ou entre un client et un autre client. Ce type ne permet pas à un attaquant d'accéder directement à la machine attaquée, ce qui donne une forte protection supplémentaire [5].

2. **Applicatif** :Le pare-feu détecte les flots applicatifs et les interrompt ou non suivant les éléments filtrés [5].

2-Supports physiques

-Paire de fils torsadés : C'est le support de transmission le plus simple,elle est constituée d'une ou de plusieurs paires de fils électriques agencés en spirale. Ce type de support convient à la transmission analogique comme numérique. Les paires torsadées peuvent être blindées, une gaine métallique enveloppant complètement les paires métalliques, ou non blindées. Elles peuvent être également « écrantées »,dans ce cas, un ruban métallique entoure les fils [6].

-Câble coaxial : Il est constitué de deux conducteurs cylindriques de même axe, l'âme et la tresse, séparés par un isolant ce dernier permet de limiter les perturbations dues au bruit externe. Si le bruit est important, un blindage peut être ajouté. Quoique ce support perde du terrain, notamment par le support à la fibre optique, il reste encore très utilisé [6].

-Fibre optique : C'est un faisceau lumineux modulé ,elle comporte des composantes extrémités qui émettent et reçoivent les signaux lumineux [6].

1.2.2 Le parc logiciel

GNS3 est un simulateur d'équipements Cisco. Cet outil permet donc de charger de véritable IOS (Internetwork Operating System) Cisco et de les utiliser en simulation complète sur un simple ordinateur. Il est utilisé par des ingénieurs réseaux dans le monde pour émuler, configurer, tester et dépanner des réseaux virtuels et réels, comme il permet de connecter l'hyperviseur de machines virtuelles depuis Vmware ou Virtualbox. En bref,il permet d'architecturer les réseaux simples et complexes, et les simuler virtuellement c'est un logiciel libre qui fonctionne sur de multiples plateformes : Windows, Linux et MacOs [7] .

FIGURE 1.1 – GNS3

1-Vmware Workstation 16

Machine Virtuel (VM)est un environnement entièrement virtualisé qui fonctionne sur une machine physique. Elle exécute son propre système d'exploitation (OS) et bénéficie des mêmes équipements qu'une machine physique : CPU, mémoire RAM, disque dur et carte réseau. Plusieurs machines virtuelles avec des OS différents peuvent coexister sur le même serveur physique : Linux, Mac Os, Windows... [8].

FIGURE 1.2 – Vmware Workstation

2-Windows server 2016

Windows Serveur 2016 est un système d'exploitation de Microsoft orienté serveur basé sur l'architecture Windows NT. Il relie les environnements locaux avec Azure. Il ajoute de nouvelles couches de sécurité tout en vous aidant à moderniser les applications et l'infrastructurer.Il propose ainsi différents services orientés serveur, comme la possibilité d'héberger un site web, la gestion des ressources entre les différents utilisateurs et applications, ainsi que des fonctionnalités de messagerie et de sécurité [8].

FIGURE 1.3 – Windows Server 2016

3-Windows 10

Windows 10 est un système d'exploitation de Microsoft sorti le 29 juillet 2015. Il succède Windows 7 et Windows 8.1. Cette nouvelle version introduit plusieurs changements importants. Tout d'abord, elle est la première à fonctionner sur toutes les plateformes existantes : ordinateurs de bureau et portables, smartphones, tablettes et montres connectées. L'interface de l'OS s'adapte automatiquement au format et au mode de saisie,par ailleurs, Microsoft a indiqué que Windows 10 marquait la fin des grandes mises à jour distribuées sur des supports physiques. Désormais, Windows évolue en continu sous forme de service en packs qui sont distribués gratuitement par Internet [9] .

FIGURE 1.4 – Windows 10

4-Wireshark

Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie [10].

FIGURE 1.5 – Wireshark

5-Putty

PuTTY est un émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin, et TCP brut. Il permet également d'établir des connexions directes par liaison série RS-232 [11].

FIGURE 1.6 – Putty

1.2.3 Les serveurs

1-Serveur DHCP

Le rôle de DHCP est d'allouer les adresses IP aux différentes machines utilisées au sein de l'entreprise , ainsi il permet d'avoir une gestion centralisée des adresses IP et d'éliminer la corvée de la configuration des nouvelles machines [12].

DHCP snooping :est une fonctionnalité qui permet d'améliorer la sécurité d'une infrastructure utilisant un DHCP. Le DHCP snooping permet de :

1. Choisir les ports derrière lesquels peut se trouver un DHCP.
2. S'assurer que les hotes utilisent l'IP qui leur a été associée.
3. Définir un maximum de requêtes DHCP par port.

2-Serveur DNS

DNS est un service dont la principale fonction est de traduire un nom de domaine en adresse IP. Pour simplifier, le serveur DNS agit comme un annuaire que un ordinateur consulte au moment d'accéder à un autre ordinateur via un réseau. Autrement dit, le serveur DNS est le service qui permet d'associer à un site web (ou un ordinateur connecté ou un serveur) une adresse IP, comme un annuaire téléphonique permet d'associer un numéro de téléphone à un nom d'abonné [12].

3-Active Directory(AD)

Active Directory 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 des ressources réseau dont des fichiers, utilisateurs, groupes, périphériques et appareils réseau [13].

4-Serveur de voix IP(Call Manager)

C'est un serveur de téléphone IP utilisé pour l'établissement de la communication au sein de l'entreprise et vers le site distant via le réseau LAN.

5-Serveur mandataire

C'est un serveur qui a pour fonction de relayer les différentes requêtes et d'entretenir un cache des réponses connu en anglais sous le terme de "Proxy server", il a été inventé par le centre européen de recherche nucléaire.Il a été prévu à l'origine pour relier à internet des réseaux locaux n'utilisant pas le protocole TCP/IP, il est depuis doté de plusieurs fonctions concernant [14] :

1. Le cache.
2. La journalisation des requêtes "logging".
3. La sécurité du réseau local.
4. Le filtrage et l'anonymat.

6-Serveur radius

Radius est un processus d'arrière-plan qui s'exécute sur un serveur UNIX ou Windows. Il permet de gérer les profils des utilisateurs dans une base de données centrale .Un serveur RADIUS donne aux utilisateurs l'opportunité de contrôler la connection au réseaux ; C'est-à-dire lorsqu'un utilisateur essaie de se connecter à un client RADIUS, le client envoie des requêtes au serveur RADIUS, l'utilisateur peut se connecter au client RADIUS uniquement si le serveur RADIUS authentifie et autorise l'utilisateur [15].

802.1X : est un standard permettant d'améliorer la sécurité de notre réseau. Le principe est simple, quand l'utilisateur se connecte au réseau, un login/MDP va lui être demandé. Cela peut être valable pour les connexions Wifi(le plus courant) et pour les connexions Ethernet[15].

Le plus souvent, le 802.1X est utilisé sur les réseaux Wifi au lieu d'une clé Wifi, l'utilisateur doit fournir son identifiant.

Il existe 3 roles de 802.1X [15] :

1. **Supplicant :** La machine connectée à un port access, qui a besoin de s'authentifier.
2. **Authenticator :** L'équipement(switch ou borne wifi) qui controle l'accès au réseau.
3. **Network Authentification Server :** Serveur qui sera interrogé pour l'authentification des utilisateurs.

1.3 Partie 2 : Les modèles de référence et la sécurité informatique

1.3.1 Les modèles OSI et TCP/IP

1-Modèle OSI

C'st une norme qui préconise comment les ordinateurs devraient communiquer entre eux. Cela impliquera notamment le respect de la communication par couches. Le modèle OSI est un modèle en couches. Cela veut dire qu'il est découpé en plusieurs morceaux appelés couches chacune un rôle défini, comme le montre le schéma de la figure [17] .

1. **La couche physique** : Son rôle est de fournir le support de transmission de la communication. Elle assure l'établissement et le maintient de la liaison physique. Elle comprend donc les spécifications mécaniques (connecteurs) et les spécifications électriques (niveaux de tension).
2. **La couche Liaison de données** : Son rôle est de connecter des machines sur un réseau local, son objectif est de permettre à des machines connectées ensemble de communiquer, elle possède un autre rôle important qui est la détection des erreurs de transmission.Elle assure le maintient de la connexion logique, le transfert des blocs de données (les trames et les paquets), la détection et la correction des erreurs.
3. **La couche réseau** : Son rôle est d'interconnecter les réseaux. Elle assure l'acheminement, le routage (choix du chemin à parcourir à partir des adresses), des

blocs de données entre les deux systèmes d'extrémités, à travers des relais et elle définit la taille de ses blocs.

4. **La couche transport** : Son rôle est de gérer les connexions applicatives. Elle assure le contrôle du transfert de bout en bout des informations entre les deux systèmes d'extrémités, afin de rendre le transport transparent pour les couches supérieures. Elle assure le découpage des messages en paquets pour le compte de la couche réseau et les reconstitue pour les couches supérieures.

5. **La couche session** : Elle assure l'échange des données, et la transaction entre deux applications distantes. Elle assure aussi la synchronisation et le séquencement de l'échange par la détection et la reprise de celui-ci en cas d'erreur.

6. **La couche présentation** : Elle assure la mise en forme des données, la conversion des codes (ASCII, EBCDIC...), si nécessaire, pour délivrer à la couche application un message dans une syntaxe compréhensible. Elle peut aussi assurer le cryptage et la compression des données. C'est donc la première couche non impliquée dans le mécanisme de transfert d'informations.

7. **La couche application** : Elle ne contient pas les applications utilisateurs, mais elle assure la communication, à l'aide de processus, entre les couches inférieures et les application utilisateurs (transfert de fichiers, courrier électronique).

2-Modèle TCP/IP

Le modèle de protocole TCP/IP pour les communications sur l'internet a été créé au début des années 1970 et il est parfois appelé le modèle internet. Ce type de modèle correspond étroitement à la structure d'une suite de protocoles particuliers. Le modèle TCP/IP est un modèle de protocole, car il décrit les fonctions qui interviennent à chaque couche de protocoles au sein de la suite TCP/IP. TCP/IP est utilisé comme modèle de référence [16].

1. **La couche Accès réseau** : Elle Contrôle les périphériques matériels et les supports qui constituent le réseau.

2. **La couche Internet** : Elle Détermine le meilleur chemin à travers le réseau.

3. **La couche Transport** : Elle Prend en charge la communication entre plusieurs périphériques à travers divers réseaux.

4. **La couche Application** : Elle Représente les données pour l'utilisateur, ainsi que le codage et un contrôle du dialogue.

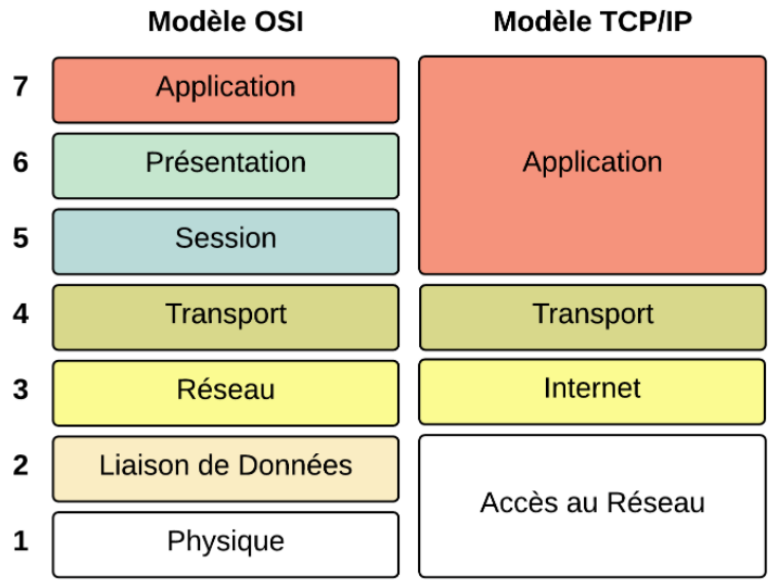

FIGURE 1.7 – Modèle OSI et TCP/IP

1.3.2 La sécurité informatique

La sécurité informatique est l'ensemble des moyens, outils, techniques et méthodes mis en oeuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

1-Objectif de la sécurité

La notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité. Elle s'exprime le plus souvent par les objectifs de sécurité suivants :

- **La disponibilité :** Est le fait qu'une ressource soit disponible afin que les utilisateurs sachent ce qui'ils ont à faire.
- **L'intégrité :** Est le fait que les ressources n'ont pas été détruites ou modifiées à l'insu de leurs propriétaires.
- **La confidentialité :** C'est le fait que les ressources sont maintenues en secret contre une divulgation non autorisée sauf par les personnes autorisées.
- **La non-répudiation :** C'est la priorité qui assure la preuve de l'authenticité d'un acte c'est à dire que l'auteur d'un acte ne peut denier l'avoir effectuer.
- **L'authentification :** Consiste à s'assurer que seules les personnes dûment autorisées aient accès aux données ou aux ressources souhaitées. Le but étant d'identifier de manière unique et sans équivoque qu'un individu est bien celui qu'il prétend être.

2-Attaques informatiques

Tout machine connectée à un réseau informatique est potentiellement vulnérable à une attaque. Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables. Sur Internet, des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée, ces attaques sont pour la plupart lancées automatiquement à partir de machines infectées

(par des virus,chevaux de Troie, vers,etc.),à l'insu de leur propriétaire plus rarement, il s'agit de l'action de pirates informatiques.Afin de contrer ces attaques, il est indispensable de connaitre les principaux types d'attaques afin de mettre en oeuvre des dispositions préventives [17].

1.4 Partie 3 :Sécurité des réseaux

1.4.1 Les réseaux locaux virtuels(VLAN)

Les VLANs sont une technologie implantée sur les Switch actuel. La configuration des VLANs se fait au niveau de commutateur administrateur. Il existe trois types de VLAN [18] :

1. **Niveau1 (VLAN par port)** : Le principe est affecté un port à un VLAN. Manipuler une table de correspondance N° de port/N° de VLAN.
   - **Avantage** :Performant en temps de traitement.
   - **Inconvénient** : Reconfigurer le VLAN en cas de changement des ports des machines.
2. **Niveau2 (VLAN par adresse MAC)** : VLAN en fonction des adresses Mac. Manipuler une table de correspondance adresse MAC/N° de VLAN.
   - **Avantage** :Indépendance de la localisation de la station.
   - **Inconvénient** : déplacement d'un utilisateur entraine une redéfinition dynamique de la topologie d'un VLAN.
     Il faut recenser toutes les adresses MAC des machines.
3. **Niveau3 (VLAN par sous réseau)** : On distingue deux types de VLAN :
   - VLAN par sous réseaux ou les VLAN sont constitué d'adresses ip.
   - VLAN par protocole ou les VLANs sont constitué selon le type de protocole.

1-Avantages des VLANs

- **Sécurité** : Le groupe contenant des donnes sensibles sont séparées du reste du réseau, ce qui diminue les risques de violation de confidentialité.
- **Réduction des coûts** :Des économistes sont réalisées grâce a une diminution des mises a niveau onéreuses du réseau et a l'utilisation plus efficaces de base.
- **Mouilles performances** : Le fait de diviser des réseaux en plusieurs domaines de diffusion, réduit la quantité de trafic inutile sur le réseau et augmente les performances.
- **Réduction de taille des domaines de diffusion** : Le fait de diviser un réseau en Vlan réduit le nombre de périphériques dans le domaine de diffusion.
- **Efficacité accrue du personnel informatique** : Les Vlan facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même Vlan.
- **Gestion simplifié de projet et d'application** : La séparation des fonctions facilite la gestion du projet ou l'utilisation des applications spécialisée.

2-La norme IEEE 802.1Q

La norme IEEE 802.1Q est utilisée pour étendre la portée des VLANs sur plusieurs switch. Elle est basée sur le marquage explicite des trames dans l'en-tete de niveau 2 de

la trame est ajoutée un "tag" qui identifié le VLAN auquel elle est destinée on parle alors de VLAN "taggés". Le format de la trame et donc modifié, ce qui peut entraîner des problèmes de comptabilité avec les switchs ne supportant pas des VLANs et des soucis de taille maximale de trame sur le réseau. Il est noté que seuls les switchs ajoutent et enlèvent les "tags" dans les trames [19].

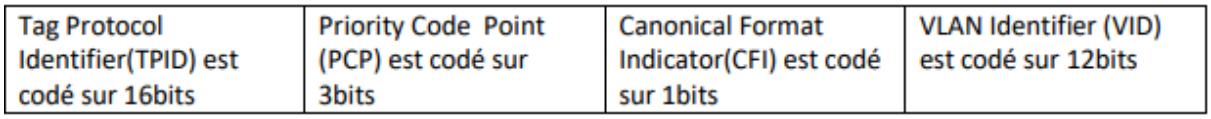

FIGURE 1.8 – Format de la trame IEEE 802.1Q

3-Le protocole VLAN Trunking Protocol(VTP)

A-Définition

VTP est un protocole de messagerie qui utilise les trames d'agrégation de couche 2 pour gérer l'ajout, la suppression et l'attribution de nouveaux noms aux VLAN sur un domaine unique. De plus, VTP autorise les changements centralisés qui sont communiqués à tous les autres commutateurs du réseau. Les messages VTP sont encapsulés dans des trames de protocole Cisco ISL (Inter-Switch Link) ou IEEE 802.1Q, puis transmis sur des liens multi-VLAN aux autres unités. Son rôle est de maintenir la cohérence de la configuration VLAN sur un domaine d'administration réseau commun [19].

B-Les modes de VTP

Chaque commutateur Cisco peut fonctionner dans l'un de ces trois modes VTP [19] :

1. Mode VTP serveur : Les commutateurs Cisco sont des serveurs VTP par défaut. Lorsqu'un commutateur fonctionne comme un serveur VTP, les utilisateurs peuvent supprimer, modifier et créer des VLAN. Il est également possible de définir d'autres paramètres de configuration sur le serveur, tels que l'élagage VTP et la version VTP.
2. Mode VTP client : Lorsqu'un switch fonctionne en mode client VTP, il ne peut pas modifier sa configuration. Les utilisateurs ne peuvent pas supprimer, modifier ou créer des VLAN sur les clients VTP. Il ne peut obtenir les informations que d'un serveur VTP. Un client VTP synchronisera sa base de données VLAN à partir du serveur avec le numéro de révision le plus élevé.
3. Mode VTP transparent : Les commutateurs fonctionnant en mode transparent VTP ne font pas partie du domaine VTP. Les commutateurs transparents VTP n'annoncent ni n'apprennent les informations VLANs, mais ils transmettent les annonces reçues. Les utilisateurs peuvent supprimer, modifier et créer des VLANs sur des commutateurs transparents VTP, mais ils sont plutôt stockés dans sa base de données VLANs locaux.

1.4.2 Les VLANs privés

Le Private VLANs a été inventé afin d'isoler les hôtes au niveau 2. Ils permettent d'avoir un VLAN (et donc un sous réseau), dans lequel les utilisateurs ne peuvent pas discuter. PVLAN se compose d'une association de VLAN :

1. Un VLAN Primary
2. Un ou plusieurs VLAN Secondary qui peuvent être de deux types :
   — **Isolated** : Les membres de ce VLAN ne peuvent pas communiquer entre eux.
   — **Community** : Les membres de ce VLAN peuvent communiquer entre eux.

Enfin, le port d'un switch peut fonctionner dans l'un des deux modes suivants :

— **Host** : Le port à un comportement qui découle du type de PVLAN auquel il est associé (Isolated ou Community).
— **Promiscuous** : Le port peut communiquer avec les ports membres du même VLAN.

1.4.3 Les VLANs ACL

Les VACL ou Vlan ACL sont des Access List à appliquer sur des VLAN. Elles se configurent sur un switch.

A la différence des ACL classiques qui s'appliquent sur un routeur, et qui ne peuvent que filtrer qu'entre les VLAN, les VACL permettent de filtrer le trafic au sein d'un même VLAN.

De manière générale, une VACL fonctionne sur un principe similaire à celui des route-maps. Il s'agit d'une liste ordonnée de règles, chacune ayant un numéro de séquence. Pour chacune de ces règles nous devons identifier le trafic correspondant à laide d'une clause « match », à laquelle nous ferons correspondre une « action » qui peut être l'une des trois suivantes [20] :

— **forward** : Le trafic est traité normalement en suivant la logique de commutation du switch.
— **drop** : Le trafic est rejeté.
— **redirect** : Le trafic est redirigé vers une interface spécifique, indépendamment de la logique de commutation du switch.

Les clauses « match » utilisent des ACL (soit IP, soit MAC). C'est donc par là que nous devrons commencer.Chose importante A l'instar d'une ACL classique, les VACL rejettent tout ce qui n'est pas permis. Une VACL sans règle « forward » bloquera tout simplement tout le trafic dans le vlan donné.Il existe 3 étapes pour créer les ACLs qui sont [20] :

— **Etape n°1** : Créer une ACL (classique) pour identifier le trafic à traiter.
— **Etape n°2** : Créer la VACL pour associer des « match » à des « action ».
— **Etape n°3** :Appliquer la VACL au(x) VLAN(s) désiré.

1.4.4 Les ports de sécurité

Il est important de sécuriser le niveau 2 dans un réseau, car il s'agit de la porte d'entrée de ce dernier.

De nombreuses menaces existent sur ces ports de sécurité qui sert à :

1. Limiter le nombre d'adresse MAC dernière un port.
2. Se protéger du MAC Address Flooding.
3. Restreindre l'accès à certaines adresses MAC.
4. Désactiver le port / envoyer des logs en cas de violation.

Il y a trois options de gestion des adresses MAC :

— **Dynamique** : En ce mode, le switch apprend automatiquement les adresses. Il se base sur les trames reçues. Les Mac autorisées seront donc les premières apprises. Par contre, les adresses Mac ne sont pas conservées dans la configuration.

— **Static** : En ce mode, nous définissons nous même les adresses Mac autorisées. L'avantage est que les adresses définies sont stockées dans la configuration. Elles sont donc conservées en permanence.

— **Sticky** : Ce mode permet au mode Dynamic d'enregistrer les adresses. On les retrouve alors dans la configuration comme si elles avaient été configurées en Static.

On appel violation de port, quand les règles de sécurité ne sont pas respectées. Il existe 3 options pour la violation de port :

— **Shutdown** : En ce mode , le port est désactivé s'il y a violation. Il passe en Err-Disabled. Une Trap SNMP est envoyée, un message Syslog est logué et le compteur de violation augmente.

— **Protect** :En ce mode , les adresses MAC en trop sont ignorées. Les messages avec une adresse Mac source non connue sont ignorés.

— **Restrict** : Le mode fait la même chose que le mode Protect, En plus, une Trame SNMP est envoyée, un message Syslog est logué et le compteur de violation augmente.

1.4.5 Les réseaux privés virtuels(VPN)

Les VPN sont des connexions privées, ou des tunnels, sur des réseaux publics comme internet.Ils sont déployés afin de connecter des télétravailleurs, des employés mobiles, des succursales et des partenaires commerciaux entre eux et aux réseaux d'entreprise.Tous les dispositifs matériels et logiciels de VPN prennent en charge la technologie de cryptage afin de fournir la meilleur protection possible des données tronsportées [21].

Il existe plusieurs protocoles dits de tunnelisation qui permettent la création des réseaux VPN .

1. **Protocole IPSec :**Nous avons choisi IPSec comme protocole de tunnelisation qui est plus performant coté sécurité par apport au protocole MPLS, vu que IPSec est un protocole de sécurité totale grâce à la combinaison de certificat numérique et de PKI pour l'authentification ainsi qu'a une série d'options de cryptage, triple DES AES notamment. Il est basé sur deux mécanismes de sécurité AH(Authentification Header) et ESP(Encapsulating Security Payload)[21].

2. **Protocole HSRP(Hot Standby Routing Protocol) :** Est un protocole propriétaire de "continuité de service" implémenté dans les routers Cisco pour la gestion des "liens de secours".

   HSRP sert à augmenter la tolérance de pannes sur le réseau en créant un routeur virtuel à partir de 2(ou plus) routeurs physique "en actif" et l'autre "en attente" (ou "standby")en fonction des priorités accordées à chacun de ces routeurs .

3. **Protocole SSH :**Il est préférable d'utiliser le protocole SSH pour l'accès à distance aux équipements réseau qui chiffre les informations afin d'apporter une couche de sécurité à la connexions à distance. De ce fait, c'est primordial de mettre en place un accès SSH sur un switch Cisco ou sur un routeur Cisco plutôt qu'un accès Telnet qui transfère les données en clair sur le réseau.

   Network Address Translating(NAT) :

Le NAT permet à une organisation de n'utiliser qu'une adresse IP publique,celle de l'interface externe de la passerelle de son réseau, et de numéroter sans réstriction les machines internes de son réseau avec des adresses valables localement. Lorsque des paquets sont échangés avec l'extérieur, une passerelle se charge de traduire les adresses dans les deux sens .

1.4.6 Spanning Tree

Spanning Tree est l'un des principaux protocoles que l'on retrouve au niveau 2. Il permet d'éviter les boucles dans un réseau, mais aussi de profiter des topologies redondantes, sans risque de créer des boucles.Son rôle de désactiver les liens qui peuvent créer une boucle. Il se chargera de les réactiver si nécessaire (en cas de panne d'un autre lien).

Afin de détecter les boucles, les switchs émettent des messages appelés BPDU – Bridge Protocol Data Units.Il existe 3 types de BPDU [20] :

1. BPDU de configuration, utilisé pour le calcul de Spanning Tree.
2. BPDU de notification de changement (TCN – Topology Change Notification BPDU), utilisé quand la topologie change.
3. BPDU d'acquittement de changement.

Les BPDU vont permettre de découvrir la topologie et d'élire le Root Bridge. Ce dernier est en quelque sorte le chef de la topologie Spanning Tree. Une fois le Root Bridge élu, les switchs vont rechercher le meilleur chemin vers le Root Bridge.

1-Portfast Spanning Tree

Portfast est une fonctionnalité à activer sur les ports faisant face à des PC, Serveur, etc. Cela va tout simplement désactiver Spanning Tree sur le port en question. Le résultat est simple [20] :

1. Plus de BPDU envoyé
2. Plus d'état Spanning Tree –> activation du port immédiate

Cette fonctionnalité est indispensable sur les ports qui font face à des PC. Sinon, les ports mettront 30s à répondre lorsque l'on y connectera un PC. Cela donnera l'impression que le port ne fonctionne pas.Portfast ne fonctionne pas sur les liens Trunk, ce qui est logique. En effet Portfast ne doit pas être utilisé entre des switchs.

2-Rapid Spanning Tree

Rapid Spanning Tree est un protocole standard qui est apparu suite à une version propriétaire Cisco.

Pour faire simple, RSTP est beaucoup plus rapide que le Spanning Tree classique. Les Timers ont été réduits ou supprimés.Des BPDU sont envoyés tous les HELLO-Time (2s par défaut).

1.4.7 EtherChannel

Etherchannel est une technique permettant l'agrégation de lien. Il est souvent utilisé pour augmenter la bande passante entre deux switchs. Il s'agit de combiner plusieurs liens

pour obtenir un lien virtuel de meilleure capacité. peut regrouper jusqu'à 8 liens.

Il existe deux manières de créer une agrégation de lien soit en forçant l'agrégation ou on utilisant un protocole de négociation. Pour la négociation de l'agrégation, il existe deux protocoles [20] :

1-PAGP – Port Agregation Protocol

PAGP est le protocole de négociation propriétaire Cisco. En choisissant ce protocole, il est possible de configurer les ports dans 2 modes différents :

- **Auto** : Avec PAGP, si le port est en mode Auto, une agrégation de lien sera créée si le port d'en face est en mode Desirable. Si le port d'en face est en mode Auto, aucune agrégation n'est créée.
- **Desirable** : Si le port est configuré en mode Desirable, une agrégation sera créée à condition que le port d'en face soit en mode Auto ou Desirable.

2-LACP – Link Agregation Control Protocol

LACP est un protocole standard (802.3AD) très similaire à PAGP. La seule différence est le nom des modes de port. Nous retrouvons donc deux modes de ports :

- **Passive** : Correspond au mode Auto de PAGP C'est la création d'une agrégation si le port en face est en Active.
- **Active** : Correspond au mode Desirable de PAGP C'est la création d'une agrégation si le port d'en face est en Passive ou Active.

1.4.8 Zone démilitarisée (DMZ)

La DMZ a pour fonction principale de permettre aux ordinateurs ou aux hôtes de fournir des services au réseau externe et de fonctionner comme un filtre de protection pour le réseau interne, agissant comme un « pare-feu » et le protégeant des intrusions malveillantes qui pourraient compromettre la sécurité.

1.5 Conclusion

Ce chapitre, nous a permis en premier lieu de bien comprendre les notions de base des réseaux informatiques . En deuxième lieu, nous avons présenté les modèles de référence et la sécurité informatique. Pour bien terminer le chapitre, on a parlé de la sécurité des réseaux notamment les VLAN, VTP, VPN et le DMZ.

Chapitre 2

Présentation de l'organisme d'accueil, problématique et solution proposée

2.1 Introduction

Dans ce chapitre, une étude sera faite sur le réseau existant qui consiste à identifier et collecter des informations, pour une meilleure compréhension de l'environnement du réseau informatique d'Amimer Énergie, qui va nous permettre de déterminer la portée du projet et la solution à implémenter pour une nouvelle architecture sécurisée.

Dans ce chapitre ,nous avons trois parties ; dans la première partie nous allons décrire l'entreprise Amimer Energie pour qu'on passe à l'état des lieux dans la deuxième partie dont on présente l'infrastructure du réseau actuel et les problèmes qu'on a déduit durant notre stage et on terminera dans la troième partie par la proposition des solutions à ces problèmes.

2.2 partie1 : Présentation de l'entreprise Amimer Energie

C'est en 1989 et dans la localité de SEDDOUK, située dans la vallée de la Soummam (wilaya de Bejaïa), que commence le somptueux périple de la société Amimer Energie, autrefois fondée par son propriétaire et visionnaire Mr Amar Boukheddami sous la dénomination "Etablissement Boukheddami" et versée dans la fabrication des postes à souder.

La société a vite cerné le rôle qu'elle devrait jouer et les enjeux d'un secteur très sensible et stratégique pour le pays, l'Energie. Cette dérnière indispensable à l'épanouissement d'un peuple, au développement d'un pays allait être le centre d'intérêt premier de la société. La société élargit ses activités et se développe autours des métiers de la fabrication et de l'installation de Groupes électrogènes de moyenne intensité, avec une nouvelle dénomination, elle devient la société Amimer Énergie.

Grâce à la vision et la persévérance de son fondateur, l'entreprise qui n'était au départ qu'une simple PME, commence à prendre de l'ampleur et à devenir un acteur majeur dans les équipements et solutions énergétiques en Algérie et dans la région de l'Afrique du nord et de l'Afrique subsaharienne.

Aujourd'hui, la qualité, la rigueur, le sérieux de leur travail sont leur meilleurs atouts. Le professionnalisme a permis à leur Groupe de devenir un acteur incontournable de la scène économique algérienne et de figurer parmi les fleurons des entreprises algériennes dans le secteur de l'énergie.

Le professionnalisme, leur savoir faire transcende les frontières et se place aujourd'hui parmi les pionniers de la région dans les solutions énergétiques les plus innovantes.

L' entreprise doit cette irrésistible et formidable ascension à toutes les femmes et à tous les hommes qui, dès le début, ont cru en elle et en leurs capacités d'aller toujours de l'avant. Ce noyau qui n'hésitera jamais de se surpasser pour apporter à leur client le service optimale et irréprochable au standards internationaux, de s'affranchir des sites et régions éloignées, isolées pour apporter ce brin d'espoir, cette lumière tant attendue à des populations démunies. Leur passion est d'apporter une source d'énergie, et d'innover même s' il faut l'apporter du vide.

L'etreprise offre à ses clients une variété de solutions optimales étudiées à leurs besoins, allant de la simple fabrication de groupes électrogènes diesel ou gaz, à l'engineering et la réalisation de centrales électriques complexes et de grande capacité, fonctionnant par différentes sources d'énergies. Cette société demeure à la quête des meilleures solu-

tions économiques pour ses clients, n'hésitant pas à innover en apportant des solutions de génération d'énergie à base de solaires, gaz, éolien et en hybridation de ces différentes sources. ;

2.2.1 Historique

Les Ets Boukheddami one été créés en juillet 1990 puis transformés en 1993 en Sarl Amimer Energie avec un capital social de 40.000.000 DA et en SPA (société par action) en 2009 avec un capital social de 1 000 456 500,00 DA.

Le siège social et l'usine se situent à Seddouk dans la Wilaya de Bejaia en Algérie, entre la rive droite de l'oued Soummam et le mont Achtoug , l'usine s'étent sur une superficie de 7.672 m2 dont 4816 m2 construits en dur et 2.856 m2 nue.

2.2.2 Organigramme de l'organisation globale de l'entreprise Ammimer Energie

L'entreprise est organisée selon l'organigramme suivant :

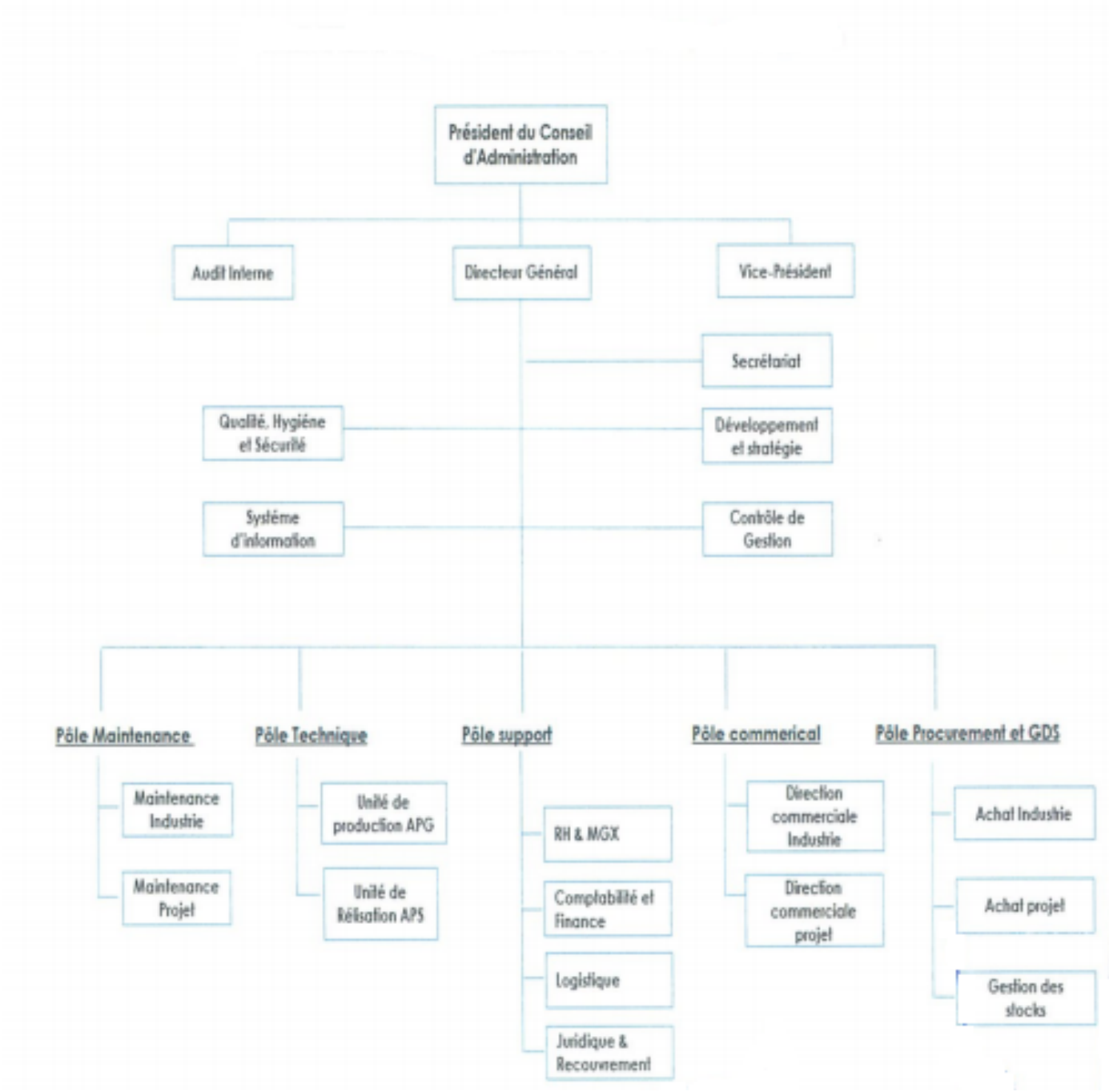

FIGURE 2.1 – L'organigramme de l'entreprise Amimer Energie.

2.2.3 Missions d'Amimer Energie SPA1

Ses activités sont centrées sur la conception, fabrication, la vente, installation, service après vente des groupes électrogènes et centrales électriques.

Sa première activité fut la fabrication des postes à souder et des chargeurs de batterie. Amimer Energie a ainsi migré naturellement vers la moto soudeuse puis le groupe

électrogène pour devenir le premier producteur Algérien de groupes électrogènes de puissance à usage professionnel et industriel(de 2 ,5 KVa1 à 5000KVa) en fabriquant de micro et mini-centrales de production d'électricité .

Amimer Energie a su au cours des années mettre son expérience à la disposition d'un arsenal de clients aussi variés que connaisseurs et ceci grâce a sa recherche conditionnelle de l'efficience qui se traduit par sa certification à la norme ISO 9001 v.20082 , et le renouvellement de la certification des paramètres de qualité.La qualité est le mot d'ordre de notre organisation, fournir un produit de Qualité confirmée, répondre en Volume à la demande exprimée, respecter et alléger le circuit Administratif et les Interactions qui la lient avec ses clients, livré en Lieu et Temps voulus à un moindre cout Economique.

2.2.4 Services de l'entreprise

1-Le service d'Engineering

Il est composé d'une équipe de spécialistes multidisciplinaire dont la mission et l'étude et l'analyse de besoin du client pour une solution optimale propre à son projet. Son équipe n'hésite pas à se déplacer sur le terrain pour une prise de connaissance poussée de l'état de projet afin de parer à toutes difficultés pouvant naitre antérieurement.

L' équipe est composée d'ingénieurs mécaniques, électriques, instrumentation et contrôle commande, Génie civil, énergie renouvelable et énergéticiens. Elle offre des études en et en électriques et son offre élargie à d'autres domaines de l'engineering.

2-Etude technico commerciale

Leurs offre ne se limite pas à une simple fourniture standard. Ils disposent d'une équipe capable de déceler les besoins des clients et de les dimensionner correctement afin d'apporter la meilleure solution. Pour leur solutions énergétiques,ils élaborent des bilans énergétiques .

Réparation et maintenance

Un réseau d'expert assure le service après vente de nos produits sur tout le territoire national, ils utilisent dans leur interventions un outillage spécifique dédié, une équipe d'expert et des pièces de rechange d'origine. Ils sont dédié toute une filiale pour être proche de leurs besoins et les prendre en charge efficacement et dans les meilleurs délais.

Leur service après vente intervient sur tout les produits qu'ils commercialisent ; groupes électrogènes, centrales électriques, motopompes, motosoudeuses, armoires électriques.

4-Transport et manutention

Une équipe ayant déjà réalisé de beaux challenges dans le transport conventionnel, exceptionnel et en opérations de manutention complexes sur le territoire national et principalement dans des zones difficilement accessibles à travers tout le territoire national à l'instar du sud algérien. Leurs équipes bravent avec brillance et professionnalisme les complexités et les dangers de ce métier.

Leurs équipes ont pour mission d'assister et accompagner le client hors du simple service de transport lui-même, ce qui permet d'apporter la solution la plus optimale au besoin du client ainsi qu'une assurance tout le long de la réalisation de leur opérations.

5-Service Location

Grace à cette solution, ils apportent aux clients l'énergie nécessaire à leurs projets ponctuels, urgents, ils lui permettent de ne pas mobiliser ses ressources sur une solution de production d'Energie. Ils proposent des locations de groupes électrogènes individuels ou des groupes connectés et synchronisés.

leurs solutions sont modulaires et permettent de répondre aux besoins du client en agençant des modules de puissance isolés La conception de leur produits permet une installation rapide sans risque ainsi qu'un redéploiement facile.

Leurs solutions sont capotées ou conteneurisés, sécurisées pour un accès contrôlé leurs équipes effectueront pour le client la maintenance, l'entretien et le suivi du produit. Ils garantissent une source d'énergie disponible en toutes circonstances.

6-Formations

Conscient que le bon fonctionnent de produit, sa maintenance régulière et la lecture rapide des principales anomalies est un gage de sécurité et de durabilité, leurs équipes ont mis en place des programmes de formation adéquat pour une meilleure prise en main de nos produits et une utilisation optimale.

Leurs équipes interviennent sur vos sites ou sur les sites d'Amimer afin d'inculquer différentes types de formations dans divers domaines, mécaniques, électriques, contrôle commande, maintenance.

2.2.5 Effectifs du service

L'effectif du service informatique au sein d'Amimer Energie APG est comme suit :
— Un administrateur de système d'information.
— Un informaticien en administration et sécurité des réseaux.

2.2.6 Localisation de l'entreprise

L'entreprise Amimer Energie se situe à Seddouk,

FIGURE 2.2 – localisation de l'entreprise via Google maps

2.3 partie 2 :Etat des lieux

2.3.1 Présentation du réseau Amimer Energie

L'entreprise posséde trois sites au sein du territoire Algérien (site Seddouk,alger et Blida)et pour garantir une communication entre ses sites ,elle doit relier ses différents LANs pour cela l'entreprise a opté pour une connexion ADSL fournie par un fournisseur d'accès internet.La figure ci-dessous nous montre l'infrastructure réseau d'APG Seddouk.

2.3.2 Présentation de l'infrastructure réseau de l'entreprise

Amimer a mis en place son réseau en choisissant une topologis en bus pour relié ses differents équipements comme le montre la figure suivante :

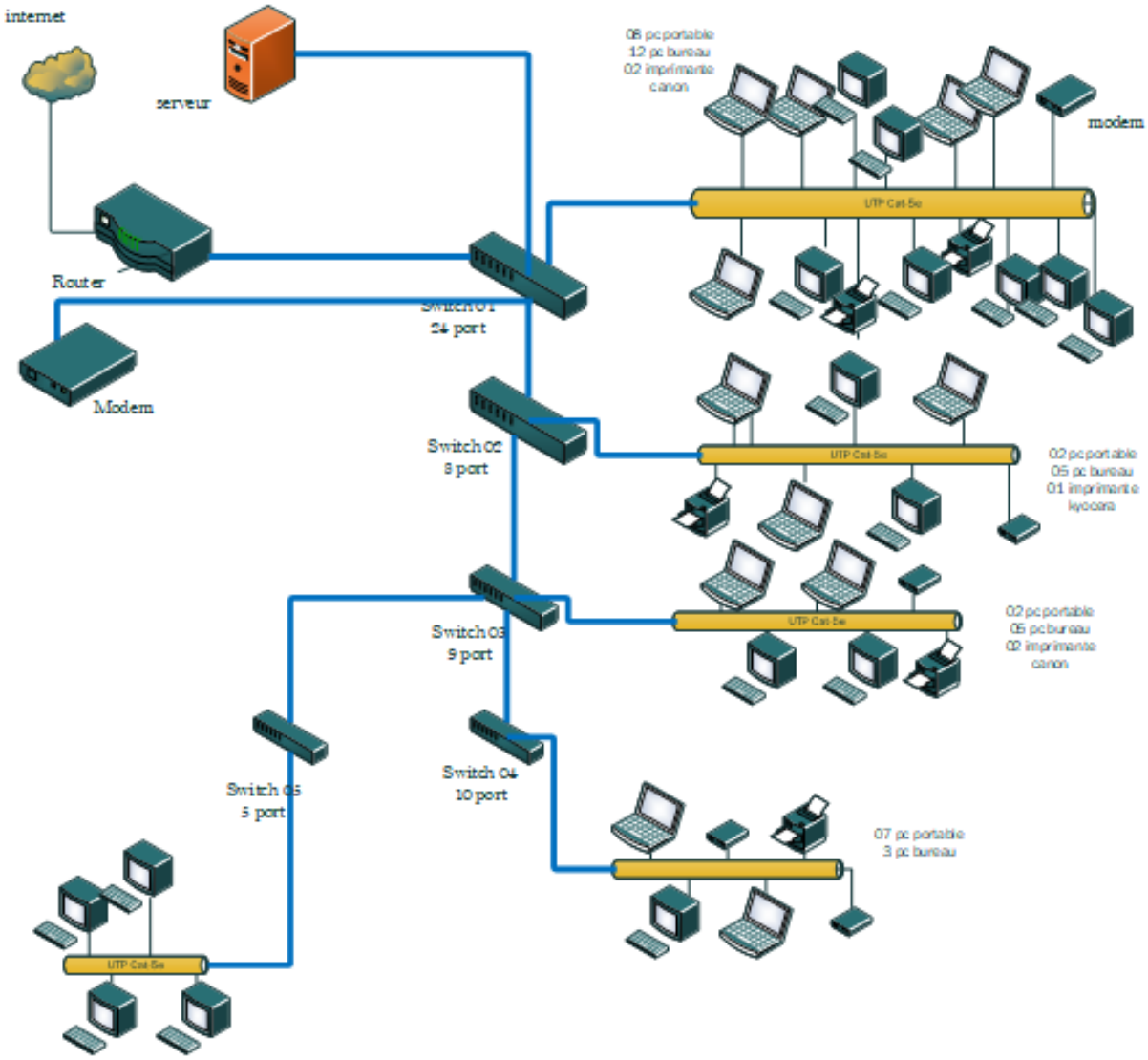

FIGURE 2.3 – L'infrastructure réseau de l'entreprise

2.3.3 Analyse du parc informatique

Armoire de brassage(DATA center)

La DATA CENTER : c'est une salle qui se situe au niveau de service information technology, avec un accès réservé pour les administrateurs réseau et les agents de maintenance. Il contient la majorité du matériel nécessaire pour le bon fonctionnement du réseau LAN de l'entreprise .Dans notre cas elle posséde cinq armoires :

1. **Armoire1** :
   - Server physique
   - Router
   - Switch
   - Convertisseur
   - Serveur de partage de données QWS
2. **Armoire 2,3,4 et 5** :
   - Switch Dlink
   - Point d'accès wifi

Nom de l'équipement	Modèle	Caractéristique
Router 	Cisco 1900 Series	RAM : 2GO Mémoire Flash : 4GO Debit :25 Mbps
Switch 	D-Link	Mémoire Flash :128MO Mémoire cache de paquet :3MO Capacité de commutation :104Gbit/S
Pare-feu 	SOPHOS XG	Débit :4000Mbit/S Débit IPS : 2700Mbit/S Débit VPN IPsec : 560 Mbit/S http://172.16.16.16/4444
Server 	HP Proliant DL380P	Processeur Intel Xeon Silver 4110 (Octo-Core 2.1 GHz / 3.0 GHz Turbo - 16 Threads - Cache 11 Mo) 16 Go DDR4 RDIMM (1x 16 Go - 12 slots)
Modem 	TP-LINK Wireless-G	Débit : 2MO/S
Pc Portable 	HP 350	AMD core :i5 RAM :8GO Disque :1000GO Ecran :15 pouces
Imprimante 	HP OfficeJet 7510 series(réseau)	Vitesse d'impression :33ppm RAM,precesseur :NC

FIGURE 2.4 – Détails des Ressources disponibles de l'entreprise

2.3.4 Les différents serveurs et applications du réseau de l'entreprise

Le service informatique de l'entreprise est doté des serveurs suivant :

— Machine virtuel AD
— Antivirus
— Serveur d'impression
— ERP

Pour une bonne gestion, l'entreprise Amimer utilise différentes applications.
— Solide works :autocod
— Microsoft NAV dynamique (gestion+comptabilité)
— SysNet (DRH)

2.4 partie 3 :Problématique et solutions proposées

2.4.1 Problématique

Durant notre période de stage au sein de l'entreprise Amimer Energie de Seddouk, nous avons constaté qu'elle dispose d'un réseau local composé d'une plateforme de divers services différents , nous avons pu mettre le point sur :

- le manquement du réseau a savoir l'architecture du réseau de l'entreprise est en bus, et cela pose énormément de problèmes dont la vulnérabilité de réseaux étant donné que si l'une des connexions est défectueuse, l'ensemble de réseau en est affecté... De plus,la majorité des ports des commutateurs sont sur le VLAN natif, ce qui augmente les domaines de diffusion et les risques de compromettre la sécurité.Ceci est en contradictions avec le but de l'utilisation des VLANs qui est de micro segmenter le réseau en petits domaines de diffusion.
- Absence de contrôle d'accès à certains sites internet gourmand en termes de bande passante qui ralentissent les employés dans leur travail (Youtub, Facebook...etc).
- l'entreprise s'étend sur des sites distants et plusieurs centre de distributions par conséquent, elle détient un grand nombre de réseau et le besoin d'interconnexion permanente fiable et privé de ces différents sites.
- Le risque des attaques depuis l'extérieur contre le réseau interne de l'entreprise .
- L'entreprise traite de grandes quantités informations aussi nombreuses que variées c'est est ainsi que l'entreprise amimer éprouve le besoin d'une grande bande passante pour communiquer et partager ses bases de données critiques en son sein, c'est pour cela que les responsables des systèmes d'information focalisent leurs esprits sur la grande question d'optimisation de la bande passante.
- La construction d'un réseau résilient à haute disponibilité (redondance, technologie, personnel, les processus et les outils) est extrêmement importante car la majorité des sociétés dépendent du réseau pour leurs activités commerciales.La haute disponibilité doit faire en sorte qu'il existe toujours un chemin possible entre deux extrémités.

2.4.2 Mise en place de la solution

L'enjeu principal d'une architecture réseau sécurisée est de pouvoir réglementer les accès aux ressources du réseau tant à partir du réseau local qu'à l'extérieur , tout en essayant au maximum de limiter les failles d'éventuelles attaques ou vols d'informations afin d'accroître la sécurité du réseau local.Pour cela nous proposons plusieurs solutions au problèmes qu'on a déjà citer :

- Les VLANs pour réduire les domaine de diffusion et augmenter la sécurité du réseau.
- VLANs privé pour économiser des adresses IP et d'améliorer la sécurité des ports de commutation dans la couche 2.
- VLANs ACL qui permettent de filtrer du trafic qui passe d'un réseau à un autre.
- Mettre en place une solution Pare'feu en utilisant ses fonctionnalités configuration, répartition des utilisateurs en groupe selon le besoin d'accès au réseau internet et filtrage.
- Port de sécurité pour filtrer et de restreindre le nombre d'adresse MAC autorisées

à se connecter sur le port d'un switch Cisco.
— Mettre en place d'une liaison VPN entre les deux sites Seddouk et Alger.
— Mettre une zone démilitarisée (DMZ) qui va aider l'entreprises à détecter et corriger les failles de sécurité avant qu'elles atteignent le réseau interne, où sont stockées les ressources les plus précieuses.
— Intégrer le protocole Spanning Tree(STP) qui fournit une redondance à tous les périphériques du réseau c'est à dire dans le cas où le chemin actif rencontre une erreur , une autre voie sera ouverte.
— Mettre en place une technologie Etherchannel dans le but d'augmenter la vitesse et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs.
— mise en place d'une zone démilitarisée permet désactiver les services qui ne sont pas utilisés pour empêcher d'autres personnes d'accéder à l'information qui contiennent les équipements interconnectés au réseau.
— Intégrer l'agrégation de liens pour optimiser la bande passante.
— Mettre en place des protocoles de redondances de premier saut ce qui accroît la complexité de la structure du réseau.Quand des liaisons amont sont défaillantes, les chemins et le temps de convergence doivent être pris en compte pour évaluer l'impact d'une défaillance dans l'infrastructure réseau.

2.5 La nouvelle architecture proposée

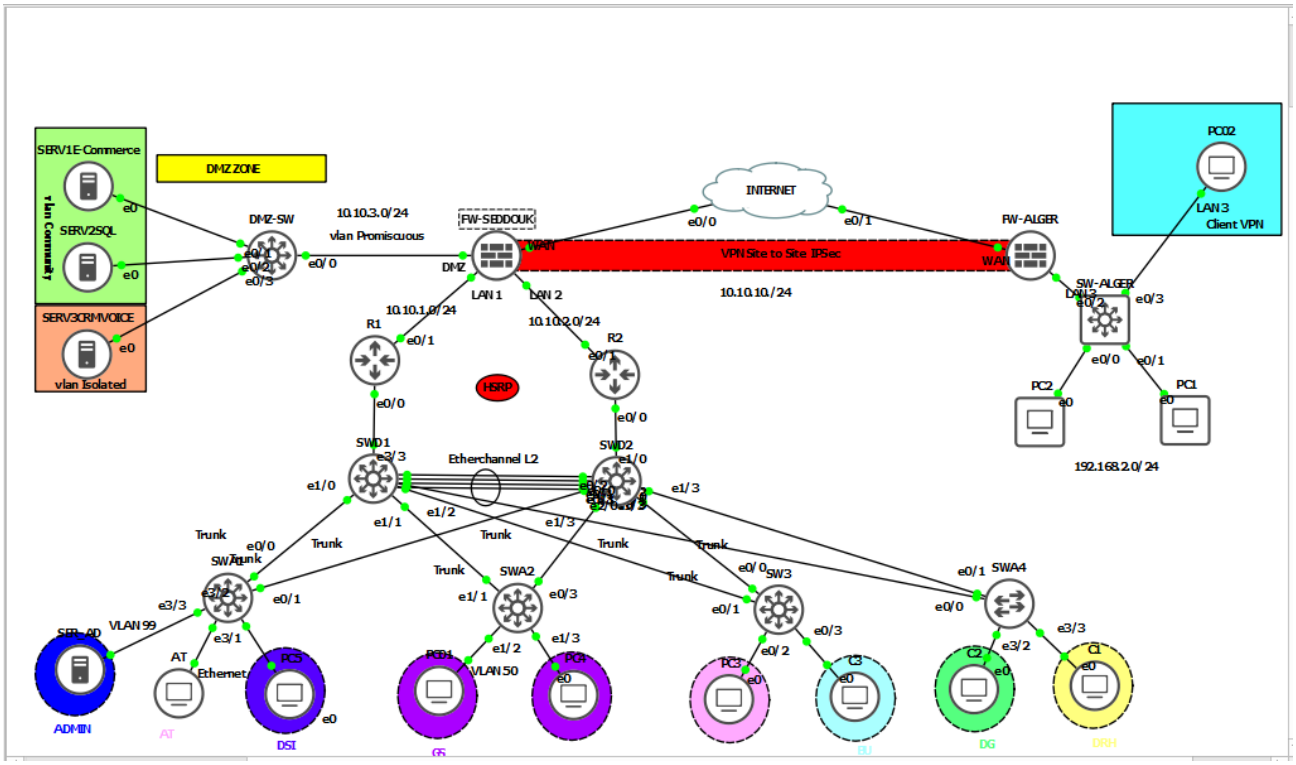

FIGURE 2.5 – Nouvelle architecture réseau de l'entreprise Amimer Energie

2.6 Conclusion

Dans ce chapitre, nous avons donné un aperçu général sur l'entreprise Amimer Energie , par la suite nous avons dégagé une problématique qui nous a conduit à la proposition d'une solution qui consiste la mise en place d'une nouvelle architecture réseau sécurisée en utilisant les VLANs. L'implémentation de la solution proposée sera développée dans le chapitre qui suit...

Chapitre 3

Réalisation

3.1 Introduction

Après avoir décrit les solutions dans le chapitre précédent nous passerons à l'implémentation.

3.2 Environnement de travail

3.2.1 Installation de GNS3 sous windows

Pour installer GNS3, il faut tout d'abord télécharger le fichier exécutable, ensuite le lancer et suivre les étapes d'installation jusqu'à la fin puis cliquer sur le bouton «Finish». La figure suivante représente l'interface de GNS3.

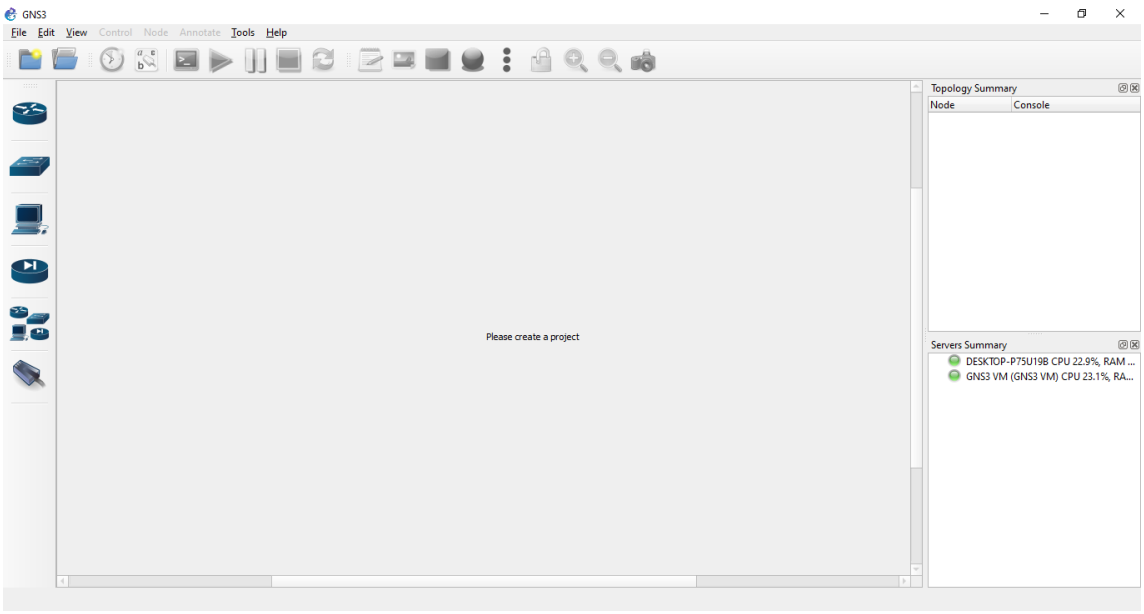

FIGURE 3.1 – Interface d'accueil GNS3

3.2.2 Installation de VMware Workstation version 16.1.2

Afin de créer les machines utilisateurs virtuelles au sein du meme pc, nous sommes appelés à installer VMware Workstation en suivant les étapes ci-dessous

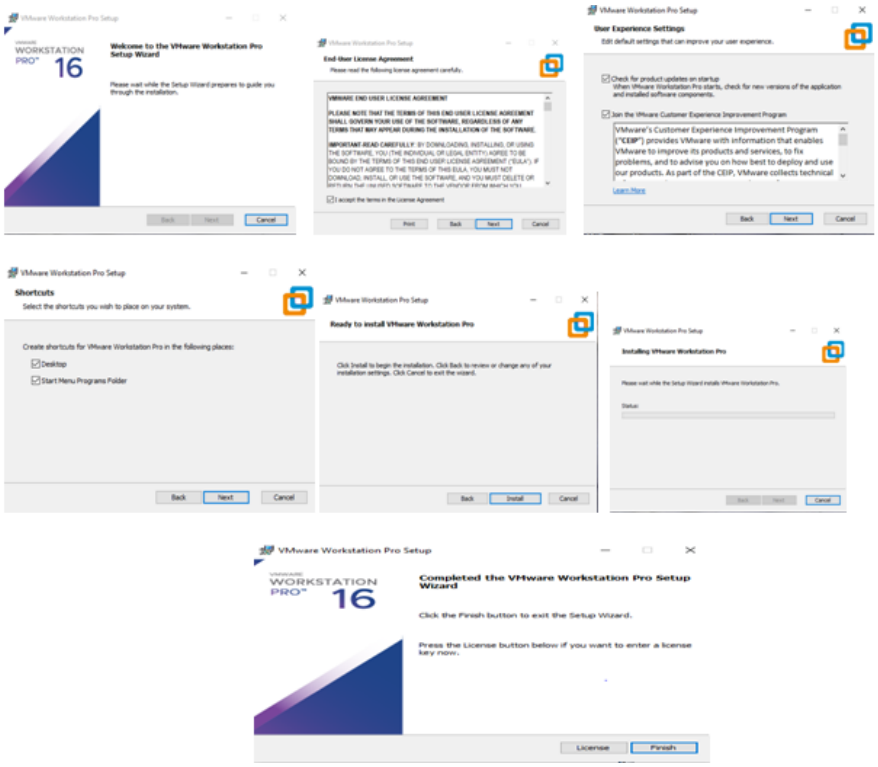

FIGURE 3.2 – Installation de VMware workstation

Après l'installation de VMware une page d'accueil apparaitera .

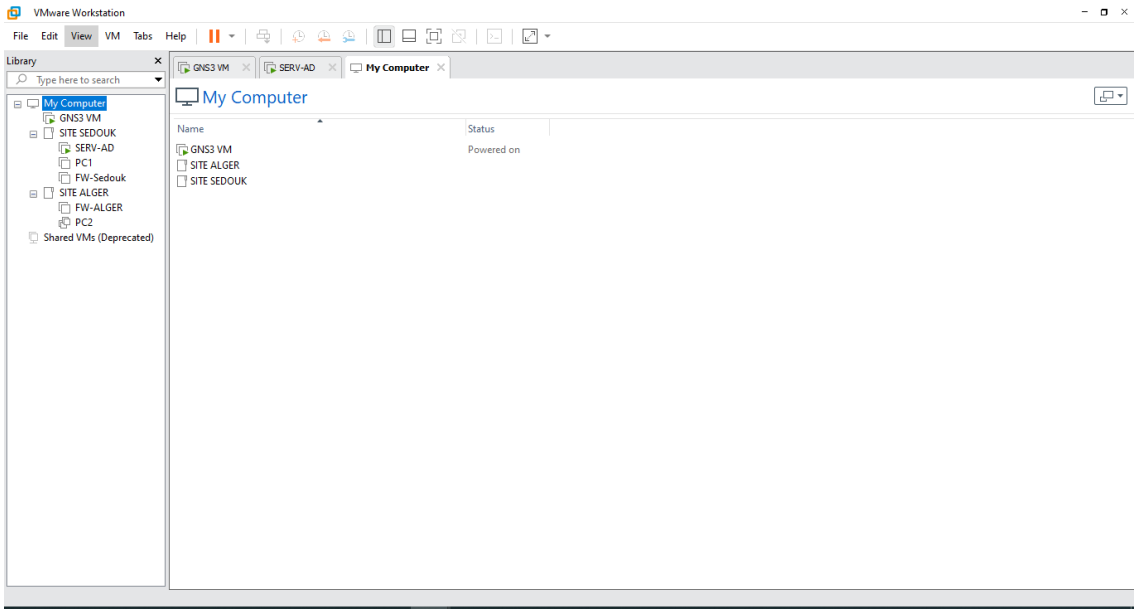

FIGURE 3.3 – Page d'accueil de VMware Workstation 16.1.2

3.2.3 Création des machines virtuelles

Installation du Windows 10 sous VMwar Workstation

Nous avons créé une machine après avoir ajouter l'image de Windows 10 sur VMware. A qui on a attribué les caractéristiques suivantes :

— **A**llocation de la mémoire pour la machine fixé à 2GB

— **D**eux processeurs
— **D**isque dur 30GB

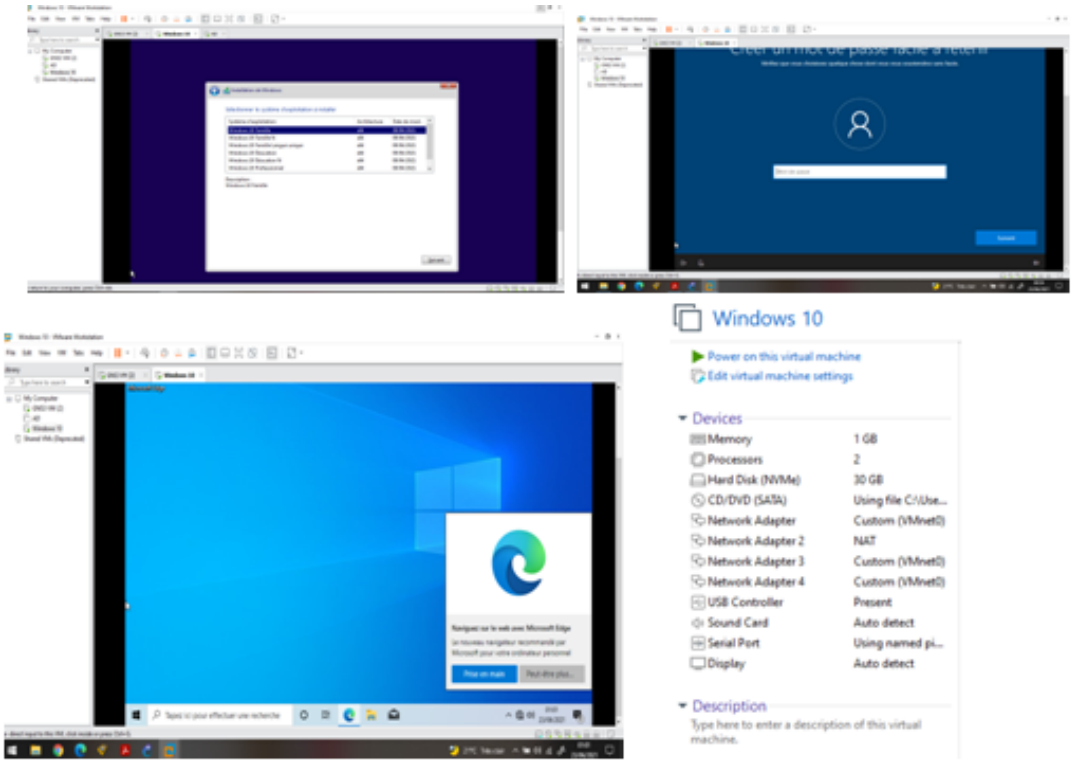

FIGURE 3.4 – Installation de la machine virtuelle Windows 10

3.3 Installation des serveurs

3.3.1 Installation du Windows Server 2016

Dans cette partie nous allons voir les différentes étapes d'installations de Windows Server 2016.

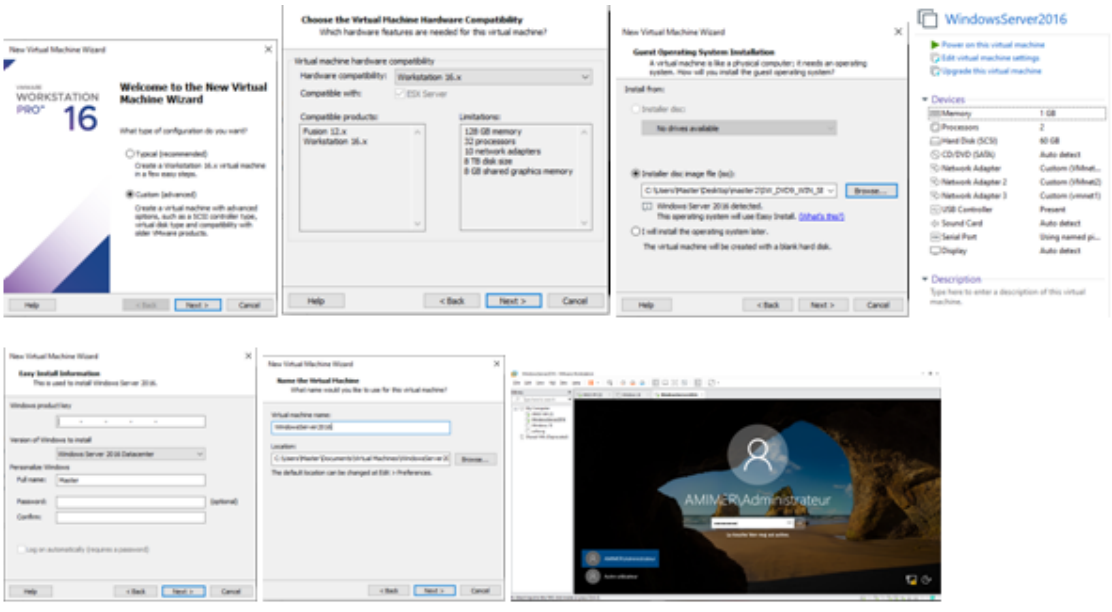

FIGURE 3.5 – Installation de la machine virtuelle Windows Server 2016

L'interface de Windows Serveur 2016 se présente comme ceci :

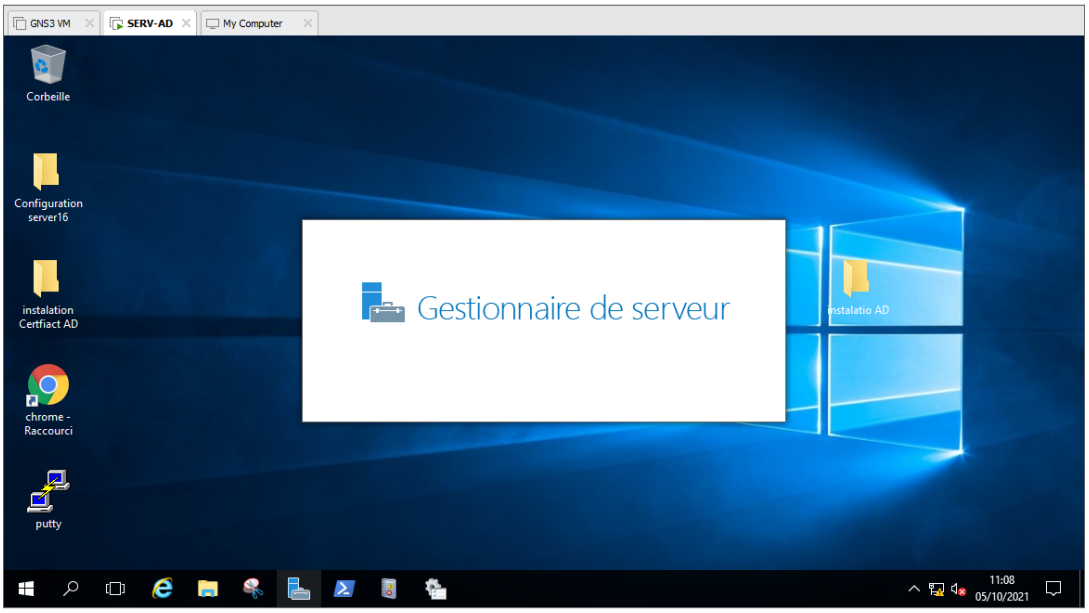

FIGURE 3.6 – Interface de la machine virtuelle Windows Server 2016

3.3.2 Installation de l'Active Directory (AD)

Sur la machine Windows serveur 2016 nous avons installé un controlleur de domaine dont le nom de domaine est amimerenergie.local .

Pour commencer l'installation, il va falloir ajouter le Service de Role Active Directory. Lancer l'installation et ajouter les fonctionnalités qui nous manquent.

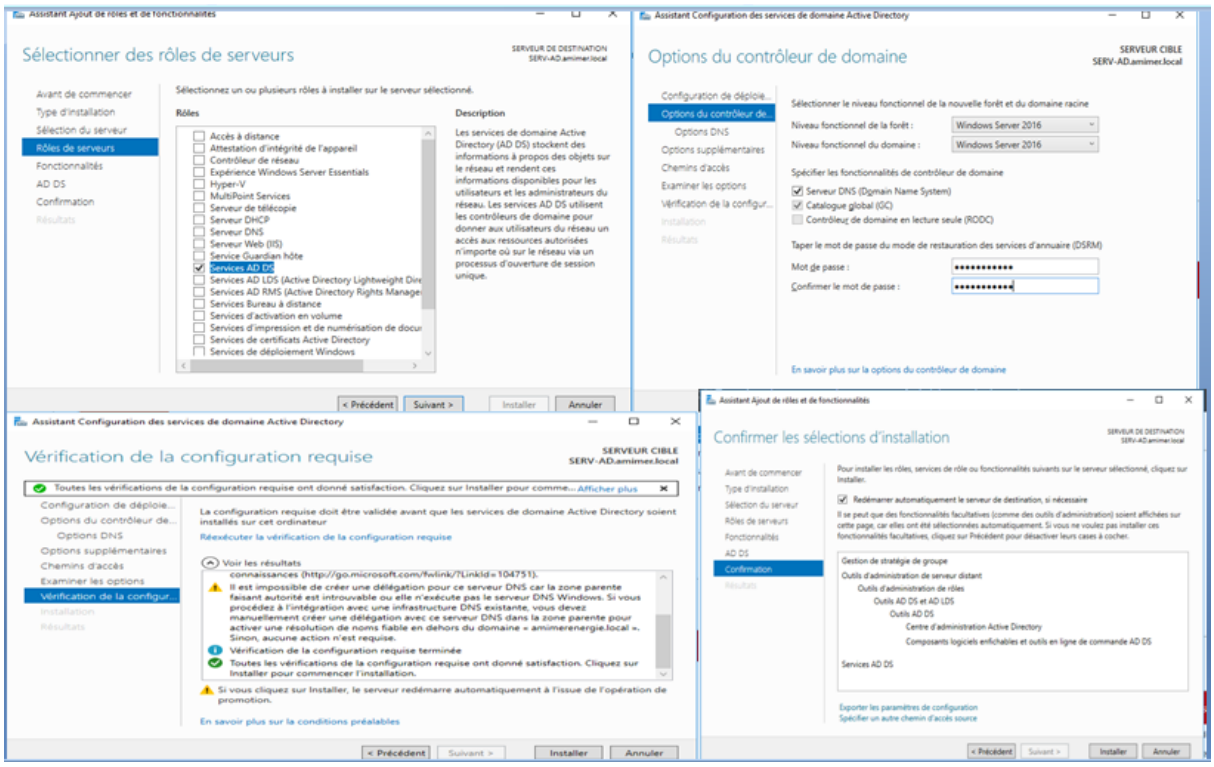

FIGURE 3.7 – Installation de l'Active Directory

Comme on a déployé une autorité de certification en installant le rôle "Services de

certificats Active Directory (AD CS)" qui permettent de sécuriser gratuitement de nombreux services accessibles uniquement depuis les ordinateurs de l'entreprise. Les étapes sont les suivantes :

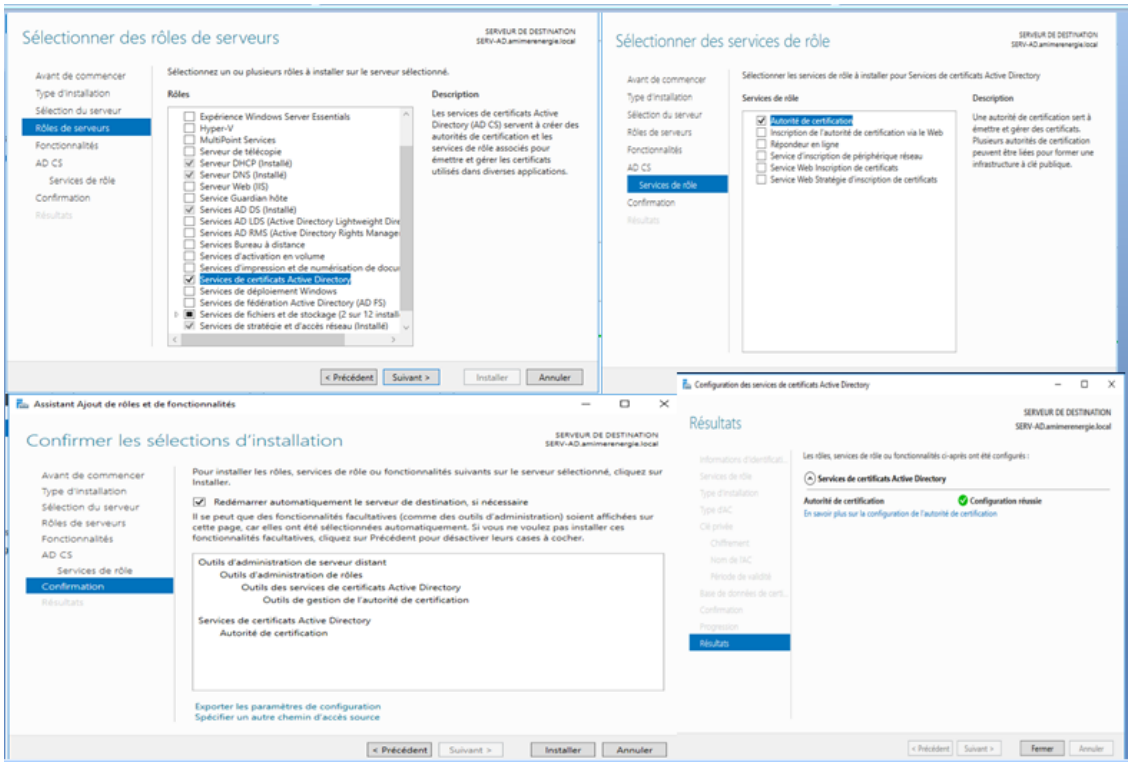

FIGURE 3.8 – Installation de l'Active Directory Certificat

Maintenant nous allons commencer la configuration de notre Active Directory. La première étape consiste à créer une nouvelle foret, nommé amimerenergie.local . Le nom affecté, Windows nous demande de choisir le niveau fonctionnel de notre foret Active Directory. Dans notre exemple, nous mettrons un niveau fonctionnel 2016. Windows nous propose ensuite d'installer des options supplimentaires , tel qu'un serveur DNS compatible avec notre Active Directory. Le domaine créé amimerenergie.local est notre premier controleur de domaine catalogue global activé. Lorsque les services seront installés et configurés, cliquant sur FIN le système devra rédemmarer. A la fin de l'installation on aura les deux roles installés comme le montre la figure suivante :

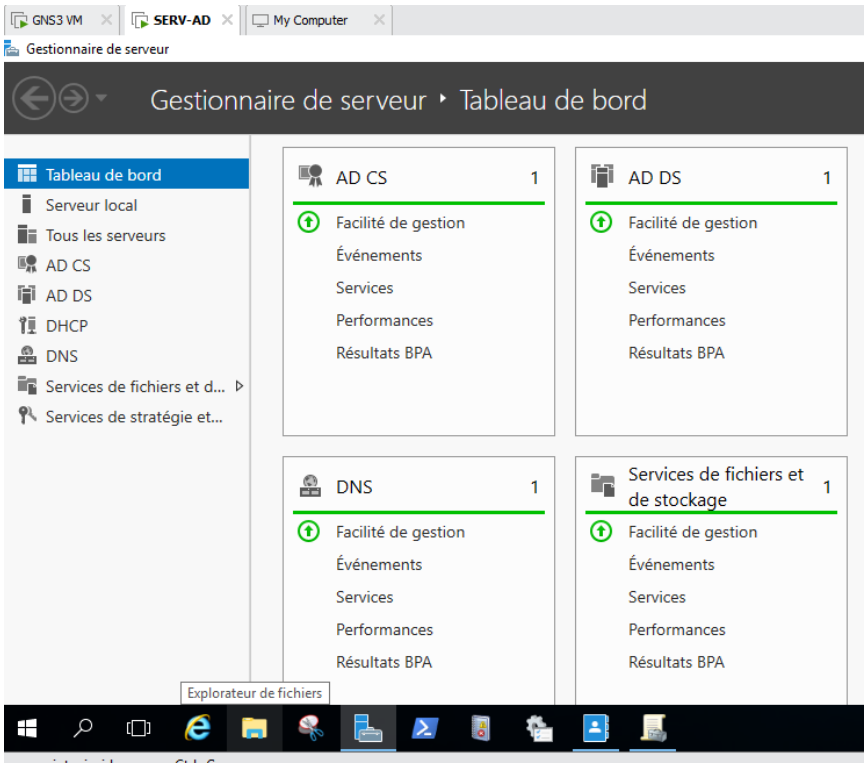

FIGURE 3.9 – Les deux roles AD et DNS

On a commencé par créer une unité d'organisation, il suffit d'aller sur le nom de notre domaine amimerenergie.local –> en cliquant sur le bouton droit, on sélectionne nouveau –> Unité d'organisation puis on va entrer le nom de notre unité de l'organisation qui est UO-amimerenergie.

pour créer des comptes pour les utilisateurs il faut aller sur utilisateur –> cliquer sur le bouton droit nouveau –> utilisateur pour remplir les informations correspondantes à l'utilisateur ainsi le mot de passe d'ouverture de sa session –> valider.

Ensuite on passe à la création des groupes et des ordinateurs pour les utilisateurs déjà crée.

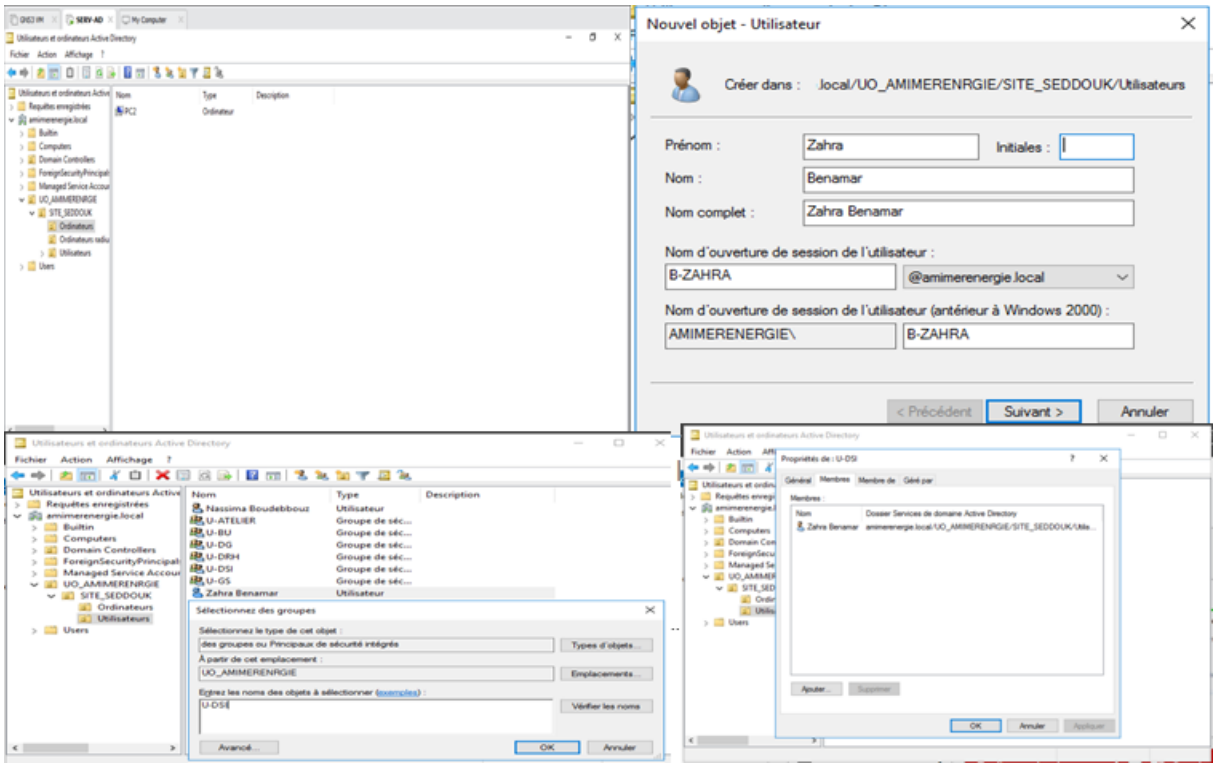

FIGURE 3.10 – Création des unités d'organisations ,utilisateurs ,groupes et ordinateurs

Maintenant, après avoir crée les groupes et les utilisateurs, on passe au GPO qui définissent les droits des utilisateurs, et des stratégies de groupes qui sont applicables aux Sites, Domaines et UO.Pour créer des GPO, nous allons dans le menu démarrer, puis outils d'administration et cliquant sur gestion des stratégies de groupe.

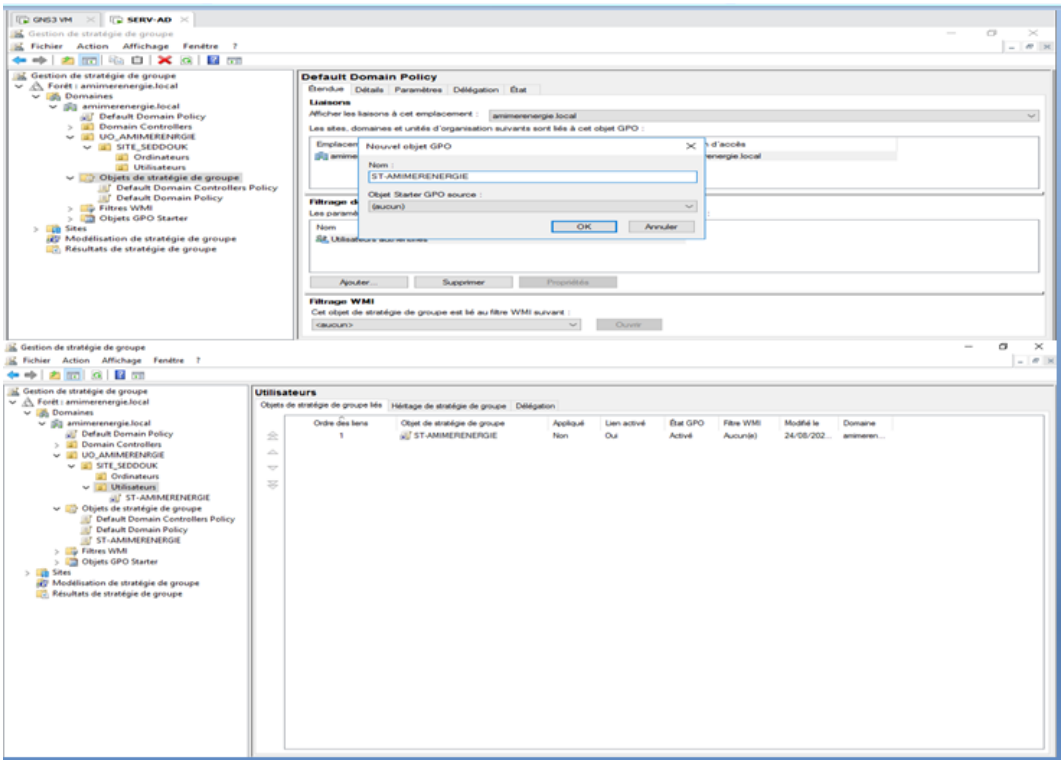

FIGURE 3.11 – Création de la GPO

Pour la mise en place de la GPO par exemples dans notre cas on veut supprimer la corbeille dans le bureau, nous allons dans la configuration utilisateur et nous choisissons l'ongle modèle d'administration –> Bureau –> Supprimer l'icone de la corbeille du bureau puis on clique sur le bouton Activé comme la montre la figure suivante :

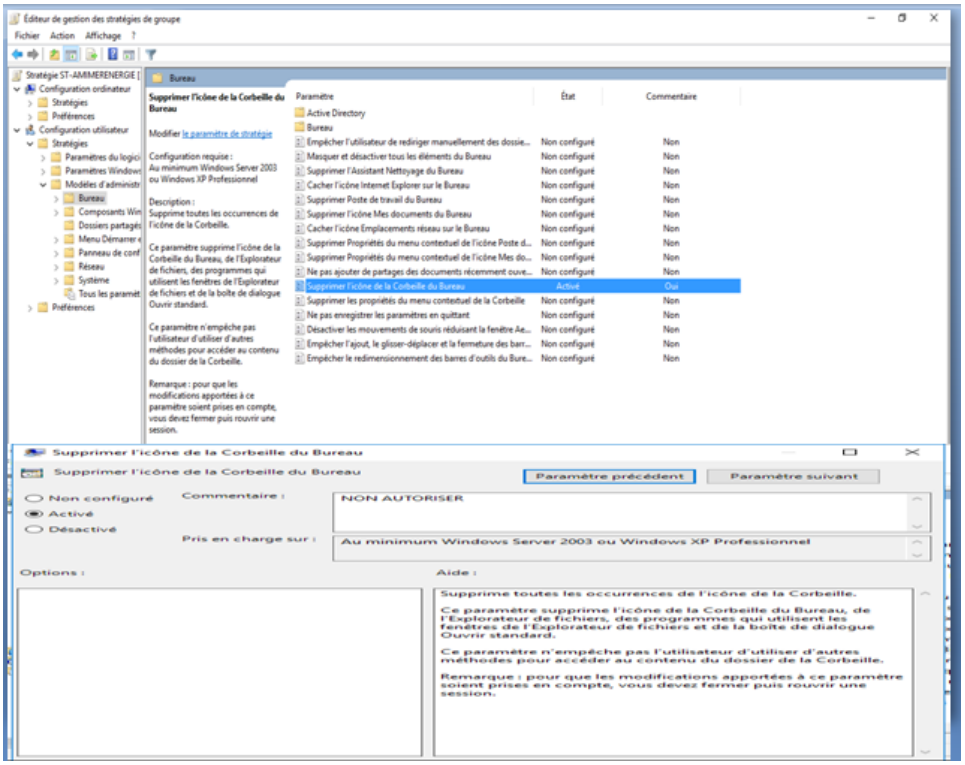

FIGURE 3.12 – La mise en place de la stratégie de la GPO

Vérification la suppression de la corbeille :

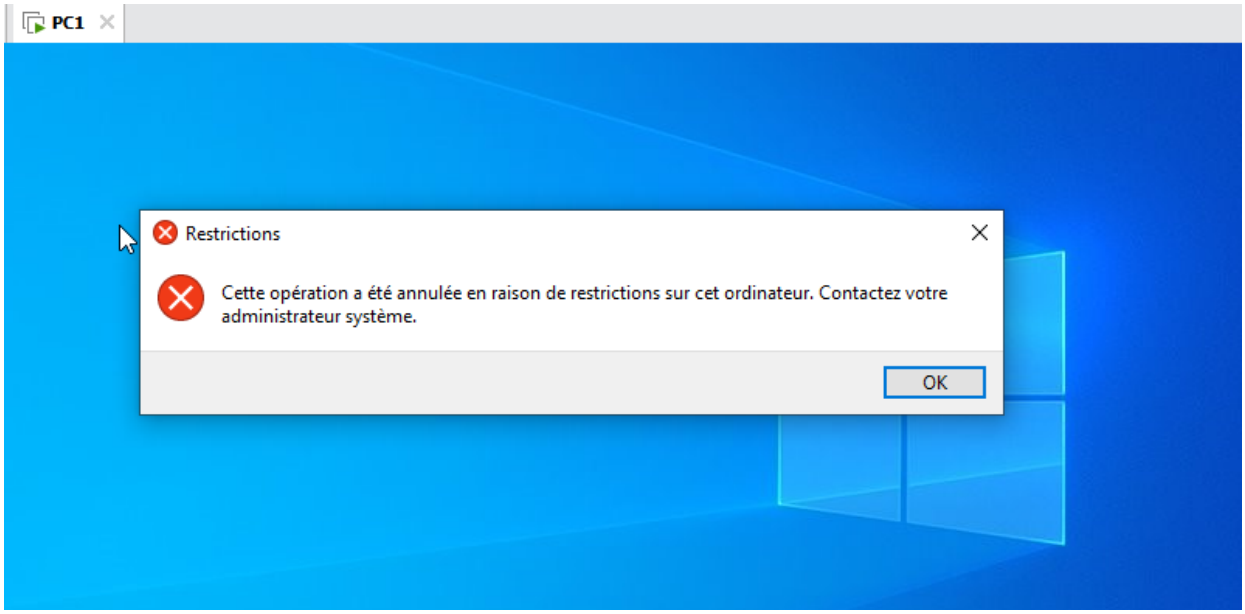

FIGURE 3.13 – La corbeille est supprimée

Comme on a ajouté d'autres GPO comme presente la figure ci-dessous :

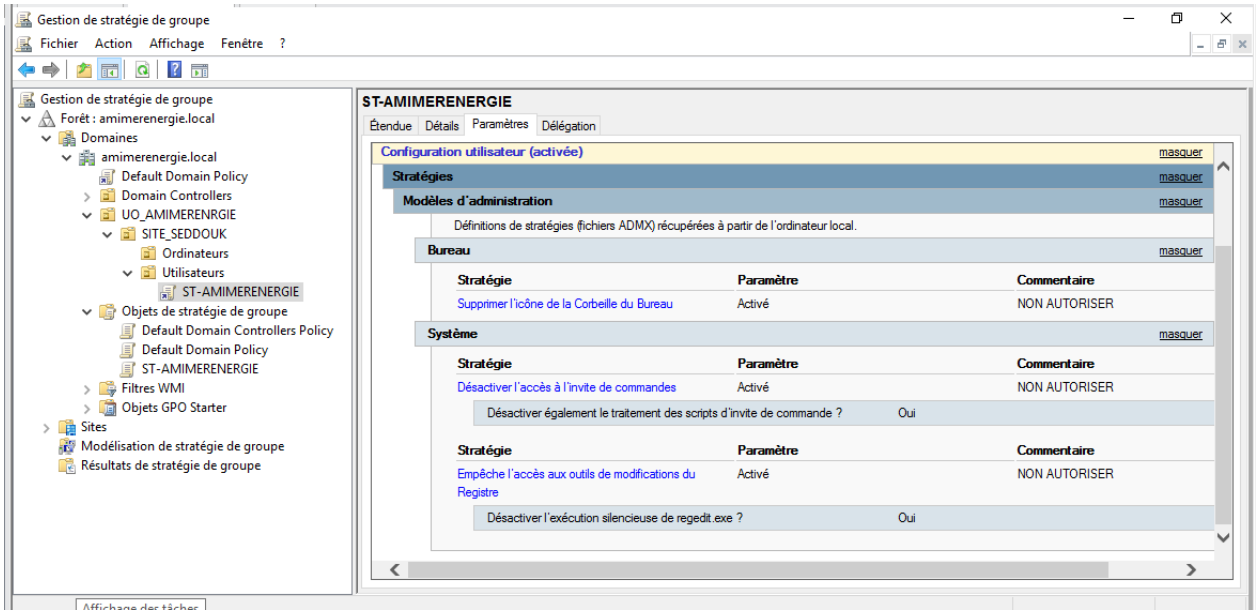

FIGURE 3.14 – La mise en place d'autres stratégie de la GPO

Pour forcer la mise à jour de la stratégie appliqué sur les utilisateurs on doit saisir la commande gpupdate sur l'invite de commande et redémarrer le serveur.

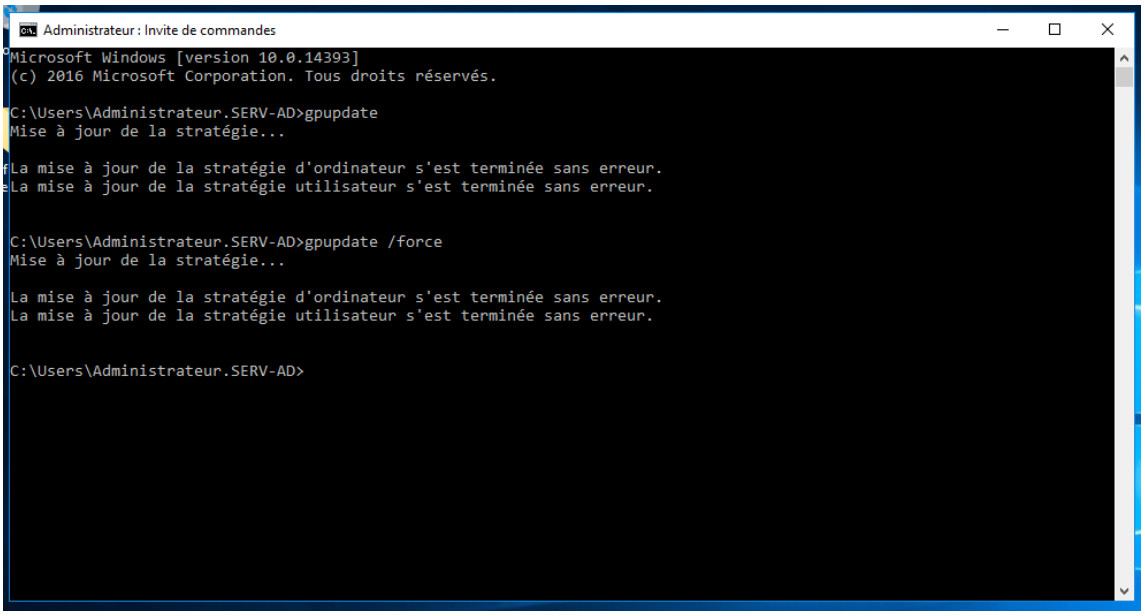

FIGURE 3.15 – La mise à jour de la stratégie

3.3.3 Installation de Dynamic Host Configuration Protocol (DHCP)

Nous avons installé DHCP server sur la machine Windows server 2016 Pour commencer l'installation, il va falloir ajouter le Service de DHCP Server et ajouté les fonctionnalités nécessaires .

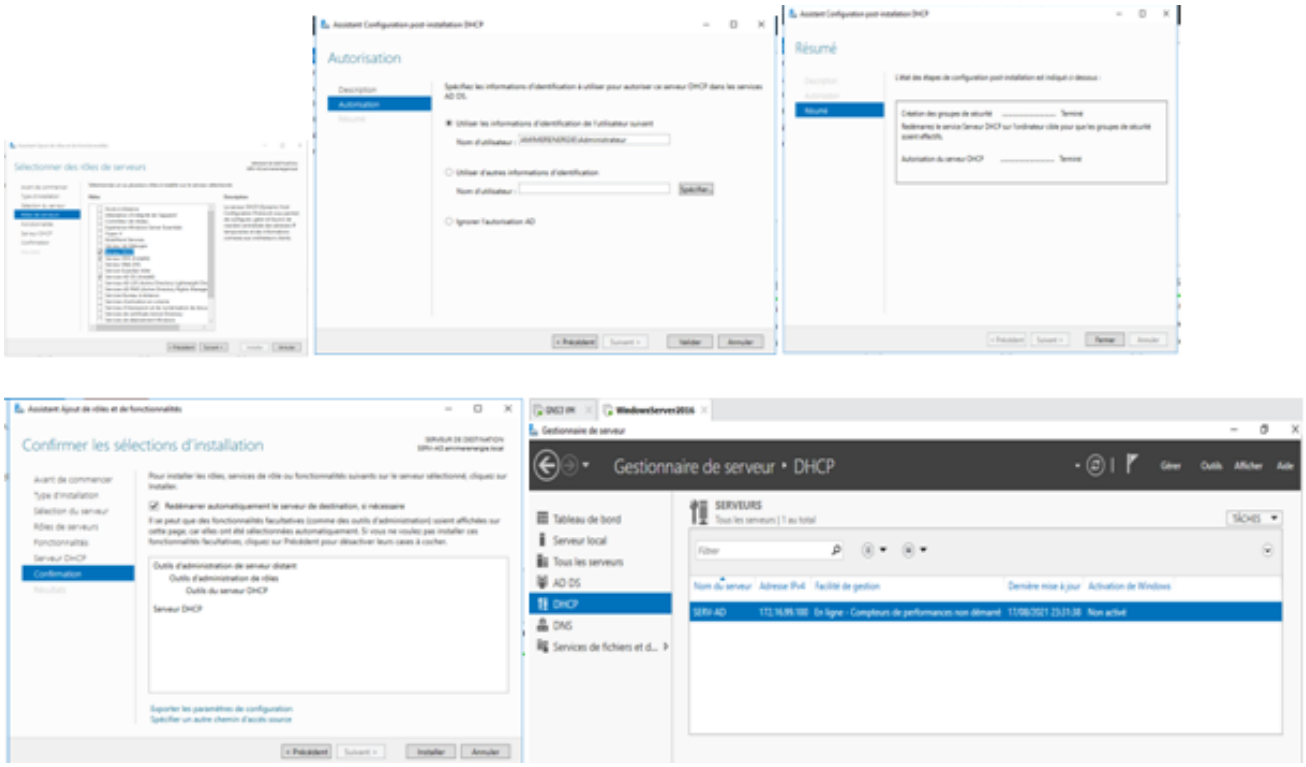

FIGURE 3.16 – Installation de DHCP

On va commencer par créer des étendus pour chaque vlan déjà crée, nous allons dans serv-ad.amimerenergie.local –> ipv4 –> nouvelle etendu , comme la montre la figure suivante :

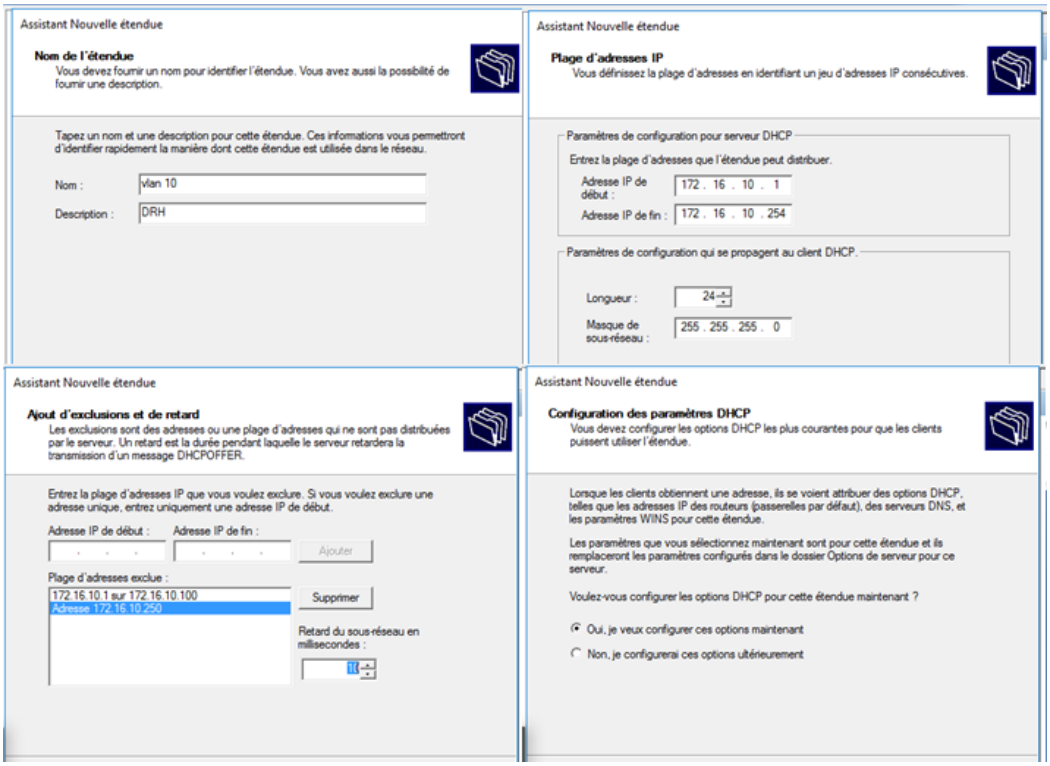

FIGURE 3.17 – création de l'étendu

la figure ci-dessous montre toutes les étendus qu'on a créés et vérifiés et que le DHCP server a attribué une adresse au pc dans la plage d'adresse qu'on a déjà donné sur l'etendu.

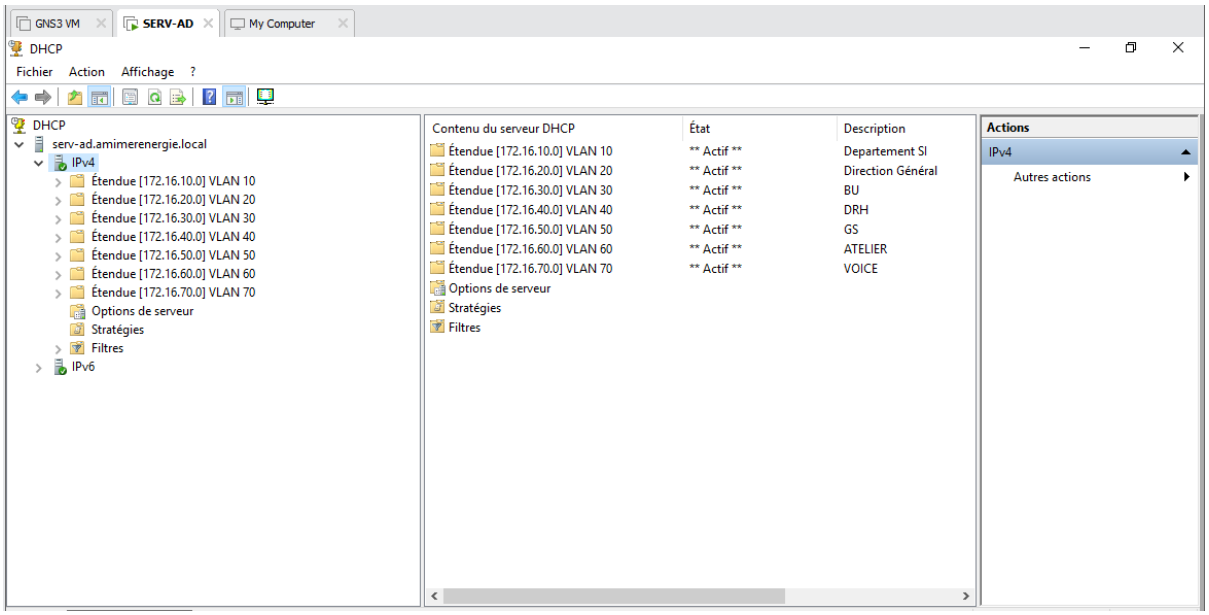

FIGURE 3.18 – Vérification des étendus crée

3.3.4 Installation de Domain Name System (DNS)

Nous avons installé DNS server sur la machine Windows server 2016 Pour commencer l'installation, il va falloir ajouter le Service de DNS Server et ajouté les fonctionnalités nécessaires .

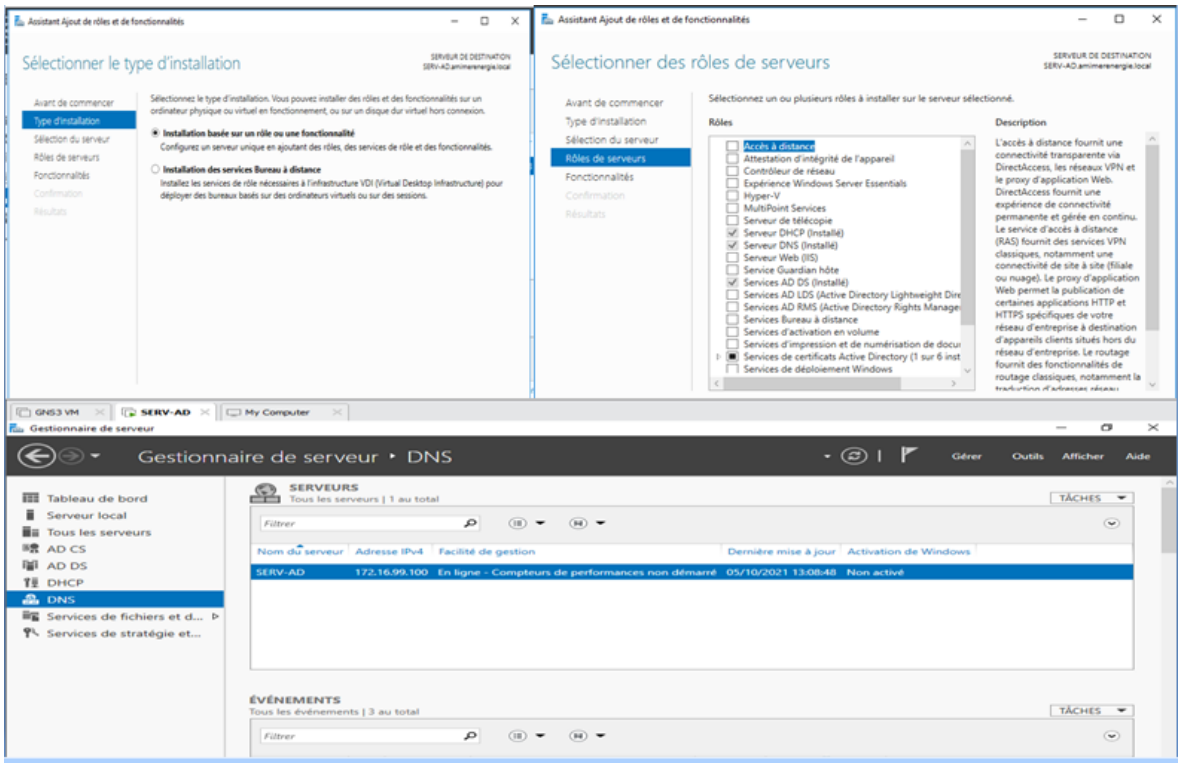

FIGURE 3.19 – Services DNS

On a créé une zone de recherches directes qu'on l'a nommé amimerenergie local d'où on a ajouté les différents hôtes qu'on a utilisés avec leurs adresses IP .

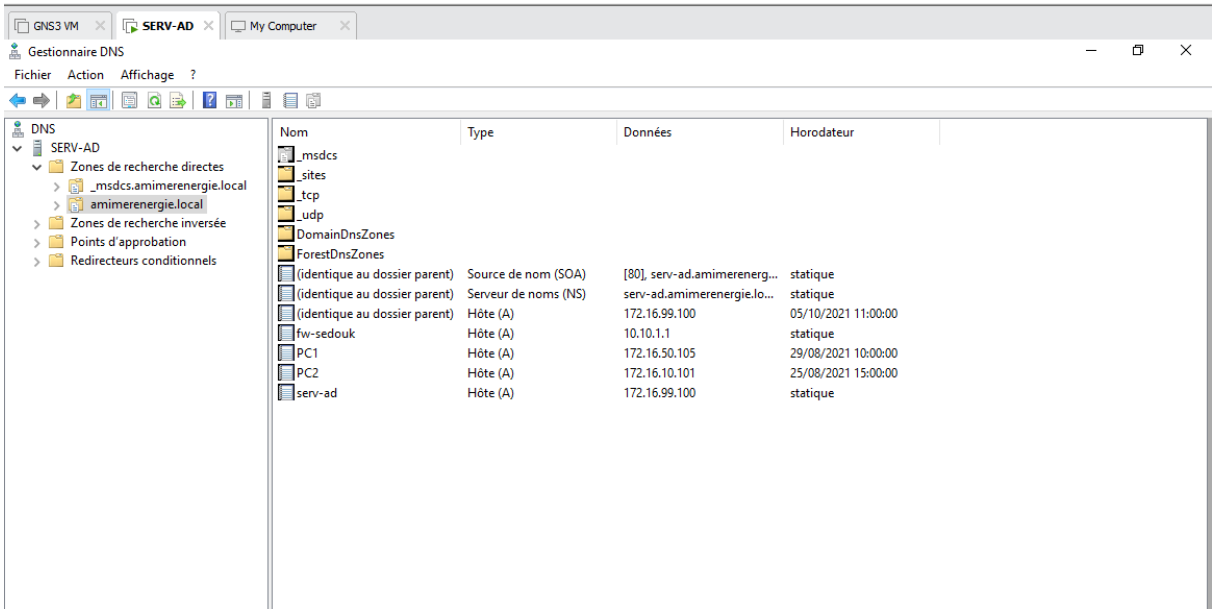

FIGURE 3.20 – DNS

Installation de radius

Sur le même serveur2016 on a installé le serveur RADIUS, comme la montre la figure qui suit :

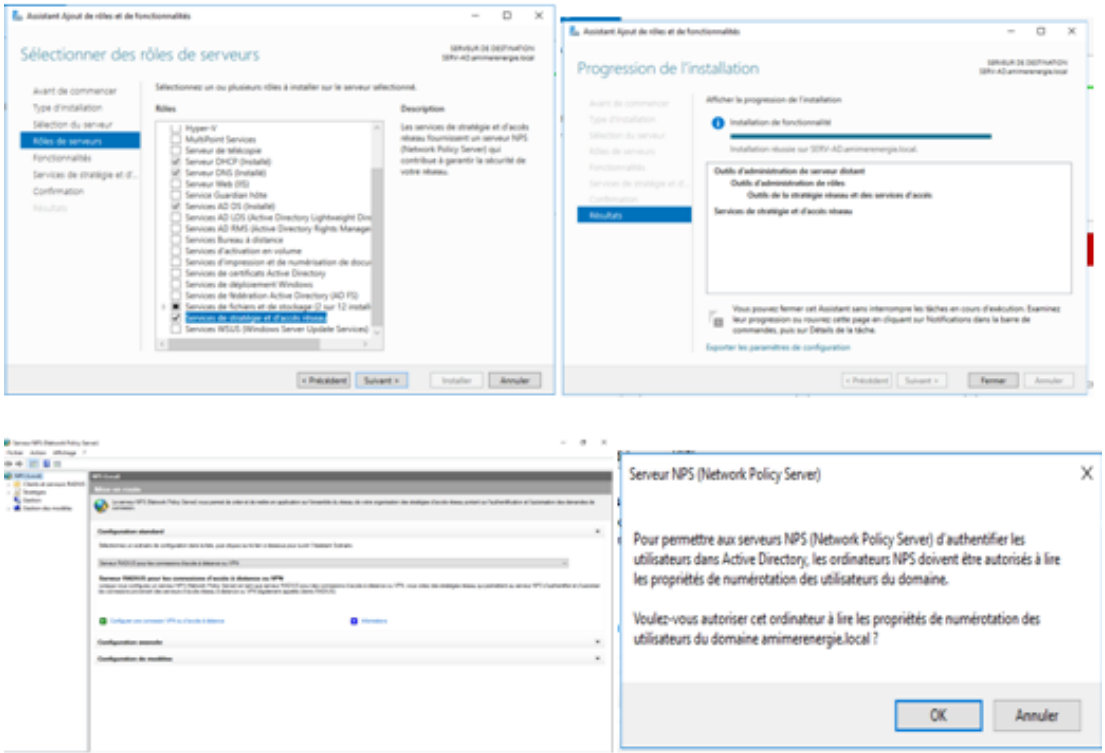

FIGURE 3.21 – Installation de RADIUS

Interface Radius se présente comme ceci :

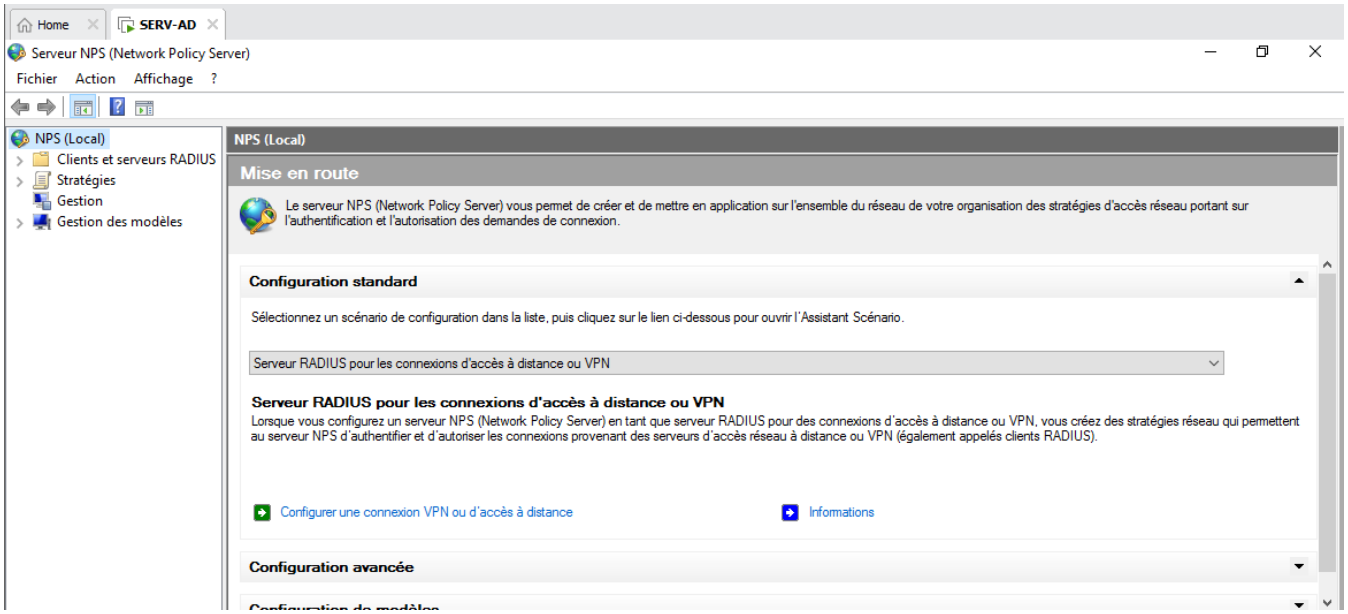

FIGURE 3.22 – Interface de RADIUS

D'abords, on va configurer la carte réseau du serveur radius pour qu'elle puisse connecter automatiquement.

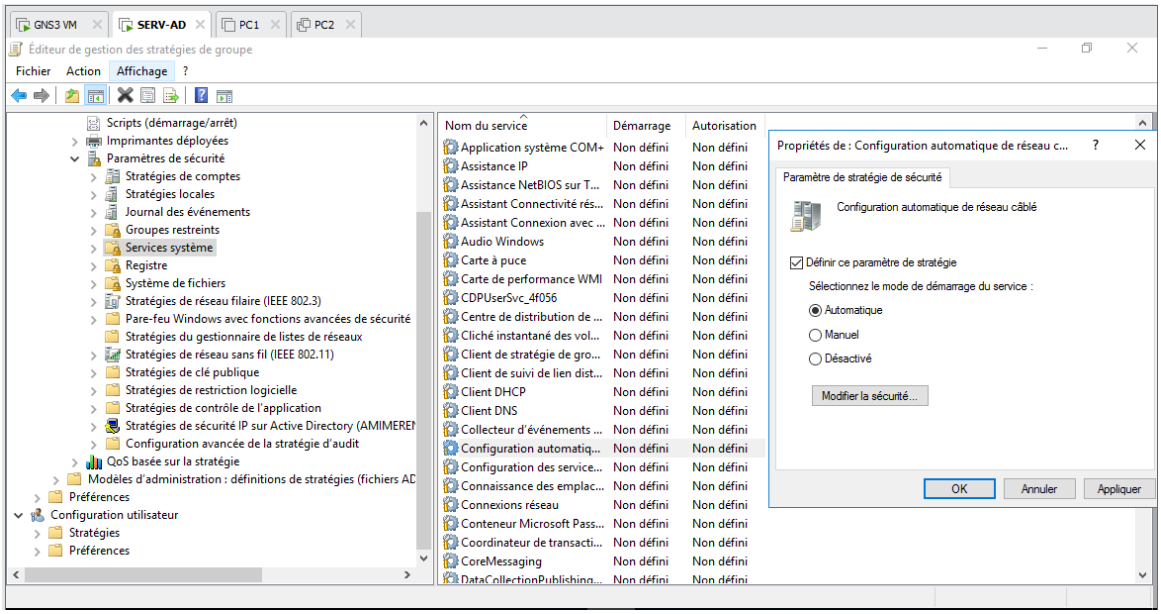

FIGURE 3.23 – Configuration de la carte réseau RADIUS

pour créer des comptes pour les utilisateurs Radius il faut aller sur utilisateur –> cliquer sur le bouton droit nouveau –> utilisateur pour remplir les informations correspondantes à l'utilisateur Radius ainsi le mot de passe d'ouverture de sa session –> valider. Ensuite on passe à la création des groupes et des ordinateurs Radius pour les utilisateurs déjà crée.

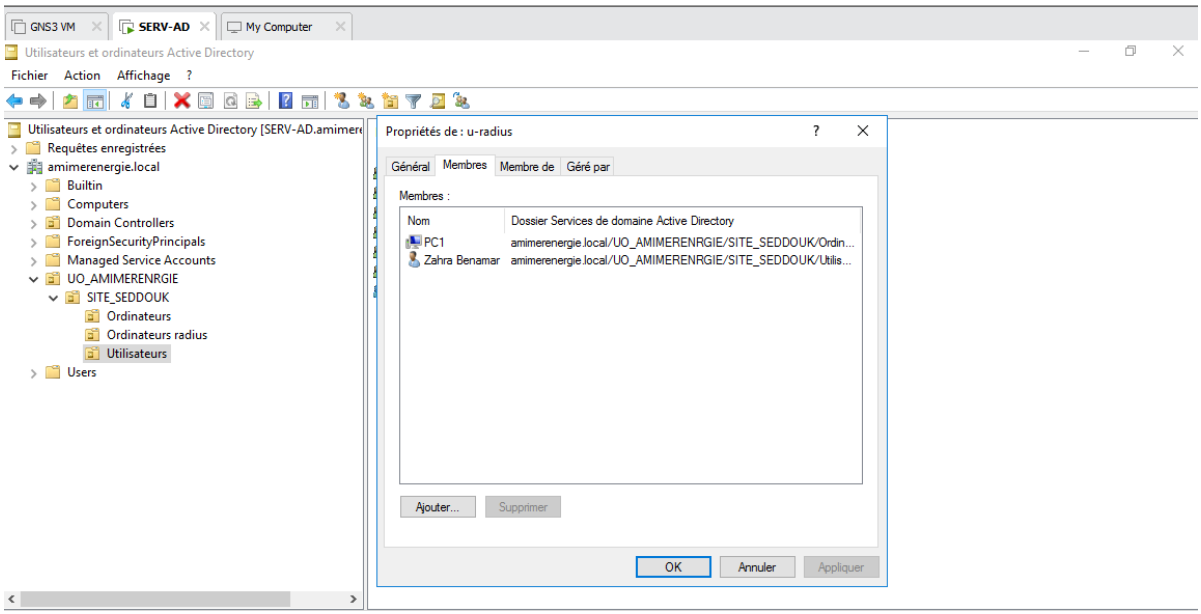

FIGURE 3.24 – Création des utilisateurs et groupes RADIUS

On a configuré le client RADIUS sur le SWA2 du vlan 50 avec une clé secrète partagé " AMIMER " .

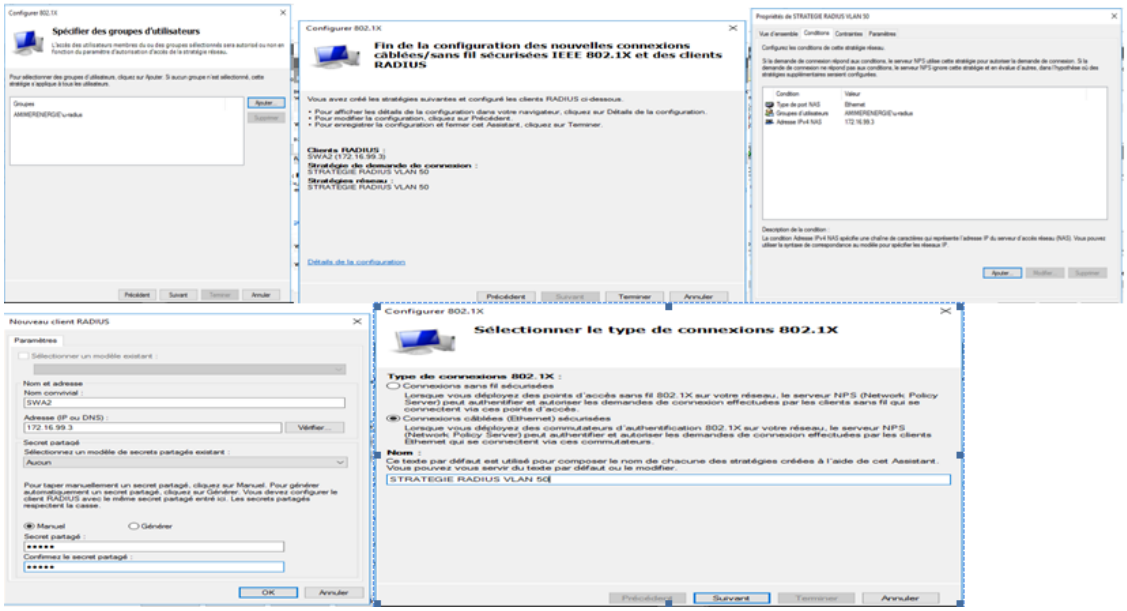

FIGURE 3.25 – Configuration de client RADIUS

Après avoir crée les groupes et les utilisateurs Radius, on va créer maintenant des stratégies de groupes Radius , nous allons dans le menu démarrer, puis outils d'administration et cliquant sur gestion des stratégies de groupe.

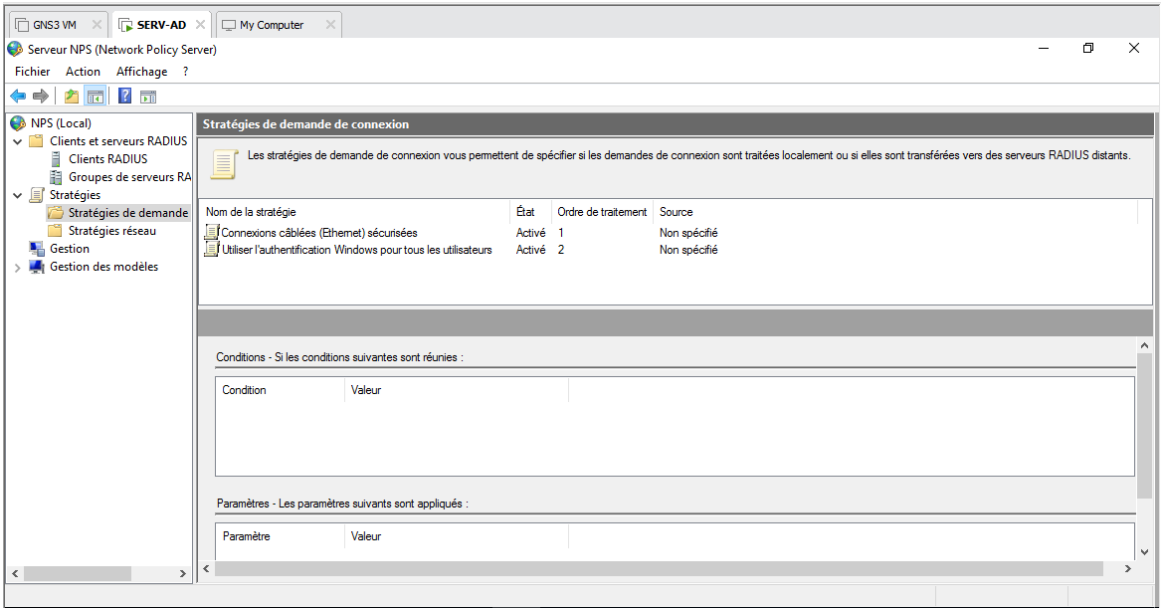

FIGURE 3.26 – Stratégies de groupes RADIUS

Après, on passe à la stratégie de sécurité RADIUS, où on a choisi la méthode d'authentification PEAP pour la stratégie du réseau filaire.

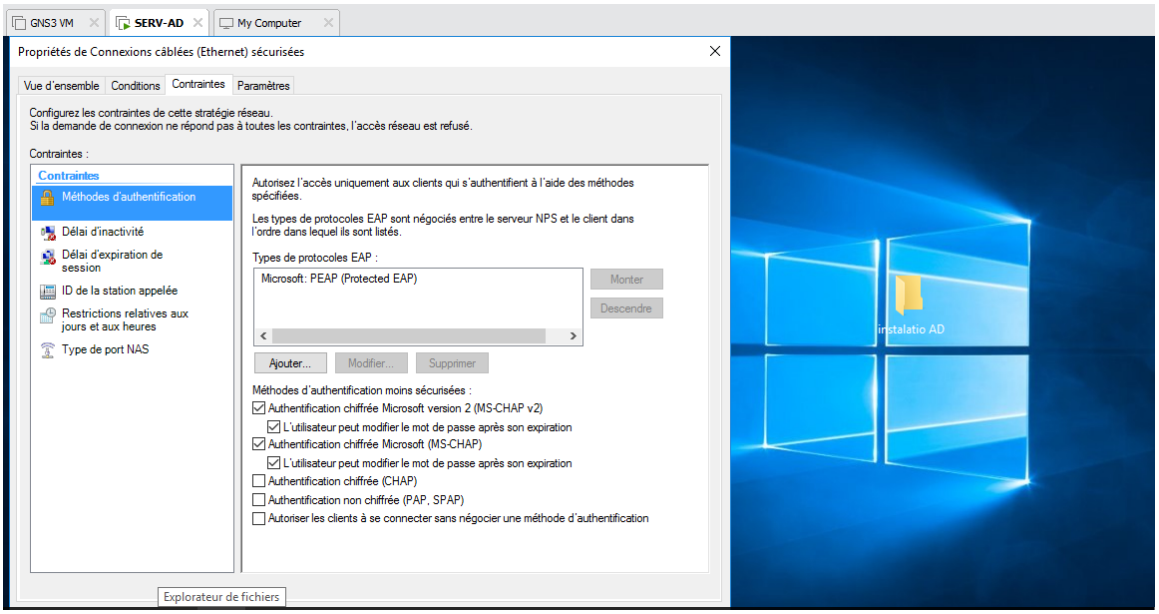

FIGURE 3.27 – Sécurité RADIUS

Pour envoyer des attributs supplémentaires au client RADIUS , on a sélectionner des attributs tunnels au fournisseur spécifique.

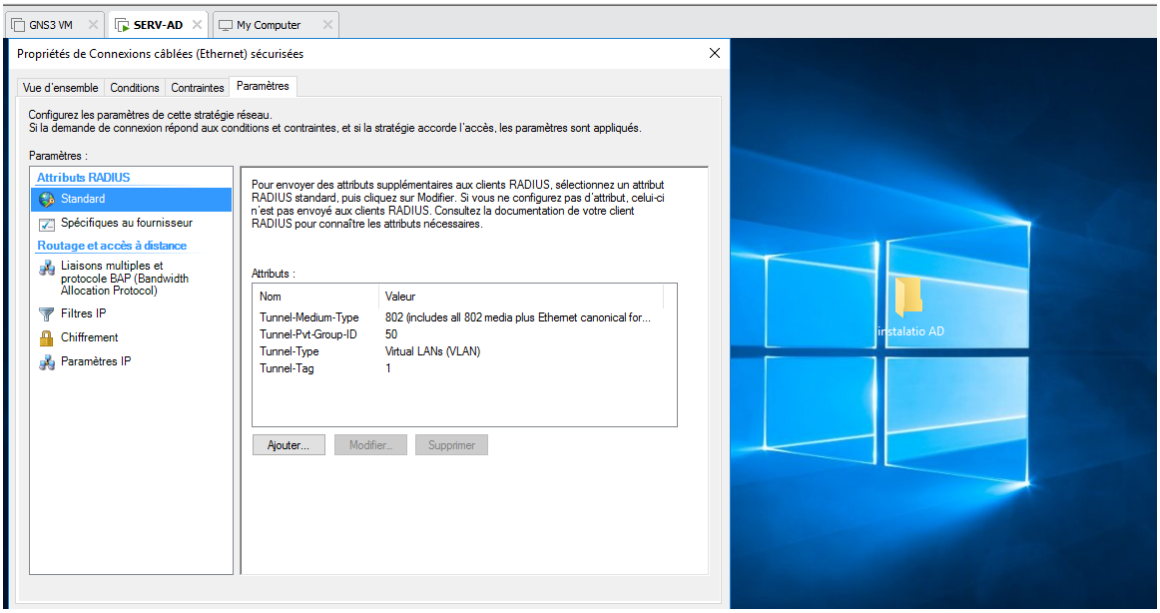

FIGURE 3.28 – Attributs de tunnels RADIUS

3.4 Installation et configuration du Sophos UTM

3.4.1 Installation Firewall Sophos UTM

Premièrement, on a commencé par l'installation des deux machines virtuelles sophos UTM version 18. pour les deux sites Seddouk et Alger, ensuite on a attribué des adresses IP pour les deux interface LAN et WAN du pare-feu.

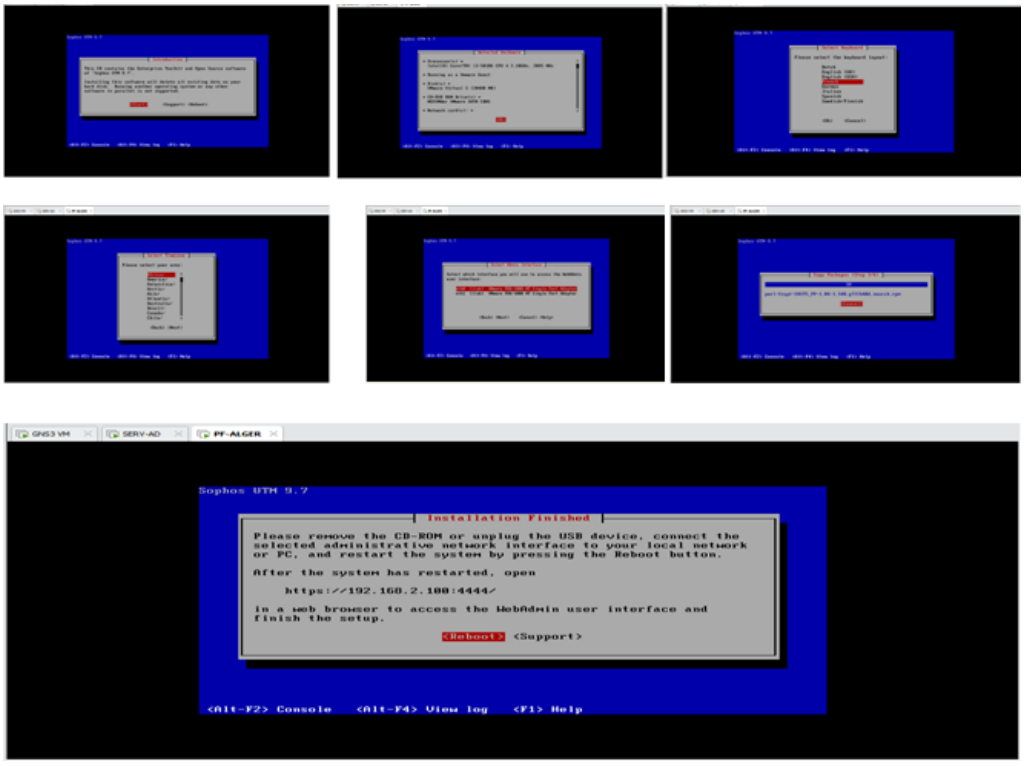

FIGURE 3.29 – Installation de pare-feu Sophos UTM

La prochaine étape consistera à configurer le pare-feu Sophos que nous avons déjà installé ou la configuration de la page d'authentification est nécessaire :

Tout d'abord il faut se rendre dans le site du pare-feu ou une configuration de la page d'authentification est nécessaire au début et ceux en y insérant quelques information sur l'entreprise suivi du mot de passe avec lequel accédera l'administrateur à Sophos.

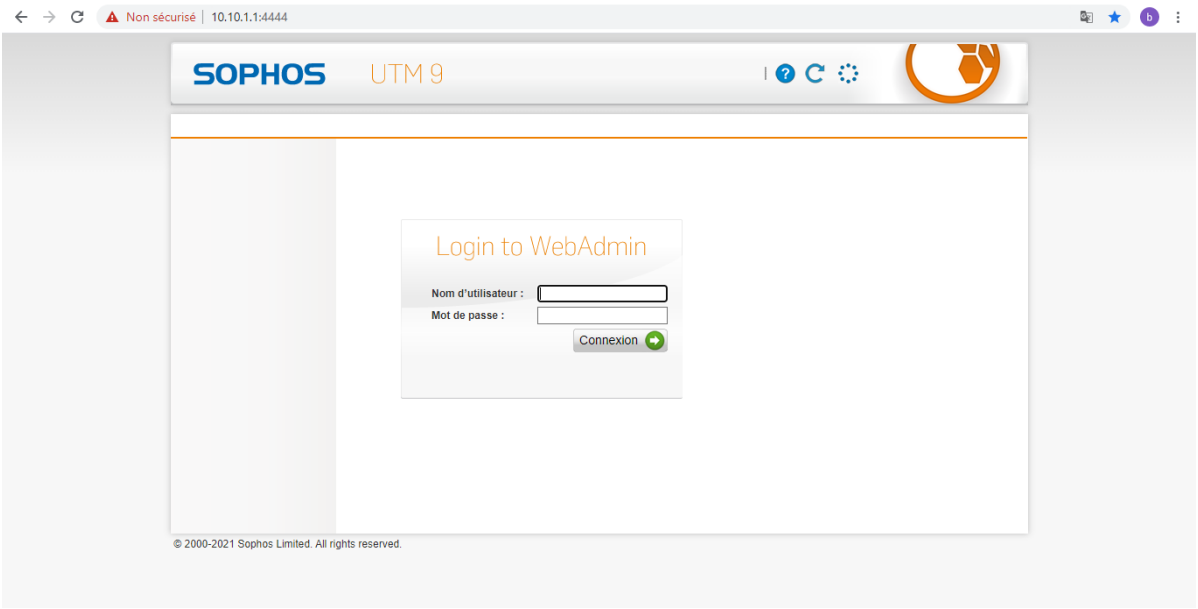

FIGURE 3.30 – La page d'authentification de Sophos UTM

Après avoir introduit le mot de passe et le nom d'utilisateur(s'authentifier) l'interface d'accueil s'affichera comme suit :

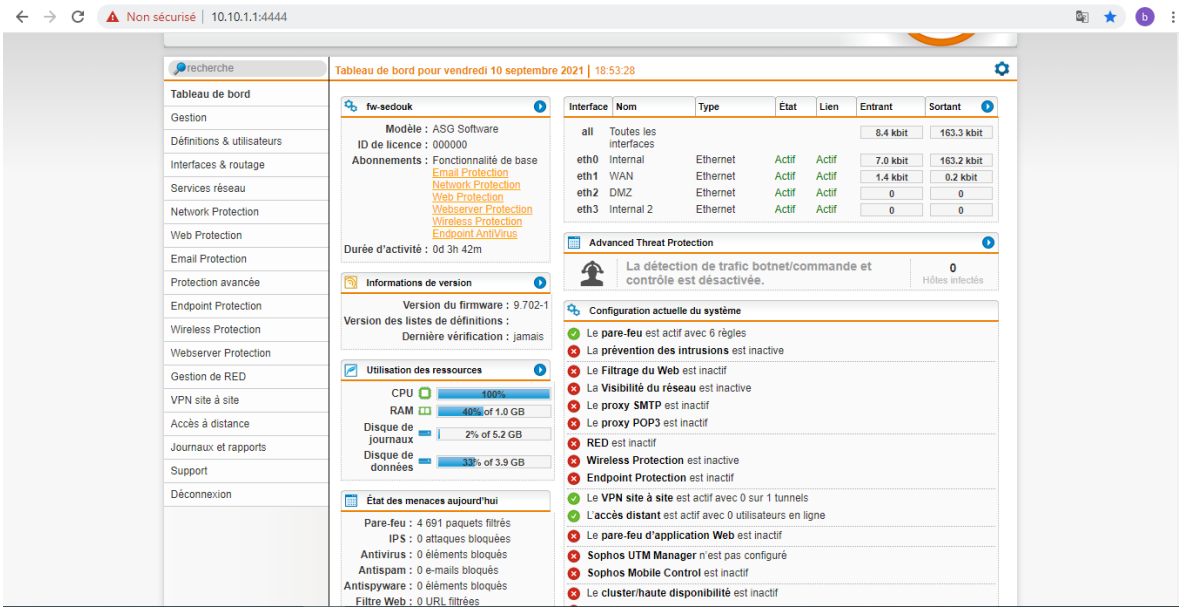

FIGURE 3.31 – Vu globale de l'interface d'accueil

3.4.2 Création des utilisateurs

La création des utilisateurs se fait en allant à "Définitions utilisateurs" –> "utilisateur Groupes"–> "Nouveau utilisateur" et puis on insère les informations nécessaires pour que l'utilisateur s'authentifiera par la suite afin d'accéder au réseau internet.

La figure ci-dessous représente les utilisateurs que nous avons créés :

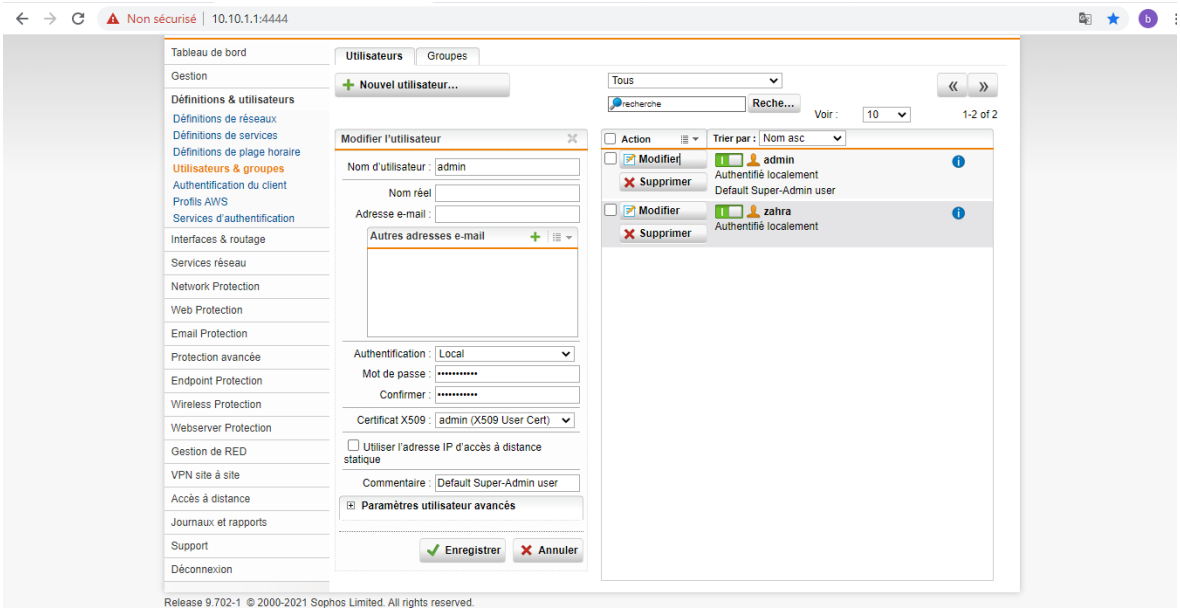

FIGURE 3.32 – La liste des utilisateurs UTM

3.4.3 Création des groupes

Les groupes sont créés de la même façon seulement à partir de l'onglet groupe, nous avons céé des groupes et attribuer chaque utilisateurs à son groupe.

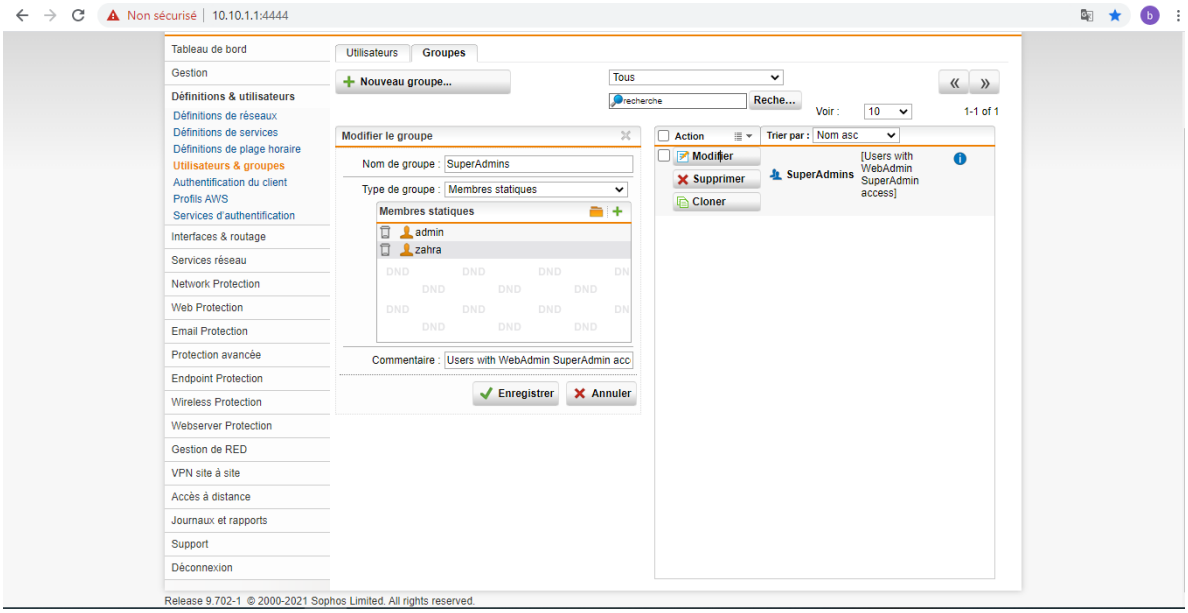

FIGURE 3.33 – La liste des groups UTM

3.4.4 Gestion des objets réseaux

Pour créer des objets réseaux , on allons sur Définitions utilisateurs > Définitions de réseaux > Nouvelle définition de réseau puis on insère les informations nécessaires le nom de la définition , le type qui peut étre un réseau, hôte, plage... , son adresse ip et masque réseau.

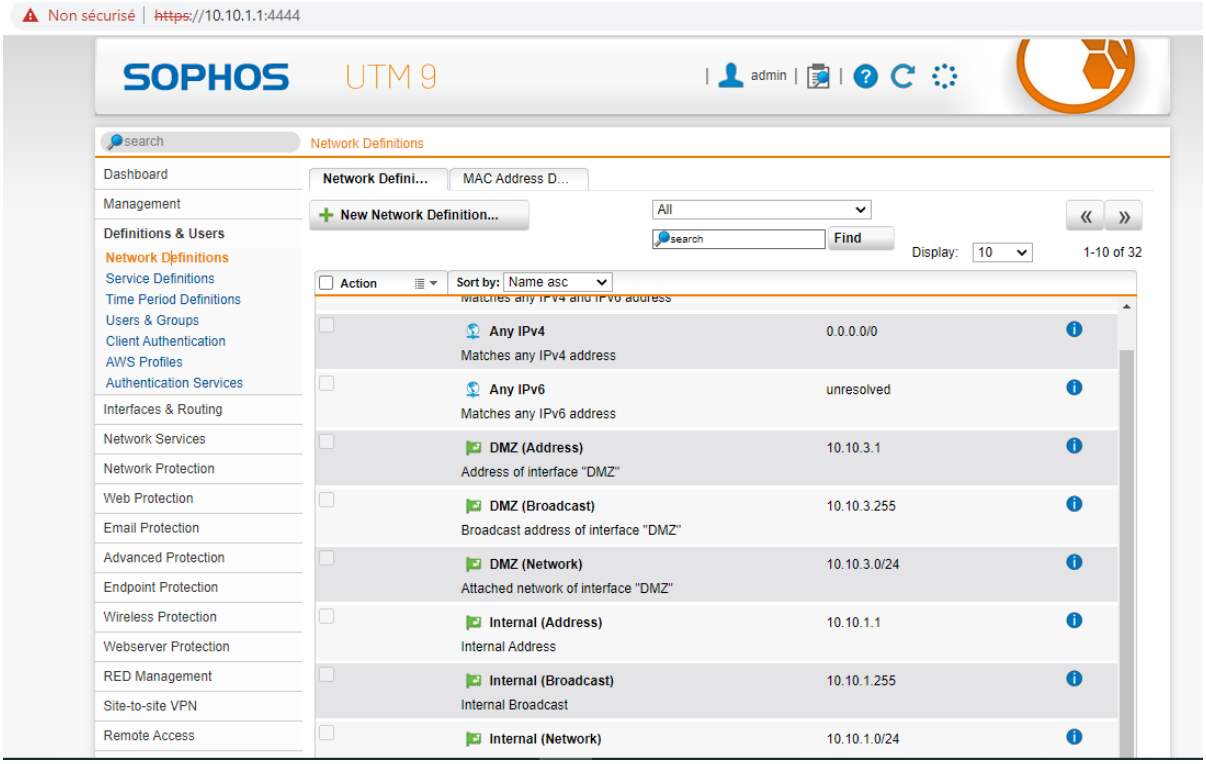

FIGURE 3.34 – Les objets réseaux du parfeu de Seddouk

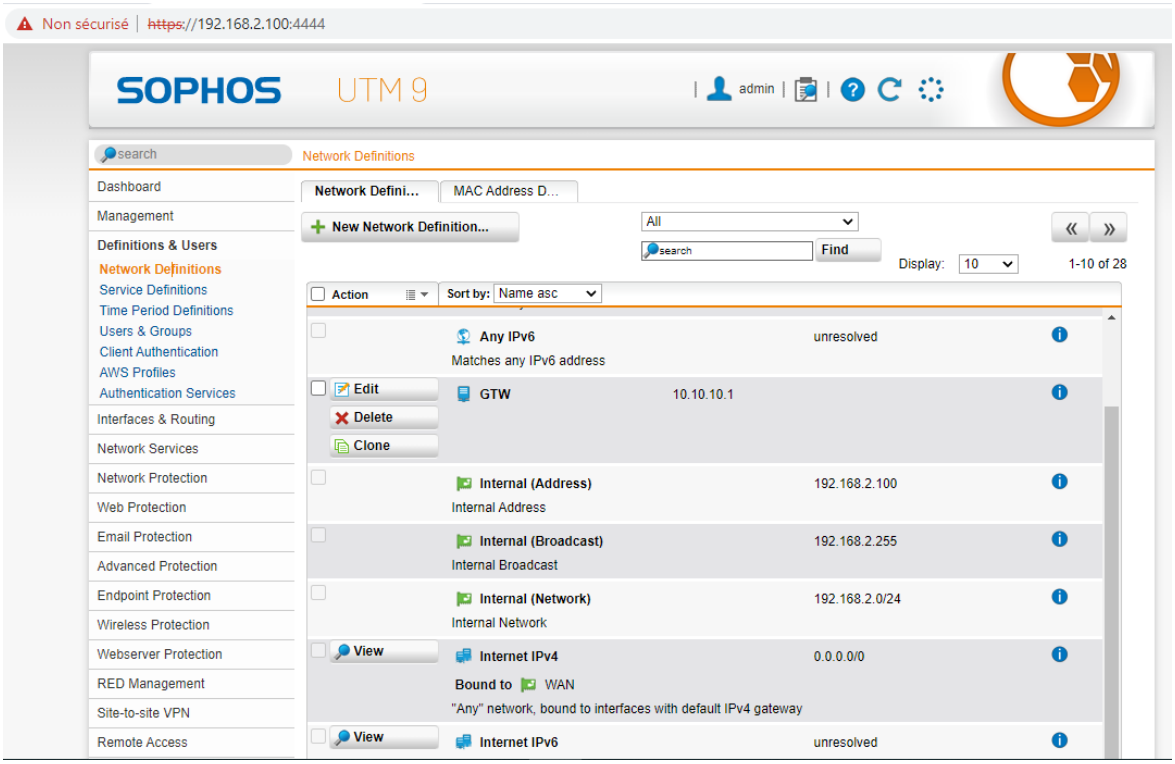

FIGURE 3.35 – Les objets réseaux du parfeu d'Alger

3.4.5 Création et activation des interfaces

nous avons besoin dans le parfeu de Seddouk de créer quatre interfaces une externe avec laquelle le site communiquera avec l'extérieur (Alger) et deux pour le réseau interne du site et l'autre pour la DMZ .Pour le parfeu d'Alger deux interfaces une pour le réseau interne et l'autre pour le réseau externe avec laquelle le site communiquera avec le site de Seddouk ou nous devons suivre les étapes suivantes :

— Aller à interfaces and routage –> interfaces –> nouvelle interface.
— Entrer les informations correspondantes (nom de l'interface, le type , matériel, l'adresse ip , masque réseau et l'adresse de la passerelle).

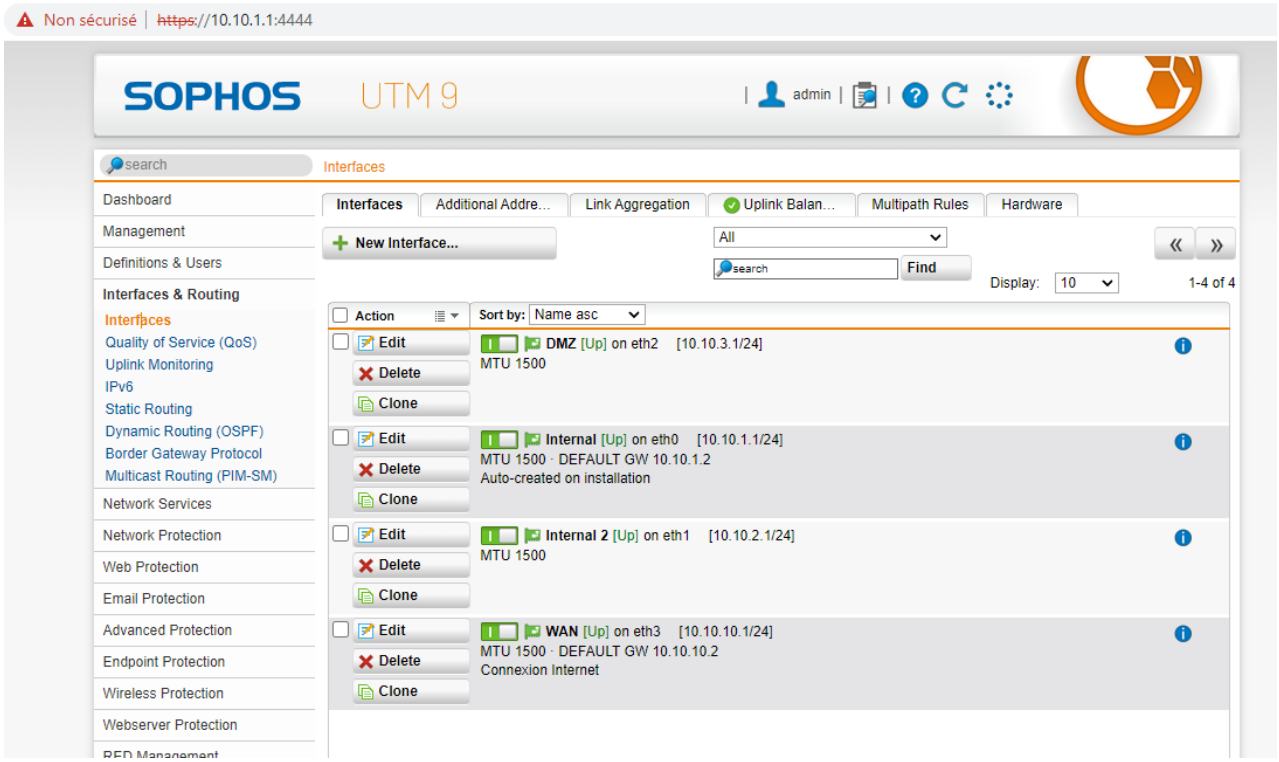

FIGURE 3.36 – Les interfaces externes et internes du parfeu de Seddouk

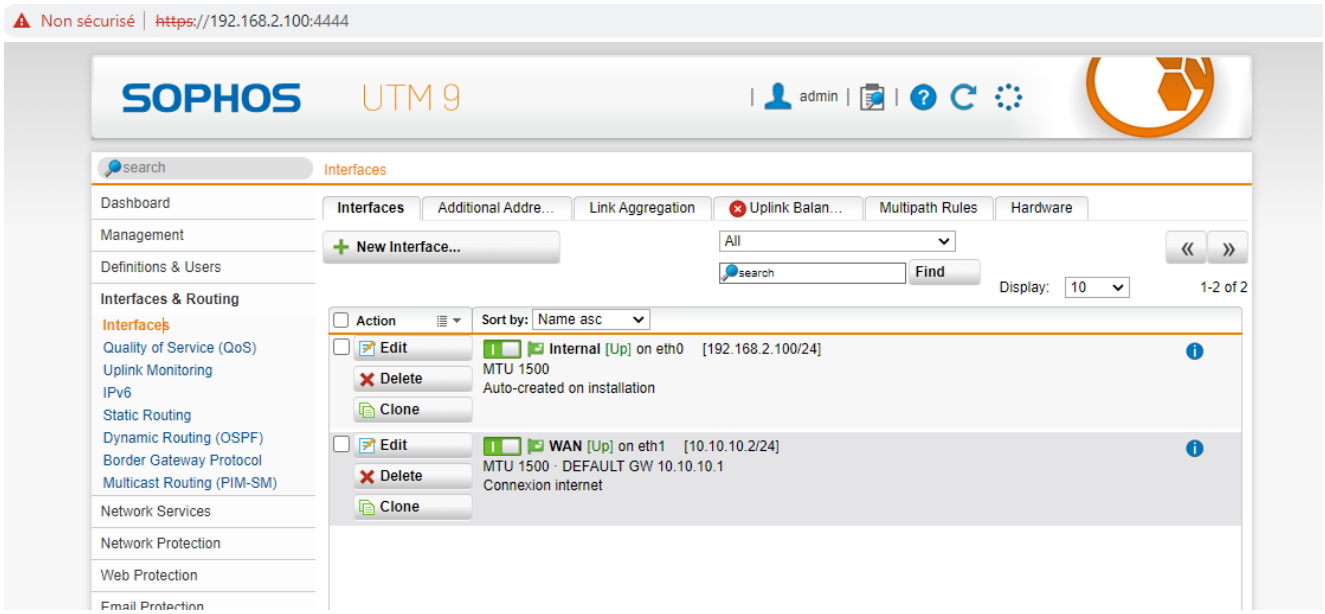

FIGURE 3.37 – Les interfaces externes et internes du parfeu d'Alger

3.4.6 Routage statique

On veut router vers le VLAN 99 ou il y a le serveur et le VLAN 10 donc d'abors nous allons à Interfaces routage –> Routage statique –> Nouvelle route statique ,puis on doit choisir le type de routage comme dans notre cas on a choisi le routage par interface afin de router les paquets pour atteindre le réseau distant .

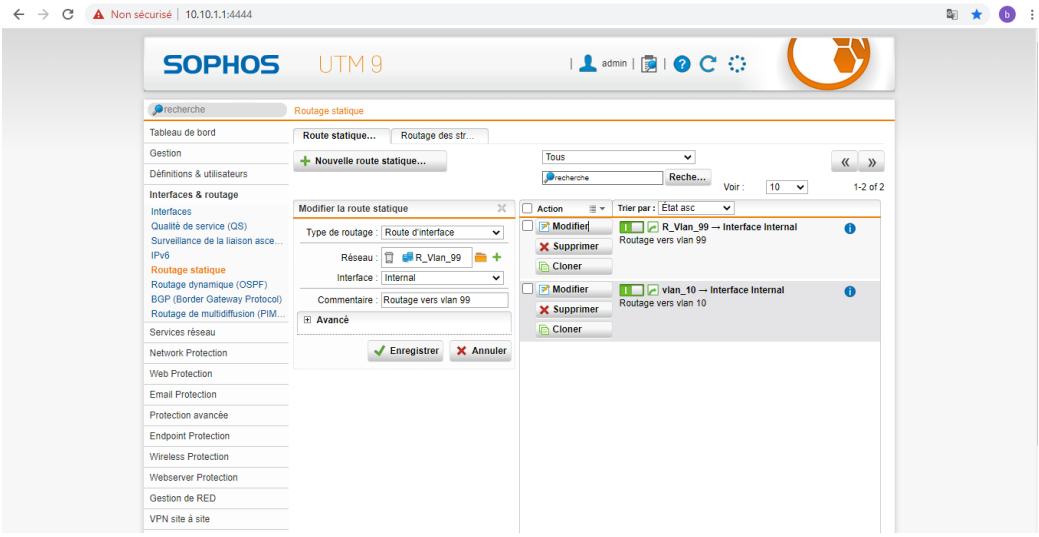

FIGURE 3.38 – Le routage statique

3.4.7 Serveurs DNS

Pour DNS, on doit lister le réseau autorisé à utiliser le système comme un résolveur DNS récursif , on allons sur Services réseau > DNS .

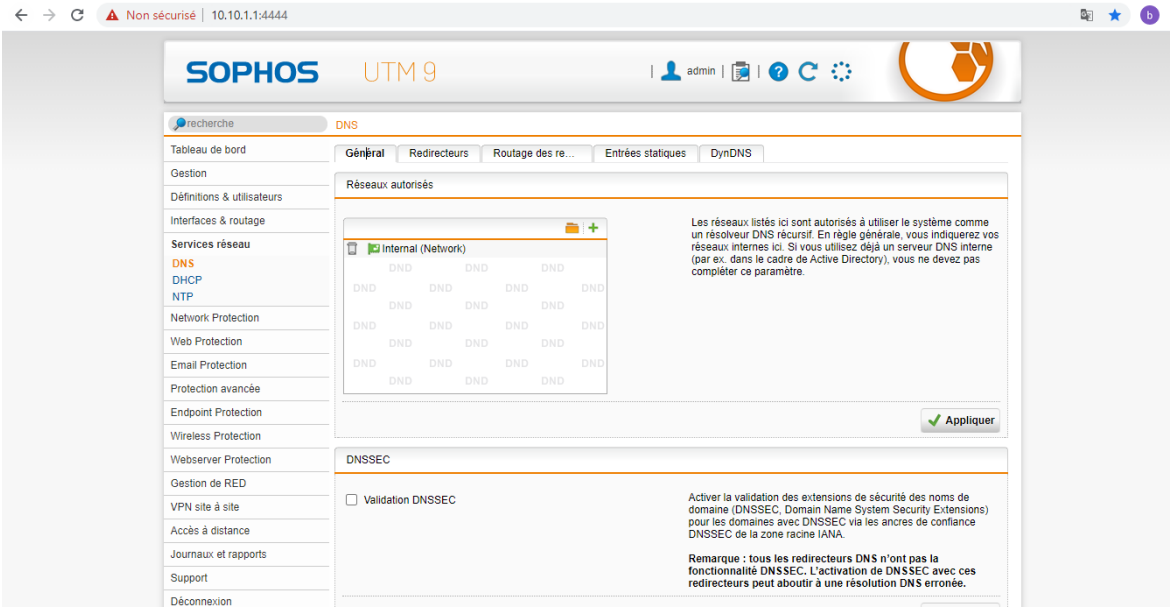

FIGURE 3.39 – Serveur DNS

3.4.8 Création des règles de parfeu

Après avoir crée l'ensemble des utilisateurs et des groupes, nous devons définir la manière dont le parfeu assure la protection des ordinateurs. On va sur Network Protection> Pare-Feu> Nouvelle régler.

Premièrement on doit choisir le réseau source de nos paquet , le service adéquat et on sélectionne l'adresse ip du réseau de destination ce qui veut dire que notre réseau est autorisé à connecter à n'importe quelle destination on utilisant les services sélectionnés. Deuxièmement on spécifie l'action à appliquer qui va être soit autorisé ,rejeté ou bien abondonner.

La figure ci-dessous montre les règles de parfeu que nous avons définis :

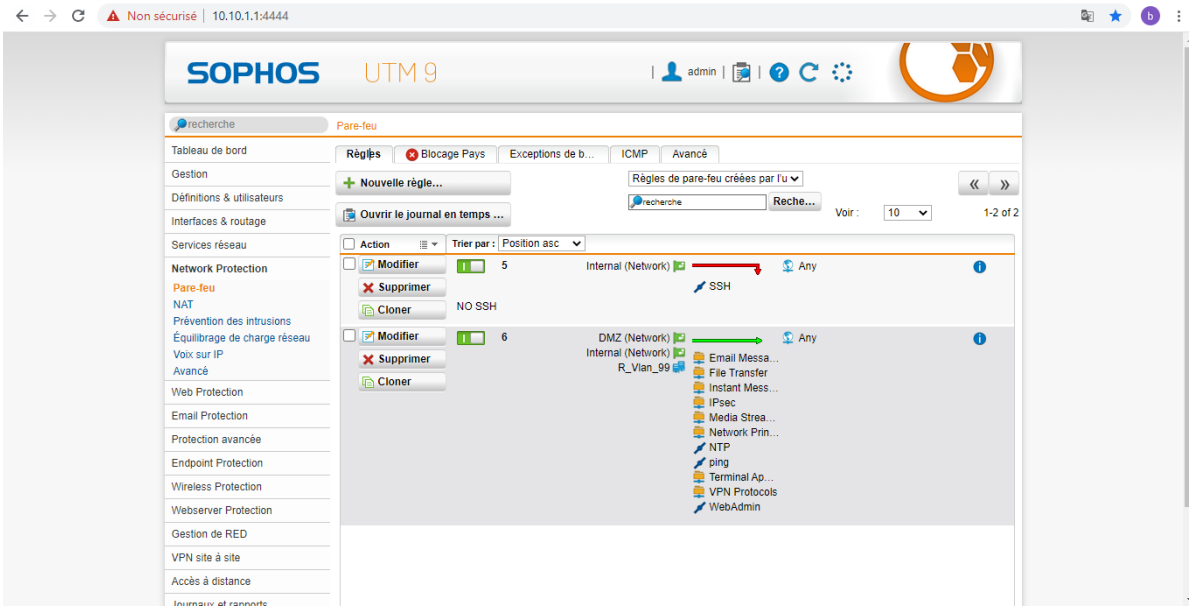

FIGURE 3.40 – les règles de parfeu

3.4.9 Le NAT et la redirection des ports

Sur le site Seddouk, On a créé deux règles fictives l'une pour le réseau local vers le WAN et l'autre pour le DMZ vers le WAN .On allons sur Network Protection > NAT > Masquerading > Nouvelle règle fictive .

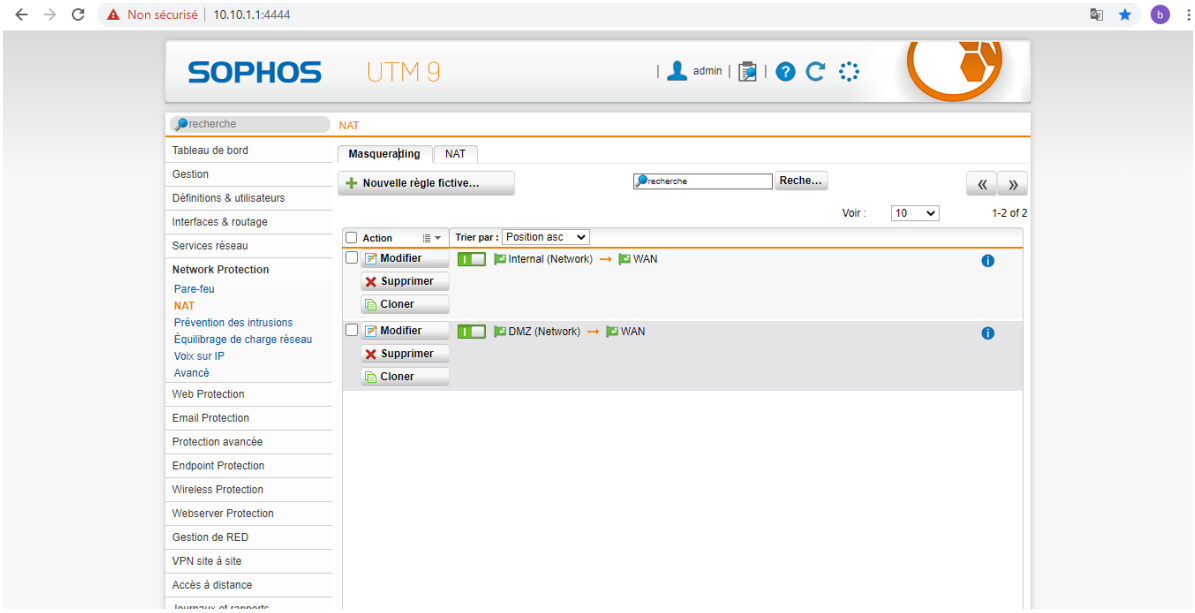

FIGURE 3.41 – Les règles NAT sur Sophos de seddouk

On allons sur Network Protection > NAT > Nouvelle règle NAT. On a créé une redirection de port vers le serveur Ecommerce pour le trafic provenant de l'internal vers le WAN à l'aide du service HTTPS-serveur Ecommerce.

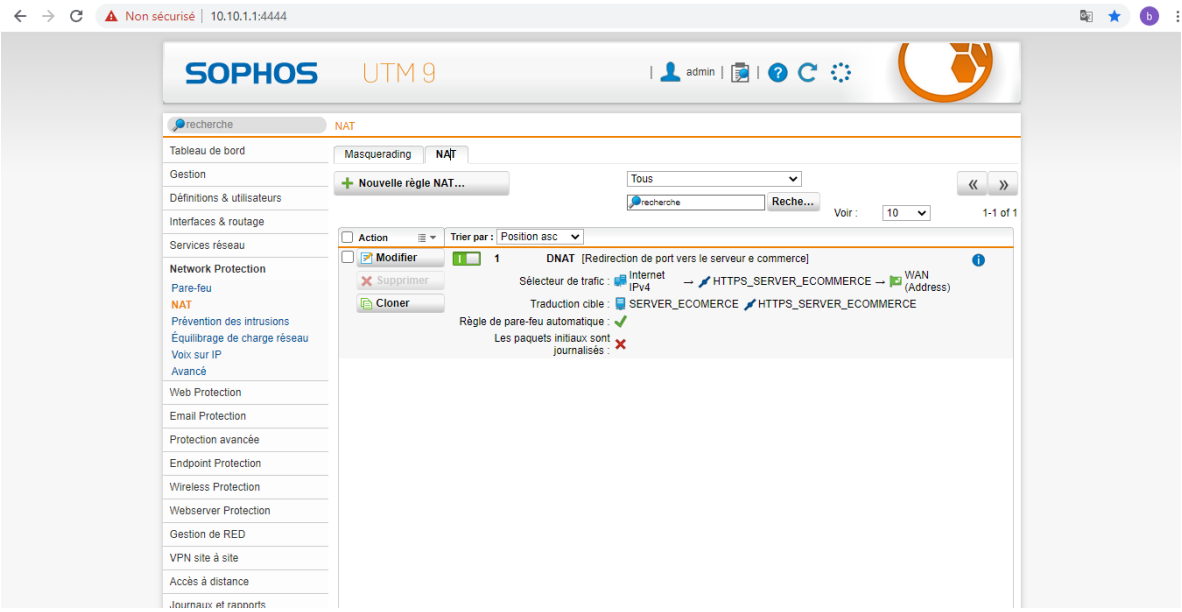

FIGURE 3.42 – La redirection des ports sur Sophos de seddouk

3.4.10 Création du portail utilisateur

Ce portail c'est une interface que seulement les utilisateurs finaux peuvent la exploité. Pour le crée on allons à Gestion –> Portail utilisateur .

D'abord on doit spécifier le réseau autorisé à accéder au portail d'utilisateur final et également limiter l'accès au portail à certains comptes utilisateur, après on sélectionne une langue par défaut pour le portail de l'utilisateur. Ensuite on télécharge le certificat sur l'un des Webserver Protection > Gestion des certificats, d'où on va désactiver certains éléments du portail toutefois Les éléments désactives ne seront pas affichés dans le portail de l'utilisateur. Enfin on spécifier un nom d'hôte de portail et un port d'écoute comme on peut modifier le message qui s'affichera sur la page d'accueil du portail.

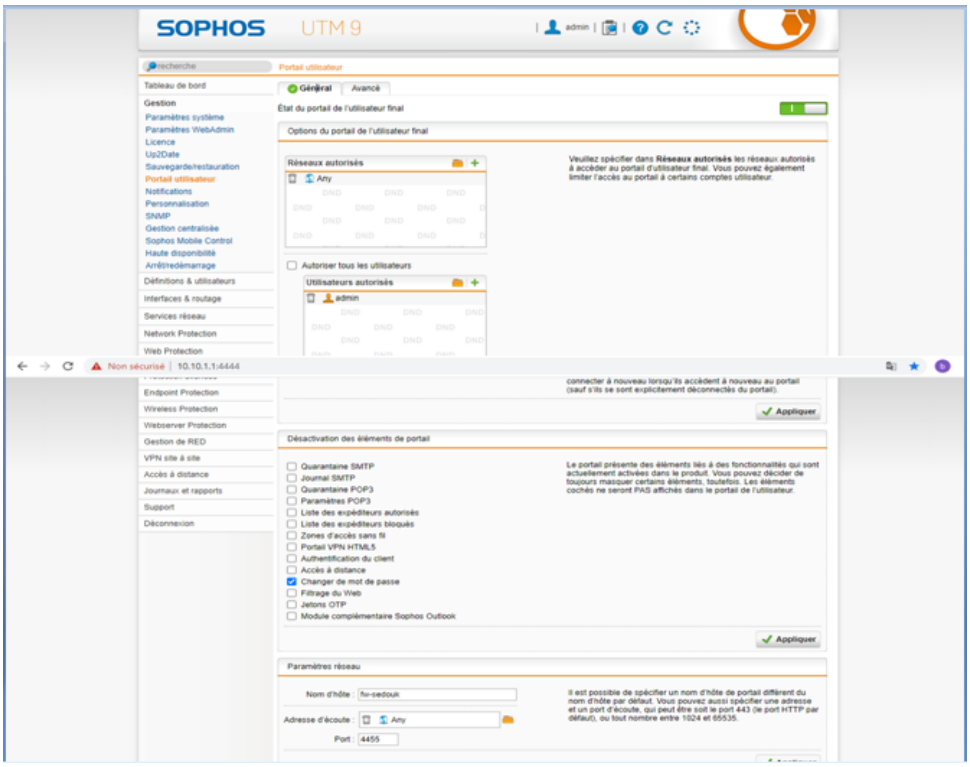

FIGURE 3.43 – Création du portail utilisateur

Maintenant, nous allons connecter au portail avec le port 4455 , une interface d'accueil s'affichera comme suit :

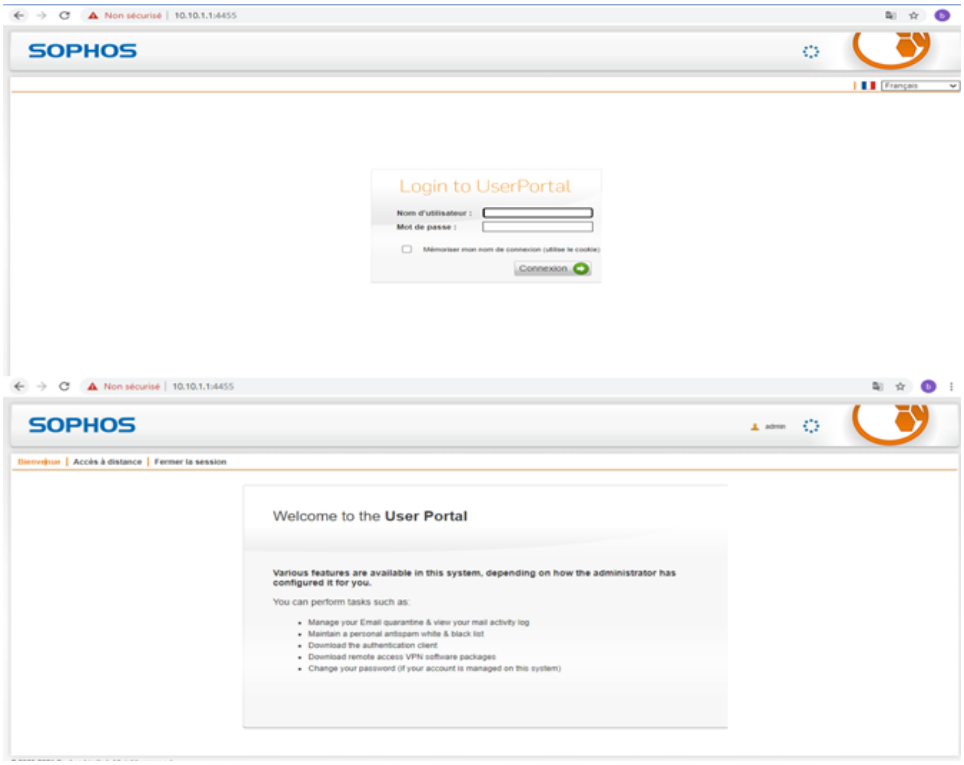

FIGURE 3.44 – portail utilisateur

3.4.11 Configuration du VPN site à site IPsec

Création de la passerelle distante

Pour creer la passerelle distante sur là qu'elle le cite d'Alger va demander la connexion auprès du site de Seddouk , d'abord faut aller au VPN cite à s-Ite-Ipsec> Passerelles distantes> nouvelle passerelle VPN , ensuite on va remplir les informations nécessaires le nom de la passerelle et son type, la clé partagée sur le tunnel entre les deux sites, type id vpn et on sélectionne le réseau distant qu'on veut atteindre .

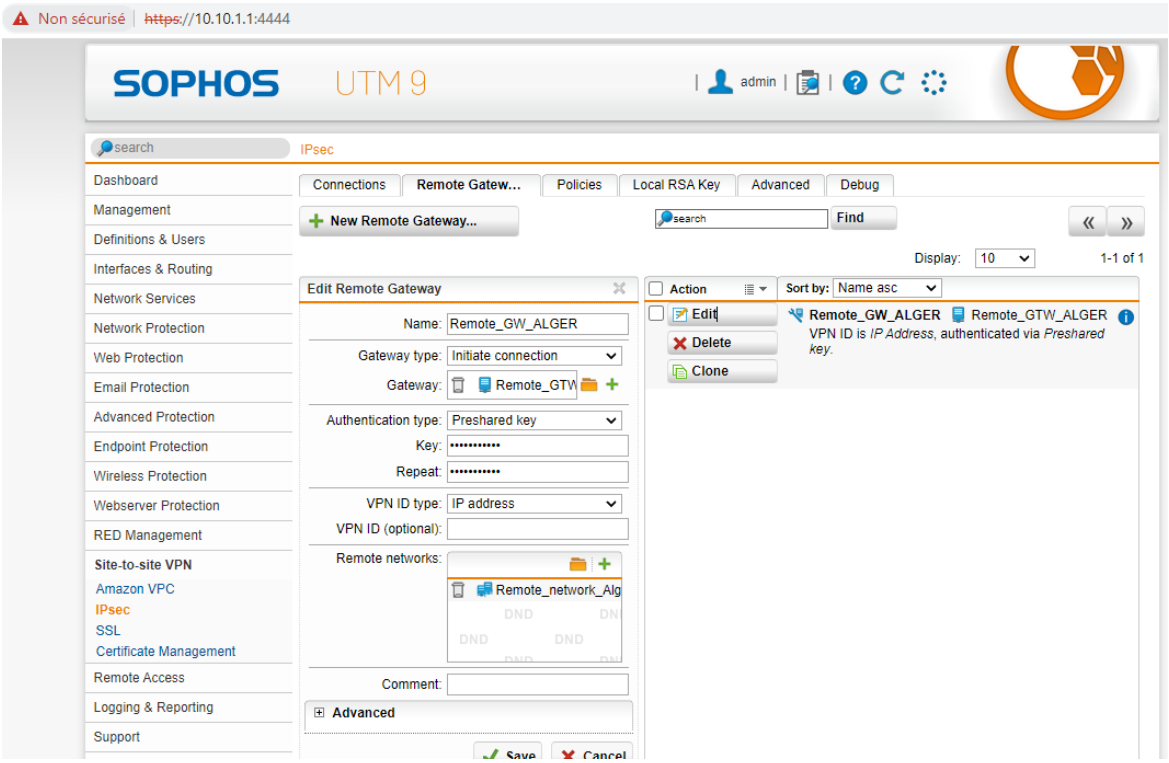

FIGURE 3.45 – La passerelle distante VPN du parfeu de Seddouk

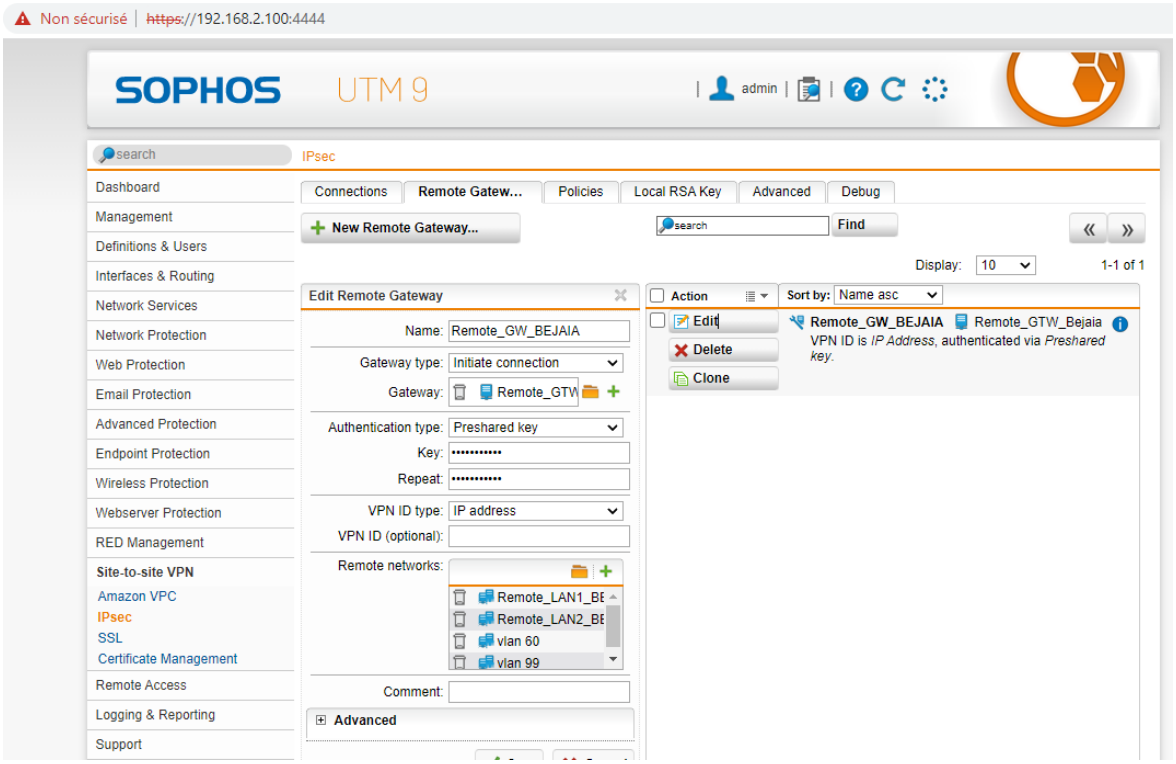

FIGURE 3.46 – La passerelle distante VPN du parfeu d'Alger

Création de connexion IPsec

Pour créer la connexion IPsec on va aller au VPN site à site –> IPsec –> Connexions –> Nouvelle connexion IPsec , d'ou on va sélectionner la passerelle distante que on vient de créer , l'interface local WAN dont laquelle on va sortir sur ce tunnel et on va sélectionner le réseau LAN local .

On crée la même chose sur le site distant (Alger) dans le sens inverse.

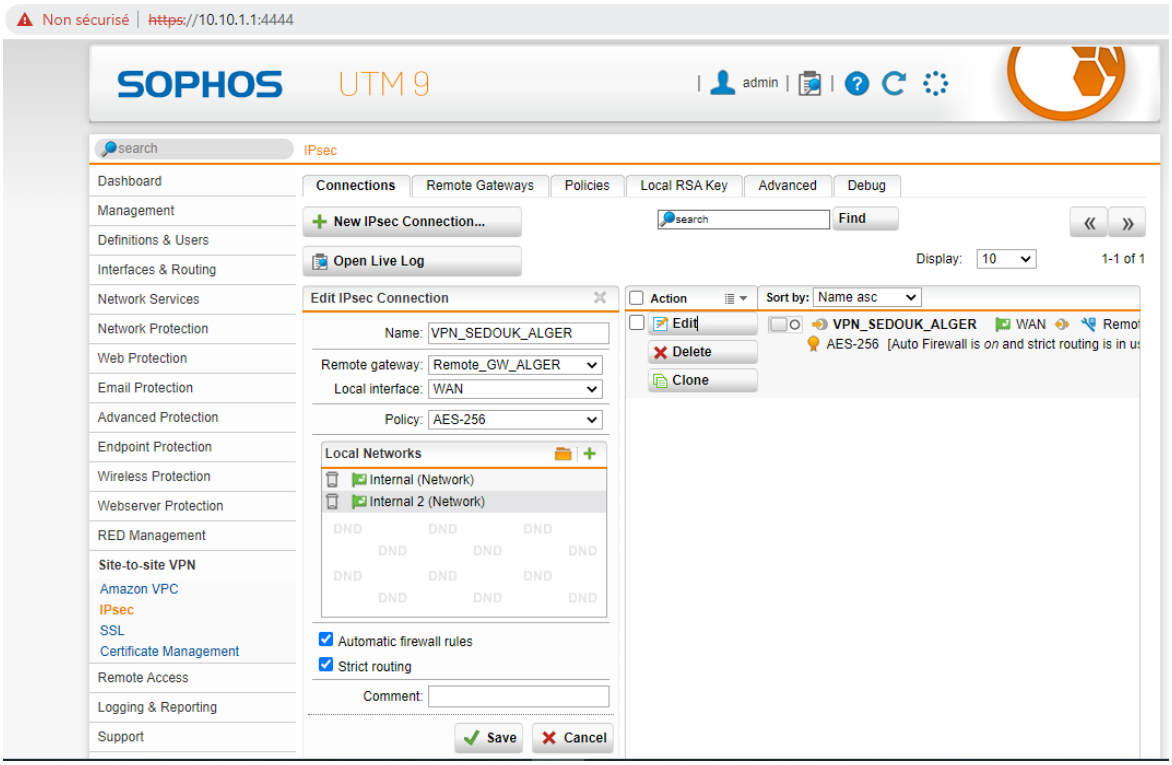

FIGURE 3.47 – La connexion IPsec du parfeu de Seddouk

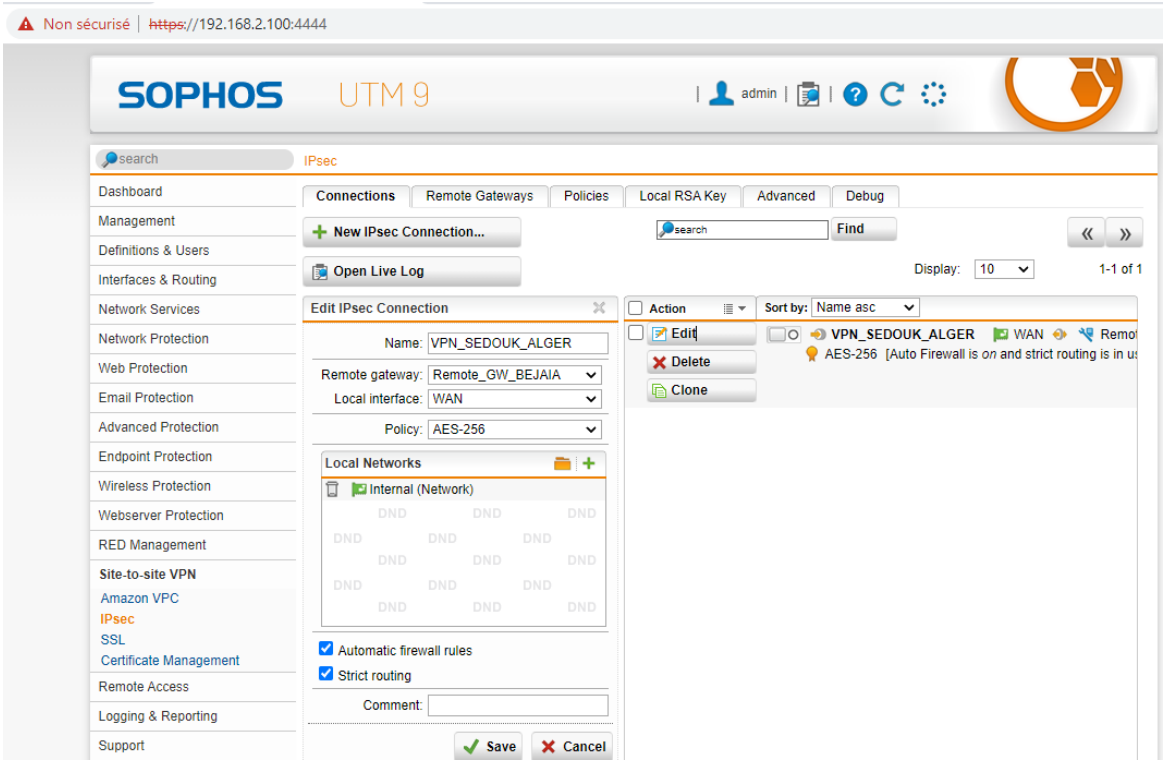

FIGURE 3.48 – La connexion IPsec du parfeu d'Alger

Pour la vérification aller à VPN site à site –> État du tunnel . Il doit être on vert.

— vert : le tunnel a été crée.

— rouge :le tunnel n'a pas été crée.

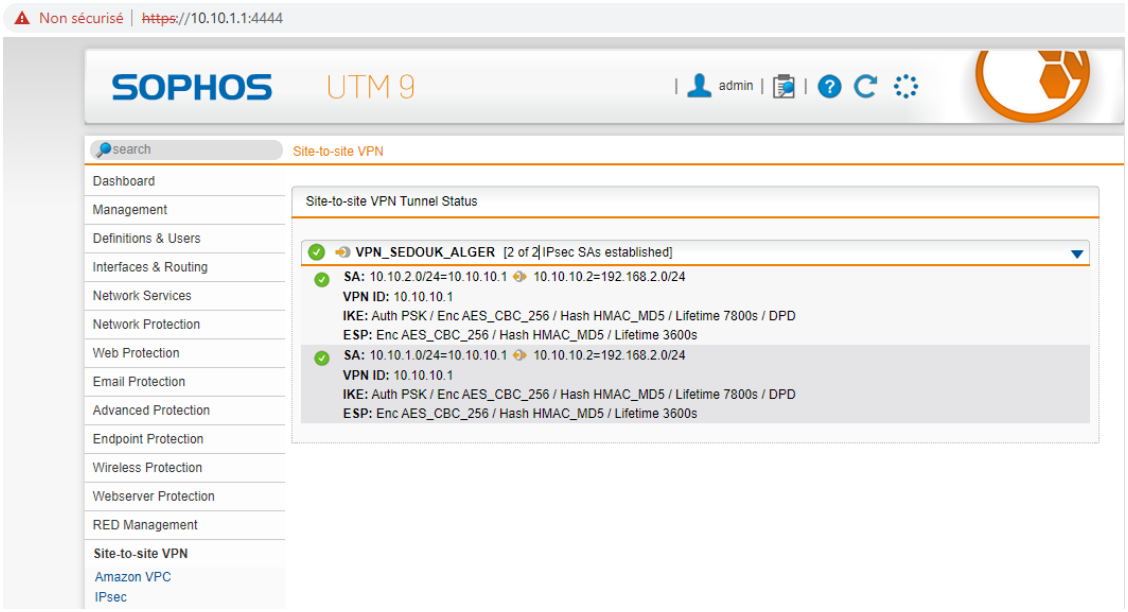

FIGURE 3.49 – Le tunnel VPN du parfeu de Seddouk

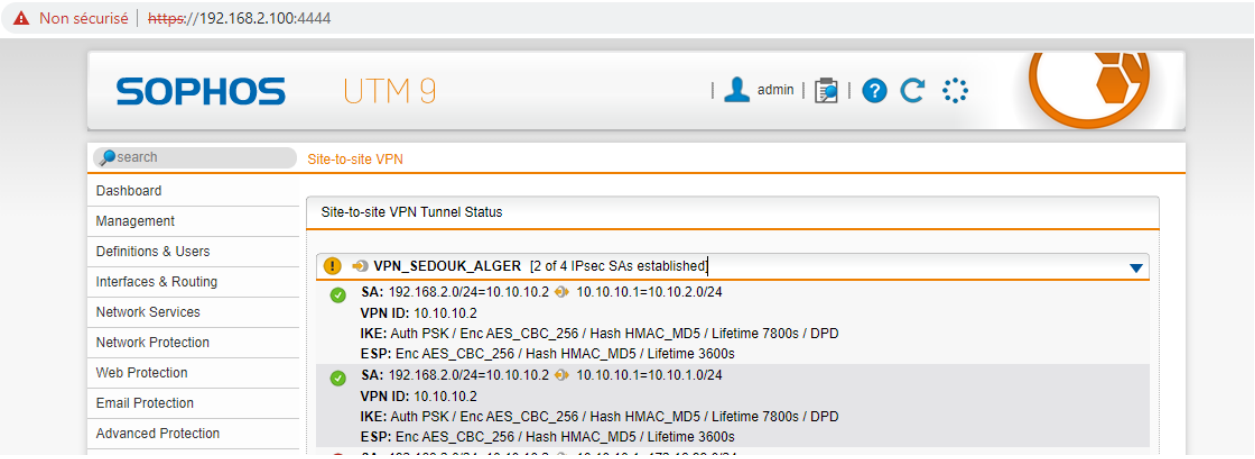

FIGURE 3.50 – Le tunnel VPN du parfeu d'Alger

3.5 Configuration du VPN client à site

Le client d' acces VPN SSL est un logiciel qui permet aux utilisateurs ambulants aux ressources locales depuis n'importe ou

Pour configurer le configurer on va aller à Accès à distance SSL –> Profils –> Nouveau –> profil d'accès distant. On va entrer le nom du profil , puis on va choisir les utilisateur ou les groupes qui vont utiliser ce profil , ensuite On sélectionne le réseau que ce profil doit avoir accée .

On va accéder au portail utilisateur, on clique sur le onglet Accès à distance , un menu VPN SSL s'affiche puis on doit télécharger le package d'installation complet comprenant le logiciel client, les clés et la configuration automatique pour Windows Vista/7/8/10.

Un foie l'installation du package est faite on a reçu un message qui va nous permettre d'installer la carte réeau dédier pour la convection vpn ; Donc on va sur le panneau de configuration> réseau et internet> Centre réseau et partage> Modifié les paramètres de la carte . On remarque la présence d'une seule carte réseau et un foie on installe la configuration on remarque qu'une nouvelle carte réseau virtuelle vient d'être créé.

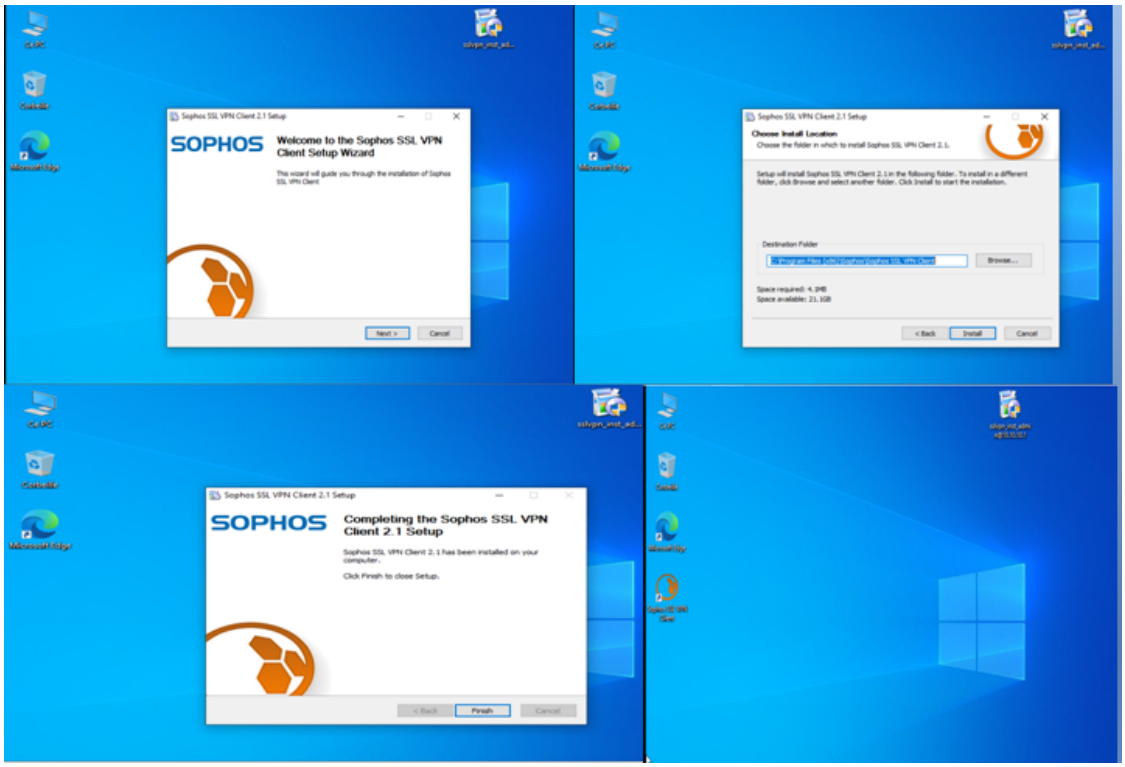

FIGURE 3.51 – Installation logicielle client

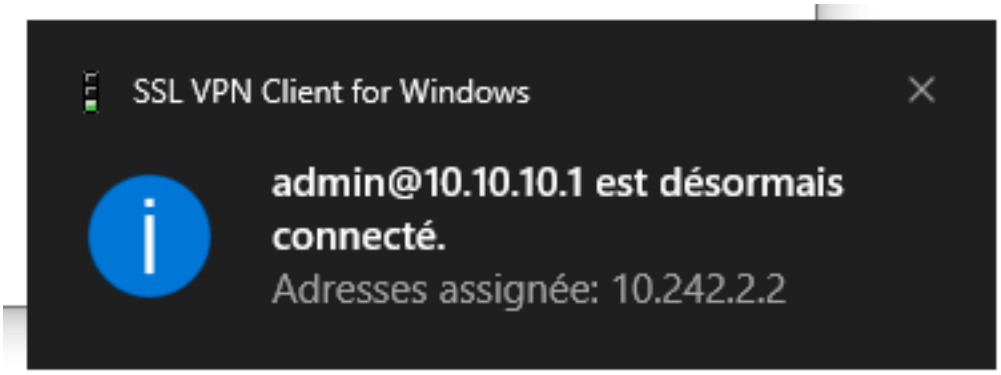

FIGURE 3.52 – Connexion réussite du client

3.6 Configuration des équipements

Dans ce qui suit, nous allons présenter la configuration en générale des équipements qui vont nous permettre de mettre en place la nouvelle architecture proposée.

3.6.1 Le plan d'adressage des VLANs

Nom de VLAN	ID VLAN	Adresse de sous réseau	passerelle de sous réseau
Service DRH	10	172.16.10.0	172.16.10.250
Service DG	20	172.16.20.0	172.16.20.250
Service BU	30	172.16.30.0	172.16.30.250
Service voice	40	172.16.40.0	172.16.40.250
Service GS	50	172.16.50.0	172.16.50.250
Service DSI	60	172.16.60.0	172.16.60.250
Service atelier	70	172.16.70.0	172.16.70.250
admin	99	172.16.99.0	172.16.99.250

TABLE 3.1 – Plan d'adressage des VLANs

3.6.2 Le plan d'adressage des PVLANs

Nom de PVLAN	ID PVLAN	Adressage	Passerelle
Serveur1-commerce	200	10.10.3.10	10.10.3.1
Serveur2-SQL	200	10.10.3.11	10.10.3.1
Serveur3-voice	201	10.10.3.12	10.10.3.1

TABLE 3.2 – Plan d'adressage des private VLAN(PVLAN)

3.6.3 L'encapsulation dot1Q sur les deux routeurs

Equipement	Interface	AdressesIP	Passerelle virtuel
Router1	e0/0.10	172.16.10.1	172.16.10.250
	0/0.20	172.16.20.1	172.16.20.250
	e0/0.30	172.16.30.1	172.16.30.250
	e0/0.40	172.16.40.1	172.16.40.250
	e0/0.50	172.16.50.1	172.16.50.250
	e0/0.60	172.16.60.1	172.16.60.250
	e0/0.70	172.16.70.1	172.16.70.250
	e0/0.99	172.16.99.1	172.16.99.250
Router2	e0/0.10	172.16.10.2	172.16.10.250
	0/0.20	172.16.20.2	172.16.20.250
	e0/0.30	172.16.30.2	172.16.30.250
	e0/0.40	172.16.40.2	172.16.40.250
	e0/0.50	172.16.50.2	172.16.50.250
	e0/0.60	172.16.60.2	172.16.60.250
	e0/0.70	172.16.70.2	172.16.70.250
	e0/0.99	172.16.99.2	172.16.99.250

TABLE 3.3 – Plan d'adressage encapsulation xdot1q pour le routeur 1 et 2

3.6.4 Le plan d'adressage des équipments

Equipement	Interface	Adressage
FW-Seddouk	DMZ	10.10.3.1
	LAN1	10.10.1.1
	LAN2	10.10.2.1
	WAN	10.10.10.1
FW-ALGER	LAN3	192.168.2.100
	WAN	10.10.10.2
R1	e0/0	encapsulation dot1Q
	e0/1	10.10.1.2
R2	e0/0	encapsulation dot1q
	e0/1	10.10.2.2
DMZ-SW	e0/1	10.10.3.10
	e0/2	10.10.3.11
	e0/3	10.10.3.12
SWD1	e0/0-3	172.16.0.0
	e1/0-3	
	e2/0-3	
	e3/0-3	
SWD2	e0/0-3	172.16.0.0
	e1/0-3	
	e2/0-3	
	e3/0-3	
SWA1	e3/1	172.16.70.0
	e3/2	172.16.60.0
	e3/3	172.16.99.0
SWA2	e1/2	172.16.50.0
SWA3	e0/2	172.16.40.0
	e0/3	172.16.30.0
SWA4	e3/2	172.16.20.0
	e3/3	172.16.10.0

TABLE 3.4 – Plan d'adressage des équipements

3.6.5 Configuration des commutateurs

Nous commençons par la configuration des commutateurs qui permettent l'interconnexion des différents réseaux hétérogènes.

Configuration des interfaces trunk

Un trunk est une liaison d'agrégation de VLANs. C'est une connexion physique sur lequel on transmet le trafic de plusieurs VLANs. Pour configurer les interfaces trunk entre deux switchs on suit les étapes suivantes.

Vu le nombre d'interface à configurer on utilisera la même configuration.

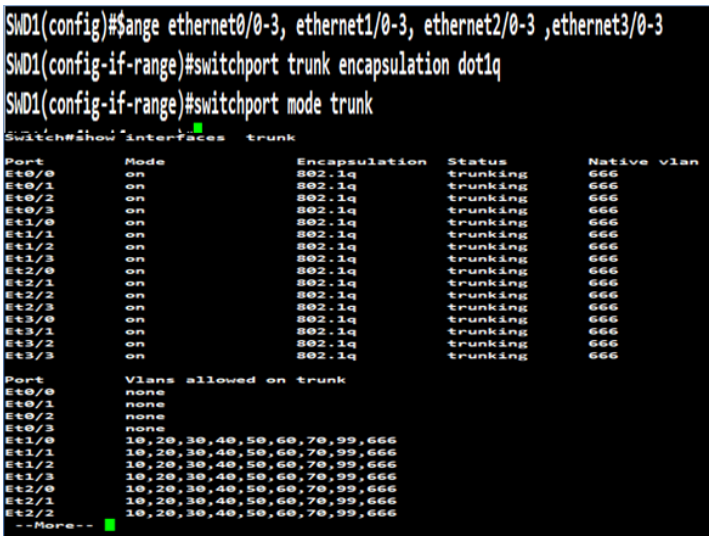

FIGURE 3.53 – Configuration trunk sur le switch distribution SWD1 et vérification

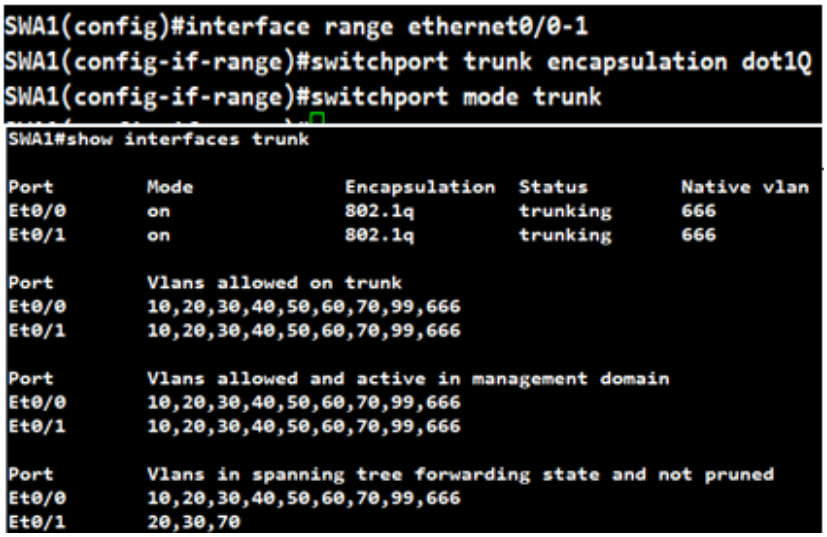

FIGURE 3.54 – Configuration trunk sur le switch access SWA1 et vérification

Configuration d'un domaine VTP

VTP permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau.

On a configuré le VTP server sur le switch distribution et le VTP client sur le switch access.

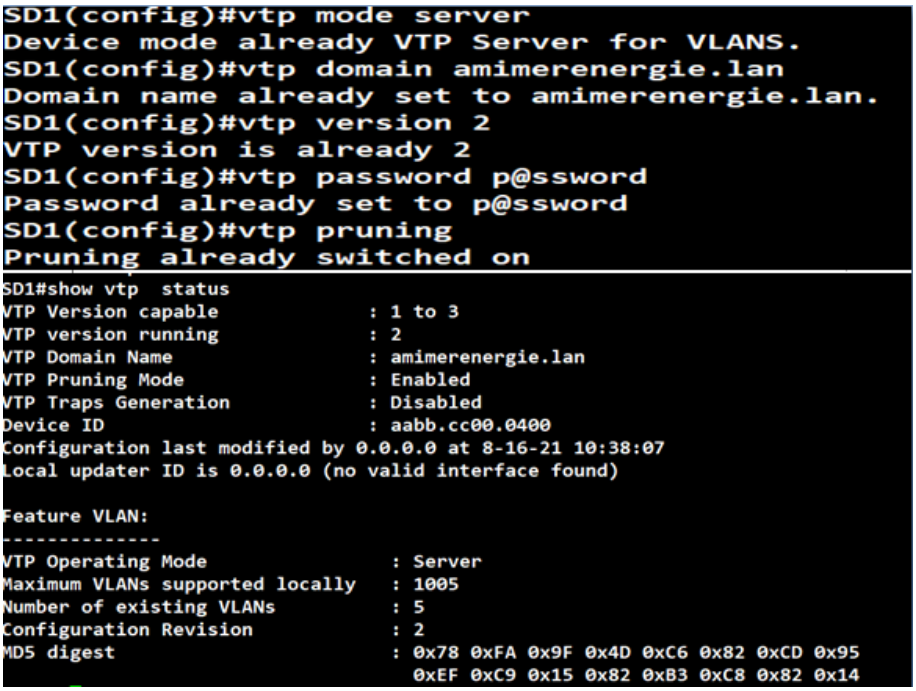

FIGURE 3.55 – Configuration VTP serveur sur le switch distribution SWD1 et vérification

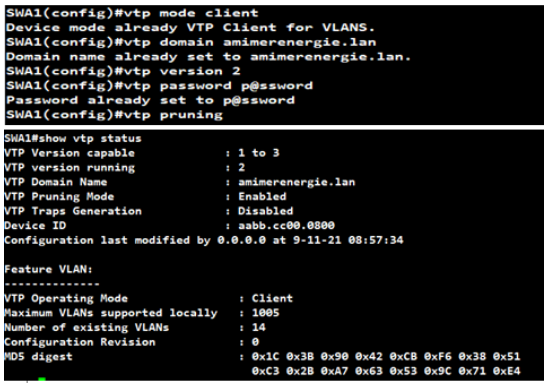

FIGURE 3.56 – Configuration VTP client sur le switch access SWA1 et vérification

Création des VLANs

La création des VLANs permet de regrouper d'une part les périphériques et d'autre part les utilisateurs et de gérer individuellement les droites et priorités d'accès des utilisateurs .

Dans notre cas on a créé six VLANs chaque un est associé à son service de plus on a créé le VLAN voix, le VLAN native et VLAN management.

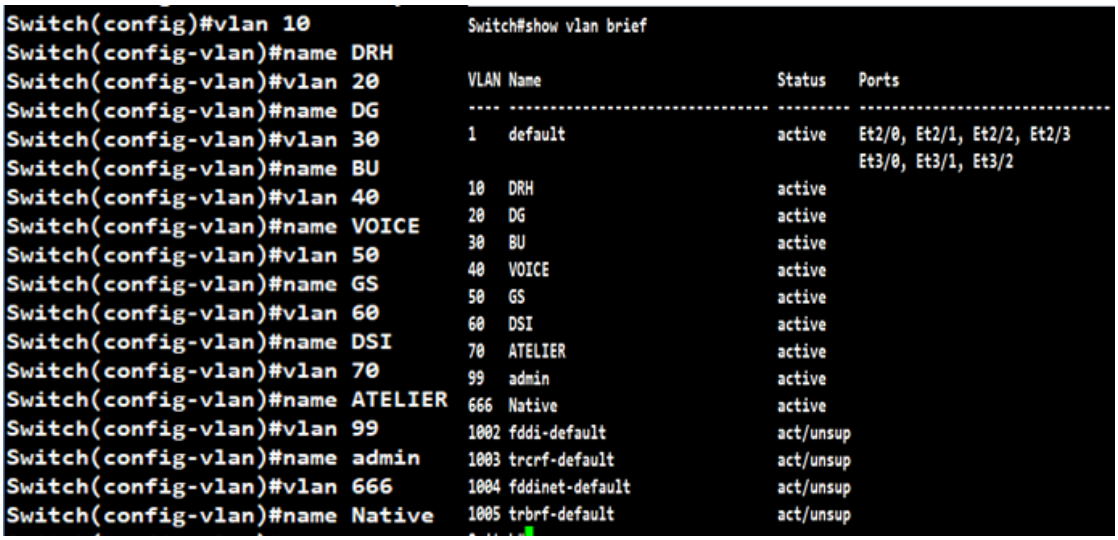

FIGURE 3.57 – Création des VLANs sur le switch SWD1 et vérification

Configuration des interfaces Access

Passons maintenant à la configuration des interfaces Access qui veut dire qu'elle recevera que les paquets qui lui sont destinés.

On utilisera la même configuration pour les autres interfaces Access.

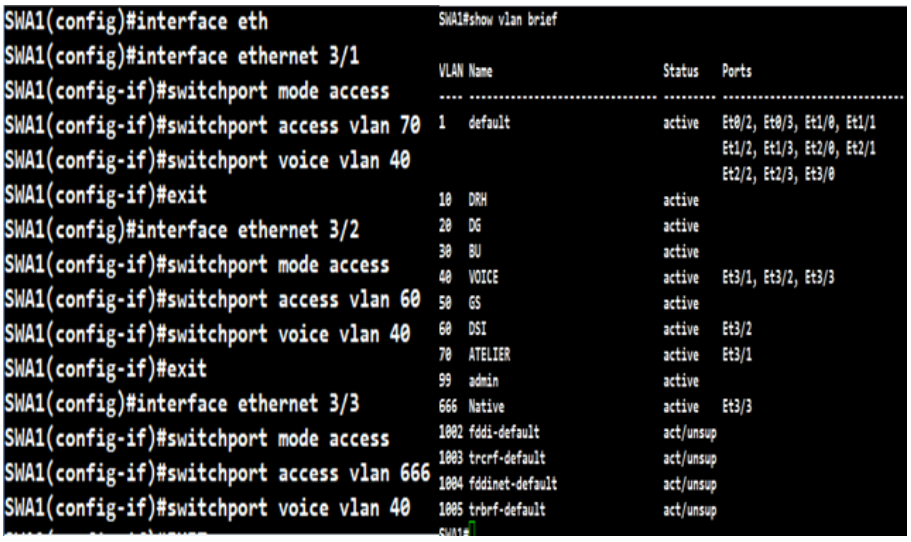

FIGURE 3.58 – Configuration Access sur le switch Access SWA1 et vérification

Configuration VLAN native

Toutes les trames passant par un "Trunks" sont ainsi étiquetées sauf les trames appartenant au VLAN natif. Donc, les trames du VLAN natif, par défaut le VLAN 1, ne sont pas étiquetées.

Donc on a changé la valeur du VLAN natif de 1 à 666 et on a forcé le tagging sur ce VLAN. Pour que ne pas véhiculer des trames de protocoles comme CDP, DTP dans le même VLAN et d'éviter qu'un utilisateur ne puisse capturer ce trafic ou de gérer des faux messages CDP, DTP afin de détourner le fonctionnement du réseau.

On a fait la même configuration pour tous les switchs.

```
SWD1(config)#interface range eth0/0-3 , eth1/0-3 , eth 2/0-3 , eth 3/0-2
SWD1(config-if-range)#switchport trunk native vlan 666
SWD1(config-if-range)#$trunk allowed vlan 10,20,30,40,50,60,70,99,666
SWD1(config-if-range)#
SWD1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et1/0       on               802.1q         trunking      666
Et1/1       on               802.1q         trunking      666
Et1/2       on               802.1q         trunking      666
Et1/3       on               802.1q         trunking      666
Et2/0       on               802.1q         trunking      666
Et2/1       on               802.1q         trunking      666
Et2/2       on               802.1q         trunking      666
Et2/3       on               802.1q         trunking      666
Et3/0       on               802.1q         trunking      666
Et3/1       on               802.1q         trunking      666
Et3/2       on               802.1q         trunking      666
Et3/3       on               802.1q         trunking      1
Po1         on               802.1q         trunking      666

Port        Vlans allowed on trunk
Et1/0       10,20,30,40,50,60,70,99,666
Et1/1       10,20,30,40,50,60,70,99,666
Et1/2       10,20,30,40,50,60,70,99,666
Et1/3       10,20,30,40,50,60,70,99,666
Et2/0       10,20,30,40,50,60,70,99,666
Et2/1       10,20,30,40,50,60,70,99,666
 --More--
```

FIGURE 3.59 – Sécurisation du VLAN native sur switch distrubution SWD1 et vérification

```
SWA1(config)#interface range ethernet 0/0-1
SWA1(config-if-range)#switchport trunk  native vlan  666
SWA1(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,60,70,99,666
SWA1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      666
Et0/1       on               802.1q         trunking      666

Port        Vlans allowed on trunk
Et0/0       10,20,30,40,50,60,70,99,666
Et0/1       10,20,30,40,50,60,70,99,666

Port        Vlans allowed and active in management domain
Et0/0       10,20,30,40,50,60,70,99,666
Et0/1       10,20,30,40,50,60,70,99,666

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       10,20,30,40,50,60,70,99,666
Et0/1       20,30,70
```

FIGURE 3.60 – Sécurisation du VLAN native sur le switch access SWA1 et vérification

Configuration des ports EtherChannel

Pour configurer un port channel sur notre switch nous devons assigner toutes les interfaces qui vont composer notre lien logique dans le même channel-group.

On a crée quatre liens logiques entre les deux switchs de distribution et on a configuré EtherChannel en mode active sur le switch distribution 1 et en mode passive sur le switch distribution 2.

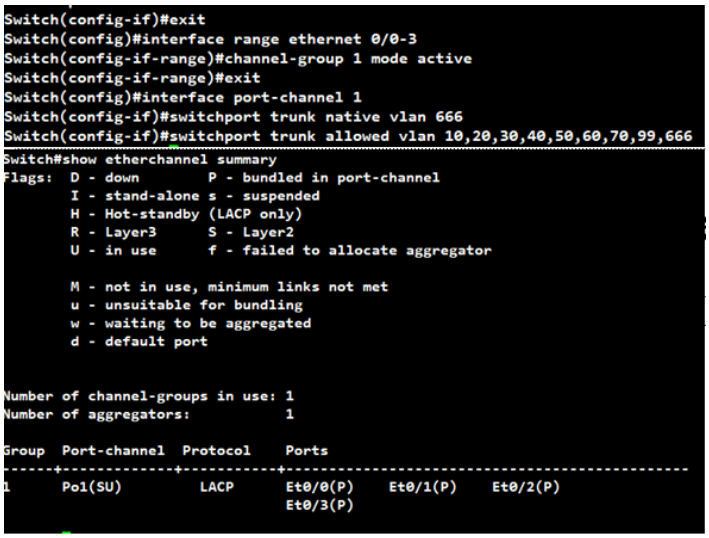

FIGURE 3.61 – Configuration EtherChannel sur le switch distribution SWD1 et vérification

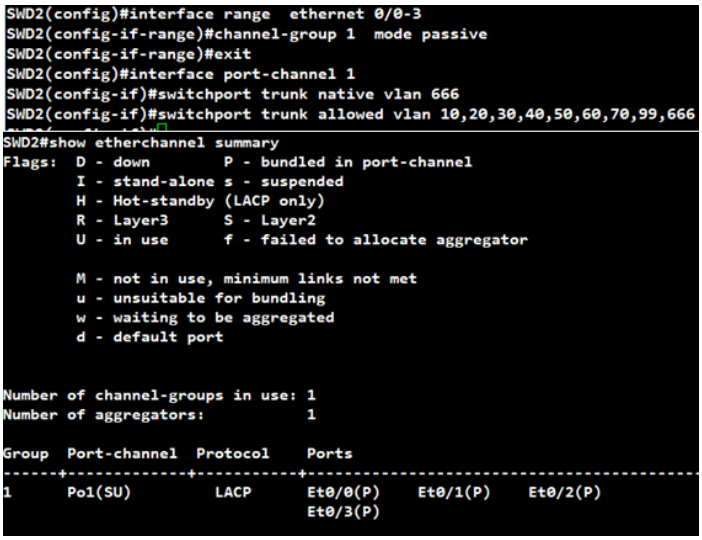

FIGURE 3.62 – Configuration EtherChannel sur le switch access SWD2 et vérification

Port security

On a sécurisé tous les ports access car la sécurité se fait sur les ports qui font face à des clients et afin de limiter le nombre d'adresses MAC dernière un port et de se protéger du MAC Address Flooding qui consiste à envoyer des milliers de messages en indiquant à chaque fois une adresse MAC source différente.

Tout d'abord, le port doit être en mode Access, ensuite activer la sécurité de port et limiter le nombre d'adresses MAC par port .Pour la gestion d'adresse Mac on a appliqué le mode sticky pour que le switch apprend automatiquement les adresses et les enregistrer . En cas où ya une violation sur le port on a appliqué le mode shutdown pour que le port se désactive automatiquement.

On utilisera la même configuration pour les autres ports Access .

```
SWA1(config)#interface ethernet 3/3
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport port-security
SWA1(config-if)#switchport port-security maximum 3
SWA1(config-if)#switchport port-security mac-address sticky
SWA1(config-if)#exit
SWA1(config)#interface ethernet 3/1
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport port-security
SWA1(config-if)#switchport port-security maximum 2
SWA1(config-if)#switchport port-security mac-address sticky
SWA1(config-if)#exit
SWA1(config)#interface ethernet 3/2
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport port-security
SWA1(config-if)#switchport port-security maximum 1
SWA1(config-if)#switchport port-security mac-address sticky
```

FIGURE 3.63 – Configuration des port security sur le switch access SWA1

Spanning three

On a configuré spinning three sur les ports access pour que les ports répondent rapidement et y aura pas de bug et on a activé la BPDU pour bloquer SNMTP sur les clients.

On utilisera la même configuration pour les autres ports Access.

```
SWA1(config)#interface range ethernet 3/1-3
SWA1(config-if-range)#switchport mode access
SWA1(config-if-range)#spanning-tree bpduguard enable
SWA1(config-if-range)#spanning-tree portfast
SWA1#show port-security interface ethernet 3/2
Port Security               : Enabled
Port Status                 : Secure-shutdown
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 1
Configured MAC Addresses    : 1
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 0050.56c0.000f:60
Security Violation Count    : 1
```

FIGURE 3.64 – Configuration spanning three sur le switch access SWA1 et vérification

Le commutateur Root sera le point central de l'arbre STP. Le choix de celui-ci dans l'architecture du réseau peut avoir son importance. Par défaut, le commutateur qui aura l'identifiant "bridge ID" (BID) le plus faible sera élu Root.

Idéalement, le choix de la route se fait dans la couche distribution. D'où On a désigné pour chaque commutateur de distribution root principal (root primary) qui est sur le VLAN 99 et son backup (root secondary) qui sur e VLAN 10.

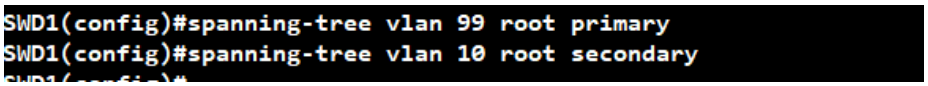

FIGURE 3.65 – Configuration root primary et secondary sur le switch distrubution SWD1

DHCP snooping

a configuré DHCP snooping affin Choisir les ports de confiances derrière lesquels un DHCP est placé . En effet, si un attaquant met en place un DHCP, cela peut créer des erreurs sur le réseau. Pire encore, l'attaquant pourrait contrôler le trafic sur le réseau. Ici, le DHCP Snooping ne sera effectué que sur le VLAN 99 .

On a utilisé la même configuration sur tous les switchs .

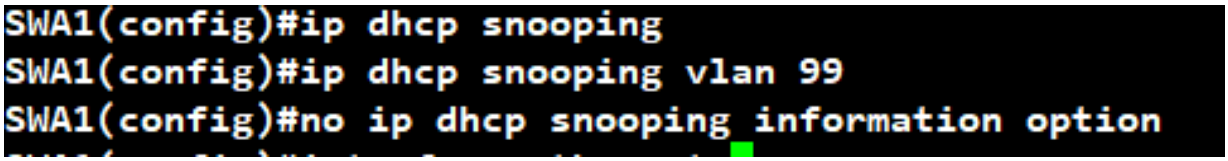

FIGURE 3.66 – Configuration DHCP snooping sur le switch access SWA1

VLANs ACLs

On a appliqué les Access Liste (ACL) sur des VLAN pour filtrer le trafic au sein d'un même VLAN. Dans notre cas à l'aide d'une VACL sur le switch access2 on a empêché les PC de s'envoyer des Ping sur le même VLAN 50.

D'abord, on a créé une ACL qui capte le trafic voulu .Ensuite, on a créé la VACL, ON on a fait la référence à l'ACL 100, qui capte le trafic ICMP voulu on choisit l'action à effectuer. Au final seul les messages ICMP sont filtrés.

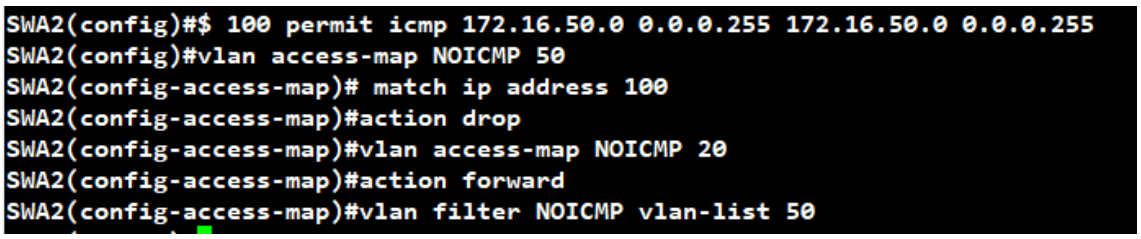

FIGURE 3.67 – Création du VACL sur le switch access SWA2

Configuration Radius

On a configuré radius sur le client switch access 2 afin d'authentifier les utilisateurs sur ce switch .D'abors on a creé un nouveau modèle aaa, apre on a créé l'ensemble aaa authentification et l'ensemble aaa autorisation à la fin on a utilisé une clé partagée AMIMER avec le serveur.

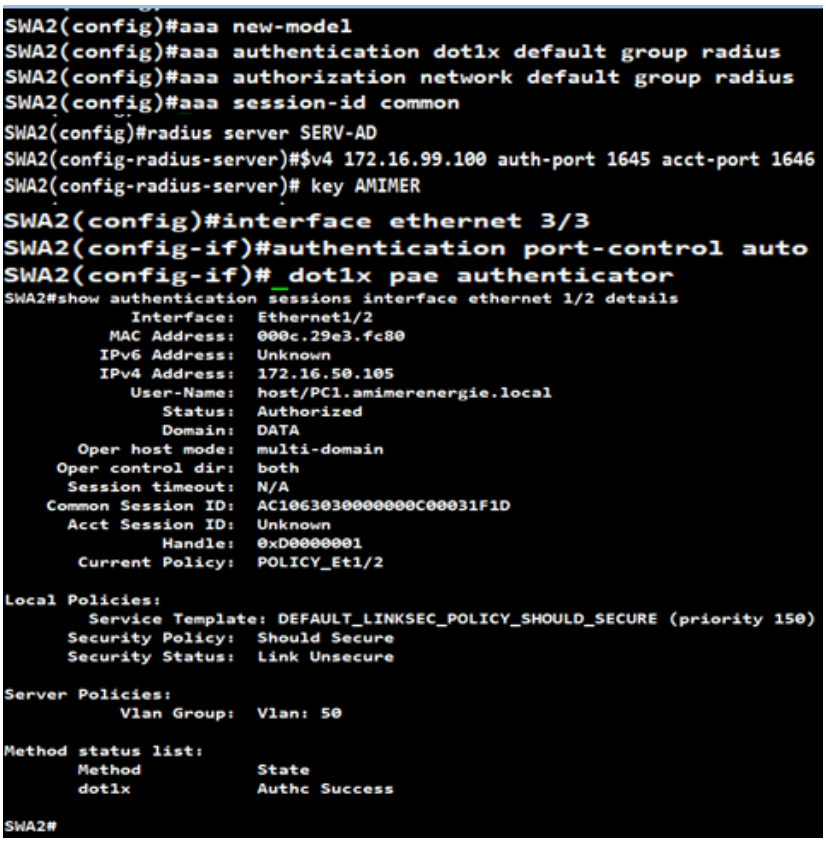

FIGURE 3.68 – Radius sur le switch access SWA2 et vérification

Configuration des VLANs privées

On a configuré les privates VLANs dans la zone DMZ afin de réduire le nombre de VLANs et filtrer les serveurs . Dans un seul réseau on a créé des différents VLANs de sorte que y aura des VLANs qui peuvent se discuter entre et d'autres non c'est le cas typique de le DMZ.

Premièrement on a configuré le VTP sur le switch-DMZ en mode transparent pour que le switch ne participe pas au processus VTP.

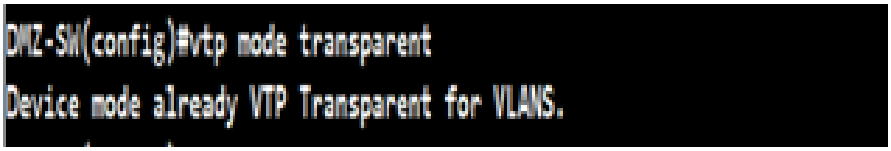

FIGURE 3.69 – Configuration VTP en mode transparent sur le switch DMZ et vérification

On a créé deux PVLANs du type Community chaque un est associée à son serveur, ces deux serveurs seront donc capables de communiquer entre eux.

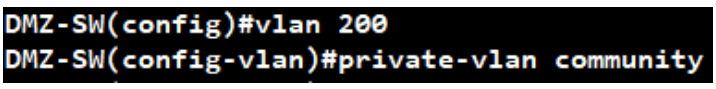

FIGURE 3.70 – Création PVLANs community sur le switch DMZ

on a créé un PVLAN de type isolated sur lequel le serveur ne pourra donc pas communiquer avec les autres serveurs.

```
DMZ-SW(config-vlan)#vlan 201
DMZ-SW(config-vlan)#private-vlan isolated
```

FIGURE 3.71 – Création PVLAN isolated sur le switch DMZ et vérification

on a créé un PVLAN du type primary sur lequel il sera capable de communiquer avec tous les PVLANs et les a englobé.

```
DMZ-SW(config-vlan)#vlan 203
DMZ-SW(config-vlan)#private-vlan primary
DMZ-SW(config-vlan)#private-vlan association 200,201
```

FIGURE 3.72 – Création PVLAN primary sur le switch DMZ

Après, on a associé chacun PVLAN à son port .Pour le PVLAN primary est connecté au port du type promiscuous et pour les PVLANs community et isolated sont connectés au port de type host.

```
DMZ-SW(config)#interface ethernet0/3
DMZ-SW(config-if)#switchport mode private-vlan host
DMZ-SW(config-if)#switchport private-vlan host-association 203 200
*Aug 24 14:28:47.924: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
DMZ-SW(config-if)#switchport private-vlan host-association 203 201
```

```
DMZ-SW(config)#interface ethernet0/2
DMZ-SW(config-if)#switchport mode private-vlan host
DMZ-SW(config-if)#
*Aug 24 14:28:04.269: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to down
DMZ-SW(config-if)#switchport private-vlan host-association 203 200
DMZ-SW(config-if)#exit
```

```
DMZ-SW(config)#interface ethernet0/1
DMZ-SW(config-if)#switchport mode private-vlan host
DMZ-SW(config-if)#switch
*Aug 24 14:26:41.603: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down
DMZ-SW(config-if)#switchport private-vlan host-association 203 200
```

```
DMZ-SW(config)#interface ethernet0/0
DMZ-SW(config-if)#switchport mode private-vlan promiscuous
DMZ-SW(config-if)#switchport  private-vlan mapping 203 200,201
```

FIGURE 3.73 – Affectation des ports aux PVLANs sur le switch DMZ et vérification

3.6.6 Configuration des routeurs

Routage inter VLANs

Nous allons configurer une des interfaces réseaux du routeur, le principe est toujours le même pour chacune des interfaces réseaux.

Pour chaque sous-interface on l'a encapsulé avec le protocole 802.1q en précisant l'Id du VLAN ensuite on lui a attribué une address IP et un masque et un DHCP relay avec l'adresse du notre serveur DHCP pour s'assurer que seul le serveur DHCP qui est sur le VLAN 99 qui va attribuer les adresses IP..

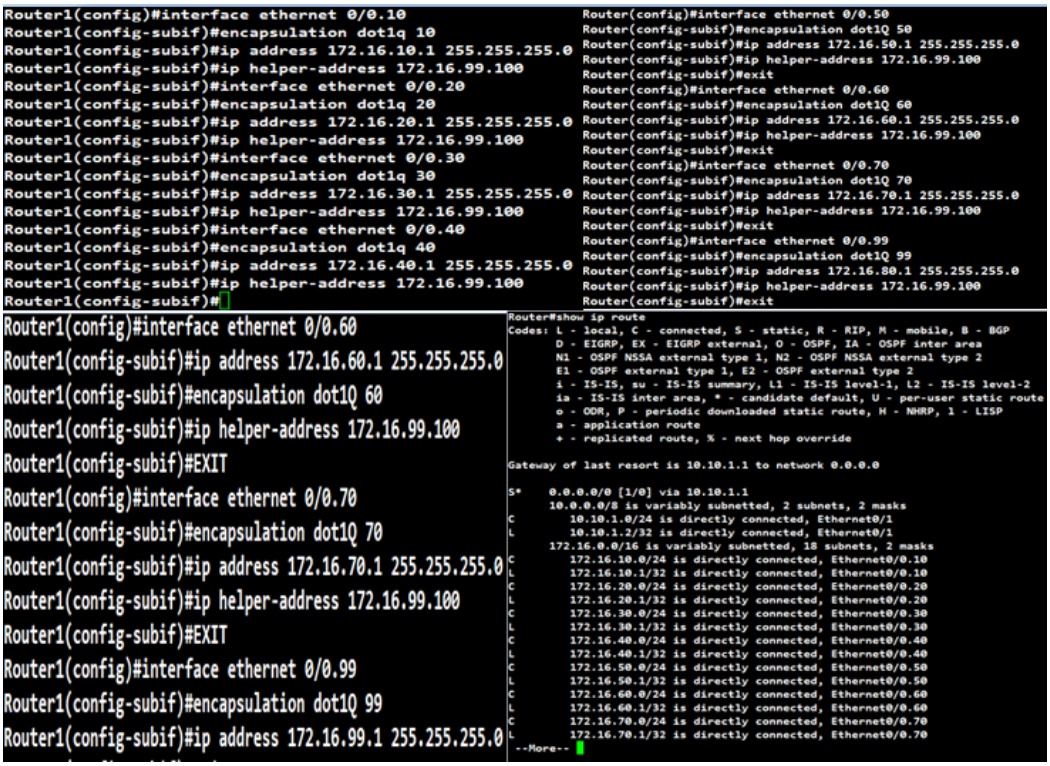

FIGURE 3.74 – Configuration des interfaces sur le routeur1 et vérification

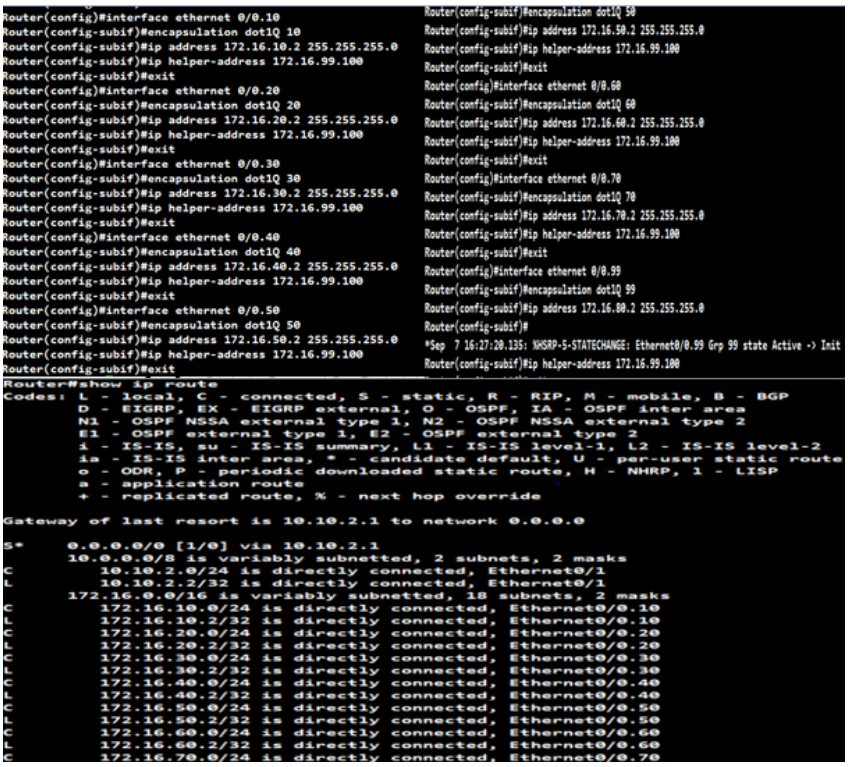

FIGURE 3.75 – Configuration des interfaces sur le routeur2 et vérification

Configuration du Routage Passerelle Par Defaut

On a routé du réseau 0.0.0.0 vers n'importe de quell réseau 0.0.0.0 par la passerelle de sortie du routeur.

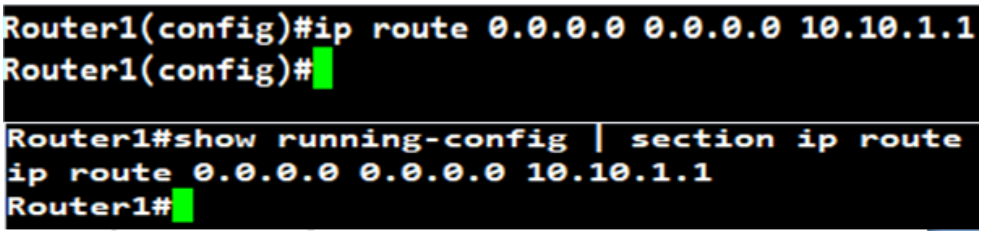

FIGURE 3.76 – Le routage sur le routeur1 et vérification

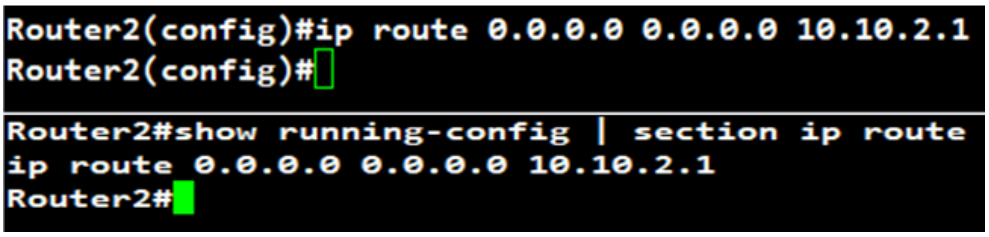

FIGURE 3.77 – Le routage sur le routeur2 et vérification

Configuration du protocole HSRP

Maintenant, on va passer à la mise en place du HSRP, sur chaque routeur on a défini une adresse IP qui sera l'IP du routeur virtuel, une priorité et un mode Actif sur le router 1 et un mode standby sur le routeur 2 de secours. Le routeur actif assure le rôle de passerelle par défaut pour le sous-réseau. S'il vient à tomber en panne, le routeur standby prendra le relai.

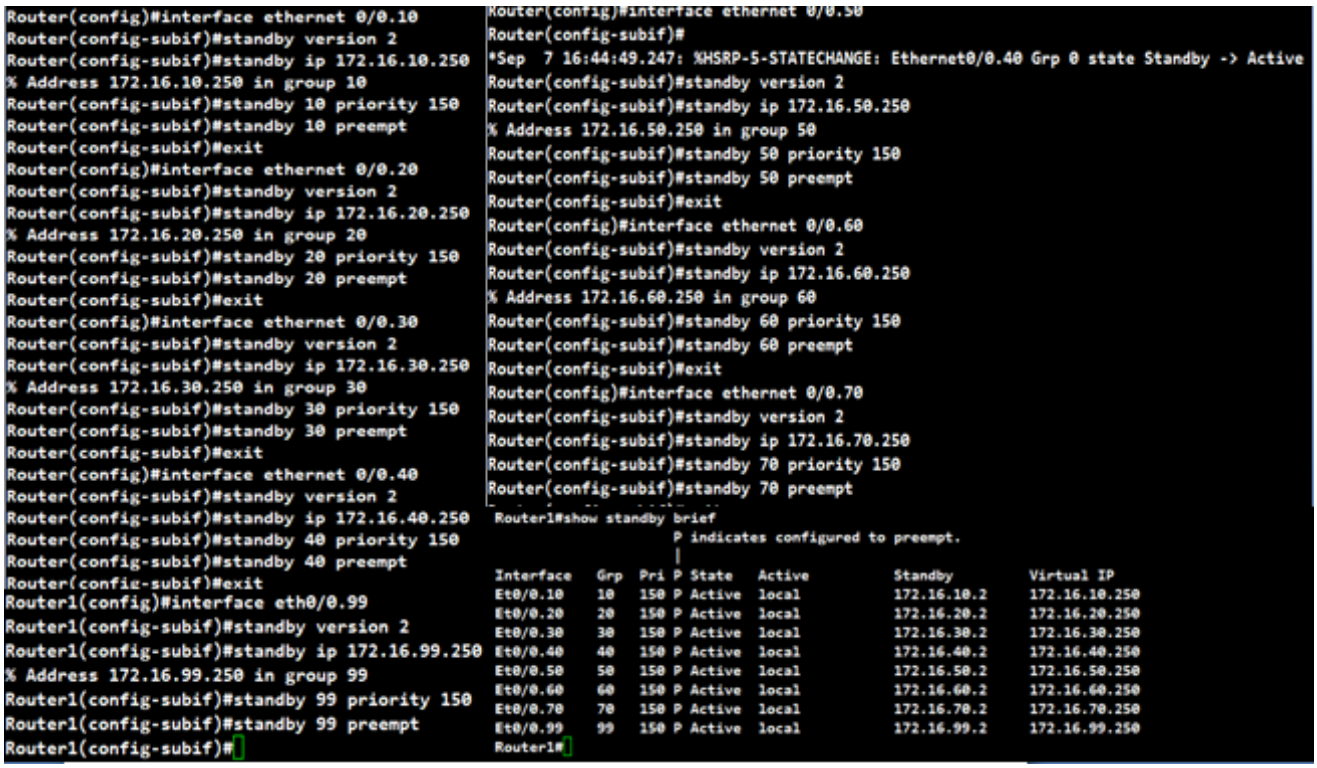

FIGURE 3.78 – Configuration de HSRP sur le routeur1 et vérification

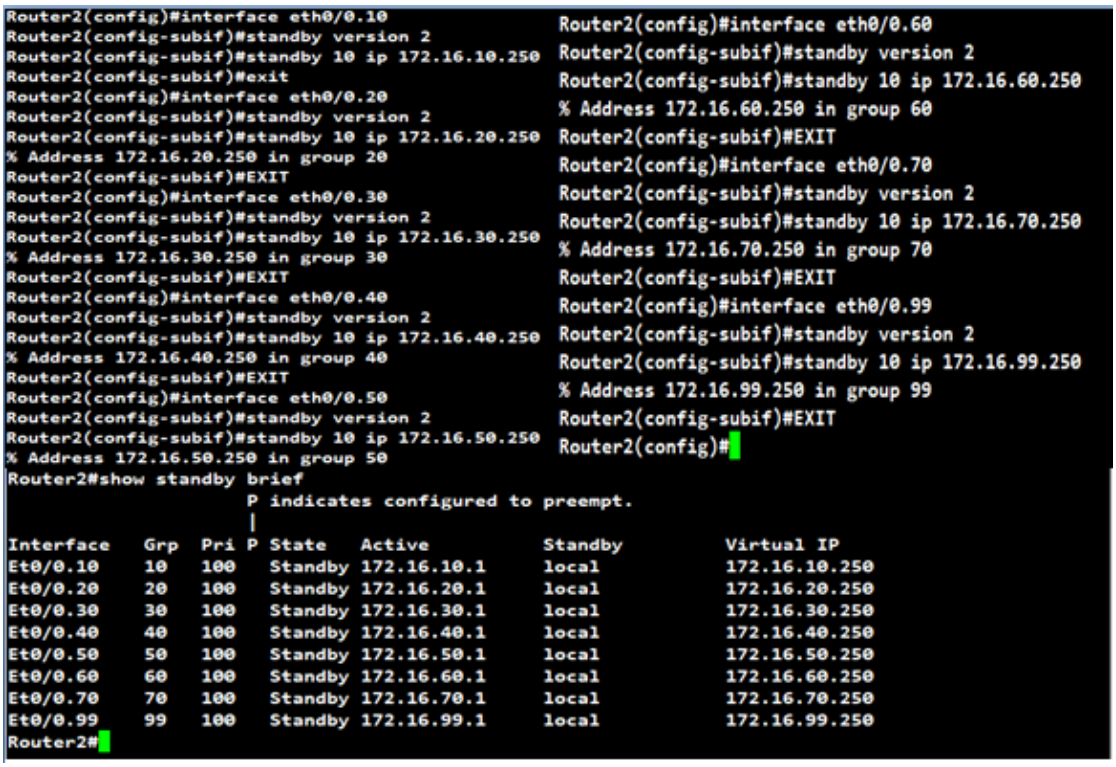

FIGURE 3.79 – Configuration de HSRP sur le routeur2 et vérification

Configuration du protocole SSH

D'abord, on a activé le SSH, après on a ajouté le compte administrateur .

FIGURE 3.80 – Configuration de SSH sur le routeur1 et vérification

SSH est maintenant activé. Nous pouvons accéder aux routeurs avec un client SSH dans notre cas par l'outil putty pour Windows.

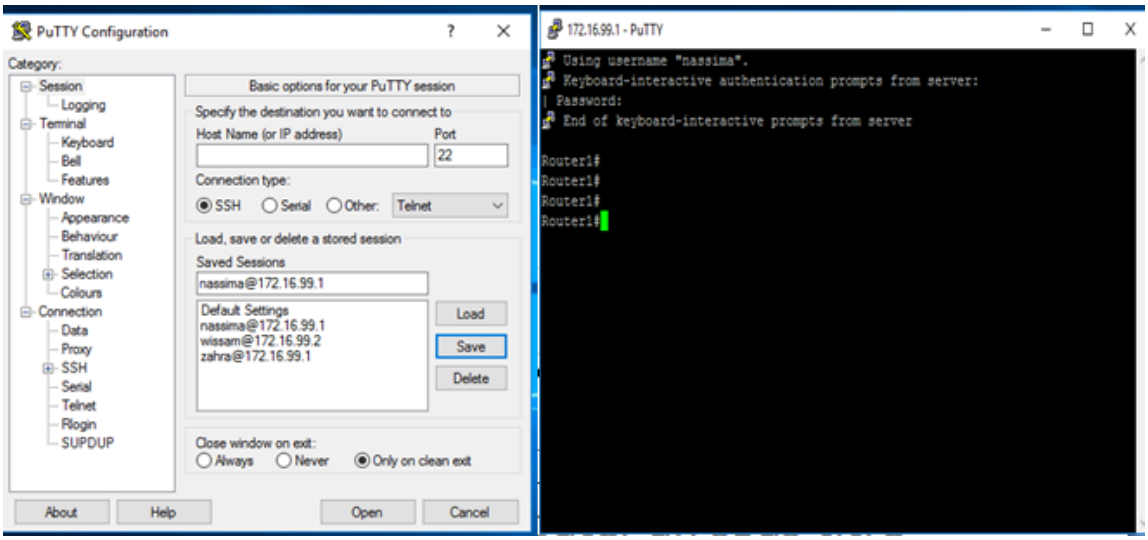

FIGURE 3.81 – Client SSH putty

3.7 conclusion

Dans ce chapitre consacré à la pratique, plus exactement à la mise en place et la sécurisation de notre architecture réseau qu'on a présenté précédemment, avec des précisions sur la configuration de chaque équipement et serveurs de l'architecture réseau qu'on a simulés avec GNS3.

Chapitre 4

Evaluations et tests

4.1 Introduction

Nous allons finaliser notre travail par des tests aux configurations déjà faites et qui sont présenté dans le chapitre précédent pour s'assurer que le réseau est bien sécurisé. Pour effectuer des tests on utilise la commande PING dans chaque console d'un l'équipement.

4.2 Les tests effectués sur le serveur

On va tester l'adresse du serveur et sa passerelle avec la commande IPCONFIG.

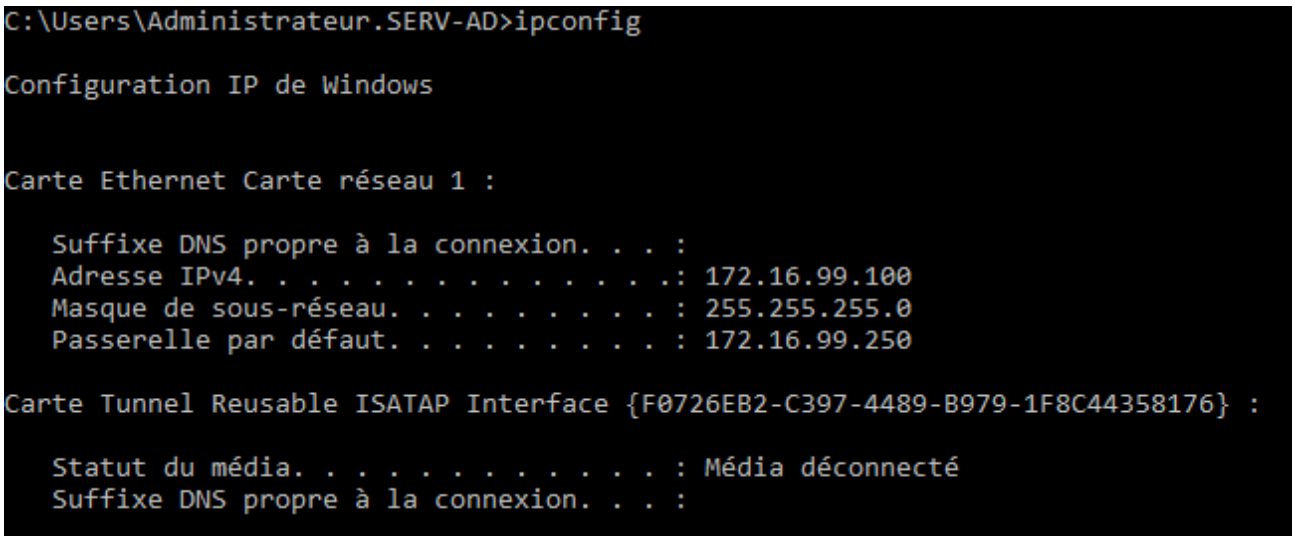

FIGURE 4.1 – Test réussi sur le serveur

On va pinguer à partir du serveur vers la passerelle de sortie..

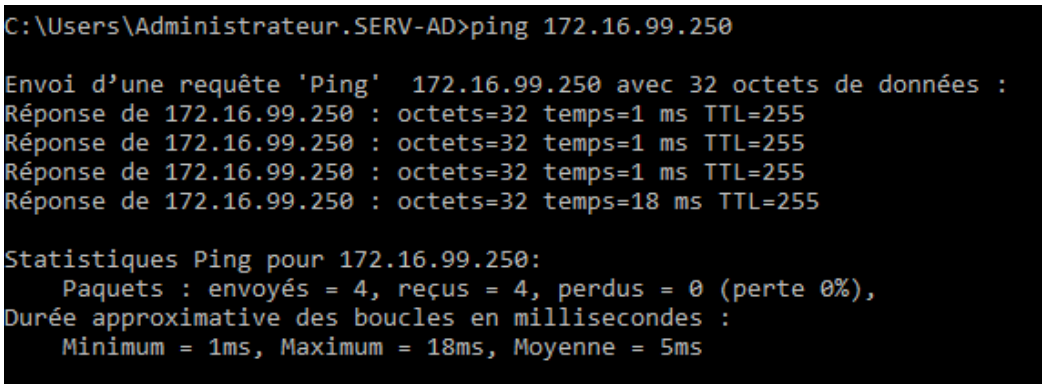

FIGURE 4.2 – Ping réussi sur le serveur

On va pinguer à partir du serveur vers la Passerelle de sortie du VLAN 20 (service DG).

```
C:\Users\Administrateur.SERV-AD>ping 172.16.20.250

Envoi d'une requête 'Ping'  172.16.20.250 avec 32 octets de données :
Réponse de 172.16.20.250 : octets=32 temps=2 ms TTL=255
Réponse de 172.16.20.250 : octets=32 temps=1 ms TTL=255
Réponse de 172.16.20.250 : octets=32 temps=2 ms TTL=255
Réponse de 172.16.20.250 : octets=32 temps=2 ms TTL=255

Statistiques Ping pour 172.16.20.250:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

FIGURE 4.3 – Ping reussi entre le serveur et la DG

On va pinguer à partir du serveur vers le service BU (VLAN 30) .

```
C:\Users\Administrateur.SERV-AD>ping 172.16.30.1

Envoi d'une requête 'Ping'  172.16.30.1 avec 32 octets de données :
Réponse de 172.16.30.1 : octets=32 temps=2 ms TTL=255
Réponse de 172.16.30.1 : octets=32 temps=1 ms TTL=255
Réponse de 172.16.30.1 : octets=32 temps=1 ms TTL=255
Réponse de 172.16.30.1 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 172.16.30.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

FIGURE 4.4 – Ping réussi entre le serveur et le BU

On va pinguer à partir du serveur vers le service ATELIER (VLAN 70).

```
C:\Users\Administrateur.SERV-AD>ping 172.16.70.2

Envoi d'une requête 'Ping'  172.16.70.2 avec 32 octets de données :
Réponse de 172.16.70.2 : octets=32 temps=7 ms TTL=255
Réponse de 172.16.70.2 : octets=32 temps=2 ms TTL=255
Réponse de 172.16.70.2 : octets=32 temps=3 ms TTL=255
Réponse de 172.16.70.2 : octets=32 temps=3 ms TTL=255

Statistiques Ping pour 172.16.70.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 7ms, Moyenne = 3ms
```

FIGURE 4.5 – Ping réussi entre le serveur et l'atelier

On va pinguer à partir du serveur vers le service DRH (VLAN 10) .

```
C:\Users\Administrateur.SERV-AD>ping 172.16.10.1

Envoi d'une requête 'Ping'  172.16.10.1 avec 32 octets de données :
Réponse de 172.16.10.1 : octets=32 temps=1 ms TTL=255
Réponse de 172.16.10.1 : octets=32 temps=4 ms TTL=255
Réponse de 172.16.10.1 : octets=32 temps=5 ms TTL=255
Réponse de 172.16.10.1 : octets=32 temps=46 ms TTL=255

Statistiques Ping pour 172.16.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 46ms, Moyenne = 14ms
```

FIGURE 4.6 – Ping réussi entre le serveur et le service DRH

On va pinguer à partir du serveur vers le parfeu de Seddouk .

```
Configuration IP de Windows


Carte Ethernet Carte réseau 1 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 172.16.99.100
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.16.99.250

Carte Tunnel Reusable ISATAP Interface {F0726EB2-C397-4489-B979-1F8C44358176} :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

C:\Windows\system32>ping 10.10.10.1

Envoi d'une requête 'Ping'  10.10.10.1 avec 32 octets de données :
Réponse de 10.10.10.1 : octets=32 temps=2 ms TTL=63
Réponse de 10.10.10.1 : octets=32 temps=2 ms TTL=63
Réponse de 10.10.10.1 : octets=32 temps=16 ms TTL=63
Réponse de 10.10.10.1 : octets=32 temps=47 ms TTL=63

Statistiques Ping pour 10.10.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 47ms, Moyenne = 16ms
```

FIGURE 4.7 – Ping réussi entre le serveur et le parfeu de Seddouk

On va pinguer à partir du serveur vers le pare-feu d'Alger .

```
C:\Windows\system32>ping 10.10.10.2

Envoi d'une requête 'Ping'  10.10.10.2 avec 32 octets de données :
Réponse de 10.10.10.2 : octets=32 temps=5 ms TTL=62
Réponse de 10.10.10.2 : octets=32 temps=62 ms TTL=62
Réponse de 10.10.10.2 : octets=32 temps=3 ms TTL=62
Réponse de 10.10.10.2 : octets=32 temps=20 ms TTL=62

Statistiques Ping pour 10.10.10.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 62ms, Moyenne = 22ms
```

FIGURE 4.8 – Ping réussi entre le serveur et le parfeu d'Alger

On va pinguer à partir du serveur vers le réseau d'alger .

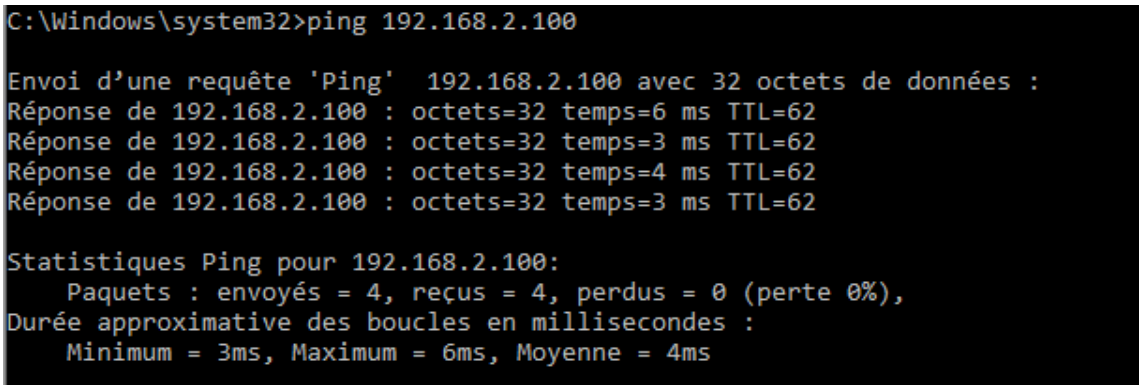

FIGURE 4.9 – Ping réussi entre le serveur et le réseau d'Alger

4.2.1 Les tests effectués sur les PC clients

On va tester si le DHCP server a attribué une adresse au pc avec la commande IP DHCP.

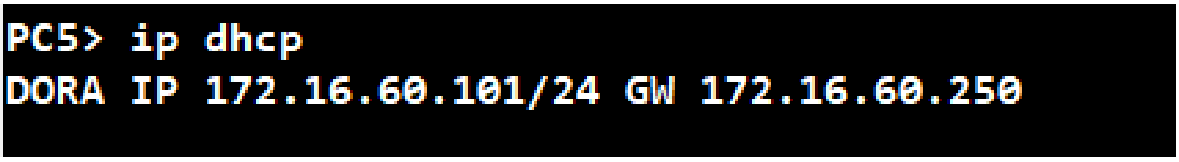

FIGURE 4.10 – Test réussi sur le pc client

On va tester l'adresse du pc1 client et sa passerelle avec la commande SHOW IP.

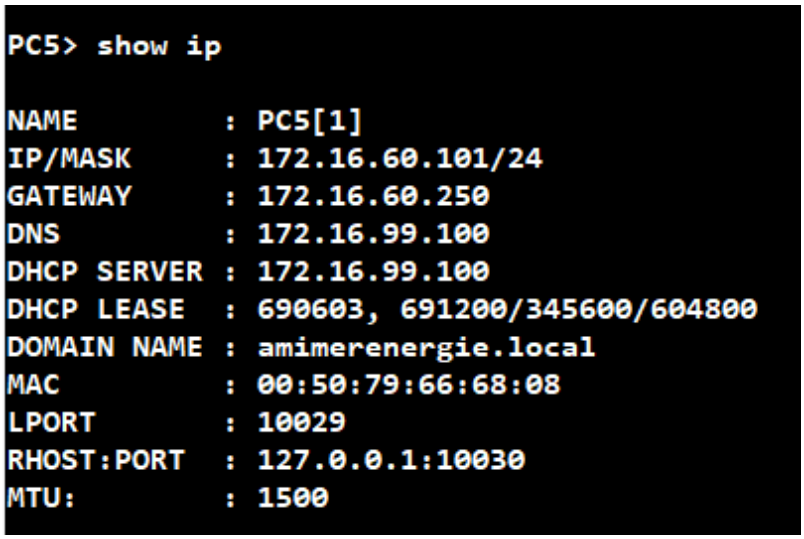

FIGURE 4.11 – Test réussi sur le PC1

On va pinguer a partir du pc client vers la passerelle de sortie .

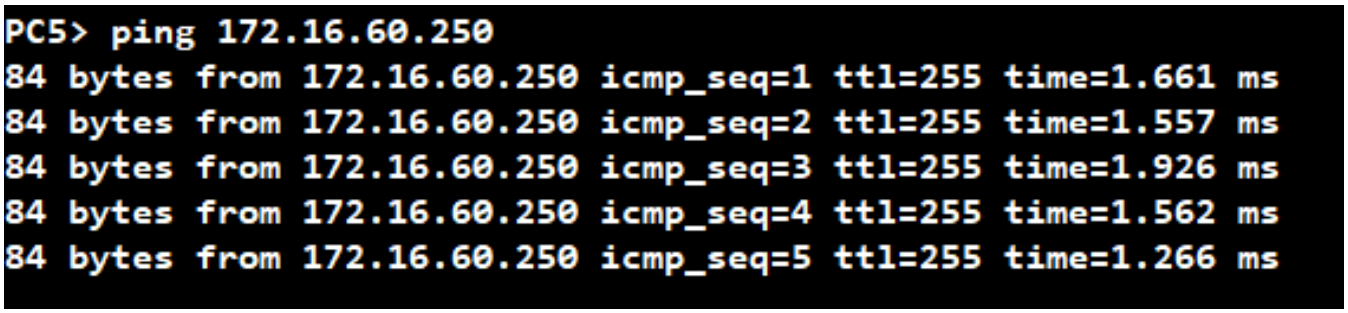

FIGURE 4.12 – Ping réussi entre le pc client et le routeur

On va pinguer apartir du pc client vers le serveur .

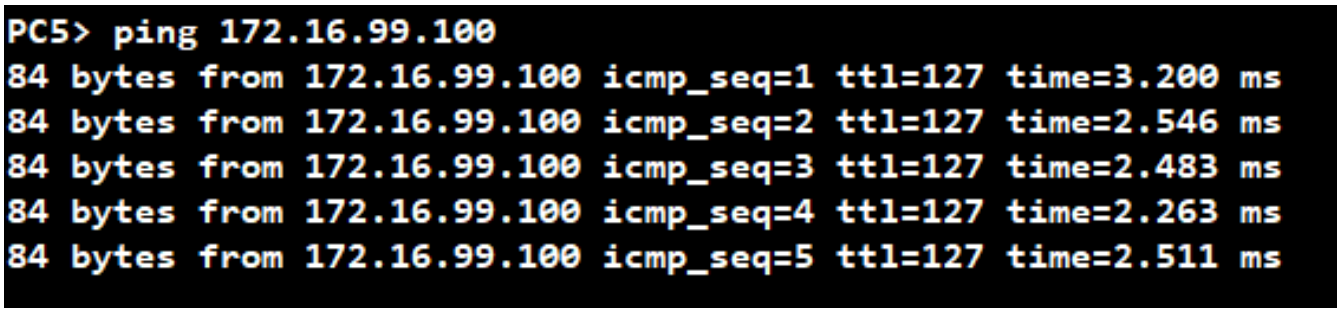

FIGURE 4.13 – Ping réussi entre le pc client et le serveur

On va pinguer apartir du pc client vers le service DRH (VLAN 10) .

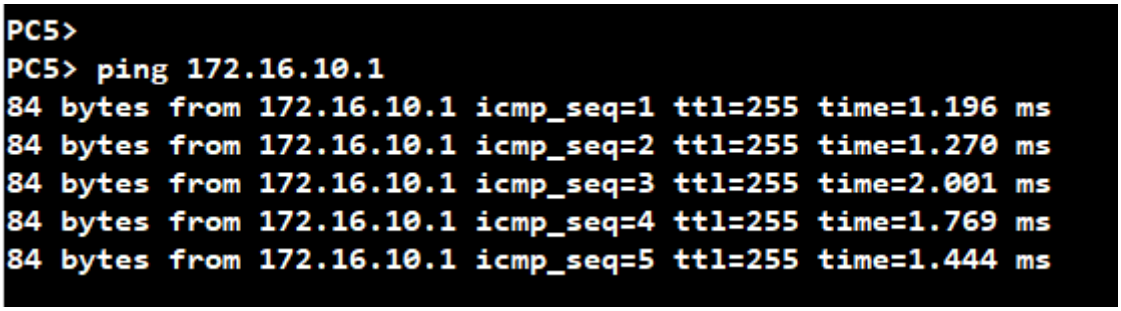

FIGURE 4.14 – Ping réussi entre le pc client et DRH

On va pinguer du service DSI (VLAN 60) vers le service DRH (VLAN 10) .

```
PC5>
PC5> ping 172.16.10.1
84 bytes from 172.16.10.1 icmp_seq=1 ttl=255 time=1.196 ms
84 bytes from 172.16.10.1 icmp_seq=2 ttl=255 time=1.270 ms
84 bytes from 172.16.10.1 icmp_seq=3 ttl=255 time=2.001 ms
84 bytes from 172.16.10.1 icmp_seq=4 ttl=255 time=1.769 ms
84 bytes from 172.16.10.1 icmp_seq=5 ttl=255 time=1.444 ms
```

FIGURE 4.15 – Ping réussi sur le PC client

On va tester l'adresse du PC2 client qui est sur le site d'Alger et sa passerelle avec la commande IPCONFIG.

```
C:\Users\PC1>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::2466:3d51:8b62:4684%3
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.2.4
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.2.100
```

FIGURE 4.16 – Test réussi sur le PC2 client

On va va pinguer apartir du pc2 client d'Alger vers le parfeu de seddouk .

```
C:\Users\PC1>ping 10.10.10.1

Envoi d'une requête 'Ping'  10.10.10.1 avec 32 octets de données :
Réponse de 10.10.10.1 : octets=32 temps=209 ms TTL=63
Réponse de 10.10.10.1 : octets=32 temps=210 ms TTL=63
Réponse de 10.10.10.1 : octets=32 temps=27 ms TTL=63
Réponse de 10.10.10.1 : octets=32 temps=12 ms TTL=63

Statistiques Ping pour 10.10.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 12ms, Maximum = 210ms, Moyenne = 114ms
```

FIGURE 4.17 – Ping réussi sur le PC2 client et parfeu seddouk

On va tester le SSH sur le pc1 client avec putty.

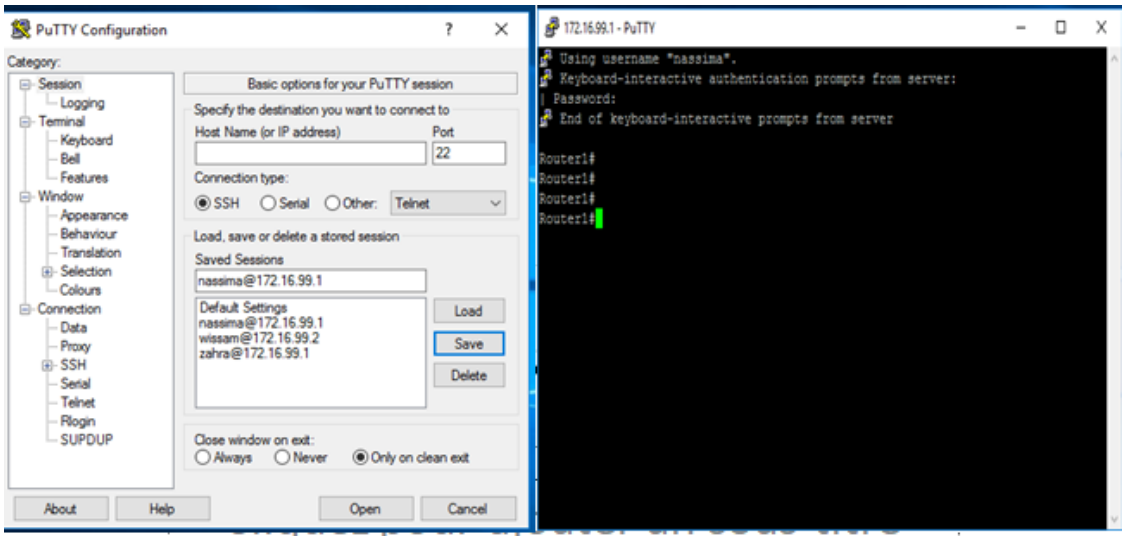

FIGURE 4.18 – Test réussi sur le PC1

On va pinguer apartir du pc client de Seddouk vers le parfeu d'Alger .

```
PC5> ping 10.10.10.2
84 bytes from 10.10.10.2 icmp_seq=1 ttl=62 time=11.111 ms
84 bytes from 10.10.10.2 icmp_seq=2 ttl=62 time=26.510 ms
84 bytes from 10.10.10.2 icmp_seq=3 ttl=62 time=3.337 ms
84 bytes from 10.10.10.2 icmp_seq=4 ttl=62 time=19.315 ms
84 bytes from 10.10.10.2 icmp_seq=5 ttl=62 time=5.655 ms
```

FIGURE 4.19 – Ping réussi sur le PC client et parfeu Alger

On va pinguer apartir du pc client de Seddouk vers le réseau d'Alger .

```
PC5> ping 192.168.2.100
84 bytes from 192.168.2.100 icmp_seq=1 ttl=62 time=4.601 ms
84 bytes from 192.168.2.100 icmp_seq=2 ttl=62 time=3.973 ms
84 bytes from 192.168.2.100 icmp_seq=3 ttl=62 time=5.127 ms
84 bytes from 192.168.2.100 icmp_seq=4 ttl=62 time=2.428 ms
84 bytes from 192.168.2.100 icmp_seq=5 ttl=62 time=3.207 ms
```

FIGURE 4.20 – Ping réussi sur le PC client et réseau Alger

On va pinguer apartir du pc client de Seddouk vers le réseau d'Alger .

```
PC5> ping 192.168.2.100
84 bytes from 192.168.2.100 icmp_seq=1 ttl=62 time=4.601 ms
84 bytes from 192.168.2.100 icmp_seq=2 ttl=62 time=3.973 ms
84 bytes from 192.168.2.100 icmp_seq=3 ttl=62 time=5.127 ms
84 bytes from 192.168.2.100 icmp_seq=4 ttl=62 time=2.428 ms
84 bytes from 192.168.2.100 icmp_seq=5 ttl=62 time=3.207 ms
```

FIGURE 4.21 – Ping réussi sur le PC client et réseau Alger

On va pinguer apartir du pc2 client de Alger vers le parfeu de Seddouk .

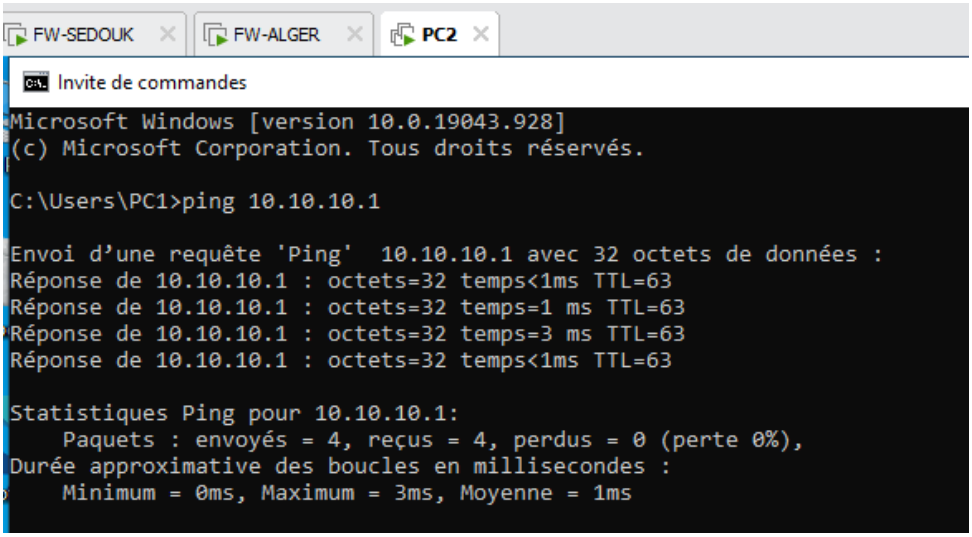

FIGURE 4.22 – Ping réussi sur le PC client et parfeu de Seddouk

On va pinguer apartir du pc2 client de Alger vers le parfeu d'Alger .

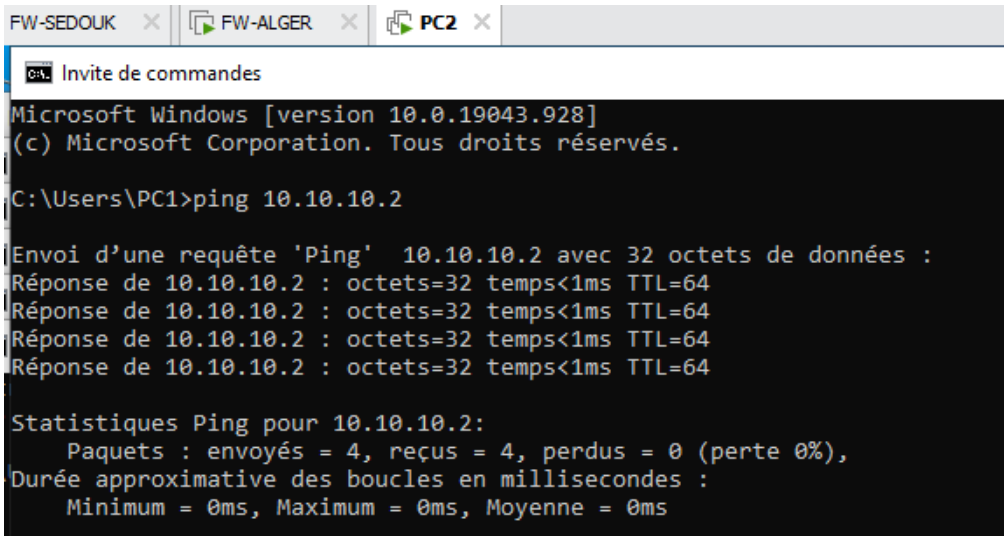

FIGURE 4.23 – Ping réussi sur le PC client et parfeu d'Alger

On va pinguer apartir du pc2 client de Alger vers la DMZ .

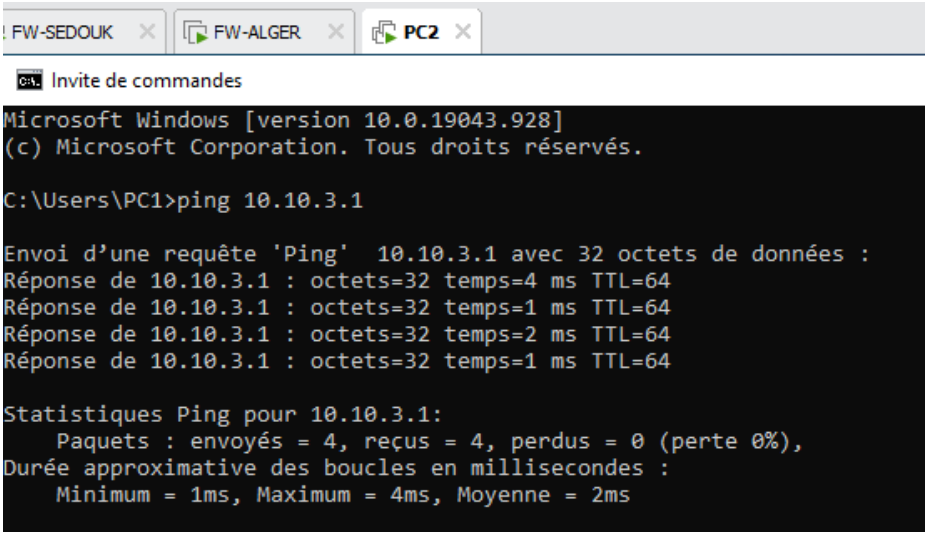

FIGURE 4.24 – Ping réussi sur le PC client et la DMZ

On va pinguer apartir du pc2 client de Alger vers le VLAN 99.

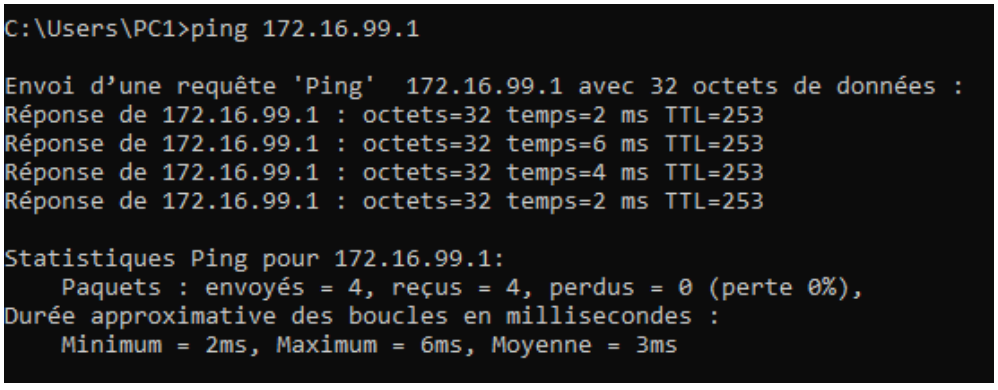

FIGURE 4.25 – Ping réussi sur le PC client et le VLAN 99

4.2.2 Les tests effectués sur les switchs

On va tester la securite de port du VLAN 10 avec un autre pc client sur le port , d'ou le port doit s'eteindre car on a limiter le nombre des adresses mac à 1 sur ce port.

```
SWA1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES unset  up                    up
Ethernet0/1            unassigned      YES unset  up                    up
Ethernet0/2            unassigned      YES unset  up                    up
Ethernet0/3            unassigned      YES unset  up                    up
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES unset  up                    up
Ethernet1/2            unassigned      YES unset  up                    up
Ethernet1/3            unassigned      YES unset  up                    up
Ethernet2/0            unassigned      YES unset  up                    up
Ethernet2/1            unassigned      YES unset  up                    up
Ethernet2/2            unassigned      YES unset  up                    up
Ethernet2/3            unassigned      YES unset  up                    up
Ethernet3/0            unassigned      YES unset  up                    up
Ethernet3/1            unassigned      YES unset  up                    up
Ethernet3/2            unassigned      YES unset  down                  down
Ethernet3/3            unassigned      YES unset  up                    up
Vlan1                  unassigned      YES unset  administratively down down
SWA1#
```

FIGURE 4.26 – Test réussi sur le switch access 1

On va tester l'auhentification RADIUS sur le switch client (SWA2).

```
SWA2#show authentication sessions interface ethernet 1/2 details
            Interface:  Ethernet1/2
          MAC Address:  000c.29e3.fc80
         IPv6 Address:  Unknown
         IPv4 Address:  172.16.50.105
            User-Name:  host/PC1.amimerenergie.local
               Status:  Authorized
               Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  AC106303000000C00031F1D
     Acct Session ID:  Unknown
              Handle:  0xD0000001
      Current Policy:  POLICY_Et1/2

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:
         Vlan Group:  Vlan: 50

Method status list:
       Method           State
       dot1x            Authc Success

SWA2#
```

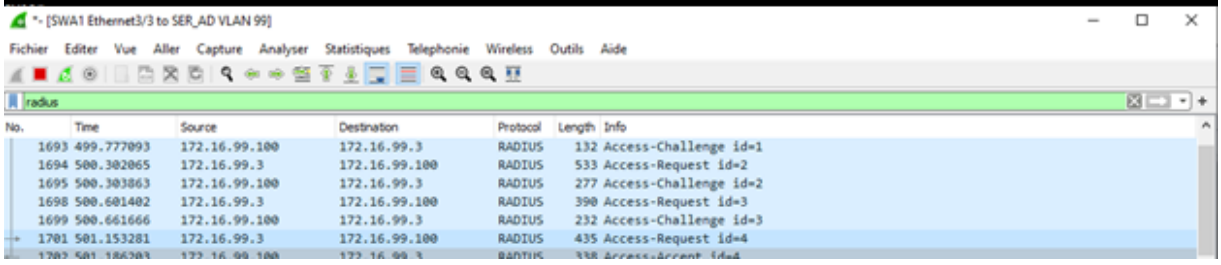

FIGURE 4.27 – Test réussi sur le switch access 2

On va tester les privates VLANs (PVLANs) sur le switch DMZ.

1. On va pinger sur les trois serveurs (commerce , SQL , voice) vers la passerelle de la DMZ.

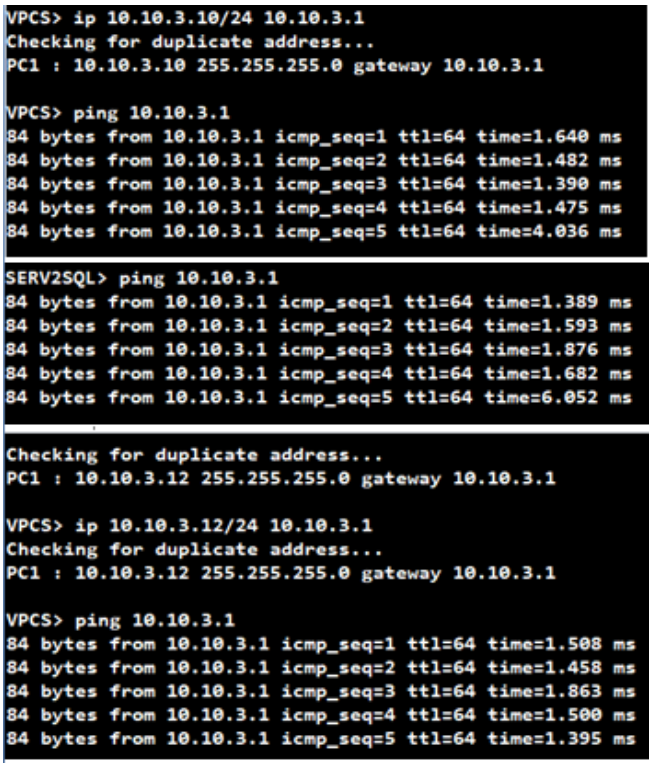

FIGURE 4.28 – Ping réussi sur les trois serveurs

2. On va pinger du serveur commerce (VLAN community) vers le serveur SQL (VLAN community) et vers le serveur voice (VLAN isolated).

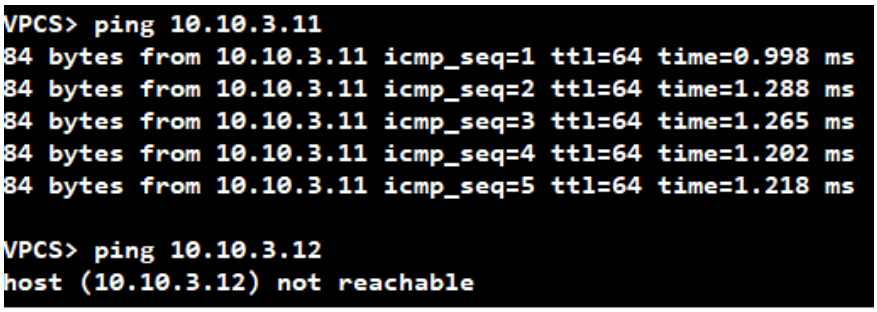

FIGURE 4.29 – Ping réussi sur le serveur commerce

3. On va pinger du le serveur SQL (VLAN community) vers serveur commerce (VLAN community) et vers le serveur voice (VLAN isolated).

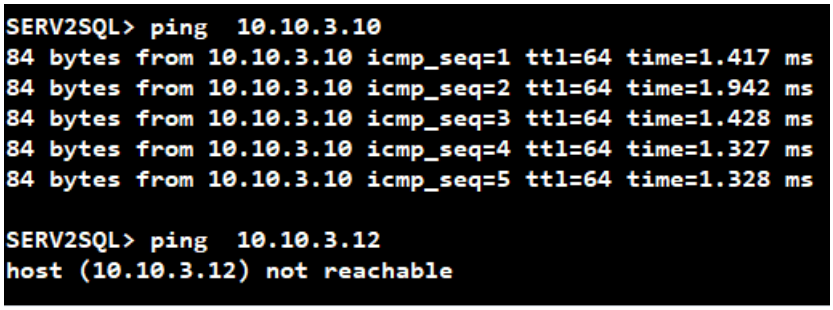

FIGURE 4.30 – Ping réussi sur le serveur SQL

4.2.3 Les tests effectués sur les pare-feus

On va tester l'interconnexion des deux sites à partir de chaque interface de sophos de chaque site, on va pinguer l'adresse du second site.

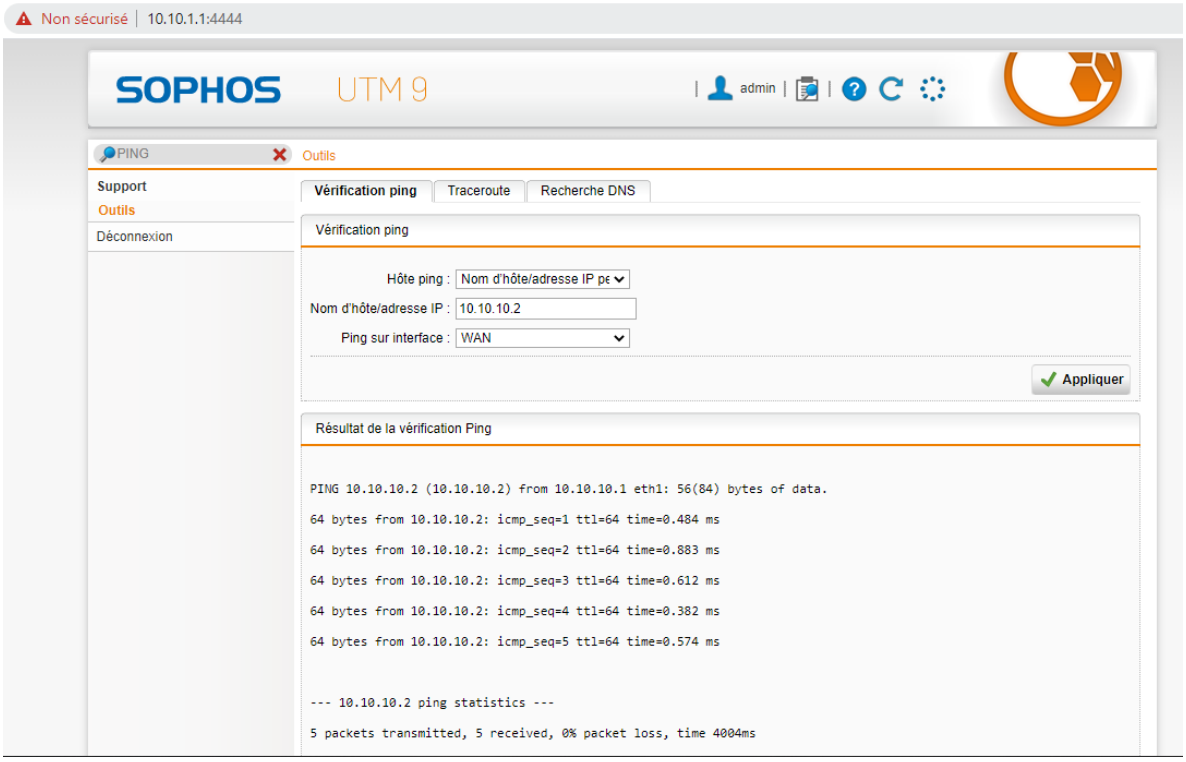

FIGURE 4.31 – Ping réussi de site Seddouk vers Alger

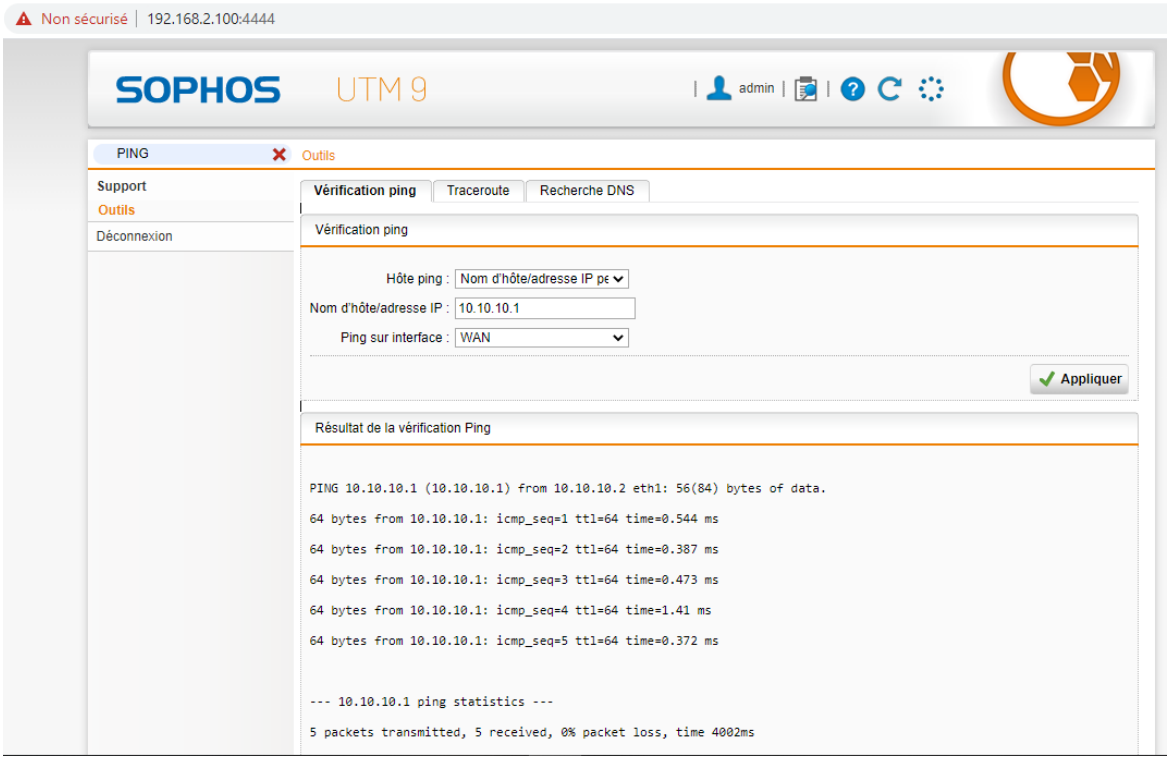

FIGURE 4.32 – Ping réussi de site Alger vers Seddouk

On va pinguer à partir du pare-feu du site Seddouk vers la DMZ.

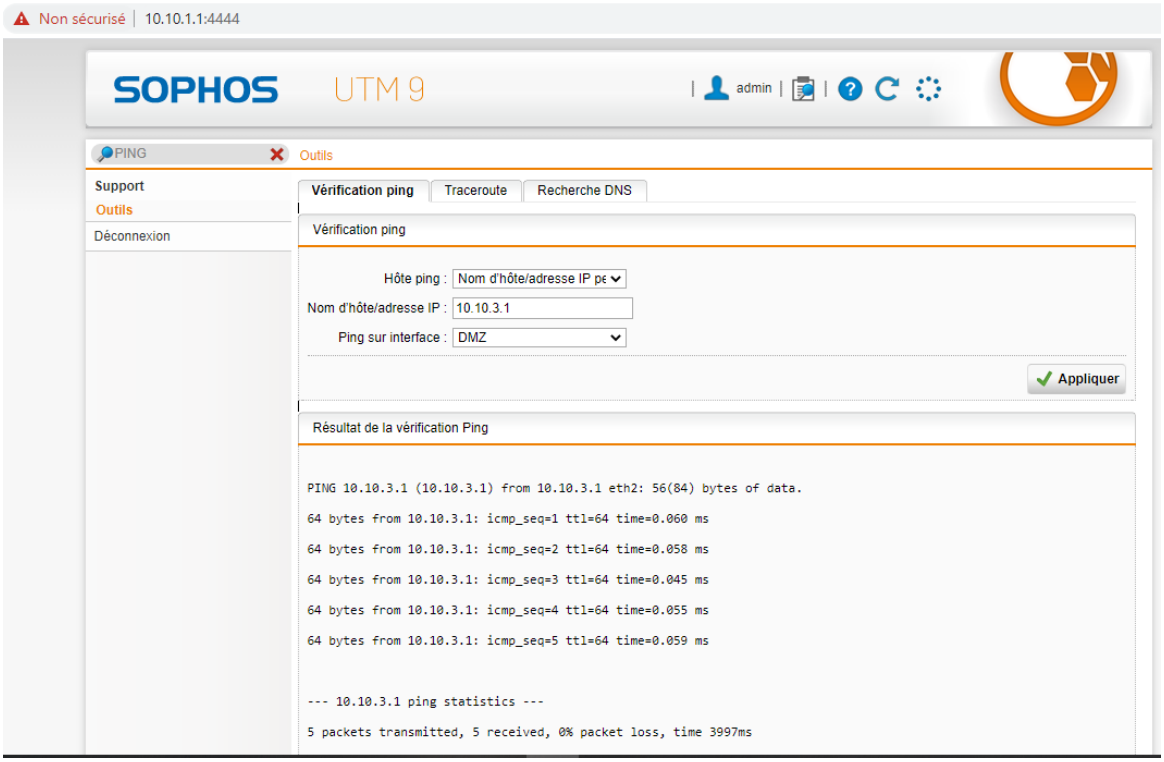

FIGURE 4.33 – Ping réussi sur le pare-feu de Seddouk

On va pinguer à partir du pare-feu du site Alger vers la DMZ.

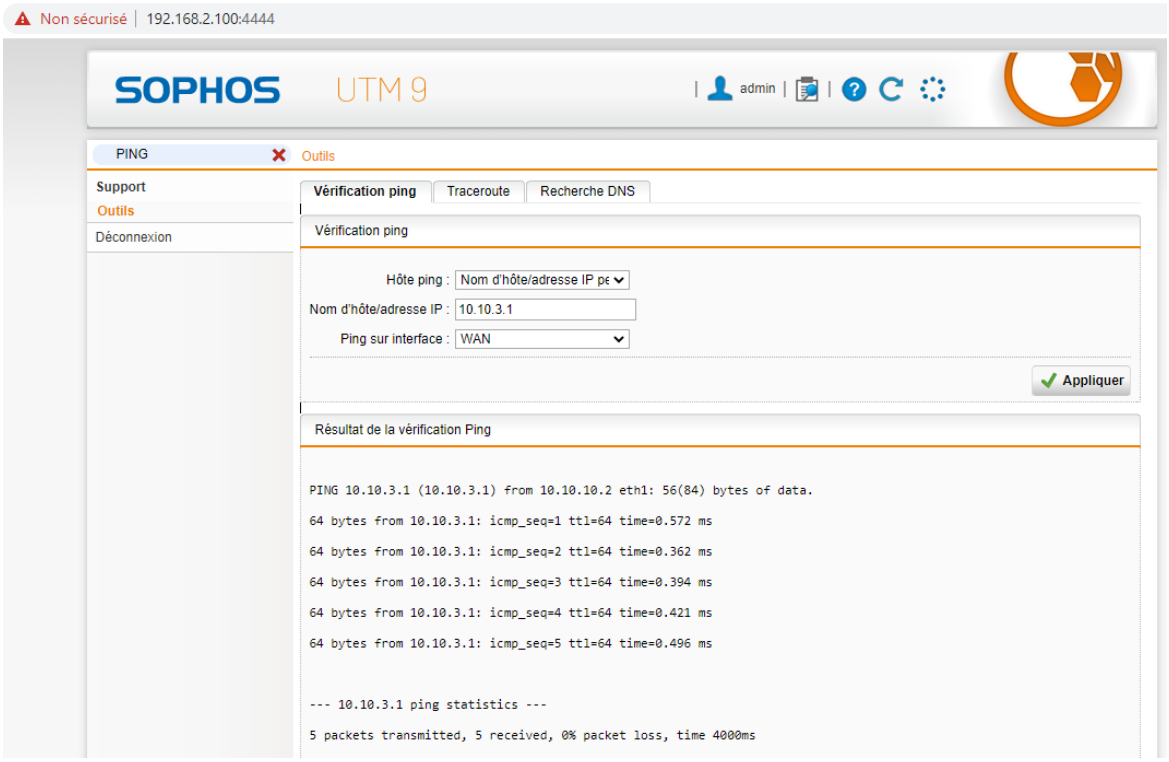

FIGURE 4.34 – Ping réussi sur le pare-feu d'Alger

On va pinguer à partir du pare-feu du site Seddouk vers le LAN 1.

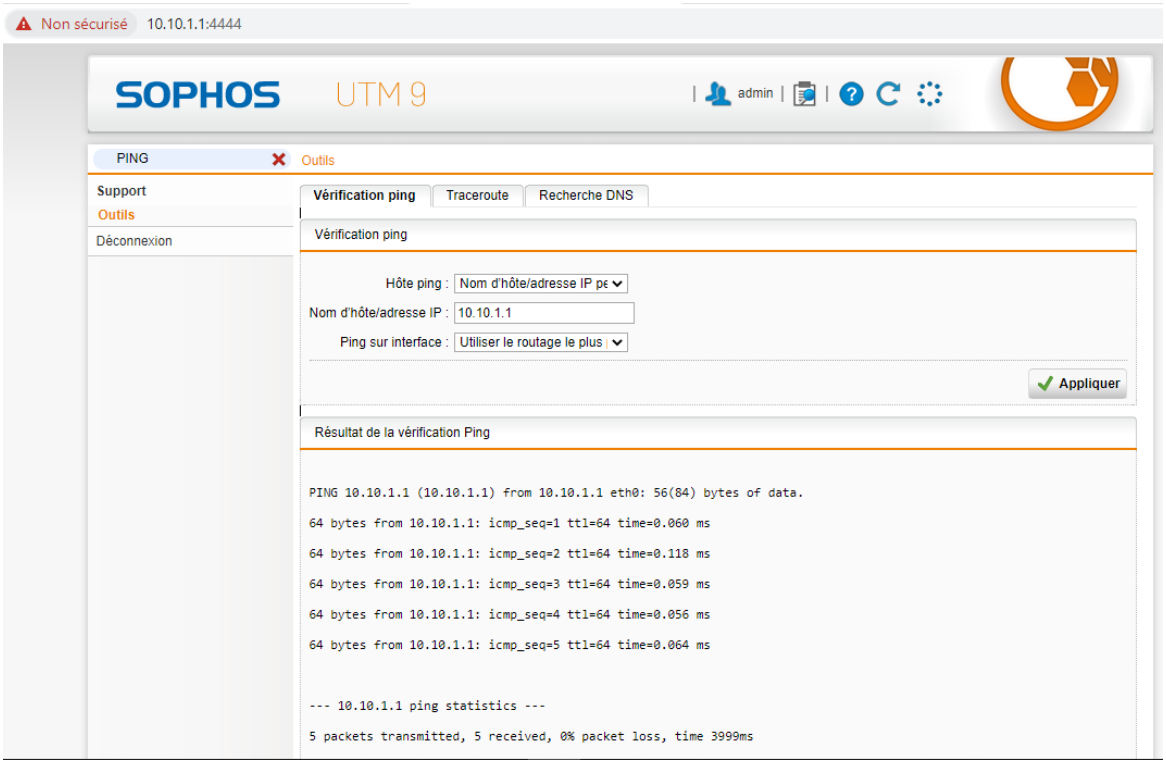

FIGURE 4.35 – Ping réussi sur le parfeu de Seddouk

On va pinguer à partir du pare-feu du site Seddouk vers le service DRH (VLAN 10).

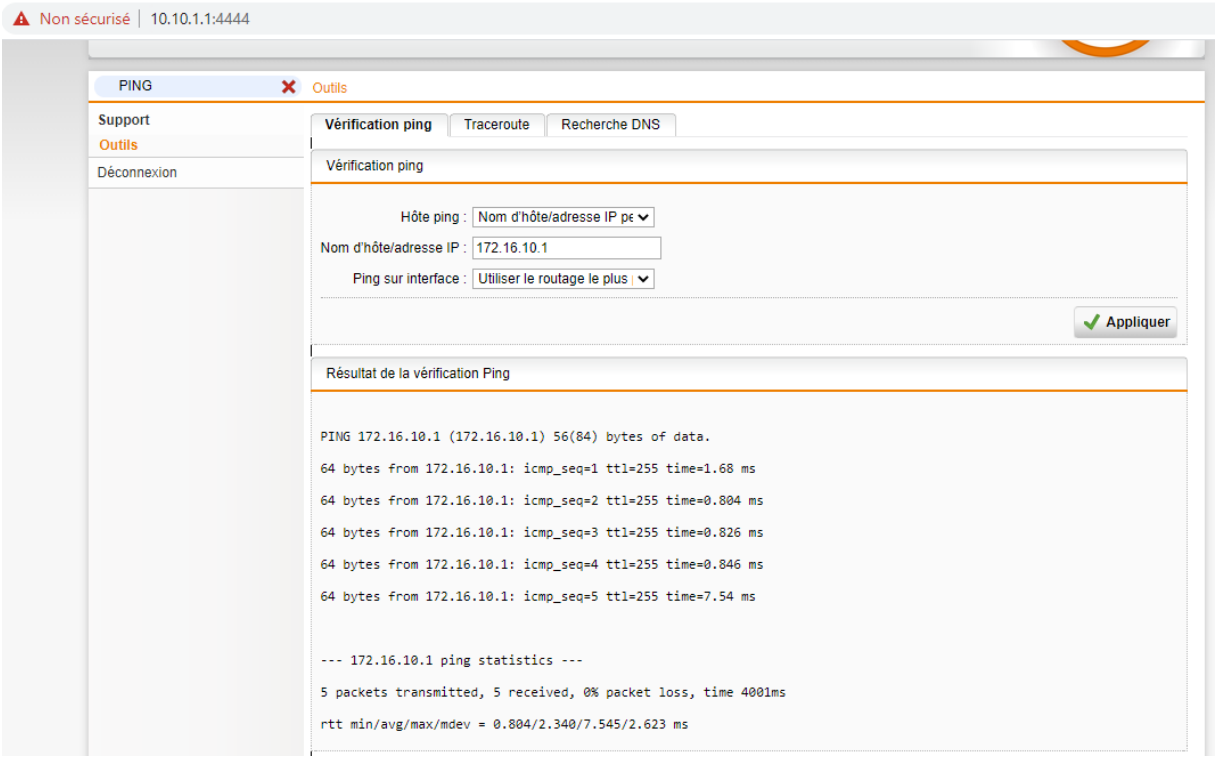

FIGURE 4.36 – Ping réussi sur le pare-feu de Seddouk

On va pinguer à partir du pare-feu du site Seddouk vers l'interface de sortie de management (VLAN 99).

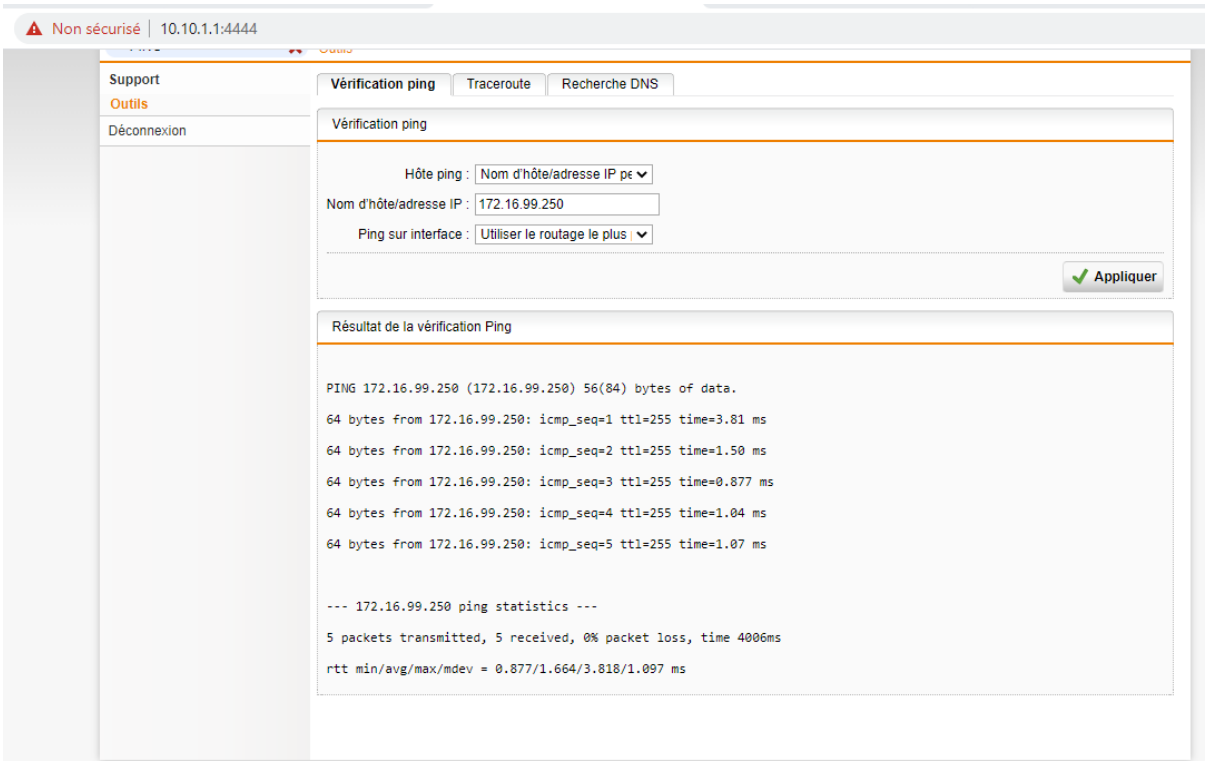

FIGURE 4.37 – Ping réussi sur le pare-feu de Seddouk

On va pinguer à partir du pare-feu du site Seddouk vers le serveur.

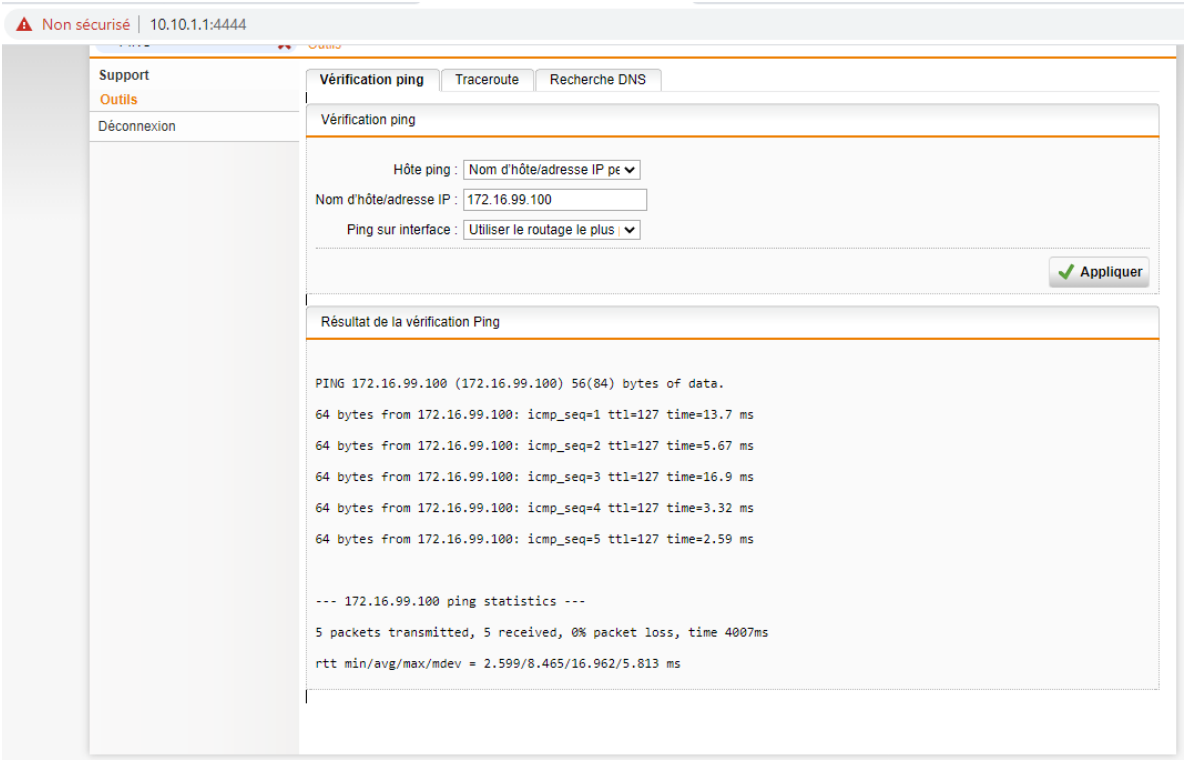

FIGURE 4.38 – Ping réussi sur le pare-feu de Seddouk

On va pinguer à partir du pare-feu du site Alger vers le pc client de LAN3 d'alger.

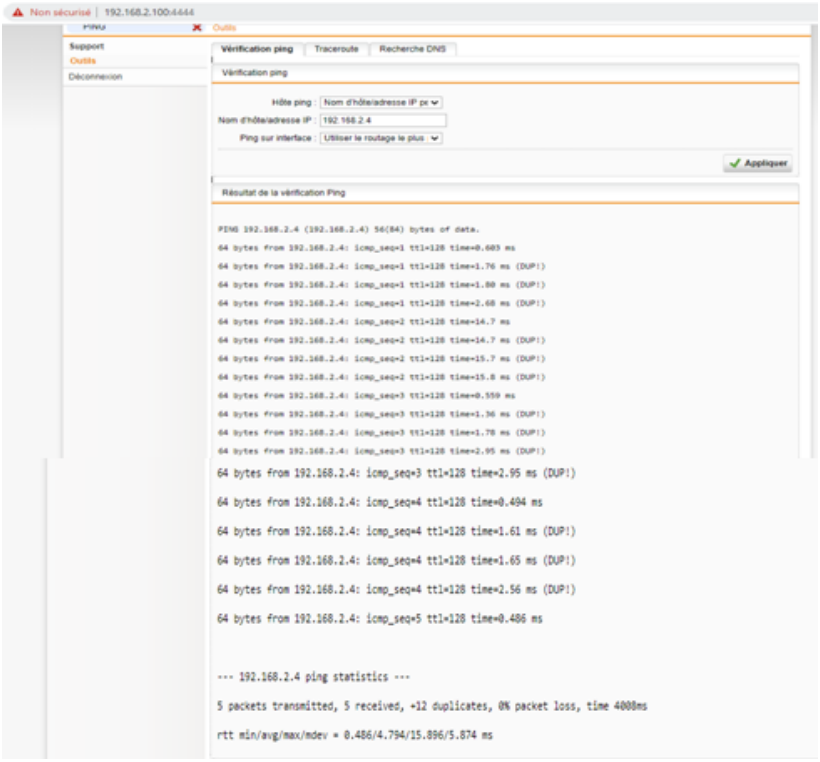

FIGURE 4.39 – Ping réussi sur le pare-feu de Alger

On va tester l'accès à distance avec SSL du client d'alger vers le site de Seddouk.

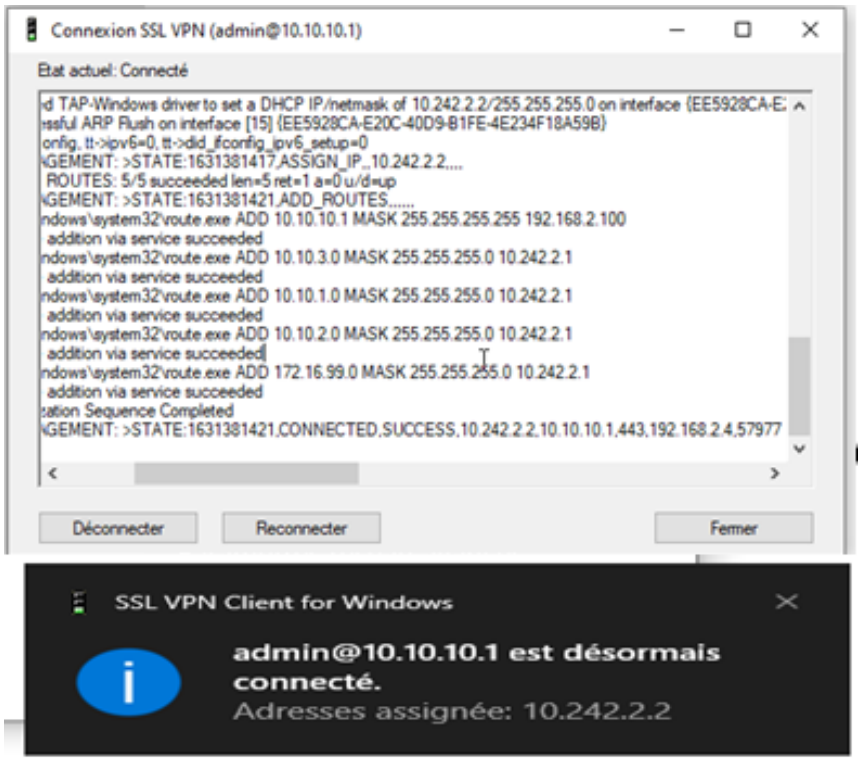

FIGURE 4.40 – Test réussi du client

4.3 Conclusion

À travers les démarches entretenues dans ce chapitre, nous avons pu constater qu'on a atteint notre objectif grâce aux captures ci-haut.

Conclusion générale

Durant notre période de stage au sein de l'entreprise Amimer Energie nous avons pu faire une analyse détaillée du réseau informatique et relever la différente insuffisance présentée en terme de sécurité.

Ensuite, nous avons abordé les différentes solutions adéquates selon les anomalies soulignées permettant de rendre le réseau plus sécurisé en prenant compte les besoins actuels de l'entreprise pour le bon fonctionnement de son réseau informatique et sa sécurité.

Afin d'améliorer son architecture réseau, nous avons configuré les VLANs en se basant sur le protocole VTP qui sert à la propagation de création, suppression et modification des VLANs sur tous les Switch de réseau de l'entreprise apartir d'un seul Switch ainsi nous avons integré le radius qui assure l'authentification pour ses clients et nous avons aussi utilisé plusieurs protocoles de sécurité comme le SSH pour un accès à distance sécurisé, HSRP pour assurer la disponibilité accrue de la passerelle d'un réseau,LACP pour contrôler l'agrégation de plusieurs liens physiques en un lien logique,...comme nous avons intégré une technologie d'agrégation de liens pour augmenter la vitesse et la tolérance aux pannes entre les équipements du réseau.Ainsi pour assurer le partage des ressources et l'échange des données de manière sécurisée entre les deux sites distants(Alger et Seddouk) nous avons utiliser un VPN IPSec.

La réalisation de ce projet nous a permis d'apporter une contribution à l'entreprise Amimer Energie de Seddouk mais aussi d'acquérir de nouvelles connaissances sur les protocoles de sécurité grâce à une étude détaillée sur leurs fonctionnements et leurs principes.

Annex

Les commandes CISCO

Commandes	Descriptions
configure terminal ou conf t	entre dans le mode de configuration globale
CTRL-Z	Permet de retourner à la racine du menu
Exit	Sort et remonte d'un écran dans la hiérarchie des menus
Hostname	permet de modifier le nom de l'équipement réseau
Enable secret passeword	assigne un mot de passe encripté à enable
Interface ethernet|fastethernet| Serial looback <interface> ou int e|fa|s	entre dans le mode de configuration de l'interface
ip address <address><masque> ou ip add	configure l'interface avec l'IP et le masque de réseau
bandwidth ou band	indique une bande passante
Encapsulation<encap> [<type>]ou encap	fourmit l'encapsulation de l'interface
No shutdown ou no sh	Active ou disactive l'interface
Les commande de suvegarde :	
Copy runnig-config startup-config ou copy run star	Sauvegade la configuration courante en NVRAM
copy running-config tftp ou copy run tftp	Sauvegarde la configuration courante vers un serveur TFTP
copy startup config tftp ou copy start tftp	Sauvegarde la configuration NVRAM vers un serveur TFTP
copy tftp startup-config ou copy tftp star	charge un fichier de configuratio n de TFTP en NVRAM
copy tftp running-config ou copy tftp run	charge un fichier de configuration d'un serveur tftp dans la configuration courante
erase startup-config ou erase start	Efface la configuration de la NVRAM

Configuration d'une connexion en telnet	
routerconf t	
router(fonfig)line console 0	
router(config)login	
router(config)passeword cisco	
Les commandes sur un switch :	
vlan database vlan 1 name[vlan name]	Accès à la base de donnée et écriture dans le fichier vlan.dat
Exemple de configuration d'un vlan :	
switch vlan database	
switch(vlanvlan[number][name])	
switch(vlan)exit	
switch(config)interface f1[iface-number	Affectation sur un port
switch(config)interface range fa...	Affectation sur un ensemble de ports
switch(config-if)switchport mode access	on passe le mode de configuration de l'interface
switch(config-if)switchport access vlan[number-name]	on active le vlan sur le ou les interfaces
switchport trunk encap dot1q	on active le mode trunk,il y a deux protocoles utilisés dans l'étiquetage :le protocole ISL(CISCO) et le protocole 802.1q(IEEE)
switchport mode trunk	on active le mode trunk sur le port de commutateur serveur et client qui font le trunk le reste des port sont en mode access
vlan database vtp domain[domain-name] vtp server	Création d'un serveur vtp
vlan database vtp domai[domain-name] vtp client	Crésation d'un client VTP
ip default-gateway[ip-gateway]	on peut définir un passerelle par défaut pour communiquer entre vlan, pour se faire on utilise un routeur
encapsulation ISL | dot1q[vlan-number]	en mode interface on peux spécifier le type d'encapsulation sur le routeur
D'autres commandes communes	
reload	Redémarrer l'équipement réseau
setup	passe en mode de configuration assisté

ping [address]	ping seule,permet de faire un ping étendu de spécifié une interface particulière...ping*address IP ping l'interface avec l'interface directement connecté
Les commandes show	
show interface ou sh int	Donne une déscription détaillée sur les interfaces
show running-config ou sh run	Affiche la configuration courante
show startup-config ou sh star	Affiche la configuration en NVRAM
show ip route ou sh ip route	Affiche la table de routage
show ip [routing-protocol][option]	Affiche les informations sur le protocole de routage défini
show ip protocols	Affiche des informations sur les protocoles utilisés
show ?	Donne toutes les commandes show disponibles

Table 4.1 – Auteur :RAMJANALLY Gboulseine

Bibliographie

[1] https ://pjacob.scenari-community.org/

[2] https ://eduscol.education.fr/sti/sites/eduscol.education.fr

[3]] https ://blog.netwrix.fr/2019/07/24/tout-ce-quil-faut-savoir-sur-les-equipements-reseau/

[4] https ://www.journaldunet.fr/

[5] https ://www.futura-sciences.com/

[6] Dental.Lifeline, NETWORK, Metropolitan Area, NETWORK,Local Area, et al.Definition.Available at : dentalifeline.org.Accessed February,2016,vol.9.

[7] https ://www.coursehero.com/ W

[8] https ://www.oracle.com/

[9] https ://fr.wikipedia.org/

[10] https ://www.wireshark.org/docs/wsug-html-chunked/ChapterIntroduction.html

[11] https ://www.merriam-webster.com/dictionary/puttyhttps ://www.merriam-webster.com/dictionary/putty

[12] http ://www.linux-france.org/

[13] https ://www.paessler.com

[14] Raymond Panko - Sécurité des Systèmes d'information et des Réseaux - Pearson Education,2004.

[15] https ://www.networklab.fr/category/ccnp-switch/securite/

[16] P.Guy. Initiation-ux-réseaux, Eyrolles 8ème édition,2014.

[17] Solange Ghernaouti-Hélie - Sécurité informatique et réseaux - Dunod,2011.

[18] Guemati F.," Configuration sécurisée et efficace du routeur du réseau Intranet de l'université de bejaia" , mémoire Master en informatique , Université de Bejaia, 2008.

[19] Arnaud S. et Guillaume D ., " Les VLANs ; les protocoles de transport et de controle",2006.

[20] https ://www.networklab.fr/category/ccnp-switch/securite/

[21] Jean-Paul Archier.Les VPNs Fonctionnement en oeuvre et maintenance des réseaux privés virtuels.2éme édition,Décembre 2013.

Résumé

Le réseau informatique est au cœur de l'entreprise, quelle que soit son secteur d'activité. On peut facilement comparer la place que joue le réseau informatique au sein d'une entreprise à celle que joue le système nerveu chez l'être humain. En effet, il doit fonctionner pleinement et en permanence pour garantir l'activité. Les problèmes de sécurité doivent donc être réduits au minimum, car une indisponibilité du système d'information ou la perte de son authenticité peut être une cause de plusieurs pertes pour notre entreprise.

Pour cela, on a fait un tour sur l'une des plus importantes technologies de réseau informatique, c'est l'installation, la configuration et la sécurisation d'un réseau d'entreprise, nous avons exploité GNS3 pour la simulation de la configuration et VMWARE.

L'objectif de ce travail est de proposer une amélioration pour l'architecture du réseau Amimer Energie afin de gérer d'une façon efficace et sécuriser la communication entre les services des deux sites distants.A cet effet, nous avons segmenté le réseau en plusieurs VLANs comme nous avons configuré un VPN sécurisé entre les deux réseau Seddouk et Alger et pour sa réalisation ,comme nous avons intégré plusieurs protocoles de sécurité (RADIUS,DHCP,DNS,spanning tree,SSH,HSRP,VTP,LACP..) nous avons choisi de travaillé sur le pare-feu Sophos qui fournit des services d'authentification et de filtrage.

Abstract

The computer network is at the heart of the company, whatever its sector activity. We can easily compare the place played by the computer network within a enterprise to that of the nervous system in humans. Indeed, it must work fully and permanently to guarantee activity. Security concerns must therefore be reduced to a minimum, because unavailability of the information system or loss of sound authenticity can be a cause of loss for our business. par For that, we took a look at one of the most important computer network technologies, it is the installation, the configuration and the securing of a company network, we used GNS3 for the simulation configuration and VMWARE. par The objective of this work is to propose an improvement for the architecture of the Amimer Energie network in order to efficiently manage and secure the communication between the services of the two remote sites. VLANs as we have configured a secure VPN between the two networks Seddouk and Algiers and for its realization, we have chosen to work on the Sophos firewall which provides authentication and filtering services.