République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderahmane Mira de BEJAIA
Faculté des Sciences Exactes
Département Informatique

Mémoire de Fin de Cycle

En vue de l'obtention du diplome de Master en Informatique

Option: Administration et Sécurité des Réseaux

THEME

Mise en place de la norme de sécurité 802.1X au sein du réseau de SONATRACH

Réalisé par :
Mlle DJIDJELI Amira
Mlle IKHLEF Lilia

Soutenu le 14 Octobre 2021, Devant le jury composé de :

Président	M. Hachem SLIMANI	Université Béjaïa
Examinatrice	Mme Zineb TAHAKOURT	Université Béjaïa
Encadrant	M. Kamel AMROUN	Université Béjaïa
Encadrant	M. Nadim EL-SAKAAN	Université Béjaïa

Année universitaire : 2020/2021

Dédicace

Je dédie ce travail à :

Je remercie le bon **dieu** de m'avoir donné le courage, la santé, la volonté afin de mener à bien ce modeste travail.

A **ma maman** et **mon papa**, qui m'a doté d'une éducation digne, leurs amour, présence, soutien, sacrifices à fait de moi ce que je suis aujourd'hui,que dieu les garde et les protège.

A mon frére **Amine**, qui m'avez toujours soutenu et encouragé, malgré la distance je t'aime plus que tout.

A mon petit frère **saou** que j'aime trop.

A celui que j'aime **Yanis**, tu as toujours été à mes cotés pour me soutenir et m'encourager.

A **Chanez**, ma meilleure amie mon ame soeur qui m'encourage et toujours a mes cotés.

A ma cousine adorable,**Wissem**.

A tout mes amies qui m'ont toujours encouragé, et à qui je souhaite plus de succès.

A mon amie **Yacine**, pour son soutien et son aide.

A **Lilia**, chère amie avant d'etre binome et sa famille.

Amira

Dédicace

Avec l'expression de ma reconnaissance, je dédie ce modeste travaille à ceux qui quelles que soient les termes embarrassé je n'arriverai jamais à leur exprimer mon amour sincère.

A toute la famille**IKHLEF**.

À l'homme mon précieux offre du dieu, qui doit ma vie, ma réussite et tout mon respect, mon cher père **Mourade**.

À la femme qui a souffert sans me laisser souffrir, qui n'a jamais dit non à mes exigences et qui n'a épargné aucun effort pour me rendre heureuse mon adorable mère **LILA**.

À mon adorable petite sœur **Amanda** et mon fiancé **Mohamed** qui n'ont pas cessé de me conseiller encourager et soutenir, que Dieu les protège et leur offre la chance et le bonheur.

À ma grand-mère **Taklit**, mes oncle, mes tantes, et toutes mes cousines une par une que Dieu leur donne une longue et joyeuse vie.

À la meilleur copine **Nesrine**, et toute sa famille.

A mon amie **Yassine** pour son aide.

Merci pour leur amour et leurs encouragements.

Sans oublier ma très cher copine **Amira** mon binôme, et toute sa famille.

Lilia

Résumé

Ce document s'inscrit dans le cadre de notre projet de fin d'études pour l'obtention du diplôme de master en Informatique, spécialité Administration et Sécurité des Réseaux à l'université ABDERRAHMANE Mira de Bejaia. Il décrit notre travail durant notre stage au sein de la RTC Sonatrach.

L'objectif de la présente étude consiste à étudier la norme IEEE 802.1X qui se base sur le protocole RADIUS.

Pour l'implémentation de ce travail, nous avons choisi Windows Server 2016 qui inclut le serveur d'authentification RADIUS pour la gestion des utilisateurs.

Mots-clés : IEEE 802.1X, authentification, RADIUS, Windows Server 2016.

Abstract

This document is part of our end of studies project for obtaining a master's degree in Computer Science, specializing in Network Administration and Security at ABDERRAHMANE Mira de Bejaia University.It describes our work during our internship at RTC Sonatrach.

The objective of this study is to investigate the IEEE 802.1X standard which is based on the RADIUS protocol.

For the implementation of this work, we have chosen Windows Server 2016 which includes the RADIUS authentication server for user management.

Keywords : IEEE 802.1X, authentication, RADIUS, Windows Server 2016.

Remerciements

Nous tenons tout d'abord à remercier dieu le tout puissant qui nous a donné la force et la patience d'accomplir ce modeste travail.

Nous voudrions présenter nos sincères remerciements à notre encadreur Mr EL SAKAAN Nadim pour sa disponibilité et ses orientations et conseils et lui témoigner notre gratitude pour sa patience et son soutien qui nous ont été précieux afin de mener notre travail à bon port.

Nous remercions vivement Mr AMROUN Kamal d'avoir accepté d'être notre encadreur.

Nous remercions également les membres du jury Mme TAHAKOURT Zineb, et Mr SLIMANI Hachem d'avoir accepté d'examiner ce travail.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AAA *Authentication Authorization Accounting*

AD *Active Directory*

CA *Certificate Authority*

CHAP *Challenge Handshake Authentication*

DHCP *Dynamic Host Configuration*

DNS *Domain Name System*

EAP *Extensible Authentication*

EAP-Fast *Extensible Authenticationg*

EAPOL *Extensible Authentication Protocol Over the LAN*

EAP-TLS *Extensible Authentication Protocol-Transport Layer Security*

EAP-TTLS *Extensible Authentication Protocol-Tunneled Transport Layer Security*

GPO *Group Policy Object*

IEEE *Institute of Electrical and Electronics Engineers*

IP *Internet Protocol*

ISO *International Standards Organization*

LAN *Local Area Network*

LEAP *Lightweight Extensible Authentication Protocol*

MAC *Media Access Control*

MD5 *Message Digest 5*

MS-CHAP *Microsoft Challenge Handshake Authentication Protocol*

NAP *Network Access Protection*

NAS *Network Access Server*

NPS *Network Policy Server*

OSI *Open Systems Interconnection*

PC *Personnel Computer*

PEAP *Protected Extensible Authentication Protocol*

RADIUS *Remote Authentication Dial-In User Service*

SONATRACH *Société nationale pour la recherche, la production, le transport, la transformation, et la commercialisation des hydrocarbures*

TCP *Transmission Control Protocol*

UDP *User Datagram Protocol*

VLAN *Virtual Local Area Network OU Organization Unit*

VMwar *Virtual Machine*

VPN *Virtual Private Network*

VTY *Virtual Terminal*

WAN *Wide Area Network*

WEP *Wired Equivalent Privacy*

WLAN *Wireless Local Area Network*

Introduction générale

La sécurité des réseaux informatiques est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines. Vu l'expansion et l'importance grandissante des réseaux informatiques, lesquels réseaux ont engendré le problème de sécurité des systèmes d'information.

Dans la plupart d'organisations informatisées, partager les données directement entre machines est leur souci majeur. Il s'avère indispensable de renforcer les mesures de sécurités, dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques, sur ce, il s'avère donc essentiel de connaître les ressources de l'entreprise à protéger et ainsi maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés. L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau. Faisant partie de cette stratégie de sécurisation, le contrôle de l'accès physique au réseau qui s'avère une opération efficace pour limiter les possibilités d'accès au réseau des entités non désirées.

L'un des moyens pour réaliser ce contrôle est l'authentification des utilisateurs et l'application de droits utilisateurs. Notre objectif donc est de prévoir une solution d'authentification permettant de sécuriser l'accès des utilisateurs au réseau de l'entreprise SONATRACH de Bejaia.

Pour atteindre cet objectif, nous avons à notre disposition, plusieurs solutions d'authentification parmi lesquelles, on a choisi le protocole 802.1x, dont le but principal est d'autoriser l'accès physique à un réseau local après une phase d'authentification. Ce protocole s'appuie sur l'encapsulation EAP (Extensible Authentication Protocol) pour mettre en relation le serveur d'authentification RADIUS (Remote Access Dial In User Services) et le système à authentifier.

Notre mémoire est organisé en quatre chapitres :

Le premier chapitre consiste à définir quelques notions sur le système d'information et différents notions de la sécurité informatique.

Le deuxième chapitre porte sur la présentation de l'organisme d'accueil de l'entreprise

SONATRACH avec la problématique posée de son réseau.

Le troisième chapitre traite l'étude de la solution proposée et la mise en œuvre de service d'authentification RADIUS pour le réseau de SONATRACH de Bejaia, il présente les différents moyens et outils déployés pour l'implémentation de cette solution, ainsi les étapes de configuration.

Dans le quatrième chapitre, nous testons l'authentification des utilisateurs par le mécanisme de sécurité retenu.

Enfin, notre travail se clôture par une conclusion générale, décrivant les éléments essentiels qui ont été développés dans ce mémoire, ainsi quelques perspectives pour ce projet.

Chapitre 1

Généralités sur le système d'information et la sécurité informatique

1.1 Introduction

Le système d'information (SI) peut être défini comme un ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures...) permettant d'acquérir, de stocker, de traiter, de communiquer des informations de toutes formes dans une organisation.

Il y a donc tout d'abord des individus : Ce sont toutes les personnes qui utilisent le système, qu'elles soient simples employés ou cadres. Elles sont concernées soit en utilisant de l'information pour réaliser leurs tâches, soit en participant aux tâches liées à l'acquisition, au stockage, au traitement ou à la communication d'informations. Ce sont aussi les spécialistes des systèmes d'Information dont le rôle est la conception, la mise en œuvre et la gestion quotidienne du Système d'Information.

Il y a également des moyens matériels : Ce sont tous les dispositifs physiques permettant de recevoir, manipuler et émettre l'information ainsi que les supports de l'information, qu'ils soient papiers, magnétiques, optiques ou encore électronique s.

Il y a ensuite des logiciels et des procédures : Les logiciels correspondent à l'ensemble des programmes qui sont nécessaires au fonctionnement du système d'Information (lorsqu'il est informatisé bien évidemment). Comme un système d'Information n'est que très rarement entièrement automatisé, les procédures décrivent comment sont articulés les traitements manuels et les traitements automatisés.

Il y a enfin les données qui constituent la matière première des traitements. Elles sont soit saisies et dans cette hypothèse, correspondent à des événements nouveaux pour le système d'information, soit calculées et sont alors des résultats de traitement.

Le SI ne doit donc pas être assimilé au système informatique qui n'en est qu'un sous ensemble. Le système informatique constitue un support du SI qui prend en charge l'information numérisée et les traitements automatisés. D'une manière générale, ce sont

la taille, le secteur d'activité, l'ancienneté de l'organisation mais aussi la stratégie des dirigeants qui déterminent le niveau d'automatisation d'un SI.

1.2 Modèle en couche de système d'information

Les couches de système d'information fonctionnent conjointement. Un « modèle en couches » fait apparaître leur juxtaposition et leur articulation de ces logiques. La délimitation des couches peut toujours se discuter ; voici celle que nous allons utiliser (fig 1.1) :

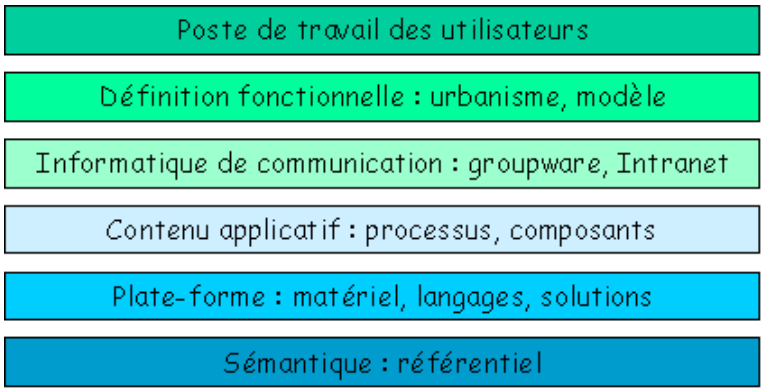

FIGURE 1.1 – Couche de système d'information[1].

1.2.1 Les couches de système d'information

Les couches de système d'information fonctionnent conjointement. Un « modèle en couches » fait apparaître leur juxtaposition et leur articulation de ces logiques. La délimitation des couches peut toujours se discuter ; voici celle que nous allons utiliser [1] :

a)Socle sémantique : A la base du SI se trouve le socle sémantique. Ce socle est géré par l'administration des données. Il fournit à l'entreprise son vocabulaire, en documente la façon dont elle classe et décrit ses processus, ses clients, ses produits etc. ainsi que les attributs qui les caractérisent.

b)Plate-forme physique : La plate-forme fournie par l'informatique comporte les matériels (machines, réseaux), les dispositifs de commande (système d'exploitation, langages de programmation, progiciels) et les solutions d'architecture technique (middleware, interfaces, etc.).

c)Contenu applicatif : Dans un SI « à l'ancienne », on nomme applications les programmes qui traitent les données saisies par les opérateurs ou transmises au SI pour fournir des résultats. Si le SI est de conception récente, on parlera plutôt de composants et de processus.

- Composants : Dans le vocabulaire des langages objet, un composant est un ensemble de classes articulées autour d'une classe maître, dans le langage courant, un composant est dans le système d'information la représentation d'un dossier (dossier

client, dossier produit, dossier commande, etc.).

- Processus : Le « processus » est la succession des tâches qui contribuent à une production de valeur. Alors que les applications ne contenaient pas d'informations sur les processus, les SI modernes automatisent le parcours du dossier entre les diverses personnes qui doivent le traiter (traitement d'une commande, d'une demande de crédit, d'une lettre de réclamation etc.).

d)Informatique de communication : Le SI fournit aux utilisateurs, outre les outils applicatifs, des ressources de bureautique et d'informatique communicante qui permettent de produire et communiquer des textes en langage naturel :
messagerie, documentation électronique, rédaction coopérative, diffusion sélective, forums etc. L'ensemble de ces outils a été désigné par le terme « groupware », de plus en plus remplacé par « Intranet » (ou par « Extranet » si la communication s'étend à plusieurs entreprises).

e)Définition fonctionnelle : Urbanisme et modèles Les qualités essentielles que doit posséder un SI sont :
- la pertinence (adéquation aux besoins des utilisateurs),
- la sobriété (il est inutile et coûteux de mettre en service des fonctionnalités qui resteront inutilisées),
- la cohérence (sans cohérence, on ne peut pas parler de système !).

f)Poste de travail : Le poste de travail (ordinateur personnel en réseau), fournit à l'utilisateur l'interface (écran, clavier) à travers laquelle il accède au SI.
Le but de l'entreprise étant d'obtenir un couple « homme – machine » efficace dans l'optique du «travail assisté par ordinateur », il convient :
- De définir le poste de travail de sorte qu'il équipe convenablement l'utilisateur,
- De former l'utilisateur au maniement du poste de travail.

1.3 Les réseaux

1.3.1 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipements informatiques reliés physiquement entre eux par un support de transmission afin de pouvoir échanger des données, transfert de fichiers, partager des ressources (imprimantes et données). Les réseaux informatiques ont plusieurs avantages dont [2] :

a)Le partage de ressources :
-Partage de ressources matérielles (imprimante, graveur, espace disque de stockage).
- Partage d'application (Logiciels, fichiers de données...).

b)La connexion à distance :
- "Émulation de terminal" sur un ordinateur central (type mini-ordinateur).
- Transfert de fichiers.

c)Le courrier électronique :
- Possibilité d'échanger des messages avec d'autres utilisateurs.

1.3.2 Etendu géographique des réseaux :

Nous distinguons, trois classes de réseaux selon l'étendue géographique :

a)Réseau local (LAN : Local Area Network) : Acronyme de Local Area Network, le terme LAN désigne un réseau informatique local. Il est constitué d'un ensemble d'ordinateurs et de périphériques reliés entre eux par des liaisons physiques (des câbles notamment). Ces ordinateurs et périphériques communiquent entre eux via des protocoles communs.
Le réseau local, ou LAN, se cantonne à un lieu physique et un environnement bien déterminé (une maison, un immeuble, etc.). On le retrouve souvent dans des entreprises qui disposent d'un parc informatique important dans une pièce (on parle alors aussi de Réseau Local d'Entreprise - RLE), mais aussi à la maison (deux ordinateurs + une imprimante reliés entre eux par exemple) ou pour les jeux en réseau.
De tels réseaux offrent en général une bande passante comprise entre 4Mbit/s et 100Mbit/s (pour les réseaux Ethernet et faste Ethernet standard) et 1Gbits/s (giga bit Ethernet par exemple mais pas trop utilisé)[3].

b)Réseau métropolitain (MAN : Metropolitan Area Network) : Ces réseaux son généralement utilisés pour interconnecter un ensemble de réseaux locaux géographiquement dispersés (la superficie d'une ville, un grand campus). Dans un réseau métropolitain, deux ordinateurs appartenant à deux réseaux locaux différents et distants peuvent communiquer ensemble comme s'ils faisaient partie du réseau local. Un MAN est formée d'équipements réseaux interconnectés par des liens à haut débit (en général à fibre optique). La maintenance de ce type de réseau n'est pas assurée localement par le personnel informatique mais par les entreprises de la télécommunication spécialisée dans la maintenance de ces types de réseaux[3].

b)Réseau étendu (WAN : Wide Area network) : Un réseau étendu (WAN) est un grand reseau d'ordinateurs qui relie des groupes d'ordinateurs sur de grandes distances.
Ces réseaux comme leurs noms l'indiquent, sont destinés à transporter l'information sur de longues distances à l'échelle d'un pays, un continent et enfin toute la planète. L'infrastructure est en général publique qui assure la maintenance de ces réseaux et qui veille à son bon fonctionnement. Le plus grand exemple à sité est le réseau global Internet qui entoure toute la planète[4].

1.3.3 Les équipements d'interconnexion

Comprendre ce que sont les équipements d'interconnexion est aisé : il apparait sous nos yeux lors de la conception d'un réseau informatique. C'est le matériel, il s'agit du câblage, des cartes réseaux, des hubs, des switches, des routeurs.....etc. et tout ce qui permet a un réseau de fonctionner autrement dit tout ce qui permet le dialogue entre 2 ordinateurs ou plus[5].

a)La carte réseau : Elle constitue l'interface physique entre l'ordinateur et le

câble réseau. Les données transférées du câble à la carte réseau sont regroupé en paquet composé d'un entête quicontient les informations d'emplacement et des données d'utilisateurs. Souvent la carte réseau est intégrée dans la carte mère. (Il faut bien noter que la carte réseau n'est fait pas partie des équipements d'interconnexion des réseaux)[6].

b)Répéteur : Le répéteur (en anglais repeater) est un équipement utilisé pour régénérer le signal entre deux nœuds du réseau, afin d'étendre la distance du réseau. On peut l'utiliser pour relier deux câbles de types différents[6].

c)Concentrateur (Hub) : Le concentrateur (appelé Hub en anglais) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Son rôle c'est de prendre les données binaires parvenant d'un port est les diffuser sur l'ensemble des ports[6].

d)Le commutateur : Comme le concentrateur, le commutateur (en anglais switch) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Sa seule différence avec le Hub, il est capable de connaître l'adresse physique des machines qui lui sont connectés et d'analyser les trames reçues pour les diriger vers la machine de destination[6].

e)les ponts : Le pont (bridge) est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Il reçoit la trame et analyse l'adresse de l'émetteur et du destinataire et la dirige vers la machine destinataire[6].

f)La passerelle : La passerelle est un système matériel et logiciel permettant de relier deux réseaux,servant d'interfaces entre deux protocoles différents. Lorsque un utilisateur distant contact un tel dispositif, celui-ci examine sa requête, et si celle-ci correspond aux règles que l'administrateur réseaux a défini, la passerelle crée un pont entre les deux réseaux.
Les informations ne sont pas directement transmises plutôt traduite pour assurer latransmission de deux protocoles. Ce système permet de relier deux systèmes informatiques qui n'utilisent pas la même architecture[6].

g)Le routeur : Le routeur est un matériel de communication de réseau informatique qui permet de choisir le chemin qu'un message va empruntés. Il est utilisé pour relier des réseaux locaux de technologie différente (par exemple Ethernet et token ring). Il intervient sur la couche réseau[6].

1.4 Modèles de communication

1.4.1 Le modèle OSI :

Il s agit d'une famille de protocoles élaborés conjointement en 1977 par l'organisation internationale de normalisation (ISO) et l'Union international des télécommunications (UIT). Le Protocole OSI comprenait également un modèle à sept couches appelé modèle de référence OSI. Le modèle référence OSI classe les fonctions de ses protocoles. Aujourd'hui OSI est principalement connu pour sont modèle en couche. Les protocoles

OSI ont été largement remplacer par TCP/IP[7].

a) Les couches OSI :
– Physique :Les protocoles de la couche physique décrivent les moyens mécaniques, électriques, fonctionnels et procéduraux pour activer, maintenir et désactiver des connexions physiques pour la transmission d'un bit vers et depuis un réseau device.

- Liaison de données :Les protocoles de la couche liaison de données décrivent les méthodes d'échange de trames de données entre les appareils sur un support commun
– Réseau :La couche réseau fournit des services permettant d'échanger les différents éléments de données individuels sur le réseau entre des dispositifs terminaux identifiés.

– Transport :La couche transport définit les services à segmenter, à transférer et réassembler les données pour les communications individuelles entre les terminaux.

-Session :La couche de session fournit des services à la couche de présentation pour organiser son dialogue et gérer l'échange de données.

– Présentation :La couche de présentation permet une représentation commune de données transférées entre les services de couche d'application.

– Application :La couche application contient les protocoles utilisés pour les processus communications[7].

1.4.2 Le modèle TCP/IP

Le modèle de protocole TCP/IP pour les communications sur l'internet a été créé au début des années 1970 et est parfois appelé le modèle internet. Ce type de modèle correspond étroitement à la structure d'une suite de protocoles particulière. 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 également utilisé comme modèle de référence [8].

a) Les couches TCP/IP :
- Accès réseau : Contrôle les périphériques matériels et les supports qui constituent le réseau.
– Internet :Détermine le meilleur chemin à travers le réseau.
– Transport :Prend en charge la communication entre plusieurs périphériques à travers divers réseaux.
– Application :Représente des données pour l'utilisateur, ainsi que du codage et un contrôle du dialogue [8].

1.5 Les services

1.5.1 Service DHCP

Le protocole DHCP (Dynamic Host Conguration Protocol) a pour but de fournir une adresse IP et un masque à tout périphérique réseau (station, serveur ou autre) qui en fait la demande. Selon la conguration, d'autres paramètres tous aussi importants seront transmis en même temps : les adresses IP de la route par défaut, des serveurs DNS à utiliser.
DHCP est souvent réservé aux stations, aux imprimantes et ne devrait servir qu'exceptionnellement aux serveurs [9].

a)Fonctionnement du protocole DHCP il faut dans un premier temps un serveur DHCP qui distribue des adresses IP. Cette machine va servir de base pour toutes les requêtes DHCP, aussi elle doit avoir une adresse IP fixe[9].
Dans un réseau, on peut donc n'avoir qu'une seule machine avec adresse IP fixe, le serveur DHCP.

Quand une machine démarre, elle n'a aucune information sur sa configuration réseau, et surtout, l'utilisateur ne doit rien faire de particulier pour trouver une adresse IP. Pour se faire, la technique utilisée est le broadcast : pour trouver et dialoguer avec un serveur DHCP, la machine va émettre un paquet de broadcast (broadcast sur 255.255.255.255 avec d'autres informations comme le type de requête, les ports de connexion...) sur le réseau local.

1.5.2 Service DNS

DNS (Domain Name Server) correspond tout d'abord à un protocole permettant à des clients (du réseau) d'interroger une base de données contenant des informations sur les machines et les services hébergés par ces machines. DNS est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement une information à partir d'un nom de domaine [9].

1.5.3 Service radius

Le protocole RADIUS acronyme de Remote Authentication Dial-In User Service est un protocole client- serveur qui repose principalement sur :
- un serveur (le serveur RADIUS), relié à une base d'identification (base de données).
- un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur.
L'ensemble des transactions entre le client RADIUS et le serveur RADIUS sont chiffrés et authentifiée grâce à un secret partagé.

L'identification effectuée par un serveur RADIUS est une vérification de nom d'utilisateur

et de mot de passe.
Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée. Enfin, le client final qui se connecte au réseau envoie tout simplement sa demande au point d'accès. Il n'échange aucune donnée avec le serveur radius. Il envoie juste son identifiant et son mot de passe sur le réseau qui est relayé jusqu'au serveur[10].
Exemples d'utilisation de RADIUS représenté ci-dessus :

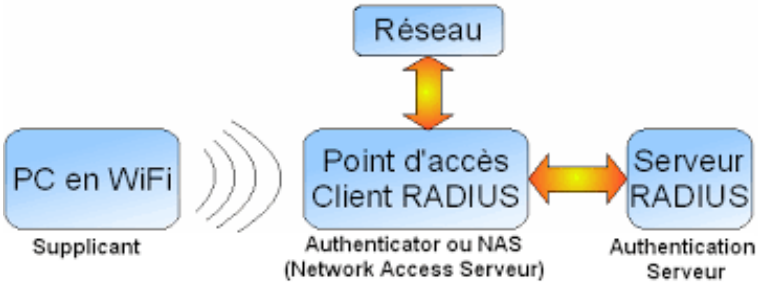

FIGURE 1.2 – Utilisation radius [10].

1.6 Objectifs de la sécurité

La sécurité informatique vise généralement cinq principaux objectifs :

- L'intégrité : garantir que les données sont bien celles que l'on croit être
-La disponibilité : maintenir le bon fonctionnement du système d'information
-La confidentialité : rendre l'information inintelligible à d'autres personnes que les seuls acteurs d'une transaction.
-La non répudiation : garantir qu'une transaction ne peut être niée
-L'authentification : assurer que seules les personnes autorisées aient accès aux ressources.

1.7 Méthodes de sécurité

Les méthodes de sécurité sont comme suit :
a)La protection par mot de passe :
Pour se connecter au réseau, l'utilisateur doit donner le mot de passe. Cette protection est également très simpliste. Il est facile pour un intrus de capturer le mot de passe et de l'utiliser par la suite pour se connecter au réseau.

b)La protection par adresse MAC :
Chaque adaptateur réseau possède une adresse physique unique appelée adresse MAC, représentée par douze chiffres hexadécimaux.
Les points d'accès permettent généralement dans leur interface de configuration, de gérer une liste de droits d'accès basée sur les adresses MAC des équipements autorisés à se connecter au réseau. Le filtrage MAC peut aussi être contourné. Une écoute passive du réseau permet de récupérer les adresses MAC reconnues par le réseau.

c)la Protection par les certificats
L'authentification basée sur les certificats désigne l'utilisation d'un certificat numérique pour identifier un utilisateur, une machine ou un périphérique avant de lui octroyer l'accès à une ressource, un réseau, une application, etc. Pour authentifier un utilisateur, cette méthode est souvent déployée conjointement à d'autres méthodes classiques comme l'authentification basée sur un nom d'utilisateur et un mot de passe.

1.7.1 Avantages des certificats

- Facilité de déploiement et gestion continue :
Aujourd'hui, la plupart des solutions basées sur des certificats sont fournies avec une plate-forme de gestion sur le cloud qui facilite les émissions de certificat pour les nouveaux employés. Cette solution séduit les administrateurs chargés en prime du renouvellement et de la révocation des certificats après le départ des collaborateurs. Grâce à l'automatisation des commandes et l'activation de l'installation en mode silencieux, les solutions qui s'intègrent à Active Directory simplifient encore davantage les processus de commande et d'émission.

Contrairement à certaines méthodes d'authentification comme la biométrie ou les jetons OTP, aucun matériel supplémentaire n'est nécessaire. Les certificats sont stockés en local sur la machine ou le périphérique. Outre les économies sur les coûts, la méthode facilite également la distribution, le remplacement et la révocation des jetons.

-Convivialité :
Entre renforcer la sécurité, ou réduire les coûts et la pénibilité pour les utilisateurs finaux, c'est toujours une affaire de compromis. On omet bien souvent ce critère, mais les certificats sont extrêmement simples à manier pour les utilisateurs finaux. Une fois le certificat installé (dans certains cas, l'opération s'effectue même automatiquement), il n'y a rien d'autre à faire. De plus, la plupart des solutions d'entreprise prennent déjà en charge l'authentification basée sur les certificats.

Autre avantage : l'utilisation des certificats permet une authentification mutuelle. En clair, les deux parties engagées dans une communication s'identifient elles-mêmes, qu'il s'agisse d'une communication entre deux utilisateurs, entre un utilisateur et une machine ou entre deux machines. Ainsi, avant qu'une connexion puisse être établie, un client doit prouver son identité pour accéder à l'intranet de l'entreprise et l'intranet doit prouver son identité au client.

La facon de s'authentifier avec certaficat est comme suit :
Authentification des utilisateurs :
-Ouverture de session Windows
-Accès aux e-mails d'entreprise, réseaux internes ou intranets
-Accès aux services cloud comme Google Apps, SharePoint et Salesforce
Authentification des machines et périphériques :
-Identification des machines sur site/sur le terrain qui doivent communiquer avec les services de back-end (bornes de paiement situées dans les magasins, par exemple).
-Identification de tous les ordinateurs portables et mobiles des employés avant d'autoriser

l'accès aux réseaux WiFi, aux VPN, passerelles, etc.
-Identification de tous les serveurs dans l'entreprise afin de permettre l'authentification mutuelle.

1.8 Sécurité renforcé

1.8.1 Mise en place d'un pare-feu

Un pare-feu(en anglais firewall), est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il mesure la prévention des applications et des paquets. Il a pour principale tâche de contrôler le trafic entre différentes zones en filtrant les flux de données entrant et sortant son but est de fournir une connectivité contrôlée et maîtrisée entre des zones différents.

1.8.2 Mise en place d'un VPN

Le VPN permet de simuler un réseau privé via internet en cryptant les paquets entre deux points distant une fois que le tunnel est crée à travers le réseau public (internet), entre deux machines (réseaux), ces derniers peuvent s'échanger des données de manière sécurisé, comme s'ils se trouvaient sur le même réseau local.
Le VPN permet aux entreprises de bénéficier d'une liaison sécurisée à moindre coût. Ils peuvent aussi utiliser les lignes spécialisées pour créer le VPN.

1.8.3 Le cryptage

La cryptographie est une méthode permettant de rendre illisible les informations, afin de garantir l'accès au distributeur authentifié uniquement. On distingue deux types de cryptage :

Cryptage symétrique : appelé aussi cryptage à clé secrète. Ce type de cryptage utilise la même clé pour crypter et décrypter le message. Le principal problème de cette technique est la distribution de la clé dans un réseau.
Cryptage asymétrique : ce type de cryptage utilise deux clés différentes, une rivée et n'est connue que de son propriétaire et une autre public et accessible par tout le monde.

Les deux clés (privé et public) sont liées par l'algorithme de cryptage utilisé. Un message crypté par une clé publique ne peut être décrypté qu'avec la clé privé correspondante. Le principal avantage de cette technique est de résoudre le problème de l'envoi de clé privé sur le réseau.

1.9 Conclusion

Une bonne compréhension de l'ensemble des concepts de bases de son sujet, permettra d'avoir une idée claire sur les réseaux informatiques et d'aborder son thème, en s'appuyant ainsi, sur une étude d'état des lieux. Dans le chapitre suivant, nous présenterons l'organisme d'accueil.

Chapitre 2

Présentation de l'organisme d'accueil

2.1 Introduction

L'étude de l'organisme d'accueil est une étape importante qui sert à représenter les contraintes sous lesquelles se réalisera notre projet. Dans ce chapitre, nous allons présenter l'entreprise SONATRACH, citer les différents départements qui la constituent et donner quelques informations qui nous seront utiles dans notre travail, tout en posant la problématique autours de laquelle tournera notre mémoire.

2.2 Présentation général de l'organisme d'accueil

2.2.1 Présentation de SONATRACH :

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

2.2.2 Historique et missions :

L'entreprise "SONATRACH" (Société Nationale pour le Transport et la Commercialisation des Hydrocarbures) a été créé le 31 Décembre 1963 par le décret n°63/491, les statuts ont été modifiés par le décret n°66/292 du 22 Septembre 1966, et SONATRACH devient "Société nationale pour la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures", cela a conduit à une restructuration de l'entreprise dans le cadre d'un schéma directeur approuvé au début de l'année 1981 pour une meilleure efficacité organisationnelle et économique, de ces principes SONATRACH a donné naissance à 17 entreprises : (NAFTAL, ENIP, ENAC,...etc.).

Après sa restructuration en 1982, et sa réorganisation en 1985, SONATRACH s'est recentrée sur ses métiers de base que constituent les activités suivantes : Exploration et recherche, Exploration des gisements d'hydrocarbures, Le transport par canalisation, La liquéfaction et la transformation de GAZ, La commercialisation [11].

SONATRACH est divisé en cinq branches différentes représentées dans la figure suivante (fig 2.1) :

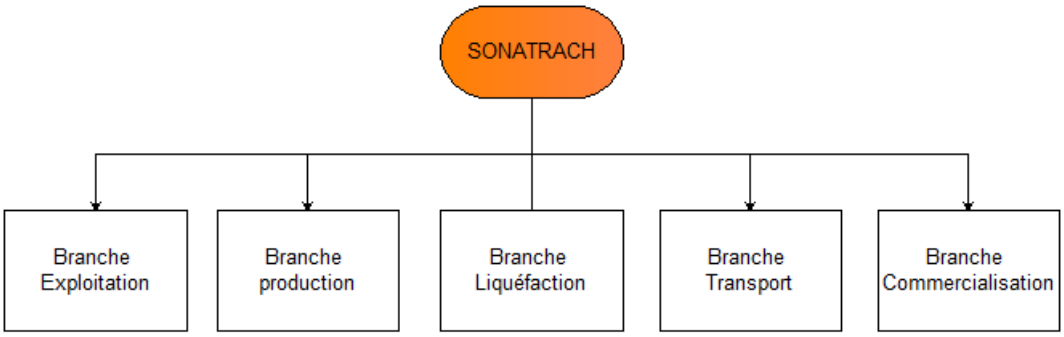

FIGURE 2.1 – Organigramme de la RTC [25].

2.3 Présentation de la région transport centre (RTC)

2.3.1 Structure de RTC (Région transport centre)

L'activité de Région transport centre (RTC) est en charge de l'acheminement des hydrocarbures pétroles brut, gaz et condensat vers les ports pétroliers, les zones de stockages et les pays d'exploitation. Les missions affectées à la branche transport par canalisation sont :
- La gestion et l'exploitation des ouvrages et canalisations de transport d'hydrocarbures.
- La coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation.
- La maintenance, l'entretien et la protection des ouvrages et canalisations.
- L'exécution des révisions générales, des machines tournantes et équipements.
- La gestion de l'interface transport des projets internationaux du groupe ou en partenariat.

La SONATRACH possède cinq Région transport des hydrocarbures :
- La Région transport Est (Skikda).
- La Région transport Centre (Béjaia).
- La Région transport Ouest (Arzew).
- La Région transport de Haoud-El-Hamra.
La Région transport d'Ain Amenas.

2.3.2 Organigramme de RTC (Région transport centre) :

Nous illustrons les directions et sous-directions dans le diagramme de la figure (fig 2.2) Comme suit :

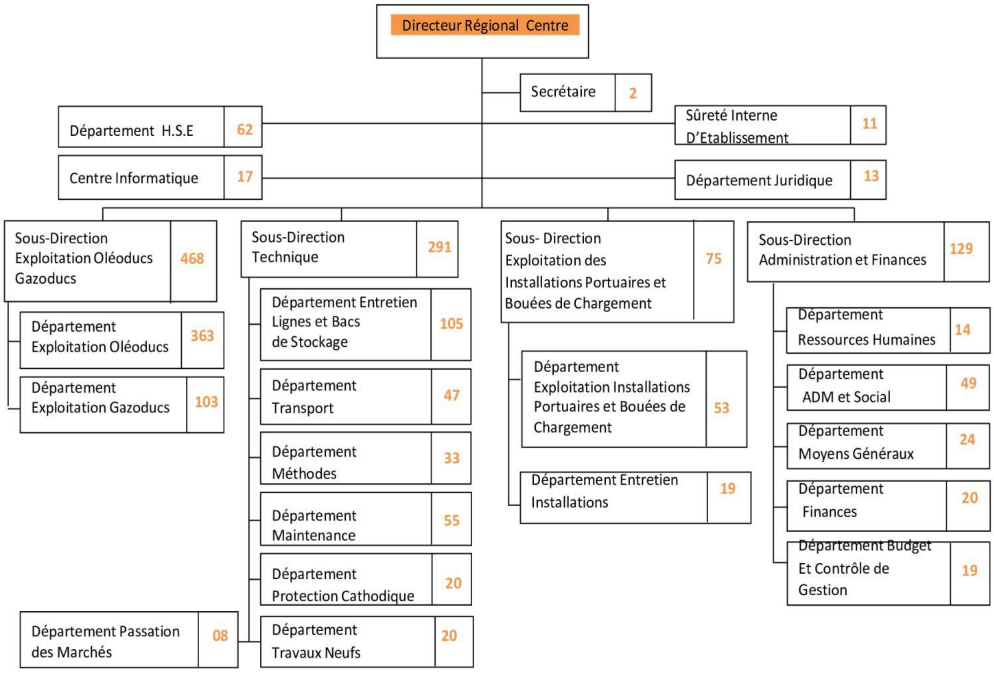

FIGURE 2.2 – Organigramme du centre informatique [25].

2.3.3 Organisation structurelle

L'organisation du centre ne cesse de subir des changements et l'évolution rapide de l'informatique pousse le centre à adopter des actions nouvelles à chaque fois afin de subvenir aux nouveaux besoins de l'entreprise. Pour mener à bien sa mission, le centre informatique s'organise en trois services tels qu'ils sont schématisés dans la figure suivante(fig 2.3) :

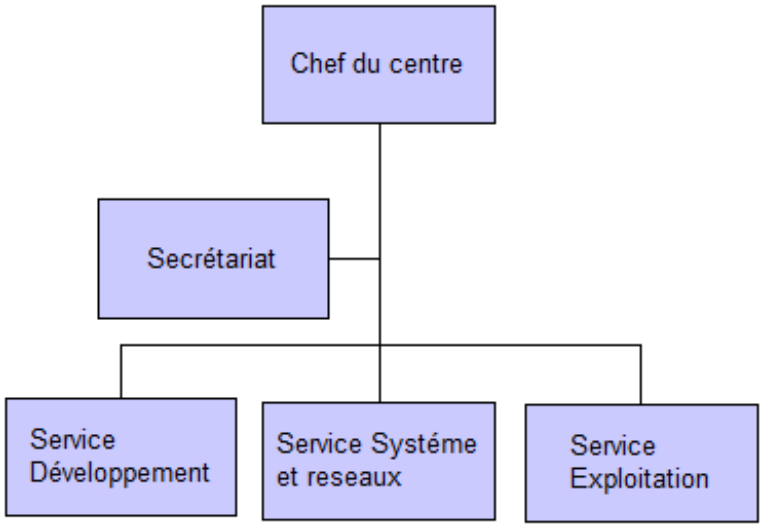

FIGURE 2.3 – Organigramme de la RTC [25].

2.4 Etude des lieux (réseau de l'entreprise)

L'architecture physique du réseau LAN est structurée suivant le modèle hiérarchique en 3 couches : une couche cœur (core layer), une couche distribution (distibution layer), et une couche d'accès (access layer), comme le représente la figure (fig 2.4).

2.4.1 Modèle Hiérarchique :

Le modèle hiérarchique est composé de trois couches présentées ci-dessous :
-La couche cœur de réseau (Core layer) :
'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 [12].

-La couche distribution (Distribution layer) :
Le rôle de cette couche a pour rôle 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 « liaison » 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 d'accès [12].

-La couche d'accès (Access layer) :
Cette couche qui est la dernière du modèle hiérarchique permet de connecter les périphériques des utilisateurs finaux au réseau. A ce niveau, on utilise des switches de niveau 2 car la configuration de ce type de switches pose moins de contraintes : le besoin en performance n'est plus vraiment une nécessité car chaque switch aura un nombre d'utilisateur égal à son nombre de ports (moins 1 ou 2 pour le trunk entre la couche d'Access et de Distribution). Les traitements restent basiques et ne demandent peu de ressources [12].

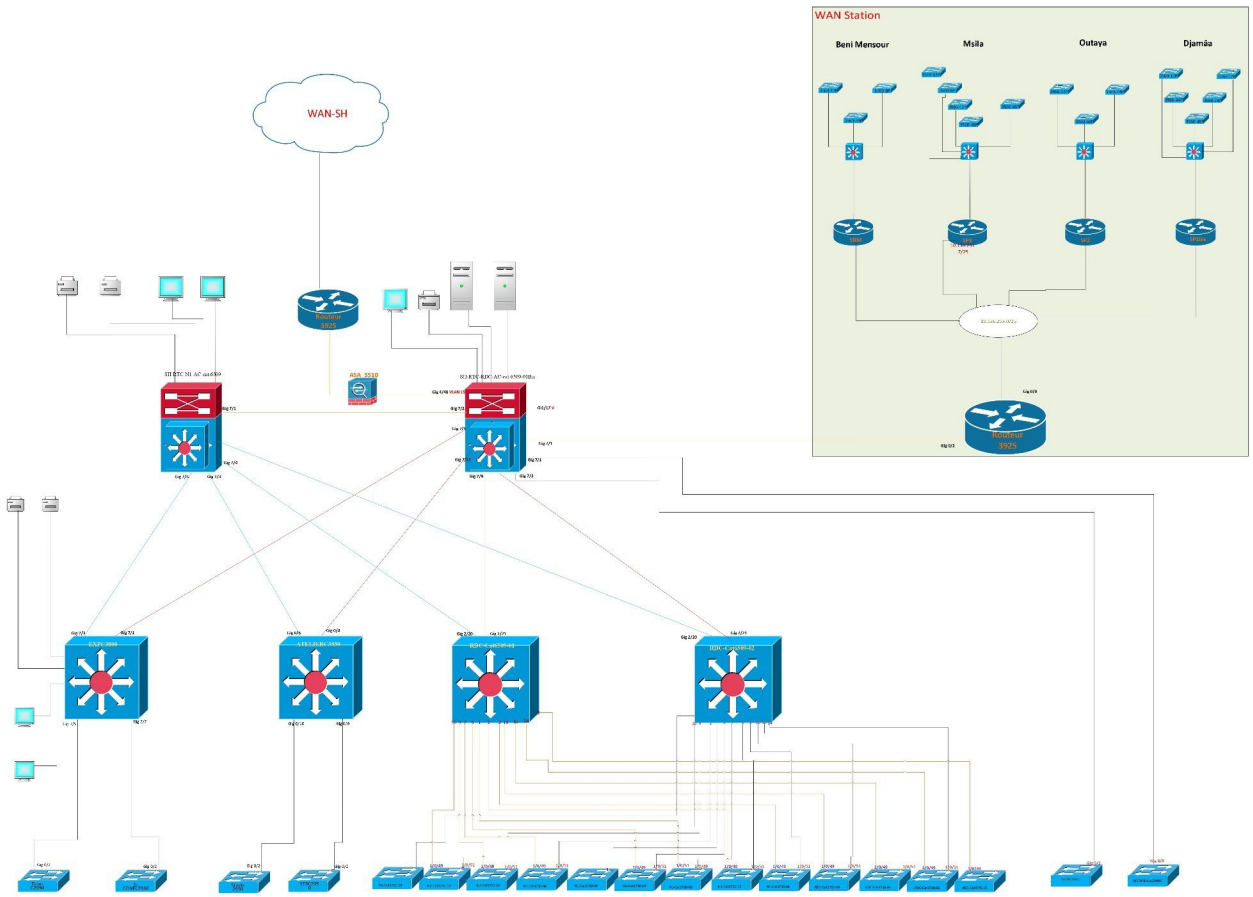

FIGURE 2.4 – Modèle hiérarchique du réseau de l'entreprise [25].

2.4.2 Commutateurs utilisés dans le réseau de la RTC :

Le réseau de la RTC utilise les commutateurs suivant :

-Catalyst Cisco 6509 :

La gamme Catalyst 6509 offre des moyens pour soutenir la capacité de la bande passante du système et des capacités améliorées de gestion des câbles. Elle fournit également des flux d'air d'avant en arrière qui est optimisé pour les conceptions allée chaude et froide dans le centre de données co-localisées et les déploiements de services. En outre elle offre une protection exceptionnelle des investissements en soutenant plusieurs générations de produits sur le même châssis, réduisant ainsi les coûts totaux de propriété. Le cadre Cisco Catalyst 6509 supporte à la fois la gamme Cisco Catalyst 6500 Supervisor Engine 32 et Cisco Catalyst 6500 Series Supervisor Engine 720 familles, avec LAN associés, WAN, et des modules de services [13].

FIGURE 2.5 – Commutateur Catalyst Cisco 6509 [13].

-Catalyst Cisco 3750 :

La gamme Cisco Catalyst 3750 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWiseTM, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de construire un système unique de commutation à haute disponibilité, vu comme un simple commutateur virtuel [14].

FIGURE 2.6 – Commutateur Catalyst Cisco 3750 [14].

-Catalyst Cisco 3550 :

Le commutateur Ethernet intelligent de la gamme Cisco Catalyst 3550 est une gamme de commutateurs multicouches empilables qui offrent une haute disponibilité, une qualité de service (QoS) et une sécurité pour améliorer les opérations réseau. Avec une gamme de configurations Fast Ethernet et Gigabit Ethernet, la gamme Cisco Catalyst 3550 est une option puissante pour les applications d'accès d'entreprise et métropolitaine [15].

FIGURE 2.7 – Commutateur Catalyst Cisco 3550 [15].

-Catalyst Cisco 2950 :
Série Catalyst 2950 commutateur Cisco configuration fixe, empilables, qui fournit à vitesse filaire Fast Ethernet et Gigabit Ethernet. Ce commutateur offre deux différents ensembles de fonctionnalités logicielles et une large gamme de configurations afin de permettre aux petites et moyennes entreprises et/ou les branches de l'entreprise dans des environnements industriels, pour obtenir la bonne combinaison pour l'environnement réseau [16].

FIGURE 2.8 – Commutateur Catalyst Cisco 2950 [16].

2.5 Problématique

De nos jours, la plupart des entreprises possèdent de nombreu postes informatiques qui sont en général reliées en eux par un réseau local. Ce réseau permet d'échanger des données entre les divers collaborateurs internes à l'entreprise et aussi de connecter à internet. Ouvrir l'entreprise vers le monde extérieur signifie laisser un porte ouverte à divers acteurs étrangers. Cette porte peut être exploité pour la destruction des données ou pour le piratage des données. C'est pour quoi on doit sécuriser notre réseau en utilisant :
- Serveur d'authentification.
- VPN
- Firewall

2.6 Conclusion

Dans ce chapitre, nous avons appris à mieux comprendre la structure et l'organisation du réseau de la RTC de Béjaïa, et d'étudier notre problématique afin de proposer les solutions adéquates et les objectifs à atteindre.

Chapitre 3

Implémentation de la solution et configuration

3.1 Introduction

Dans ce chapitre, nous allons passer à la troisième étape qui est l'implimentation de la solution et configuration. Cette phase est cruciale pour la mise en place de tout ce que nous avons vu et fait auparavant.Nous ferons appel aux VLANs pour le réseau câblé, à la norme 802.1x, en mettant en oeuvre une solution d'authentification autour de serveurs Radius.

3.2 Présentations des outils

3.2.1 Vmware

Pour la virtualisation nous avons utilisé VMware Workstation Pro 16, Elle nous a permet la création de plusieurs machines virtuelles au sein d'un même système d'éxploitation.

3.2.2 GNS3

Nous avons utilisé GNS3 (Graphical Network Simulator) pour l'émulation et la simulation de notre architecture réseaux.

3.2.3 Putty

PuTTY est un émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin. Il sert à l'accès et à l'administration à distance des équipements.

3.2.4 RDP (Remote Desktop Protocol)

Le protocole RDP (Remote Desktop Protocol) permet aux employés de se connecter à leur ordinateur de bureau lorsqu'ils travaillent à distance.

3.2.5 Wireshark

Wireshark est un outil de capture et d'analyse de paquets. Il capture le trafic du réseau local et stocke les données ainsi obtenues pour permettre leur analyse hors ligne.

3.2.6 Client windows

Nous avons 5 clients Windows pour faire nos différents tests, 5 PC sous Windows et un pour le client VPN et 4 pour nos diffèrent tests.

3.2.7 Serveur

Comme serveur, nous avons installé Windows server 2016. Il permet d'authentifier les différents utilisateurs finaux.

3.2.8 Pare-feu

Nous avons utilisé le par-feu pfSense, c'est un open source basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise.

3.2.9 IOU cisco

Cisco IOS sur UNIX (IOU) est une version entièrement fonctionnelle d'IOS qui s'exécute en tant que processus UNIX en mode utilisateur (Solaris). IOU est construit comme une image Solaris native et s'exécute comme n'importe quel autre programme. IOU prend en charge tous les protocoles et fonctionnalités indépendants de la plate-forme. En ce qui concerne la fonctionnalité, il est très similaire à GNS3 mais il ne nécessite pas autant de ressources que plusieurs routeurs virtuels fonctionnant sous dynamips.

3.3 L'architecture proposée

Topologie de notre solution implémentée sous GNS3 (fig 3.1) :

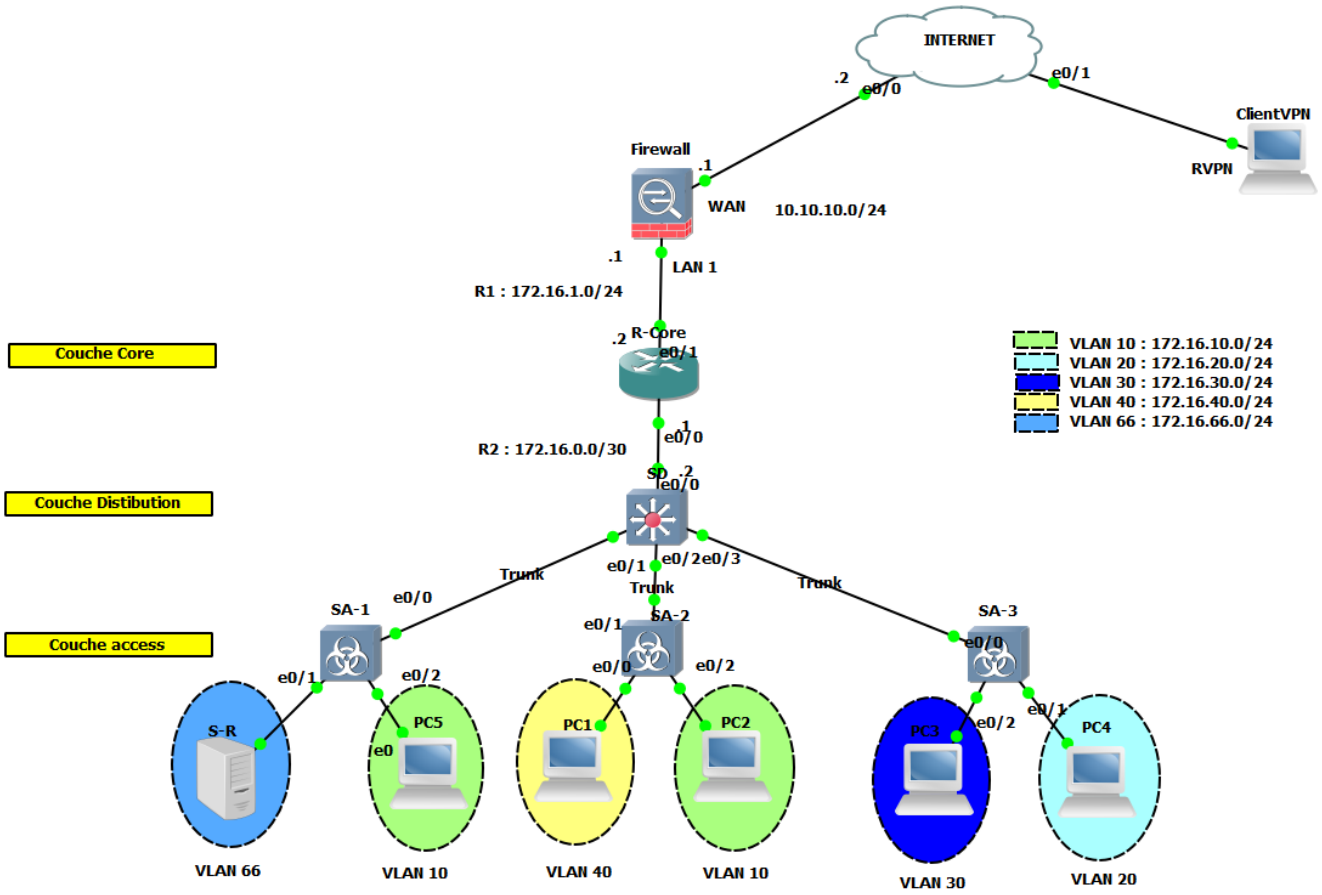

FIGURE 3.1 – Architecture Réseaux

	Numéro de VLAN	Déscription	Adresse IP
1	10	Département Informatique	172.16.10.0 /24
2	20	Département Juridique	172.16.20.0 /24
3	30	Département GRH	172.16.30.0 /24
4	40	Département Finance	172.16.40.0 /24
5	66	Manager (Vlan Native)	172.16.66.0 /24

Table 3.1 – Les VLANs utilisés

3.4 Virtuel Local Area Network (VLAN)

Nombreuse sont les entreprises à recourir à la technologie VLAN, afin d'améliorer la sécurité et les performances de leurs réseaux locaux.
Un VLAN ou réseau local virtuel est un regroupement de stations de travails indépendamment de la localisation géographique sur le réseau, ces dernières pourront communiquer comme si elles étaient sur le même segment.
Un VLAN permet de créer des domaines de diffusion (domaines de broadcast) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement, il existe plusieurs méthodes pour créer des VLAN :

a)VLAN par port : Également appelé VLAN de niveau 1, chaque port des commutateurs est affecté à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN.

b)VLAN par adresse MAC : ou VLAN par adresse IEEE sont des vlan de niveau 2, chaque adresse Mac est affectée à un VLANS, l'intérêt de ce type de VLAN est l'indépendance vis à vis de la localisation géographique.

c)VLAN par protocole : Dans ce cas, la communication ne se fera qu'entre les machines qui utilisent le même protocole, par application, c'est-à-dire par le numéro de port par exemple, ou par mot de passe suivant le login de l'utilisateur.

3.4.1 Les VLANs utilisés

Pour notre travail nous allons utilisées les Vlans sur le tableau ci-dessous :

3.5 Présentation de notre solution

Le standard 802.1x est une solution de sécurisation, mise au point par l'IEEE en juin 2001. Il permet d'authentifier les équipements connectés sur un port avant d'accéder à un réseau (sans fil ou filaire) grâce à un serveur d'authentification.Il repose sur le protocole EAP (Extensible Authentification Protocol) .
Le protocole EAP est intégré au protocole d'authentification PPP et crée une infrastructure généralisée supportant différentes méthodes d'authentification. Avec le protocole EAP standardisé, la compatibilité des méthodes d'authentification est plus simple. IEEE

802.1X est la norme utilisée pour passer l'EAP sur un réseau LAN filaire ou sans fil. L'encapsulation d'EAP sur IEEE 802.1x est connue sous le nom de "EAP over LAN" ou EAPOL. Le 802.1X se base sur trois éléments (fig 3.2) [17] :
-Le demandeur(Supplicant) : Ce terme désigne le dispositif client ou utilisateur qui doit être authentifié et souhaite accéder au réseau.
-Serveur d'authentification : Le serveur qui effectue l'authentification qui peut être un serveur RADIUS.
-Authenticator : Ce terme désigne le dispositif situé entre le supplicant et le serveur d'authentification.

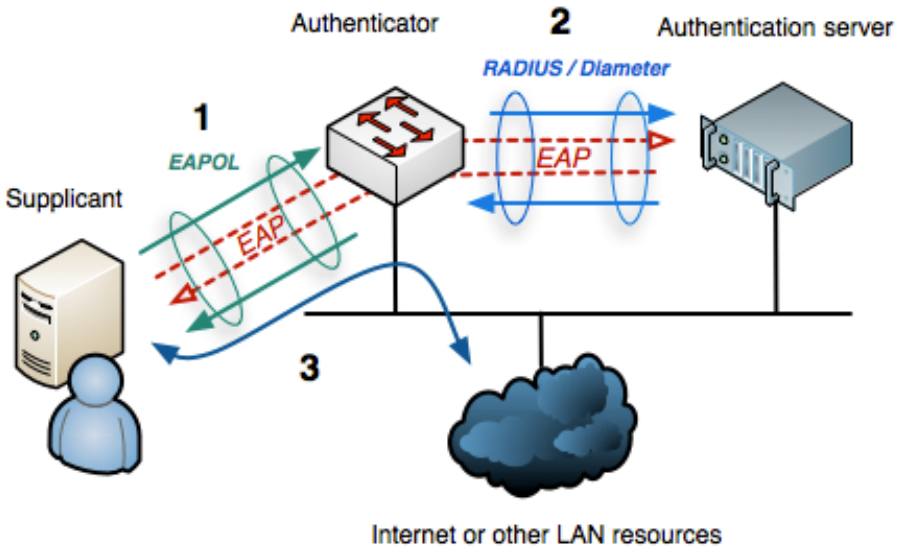

FIGURE 3.2 – Acteurs principaux de 802.1x [17].

3.6 Fonctionnement de notre solution

Le fonctionnement de notre solution se déroule comme suit :
802.1X est une norme IEEE qui implémente l'authentification basée sur les ports. Si un port d'un commutateur réglé en mode 802.1x peut se trouver dans deux états distincts :
- État "contrôlé" si l'authentification auprès du serveur RADIUS a réussi.
- État "non contrôlé" si l'authentification a échoué.
La réussite ou l'échec de l'authentification va donc ouvrir ou fermer le port à toute communication. Un port ouvert va, par exemple, permettre au client final d'obtenir une adresse IP auprès d'un serveur DHCP.
Dans des implémentations plus cloisonnées, le serveur RADIUS indiquera par exemple au client RADIUS dans quel VLAN placer le client final.

Au démarrage de la communication "EAP (Start)", le client final est prié d'envoyer ses identifiants au serveur RADIUS "EAP (Response Identity)", "RADIUS (Access-Request)" Or, à ce moment là, le client final ne connaît pas l'adresse du serveur RADIUS du réseau. Il ne dispose peut-être même pas d'adresse IP. De même, le port du commutateur sur lequel il est connecté est censé être fermé.

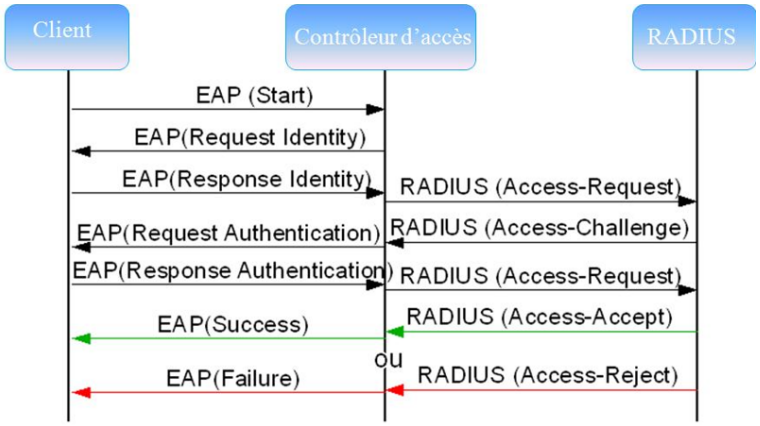

FIGURE 3.3 – Protocol EAP et Radius.

En réalité, le port contrôlé du commutateur n'est pas totalement fermé. Il va laisser passer le protocole EAP. Le client final peut donc envoyer son identité dans un paquet EAP au commutateur "EAP (Response Identity)". Celui-ci le retransmet, encapsulé dans un paquet au format RADIUS , au serveur RADIUS, le serveur RADIUS reçoit le paquet et interroge sa base de données. Il renvoie le résultat de cette interrogation au commutateur , sous forme d'un commandement d'ouverture du port "RADIUS (Access-Accept)", éventuellement assorti d'un numéro de VLAN dans lequel placer le client final. A partir de ce moment seulement, il peut y avoir d'autres trames échangées entre le client final et le reste du réseau, comme une trame de requête DHCP par exemple (fig 3.3).

3.7 Méthodes d'authentification de 802.1x

Le protocole 802.1x implique une communication indirecte entre le poste de travail et le serveur Radius. La communication entre le poste de travail et le NAS s'appuie sur le protocole EAP.

3.7.1 Protocole EAP

Le protocole EAP (Extensible Authentication Protocol) est une norme IETF(Internet Engineering Task Force), qui définit une infrastructure permettant aux clients d'accès réseau et aux serveurs d'authentification.
Microsoft Windows utilise EAP pour authentifier l'accès réseau pour les connexions PPP (Point-to-Point Protocol) (accès distant et réseau privé virtuel) et pour l'accès réseau basé sur IEEE 802.1X aux commutateurs Ethernet et points d'accès sans fil[18].
On distingue deux types de trafic EAP :
– Entre le système à authentifier et le point d'accès (support : 802.11a, b, g ou 802.3) :**EAP over LAN (EAPOL)**.
– Entre le point d'accès et le serveur d'authentification (de type RADIUS) :**EAP over Radius**[18].

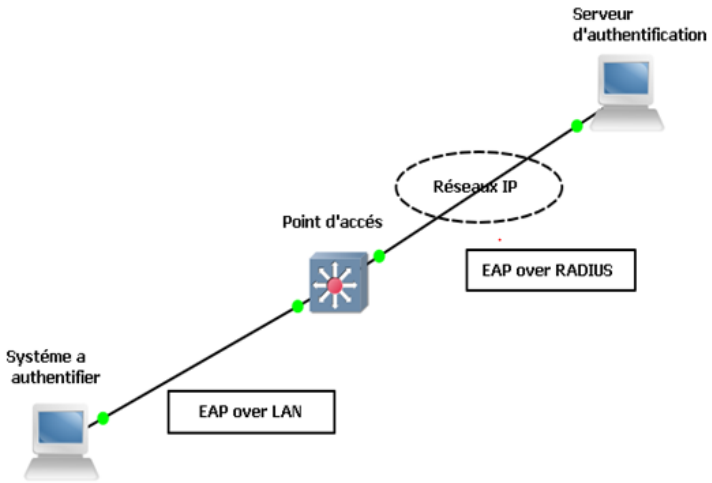

FIGURE 3.4 – Type de EAP[18].

3.7.2 Méthodes associées à EAP :

Les méthodes associées à EAP sont les suivantes :
a)EAP- TLS (EAP Transport Layer Security) : Apparaît sous forme de carte à puce ou d'autres propriétés de certificat dans le système d'exploitation. EAP-TLS peut être déployé en tant que méthode interne pour PEAP ou en tant que méthode EAP autonome.

b)EAP-MD5 (EAP Message Digest 5-Challenge) :L'utilisateur va être authentifié via son login et son mot de passe mais ce dernier ne sera pas transmis en clair sur le réseau. Grâce au mécanisme de challenge / réponse, le serveur envoie un challenge au client, celui renvoie son mot de passe associé au challenge, le serveur compare le résultat avec le mot de passe qu'il détient dans sa base plus le challenge envoyé. Si le résultat est identique alors l'accès est autorisé, sinon il est refusé.

c)LEAP (Lightweight EAP) : Est une implémentation propriétaire d'EAP conçu par Cisco systems assurant une authentification simple par mot de passe via une encapsulation sécurisée, ce protocole est vulnérable aux attaques (cryptage MD5) sauf si l'utilisateur utilise des mots de passe complexes.

d)PEAP : est un protocole propriétaire développé par Microsoft, Cisco et RSA Security.Ici seul le serveur d'authentification dispose d'un certificat numérique. Il le transmet au client qui va pouvoir l'authentifier. Un tunnel sécurisé TLS est alors établit entre les deux parties. Le client va s'authentifier via une encapsulation sécurisée, ce protocole est vulnérable aux attaques (cryptage MD5) sauf si l'utilisateur utilise des mots de passe complexes.

e)EAP-FAST (EAP-Flexible Authentication via Secure Tunneling) : Est une proposition de Cisco Systems pour fixer les faiblesses de LEAP en garantissant une flexibilité d'authentification via une encapsulation sécurisée .

3.8 Protocoles de transport sécurisés

Un protocole de transport sécurisé permet de porter l'information d'un lieu à un autre suivant des règles prédéfinies sans que l'objet transporté ne soit en danger. Étant donné que la majorité des réseaux utilisés à travers le monde sont de type TCP/IP et que le choix des entreprises se porte souvent vers ce type de réseau, nous présentons les protocoles sécurisées suivants :

a) Protocole PPP : Le protocole point à point (PPP) est un protocole de liaison de données assurant l'échange de données de manière fiable sur une liaison point à point (par exemple, une liaison RTC). Sa principale caractéristique est, une fois la liaison établie et configurée, de permettre à plusieurs protocoles de transférer des données simultanément. De ce fait, ce protocole est très utilisé dans l'environnement de l'internet[19].
b) Protocole PAP : PAP est un protocole réseau bidirectionnel ayant lieu en deux étapes et qui n'utilise pas le chiffrement : les noms d'utilisateur et mot de passe sont envoyés en clair dans le réseau informatique . S'ils ont acceptés, la connexion est autorisée. L'authentification a lieu une seule fois.
configuration-des-protocoles-reseau-pap-et-chap[20].
c) Protocole CHAP :Le protocole PAP procède à une seule authentification lors de l'établissement de a connexion réseau,le protocole CHAP effectue des vérifications régulières pendant l'existence de la liaison[21].
d) Protocole MS-CHAP :Noté parfois MS-CHAP version 1.Ce protocole propose une fonction de hachage propriétaire permettant de stocker un haché du mot de passe sur le serveur.
Le protocol MS-CHAP version 1 souffre malheureusement de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaires, ce qui a mené à une nouvelle version nommée MS-CHAP version2[22].

e) Protocole MS-CHAP-v2 :Cette méthode définit une nouvelle version dite d'authentification mutuelle,permettant au serveur d'authentification et la machine distante d'identifier leurs identités respectives[23].

3.9 Active directory

Active Directory Domain Services (AD DS) est supporté par Windows Server et à pour but la gestion d'annuaires, il est utilisé pour toutes les tâches d'administration demandant un forte composant réseau, en particulier pour la création de domaines. AD DS n'est pas installé par défaut et au cours de son installation, un domaine doit être défini.

3.10 Protocol RADIUS (Remote Authentication Dial In User Service

RADIUS (acronyme de Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des demandes d'authentification relayées par des équipements de réseau, comme des commutateurs ou bornes Wifi, considérés alors comme ses clients. Par extension, un serveur qui centralise des demandes d'authentification et

les soumet à un service d'annuaire LDAP ou à un service de base de données SQL est appelé serveur RADIUS. RADIUS interroge une base de données d'authentification et d'autorisation qui peut être un domaine Active Directory, une base LDAP ou une base de données SQL. Ces bases ou annuaires peuvent se trouver sur le serveur lui-même ou sur un serveur tiers. Certaines implémentations de RADIUS disposent d'une base de données en propre. A l'origine, RADIUS était surtout utilisé pour l'identification des clients des FAI, ses capacités de comptabilisation des accès (accounting) permettant notamment la journalisation des accès et leur facturation. RADIUS a été utilisé par la suite en entreprise pour l'identification des clients finals WIFI et pour l'identification des clients finals câblés.

Rôle serveur RADIUS :

Rôles du serveur RADIUS En premier lieu, RADIUS doit authentifier les requêtes qui sont issues des clients finals, via les clients RADIUS. Cette authentification se basera soit sur un couple identifiant/mot de passe, soit sur un certificat. Cela dépendra du protocole d'authentification négocié avec le client final. En deuxième lieu, RADIUS a pour mission de décider quoi faire du client authentifié, et donc de lui délivrer une autorisation, un "laissez-passer". Pour ce faire, RADIUS envoie des informations (on parle "d'attributs") aux clients RADIUS. Un exemple typique d'attribut est un numéro du VLAN dans lequel placer le client authentifié et autorisé. Enfin, en bon gestionnaire, RADIUS va noter plusieurs données liées à la connexion, comme la date et l'heure, l'adresse MAC de l'adaptateur réseau du client final, le numéro de VLAN...). C'est son rôle comptable ou "d'accounting". RADIUS est donc un serveur d'authentification, d'autorisation et de comptabilité. De façon imagée, c'est le "chef d'orchestre" des connexions 802.1X et les clients RADIUS sont ses sbires... En ce sens, il se range dans le modèle AAA (Authentication, Authorization, Accounting). NPS (Network Policy Server) est le nom du service RADIUS des systèmes Microsoft Windows 2008 Server, en remplacement du "Service d'Authentification Internet" de Windows 2003 Server. D'autres solutions propriétaires existent, comme CISCO ACS (Access Control Server). Différentes versions libres de RADIUS existent également, comme FreeRADIUS (sous Linux ou Windows) ou OpenRADIUS (sous Linux). RADIUS peut aussi servir à centraliser les accès sécurisés aux pages ou aux terminaux de paramétrage de tous les équipements réseau : commutateurs, routeurs, bornes wifi, contrôleurs wifi, etc.

Le client RADIUS
Le client RADIUS Dans le schéma général d'une connexion 802.1x, l'élément central est l'équipement de réseau (commutateur, borne wifi, ...) désigné comme client RADIUS. Cet équipement doit donc être en capacité de gérer le protocole 802.1x et le protocole d'authentification EAP.

3.10.1 Fonctionnement du protocol RADIUS :

RADIUS (acronyme de Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des demandes d'authentification relayées par des équipements de réseau, comme des commutateurs ou bornes Wifi, considérés alors comme ses clients. Par extension, un serveur qui centralise des demandes d'authentification et les soumet à un service d'annuaire LDAP[24].

3.11 Configuration des serveurs

3.11.1 Configuration de Active Directory

Création de l'unité d'organisation dans Active Directory : afin d'assurer la flexibilité nous avons opté pour la création des unités d'organisation, une unité d'organisation centrale (Sonatrach Central Alger) et dans Sonatrach Central Alger on a créé une Unité d'organisation (Sonatrach Béjaia) qui contient deux autre unité d'organisation (Ordinateurs et Utilisateurs) (fig 3.5) (fig 3.6).

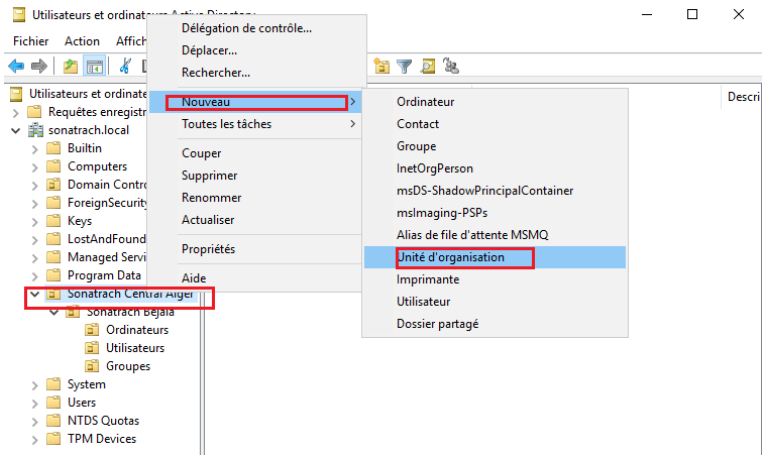

FIGURE 3.5 – -Création d'une unité d'organisation dans Active Directory

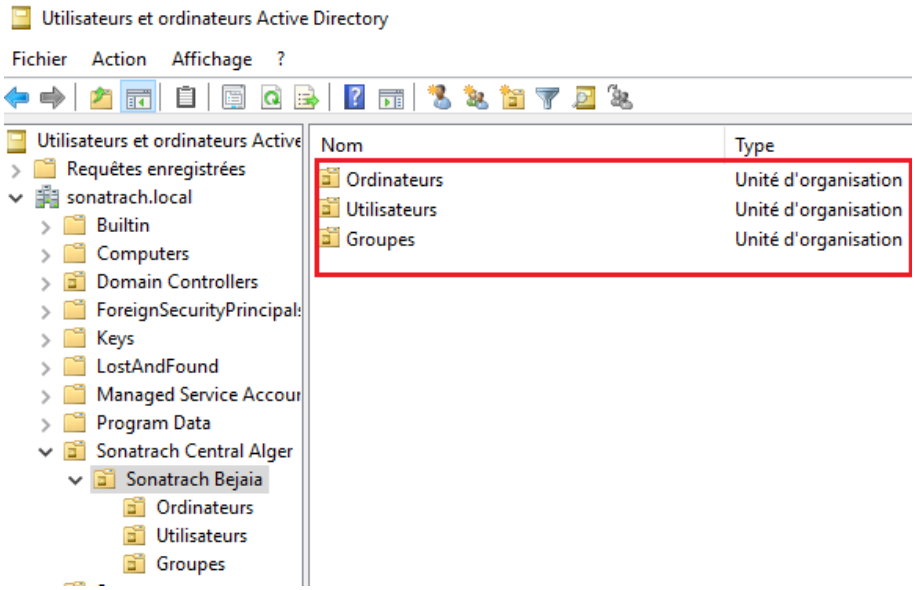

FIGURE 3.6 – Les unités d'organisations créer

-Création des groupes VLAN Radius : aprés avoir créé l'unité d'organisation « Utilisateur » dans cette dernière nous allons créer des groupes et des utilisateurs (fig 3.7), (fig 3.8).

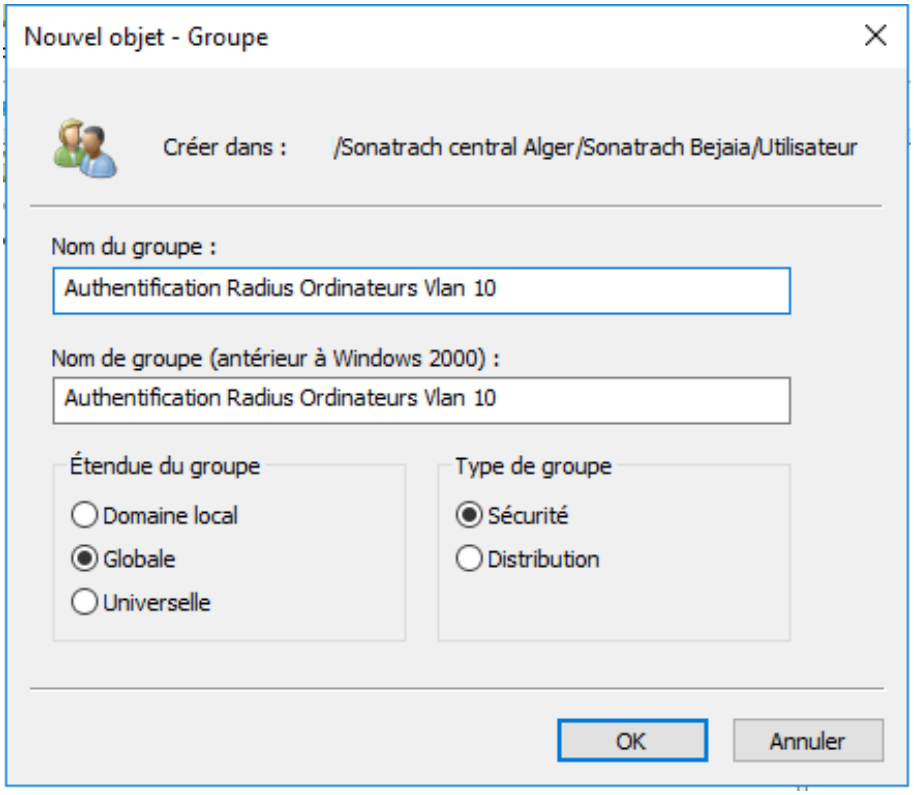

FIGURE 3.7 – Création d'un groupe dans Active Directory

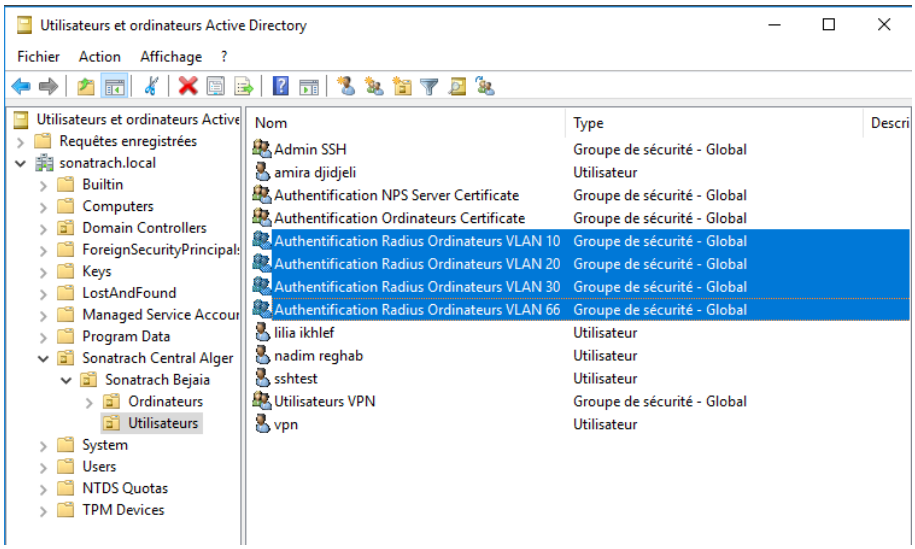

FIGURE 3.8 – les groupes VLANs radius crée

- Création d'utilisateur dans Active Directory : pour crée un utilisateur dans active Directory il suffit d'un clique droit sur l'unité d'organisation Utilisateur, nouveau, utilisateur (fig 3.9),(fig 3.10).

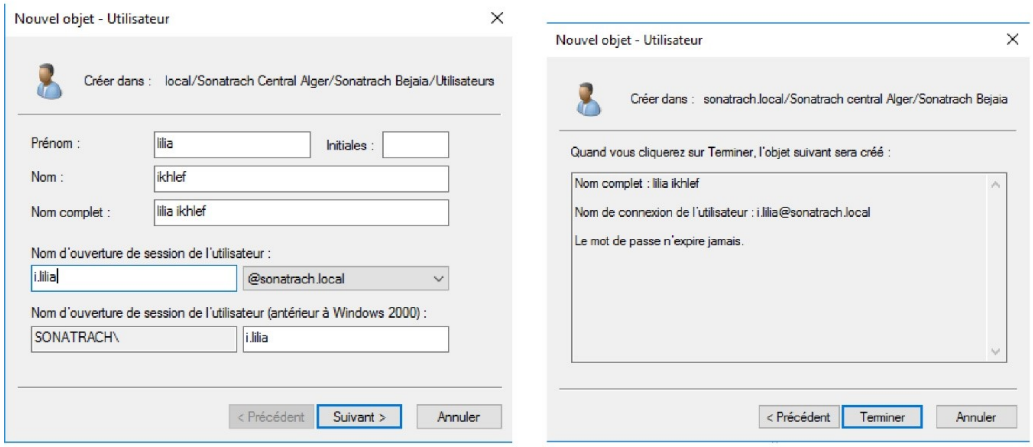

FIGURE 3.9 – Création d'un utilisateur dans Active Directory.

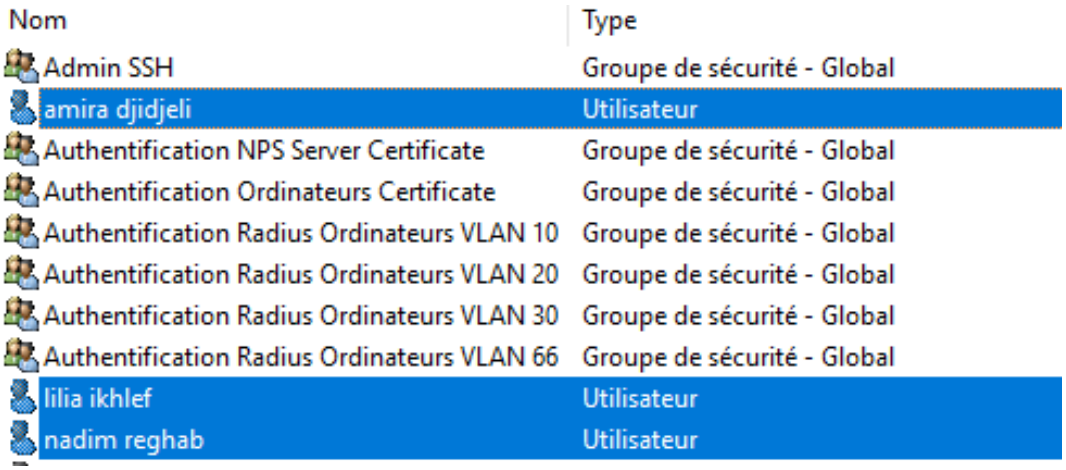

FIGURE 3.10 – les utilisateurs crées

-Créations d'une stratégie de groupe d'objet (GPO) : dans cette partie nous allons créer une GPO appelée " DOT1XCLIENT", qu'on applique sur l'unité d'organisation Ordinateur (3.11).

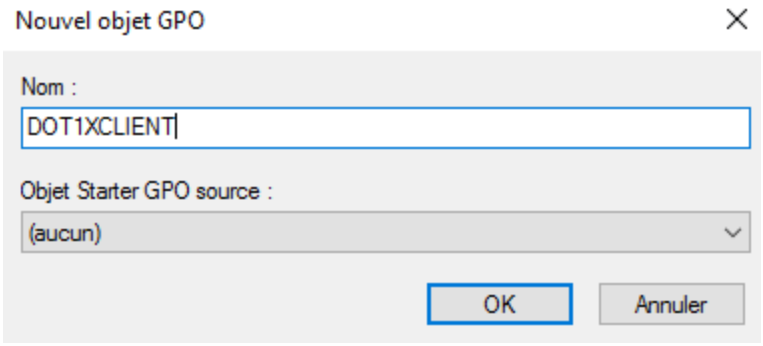

FIGURE 3.11 – Création d'une nouvelle GPO

Dans la figure (fig 3.12) on voit bien que la GPO à été créé dans l'unité d'organisation Ordinateur.

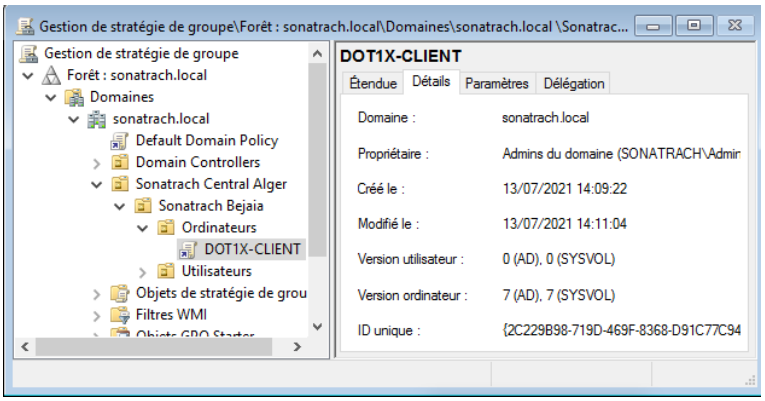

FIGURE 3.12 – GPO DOT1X-CLIENT

- Configuration de la GPO : pour la configuration de la GPO , on procède comme suit :
+ Activation automatique des services : mettre la configuration des réseaux câblé automatique (fig 3.13).

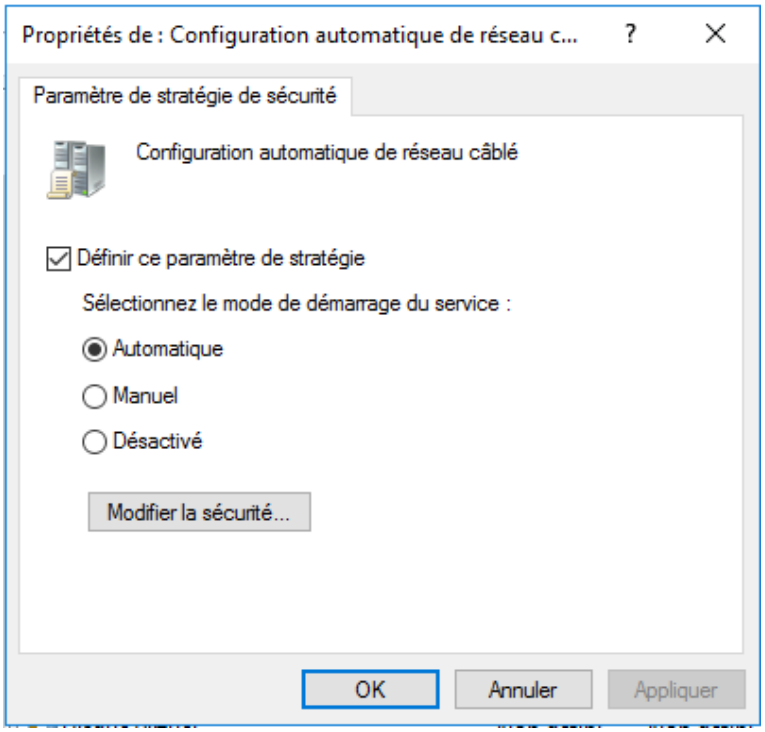

FIGURE 3.13 – Activation automatique des services

-Configuration du serveur DNS
Configuration d'un hote dns Nous allons ajouter un nom pour le firwel"pf.sonatrach.local" (fig 3.14) (fig 3.15).

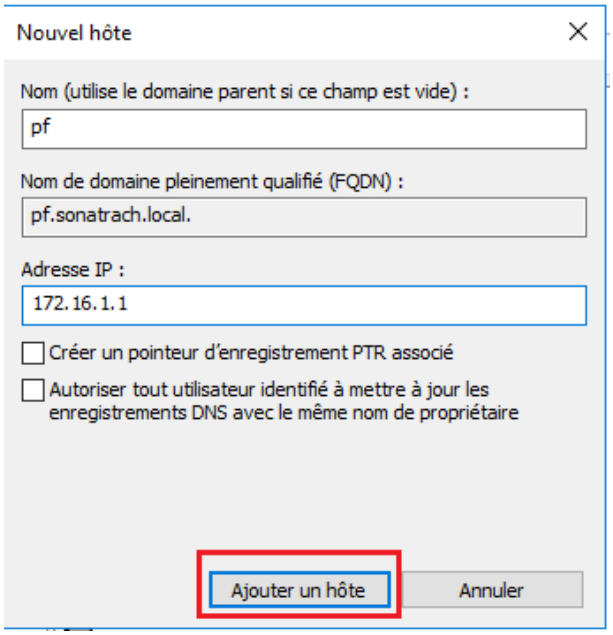

FIGURE 3.14 – Configuration du dns d'un hote

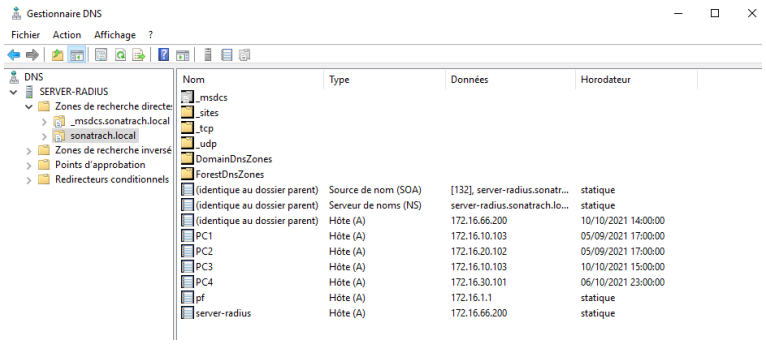

FIGURE 3.15 – Serveur DNS

- Configuration du serveur DHCP : lors de la configuration du serveur DHCP, un nom et un intervalle d'adresses doit être mentionnée comme l'affiche la figure ci-dessous (fig 3.16).

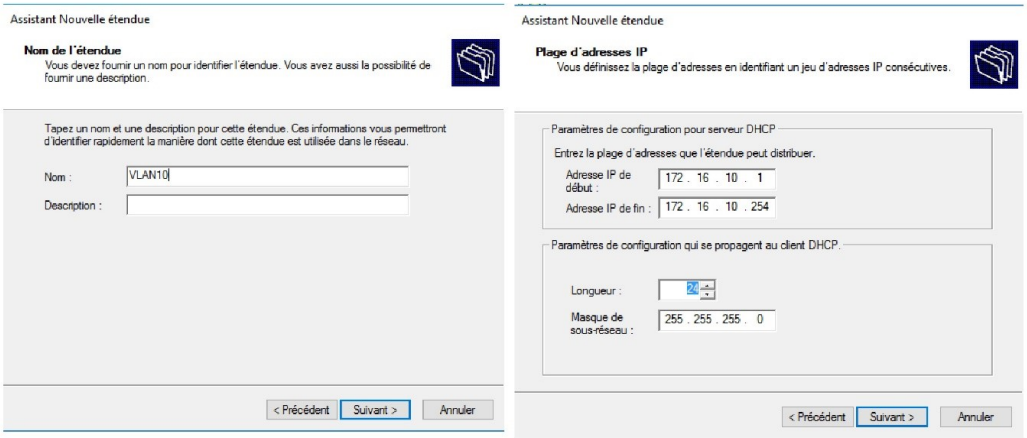

FIGURE 3.16 – Configuration d'une plage d'adresse du serveur DHCP

L'étape suivant consiste à exclure une plage d'adresse, on a réservé l'intervalle d'adresse « 172.16.10.1, 172.16.10.100 », tous les PC dans le VLAN 10 est doté d'une adresse dans l'intervalle « 172.16.10.101, 172.16.10.254» comme le présente les deux figures ci-dessus (fig 3.17) , (fig 3.18).

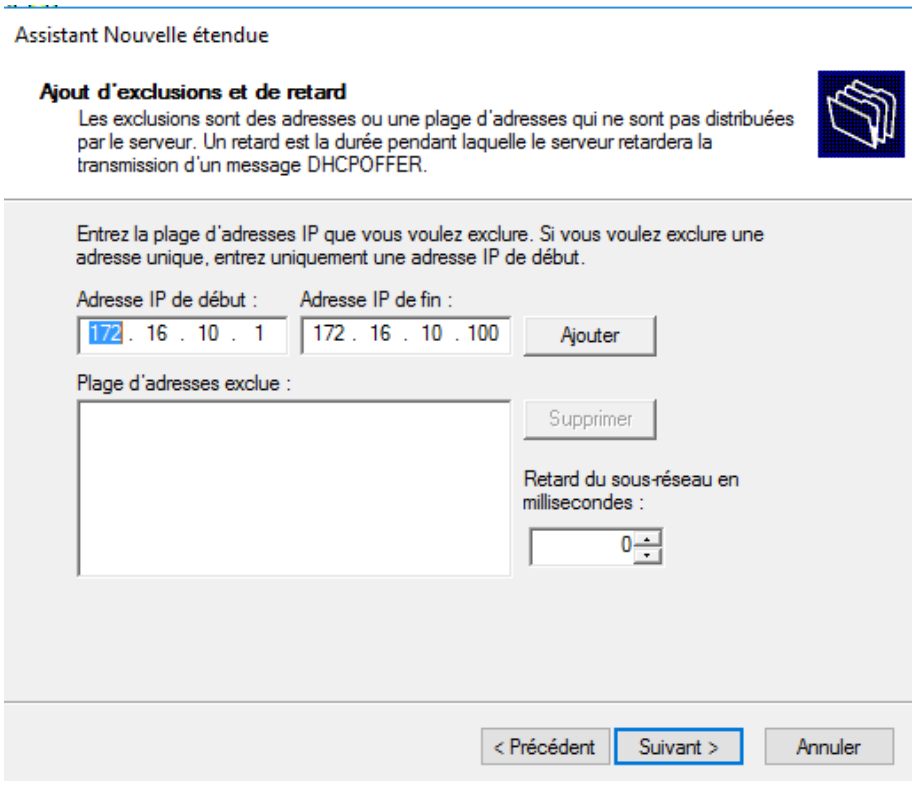

FIGURE 3.17 – Exclusion d'adresse

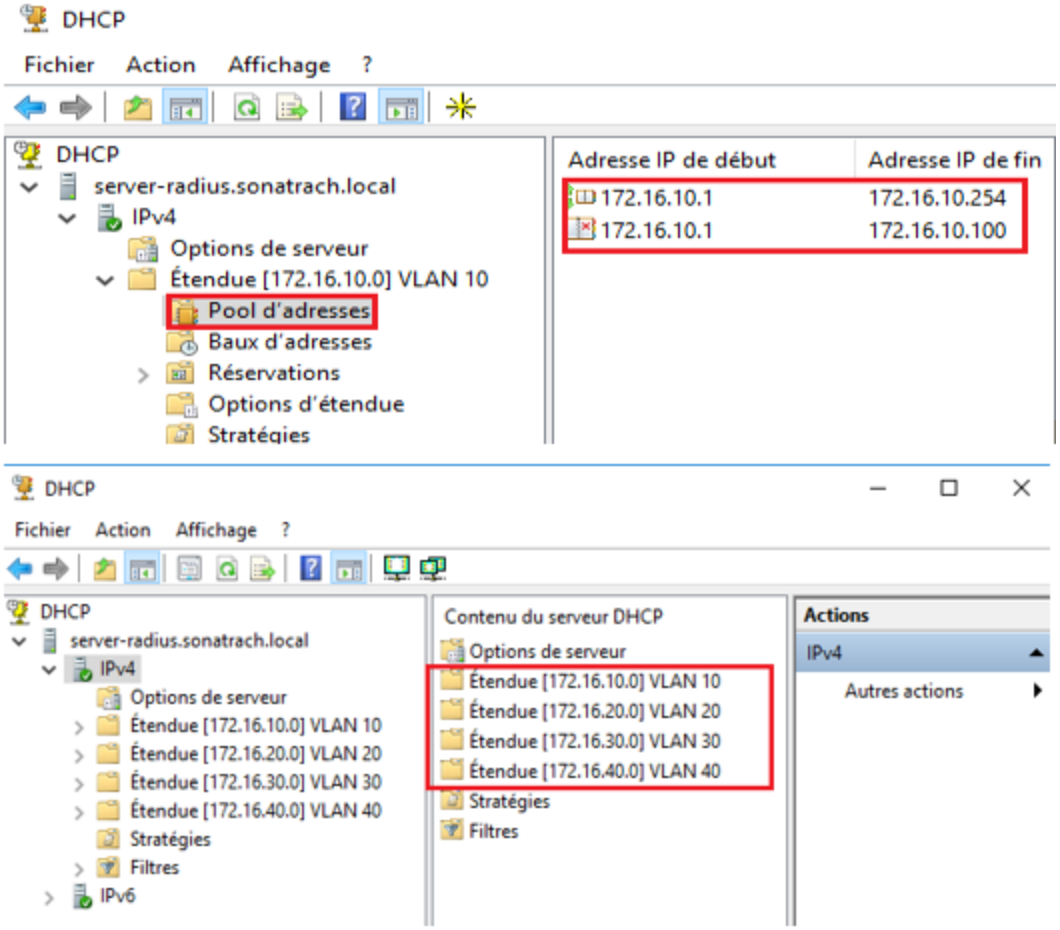

FIGURE 3.18 – Ensemble des plages d'adresses

- Configuration AD certificate :

+ Création des groupes Certificats : pour notre travaille nous allons créér deux groupe de certificat un groupe de certificat pour le serveur. Et un autre groupe de certificat pour les ordinateurs (fig 3.19).

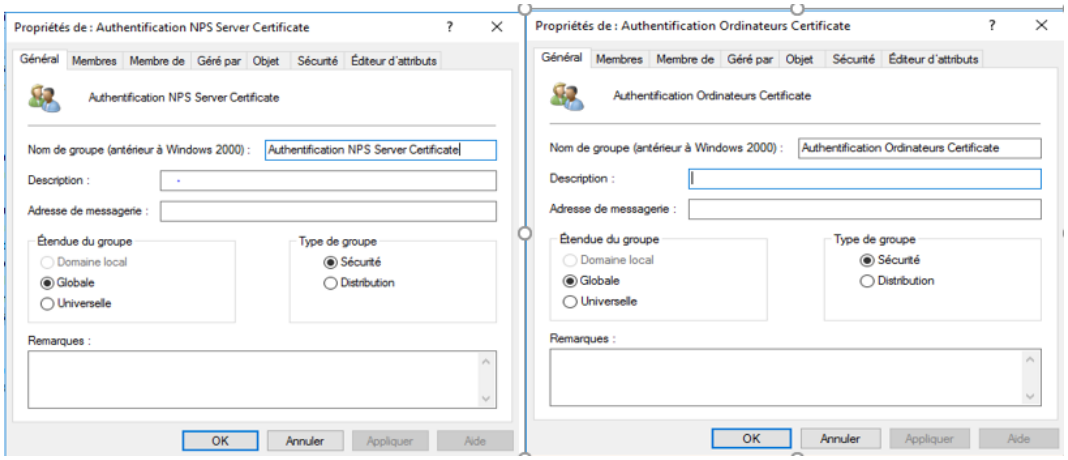

FIGURE 3.19 – Création du groupe certificat server et ordinateur

+ Certificat server : pour les certificats on a besoin de deux certificat un certificat pour le serveur et un autre pour les stations de travail, dans le dossier modèle de certificat on a dupliqué le serveur RAS et IAS puis on l'a renommé "Certificate Server Radius" (fig 3.20) (fig 3.21).

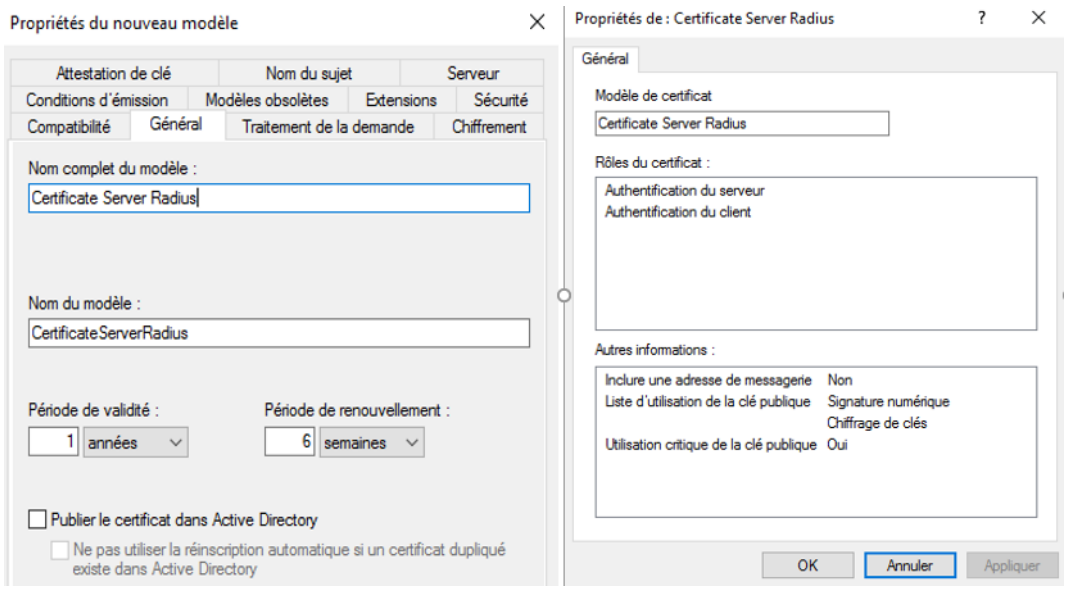

FIGURE 3.20 – Vue générale de (certificat server)

+ **Certificat Pc (Station de travail) :** dans cette étape on a dupliquer le modéle "Authentification de station de travail" puis on l'a renommé Certificate pour les stations de travail (fig 3.21).

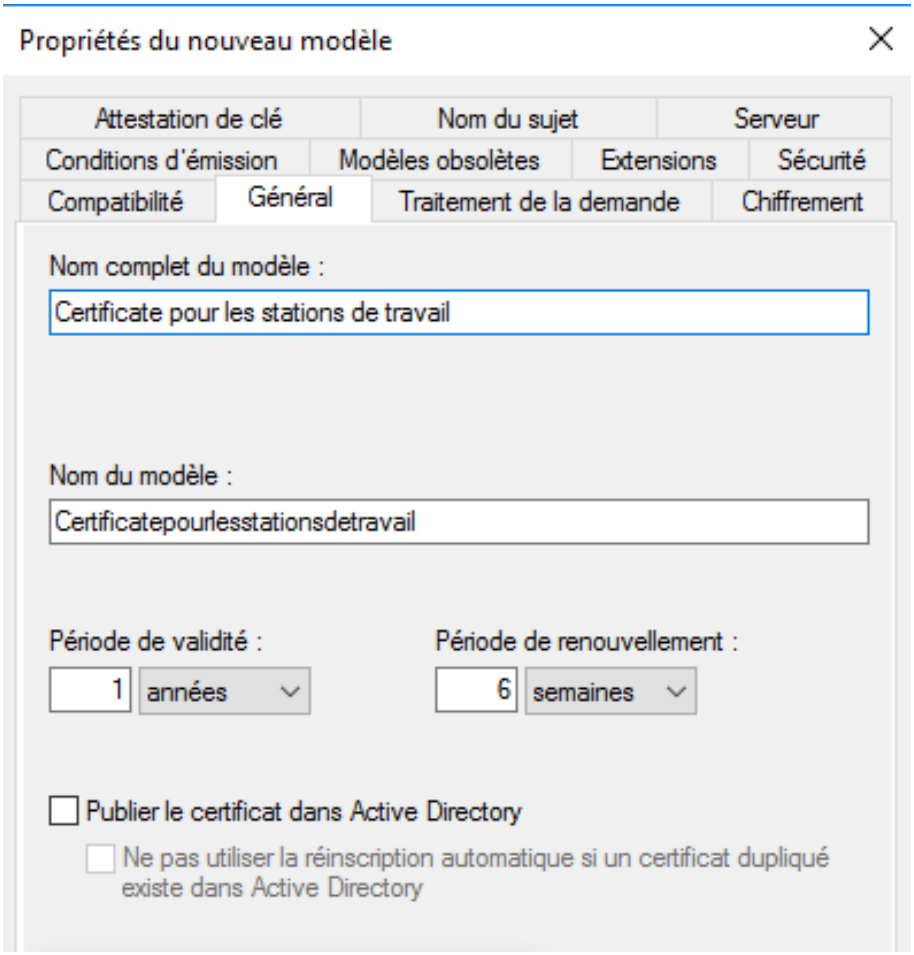

FIGURE 3.21 – Vue général du modèle certificat pour les stations de travaille

- Activer la distribution du certificat automatiquement : nous allons activer la distribution automatique des certificats, pour chaque PC une certification sera délivrée automatiquement(fig 3.22) .

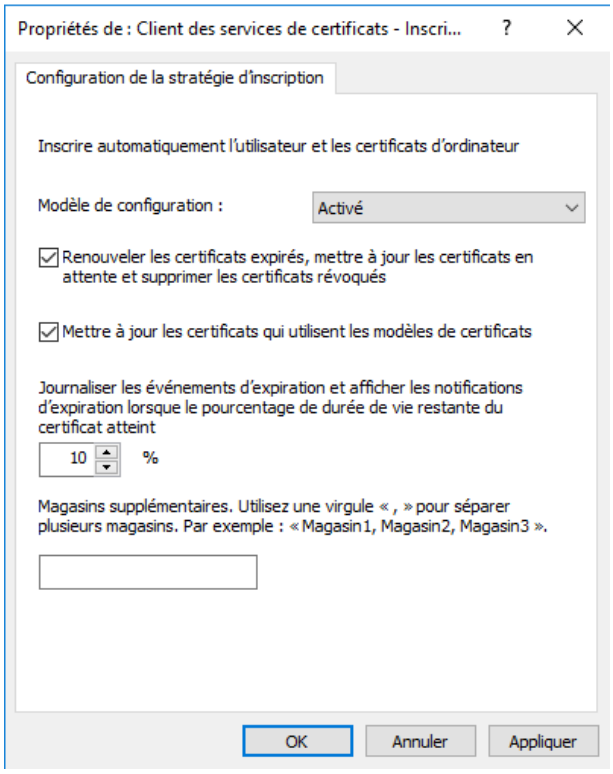

FIGURE 3.22 – Activation automatique des certificats

+ Création d'une nouvelle stratégie des réseaux câblés dans le dossier (paramètre Windows -paramètre sécurité - stratégie de réseau filaire) un clique droit est nécessaire pour créer la stratégie global(fig 3.23).

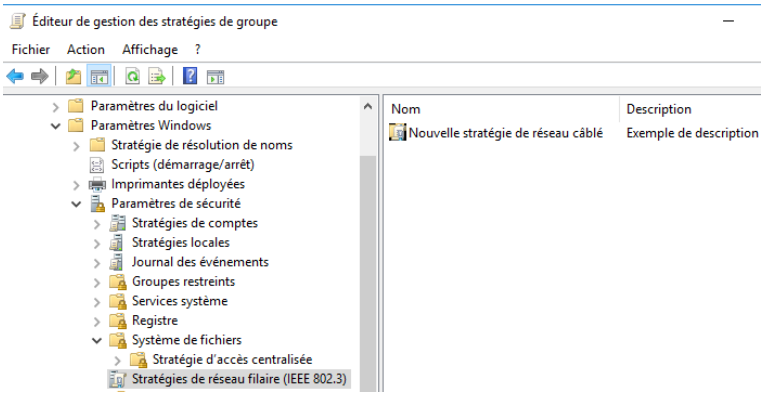

FIGURE 3.23 – Stratégies de réseau câblé

Apres avoir créé cette dernière on va apporter certain modification pour notre cas on nous allons choisir le protocole PEAP pour la méthode d'authentification et pour le mode d'authentification nous allons choisir de l'appliquer sur les hôtes (Ordinateur) (fig 3.24).

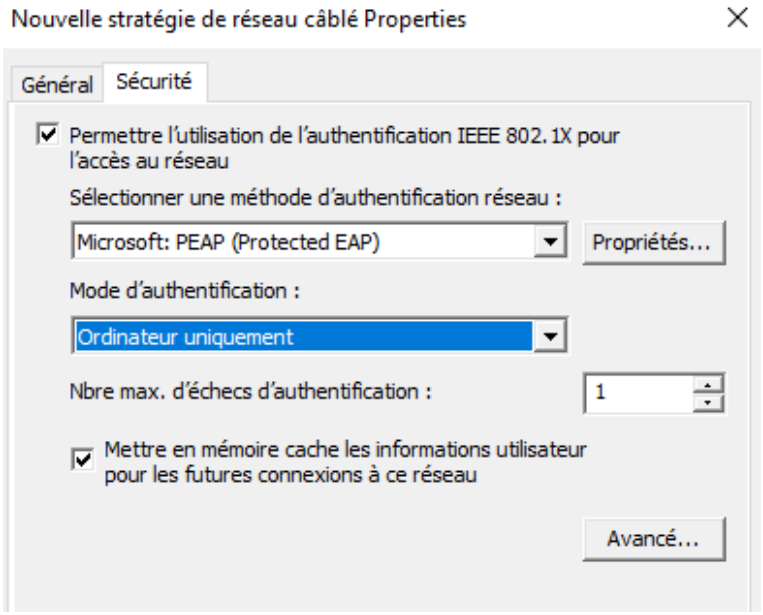

FIGURE 3.24 – Choix d'une méthode et d'un mode d'authentification

Nous allons apporter d'autre modification au niveau de la méthode d'authentification EAP, choisir la méthode d'authentification par certificat, car notre solution comporte sur l'authentification des hôtes, choisir (Carte à puce ou certificat) puis cocher la case (Activer la connexion rapide) (fig 3.25).

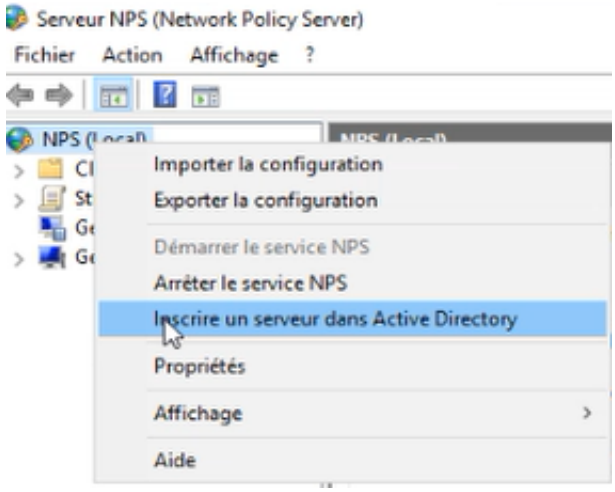

FIGURE 3.25 – Choix d'une méthode d'authentification

- Configuration RADIUS et le triple AAA : dans notre travaille le serveur Radius est le Network Policy Server (NPS), lorsque on configure le serveur NPS (Network Policy) comme un serveur RADIUS , NPS effectue l'authentification, autorisation et la gestion des demandes de connexion pour le domaine. Les étapes sont la suivante :
+ Inscrire NPS dans active directory : pour que le serveur NPS aura l'accès au infirmation d'identification et des utilisateur finaux dans Active Directory, Le serveur NPS doit être inscrit dans (AD) (fig 3.26).

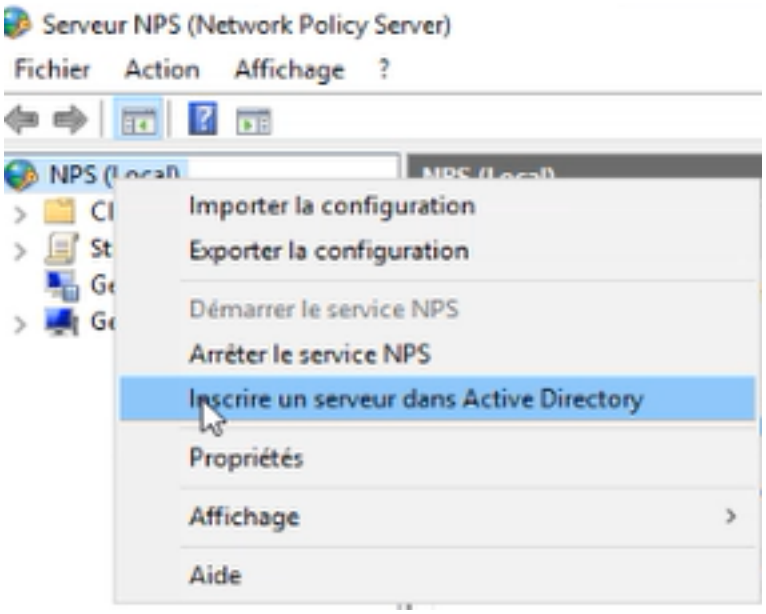

FIGURE 3.26 – Inscrire NPS dans AD

Nous allons configuré 3 type de connexion radius cablé :
a)Authentification des hotes
b)Authentification de SSH
c)Authentification de VPN

a)Authentification des hotes :
+ Création des clients radius : les clients RADIUS c'est l'intermédiaire entre le serveur RADIUS et le Client (Utilisateur) comme le montre la figure ci-dessus (fig 3.27).

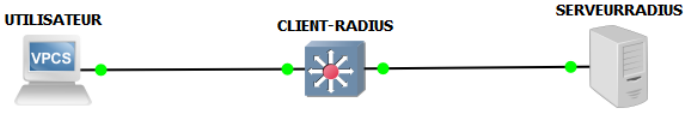

FIGURE 3.27 – (Client-Client Radius- Serveur)

Pour crée des clients radius il suffit d'un clic droit sur Client Radius puis ajouter et la figure (fig 3.29) s'affichera on va saisir un nom, une adresse IP et une clé partagé .

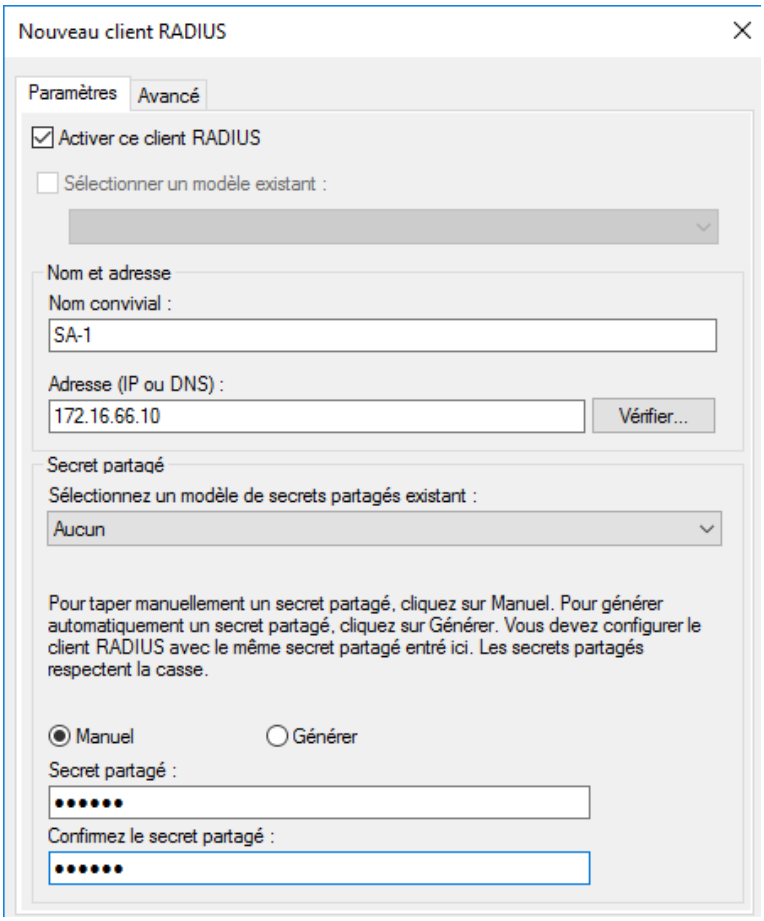

FIGURE 3.28 – Création d'un client radius

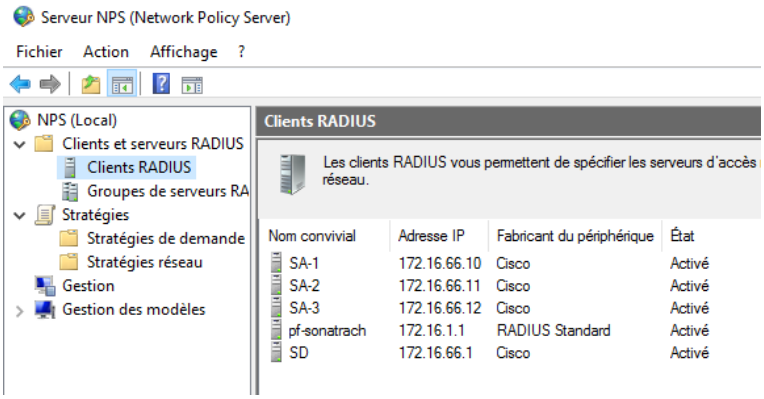

FIGURE 3.29 – Les clients créé

+ **Configuration de la 802.1x :** pour la configuration de la 802.1X il suffit de cliquer sur NPS choisir le scénario de configuration (Serveur RADIUS pour la connexion câblées ou sans fil 802.1X) puis sur Configurer 802.1X (fig 3.30) (fig 3.31).

FIGURE 3.30 – Choix de la configuration réseaux

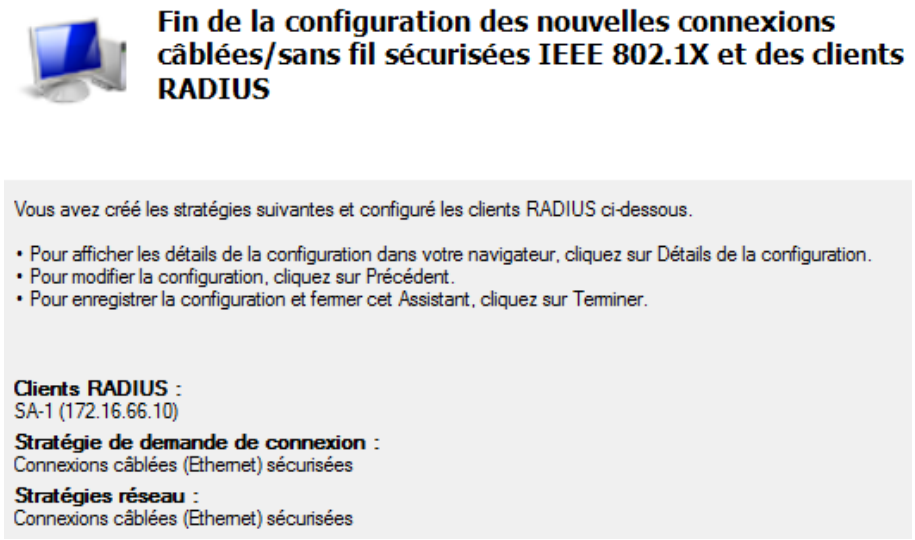

FIGURE 3.31 – la stratégie crée

+ **Propriétés de la connexion câblée :** aprés avoir créé la stratégie (Connexions câblées (Ethernet) sécurise – VLAN 10), les figures (fig 3.32),(fig 3.33),(fig 3.34),(3.35) représente le contenu de cette dernière .

Ensuite au niveau des conditions on a associer le groupe Authentification Radius Ordinateurs VLAN 10 a la stratégie de connexion, et spécifier le type du port NAS (fig 3.34).

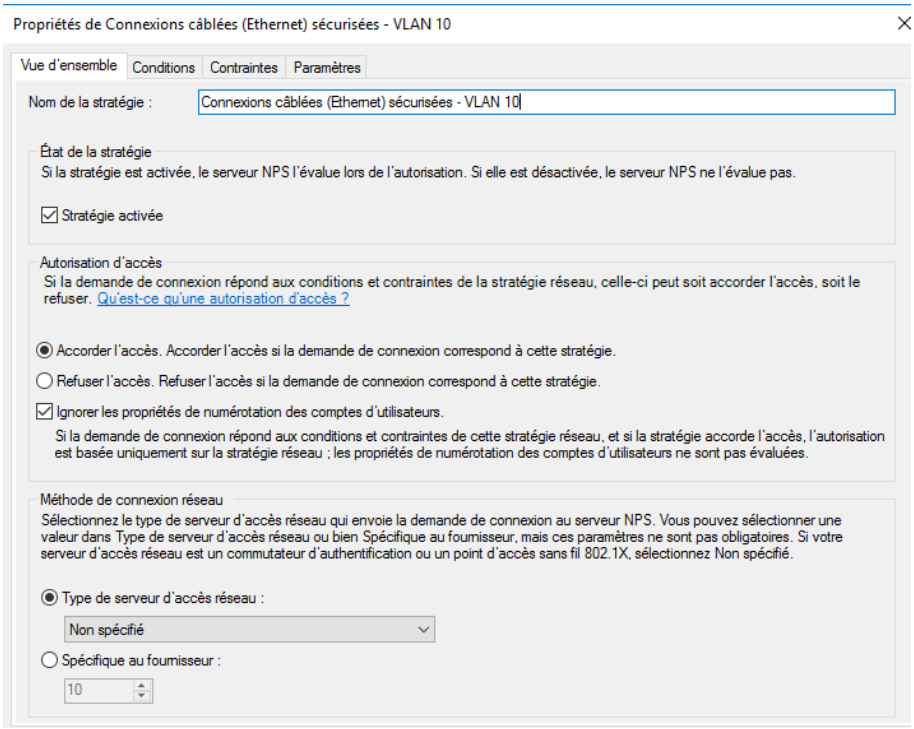

FIGURE 3.32 – Vue globale de la stratégie

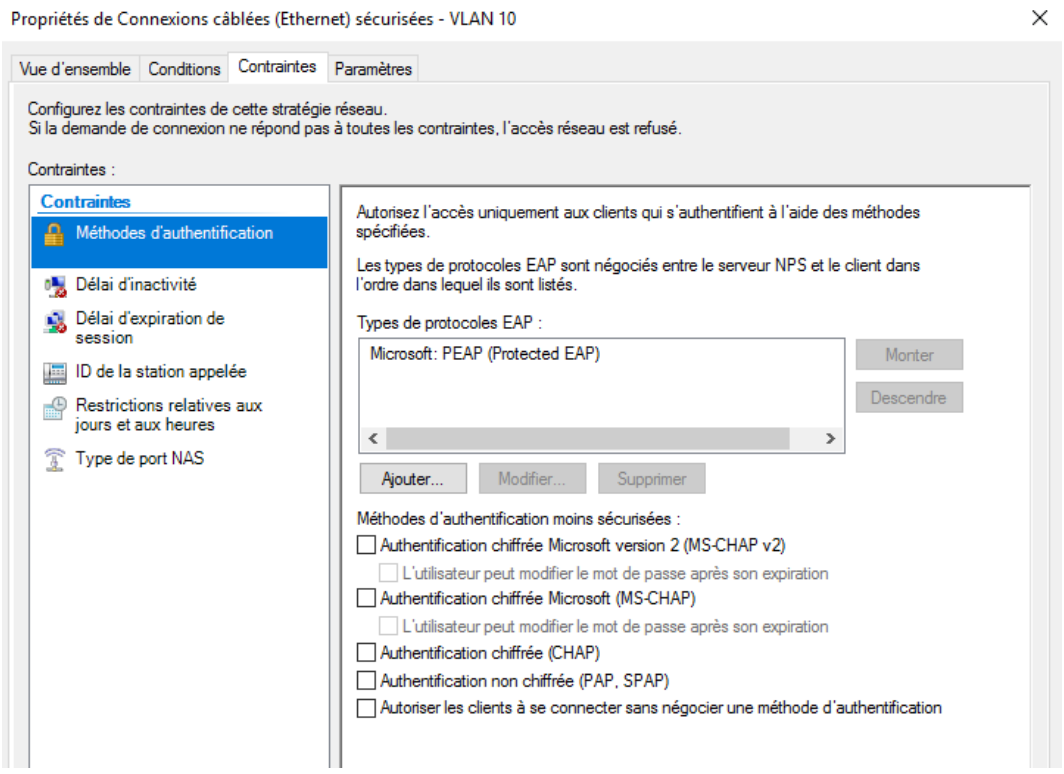

FIGURE 3.33 – Condition de la stratégie

Et pour les Contraintes on a choisi le PEAP (Protocole EAP) comme méthode d'authentification (fig 3.34).

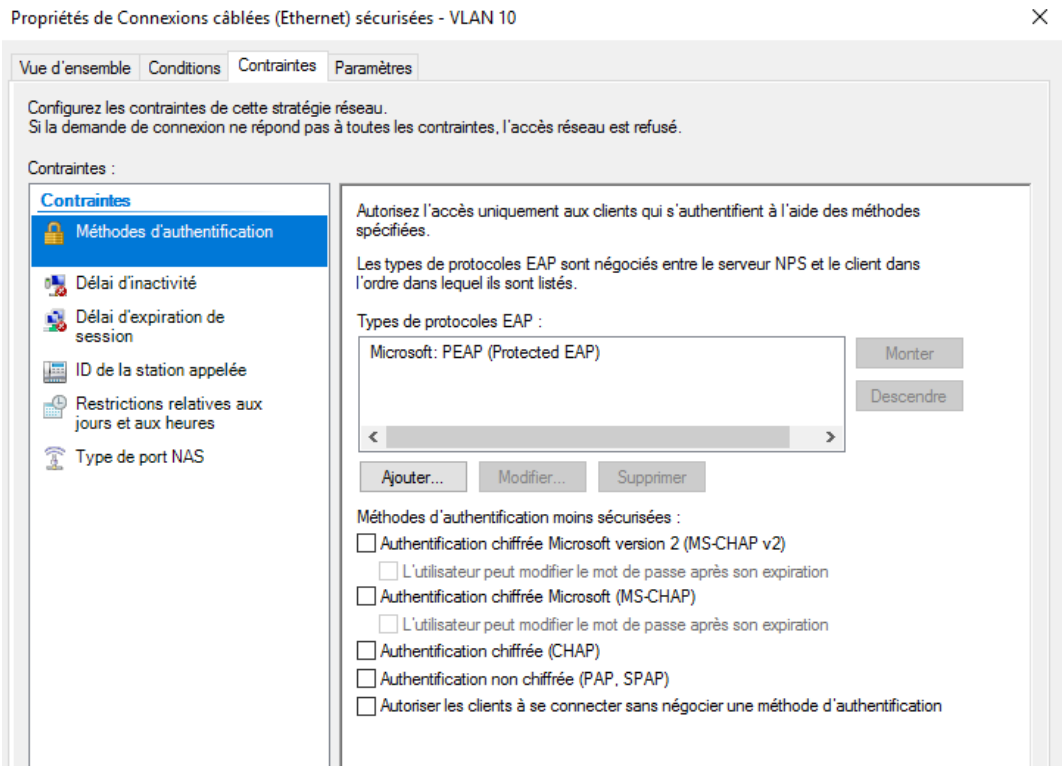

FIGURE 3.34 – Contraints de la stratégie

Et pour les paramètres sont comme suit (fig 3.35) :

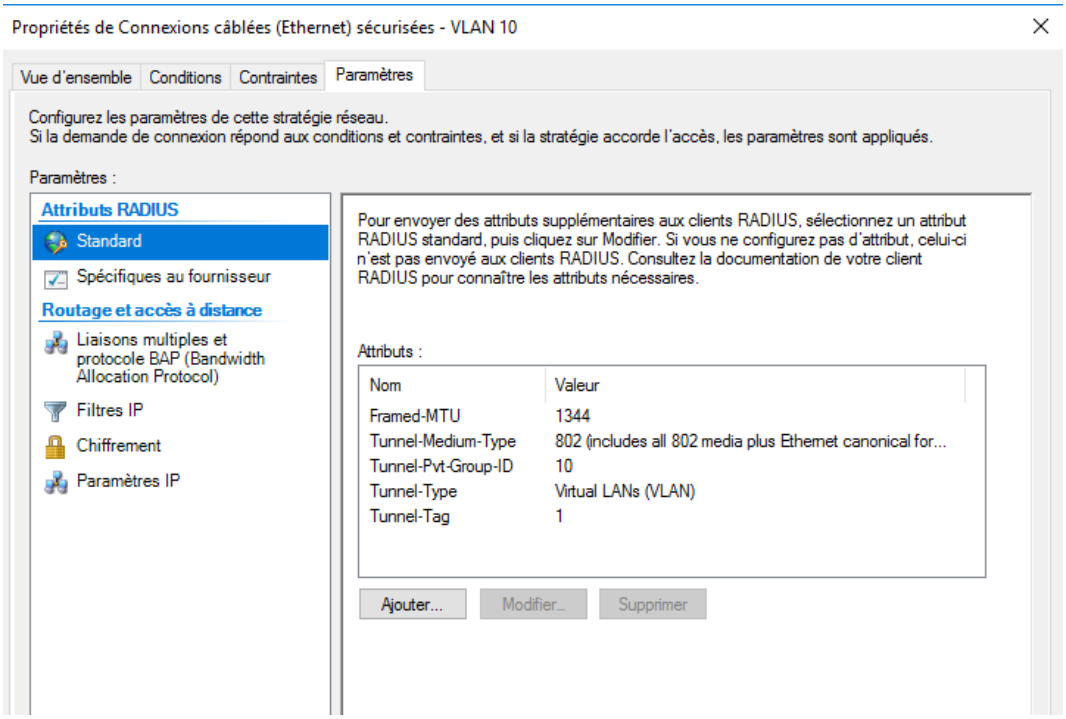

FIGURE 3.35 – Paramètre de la stratégie

Framed-MTU : la taille de la trame.
Tunnel-Medium-Type : Spécifie de type de connexion.
Tunnel-Pvt-Group-ID : L'identifiant du Vlan.
Tunnel-Type : Pour spécifié que RADIUS il va encapsuler les Vlan.
Tunnel-Tag : Pour le routage inter vlan

Etend donné que nous avons besoin d'appliquer d'autre stratégie pour notre solution nous allons créés quatre autre comme on peut voir sur la figure ci-dessus (fig 3.37).
-Pour l'authentification ssh nous allons créer la stratégie "ST SSH".
-Pour l'authentification VPN nous allons créer la stratégie "ST VPN".
Les stratégies s'applique selon l'orde de traitement.

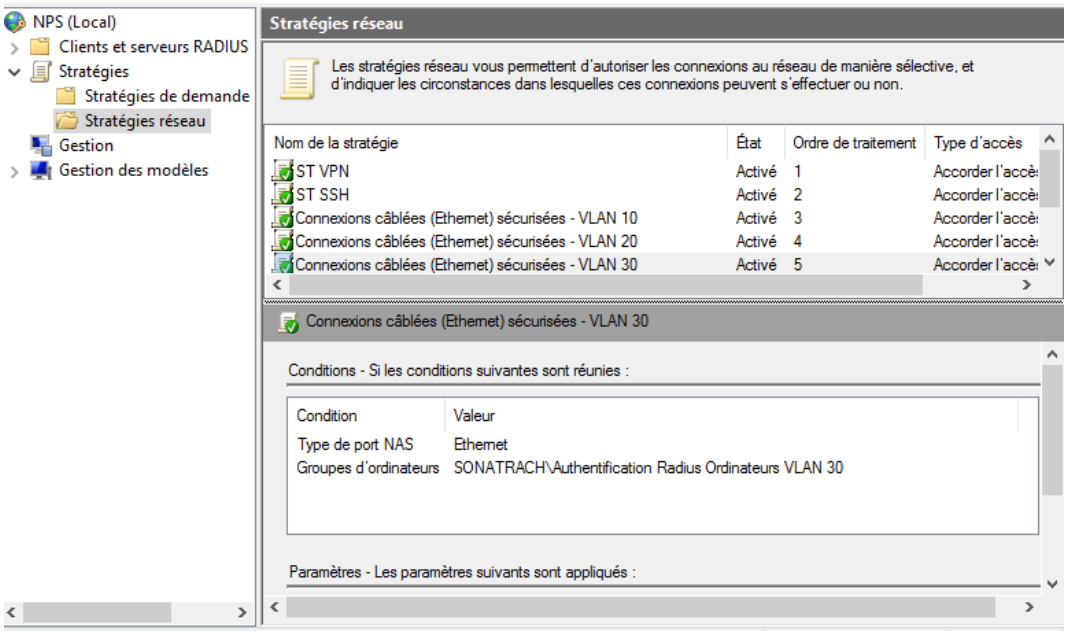

FIGURE 3.36 – Les stratégies créées

+ Configuration du client :

a)Switch

- Configuration Radius et AAA pour les switches clients

Les Configurations Radius au niveau des switches clients sont comme suit :

- Activation de triple AAA : la première commande de la figure (fig 3.37) sert à activer le service d'authentification, autorisation et accounting (AAA) et la deuxième commande définissent le groupe de serveur à utiliser pour authentifier.

```
SA-3(config)#aaa new-model
SA-3(config)#aaa authentication dot1x default group radius
SA-3(config)#
```

FIGURE 3.37 – Activation de service AAA

- Autorisé les réseaux a s'authentifié au serveur radius : la commande suivante (fig 3.8) sert à attribuer des autorisations aux utilisateurs.

```
SA-3(config)#aaa authorization network default group radius
```

FIGURE 3.38 – Autorisé les réseaux à s'authentifier au serveur radius

- Activer la 802.1x sur le commutateur : pour activer le controle des ports pour l'authentification 802.1x (fig 3.39).

```
SA-3(config)#dot1x system-auth-control
```

FIGURE 3.39 – Activation de controle pour l'authentification 802.1x

On donne l'adresse de notre serveur RADIUS, les portes qu'il utilise pour communiquer ainsi que le mot de passe (fig 3.40).

```
SA-3(config)#radius server SERVER-RADIUS
SA-3(config-radius-server)#$v4 172.16.66.200 auth-port 1645 acct-port 1646
SA-3(config-radius-server)# key sd1234
SA-3(config-radius-server)#
```

FIGURE 3.40 – Attribuation d'une adresse et d'un mot de passe au serveur RADIUS

- Configurer l'authentification basée sur le port ethernet 0/2 : Activer l'authentification 802.1x sur le port (fig 3.41)

```
SA-3(config)#interface  ethernet 0/2
SA-3(config-if)#
SA-3(config-if)#authentication port-control auto
SA-3(config-if)#dot1x pae authenticator
SA-3(config-if)#
SA-3(config-if)#
SA-3(config-if)#authentication open
SA-3(config-if)#
SA-3(config-if)#authentication host-mode multi-domain
SA-3(config-if)#
SA-3(config-if)#exit
```

FIGURE 3.41 – Configuration du port ethernet 0/2

- Indiquer l'interface source de client RADIUS :

```
SA-3(config)#ip radius source-interface Vlan 66
```

FIGURE 3.42 – Configuration de l'interface source de client

- Configuration Radius et AAA pour ssh nous allons Configurer le switche SD pour s'authentifier à l'aide de serveur radius (fig 3.43).
- Activer le service d'authentification, autorisation et accounting (1).
- Définissent le groupe de serveurs à utiliser pour authentifier et attribuer des autorisations aux utilisateurs (2) et (3).

```
SD(config)#aaa new-model
SD(config)#aaa authentication login default group radius local
SD(config)#aaa authorization exec default group radius local
SD(config)#radius server SERVER-RADIUS
SD(config-radius-server)#$v4 172.16.66.200 auth-port 1812 acct-port 1813
SD(config-radius-server)# key sd1234
SD(config-radius-server)#
*Sep 13 13:49:28.483: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
SD(config-radius-server)#
```

FIGURE 3.43 – Configuration radius sur switch et ssh

```
SD(config)#line vty 0 4
SD(config-line)#login authentication default
SD(config-line)#transport input ssh
SD(config-line)#
*Sep 13 13:51:58.514: %AMDP2_FE-6-EXCESSCOLL: Ethernet3/3 TDR=0, TRC=0
SD(config-line)#
```

FIGURE 3.44 – Configuration de ligne virtuel

Ensuite nous allons configurer les terminaux virtuels pour autoriser l'accès à distance (fig 3.44).

b)Parfeu

- Configuration Radius et AAA pour VPN : La configuration radius et AAA pour vpn est comme suit (fig 3.45) :

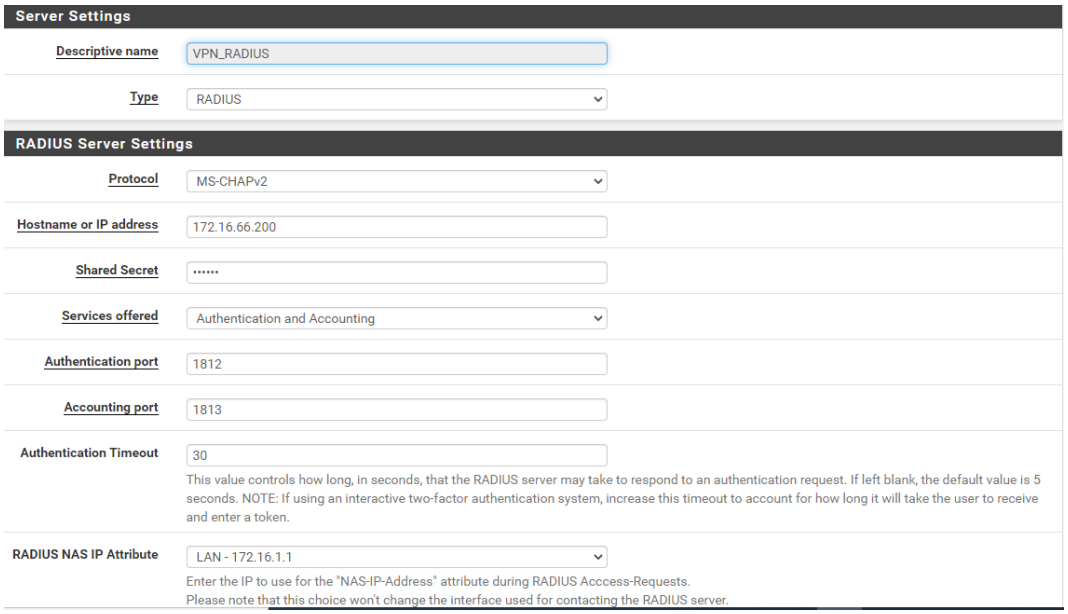

FIGURE 3.45 – Création de serveur Radius VPN

3.12 Configuration réseaux

3.13 Configuration de base coté switch et routeur

Les Configurations de switch distribution SD sont comme suit :

- Configuration de l'interface 0/0 : lors de cette étape nous allons activer la commande no switchport sur l'interface 0/0 de notre comutateur SD afin de faire fonctionner le port comme une interface de routeur plutôt que comme un port de commutateur. Ce port est donc également appelé port routé(fig), puis on a attribuée une adresse ip suivie d'un masque à notre interface avec activation de l'interface (fig 3.46) (fig 3.47).

```
SD(config)#interface ethernet 0/0
SD(config-if)#no sw
SD(config-if)#no switchport
```

FIGURE 3.46 – Configuration de port routé

```
SD(config-if)#ip address 172.16.0.2 255.255.255.252
SD(config-if)#no sh
```

FIGURE 3.47 – Affectation d'adresse à l'interface ethernet 0/0

- Configuration du routage inter-vlan : comme tout périphérique joignable sur le réseau le commutateur doit posséder une adresse ipv4 et le masque, dans cet exemple, vlan 10 est utilisé (fig 3.48).

```
SD(config)#interface vlan 10
SD(config-if)#ip address 172.16.10.1 255.255.255.0
SD(config-if)#no sh
```

FIGURE 3.48 – Affectation d'une adresse au vlan

- Dhcp relie : dans cette étape on va indiquer le dhcp est gérer par le protocole dhcp du Windows Server (fig 3.49).

```
SD(config)#interface vlan 10
SD(config-if)#ip helper-address 172.16.66.200
SD(config-if)#interface vlan 20
SD(config-if)#ip helper-address 172.16.66.200
SD(config-if)#interface vlan 30
SD(config-if)#ip helper-address 172.16.66.200
```

FIGURE 3.49 – La configuration de DHCP

- Configuration les ports des switches clients : lors de cette étape, nous allons configurer les interfaces des switches client(SA1,SA2,SA3) qui sont relier avec le switche distributeur(sd) en mode trunk (fig 3.50).

```
SA-1(config)#interface ethernet 0/0
SA-1(config-if)#switchport trunk encapsulation dot1q
SA-1(config-if)#switchport mode trunk
SA-1(config-if)#
```

FIGURE 3.50 – Configuration de port trunk

- Activé la fonction de routage du switch distribution sd : la commande suivante permet de Vérifier que notre commutateur sd est capable de remplir les taches de routages(fig 3.51).

```
SD(config)#ip routing
```

FIGURE 3.51 – Activation de la fonction de routage

- Configuration d'une route par défaut :la passerelle par défaut est 172.16.0.1 (fig 3.52).

```
SD(config)#ip route 0.0.0.0 0.0.0.0 172.16.0.1
```

FIGURE 3.52 – Configuration d'une route par défaut

3.13.1 Configuration de base sur firwall

- Création de l'autorité de certificat Dnas les figures qui suit (fig 3.53), (fig 3.54), (fig 3.56) une représentation de l'autorité de certificat crée.

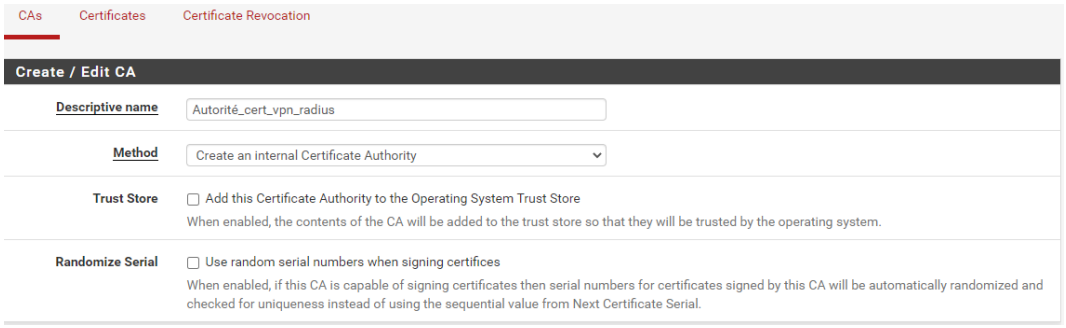

FIGURE 3.53 – Configuration de l'autorité de certificat

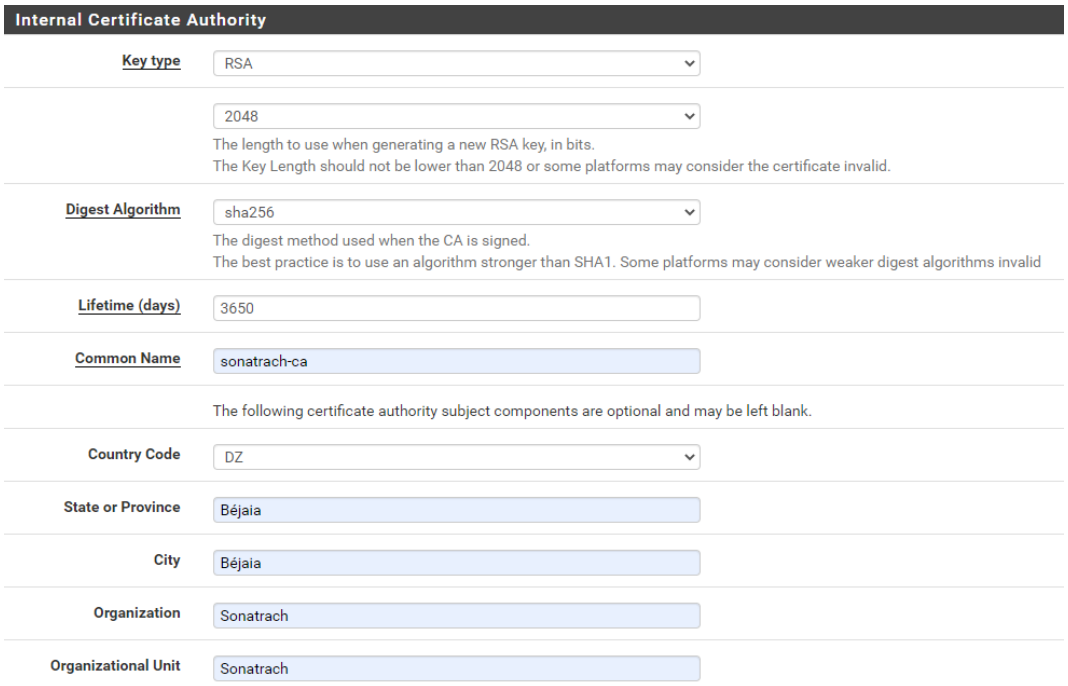

FIGURE 3.54 – Configuration de l'autorité de certificat

FIGURE 3.55 – Configuration de l'autorité de certificat

- Création de certificat server Dans la figure qui suit (fig 3.56) Nous avons créer 2 certificats serveur et utilisateur.

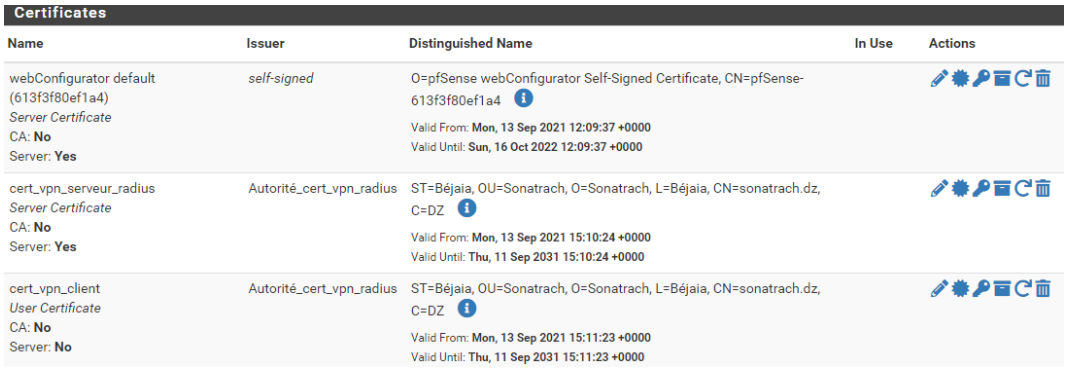

FIGURE 3.56 – Les certificats créés

Creation d'une connexion VPN radius Nous allons créer notre serveur vpn (fig 3.57).

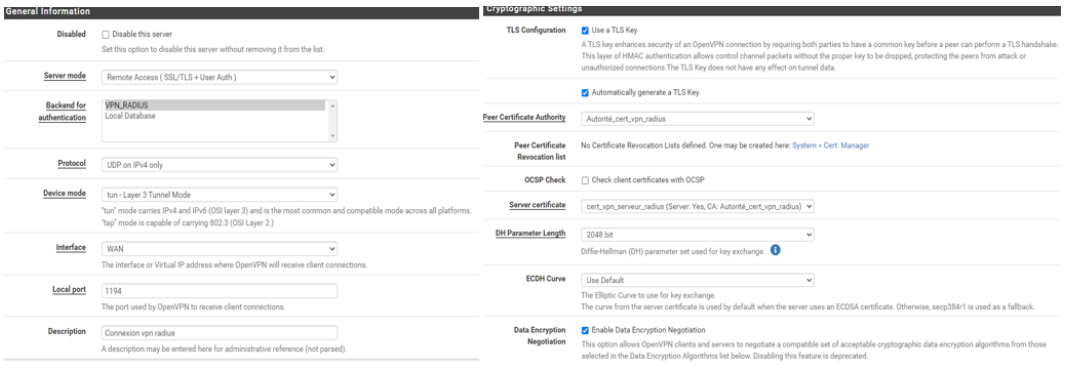

FIGURE 3.57 – Création de serveur VPN "étape1"

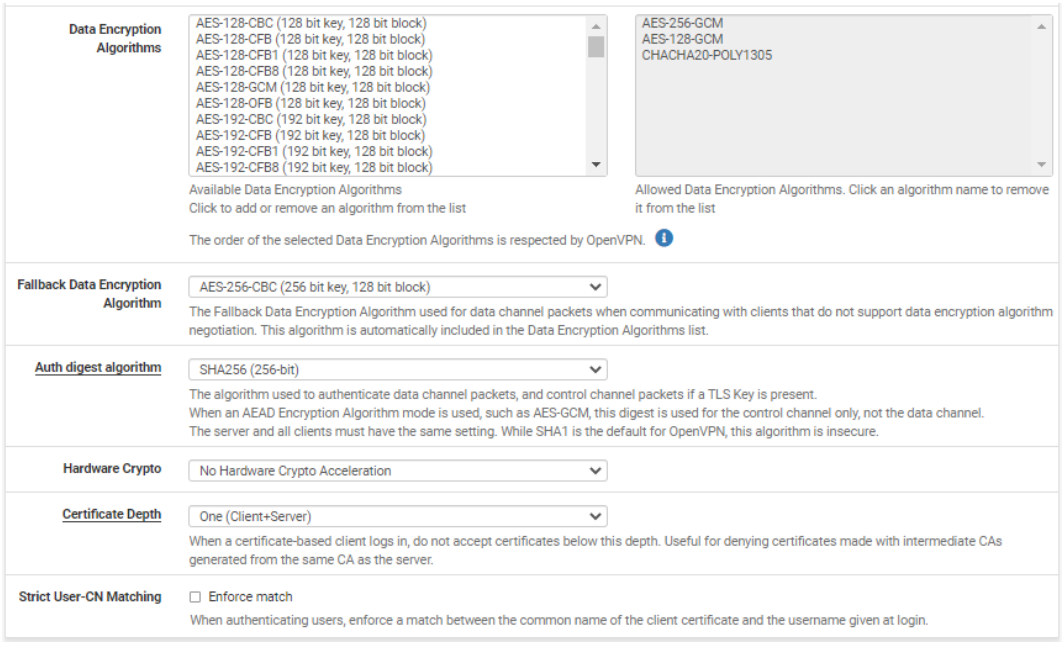

FIGURE 3.58 – Création de serveur VPN "étape2"

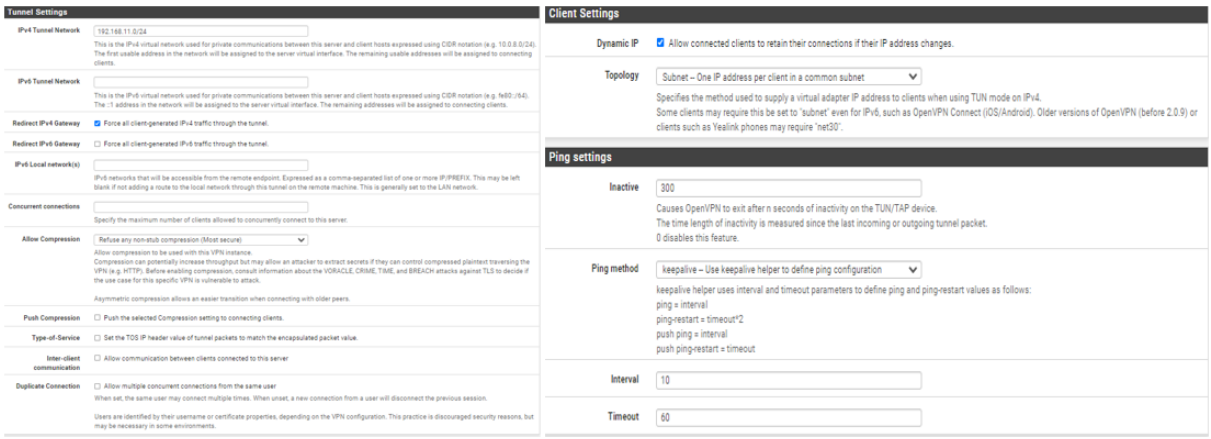

FIGURE 3.59 – Création de serveur VPN "étape3"

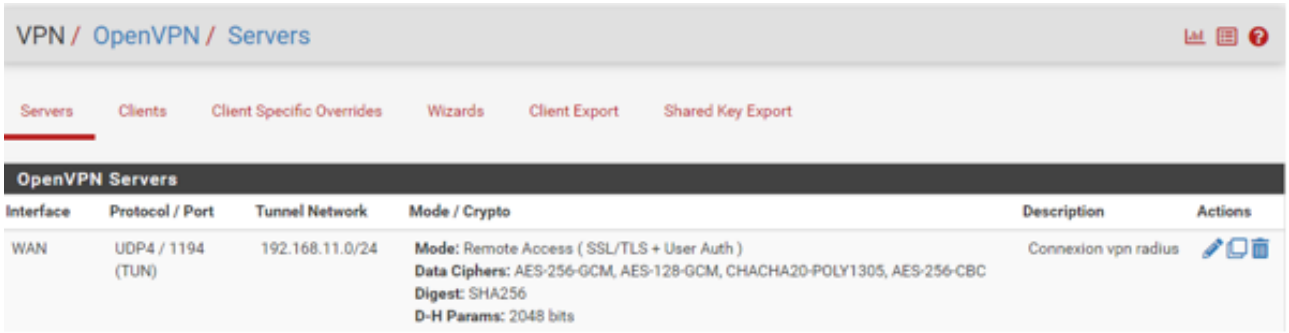

FIGURE 3.60 – Création de serveur VPN "étape4"

-Téléchargement de package pour les clients openvpn :

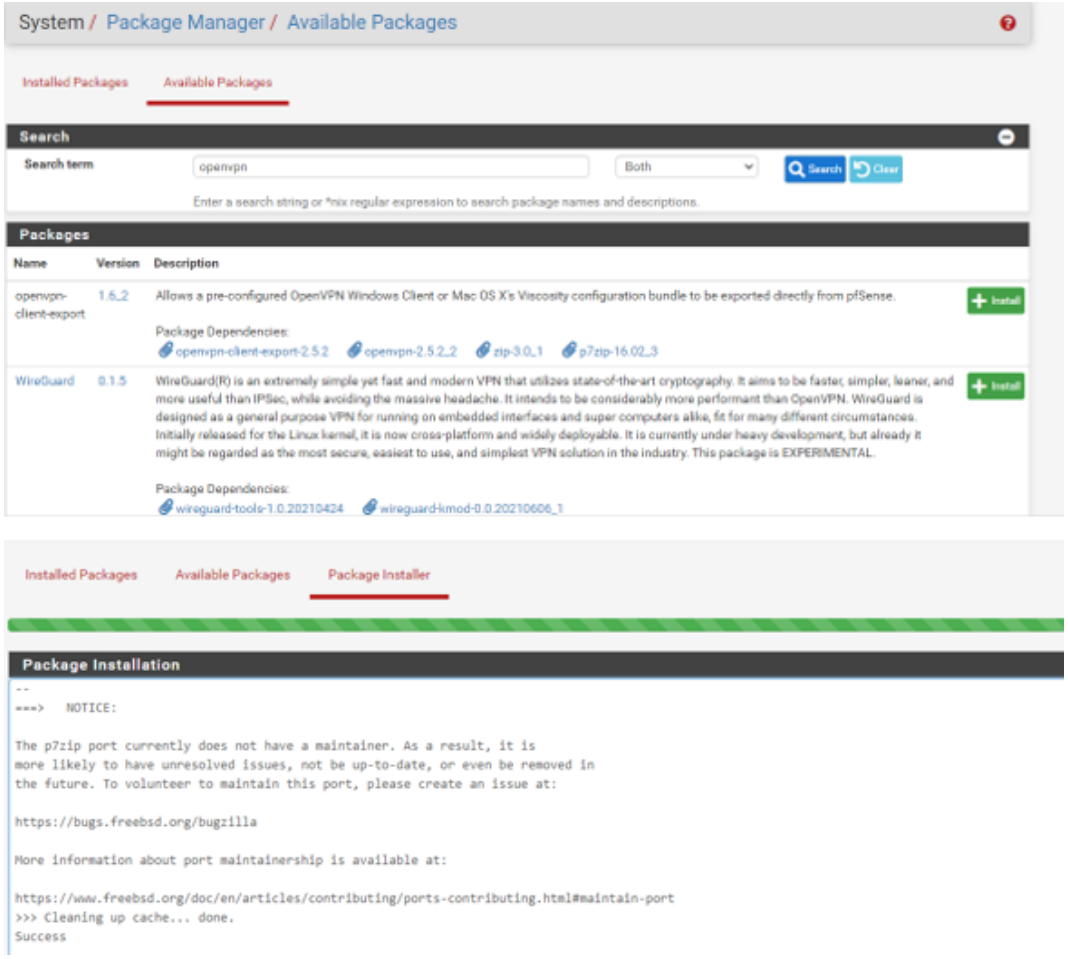

FIGURE 3.61 – Téléchargement de package pour les clients openvpn

- Exporter la configuration open VPN :

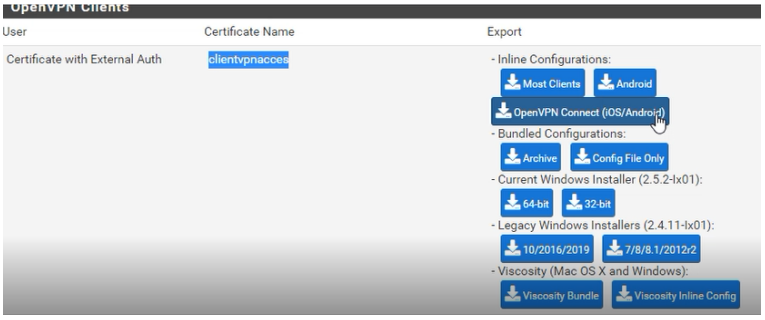

FIGURE 3.62 – Exporter la configuration open VPN

3.14 Conclusion

Dans ce chapitre, nous avons présenté les aspects technique liés à la réalisation, ainsi que l'outil matériel et logiciel pour répendre à notre solution.

Chapitre 4

Les Tests

4.1 Introduction :

Dans ce chapitre nous allons faire les différentes validations pour assurer que notre objectif a bien été atteint.

4.1.1 Test de connectivite :

Nous allons tester la connectivité entre le serveur RADIUS (S-R) et le Client RADIUS (SA-3) (fig 4.1), et entre le serveur RADIUS et le Firewall (fig 4.2) enfin entre le serveur RADIUS et le switch distribution (fig 4.3).
Pour cela nous allons sur l'invite commande (cmd) du serveur avec la commande (Ping adresse IP).

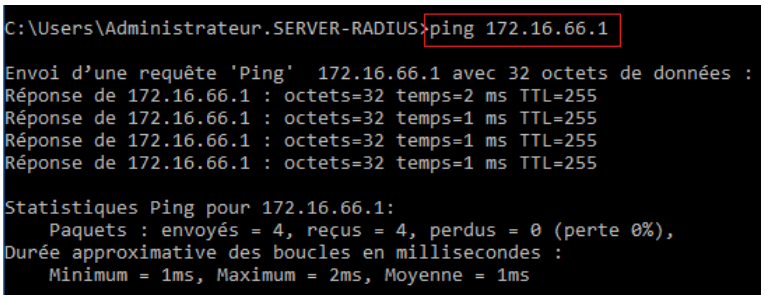

FIGURE 4.1 – Test entre le serveur et le switch client.

```
SA-2#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : sonatrach.lan
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.0400
Configuration last modified by 172.16.10.1 at 10-6-21 15:02:21

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 10
Configuration Revision          : 13
MD5 digest                      : 0x6C 0xCD 0x0D 0x7C 0x8C 0xFB 0xFC 0x83
                                  0xF6 0x89 0x88 0x6D 0xE7 0xBA 0x00 0xBE
SA-2#
```

FIGURE 4.2 – Test entre le serveur et le Firewall .

```
C:\Users\Administrateur.SERVER-RADIUS>ping 172.16.66.12

Envoi d'une requête 'Ping'  172.16.66.12 avec 32 octets de données :
Réponse de 172.16.66.12 : octets=32 temps=1 ms TTL=255
Réponse de 172.16.66.12 : octets=32 temps=2 ms TTL=255
Réponse de 172.16.66.12 : octets=32 temps=3 ms TTL=255
Réponse de 172.16.66.12 : octets=32 temps=1 ms TTL=255

Statistiques Ping pour 172.16.66.12:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 3ms, Moyenne = 1ms
```

FIGURE 4.3 – Test entre le serveur et le switch distribution.

4.1.2 Test de l'authentification RADIUS :

Pour l'authentification RADIUS nous avons deux cas :
-L'authentification réussie : Nous allons capturer le trafic radius sur Wireshark (fig 4.4), nous verrons que l'authentification est faite avec succès.

radius

No.	Time	Source	Destination	Protocol	Length	Info
135	70.175140	172.16.66.12	172.16.66.200	RADIUS	710	Access-Request id=11
138	70.278458	172.16.66.200	172.16.66.12	RADIUS	218	Access-Challenge id=11
140	70.438356	172.16.66.12	172.16.66.200	RADIUS	368	Access-Request id=12
141	70.439246	172.16.66.200	172.16.66.12	RADIUS	232	Access-Challenge id=12
142	70.658334	172.16.66.12	172.16.66.200	RADIUS	437	Access-Request id=13
143	70.662528	172.16.66.200	172.16.66.12	RADIUS	271	Access-Accept id=13

FIGURE 4.4 – Authentification réussie sur Wireshark.

Et au niveau du journal d'évènement qui se trouve dans le serveur, nous allons voir que le l'authentification du PC3 est faite avec succès.

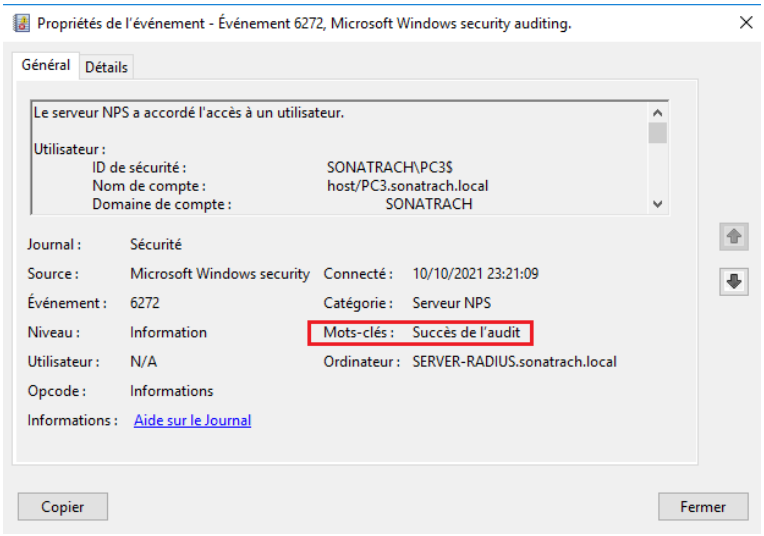

FIGURE 4.5 – Journal d'évènement.

Sur la console du switch Client Radius à l'aide de la commande show authentification sessions interface ethernet 0/2, nous allons voir si la 802.1x est configurée (fig 4.6), et à l'aide de la commande show authentification sessions interface ethernet 0/2 detail nous verrons que l'authentification est faite avec succès (fig 4.7), et comme nous pouvons voir sur la figure 3.8 les massages qui s'affichent sur la console.

```
SA-3#show authentication sessions interface ethernet 0/2

Interface    MAC Address    Method  Domain  Status Fg Session ID
-----------------------------------------------------------------------
Et0/2        000c.29de.450d dot1x   DATA    Auth      AC10420C0000000B004BB95D


Key to Session Events Blocked Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  N - Waiting for AAA to come up
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker

Runnable methods list:
  Handle  Priority  Name
    5        5      dot1x
    9       10      mab
    7       15      webauth
SA-3#
```

FIGURE 4.6 – Dot1x activé.

```
Method status list:
        Method              State
        dot1x               Authc Success
```

FIGURE 4.7 – Authentification succès.

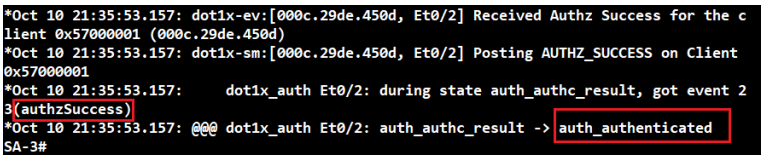

FIGURE 4.8 – Message switch.

-L'authentification échouée : Dans le cas où l'authentification a échoué, nous observons dans la machine client qu'il y a un échec d'authentification comme le représente la figure 4.9.

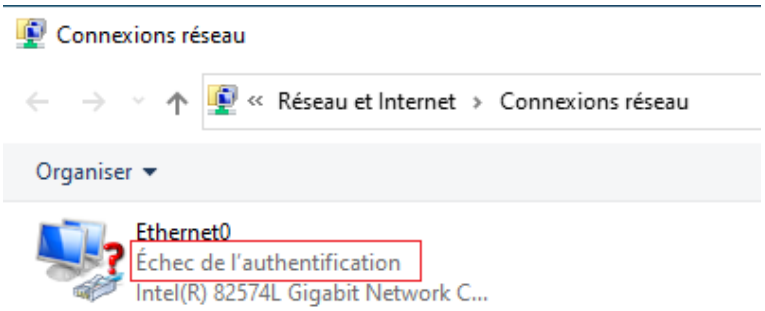

FIGURE 4.9 – Echec d'authentification .

Sur Wireshark nous verrons que l'accès est rejeté (fig 4.10).

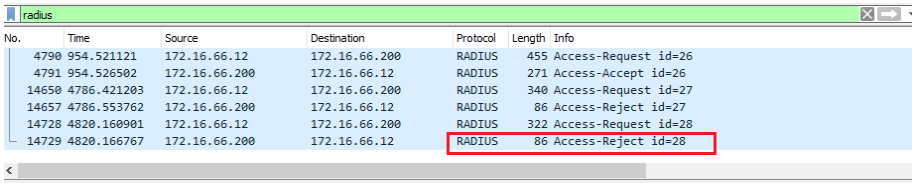

FIGURE 4.10 – Authentification rejeté sur Wireshark .

Et au niveau du journal d'évènement, nous verrons un échec d'authentification (fig 4.11).

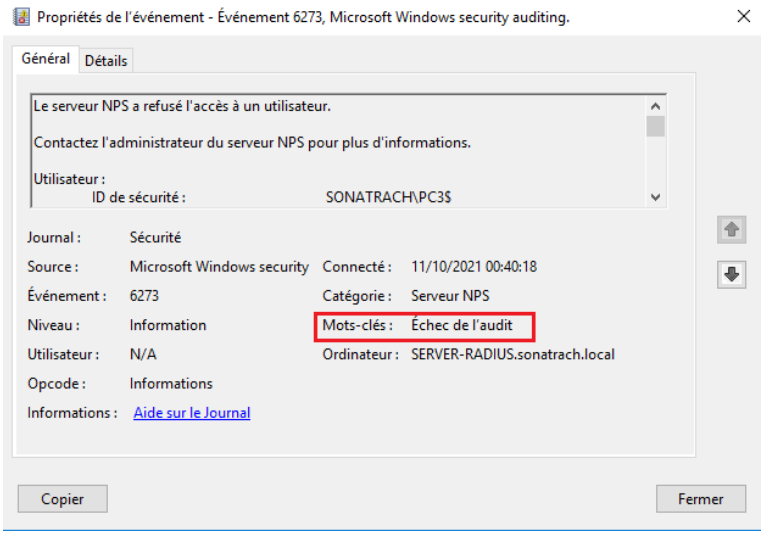

FIGURE 4.11 – Journal d'évènement .

Sur la console du switch client radius nous allons voir que l'authentification a échoué (fig 4.12).

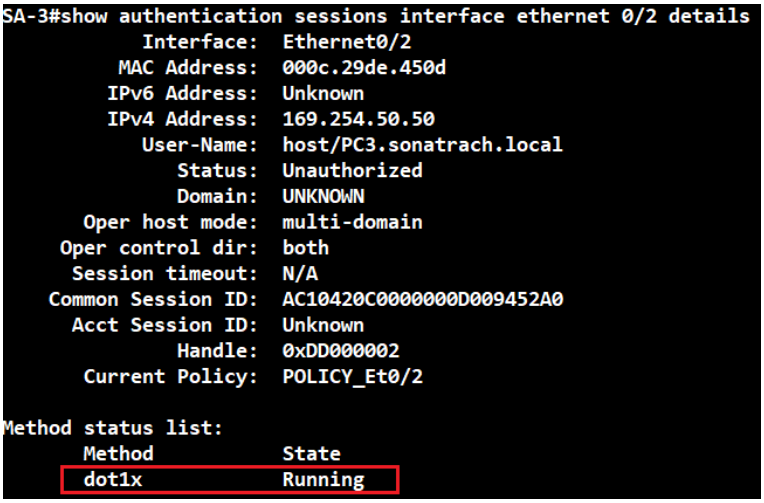

FIGURE 4.12 – Dot1x échoué.

4.1.3 Test SSH

L'accès au switch avec PuTTy :
Nous allons saisir l'adresse IP du switch ou le nom de la session (s.hachem@172.16.66.1)(fig 4.13).

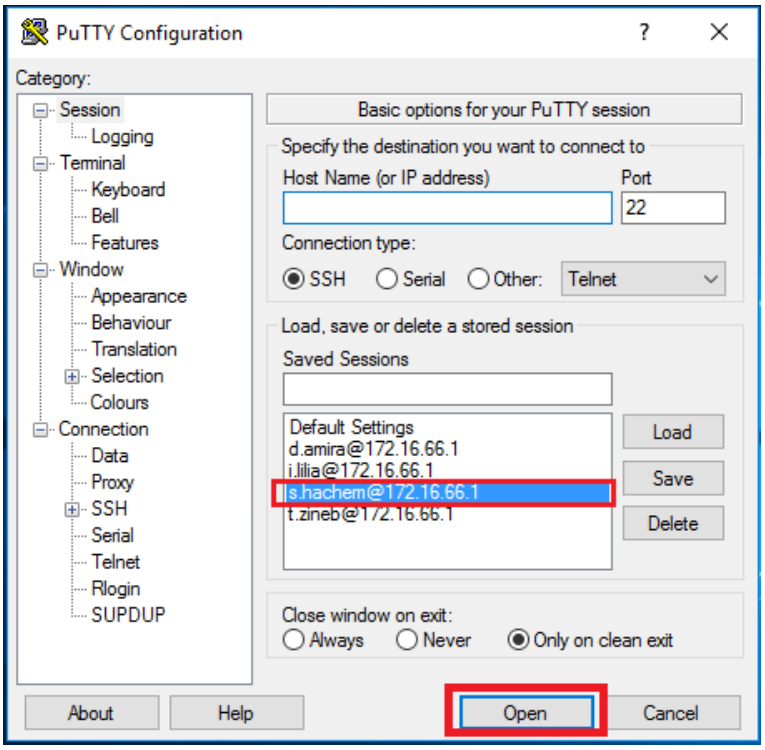

FIGURE 4.13 – l'accès au switch avec un client SSH.

Une figure apparait pour introduire le mot de passe (fig 14).

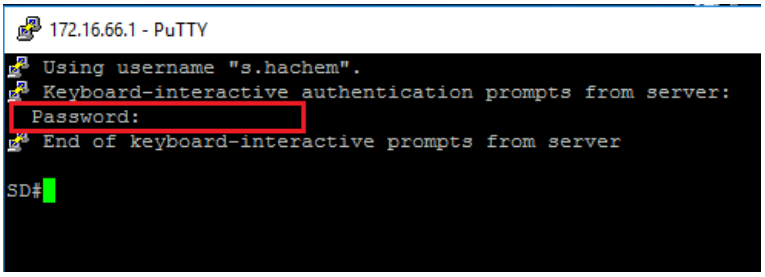

FIGURE 4.14 – L'accès au switch .

4.1.4 Test VPN

Sur la machine du client VPN nous allons tester l'accès à distance à l'aide de OpenVPN, on va saisir le nom de l'utilisateur et le mot de passe(fig 4.15).

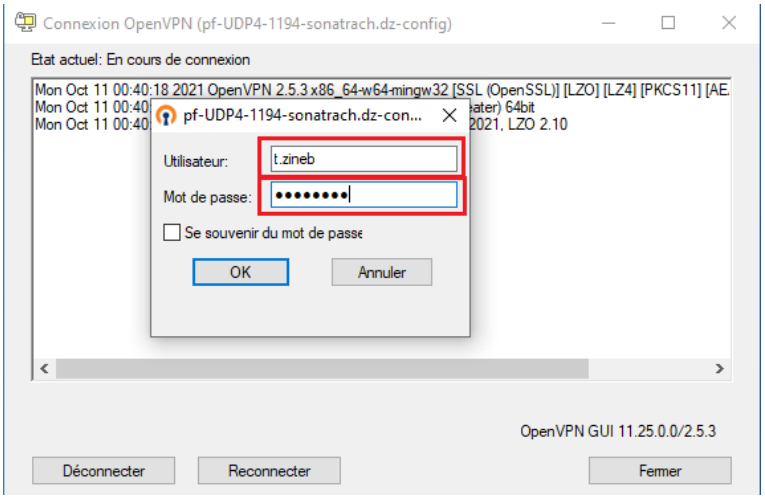

FIGURE 4.15 – Connexion VPN.

Une fois que les informations seront introduites, la machine client vpn va recevoir une adresse IP grâce au DHCP configurer au niveau du pare-feur PfSense (3.16), et nous allons remarquer qu'une nouvelle adresse a été distribuée au niveau du pare-feur figure (4.17).

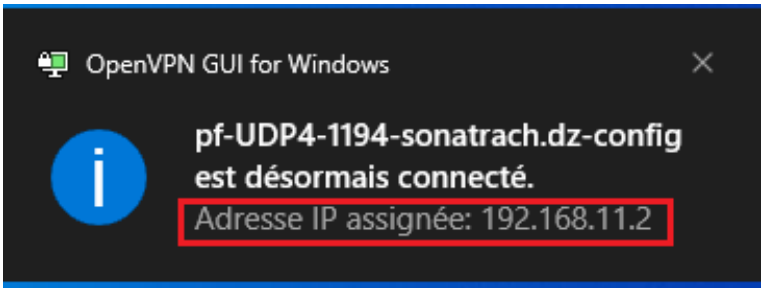

FIGURE 4.16 – Affectation d'adresse IP.

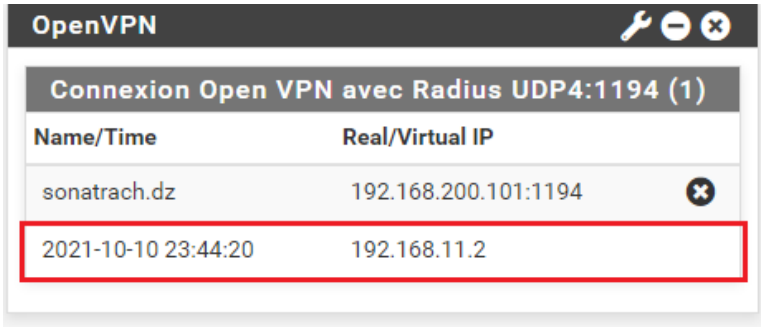

FIGURE 4.17 – connexion d'un client vpn .

A l'aide de la commande Ping on va tester la connectivité entre le client vpn et le serveur (fig 4.18).

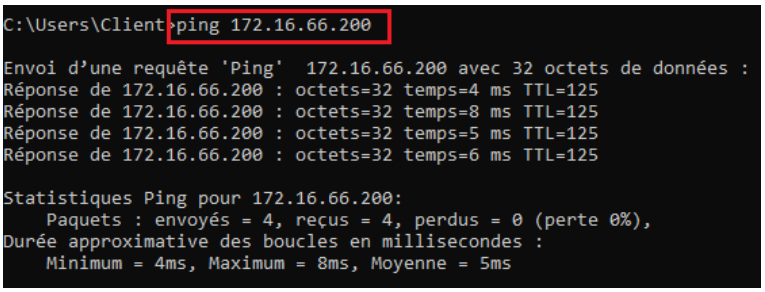

FIGURE 4.18 – Test connectivité client vpn-Serveur.

Et pour l'accès à distance nous avons utiliser le RDP (la fonctionnalité « Connexion Bureau à distance » de Windows)(fig 4.19).

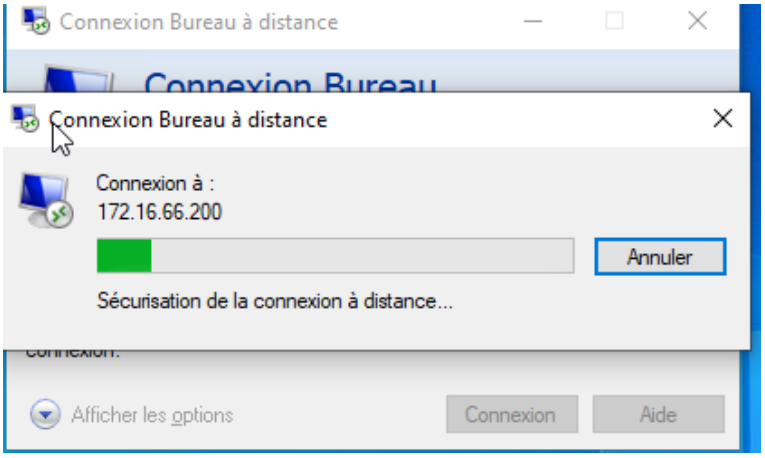

FIGURE 4.19 – Connexion Bureau à distance.

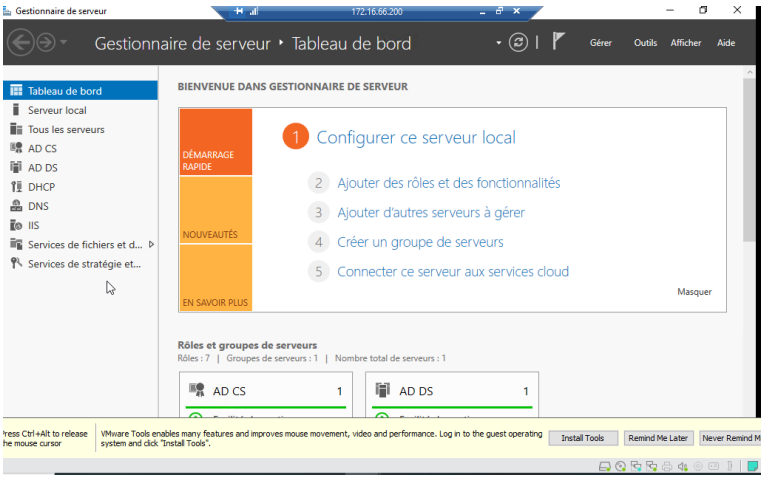

FIGURE 4.20 – Accès au serveur.

4.2 Conclusion

Ce dernier chapitre, nous avons présenté les différents tests de notre solution.

Conclusion générale

Dans ce mémoire, nous avons mis en œuvre une technique de sécurisation d'accès aux réseaux informatiques des entreprises, inter-entreprises afin de mieux garantir certains besoins de la sécurité : l'authentification, l'intégrité et la confidentialité des données échangées entre différents utilisateurs. Cette technique permet de contrôler l'accès physique aux équipements d'infrastructures réseaux en s'appuyant sur le protocole EAP pour le transport des informations d'identification en mode client/serveur, et un serveur d'identification RADIUS couplé avec à un Active Directory.

Pour la réalisation du service d'authentification RADIUS, nous avons utilisé Windows server 2016 qui inclut le serveur d'authentification RADIUS, et qui fait appel à des services de domaines Active Directory permettant d'avoir des contrôleurs de domaines.

La mise en œuvre de ce projet, nous a permis d'apporter une contribution à l'entreprise SONATRACH de Bejaia. mais aussi d'acquérir de nouvelles connaissances sur le protocole d'authentification RADIUS grâce à une étude détaillée sur son fonctionnement, ses principes et les protocoles qu'il utilise. Durant notre formation, nous avons mis en pratique ces connaissances.

Enfin, comme perspectives pour ce projet, il serait en particulier intéressant implémenter des cartes à puce.

Bibliographie

[1] Couches du système d'information. http ://www.volle.com/travaux/couchessi.htm consulté le 10/06/2021

[2] Reseau-informatique-definition. https ://www.ionos.fr/digitalguide/serveur/know-how/reseau-informatique-definition/ consulté le 10/06/2021.

[3] LAN (Local Area Network). http ://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203395-lan-local-area-network-definition-traduction/ consulté le 12/06/2021.

[4] Qu'est-ce qu'un WANhttps.http ://www.cloudflare.com/fr-fr/learning/network-layer/what-is-a-wan/ consulté le 12/06/2021.

[5] http ://sadalahsadalah.e-monsite.com/medias/files/chapitre5.pdf consulté le 12/06/2021.

[6] Les principaux composant d'connexion. https ://telecomubma.files.wordpress.com/2018/01/chapitre5-tc3a9lc3a9phonie-docx.pdf consulté le 12/06/2021.

[7] Modèles de référence OSI.https ://contenthub.netacad.com/itn/Modèles de référence OSI consulté le 12/06/2021.

[8] le modèle de référence TCP/IP. https ://contenthub.netacad.com/itn/le modèle de référence TCP/IP consulté le 12/06/2021.

[9] DHCP. https ://www.commentcamarche.net/contents/517-le-protocole-dhcp consulté le 12/06/2021.

[10] RADIUS. https ://cric.grenoble.cnrs.fr/Administrateurs/Documentations/SiteWebAuthentificatio consulté le 5/10/2021.

[11] Hocine malti, histoire secète du pétrole algérien, éditions la découverte,2010, 358 pages.

[12] Topologie-reseau. http ://bits-genius.com/topologie-reseau/ consulté le 02/10/2021.

[13] Switch 6509. https ://www.cisco.com/c/en/us/products/switches/catalyst-6509-neb-a-switch/index.html consulté le29/09/2021.

[14] Switch 3750. https ://www.cisco.com/c/dam/global/fr-fr/assets/documents/pdfs/datasheet/switching/Catalyst3750.pdf consulté le 29/09/2021.

[15] Switch 3550. https ://www.cisco.com/web/ANZ/cpp/refguide/hview/switch/3550.html consulté le 29/09/2021

[16] Swicht 2950. https ://www.mercadoit.com/fr/5-switch-cisco consulté le 29/09/2021.

[17] Port-based-network. access.shtml.https ://www.perlesystems.fr/supportfiles/port-based-network-access.html consulté le 01/10/2021

[18] K.J,GUIDE DE MISE EN PLACE D'UNE SOLUTION D'AUTHENTIFICATION NIVEAU 2,édition 2010.

[19] PPP. http ://www.labouret.net/ppp/ consulté le 01/10/2021

[20] PAP. http ://www.coursnet.com/2014/11/configuration-des-protocoles-reseau-pap-et-chap.html consulté le 01/10/2021

[21] CHAP. http ://www.coursnet.com/2014/11/configuration-des-protocoles-reseau-pap-et-chap.html consulté le 01/10/2021.

[22] Jean-philippe Bay,jean-jean-francois pillou,Tout sur la sécurité informatique.paris :DUNOD,DL 2009.

[23] https ://www.tala-informatique.fr/wiki/images/3/33/Ad intro.pdf consulté le 3/10/2021

[24] RADIUS. http ://www-igm.univ-mlv.fr/ dr/XPOSE2007/jgauth02 RADIUS/protocol.html consulté le 4/10/2021

[25] Ressource interne de l'univeristé

[26]

Annexe A

Ajout des diffèrents rôles

A.1 Ajout du rôle Active Directory

Dans cette figure nous avant les etape d'instalation d'Active Directory . On sélectionne le rôle « Active Directory Domain Services ». Pour se faire, on coche la case correspondante, ensuite on clique sur « Next ». Une fenêtre apparait on clique sur Install. Une fois que l'installation est achevée, une fenêtre apparait et ensuite cliquer sur fermer (fig A.1).

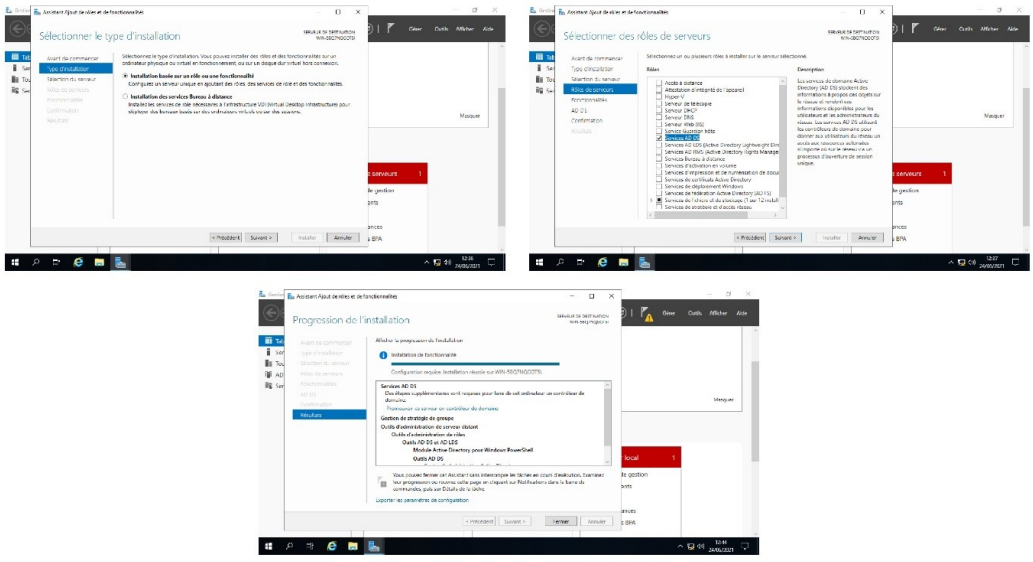

FIGURE A.1 – Installation du rôle Active Directory.

A.2 Installation du Serveur DNS

Pour l'installation du service DNS, nous procéderons comme suit (fig A.2) :

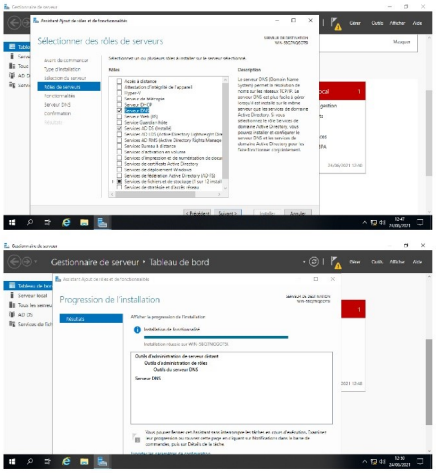

FIGURE A.2 – Installation de serveur DNS.

A.3 Installation du serveur DHCP

Pour l'installation du service DHCP, nous procéderons comme suit (fig A.4.3) :

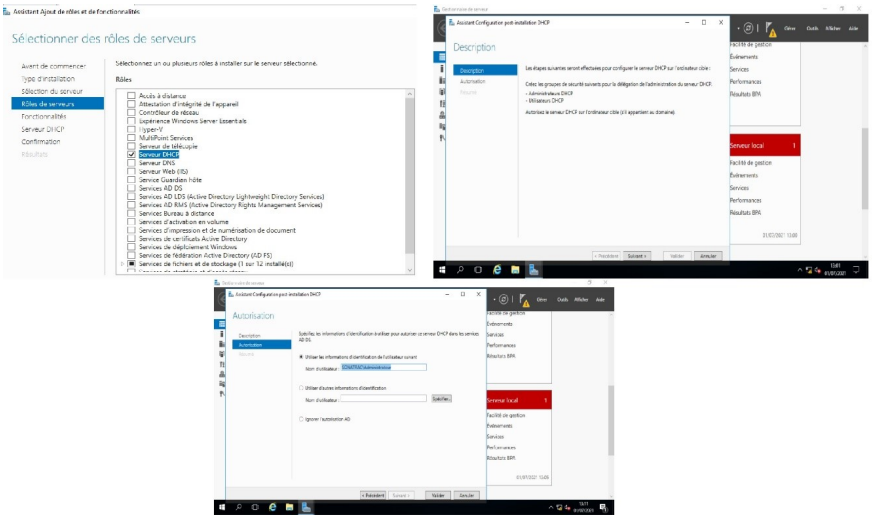

FIGURE A.3 – Installation de serveur DHCP.

A.4 Installation du serveur NPS

Pour l'installation du service NPS, nous procéderons comme suit(fig A.4) :

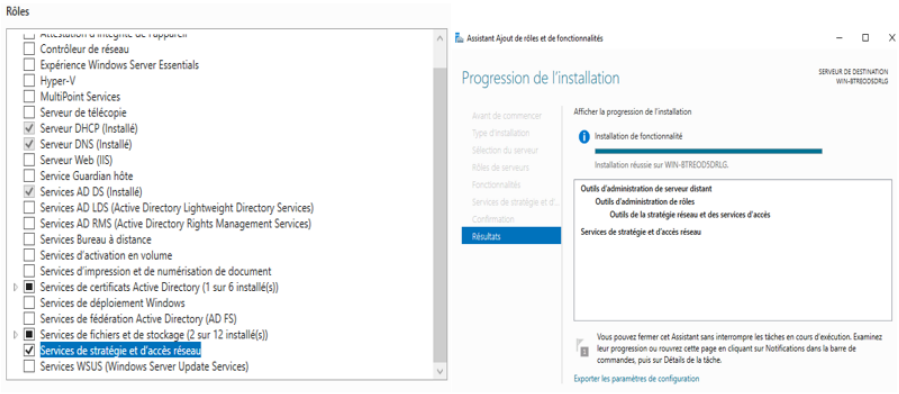

FIGURE A.4 – Installation de serveur NPS.

A.5 Installation de service de certificats Active directory :

Pour l'installation de service Active Directory, nous procéderons comme suit (fig A.5) :

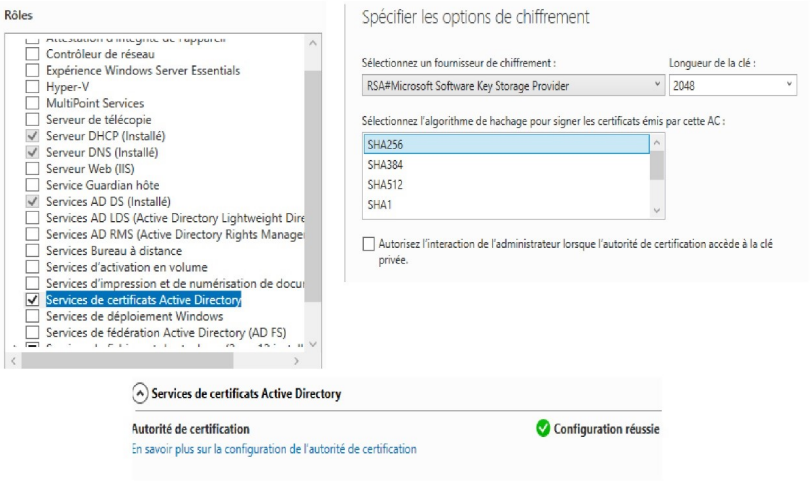

FIGURE A.5 – Installation de service de certificats Active directory.

Annexe B

Tests

B.1 Teste du protocole vtp

Afficher le statu du VTP server (fig B.1) et le vtp client (fig b.2), en utilisant la commande show vtp status sur le switch SD (Switch Distribution) et le switch client (SA-2).

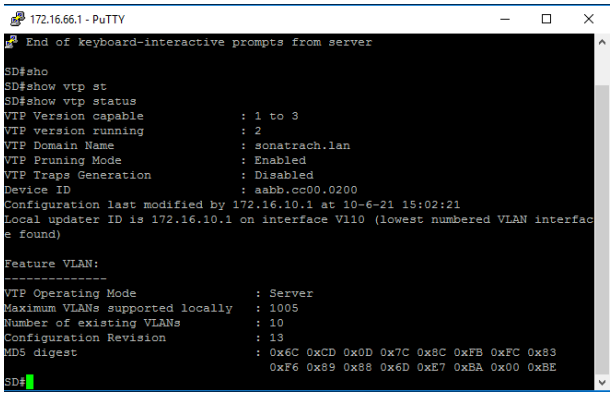

FIGURE B.1 – Test VTP server.

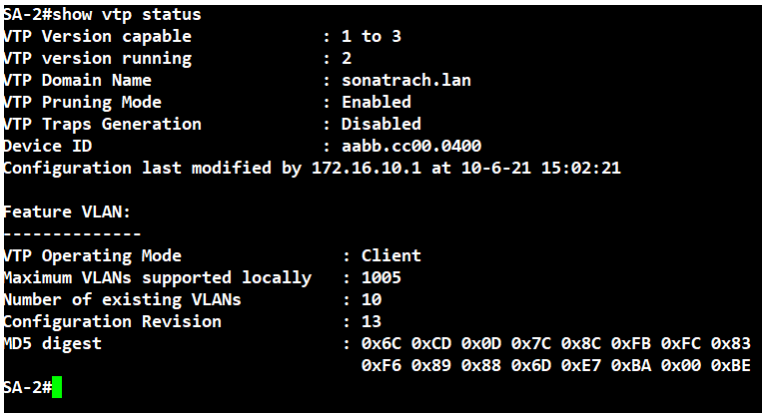

FIGURE B.2 – Test VTP client.

B.2 Teste des Vlans (Virtual Local Area Network) :

Vérification des vlans crée au niveau du switch SD (Switch Distribution), avec la commande **show vlan brief** (fig B.3).

```
SD#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
10   Informatique                     active
20   GRH                              active
30   Juridique                        active
40   Finance                          active
66   manager                          active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
SD#
```

FIGURE B.3 – Vlans créé.

Apres, nous allons vérifier la distribution des vlans sur les switchs clients avec la commande **show vlan brief** (fig B.4).

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/3, Et1/0, Et1/1, Et1/2
                                                Et1/3, Et2/0, Et2/1, Et2/2
                                                Et2/3, Et3/0, Et3/1, Et3/2
                                                Et3/3
10   Informatique                     active    Et0/2
20   GRH                              active
30   Juridique                        active
40   Finance                          active    Et0/0
66   manager                          active
```

FIGURE B.4 – Vlans créé.

B.3 Routage inter-vlan

Pour afficher le routage sur le switch distribution (SD) (fig B.5) et le routeur (R-Core) (fig B.6), nous allons utiliser les deux commandes **show ip route** et **show running-config — section ip route** .

```
172.16.66.1 - PuTTY
SD#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.0.1  (1)
      172.16.0.0/16 is variably subnetted, 12 subnets, 3 masks
C        172.16.0.0/30 is directly connected, Ethernet0/0
L        172.16.0.2/32 is directly connected, Ethernet0/0
C        172.16.10.0/24 is directly connected, Vlan10
L        172.16.10.1/32 is directly connected, Vlan10
C        172.16.20.0/24 is directly connected, Vlan20
L        172.16.20.1/32 is directly connected, Vlan20
C        172.16.30.0/24 is directly connected, Vlan30
L        172.16.30.1/32 is directly connected, Vlan30
 --More--                                                    (2)
```

FIGURE B.5 – Routage de SD.

(1),(2),(C),(L)

(1) Route par défaut.
(2) Route vers les Vlans.
(C) Ligne directement connecté.
(L) Ligne local.

```
R-Core#show running-config | section ip route
ip route 0.0.0.0 0.0.0.0 172.16.1.1
ip route 172.16.10.0 255.255.255.0 172.16.0.2
ip route 172.16.20.0 255.255.255.0 172.16.0.2
ip route 172.16.30.0 255.255.255.0 172.16.0.2
ip route 172.16.40.0 255.255.255.0 172.16.0.2
ip route 172.16.66.0 255.255.255.0 172.16.0.2
R-Core#
```

FIGURE B.6 – Routage de R-Core.

Et au niveau du pare-feu nous avons la route suivante :
• Route vers le LAN.
• Route vers le WAN.
• Route vers les Vlans.
Comme le représente la figure (fig B.7).

Static Routes

	Network	Gateway	Interface	Description	Actions
✓	172.16.0.0/30	LANGW - 172.16.1.2	LAN		
✓	192.168.200.0/24	WANGW - 10.10.10.2	WAN		
✓	les_vlans	LANGW - 172.16.1.2	LAN		

FIGURE B.7 – Routage pare-feu.

B.4 Vérification de test de connectivité :

Test de validation entre le pc (client) et le WAN (fig B.8), entre le pc et le serveur (fig B.9), enfin entre le pc et switch (fig B.10).

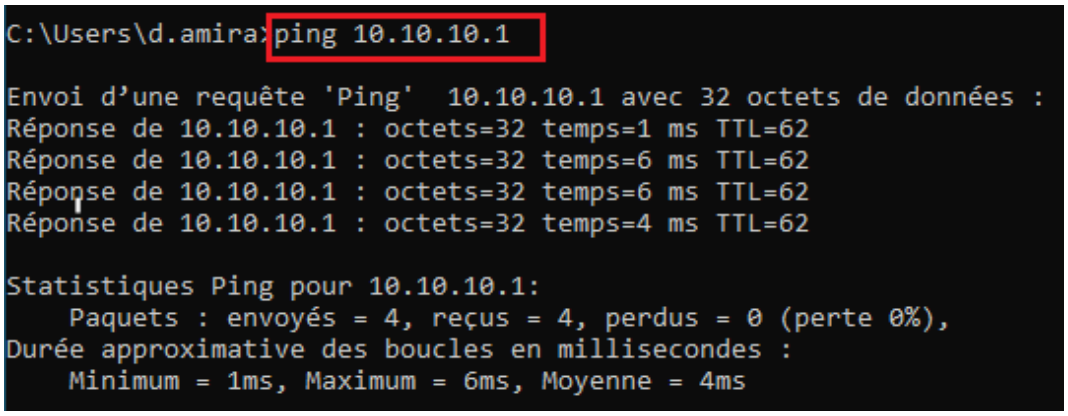

FIGURE B.8 – Test de connectivité.

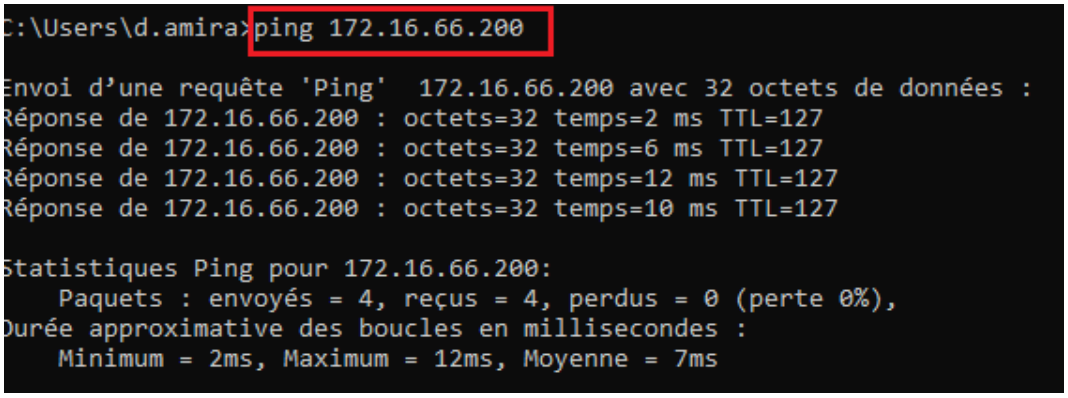

FIGURE B.9 – Test de connectivité.

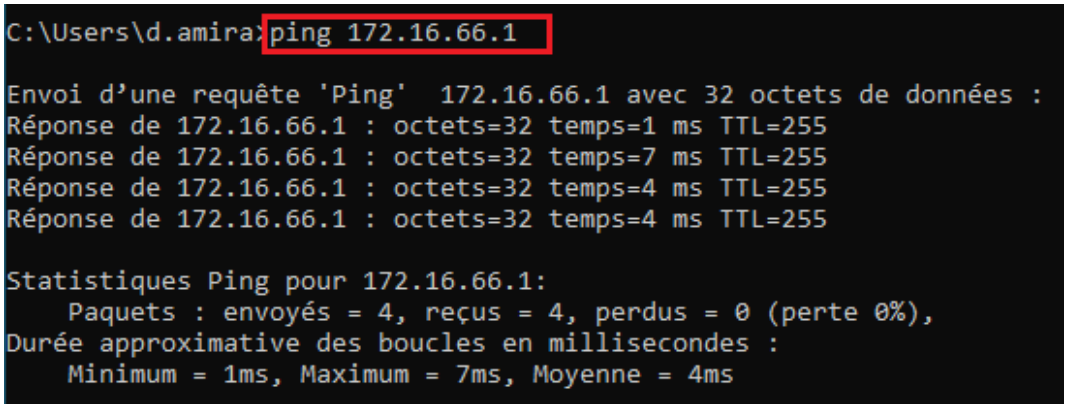

FIGURE B.10 – Teste de connectivité.

B.5 Test du serveur DHCP

Sur la machine client « Panneau de configuration Réseau et Internet Connexions réseau » nous allons voir que l'adresse IP du pc (fig B.11), et au niveau du serveur DHCP nous remarquons qune adresse IP (172.16.10.103) a été affecter au PC3 (fig B.12).

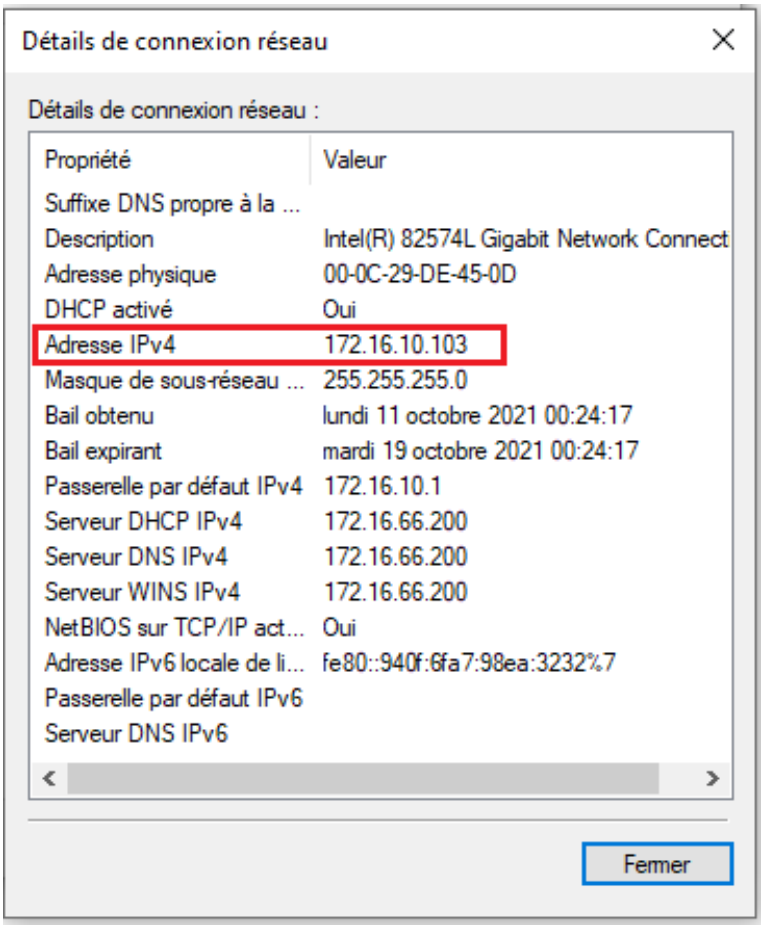

FIGURE B.11 – Adresse ipv4.

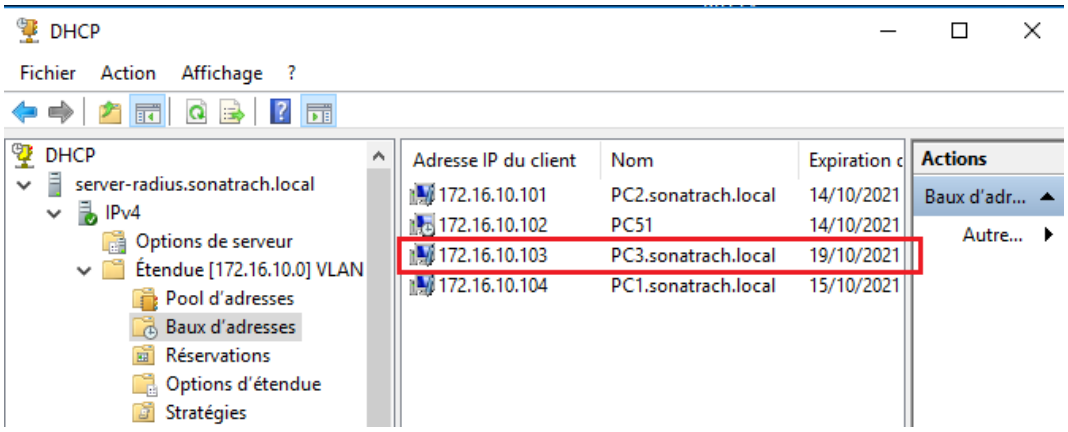

FIGURE B.12 – Serveur DHCP.

B.6 Test serveur DNS :

Pour tester le serveur DNS on va pinger vers le pare-feu à l'aide de la commande ping (nom dns) (fig B.13)et accéder au pare-feu avec (pf.sonatrach.local) au lieu de l'adresse IP (fig B.14).

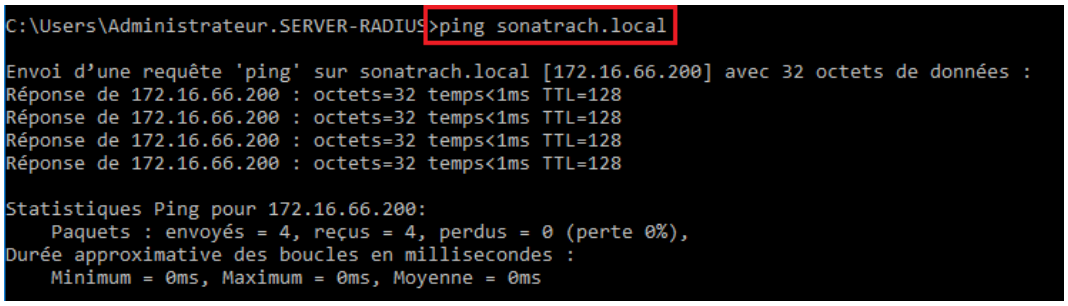

FIGURE B.13 – Ping vers le pare-feu.

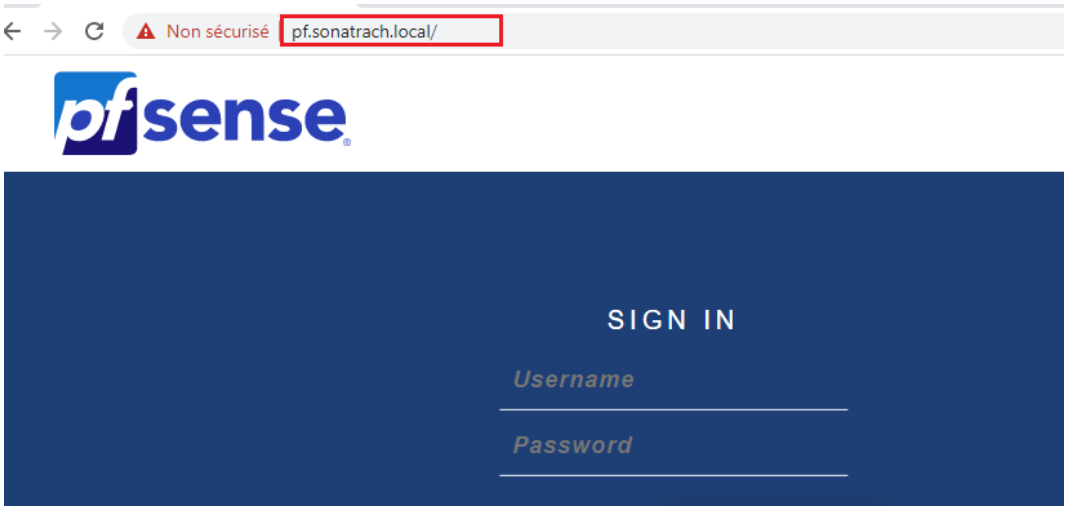

FIGURE B.14 – Accès au pare-feu.

B.7 Joindre le pc au domain

Pour joindre le pc au Domain, « Panneau de configuration Système et sécurité Système » on clique sur « Modifier les paramètre » (fig B.15).

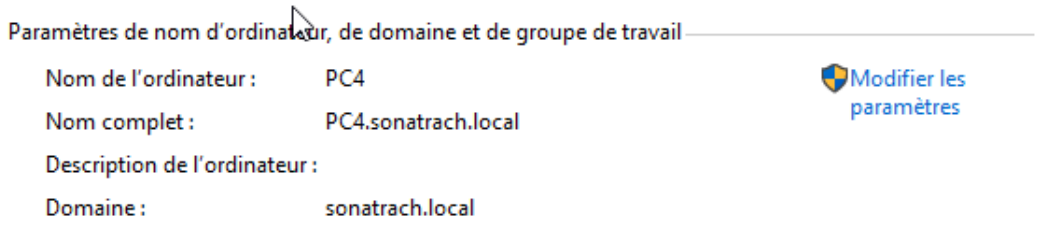

FIGURE B.15 – Joindre un domaine.

Nous allons choisir l'option qui décrit notre réseau.

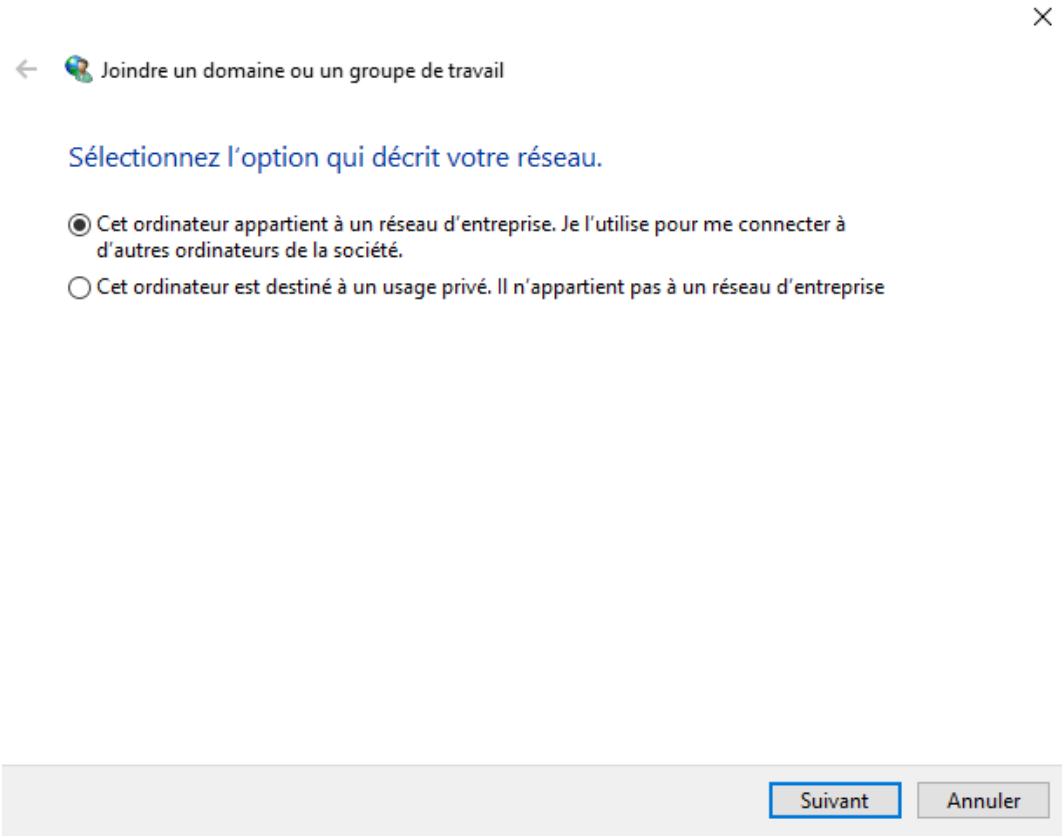

FIGURE B.16 – Choix de l'option.

Ensuite une fenêtre apparait qui nous permet d'Inséré le nom de l'utilisateur, le mot de passe et le nom du domaine (fig B.18).

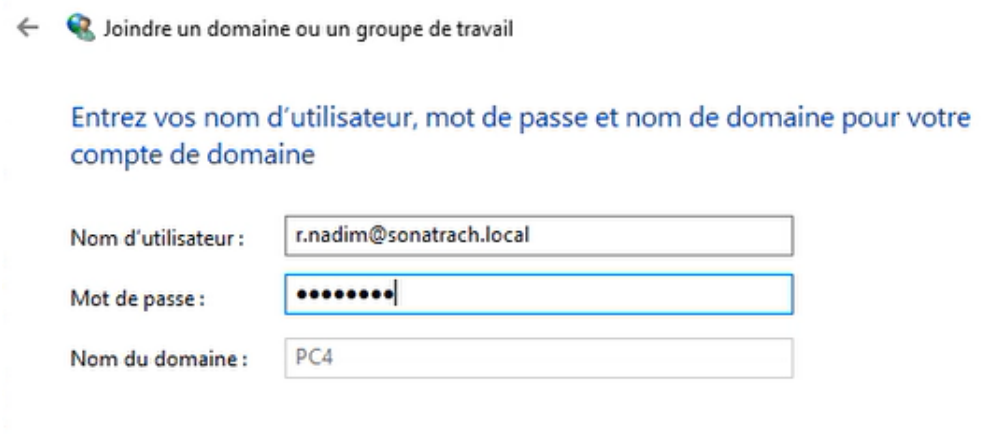

FIGURE B.17 – Information de l'utilisateur.

Ensuite nous allons choisir le type (fig B.18).

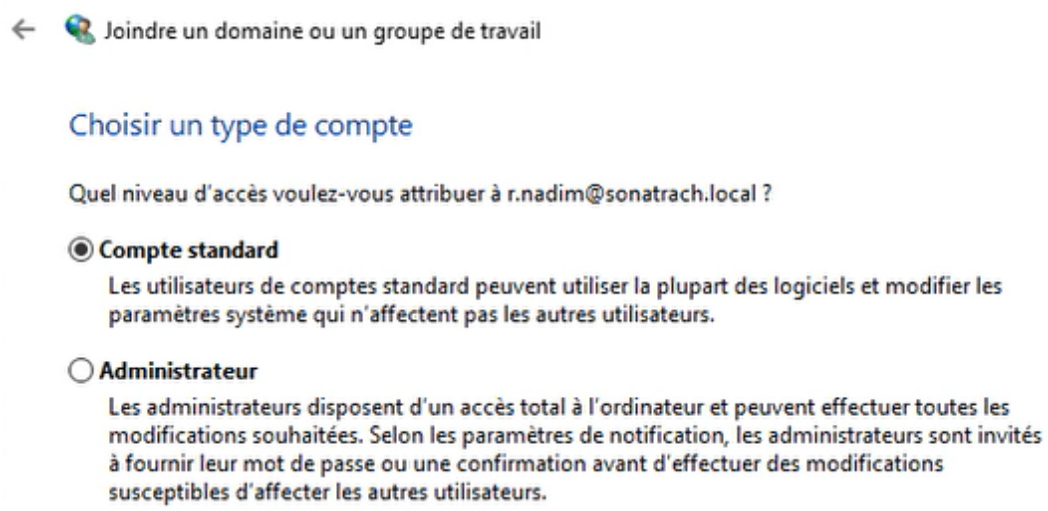

FIGURE B.18 – Choix du type de compte.

Apres avoir choisir le type du compte on va l'identifier sur le réseau, nous allons cliquer sur Identifier sur le réseau (fig B.19).

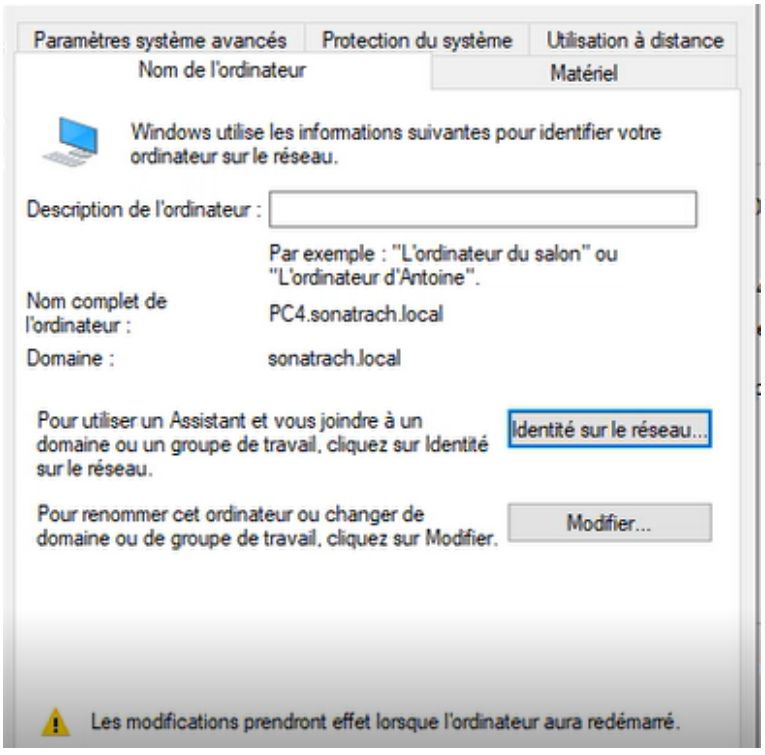

FIGURE B.19 – Joindre à un Domain.