République Algérienne Démocratique et Populaire
الجمهورية الجزائرية الديمقراطية الشعبية
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
وزارة التعليم العالي و البحث العلمي

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin d'études

En vue d'obtention du diplôme de Master professionnel en Informatique

Option : Administration et Sécurité des réseaux (ASR)

Mise en place d'une infrastructure réseau sécurisée sous Windows Server 2016 cas SONATRACH

Réalisé par :
M^{lle}.Akhelak *Chahinez*
M. Benchabane Yazid

Soutenu le 06 juillet 2022, devant le jury composé de :

Président	**Pr. Amroun Kamal**	**U. A/Mira Bejaia**
Examinateur	**Dr. Zemmoudj Salah**	**U. A/Mira Bejaia**
Encadrant	**Dr. Boudries Abdelmalek**	**U. A/Mira Bejaia**

Béjaia, Juillet 2022.

Résumé

Mettre en place un système de sécurité fiable et efficace permet aux entreprises d'assurer en quelque sorte leur progression dans le temps et de diffuser une image positive face à leurs employés et leurs clientèles, ainsi de garantir le bon fonctionnement de leurs réseaux que se soient filaires ou sans fils. Afin d'atteindre cet objectif, les administrateurs réseaux doivent mettre en place des mécanismes qui répondent le plus efficacement possible aux besoins de la sécurité de leurs réseaux, ce qui fait notre but. Pour la réalisation, nous avons commencé par un rappel sur les notions de bases des réseaux et de leur sécurité, puis, nous avons bien présenté l'organisme d'accueil SONATRACH Béjaïa afin de mieux comprendre la problématique et les concepts qui lui répondent. Enfin, nous avons passé à l'implémentation d'une solution d'authentification sécurisée sous Windows Server 2016 pour le réseau local de SONATRACH Bejaia, en utilisant le protocole RADIUS qui repose sur l'authentification 802.1x et à l'aide des protocoles HSRP et EAP et la base de données Active Directory.

Mots clés : *Authentification, Windows Server 2016, RADUIS, l'authentification 802.1x, HSRP, EAP, Active Directory.*

Abstract

Putting in place a reliable and efficient security system allows companies to ensure their progression in time and to broadcast a positive image to their employees and customers, as well as to guarantee the proper functioning of their networks whether they are wired or wireless. In order to achieve this goal, network administrators must implement mechanisms that most effectively address the security needs of their networks, which is our goal. For the realization, we started with a reminder on the basic concepts of networks and their security, then, we have well presented the host organization SONATRACH Bejaia to better understand the problem and the concepts that meet it. Finally, we moved on to the implementation of a secure authentication solution under Windows Server 2016 for the local network of SONATRACH Bejaia, using the RADIUS protocol based on 802.1x authentication and using HSRP and EAP protocols and the Active Directory database.

Keywords : *Authentication, Windows Server 2016, RADUIS, 802.1x authentication, HSRP, EAP, Active Directory.*

Dédicace

“

On dédie ce modeste travail :

A nos très chers parents, qui ont toujours été là pour nous, Vous avez tout sacrifié pour vos enfants n'épargnant ni santé ni efforts, vous nous avez donné un magnifique modèle de labeur et de persévérance. J'espère qu'ils trouveront dans ce travail toute notre reconnaissance et tout notre amour.

A nos frères et nos sœurs pour leur encouragement ainsi qu'a nos meilleurs amies

A tous nos collègues de promotion avec qui nous avons passé notre meilleure année d'études.

A toutes celles et tous ceux qui nous ont aidé dans nos études. Tous ceux qu'on connait et qu'on n'a pas pu citer.

”

Chahinez et Yazid

Remerciements

En tout premier lieu, nous remercions le bon Dieu, le tout puissant, de nous avoir accordé la force et la volonté pour achever ce travail.

Nous tenons tout d'abord à exprimer de tout cœur nos sincères remerciements à notre encadrant ***Dr. Boudries Abdelmalek*** *pour avoir bien voulu nous accompagner tout au long de la préparation de ce projet, pour les sages conseils et recommandations qui nous ont permis de réaliser ce modeste travail. Ainsi qu'aux membres de jury* ***Pr. Amroun Kamal*** *et* ***Dr Zemmoudj Salah*** *qui ont accepté d'évaluer notre travail. Qu'ils trouvent ici l'expression de notre profonde gratitude.*

Nous adressons également nos sincères remerciements au personnel de l'entreprise SONATRACH qui ont eu la gentillesse de bien vouloir nous accorder de leur précieux temps pour participer dans la réalisation de ce travail en mettant à notre disposition leurs connaissances et leur documentation.
Nos sincères remerciements vont également à tous les enseignants du département d'Informatique de l'université ***ABDERRAHMANE MIRA de Bejaia****.*

Ainsi qu'à ceux et celles qui par, leurs paroles, leurs écrits, leurs conseils et leurs critiques ont guidé nos réflexions et ont accepté à nous rencontrer et répondre à nos questions durant la réalisation de ce travail.

Nous tenons à remercier tous ceux et celles qui ont contribué de prés ou de loin à l'accomplissement de ce travail.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AAA	*Authentication Authorization Accounting*
AD	*Active Directory*
CA	*Certification Authority*
CHAP	*Challenge Handshake Authentication Protocol*
CLI	*Command Line Interface*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name Server*
DoS	*Disk Operating System*
EAP	*Extensible Authentication Protocol*
EAP-FAST	*Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling*
EAP-MD5	*Extensible Authentication Protocol Message Digest 5*
EAP-TLS	*Extensible Authentication Protocol- Transport Layer Security*
ENAC	*Entreprise Nationale de Canalisations*
ENIP	*Entreprise Nationale des Industries Pétrochimie*
GNS3	*Graphical Network System 3*
HSRP	*Hot Standby Router Protocol*
ID	*Identifier*
IEEE	*Institute of Electrical and Electronics Engineers*

IOS *Internetwork Operating System*

IP *Internet Protocol*

LAN *Local Area Network*

LDAP *lightweight Directory Access Protocol*

LEAP *Lightweight Extensible Authentication Protocol*

MAC *Media Access Control*

MAN *Metropolitan Area Network*

MS-CHAP : *Microsoft Challenge Handshake Authentication Protocol*

MS-CHAPv2 *Microsoft Challenge Handshake Authentication Protocol Version*

NAP *Network Access Protection*

NAS *Network Access Server*

NetBIOS *Network Basic Input Output System*

NPS *Network Policy Server*

OSI *Open Systems Interconnexion*

PAN *Personal Area Network*

PAP *Password Authentication Protocol*

PEAP *Protected Extensible Authentication Protocol*

PPP *Point to Point Protocol*

QoS *Quality of Service*

RADIUS *Remote Access Dial In User Service*

RTC *Region Transport Centre*

SQL *Structured Query Language*

SPAP *Shiva Password Authentication Protocol*

SSH *Secure shell*

SYSVOL *System Volume*

TCP *Transmission Control Protocol*

TTLS *Tunneled Transport Layer Security*

UDP *User Datagram Protocol*

VLAN *Virtual Local Area Network*

VM *Virtual Machine*

VoIP *Voice over Internet Protocol*

VPN *Virtual Private Network*

WAN *Wide Area Network*

Introduction générale

L'informatique est devenue un élément incontournable de gestion, d'organisation, de production et de communication. Le réseau informatique de l'entreprise met en œuvre des données sensibles, les stocke, les partage en interne, les communique parfois à d'autres entreprises. Cette ouverture vers l'extérieur conditionne des gains de productivité et de compétitivité.

Il est donc impossible de renoncer aux bénéfices de l'informatisation, d'isoler le réseau de l'extérieur, de retirer aux données leurs caractères électroniques et confidentiels. Les données sensibles du système d'information d'une entreprise sont exposées aux actes de malveillance telle que l'augmentation des nombres d'hacker, cyber crime.

Il est donc capital de veiller à la sécurité des données aussi bien en interne qu'à l'extérieur. L'entreprise prise comme exemple dans notre mémoire, dispose d'un réseau informatique qui lui permet de faire des échanges d'information avec ses partenaires. Par conséquent elle doit gérer et sécuriser son système d'information. Outre cette ouverture de l'extérieur, elle est menacée à l'intérieur de son réseau local par des virus informatiques et quelques disfonctionnements de son système informatique.

C'est pour palier à ces problèmes précités et dans le souci de rendre le réseau informatique évolutif, disponible et sécurisant, notre choix est porté à auditer et sécuriser une infrastructure réseau sous windows Server 2016 en utilisant l'authentification Radius accès à distance basé sur la norme IEEE 802.1x.

Organisation du mémoire

Ce travail est organisé en quatre chapitres :

Le premier chapitre consiste à définir les notions de base des réseaux et de la sécurité informatique.

Le deuxième chapitre se porte sur la présentation de l'organisme d'accueil de l'entreprise SONATRACH de Bejaïa avec la problématique posée de son réseau informatique.

Le troisième chapitre explique la conception, le déploiement et l'étude de l'infrastructure proposée avec la mise en œuvre d'authentification RADIUS accès à distance et l'authentification 802.1x sous Windows server 2016, en présentant les différents outils

déployés pour l'implémentation de cette solution.

Le dernier chapitre porte sur l'implémentation et les étapes de configuration ainsi que les tests de l'authentification des utilisateurs par le mécanisme de sécurité retenu.

Enfin, on clôture le travail par une conclusion générale qui décrit brièvement les éléments essentiels développés dans ce mémoire et quelques perspectives pour ce projet.

Chapitre 1

Généralités sur les réseaux et la sécurité informatique

1.1 Introduction

Les attaques informatiques ne cessent d'être dirigées contre les entreprises, petites ou grandes soient elles. En effet, la menace qui plane sur un système est un fait, plus l'entreprise possède des informations importantes, plus elle y sera soumise. Cependant, il existe des moyens qui permettent de garder le seuil de sécurité des systèmes élevé, en mettant en place des contre-mesures pour réduire les risques d'attaques et la compromission des données.La sécurité engendre généralement le déploiement de moyens techniques et surtout des solutions de préventions. Ces dernières doivent prendre en compte la formation et la sensibilisation de tous les acteurs de l'entreprise sur les risques encourus. Ainsi il faut mettre en place une bonne politique de sécurité fondée sur la collaboration de l'ensemble des employés et l'utilisation d'équipements et techniques qui répondent aux exigences du système tout en assurant un blocage d'attaques informatiques de tout genre. Dans ce chapitre, nous aborderons les différents aspects liés à la sécurité et la protection des réseaux informatiques.

1.2 Réseau informatique

1.2.1 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipement informatiques (ordinateurs et périphériques) reliés entre eux grâce à des supports de communication (câbles : réseau câblé, ou ondes : réseau sans fil...) permettant la communication (transfert des informations électroniques) et le partage de ressources (matérielles et logicielles).

1.2.2 L'architecture des réseaux

Les réseaux sont structurés du point de vue fonctionnel en deux catégories :

- Réseaux poste à poste (peer to peer).
- Réseaux à serveur dédié (client/serveur).

1.2.3 Les topologies des réseaux

Les réseaux informatiques sont spécifiés selon leurs différentes topologies [1] :

1. **Topologie en bus** : Dans cette topologie, les ordinateurs sont disposés et reliés de part et d'autre d'un câble principal appelé bus. Le support de transmission utilisé dans ce cas est le câble coaxial. Dans cette topologie, lorsqu'un ordinateur envoi une information, tous les autres ordinateurs du réseau reçoivent l'information mais seul la machine à qui l'information est destinée va l'utiliser.
2. **Topologie en anneau** : Dans cette topologie, les ordinateurs sont connectés à une boucle et communiquent chacun à leur tour. Les informations circulent dans une direction unique, d'un ordinateur à un autre .
3. **Topologie en étoile** : Dans cette topologie, les ordinateurs du réseau sont reliés à un équipement central appelé concentrateur (hub) ou un commutateur (Switch). Celui-ci a pour rôle d'assurer la communication entre les différents ordinateurs connectés à lui.
4. **Topologie en Maille** : Dans cette topologie, chaque ordinateur est directement relié à tous les autres. Ainsi lorsqu'un ordinateur veut envoyer une information à un autre celui-ci le fait de façon directe sans passer par un équipement spécifique.
5. **Topologie en Arbre** : Une topologie arborescente est une combinaison des différentes autres topologies, elle peut reposer à la fois sur des topologies en bus, en étoile et en anneau.

La figure 1.1 [2] illustre les différentes topologies citées au-dessus :

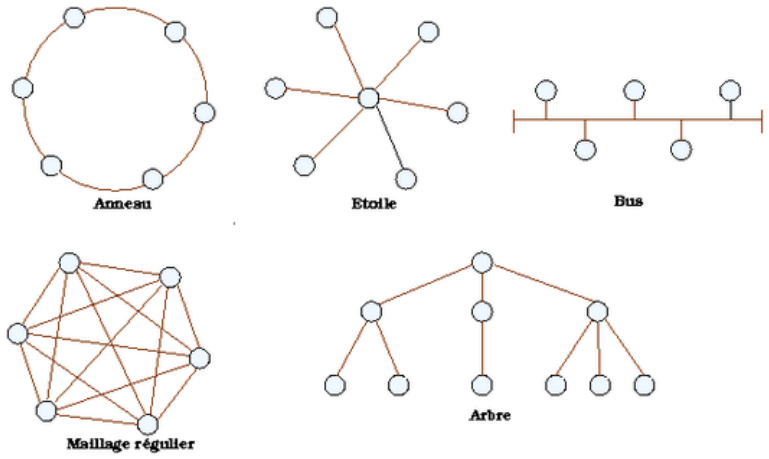

FIG. 1.1 : Les topologies réseaux.

1.2.4 Classification des réseaux selon leur étendu géographique

1. **LAN (Local Area Network = réseau local d'entreprise, RLE en français)** : est un réseau d'ordinateurs situés sur un même site. Les communications sur ce type de réseau y sont généralement rapides (100 Mbits/s ou 1Gbits/s) et gratuites puisqu'elles ne passent pas par les services d'un opérateur de télécommunication. Le fait que le réseau soit sur un site bien délimité n'implique pas nécessairement qu'il soit de taille très réduite. Il est souhaitable de le segmenter en sous-réseaux quand le nombre de nœuds y devient important. L'ensemble reste un réseau local tant qu'il est indépendant des services d'un opérateur extérieur.

2. **MAN (Metropolitan Area Network = Réseau métropolitain)** : Lorsqu'un réseau privé s'étend sur plusieurs kilomètres, dans une ville par exemple les réseaux locaux sont interconnectés via des liaisons téléphoniques à haut débit ou à l'aide d'équipements spéciaux comme des transmissions hertziennes. Ce type de regroupement de réseaux locaux peut se faire au niveau d'une ville et l'infrastructure du réseau métropolitain peut être privée ou publique.

3. **WAN (Wide Area Network = Réseau étendu)** : Ces réseaux relient plusieurs réseaux locaux en les interconnectant via des lignes louées ou via Internet. Ex. les réseaux bancaires qui établissent des liaisons entre les agences et le siège central. Dans le cas de l'utilisation d'Internet, on parle de VPN (Virtual Private Network) puisqu'on utilise alors un réseau public pour faire transiter des informations privées.

4. **PAN (Personal Area Network = réseau d'étendue limitée à quelques mètres)** : pour l'interconnexion des équipements personnels (GSM, PDA, PC et PC portable) d'un seul utilisateur.

1.2.5 Les composants matériels d'un réseau

Equipements d'interconnexion

Un réseau informatique est composé des équipements d'interconnexion suivants [3] :

1. **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 regroupées en paquet composé d'un entête qui contient 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 faite pas partie des équipements d'interconnexion des réseaux).

2. **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.

3. **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 et les diffuser sur l'ensemble des ports.

4. **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 connectées et d'analyser les trames reçues pour les diriger vers la machine de destination.

5. **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. **La passerelle** : La passerelle est un système matériel et logiciel permettant de relier deux réseaux, servant d'interfaces entre deux protocoles différents. Lorsqu'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 la transmission de deux protocoles. Ce système permet de relier deux systèmes informatiques qui n'utilisent pas la même architecture.

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

Support de transmission

1. **Câble coaxial** : il est constitué de deux conducteurs cylindriques de même axe (l'âme et la tresse).

2. **Fibre optique** : est une technologie qui permet la disposition d'un accès internet, en propageant des ondes lumineuses entre deux lieux, elle constitue un fil en verre ou en plastique qui sert dans les transmissions terrestres et océaniques de données.

3. **Câble à paires torsadées** : convient à la transmission analogique comme numérique, il existe deux types :

   - Câble à paires torsadées blindées.
   - Câble à paires torsadées non blindées.

4. **Transmission sans fil** : Le WI-FI est un ensemble de protocoles de communication sans fil, qui permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, Smartphone…etc.) au sein d'un réseau afin de permettre la transmission de données entre eux

Périphériques finaux

Forment l'interface entre les utilisateurs et le réseau de communication sous-jacent. Voici quelques exemples de périphériques finaux :

- Ordinateur.
- Imprimantes réseau.
- Téléphones VoIP.
- Caméras de surveillance.
- Serveur (physique ou virtuel).

1.2.6 Modèles de communication

Modèle OSI

Créé par l'Organisation internationale de normalisation, le modèle conceptuel OSI (Open Systems Interconnection) permet à divers systèmes de communication de communiquer à l'aide de protocoles standard. En clair, l'OSI constitue une norme permettant à différents systèmes informatiques de communiquer entre eux.
Fondé sur le concept de division d'un système de communication en sept couches abstraites, empilées les unes sur les autres, le modèle OSI peut être considéré comme un langage universel pour les réseaux informatiques. La figure 1.2 [4] illustre le modèle OSI avec ses différentes couches :

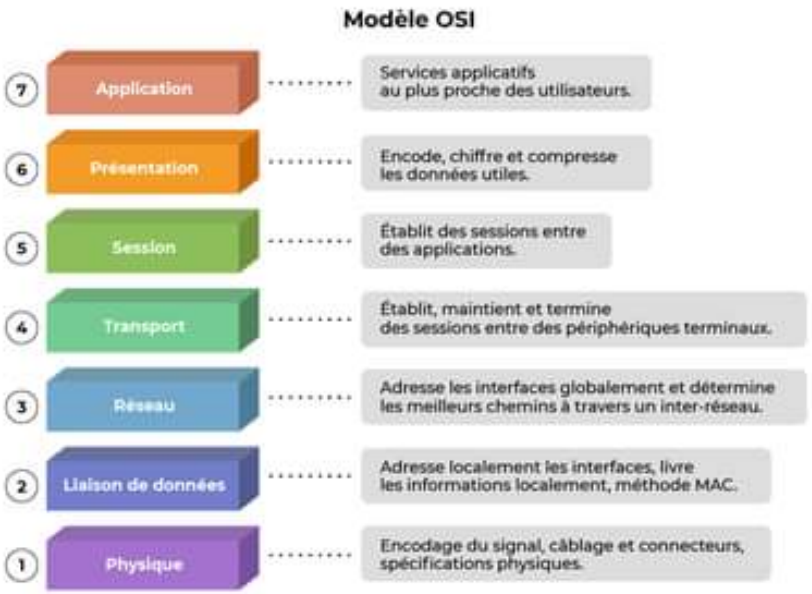

Fig. 1.2 : Le modèle OSI.

- **Les couches du modèle OSI**

  1. **Couche physique** : est chargée de la transmission effective des signaux entre les interlocuteurs.
  2. **Couche liaison de données** : gère les communications entre deux machines directement connectées entre elles, ou connectées à un équipement qui émule une connexion directe (commutateur).
  3. **Couche réseau** : gère les communications de proche en proche, généralement entre machines : routage et adressage des paquets.
  4. **Couche transport** : gère les communications de bout en bout entre processus (programmes en cours d'exécution). Cette fonction est réalisée par les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) de la famille des protocoles TCP/IP.
  5. **Couche session** : gère la synchronisation des échanges et les « transactions », permet l'ouverture et la fermeture de session.
  6. **Couche présentation** : est chargée du codage des données applicatives, précisément de la conversion entre données manipulées au niveau applicatif et chaînes d'octets effectivement transmises.
  7. **Couche application** : est le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme.

Modèle TCP/IP

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise « par-dessus » un protocole réseau, IP (Internet Protocol). Ce qu'on entend par « modèle TCPIP », c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante.
Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.
La figure 1.3 [5] représente l'architecture du modèle TCP/IP.

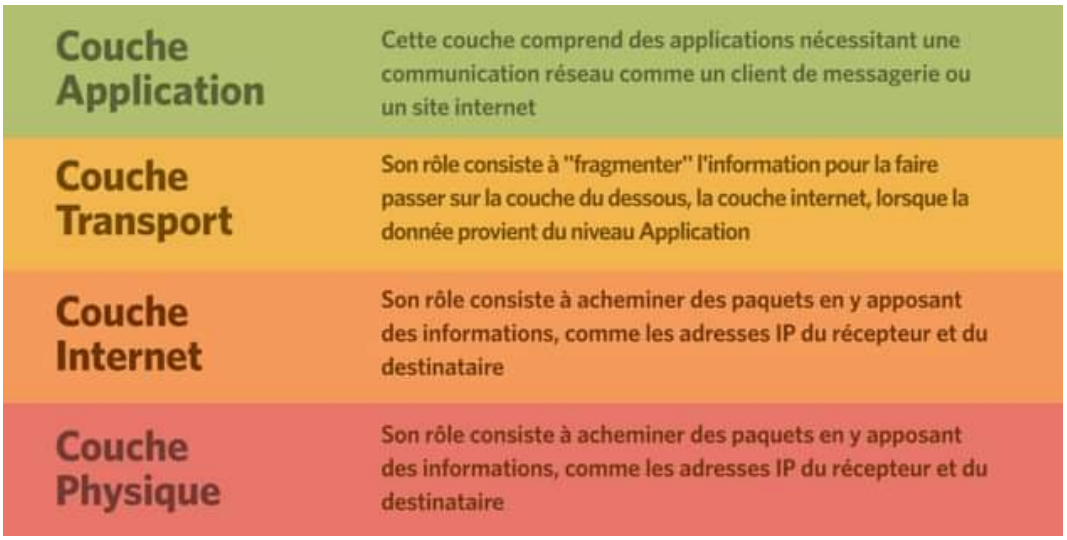

Fig. 1.3 : Le modèle TCP/IP.

1.3 La sécurité informatique

1.3.1 Définition de la sécurité informatique

La sécurité d'un réseau est un ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir sa sécurité. En général, la sécurité d'un réseau englobe celle du système informatique sur lequel il s'appuie [6].

1.3.2 Critères de la sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs [7] :

- 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.

1.3.3 Définition de la politique de sécurité

Toute technique concourant à la protection de l'information contre un large éventail de menaces afin de garantir la continuité des activités de l'entreprise, réduire les dommages éventuels et sur ces activités et maximiser le retour sur l'investissement des systèmes d'information.

1.3.4 Etablissement de la politique de sécurité

- Identifier les risques et leurs conséquences.
- Evaluation des probabilités associées à chacune des menaces.
- Evaluation du cout d'une intrusion réussie.
- Elaborer des règles et des procédures à mettre en œuvre pour les risques identifiés.
- Evaluation des couts des contre-mesures.

1.3.5 Les attaques

Les "attaques informatiques" ou "cyberattaques" sont des actions volontaires et malveillantes menées au moyen d'un réseau informatique visant à causer un dommage aux informations et aux personnes qui les traitent. Et tout le monde peut en être la cible : les particuliers, les entreprises, les institutions, les services administratifs et de santé etc.
Une cyberattaque peut être le fait d'une personne seule (hacker), d'un groupe de pirates, d'une organisation criminelle ou même d'un État. Ces attaques informatiques sont facilitées par la quantité croissante d'informations mises en ligne et par des failles de sécurité dans les systèmes [8].
Il existe deux types :

- **Attaque passive** : écoute non autorisée.
- **Attaque active** : altération des données.

Les attaques sont d'origine :

- **Interne** : Utilisateur malveillant, erreur involontaire…etc.
- **Externe** : Piratage, virus, intrusion…etc.

Programmes malveillants simples

Sont des programmes développés dans le but de nuire à un système informatique sans le consentement de l'utilisateur que son ordinateur est infecté, ils ne se propagent pas seuls mais à l'aide d'une intervention humaine.

- **Programmes commerciaux indésirables** : sont des programmes indirectement dédiés à des taches d'intrusion ou piratage.
- **Bombe logique** : Est un programme avec une fonction malveillante et destructrice ajoutée de façon illicite à un programme hôte.
- **Cheval de Troie** : Est un petit programme au sein d'un autre programme hôte qui ouvre des portes virtuelles pour les hackers.

- **Porte dérobée** : Est un programme qui surveille et qui prend le contrôle d'un ordinateur.
- **Virus** : Est un programme parasite capable de s'installer sur un ordinateur à l'insu de l'utilisateur provocant diverses perturbations dans le fonctionnement du système.

Programme malveillant autoreproducteurs

Sont des programmes qui se reproduisent seuls, à leur première exécution, ils cherchent à se reproduire donc ils seront résidants en mémoire, et dans un premier temps discret, puis la fonctionnalité malveillante s'effectue dans un délai court.

- **Ver** : est un programme qui peut se reproduire et déplacer à travers un réseau en utilisant les mécanismes réseau, lorsqu'il est exécuté, il construit des copies de lui-même et les griffent aux ordinateurs qu'il cible.

1.3.6 Les mécanismes de protection

Pare-feu

Un pare-feu (ou firewall) est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).
Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

La cryptographie

La cryptographie est une méthode de protection des informations et des communications par l'utilisation de codes, de sorte que seuls les destinataires des informations puissent les lire et les traiter.
En informatique, elle désigne des techniques d'information et de communication sécurisées dérivées de concepts mathématiques et d'un ensemble de calculs basés sur des règles, appelés algorithmes, pour transformer les messages de manière difficile à déchiffrer. Ces algorithmes déterministes sont utilisés pour la génération de clés cryptographiques, la signature numérique, la vérification pour protéger la confidentialité des données, la navigation sur Internet et les communications confidentielles telles que les transactions par carte de crédit et le courrier électronique [9].

- **Le chiffrement symétrique** : est un chiffrement dans lequel la clé de chiffrement sert également à déchiffrer. On parle alors de clé secrète.
- **Le chiffrement asymétrique** : vient concrétiser la différence entre la clé de chiffrement et de déchiffrement. En pratique, la clé de chiffrement sera nommée clé publique car elle sera librement communiquée. La clé de déchiffrement sera nommée clé privée car elle ne doit être communiquée sous aucun prétexte [9].

1.4 Conclusion

Dans ce chapitre, on a présenté les principaux concepts et notions liés aux réseaux et à la sécurité informatique, dont on a décrit les attaques et les différents mécanismes et méthodes connus pour sécuriser le réseau.
A travers les différentes sections montrées ci-dessus, on conclut qu'aucun réseau n'est sûr à 100%, et qu'il est impossible de garantir la sécurité totale d'un réseau. Il devient donc urgent de mettre en place une politique de sécurité qui doit être bien réfléchit et étudiée selon l'entreprise pour satisfaire au mieux les besoins de la sécurité. Dans le chapitre qui suit, nous présentons 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 etc.
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 approuve 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 [10]. SONATRACH est divisé en cinq branches différentes représentées dans la figure 2.1 [11] :

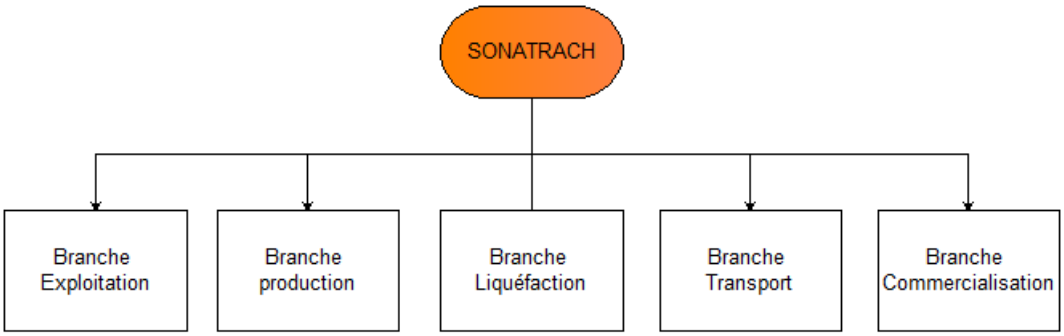

FIG. 2.1 : organigramme de SONATRACH.

2.3 Présentation du centre informatique

Le centre informatique est chargé du développement et de l'exploitation des applications informatiques de gestion pour le compte du régional centre de Bejaïa (RTC) et des autres régions.

2.3.1 Organisation de centre informatique

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 2.2 [11] :

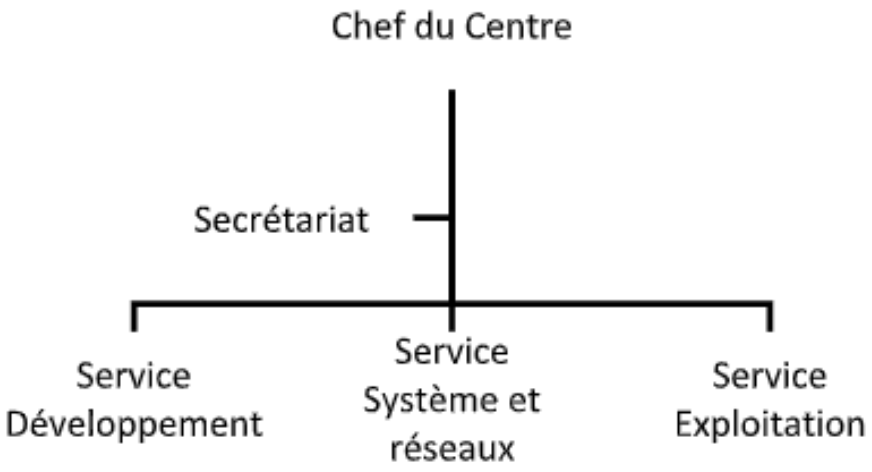

FIG. 2.2 : Organigramme du centre informatique.

2.3.2 Le rôle de chaque service

- **Service développement** : il est Chargé de bénéficier des nouvelles technologies qu'il acquière tout en optimisant leurs utilisations, ainsi que la prise en charge des besoins des différentes structures de la direction en matière de développement de nouveaux systèmes d'information :
  - Etude et analyse.
  - Réalisation d'applications informatique. Le service prend aussi en charge les taches de maintenance, ex : manque d'effectif durant la période des congés ou généralement en cas de besoins.
- **Service système et réseaux** : Il est chargé d'assurer les tâches suivantes :
  - L'administration des serveurs.
  - L'administration des bases de données sur les serveurs.
  - Installation des logiciels sur serveurs.
  - Gestion des performances système et réseau.
  - Gestion de la sécurité et des utilisateurs connectes au réseau (droits d'accès).
  - Gestion du parc informatique.
  - La prise en compte et résolution des pannes.
  - Planification et ordonnancement des travaux.
  - Sauvegarde et restauration des données.
  - Gestion des espaces disques.
  - Exploitation (saisie, validation, traitement) des anciennes applications batch pour la RTC et les autres directions régionales.

- **Service support** : Ce service assure la maintenance logicielle et matérielle informatique.

2.4 Présentation de la région transport centre (RTC)

2.4.1 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 arrêtent 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 (Bejaïa).
- La Région transport Ouest (Arzew).
- La Région transport de Haoud-El-Hamra.
- La Région transport d'Ain Amenas.

2.4.2 Organigramme de la RTC

Nous illustrons les directions et sous-directions dans le diagramme de la figure 2.3 [11] Comme suit :

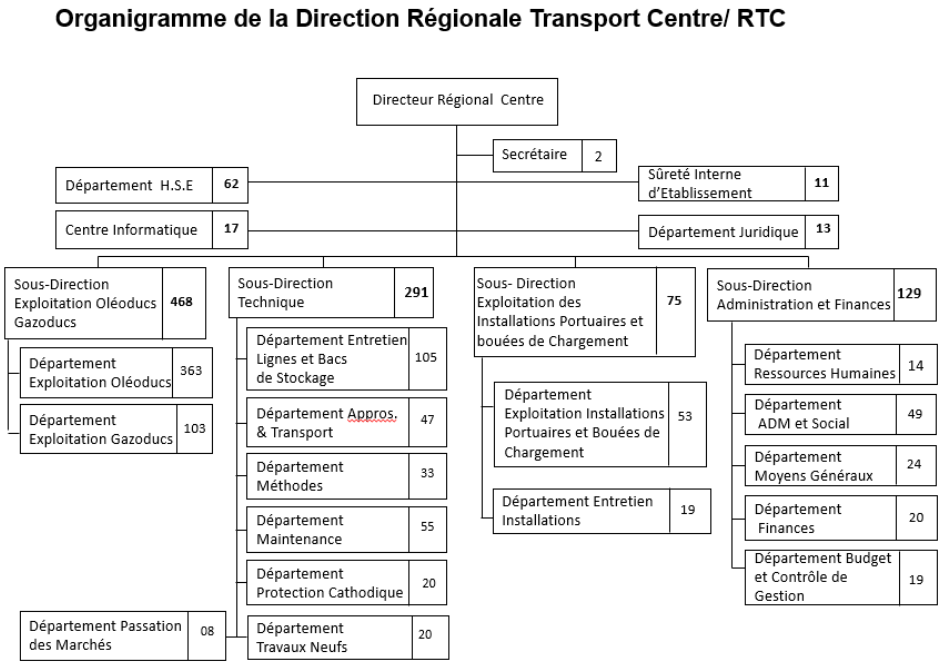

Fig. 2.3 : Organigramme de la RTC.

2.5 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 (distribution layer), et une couche d'accès (Access layer), comme le représente la Figure 2.4 [11].

2.5.1 Modèle Hiérarchique

Le modèle hiérarchique est composé de trois couches présentées ci-dessous :

- **La couche cœur de réseau (Core layer)** :

  C'est la couche supérieure dont le rôle consiste à relier entre eux les différents segments d'un réseau à savoir : les sites distants, les réseaux locaux (LANs) ou les étages de l'immeuble d'une société. Cette couche est aussi appelée Backbone [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 nécessite 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].

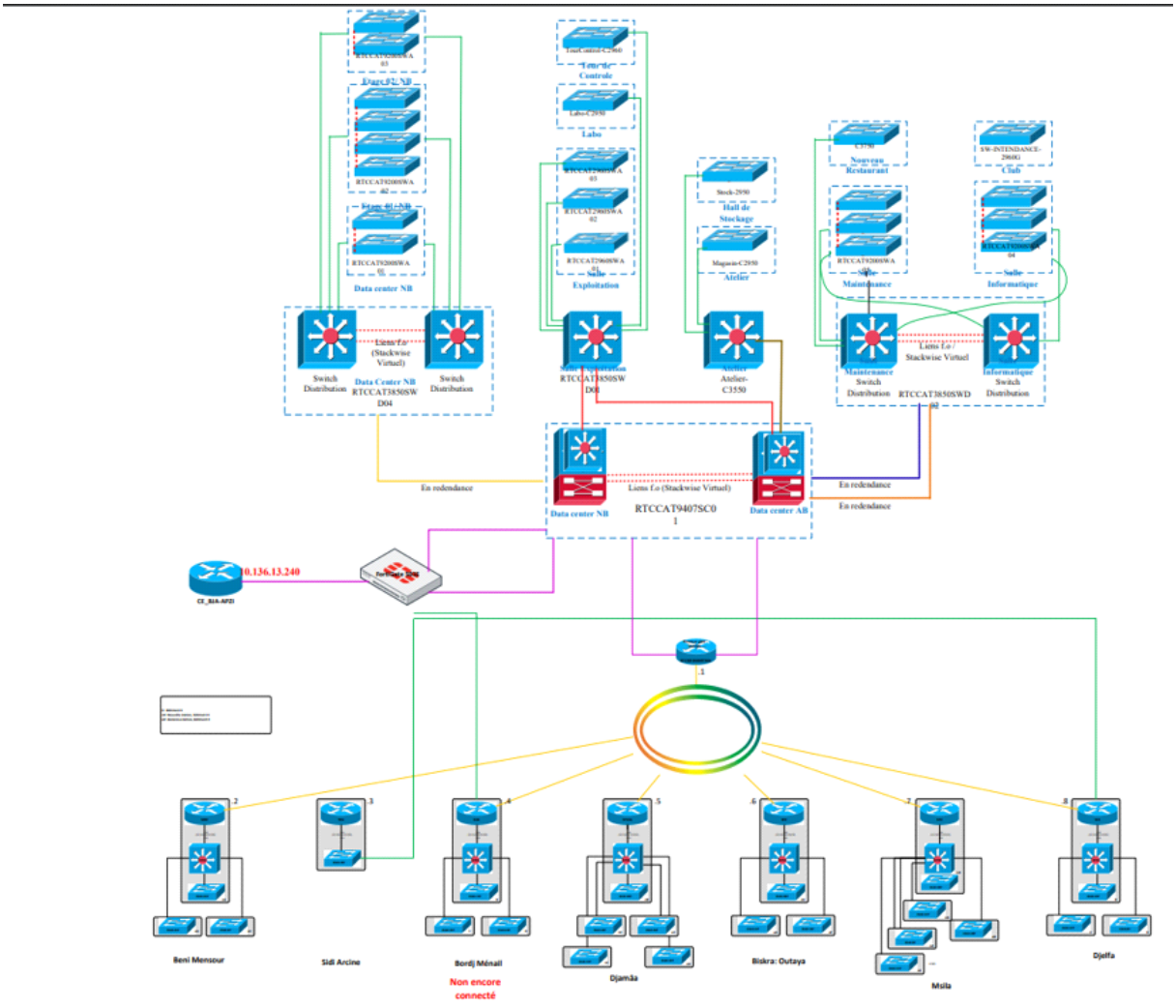

Fig. 2.4 : Modèle hiérarchique du réseau de l'entreprise.

2.5.2 Commutateurs utilisés dans le réseau de la RTC

Le réseau de la RTC utilise les commutateurs suivants :

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 colocalisées et les déploiements de services.

En outre elle offre une protection exceptionnelle des investissements en soutenant plusieurs générations de produits sur le même châssis, réduisant ainsi les coûts totaux de propriété. Le cadre Cisco Catalyst 6509 supporte à la fois la gamme Cisco Catalyst 6500 Supervisor Engine 32 et Cisco Catalyst 6500 Séries Supervisor Engine 720 familles, avec LAN associés, WAN, et des modules de services [13].

Fig. 2.5 : Commutateur Catalyst Cisco 6509.

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].

Fig. 2.6 : Commutateur Catalyst Cisco 3750.

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].

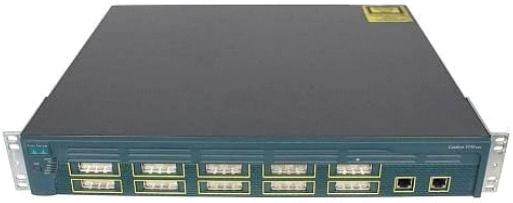

FIG. 2.7 : Commutateur Catalyst Cisco 3550.

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].

FIG. 2.8 : Commutateur Catalyst Cisco 2950.

2.6 Problématique

De nos jours, la plupart des entreprises possèdent de nombreux postes informatiques qui sont en General reliées entre 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 une porte ouverte à divers acteurs étrangers. Cette porte peut être exploitée 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** : (RADIUS pour les connexions à distance ou VPN et RADIUS pour les connexions câblées ou sans fil « norme 802.1X ») pour la sécurité du réseau local de l'entreprise.
- **Pare-feu** : Pour établir une barrière entre les réseaux internes sécurisés et contrôlés auxquels il est possible de se fier et les réseaux externes qui n'ont pas de contenu de confiance, comme Internet.

2.7 Conclusion

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

Chapitre 3

Conception et déploiement de l'infrastructure réseau

3.1 Introduction

La mise en place d'une infrastructure réseau constitue une obligation pour toute société moderne et ambitieuse. Celle-ci s'apparente à la charpente de toute organisation informatique car le bon fonctionnement des équipements et logiciels en dépend. Elle favorise une transmission rapide et sécurisée des données, c'est à dire les agents d'une société transmettent et échangent en toute sécurité des données.et ils accèdent à Internet et à des applications spécifiques.
Cet outil peut également intégrer une plateforme de travail collaboratif. Les infrastructures réseau se démarquent généralement par leur portée géographique, la technologie exploitée pour le transfert des fichiers, les types de signaux ainsi que les connexions et les liaisons physiques utilisées.

Dans ce chapitre nous allons apporter une solution à la problématique citée dans le deuxième chapitre. Nous ferons appel à la norme 802.1x, en mettant en œuvre une solution d'authentification autour de serveur RADIUS.

3.2 Présentation des outils

- **GNS3 (Graphical Network Simulator-3)** :
  On a utilisé GNS3 qui est une interface graphique frontale et une plateforme de contrôle écrite en Python pour simuler des infrastructures informatiques, on le connait généralement avec VMware ou Virtual Box, Il permet d'exécuter un IOS Cisco dans un environnement virtuel sur votre ordinateur, de plus, un utilisateur peut créer des topologies de réseau de Windows en utilisant de simples fichiers de type ini.

- **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'exploitation.

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

- **Utilisateurs Windows** :
  Nous avons 5 Utilisateurs des différents VLANs pour faire nos différents tests, 5 PC sous Windows.

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

- **Commutateur niveau 3** :

  Nous avons utilisé des switchs niveau 3 qui s'agissent simplement des switchs capables d'effectuer du routage. Ils garantissent le coté performance et réduisent la latence.

3.3 Technologie des réseaux de Cœur (CORE)

3.3.1 HSRP

HSRP est un protocole Cisco permettant d'assurer la haute disponibilité de la passerelle d'un réseau. Ce protocole peut être mis en place sur un routeur ou un switch de niveau 3.
Le but est qu'une éventuelle panne du routeur ne perturbe pas le routage [17]. Le principe d'HSRP est relativement simple. Nous avons un groupe de routeurs (en général 2), dont l'un d'eux est le routeur **Actif**.

- Le routeur de secours sera en **Standby**. Les autres en mode **Listen**.

- Le routeur actif assure le rôle de passerelle par défaut pour le sous réseau.

S'il vient à tomber en panne, le routeur standby prendra le relai. Puis un des routeurs Listen deviendra le nouveau Standby. Nous retrouverons un réseau de ce type [17] :

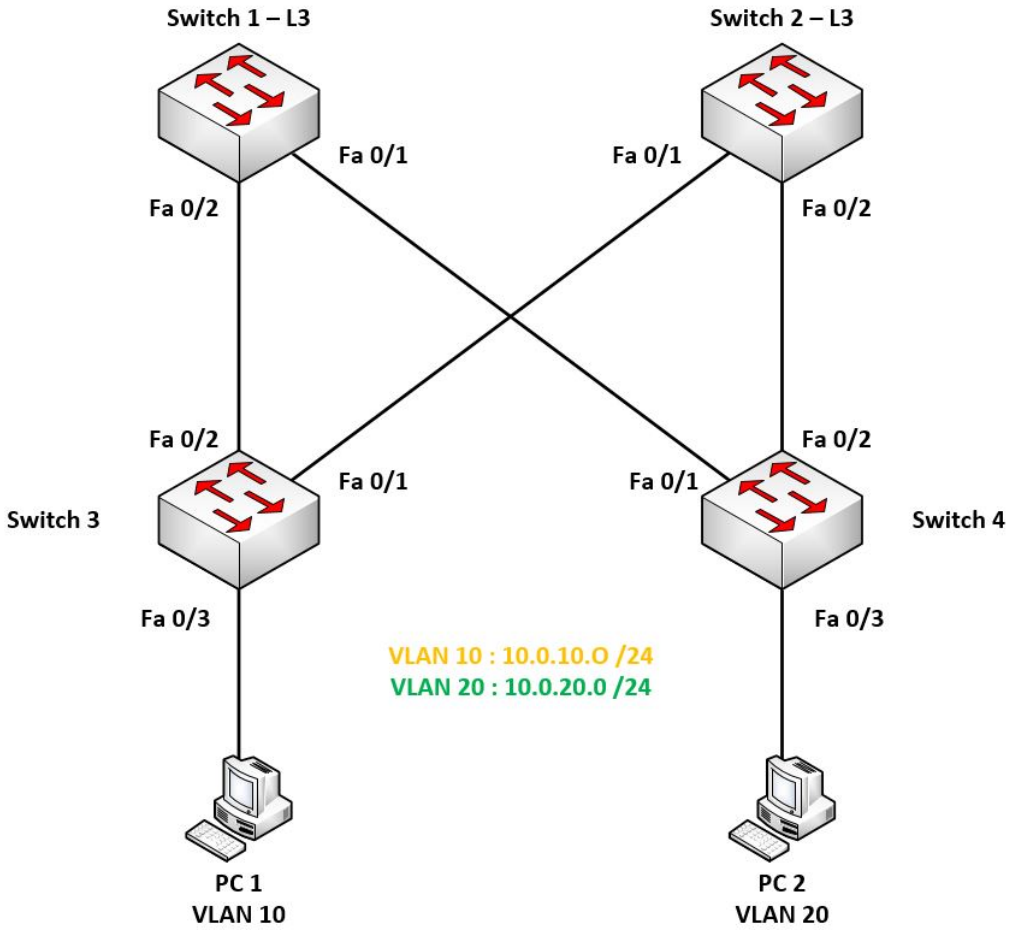

FIG. 3.1 : Fonctionnement du routeur Standby.

Le groupe de routeur est appelé **Standby Group**.

- Le routeur actif est celui qui a la priorité la plus haute.
- Le routeur standby est celui ayant la deuxième meilleure priorité. Les autres routeurs sont en mode Listen. La priorité va de 0 à 255.

En cas d'égalité sur la priorité, c'est le routeur avec la plus haute IP qui devient actif.

_ S1 et S2 sont des switchs de niveau 3. Si S1 est le switch actif, les PC utiliseront S1S1 comme Gateway.

_ Si S1 vient à tomber en panne, S2 prendra le relai, et les PC l'utiliseront comme Gateway [17].

3.3.2 SpanningTree

Définition

Est l'un des principaux protocoles que l'on retrouve au niveau 2. Il permet d'éviter les boucles dans un réseau, mais aussi de profiter des topologies redondantes, sans risque de

créer des boucles [18].

Le rôle de Spanning-Tree

Spanning-Tree aura pour rôle de désactiver les liens qui peuvent créer une boucle. Il se chargera les réactiver si nécessaire (en cas de panne d'un autre lien).

3.4 L'architecture proposée

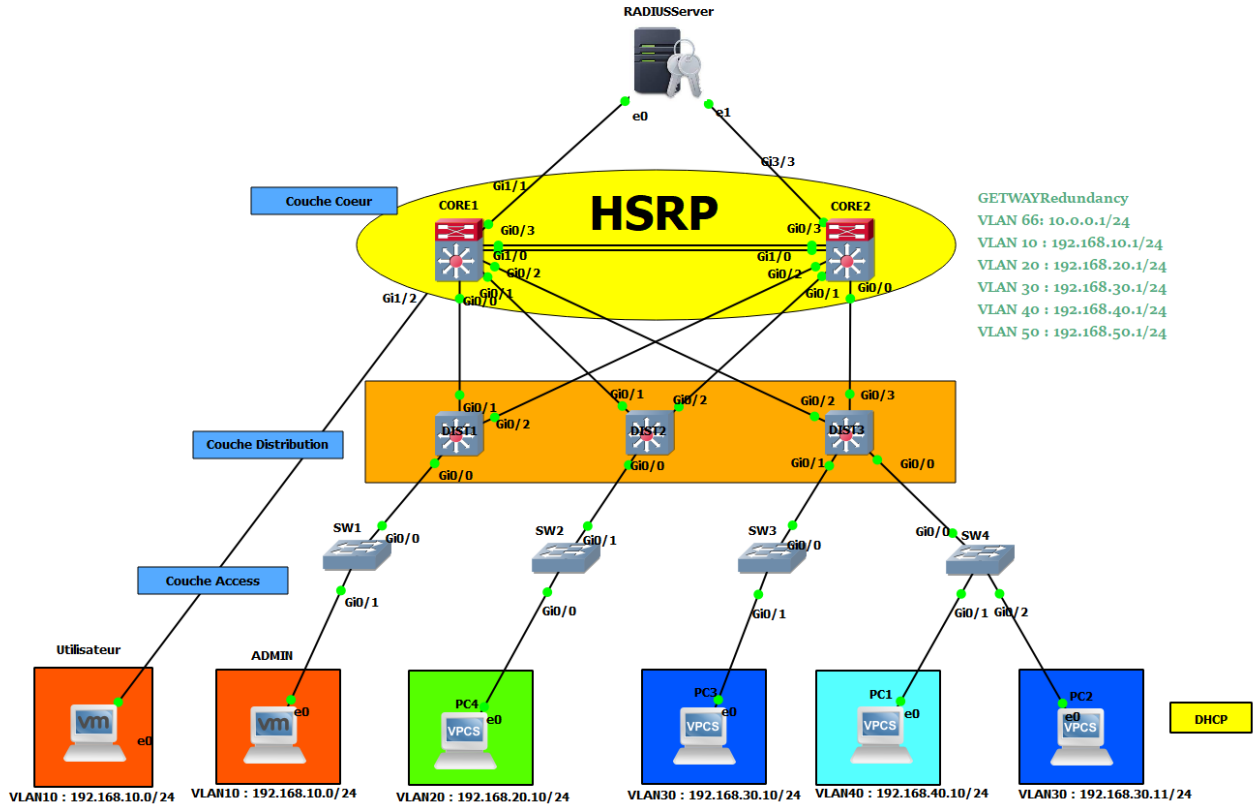

FIG. 3.2 : L'architecture proposée.

3.5 L'étude de l'infrastructure réseau

3.5.1 Modèle de conception Hiérarchique

- **Couche Cœur** : Centralise et optimise la conception, et donne une connectivité pour la couche distribution. Très utile dans des environnements LAN de grande taille.
- **Couche Distribution** : Regroupent la couche accès et fournit en plus une connectivité réglementée aux services. Elle prend en charge de nombreux services très

importants, et c'est dans cette couche que travaille le routage IP.

- **Couche Accès** : Fournit des points d'extrémité. C'est ici que les utilisateurs ont un accès direct au réseau et contient des fonctionnalités et services qui garantissent la sécurité et le bon fonctionnement du réseau.

3.5.2 Virtual 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 crever 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 :

- **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.

- **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 avis de la localisation géographique.

- **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.

Routage Inter-VLAN Layer 3 parts

Le routage inter-VLAN s'effectue par la connexion de différentes interfaces de routeur physique, il repose sur des routeurs dotés de plusieurs interfaces physiques, chaque interface devait être connectée pour un sous-réseau différent.
Le but du routage inter-VLAN c'est de réaliser la communication entre tous les VLANs qui existent dans notre réseau à travers un routeur pour communiquer les différents réseaux.
La méthode « router-on-a-stick » est un type de configuration de routeur dans laquelle une seule interface physique achemine le trafic entre plusieurs VLANs d'un réseau.
Les commutateurs multicouches peuvent effectuer des fonctions de couche 2 et 3 ce qui évite aux routeurs dédiés d'effectuer du routage de base sur un réseau, ces commutateurs prennent en charge le routage dynamique et le routage inter-VLAN, remplacent les routeurs et permettent de faire l'interconnexion desVLANs entre des différents réseaux.

3.5.3 Configuration Réseaux

- **Table des VLANs**

Switch / Vlans	CORE1 (Geteway)	CORE2 (Geteway)	GETEWAY Redundancy
Vlan 10	192.168.10.2/24	192.168.10.3/24	192.168.10.1/24
Vlan 20	192.168.20.2/24	192.168.20.3/24	192.168.20.1/24
Vlan 30	192.168.30.2/24	192.168.30.3/24	192.168.30.1/24
Vlan 40	192.168.40.2/24	192.168.40.3/24	192.168.40.1/24
Vlan 50	192.168.50.2/24	192.168.50.3/24	192.168.50.1/24
Vlan 66(Native)	10.0.0.2/24	10.0.0.3 /24	10.0.0.1/24

Tab. 3.2 : Table des Vlans.

- **Configuration de la couche cœur**

CORE1 et CORE2 vont être nos deux switches L3 qui feront partie du Standby Group. Etant donné que nous avons des liens redondants, SpanningTree va en bloquer certains. Pour que le lien vers la Geteway soit optimal, nous devons accorder le processus SpanningTreeavec le protocole HSRP.

_ **CORE 1** Sera le switch actif en HSRP, et il sera donc le Root Bridge en SpanningTree.

_ **CORE 2** Sera le switch secondaire en HSRP, il sera donc le Backup Root.

Voici maintenant la configuration de la Couche Cœur (CORE).

- **CORE1**

```
CORE1>enable
CORE1 #configuration terminal
CORE1 (config) #vlan 10
CORE1 (config-vlan) #vlan 20
CORE1 (config-vlan) #vlan 30
CORE1 (config-vlan) #vlan 40
```

```
CORE1 (config-vlan) #vlan 50
CORE1 (config-vlan) #vlan 66
CORE1 (config-vlan)#exit
CORE1 #interface range g0/0-3
CORE1 (conf-if) #switchport trunk encapsulation dot1q
CORE1(config-if) #switchport mode trunk
CORE1 (config-if) #switchport trunk allowed vlan all
CORE1 (config-if) #exit
CORE1 (config) #interface g1/0
CORE1 (config-if) #switchport trunk encapsulation dot1q
CORE1 (config-if) #switchport mode trunk
CORE1 (config-if) #switchport trunk allowed vlan all
CORE1 (config) #interface g1/1
CORE1 (config-if) #switchport mode access
CORE1 (config-if) #switchport access vlan66
CORE1 (config-if) #exit
CORE1 (config) #interface g1/2
CORE1 (config-if) #switchport mode access
CORE1 (config-if) #switchport access vlan50
CORE1 (config-if) #exit
CORE1 (config) #interface Vlan 10
CORE1 (config-if) #ip address 192.168.10.2 255.255.255.0
CORE1 (config-if) #standby 1 ip 192.168.10.1
CORE1 (config-if) #standby 1 priority 150
CORE1( config-if) #standby 1 preempt
CORE1 (config-if) #no shutdown
CORE1 (config-if) #exit
CORE1 (config) #interface Vlan 20
CORE1 (config-if) #ip address 192.168.20.2 255.255.255.0
CORE1 (config-if) #standby 2 ip 192.168.20.1
CORE1 (config-if) #standby 2 priority 150
```

```
CORE1 (config-if) #standby 2 preempt
CORE1 (config-if) #no shutdown
CORE1 (config-if) #exit
CORE1 (config) #interface Vlan 66
CORE1 (config-if) #ip address 10.0.0.2 255.255.255.0
CORE1 (config-if) #standby 66 ip 10.0.0.1
CORE1 (config-if) #standby 66 priority 150
CORE1 (config-if) #standby 66 preempt
CORE1 (config-if) #no shutdown
CORE1 (config-if) #exit
CORE1 (config) #interface Vlan 30
CORE1 (config-if) #ip address 192.168.30.2 255.255.255.0
CORE1 (config-if) #standby 3 ip 192.168.30.1
CORE1 (config-if) #standby 3 priority 100
CORE1 (config-if) #standby 3 preempt
CORE1 (config-if) #no shutdown
CORE1 (config-if) #exit
CORE1 (config) #interface Vlan 40
CORE1 (config-if) #ip address 192.168.40.2 255.255.255.0
CORE1 (config-if) #standby 4 ip 192.168.40.1
CORE1 (config-if) #standby 4 priority 100
CORE1 (config-if) #standby 4 preempt
CORE1 (config-if) #no shutdown
CORE1(config-if)#exit
(config)interface Vlan 50
CORE1(config-if)#ip address 192.168.50.2 255.255.255.0
CORE1 (config-if) #standby 5 ip 192.168.50.1
CORE1 (config-if) #standby 5 priority 100
CORE1 (config-if) #standby 5 preempt
CORE1 (config-if) #no shutdown
CORE1 (config-if) #exit
```

- **SPANNING-TREE**

```
CORE1 (config) #spanning-tree vlan 10,20,66 priority 24576
CORE1 (config) #spanning-tree vlan 30,40,50 priority 28672
```

_ **Activé la fonction de routage des switches Cœur** :
La commande suivante permet de vérifier que notre commutateur CORE1 et CORE2 sont capable de remplir les taches de routages (voir la figure 3.3).

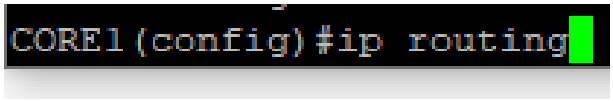

FIG. 3.3 : Commande pour activer la fonction de routage dans les switchs.

En utilisant la commande suivante pour afficher la configuration effectuée

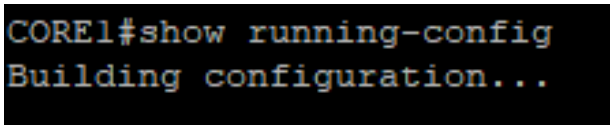

FIG. 3.4 : Commande pour afficher la configuration effectuée.

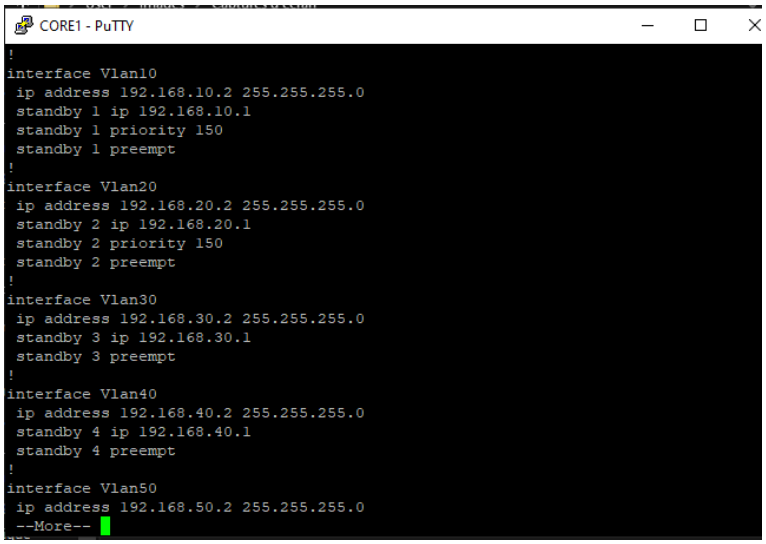

FIG. 3.5 : Afficher la configuration de la couche cœur.

- **CORE2**
  Prend la même configuration en changeant l'adresse Geteway HSRP et inversant la priorité c'est-à-dire :

  – Pour les VLANs 10 ,20,66 qui sont dans le CORE 2 avec une priorité de 100.

  Exemple :

```
CORE2 (config) #interface Vlan 10
CORE2 (config-if) #ip address 192.168.10. 3 255.255.255.0
CORE2 (config-if) #standby 1 ip 192.168.10. 1
CORE2 (config-if) #standby 1 priority 100
CORE2 (config-if) #standby 1 preempt
CORE2 (config-if) #no shutdown
CORE2 (config-if) #exit
```

  – Pour les VLANs 30,40, 50 qui sont dans le CORE 2 avec une priorité de 150 :

```
CORE2 (config) #interface Vlan 50
CORE2 (config-if) #ip address 192.168.50. 3 255.255.255.0
CORE2 (config-if) #standby 5 ip 192.168.50. 1
CORE2 (config-if) #standby 5 priority 150
CORE2 (config-if) #standby 5 preempt
CORE2 (config-if) #no shutdown
CORE2 (config-if) #exit
```

- **SPANNING-TREE**

```
CORE2 (config) #spanning-tree vlan 10,20,66 priority 28672
CORE2 (config) #spanning-tree vlan 30,40,50priority 24576
```

Configuration de la couche Distribution

Pour la couche distribution les 3 switches de niveau 3 [DIST1, DIST2, DIST3] ont la même configuration.

```
DIST1>enable
DIST1 #configuration terminal
DIST1 (config) #vlan 10
DIST1 (config-vlan) #vlan 20
DIST1 (config-vlan) #vlan 30
DIST1 (config-vlan) #vlan 40
DIST1 (config-vlan) #vlan 50
DIST1 (config-vlan) #vlan 66
DIST1 (config-vlan) #exit
DIST1 (config) #interface range g0/0-3
DIST1 (config-if) #switchport trunk encapsulation dot1q
DIST1 (config-if) #switchport mode trunk
DIST1 (config-if) #switchport trunk allowed vlan all
DIST1 (config-if) #exit
```

Configuration de la couche Access

Pour la couche Access les 4 Multi Layer switches ont la même configuration on procèdecomme suit :

- Pour les liens directs avec un utilisateur on utilise le mode Access
- Pour les liens qui sont reliée avec la couche distribution on utilise le mode trunk, pour l'activation de ce dernier il suffit de taper la commande suivante :

```
SW1 (config-if) #switchport trunk encapsulation dot1q
```

- **ACCESS**

```
SW1>enable
SW1 #configuration terminal
```

```
SW1 (config) #vlan 10
SW1 (config-vlan) #vlan 20
SW1 (config-vlan) #vlan 30
SW1 (config-vlan) #vlan 40
SW1 (config-vlan) #vlan 50
SW1 (config-vlan) #vlan 66
SW1 (config-vlan) #exit
SW1 (config) #interface g0/0
SW1 (config-if) # switchport trunk encapsulation dot1q
SW1 (config-if) # switchport mode trunk
SW1 (config-if)# switchport trunk allowed vlan all
SW1 (config-if)# exit
SW1(config) #interface g0/1
SW1 (config-if) #switchport mode access
SW1 (config-if)# switchport access vlan 10
SW1 (config-if)# exit
```

3.6 Sécurité de l'infrastructure

3.6.1 Windows Server 2016

Définition du Microsoft Windows Server 2016

Il est le système d'exploitation serveur (OS) de Microsoft. Il a été spécifiquement développé pour servir de plate-forme pour l'exécution d'applications en réseau. Il a été mis en disponibilité générale le 12 octobre 2016 et a été développé en même temps que Windows 10. Sa prise en charge standard a pris fin le 11 janvier 2022. Il fait partie de la famille de systèmes d'exploitation Windows NT.

Le système d'exploitation Microsoft Windows Server est une série de systèmes d'exploitation de serveur d'entreprise conçus pour partager des services avec plusieurs utilisateurs, offrant un contrôle administratif étendu du stockage des données, des applications et des réseaux d'entreprise. Il inclut de nouvelles fonctionnalités telles que la gestion des identités et des capacités de sécurité améliorées conçues pour aider les organisations à accéder aux données en toute sécurité si elles sont stockées localement, dans le cloud ou dans un cloud hybride [19].

Les annuaires

Un annuaire est une bibliothèque mise à jour régulièrement qui regroupe désinformations (nom, adresse, coordonnées) sur les membres d'une association, d'une entreprise ou d'un organisme professionnel [20].

Active Directory

Est un annuaire système hiérarchique. Il permet de localiser, rechercher et gérer des ressources représentées par des objets de l'annuaire. Il offre des mécanismes de sécurité pour protéger ses informations. Il permet de gérer des ressources liées à la gestion du réseau (domaines, comptes utilisateurs, stratégies de sécurité etc.. . .). La base de données d'AD est distribuée, ce qui lui permet d'améliorer la tolérance aux pannes. Certains produits Microsoft sont installés par défaut (ou fortement conseillés lors de l'installation) comme : DNS serveur web. Active Directory centralise l'authentification. Le contrôle d'accès eut être définie à la fois sur chaque objet de l'annuaire [21].

Le domaine Windows

Un domaine est l'ensemble d'objets, ordinateurs, utilisateurs et groupes définis par un administrateur réseau. Ces objets partagent une base de données d'annuaire et des stratégies de sécurité.

Serveur NPS

Network Policy Server (NPS) permet de créer et d'appliquer des stratégies d'accès au réseau à l'échelle de l'organisation pour l'authentification et l'autorisation des demandes de connexion. Il permet aussi de configurer et de gérer de manière centralisée l'authentification, l'autorisation et la comptabilité de l'accès au réseau avec les fonctionnalités suivantes :

- **Serveur RADIUS** : Lorsque NPS est utilisé en tant que serveur RADIUS, on configure des serveurs d'accès réseau, tels que des points d'accès sans fil et des serveurs VPN, en tant que clients RADIUS dans NPS. On configure également les stratégies réseau que NPS utilise pour autoriser les demandes de connexion, et on peut configurer la comptabilité RADIUS afin que NPS enregistre les informations de comptabilité dans les fichiers journaux sur le disque dur local ou dans une base de données Microsoft SQL Server [22].

- **Proxy RADIUS**. Le serveur NPS utilisé en tant que proxy RADIUS, permet de configurer des stratégies de demande de connexion qui indiquent au NPS les demandes de connexion à transférer vers d'autres serveurs RADIUS et vers quels serveurs RADIUS on souhaite transférer les demandes de connexion. On peut également configurer NPS pour transférer les données comptables devant être enregistrées par un ou plusieurs ordinateurs dans un groupe de serveurs RADIUS distants [22].

- **Serveur de stratégies NAP** : Lorsque le serveur NPS est configuré en tant que serveur de stratégie NPA, NPS évalue les déclarations d'intégrité envoyées par les ordinateurs clients compatibles avec la protection d'accès réseau (NAP) qui tentent de se connecter au réseau en assurant l'authentification et l'autorisation des demandes de connexion.
  Il peut configurer des stratégies NAP et des paramètres dans le serveur NPS, y compris les programmes de validation d'intégrité système, la stratégie de contrôle d » intégrité et le groupe de serveurs de mise à jour qui permettent aux ordinateurs clients de mettre à jour leur configuration afin de se conformer à la stratégie réseau de l'organisation.

3.6.2 Les services

Service DHCP

Le protocole DHCP (Dynamic Host Configuration 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 configuration, 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 [23].

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.

3.6.3 Les certificats

Fichier informatique signé par une autorité de certification qui garantit par cette signature que son possesseur est bien la personne ou l'entité qu'il prétend être. Les certificats permettent de signer et de chiffrer des documents et des emails, de s'authentifier sur des systèmes distants, de valider l'identité des sites web.
Les certificats numériques reposent tous sur le principe du chiffrement asymétrique, mais se distinguent avant tout par le niveau d'exigence des vérifications opérées par l'Autorité de Certification avant de les délivrer (d'une simple adresse email à un rendez-vous en personne).

3.6.4 Le contrôle d'accès

Le contrôle d'accès consiste à définir les accès au réseau et les services disponibles après identification. Le terme AAA est souvent utilisé pour désigner les facettes suivantes de la sécurité :

- **Authentification (en anglais Authentication)** : il s'agit de la vérification de l'identité d'un utilisateur ;
- **Autorisation (en anglais Authorization)** : il s'agit des droits accordés à un utilisateur, tels que l'accès à une partie d'un réseau, à des fichiers, le droit d'écriture, etc.
- **Comptabilité (en anglais Accounting)** : il s'agit des informations récoltées pendant toute la durée de la session, après identification de l'utilisateur.

3.7 L'authentification Radius accès à distance

3.7.1 Définition

Le protocole RADIUS acronyme de RemoteAuthentication 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 authentifiés grâce à un secret partagé [24].

3.7.2 Fonctionnement

- Sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.).
- Sur 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 est chiffré.
- Le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS.
- Le serveur traite les demandes d'authentification en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateur de machine ou de domaine.

- Un serveur RADIUS dispose pour cela d'un certain nombre d'interfaces ou de méthodes.
- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance.
- Le NAS achemine la demande au serveur RADIUS.
- Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur.
- Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
  - **ACCEPT** : l'identification a réussi.
  - **REJECT** : l'identification a échoué.
  - **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » [25].

3.7.3 Protocoles utilisés

- **Le protocole PAP (Password Authentication Protocol)** : est, comme son nom l'indique, un protocole d'authentification par mot de passe. Le protocole PAP a été originalement utilisé dans le cadre du protocole PPP.
  Le principe du protocole PAP consiste à envoyer l'identifiant et le mot de passe en clair à travers le réseau. Si le mot de passe correspond, alors l'accès est autorisé. Ainsi, le protocole PAP n'est utilisé en pratique qu'à travers un réseau sécurisé [26].
- **Le protocole SPAP (Shiva Password Authentication Protocol)** : est un mécanisme de cryptage réversible utilisé par Shiva. Un ordinateur exécutant Windows XP Professionnel, lorsqu'il se connecte à un Shiva LAN Rover, utilise SPAP, tout comme un client Shiva qui se connecte à un serveur exécutant routage et accès à distance.
  Cette forme d'authentification est plus sécurisée que le texte en clair, mais moins sécurisée que le protocole CHAP (Challenge HandshakeAuthentication Protocol) ou le protocole MS-CHAP (Microsoft Challenge HandshakeAuthentication Protocol). Cette forme d'authentification a cependant ses inconvénients. Même s'il est sécurisé et crypté, il peut y avoir des problèmes de piratage par ce qu'on appelle des attaques par relecture.

3.8 L'authentification 802.1x

3.8.1 Définition

Norme IEEE 802.1X pour le contrôle d'accès réseau basé sur les ports et protège les LAN Ethernet des accès non autorisés des utilisateurs.
Il bloque tout le trafic entrant et sortant d'un demandeur (client) au niveau de l'interface

jusqu'à ce que les données d'identification du demandeur soient présentées et associées au serveur d'authentification (un serveur RADIUS). Lorsque le demandeur est authentifié, le commutateur arrête de bloquer l'accès et ouvre l'interface au demandeur [27].

3.8.2 Fonctionnement

L'authentification 802.1X fonctionne à l'aide d'une entité d'accès au port d'authentificateur (le commutateur) afin de bloquer le trafic entrant d'un demandeur (équipement final) au niveau du port jusqu'à ce que les données d'identification du demandeur soient présentées et qu'elles soient associées au serveur d'authentification (un serveur RADIUS). Une fois authentifié, le commutateur arrête de bloquer le trafic et ouvre le port au demandeur.

L'équipement final est authentifié en mode unique de suppliciant, en mode de suppliciant mono-sécurisé ou en mode plusieurs demandeurs :

- **Un seul demandeur** : authentifie uniquement le premier équipement final. Tous les autres équipements finaux qui se connectent ultérieurement au port sont autorisés à accéder intégralement sans aucune autre authentification. Ils se basent sur l'authentification du premier équipement final.
- **Demandeur sécurisé unique** : permet de connecter le port à un seul équipement final. Aucun autre équipement final n'est autorisé à se connecter avant que le premier équipement ne se connecte.
- **Plusieurs demandeurs** : permet à plusieurs équipements finaux de se connecter au port. Chaque équipement final est authentifié individuellement.
  L'accès au réseau peut être défini plus en détail à l'aide de VLAN et de filtres de pare-feu, qui agissent tous deux comme filtres pour séparer et faire correspondre des groupes d'équipements finaux aux zones du réseau local dont ils ont besoin. Par exemple, vous pouvez configurer des VLAN pour gérer différentes catégories de défaillances d'authentification en fonction des éléments suivants :
  - Que l'équipement final soit compatible 802.1X ou non.
  - Que l'authentification MAC RADIUS soit ou non configurée sur les interfaces de commutation auxquelles les hôtes sont connectés.
  - Si le serveur d'authentification RADIUS devient indisponible ou envoie un message de rejet d'accès RADIUS. Reportez-vous à La configuration de la reprise d'échec du serveur RADIUS (procédure CLI) [27].

3.8.3 Protocoles de transport utilisés

1. Protocole EAP/(ExtendedAuthentication Protocol)

Il sert pour le transport des données nécessaire à l'authentification. Ce protocole est extensible, car on peut définir de nouvelles méthodes d'authentifications, il est indépen-

dant de la méthode Utilisé [28].

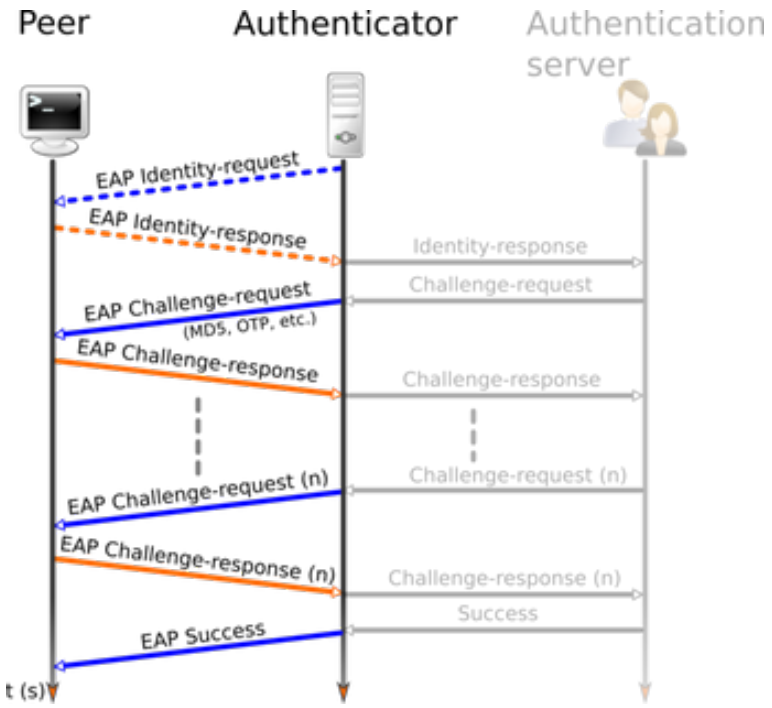

FIG. 3.6 : Le protocole EAP [29].

Méthodes associées à EAP

- **EAP-MD5 (EAP Message Digest 5-Challenge)** :
  Authentification avec un mot de passe.
- **EAP-TLS (EAP Transport Layer Security)** :
  Authentification par certificat du client et du serveur.
- **EAP-FAST (EAP-Flexible Authentication via Secure Tunneling)** :
  Authentification par certificat et mot de passe grâce à la génération d'un tunnel sécurisé .
- **LEAP (Lightweight EAP)** :
  Authentification avec mot de passe via une encapsulation sécurisée.
- **PEAP (Protected Extensible Authentication Protocol)** :
  Authentification avec mot de passe via une encapsulation sécurisée.

2. Protocole PPP

Le protocole PPP (Point-to-Point Protocol) est un protocole de communications de couche 2. PPP encapsule les données multiprotocoles sur des liaisons point à point. L'encapsulation PPP est le type d'encapsulation par défaut pour les interfaces physiques [30].

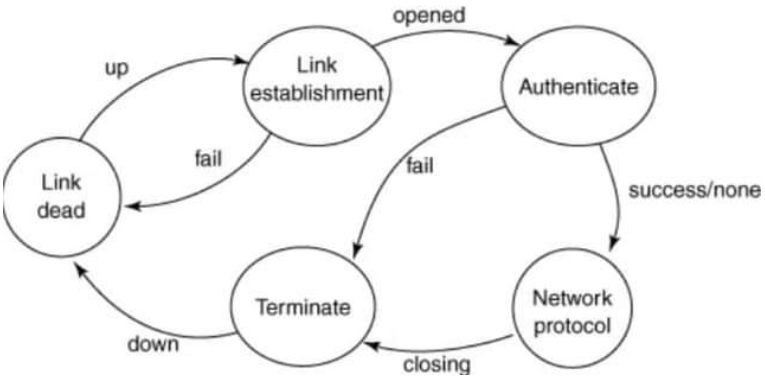

FIG. 3.7 : Le protocole PPP [31].

3. Protocole PAP

C'est un protocole d'authentification de mot de passe utilisé par les liens PPP pour valider les utilisateurs. L'authentification PAP nécessite que l'appareil appelant saisisse le nom d'utilisateur et le mot de passe. Si les informations d'identification correspondent à la base de données locale de l'appareil appelé ou à la base de données AAA distante, l'accès est autrement refusé [32].

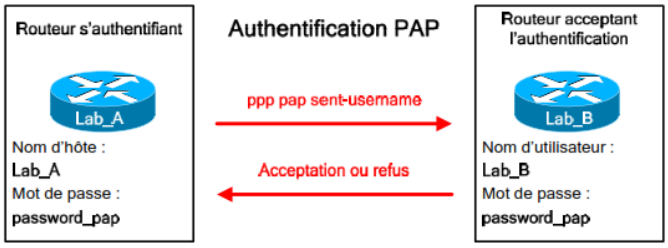

FIG. 3.8 : Le protocole PPP [33].

4. Protocole CHAP (Challenge Handshake Authentication Protocol)

C'est un protocole d'authentification basé sur la résolution d'un « défi » (en anglais « challenge »), c'est-à-dire une séquence à chiffrer avec une clé et la comparaison de la séquence chiffrée ainsi envoyée. Les étapes du défi sont les suivantes :

- un nombre aléatoire de 16 bits est envoyé au client par le serveur d'authentification, ainsi qu'un compteur incrémenté à chaque envoi. machine distante « hache » ce nombre, le compteur ainsi que sa clé secrète (le mot de passe) avec l'algorithme de hachage MD5 et le renvoie sur le réseau. serveur d'authentification compare le résultat transmis par la machine distante avec le calcul effectué localement avec la clé secrète associée à l'utilisateur.
- Si les deux résultats sont égaux, alors l'identification réussit, sinon elle échoue. Le protocole CHAP améliore le protocole PAP dans la mesure où le mot de passe n'est plus transmis en clair sur le réseau [34].

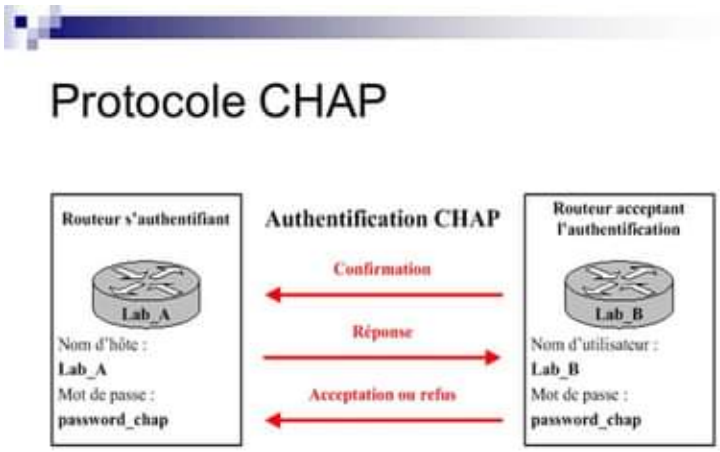

Fig. 3.9 : Le protocole CHAP [35].

5. Protocole MS-CHAP (Microsoft Challenge Handshake Authentication Protocol version 1)

Noté parfois MS-CHAP-v1, conçu pour l'amélioration globale de la sécurité. En effet, le protocole CHAP implique que l'ensemble des mots de passe des utilisateurs soient stockés en clair sur le serveur, ce qui constitue une vulnérabilité potentielle. Ainsi MS-CHAP propose une fonction de hachage propriétaire permettant de stocker un hash intermédiaire du mot de passe sur le serveur. Lorsque la machine distante répond au défi, elle doit ainsi préalablement hacher le mot de passe à l'aide de l'algorithme propriétaire.
Le protocole MS-CHAP-v1 souffre malheureusement de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaire [36].

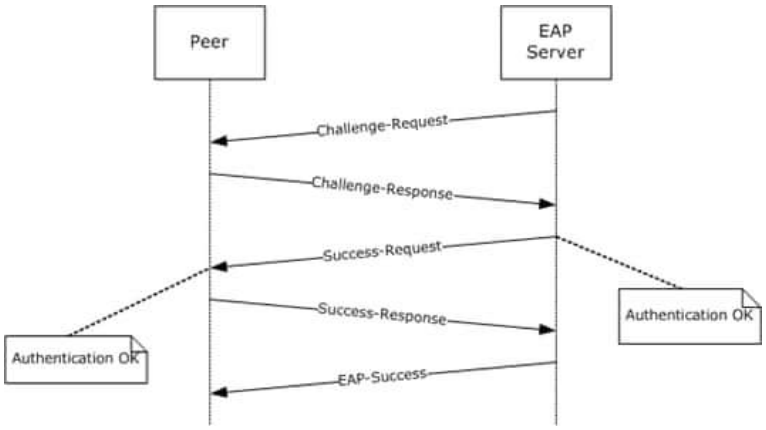

Fig. 3.10 : Le protocole MS-CHAP [37].

6. Protocole MS-CHAPv2

La version 2 du protocole MS-CHAP, baptisée MS-CHAP-V2, définit une méthode dite « d'authentification mutuelle », permettant au serveur d'authentification et à la machine

distante de vérifier leurs identités respectives. Le processus d'authentification mutuelle de MS-CHAP v2 fonctionne de la manière suivante :

- Le serveur d'authentification envoie à l'utilisateur distant une demande de vérification composée d'un identifiant de session ainsi que d'une chaîne aléatoire.
- Le client distant répond avec : son nom d'utilisateur, un haché contenant la chaîne arbitraire fournie par le serveur d'authentification, l'identifiant de session ainsi que son mot de passe, une chaîne aléatoire.
- Le serveur d'authentification vérifie la réponse de l'utilisateur distant et renvoie agave ; son tour les éléments suivants : la notification de succès ou d'échec de l'authentification, une réponse chiffrée sur la base de la chaîne aléatoire fournie par le client distant, la réponse chiffrée fournie et le mot de passe de l'utilisateur distant. Le client distant vérifie enfin à son tour la réponse et, en cas de réussite, établit la connexion [36].

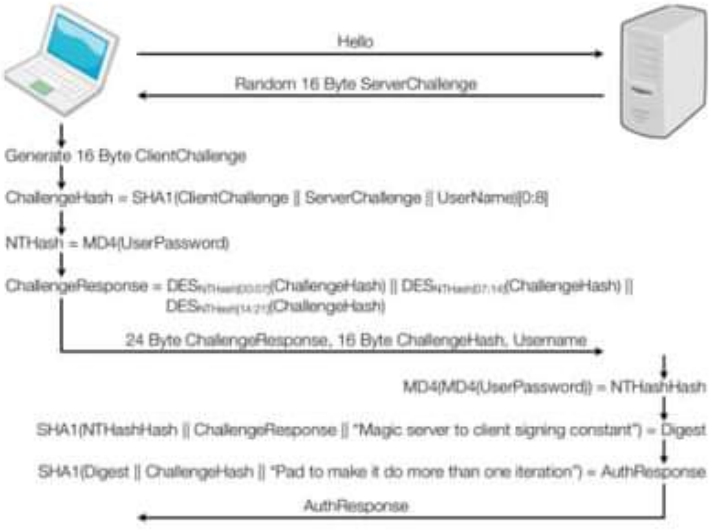

Fig. 3.11 : Le protocole MS-CHAPv2 [38].

3.9 Conclusion

Dans ce chapitre, nous avons présenté les aspects techniques liés au déploiement et à la réalisation de notre solution, en citant tous les outils matériels et logiciels qui ont contribués à répondre à cette solution.

Chapitre 4

Implémentation et configuration

4.1 Introduction

Ce chapitre est consacré à l'implémentation et la configuration des différents éléments de notre solution, ainsi que les différentes validations pour assurer que notre objectif a été bien atteint.

4.2 Ajout des rôles de fonctionnalité : (DNS, AD DS, NPAS)

La figure 4.1 montre les étapes d'installation de l'Active Directory, NPAS et DNS. Nous avons sélectionné les rôles Active Directory domaine service, DNS et NPAS en cochant les cases correspondantes puis on clique sur suivant, à ce stade, une fenêtre apparait, on clique sur installer pour commencer l'installation.

Une fois que l'installation est achevée, une autre fenêtre va apparaitre, on clique sur fermer pour terminer.

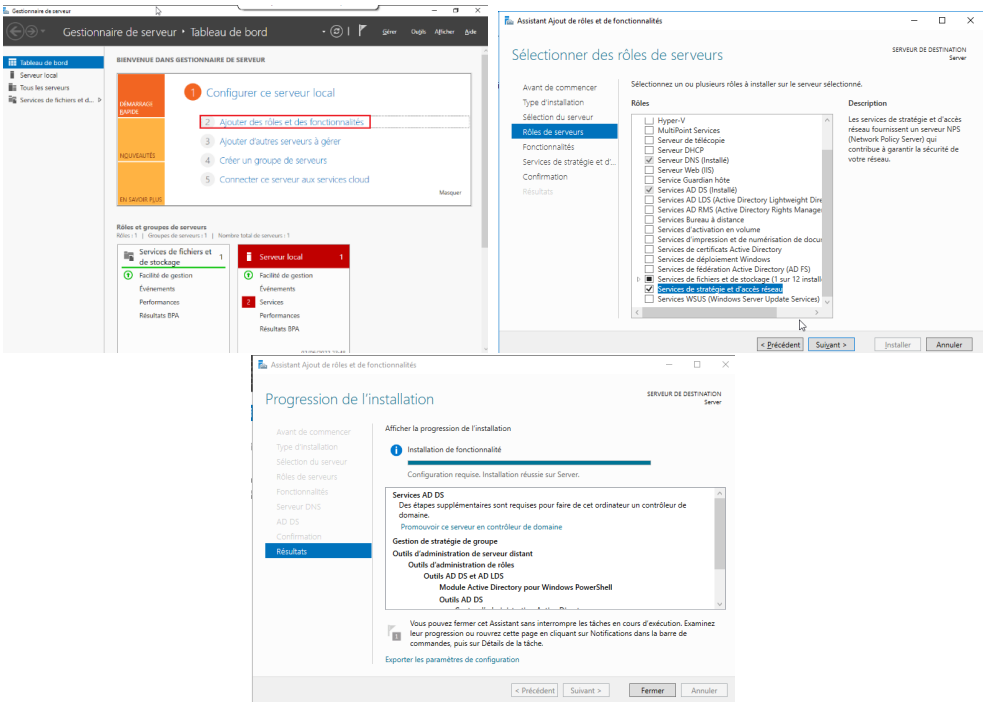

FIG. 4.1 : Ajout des rôles de fonctionnalité : (DNS, AD DS, NPAS).

4.3 Création d'un contrôleur de domaine

1. Une fois les fonctionnalités d'AD DS installées. Nous devons promouvoir ce serveur en tant que contrôleur de domaine, sinon le domaine ne sera pas créé (figure 4.2).

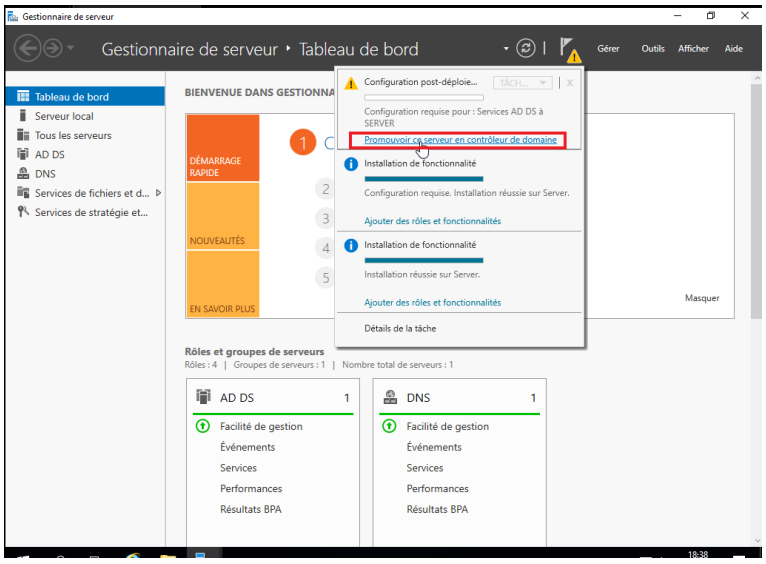

FIG. 4.2 : Promouvoir le serveur en contrôleur de domaine.

2. Vu que nous souhaitons créer un nouveau domaine, nous devons déployer une nouvelle forêt en cochant sur Ajouter une nouvelle forêt et en spécifiant le nom de domaine « sonatrach.local » (voir la figure 4.3).

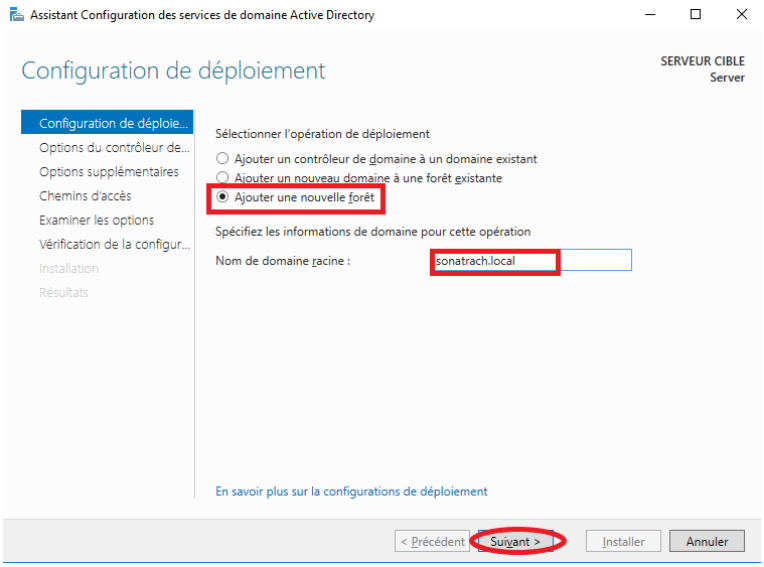

FIG. 4.3 : Création du domaine « sonatrach.local ».

3. L'étape suivante consiste à choisir le niveau fonctionnel de la forêt et du domaine ainsi pour éviter les restaurations non souhaitées d'Active Directory, il est demandé de saisir un mot de passe de restauration (Figure 4.4).

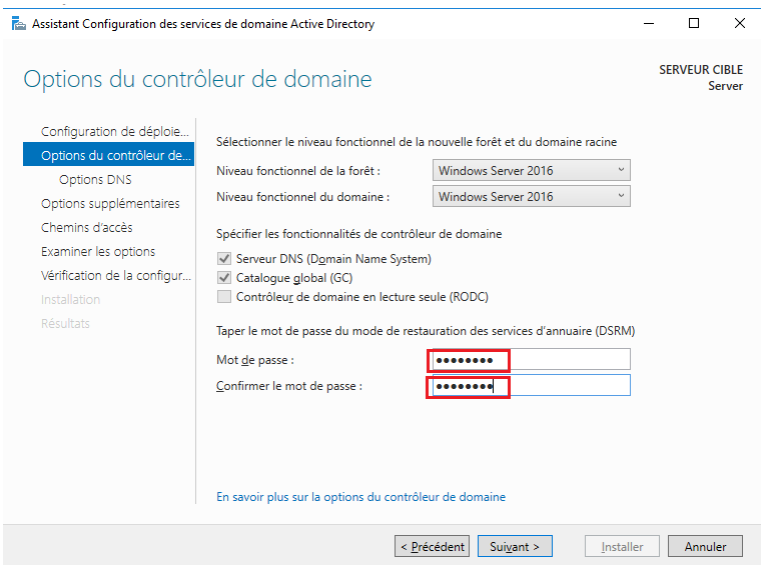

FIG. 4.4 : Niveau fonctionnel de la forêt et du domaine.

4. L'assistant suivant montre le nom NetBIOS de domaine : pour poursuivre l'installation on clique sur suivant (Figure 4.5).

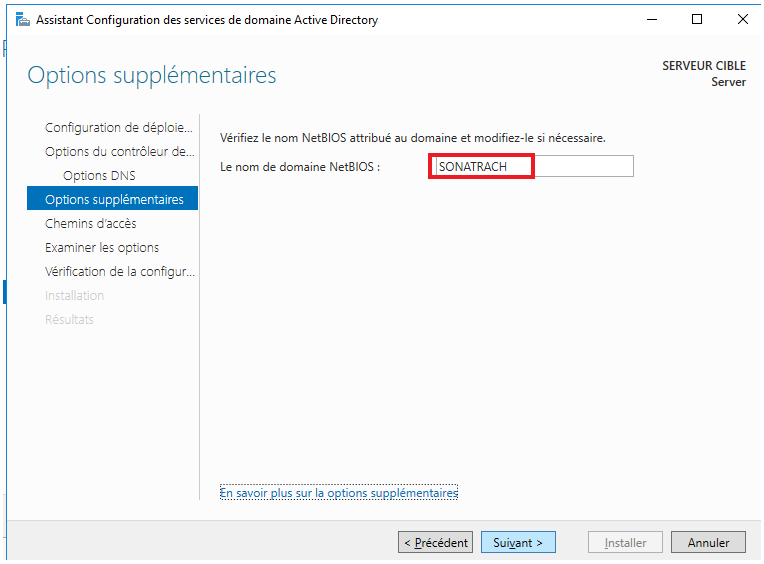

FIG. 4.5 : Nom NetBIOS de domaine.

5. Ensuite on spécifie les dossiers qui contiendront la base de données du contrôleur de domaine Active Directory, les fichiers journaux et SYSVOL (Figure 4.6).

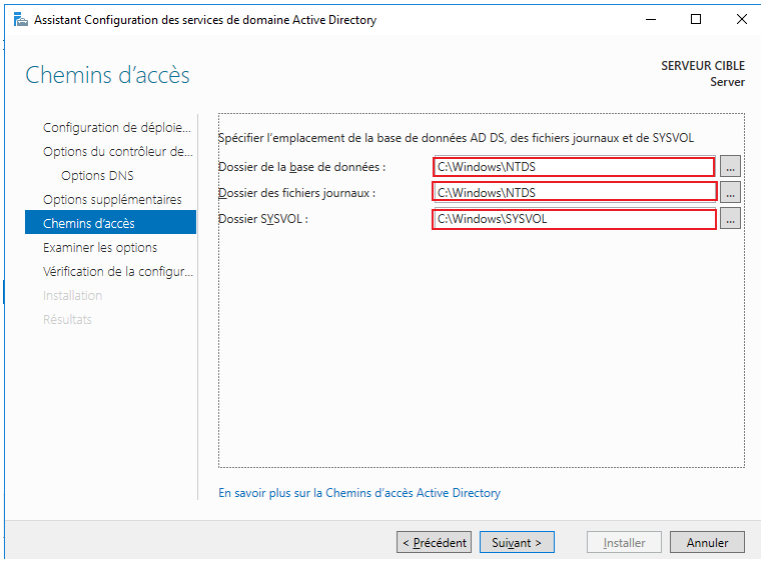

FIG. 4.6 : L'emplacement des fichiers Active Directory.

6. Lorsque nous installons les services de domaine Active Directory (AD DS), celui-ci nous donne la possibilité d'installer et de configurer automatiquement un serveur DNS.
   La zone DNS résultante est intégrée à AD DS contrôlé par le serveur SVRDC. Après configuration, le serveur redémarre automatiquement. A présent, les outils de gestion d'Active Directory sont présents dans le menu d'outils (voir la figure 4.7).

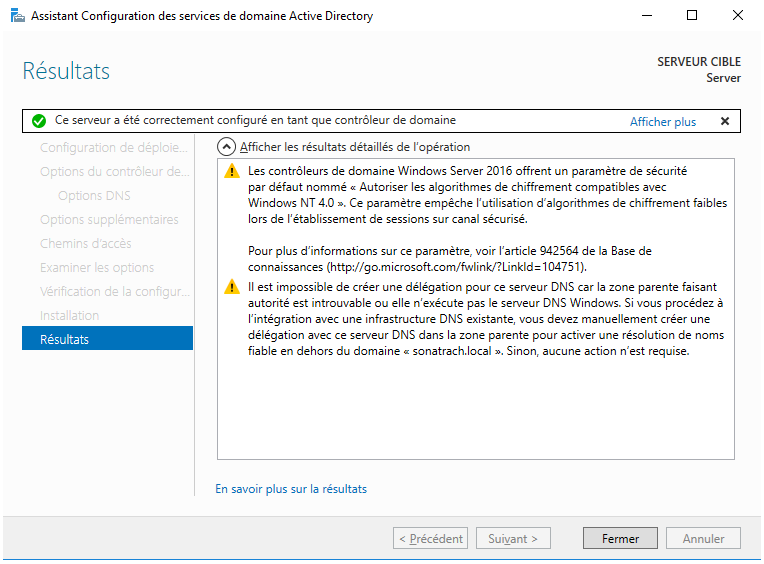

FIG. 4.7 : Création réussie du domaine et de la forêt.

4.4 Configuration de l'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 Bejaia) et dans Sonatrach Bejaia on a créé deux autres unités d'organisation (Groupe et Utilisateurs).

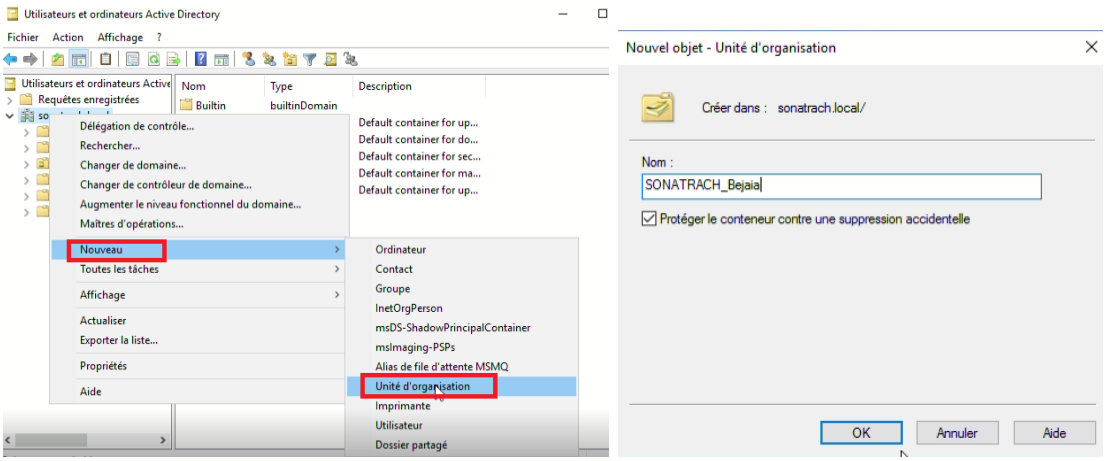

FIG. 4.8 : Création de l'unité d'organisation.

- **Création des groupes Employés :** après avoir créé l'unité d'organisation <Utilisateur> dans cette dernière nous allons créer des groupes et des utilisateurs Pour créer des groupes, un clic droit sur notre domaine « sonatrach.local », « nouveau » puis « groupe » (Figure 4.9).

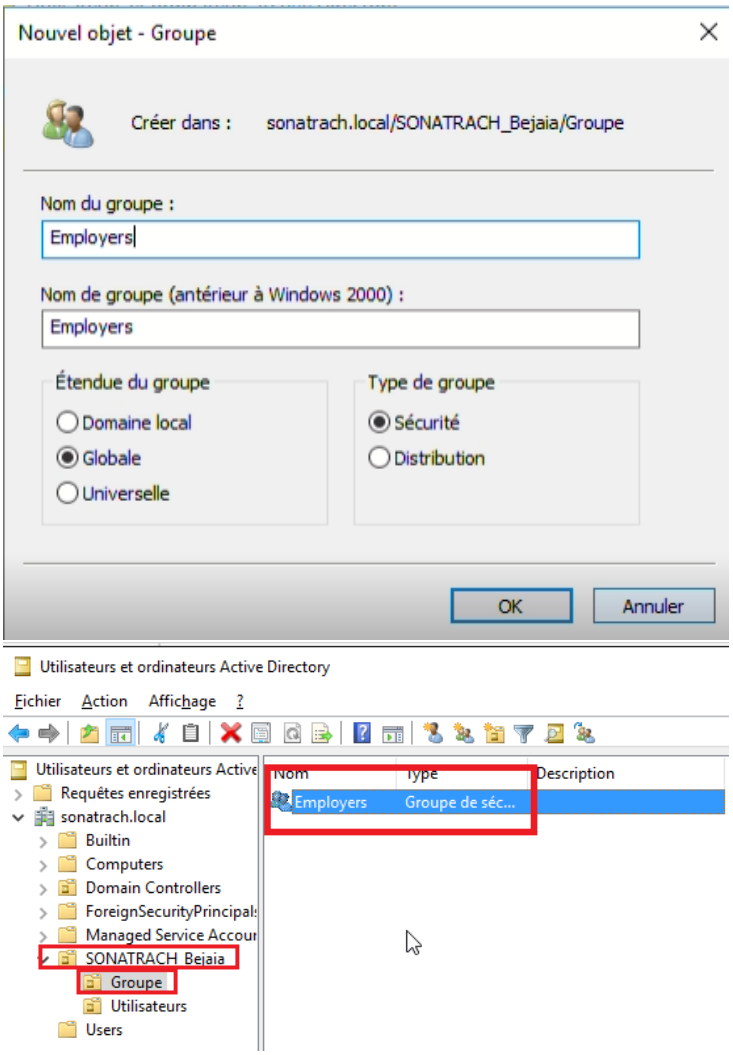

Fig. 4.9 : Création d'un groupe Employés.

- **Création d'utilisateur dans Active Directory :** pour créer un utilisateur dans Active Directory il suffit d'un clic droit sur l'unité d'organisation Utilisateur, nouveau, utilisateur.
  Après avoir cliqué sur "Suivant", on doit introduire le mot de passe, et cocher les deux cases l'utilisateur ne peut pas changer le mot de passe " et "le mot de passe n'expire jamais" (Figure 4.10).

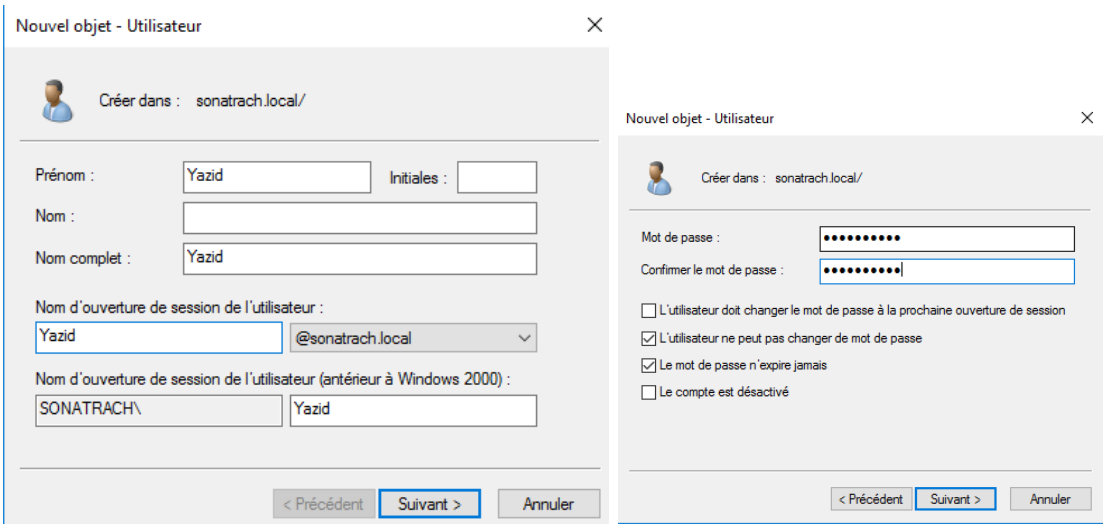

FIG. 4.10 : Création d'un utilisateur et introduction de son mot de passe.

- Ajouter les utilisateurs créés au groupe, la figure suivante montre que les utilisateurs sont bien membres de notre groupe Employés (Figure 4.11).

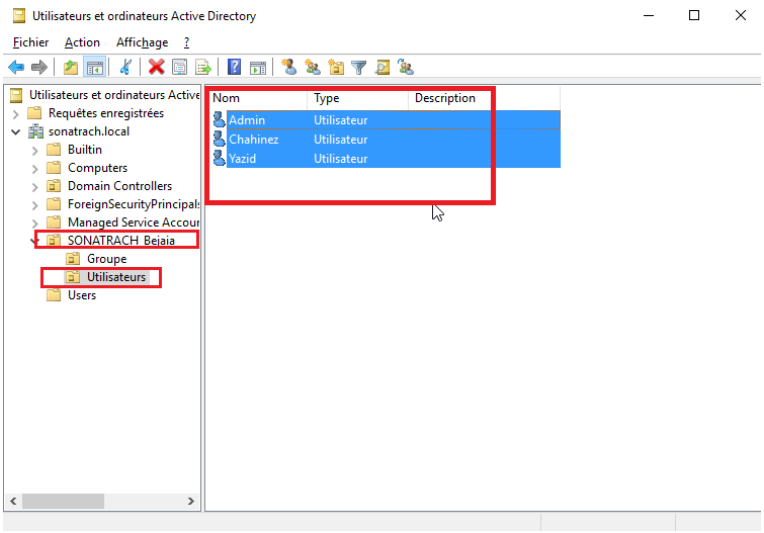

FIG. 4.11 : Membre du groupe Employés.

- **Inscrire le serveur NPS dans l'AD :** Pour que le serveur NPS ait l'accès aux informations d'identification et des utilisateurs finaux dans Active Directory, Le serveur NPS doit être inscrit dans (AD).

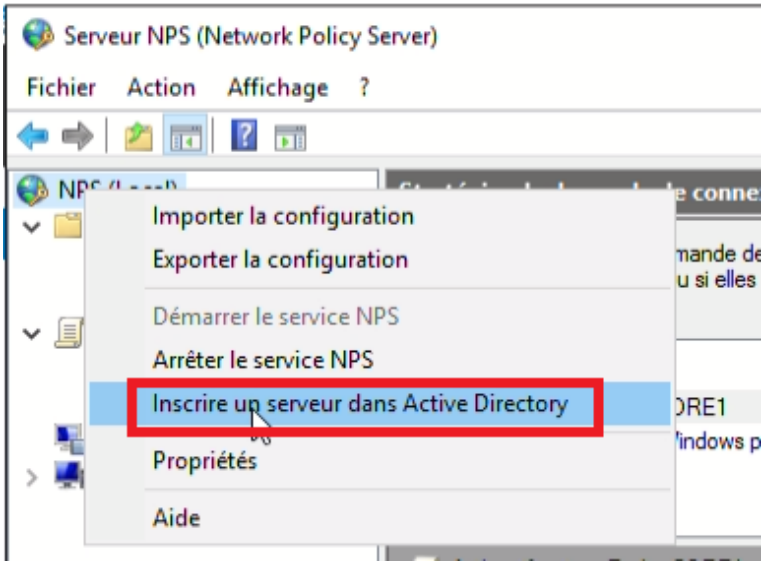

FIG. 4.12 : Inscrire le serveur NPS dans l'AD.

4.5 Authentification accès à distance

Afin de sécuriser l'accès à distance à nos commutateurs de la couche cœur via l'utilisateur (avec son identifiant, membres de groupe employés et son mot de passe), on a employé l'authentification radius accès à distance.

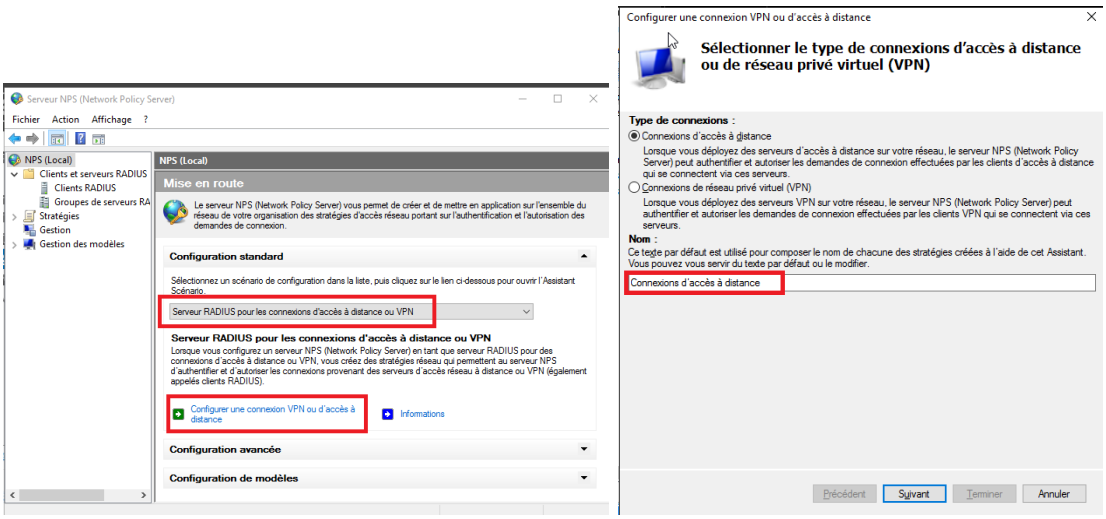

FIG. 4.13 : Configuration accès à distance.

4.5.1 Création d'un client RADIUS

Les clients Radius tel que (switch, routeur, point d'accès) sont des appareils qui seront autorisés à demander l'authentification à partir du serveur Radius. Pour la configuration du client Radius, il faut suivre les étapes suivantes :

1. NPS => Radius Clients and Servers => Radius Clients => Nouveau => cocher

pour Activer ce client Radius et remplir ces paramètres (figure 4.14) :

- **Nom convivial :** Nom pour identifier le client.
- **Adresse (IP ou DNS) :** Saisir l'adresse IP du commutateur ou DNS.
- **Secret partagé :** Indiquer un code qui sera partagé par le client et le serveur Radius puis cliquer sur **OK** (Figure 4.14).

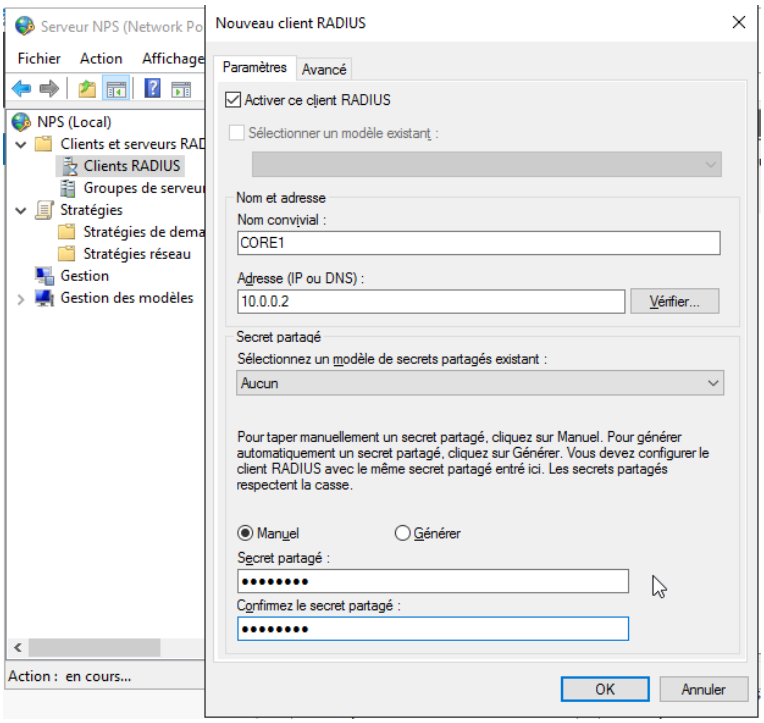

FIG. 4.14 : Création d'un client RADIUS.

4.5.2 Création d'une stratégie de demande de connexion

Pour créer une stratégie de demande de connexion on suit les étapes suivantes :

- On fait un clic droit sur "stratégie de demande de connexion".
- On ajoute le nom convivial.
- On ajoute le client radius créé pour le nom convivial.
- On clique sur suivant jusqu'à terminer.

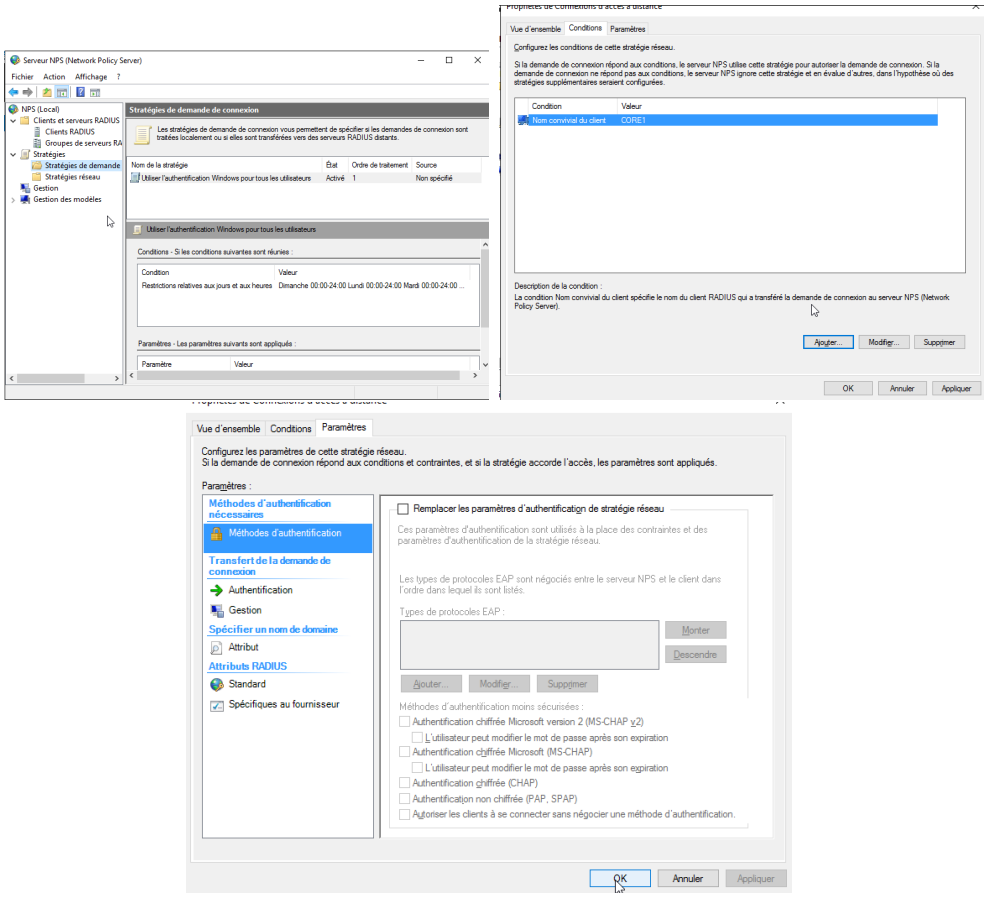

FIG. 4.15 : Création de la stratégie de demande de connexion.

4.5.3 Création d'une stratégie réseaux

Pour créer une stratégie réseaux, on suit les étapes suivantes :

- On fait un clic droit sur "stratégie réseaux".
- On crée un groupe Windows.
- On ajoute le groupe "Employés" qu'on a créés (et qui contient les utilisateurs radius) dans le groupe Windows crée.
- On clique sur suivant.
- On sélectionne les protocoles PAP et SPAP.
- On sélectionne le type d'attribut en le mettant à "autre" puis on choisit "login".
- On clique sur OK pour terminer.

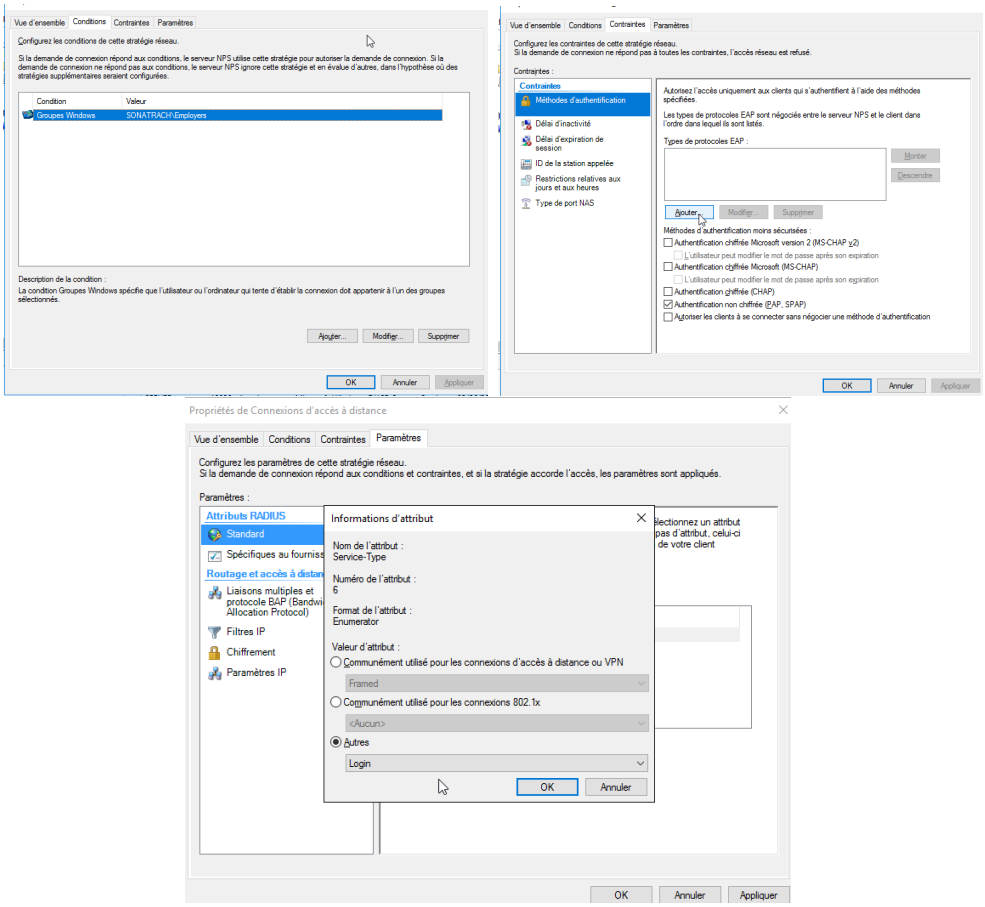

FIG. 4.16 : Création d'une stratégie réseaux.

4.6 Installation et configuration du service DHCP

Pour que les PCs et les serveurs communiquent nous devons leur donner une adresse IP, un masque de sous réseau, une passerelle et un serveur DNS qui est obligatoirement un DNS d'Active Directory.

1. Dans l'assistant de gestion des rôles, au niveau des rôles de serveurs, choisir (Serveur DHCP) en cochant la case (serveur DHCP).et faire suivant jusqu'à installer cliquer dessous (figure 4.17).

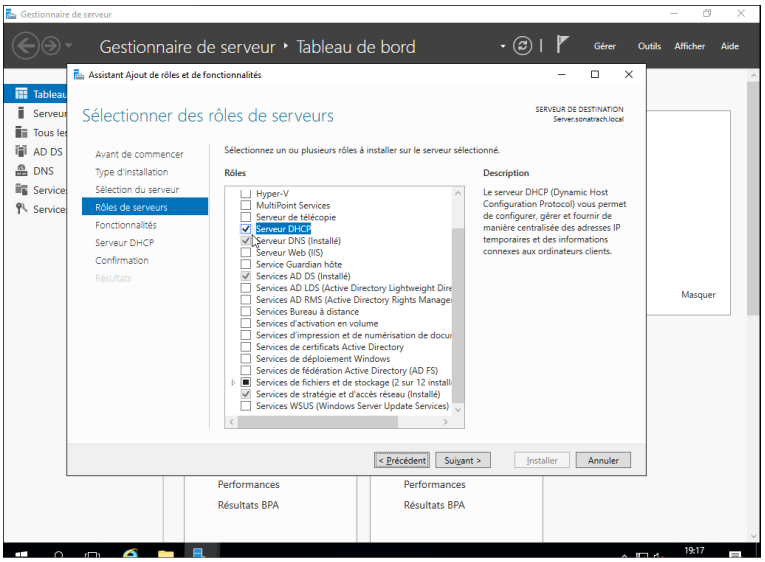

Fig. 4.17 : Ajout du serveur DHCP.

2. Après quelques minutes le rôle est installé, nous procédons à la configuration du DHCP en IP pour le client (figure 4.18).

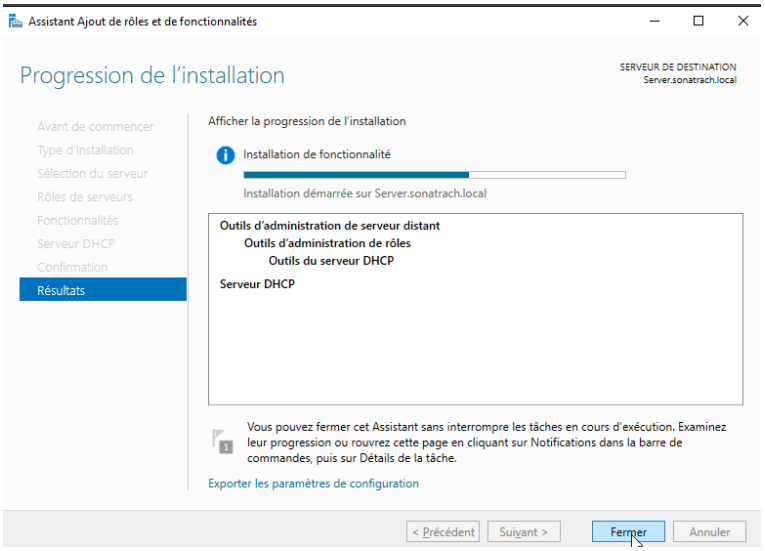

Fig. 4.18 : Installation du serveur DHCP.

3. Dans cette étape, nous avons créé des étendues pour chaque VLAN avec un simple clic droit, puis on a choisi Nouvelle étendue (Figure 4.19).

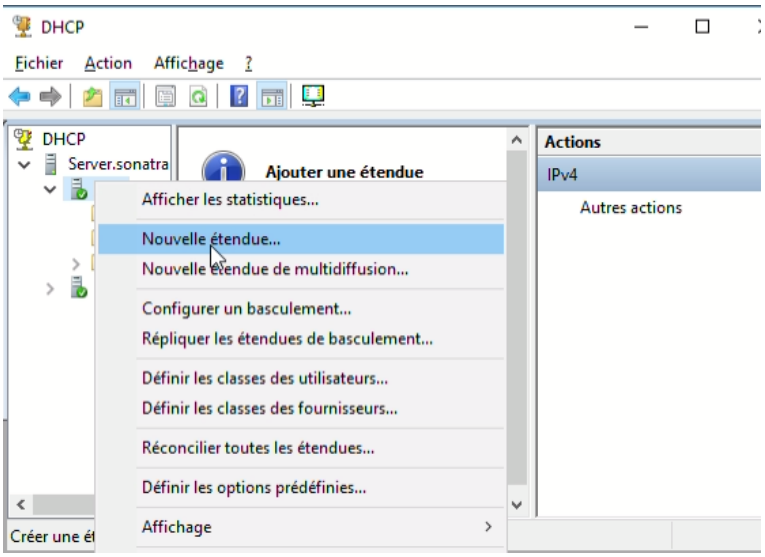

FIG. 4.19 : Création des étendus pour chaque VLAN.

4. Création de nos étendues DHCP à l'aide de la console d'administration DHCP qui a été lancée depuis le menu outils du gestionnaire de serveur (Figure 4.20).

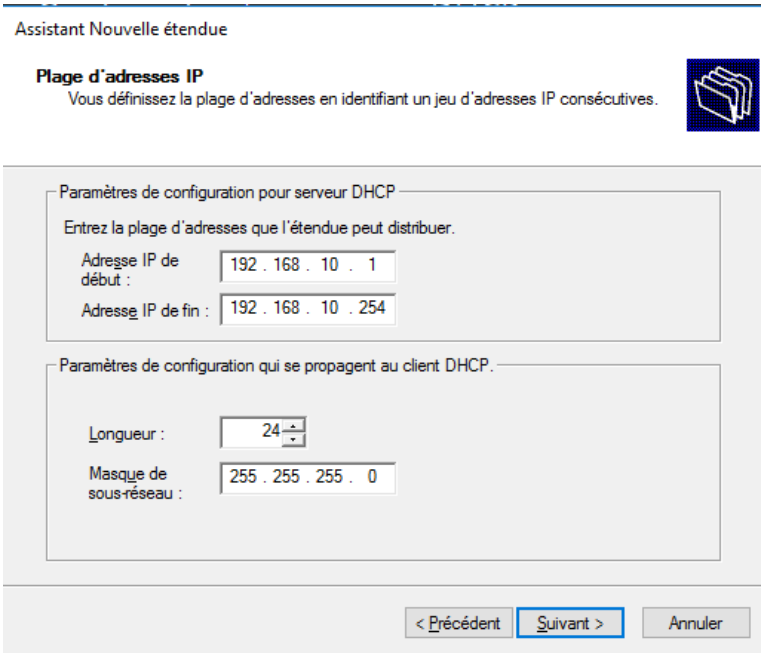

FIG. 4.20 : Plage d'adresse allouée aux machines clientes.

5. Ajouter les exclusions des adresses ou des plages qui ne sont pas distribuées par le serveur afin de ne pas provoquer de conflit avec un périphérique qui serait configuré sur ces adresses (figure 4.21).

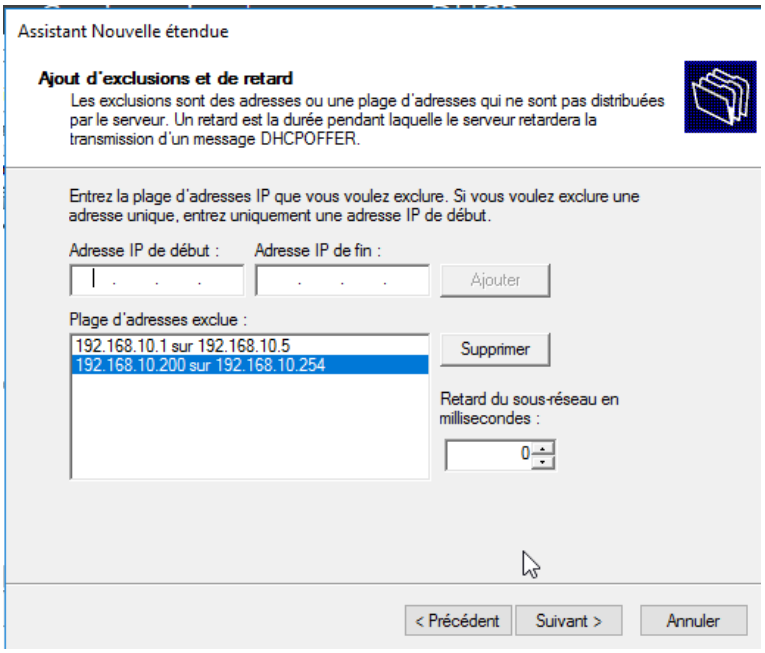

Fig. 4.21 : Ajout d'exclusion DHCP.

6. Si on utilise un serveur DNS, saisissons le nom du serveur. Cliquons sur Ajouter pour inclure ce serveur dans la liste des serveurs DNS affectés aux clients DHCP puis cliquons sur suivant et terminer (Figure 4.22).

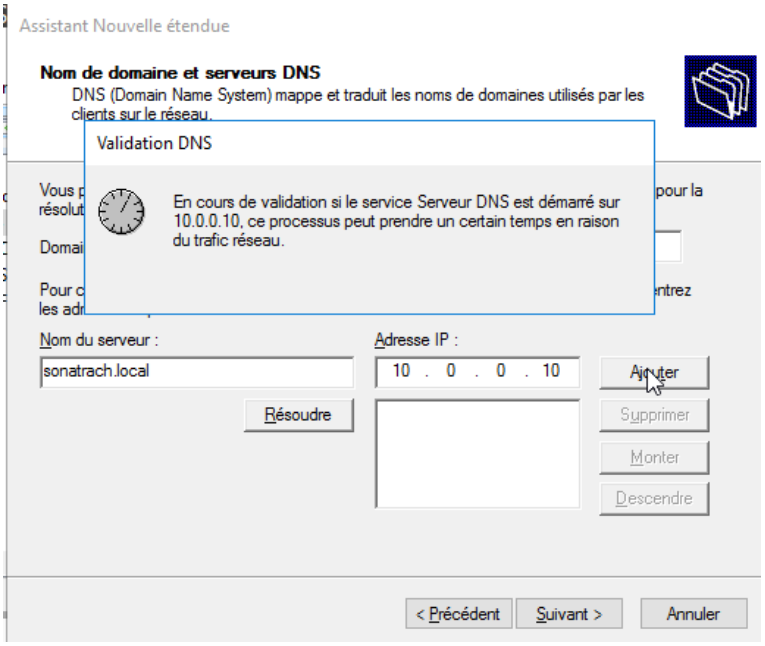

Fig. 4.22 : Ajout du nom de domaine serveur DNS.

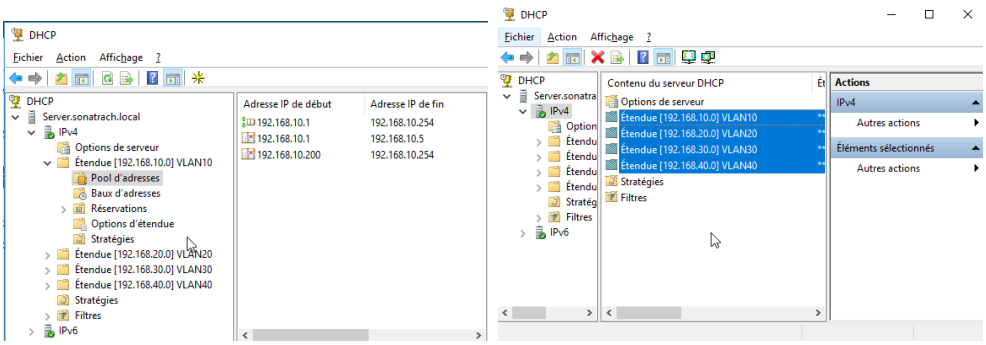

FIG. 4.23 : Ensemble des plages d'adresses.

4.7 Mise en œuvre de l'autorité de certification Active Directory

1. Directory Certificat Services (AD CS) Dans cette partie, nous allons créer une autorité de certification racine d'entreprise. Dans l'assistant de gestion des rôles, Au niveau des rôles de serveurs, choisir (services de certificats Active directory) (figure 4.24).

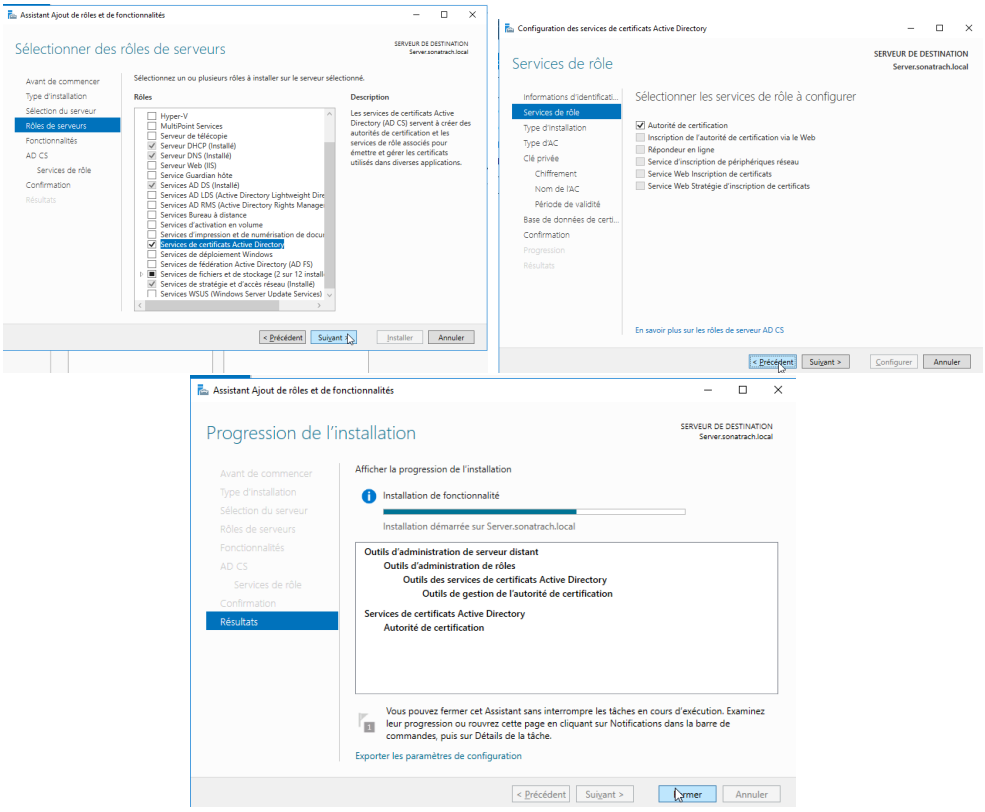

FIG. 4.24 : Ajout des services de certificats Active Directory.

2. Pour la configuration de service de certificats Active Directory, nous procèderons comme suit (Figure 4.25) :

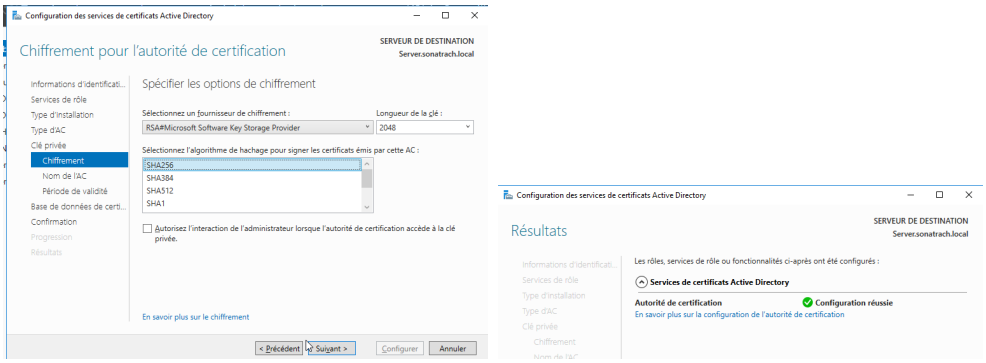

FIG. 4.25 : Configuration de service de certificats Active directory.

4.8 Authentification 802.1x

Création d'une nouvelle stratégie réseau pour switch

1. Nous allons créer une nouvelle politique 802.1x pour authentifier les utilisateurs lors de la connexion à notre commutateur. Pour cela on doit sélectionner le serveur Radius pour les connexions câblées ou sans fil 802.1x puis cliquer sur configurer 802.1x (figure 4.26).

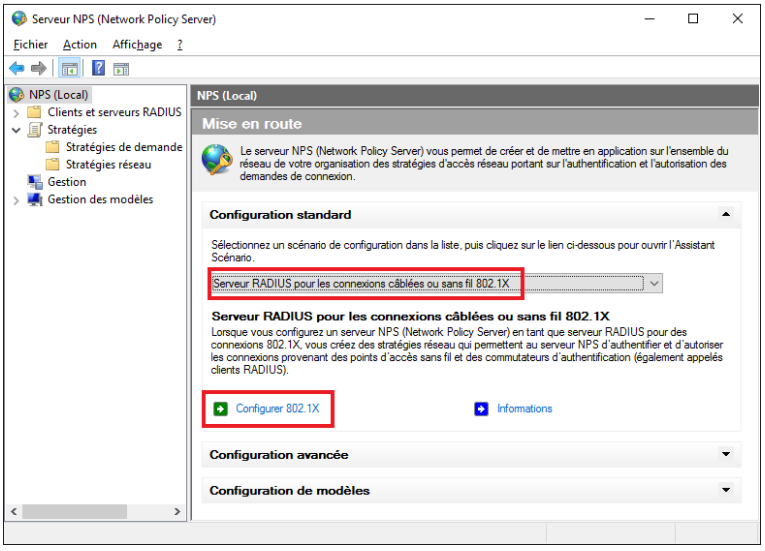

FIG. 4.26 : Sélection d'un scénario de configuration.

2. On sélectionne le type de connexion 802.1x. Cocher la case « connexions câblées (Ethernet) sécurisées => et nommer la politique qu'on a créé ensuite on clique sur suivant (figure 4.27).

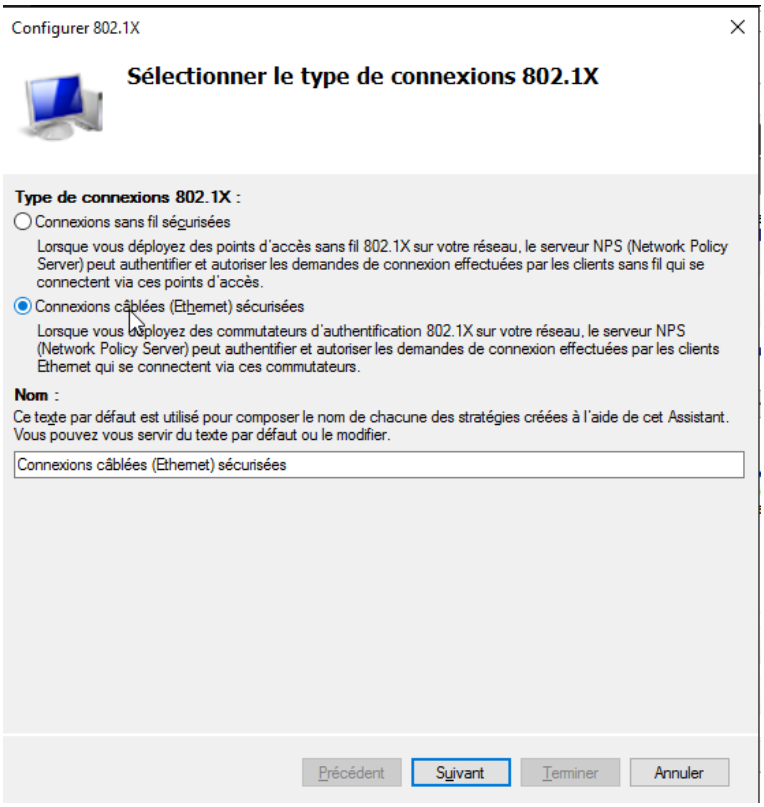

Fig. 4.27 : Type de connexion 802.1X.

3. On ajoute notre client Radius ”Core1” ou ”Core2”, l'authentificateur est le commutateur. Lorsque l'utilisateur est connecté à un port sur le commutateur, le commutateur nécessite une authentification de l'utilisateur. Nous avons signalé le client Radius ”Core1” et ”Core2”ci-dessus (figure 4.28).

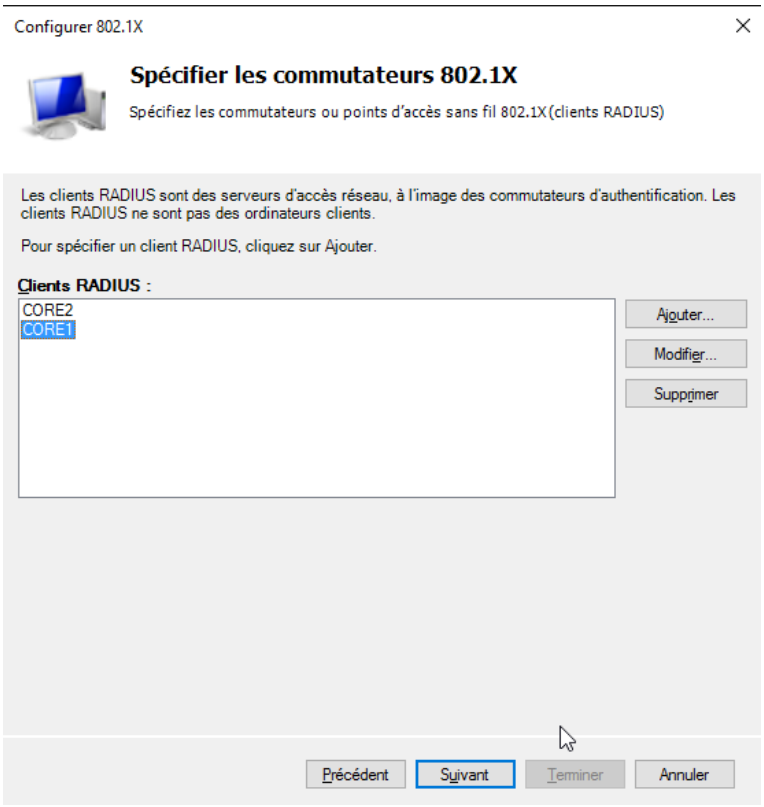

FIG. 4.28 : Ajout de client Radius.

4. Configurez en utilisant n'importe quelle méthode d'authentification. On va utiliser "Microsoft : Protected EAP (PEAP)" (figure 4.29).

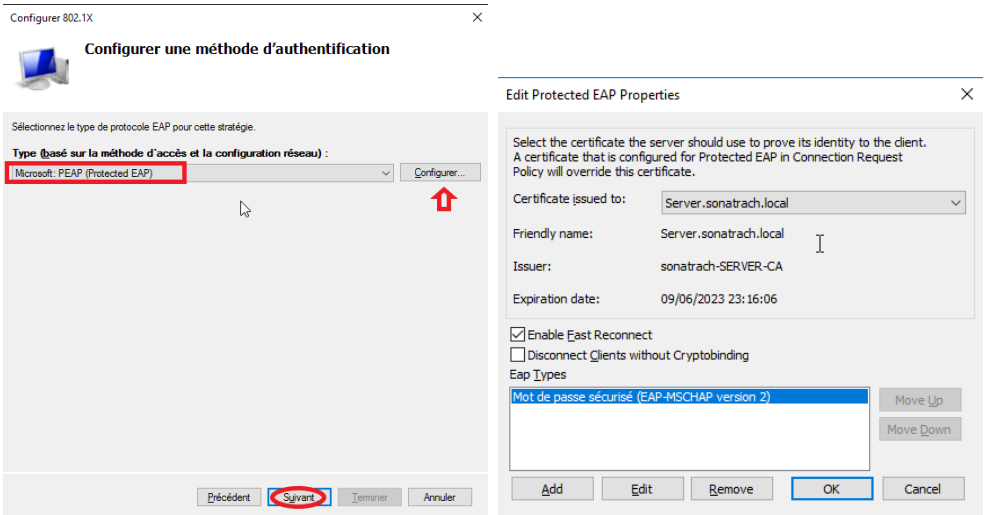

FIG. 4.29 : Type de protocole pour cette stratégie.

5. Pour configurer la nouvelle stratégie de demande de connexion on suit les étapes suivantes :

   - On fait un clic droit sur "stratégie de demande de connexion".
   - Puis on sélectionne l'onglet Conditions.

- On ajoute le client radius créé pour le nom d'utilisateur => On clique sur **OK** (Figure 4.30).

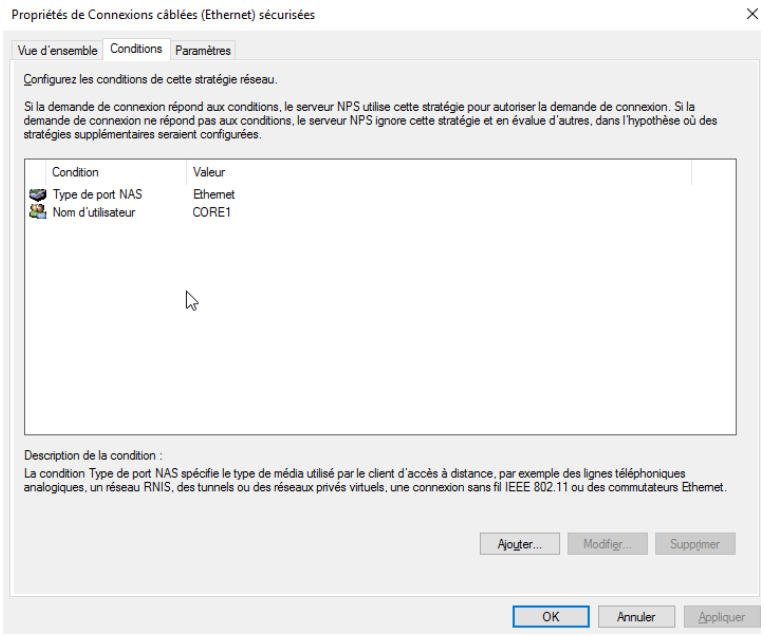

FIG. 4.30 : Configuration des conditions de la stratégie de demande de connexion.

6. Dans l'onglet "Paramètres" (Paramètres), on choisit les méthodes d'authentification dans notre cas en a ajouté type de protocole EAP : « Protected EAP » et on a coché les cases « authentification chiffrée Microsoft version 2 (MS-CHAP v2) » et « authentification chiffrée Microsoft (MS-CHAP) » (figure 4.31).

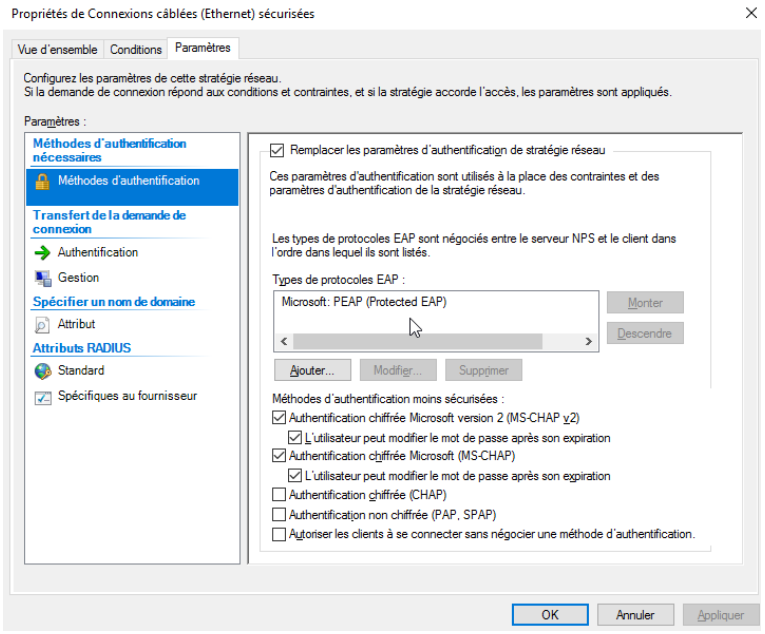

FIG. 4.31 : Choix des méthodes d'authentification pour la stratégie demande de connexion.

7. Après la création de la stratégie NPS 802.1x pour les connexions câblées, on configure les conditions pour la stratégie réseau. (Figure 4.32).

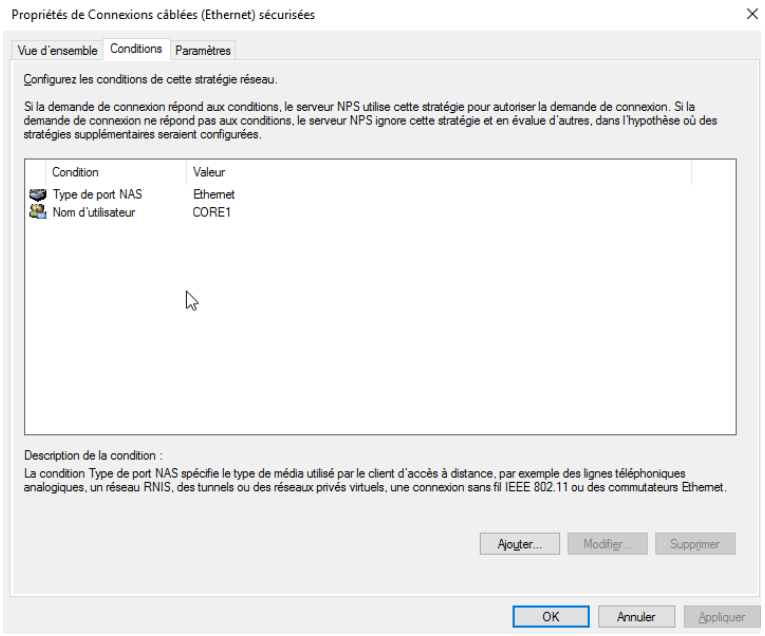

Fig. 4.32 : Configuration des conditions de cette stratégie réseau.

8. Dans le même onglet "Paramètres" => "Attributs Radius" => "Standard", on ajoute les attributs : Tunnel-Medium-Type, Tunnel-Pvt-Group-ID et l'attribut "tunnel-Type" (figure 4.33).

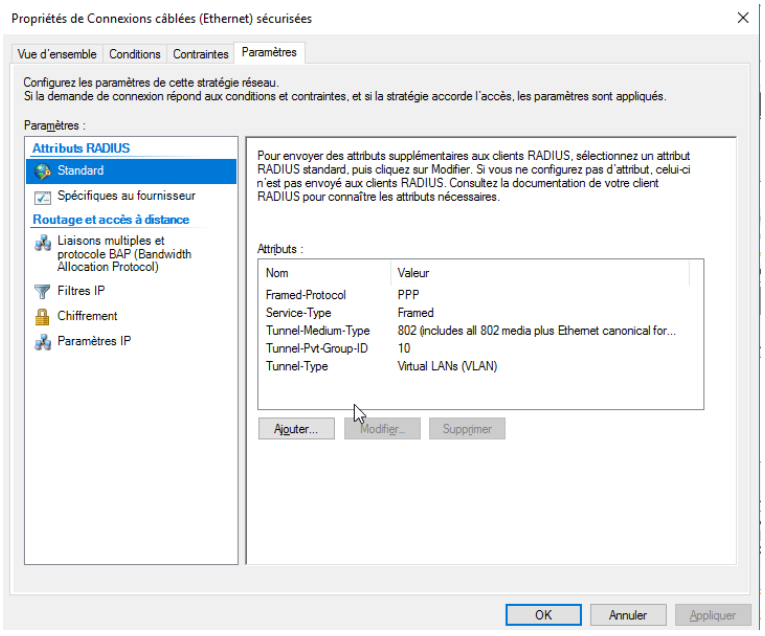

Fig. 4.33 : Ajout d'attributs Radius.

9. Dans l'onglet "Contraintes" (Contraintes), on choisit les méthodes d'authentification dans notre cas en a ajouté type de protocole EAP : « Protected EAP » et on a coché les cases « authentification chiffrée Microsoft version 2 (MS-CHAP v2) » et « authentification chiffrée Microsoft (MS-CHAP) » (figure 4.34).

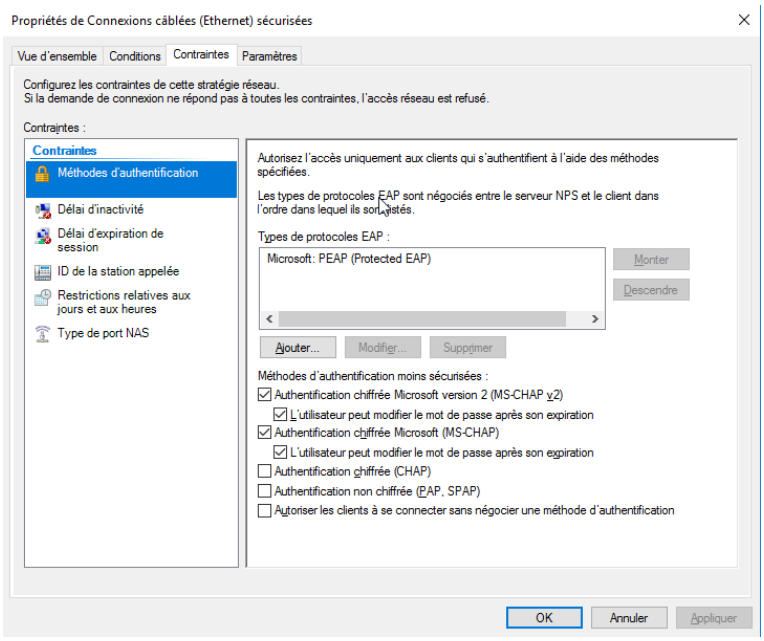

FIG. 4.34 : Choix des méthodes d'authentification pour la stratégie réseau.

Remarque :
Dans tout ce qui suit, nous allons effectuer toutes les configurations nécessaires pour le CORE1, et ça sera la même configuration pour le CORE2.

4.9 Configuration du serveur

1. Dans cette partie on vas attribuer une adresse IP statique au serveur (figure 4.35).

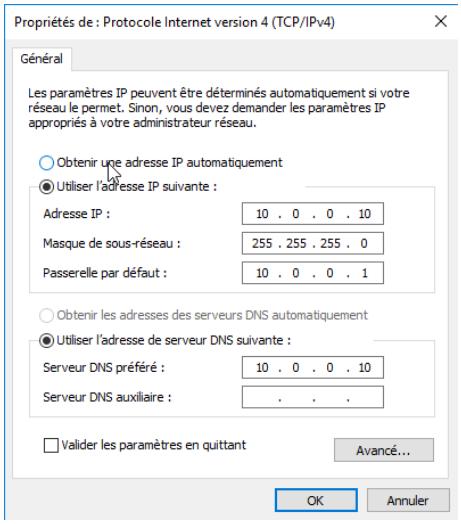

FIG. 4.35 : Configuration du serveur.

4.10 Configuration réseaux

Configuration de l'authentification accès à distance

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

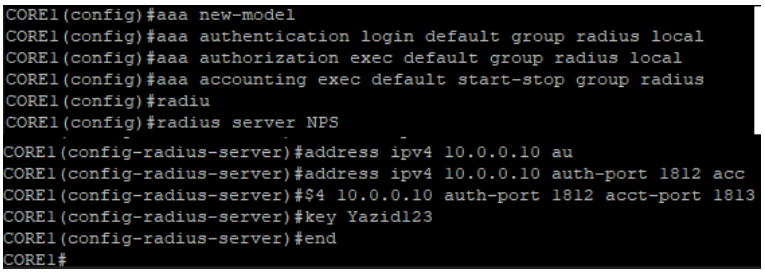

Fig. 4.36 : Activation de service AAA.

Activation de SSH

- Dans cette étape, nous avons activé le protocole SSH au niveau du CORE1 (figure 4.37).

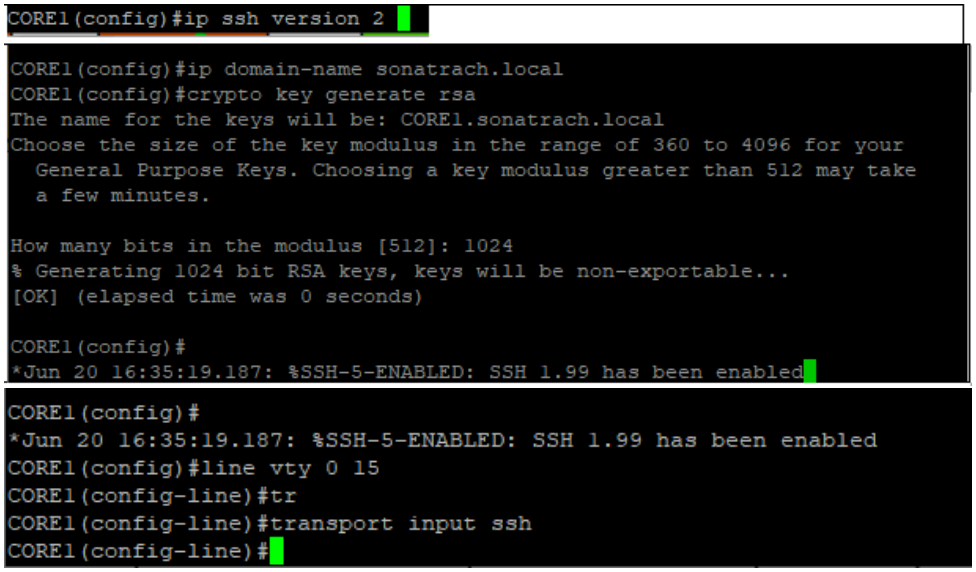

Fig. 4.37 : Activation du protocole SSH.

Configuration de l'authentification 802.1x

- La première commande de la figure sert à définir le groupe du serveur à utiliser pour l'authentification 802.1x.
- La deuxième commande sert à attribuer des autorisations aux utilisateurs.

```
CORE1(config)#aaa authentication dotlx default group radius
CORE1(config)#aaa authorization network default group radius
```

FIG. 4.38 : Définir et autoriser les réseaux à authentifier au serveur RADUIS.

- Activer la 802.1x sur le CORE1 : pour activer le contrôle des ports pour l'authentification 802.1x (Figure 4.39).

```
CORE1(config)#dotlx system-auth-control
```

FIG. 4.39 : Activation de contrôle des ports pour l'authentification 802.1x.

- Configurer l'authentification basée sur le port Gigabit 1/2 : activer l'authentification 802.1x sur le port (Figure 4.40).

```
CORE1(config)#int g 1/2
CORE1(config-if)#au
CORE1(config-if)#authentication po
CORE1(config-if)#authentication port-control auto
CORE1(config-if)#dotlx pae authenticator
CORE1(config-if)#authentication open
CORE1(config-if)#au
CORE1(config-if)#authentication host
CORE1(config-if)#authentication host-mode multi-domain
CORE1(config-if)#authentication host-mode multi-domain
```

FIG. 4.40 : Configuration du port Gigabit 1/2.

La configuration de DHCP relie

Dans cette étape on va indiquer que le DHCP est géré par le protocole DHCP du Windows Server.

```
CORE1(config)#interface vlan 10
CORE1(config-if)#ip helper-address 10.0.0.10
CORE1(config-if)#interface vlan 20
CORE1(config-if)#ip helper-address 10.0.0.10
```

FIG. 4.41 : La configuration de DHCP.

Test de DNS

- Ici, on va utiliser le programme informatique « nslookup » qui permet d'interroger le serveur DNS pour obtenir les informations définies pour le domaine « sonatrach.local » (Figure 4.42).

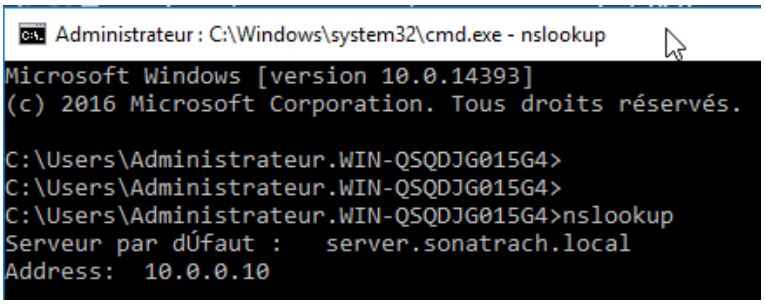

FIG. 4.42 : Le test DNS.

4.11 Tests de connectivité

Tests de connectivité entre l'utilisateur et les VLANs

- Dans cette étape, on effectue un test de connectivité de l'utilisateur VLAN 10 vers les VLANs 20 30 et 40 (Figure 4.43).

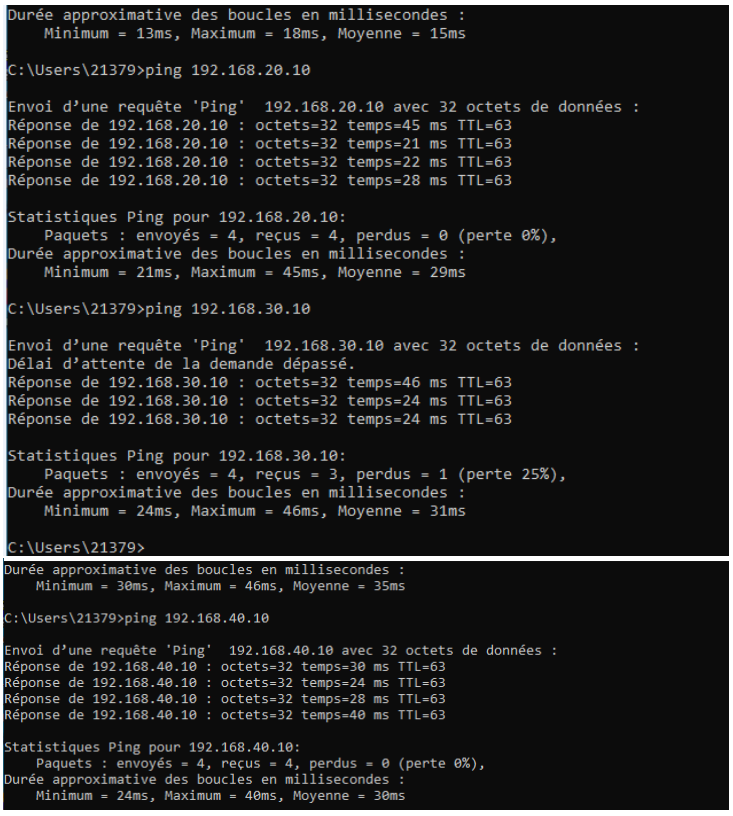

FIG. 4.43 : Ping de l'utilisateur VLAN 10 vers VLANs 20, 30 et 40.

- Maintenant, on effectue un test de connectivité de l'utilisateur VLAN 10 vers le serveur (Figure 4.44).

```
C:\Users\21379>ping sonatrach.local

Envoi d'une requête 'ping' sur SONATRACH.local [10.0.0.10] avec 32 octets de données :
Réponse de 10.0.0.10 : octets=32 temps=24 ms TTL=127
Réponse de 10.0.0.10 : octets=32 temps=12 ms TTL=127
Réponse de 10.0.0.10 : octets=32 temps=12 ms TTL=127
Réponse de 10.0.0.10 : octets=32 temps=12 ms TTL=127

Statistiques Ping pour 10.0.0.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 12ms, Maximum = 24ms, Moyenne = 15ms
```

FIG. 4.44 : Ping de l'utilisateur VLAN 10 vers le serveur RADIUS.

4.12 Configuration de l'utilisateur d'accès (Windows 10)

Pour la configuration de la machine de l'utilisateur (machine utilisateur) "Windows 10 ", on a suivi les étapes suivantes :

1. **Etape 1 :** Activer le service de configuration automatique de réseau câblé, qui est désactivé par défaut. Pour cela on doit taper " services " dans le champ de recherche présent dans la barre des tâches, On clique sur le service " configuration automatique du réseau câblé", "automatique" puis "démarrer".

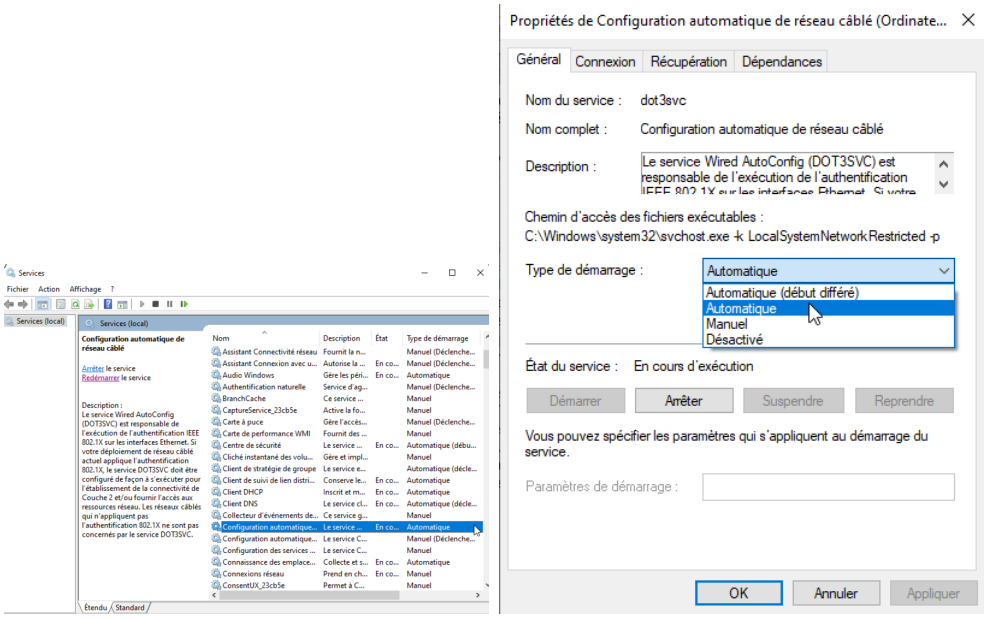

FIG. 4.45 : Démarrage de service « Configuration automatique de réseau câblé ».

2. **Etape 2 :** Pour ouvrir la connexion réseau, cliquer sur les boutons suivants : Démarrer, Panneau de configuration, Réseau et Internet, Centre réseau et partage, puis sur Gérer les connexions réseau. On clique avec le bouton droit sur la connexion pour laquelle on souhaite activer l'authentification 802.1X, puis sur Propriétés. On clique sur l'onglet " Authentification" ==> "Activer l'authentification IEEE 802.1X" puis on sélectionne "EAP protégé (PEAP) " comme Type EAP (figure 4.46).

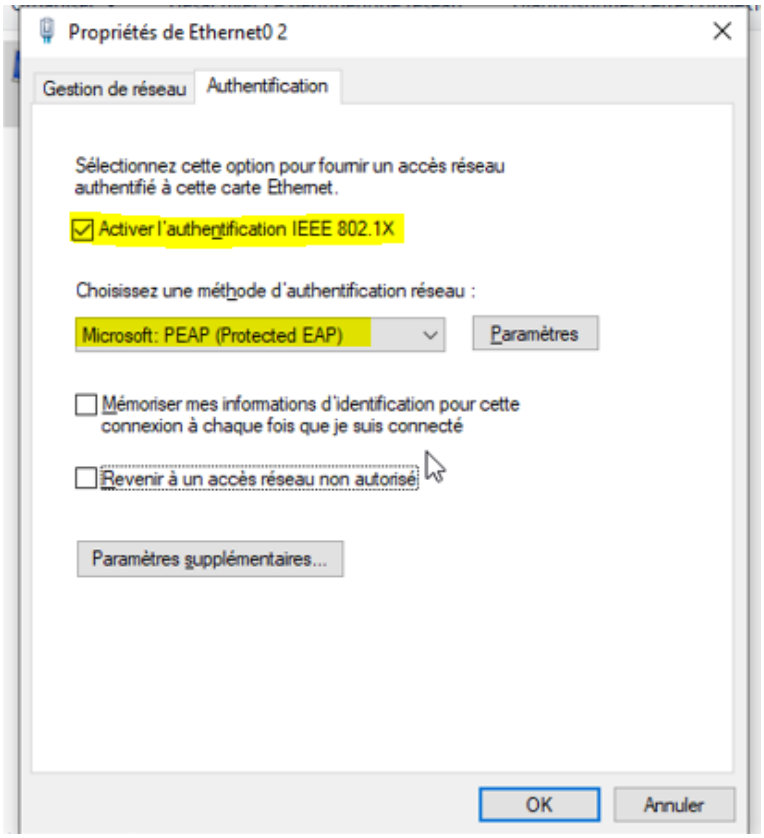

FIG. 4.46 : Activation de l'authentification 802.1x.

3. **Etape3 :** Cliquer sur propriétés du Type EAP puis cocher "Valider le certificat du Serveur" puis sélectionner le certificat qu'on a créé « sonatrach-SERVER-CA ». Puis sélectionner "EAP-MSCHAP v2" comme méthode d'authentification et cliquer sur "Configurer" pour cocher ou décocher "Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session" (figure 4.47).

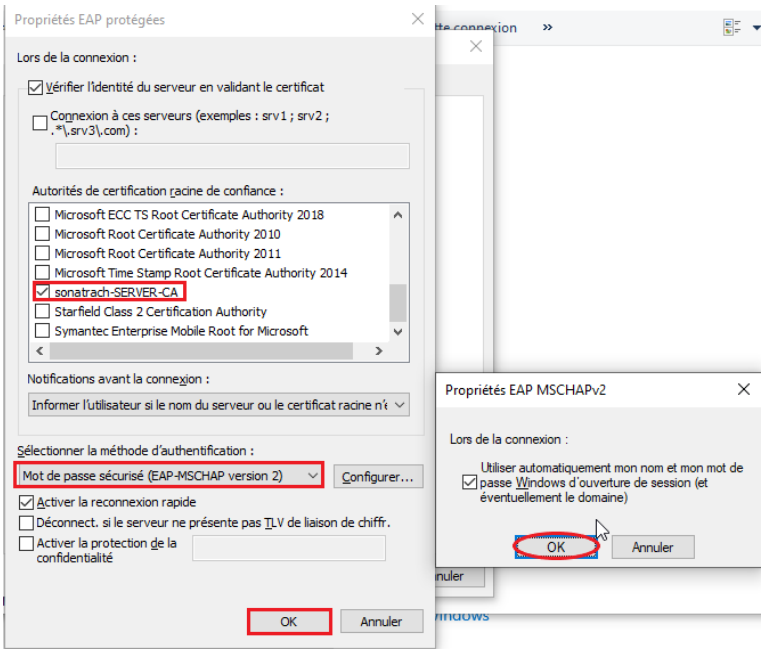

FIG. 4.47 : Sélection de méthode d'authentification " EAP-MSCHAP v2 ".

4. **Etape4 :** L'ajout de la machine au domaine "démarrer", un clic droit sur "poste de travail, puis sur "propriétés", "Nom de l'ordinateur", "Modifier", indiquer le nom de domaine (sonatrach.local) et à la fin on clique sur OK (figure 4.48).

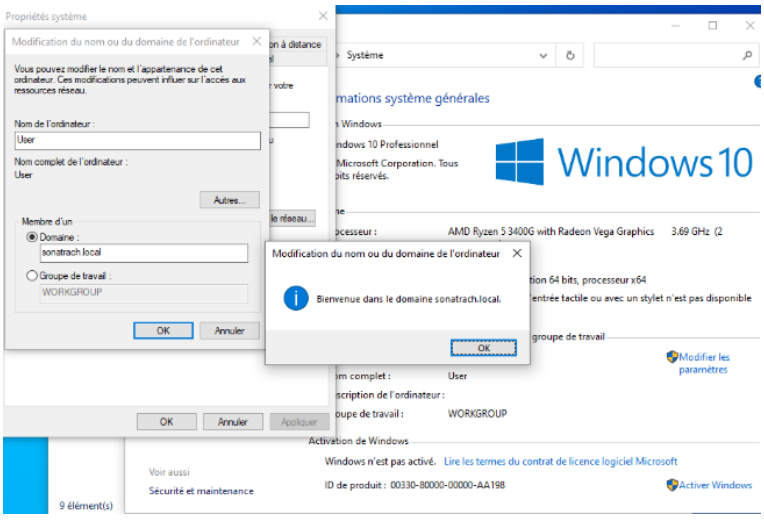

FIG. 4.48 : Ajout de la machine au domaine.

4.13 La solution de l'authentification accès à distance

1. Il faut d'abord vérifier que notre machine Windows 10 à une adresse IP (attribuée par le serveur DHCP) (Figure 4.49).

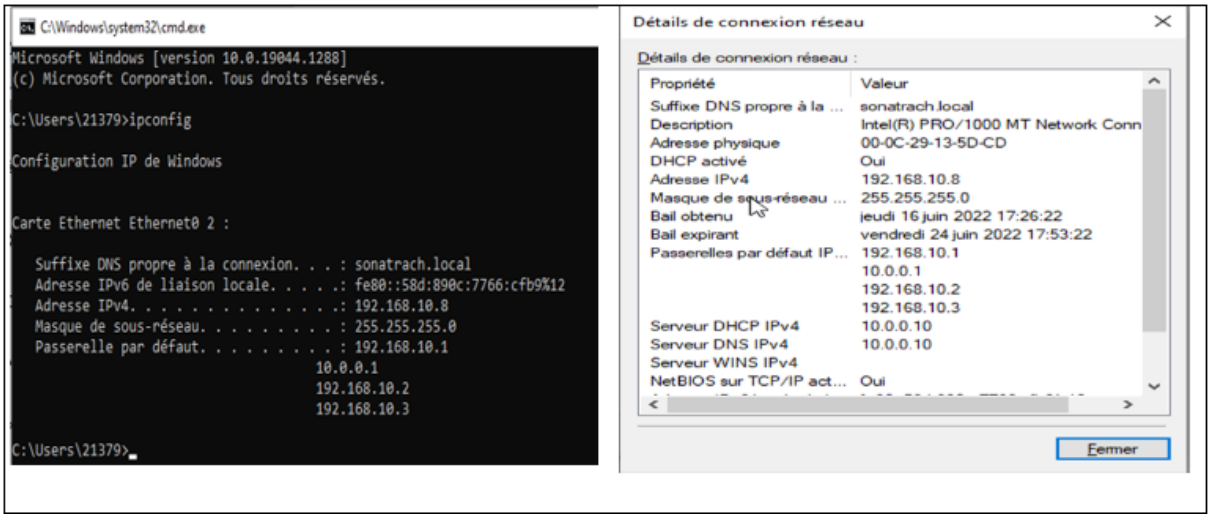

FIG. 4.49 : Vérification de l'existence d'une adresse IP.

2. L'utilisateur **Yazid** accède avec sa machine au commutateur CORE1.
   L'accès au switch avec un utilisateur **SSH** (Secure Shell) : permet de se connecter à une machine distante avec une liaison sécurisée Afin de s'assurer de notre bonne configuration, nous avons effectué des tests en faisant appel à "**PUTTY**" qui est un logiciel (et un protocole) permettant de se connecter à un ordinateur distant de façon sécurisée et permet en particulier d'ouvrir un Shell à distance.

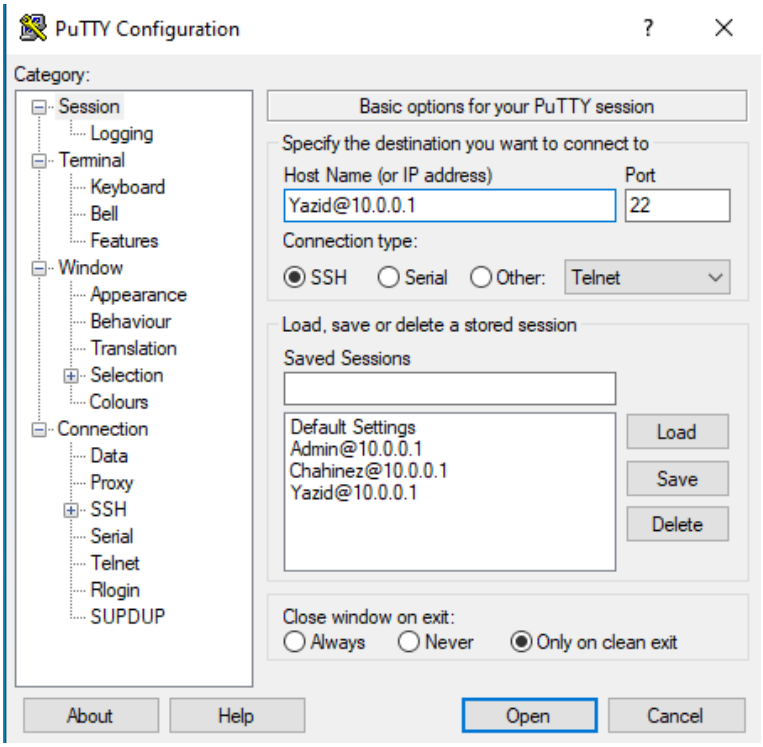

FIG. 4.50 : L'accès au switch avec un client SSH.

3. Maintenant il faut introduire le mot de passe pour accéder au switch. Sans Radius pas de gestion du mot de passe et pas de gestion des connexions d'utilisateurs à des

services distants. Ce dernier permet qu'aux membres du groupe Radius d'accéder à ces services en utilisant leur propre mot de passe.

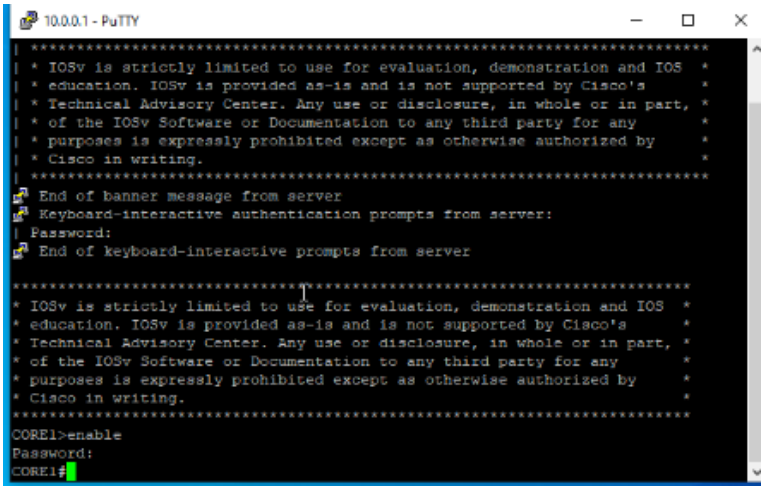

Fig. 4.51 : Accès de l'utilisateur au commutateur CORE1.

4.14 La solution de l'authentification 802.1x

Authentification d'un utilisateur au serveur radius

1. Avec l'utilisateur sous Windows 10 en test l'authentification par rapport au serveur Radius en utilisant les utilisateurs créés sur active directory qui appartient au groupe « Employés ».
   A la connexion du l'utilisateur une fenêtre s'affiche lui demandant de saisir nom de l'utilisateur ainsi que le mot de passe. Selon la zone d'accès demandée, sans Radius y'aura pas une vérification de l'identité celui-ci utilise les protocoles d'authentification CHAP ou EAP qui se chargent de définir comment l'information est cryptée et comment fonctionne le mécanisme de clé privée / clé publique sur le réseau. Ce dernier pourra exiger des informations supplémentaires pour l'authentification. Il est capable de bloquer une connexion en cours, suite par exemple à un délai d'inactivité dépassé. Enfin, il assure la journalisation des accès à partir de l'étude des ports UDP.

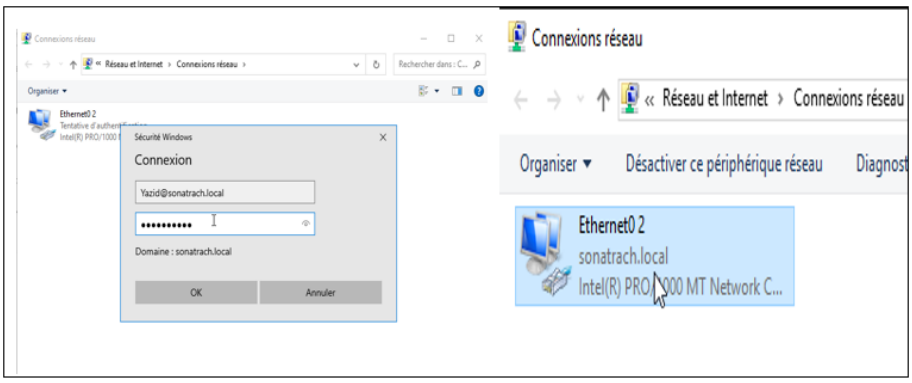

FIG. 4.52 : Utilisateur inscrit au serveur RADIUS “authentification avec succès“.

2. Sur le serveur Radius onvérifie la traçabilité de l'utilisateur en utilisant « observateur d'évènements ».

   - **Les étapes à suivre** ==> Cliquer sur observateur d'évènements puis sur affichage personnalisés aller sur rôles de serveurs et cliquer sur services de stratégie et d'accès réseau. Sans Radius n'y a pas de traçabilité des utilisateurs connectés au serveur, c'est pour cela il est conseiller d'utiliser Radius car il permet de garder trace de chaque activité.
     ==> Succès de l'audit (Figure 4.53).

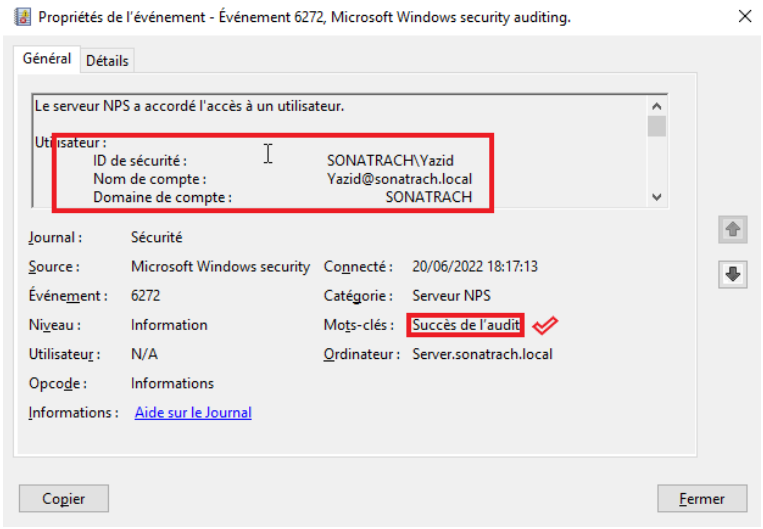

FIG. 4.53 : Succès de l'audit.

3. Comme on a vérifié précédemment l'utilisateur qui est membre du groupe « Employés », prenant maintenant un utilisateur qui n'est pas un membre du groupe (sachant que notre stratégie NPS autorise que les utilisateurs qui sont membre du groupe) (figure 4.54).

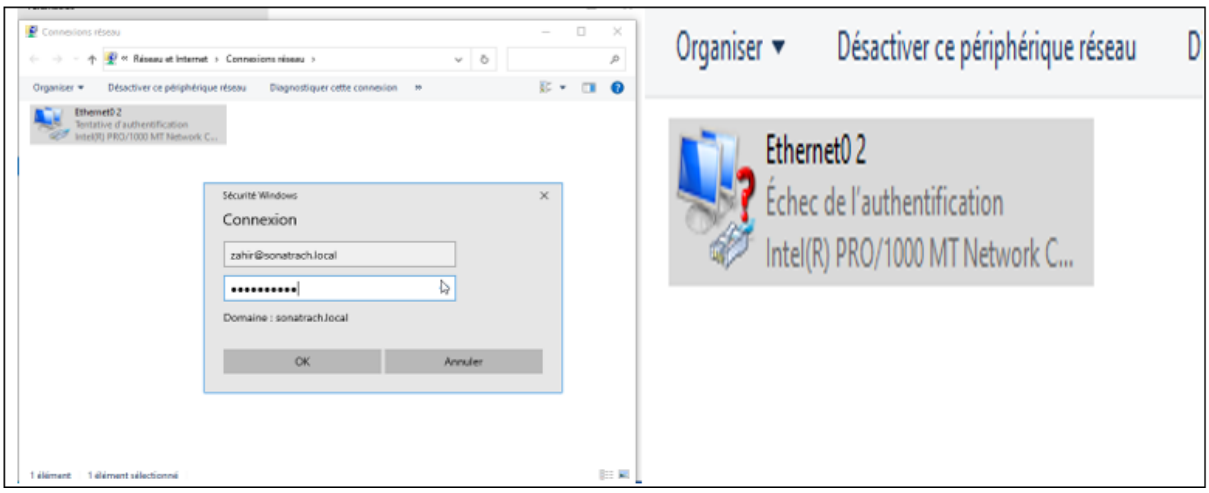

FIG. 4.54 : Utilisateur non inscrit au serveur RADIUS “échec de l’authentification“.

Sur le serveur Radius on vérifie la traçabilité de l’utilisateur qui n’est pas un membre du groupe « Employés » ==> **l’échec de l’audit** (Figure 4.55).

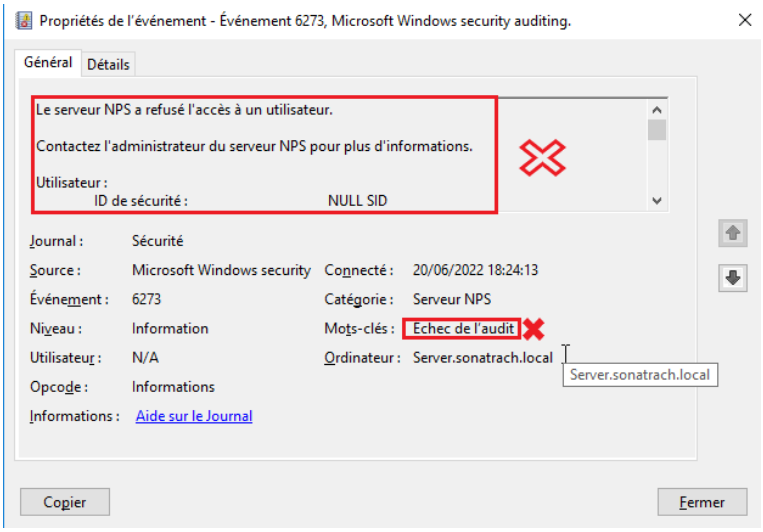

FIG. 4.55 : Echec de l’audit.

4.15 Conclusion

Dans ce chapitre, nous avons retenue qu’après l’identification des utilisateurs, leur authentification est nécessaire pour accéder aux données de notre système. Cette authentification, se fait par l’intermédiaire d’un serveur de contrôle d’accès RADIUS qui repose sur l’authentification 802.1x, chargé d’autoriser ou non l’accès aux données.
Afin de permettre ce service d’authentification et assurer son bon fonctionnement, ce serveur nécessite une configuration des ses composantes, ce qui fait le but de notre projet.

Conclusion générale et perspectives

Bien évidemment, la sécurité à 100% reste un idéal à atteindre, surtout devant le large éventail de menaces qui mettent en danger l'exploitation d'un réseau informatique dans une entreprise. Ainsi il est toujours important de bien formaliser une politique de sécurité en prenant en compte les risques réels qu'encourt un réseau informatique.
Dans ce travail, nous avons mis en œuvre une technique de sécurisation d'accès au réseau informatique de l'entreprise SONATRACH de Bejaïa, afin de mieux garantir les critères de 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 utilisant le protocole EAP pour le transport des informations d'identification en mode client/serveur, et un serveur d'identification Radius utilisant une base de données Active Directory, et s'appuyant sur le protocole AAA.
Pour la réalisation du service d'authentification RADIUS, nous avons utilisé Windows server 2016 qui inclut le serveur RADIUS, et qui fait appel à des services de domaines Active Directory permettant d'avoir des contrôleurs de domaines, on a pu aussi configurer le protocole 802.1x, ensuite nous avons appliqué l'authentification sur les différents équipements de notre réseau.

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 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, l'importance de la mise en œuvre du protocole Radius et le protocole 802.1x est capitale pour le bon fonctionnement du réseau informatique de toute entreprise. Mais ces derniers permettent uniquement de régler le problème d'authentification et ne permettent pas de faire face aux autres attaques telles que le DoS. Donc, nous devons implémenter des outils supplémentaires pour la sécurité tels que les antivirus et les cartes à puce.

Bibliographie

[1] M. LIHAN LI NDJOM Hans. *Cours sur Les Topologies Physiques des réseaux informatiques*. Ecole normale supérieur du Cameroun.

[6] Elie MABO. *La sécurité des systèmes informatiques (Théorie)*.

[10] Hocine malti. *histoire secete du pétrole algerien*. éditions la découverte, 2010.

[11] *Ressource interne de la RTC Béjaïa*.

[19] Alexander S. Gillis. *Technical Writer and EditorTaylaHolman*.

[20] M. Rizcallah. *annuaire LDAP*. EYROLLES, édition 2002.

[21] G. Mathieu. *Tester la sécurité de son annuaire Active Directory V2*. version du 30 janvier 2016. 7, édition 2013.

Webographie

[2] URL : http://zero202.free.fr/cr01-net/html/ch01s03.html (visité le 07/05/2022).

[3] *Les principaux composants de connexion.* URL : https://telecomubma.files.wordpress.com/2018/01/chapitre5-tc3a9lc3a9phonie-docx.pdf (visité le 10/05/2022).

[4] URL : https://openclassrooms.com/fr/courses/6944606-concevez-votre-reseau-tcp-ip/7236472-prenez-du-recul-sur-votre-pratique-grace-au-modele-osi (visité le 07/05/2022).

[5] URL : https://fr.m.wikibooks.org/wiki/Les_r%C3%A9seaux_informatiques/Les_mod%C3%A8les_OSI_et_TCP (visité le 10/05/2022).

[7] URL : https://www.wooxo.fr/Conseils-Cybersecurite/Principes-securite-informatique (visité le 17/05/2022).

[8] URL : https://www.futura-sciences.com/tech/definitions/piratage-cyberattaque-18946/ (visité le 13/05/2022).

[9] URL : https://actualiteinformatique.fr/cryptomonnaie/definition-cryptographie (visité le 10/05/2022).

[12] *Topologie-reseau.* URL : http%20://bits-genius.com/topologie-reseau/ (visité le 26/05/2022).

[13] *Switch 6509.* URL : https://www.cisco.com/c/en/us/products/switches/catalyst-6509-neb-a-switch/index.html (visité le 26/05/2022).

[14] *Switch 3750.* URL : https%20://www.cisco.com/c/dam/global/frfr/%20assets/documents/pdfs/datasheet/switching/Catalyst3750.pdf (visité le 29/05/2022).

[15] *Switch 3550.* URL : https://www.cisco.com/web/ANZ/cpp/refguide/hview/switch/3550.html (visité le 29/05/2022).

[16] *17 Swicht 2950.* URL : https://www.mercadoit.com/fr/5-switch-cisco (visité le 29/05/2022).

[17] URL : https://www.networklab.fr/hsrp/.

[18] URL : https://www.networklab.fr/spanning-tree-theorie/.

[22] URL : https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top%2026/05/2022.

[23] *DHCP.* URL : https%20://www.commentcamarche.net/contents/517-le-protocole-dhcpconsult%C3%A9 (visité le 06/05/2022).

[24] *RADIUS*. URL : https%20://cric.grenoble.cnrs.fr/Administrateurs/Documentations/SiteWebAuthentification/ServeurRadius.php (visité le 06/05/2022).

[25] URL : https://www.clicours.com/cours-architectures-et-protocoles-des-reseaux-chapitre-8-le-protocole-radius/ (visité le 31/05/2022).

[26] URL : https://xn--web-bfa.maths.unsw.edu.xn--au-3da/~lafaye/CCM/%C2%ACauthentification/%C2%ACpap.html.

[27] URL : https://www.juniper.net/documentation/fr/fr/software/junos/user-access/topics/topic-map/802-1x-authentication-switching-devices.html (visité le 24/05/2022).

[28] URL : http://igm.univ-mlv.fr/~dr/XPOSE2008/802.1x/EAP.html (visité le 29/05/2022).

[29] URL : https://xn--www-bfa.wikiwand.com/fr/%C2%ACExtensible_Authentica%C2%ACtion_Protocol.

[30] URL : https://www.juniper.net/documentation/fr/fr/software/junos/network-access-protocols/topics/topic-map/ppp-configuring.html (visité le 29/05/2022).

[31] URL : http://xn--www-bfa.iro.umontreal.ca/%C2%AC~kropf/ift-6052/%C2%ACnotes/ppp/index.html (visité le 29/05/2022).

[32] URL : https://fr.acervolima.com/protocole-d-authentification-par-mot-de-passe-pap/ (visité le 29/05/2022).

[33] URL : https://xn--cisco-packet-tracer-tutorial-qbbv.blogspot.xn--com-efa/2014/04/-configuration-et-comm%C2%ACandes-du-protocole.h%C2%ACtml?m=1.

[34] URL : https://web.maths.unsw.edu.au/~lafaye/CCM/authentification/chap.html (visité le 29/05/2022).

[35] URL : https://xn--slideplayer-dpa.fr/amp/%C2%AC5480222/ (visité le 29/05/2022).

[36] URL : https://web.maths.unsw.edu.au/~lafaye/CCM/authentification/ms-chap.html (visité le 29/05/2022).

[37] URL : https://xn--docs-kga.microsoft.com/%C2%ACen-us/openspecs/%C2%ACwindows_protocols/%C2%ACms-chap/%C2%AC7b03fc2e-ea27-414a-b4%C2%AC98-47d0ff84d990 (visité le 29/05/2022).

[38] URL : https://xn--security-lla.xn--stackexchange-7ra.com/questions/%C2%AC183418/%C2%ACmschapv2-authenticati%C2%ACon-and-evil-twin-att%C2%ACack (visité le 29/05/2022).