REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A. MIRA – BEJAIA
Faculté Sciences exactes
Département informatique

Mémoire de fin d'études

Présenté par

MADI Yasmine & ZADIR Ryma

En vue de l'obtention du diplôme de

Master en Informatique

Option : Réseaux et Sécurité

Thème

Intégration d'une solution d'authentification basée sur la norme 802.1x avec certificats

Soutenu le 02/07/2024

Devant le jury composé de :

Nom et Prénom			
M^me^ GADOUCHE Hania	**M.C.B**	Université deBejaia	Présidente
M^me^ SAAD Narimane	**M.C. B**	Université de Bejaia	Examinatrice
M^r^ FARAH Zoubeyr	**M.C. A**	Université de Bejaia	Encadrant
M^r^ DJEBBARI Yassine	**Ingénieur**	Campus NTS Bejaia	Encadrant de stage

Année Universitaire 2023/2024

Remerciements

Au nom du dieu le tout puissant sans lui rien de tout cela n'aurait pu être.

Nos vifs remerciements accompagnés de toute nos gratitudes vont ensuite encadrant Monsieur ***ZOUBEYR FARAH*** *d'avoir accepté de nous encadrer, pour ses conseils et ses corrections qui nous ont permis d'améliorer le document final.*

Nos remerciements à Monsieur ***DJEBBARI YASSINE*** *notre encadrant de stage pour ses remarques et conseils, pour d'avoir accepté de nous encadrer, qui nous a aidé à organiser ce stage au sein de l'entreprise campus NTS et de nous avoir fait travailler sur un sujet très intéressant qui nous a beaucoup apporté.*

Nos remerciements les plus vifs à nos parents qui nous ont soutenus. Nous ne serons jamais assez reconnaissants envers eux. Ils ont toujours tout mis en œuvre pour qu'on puisse s'épanouir dans tout ce que nous entreprenons.

Nous remercions également les membres de Jury qui ont accepté d'évaluer ce travail. Enfin, Nous remercions nos familles et nos amis pour leur aide et leur soutien précieux durant cette année.

Enfin, merci à toute personne qui nous a aidé de près ou de loin.

Dédicace

Je rends grâce au bon Dieu de m'avoir donné la force, la volonté et la sagesse afin de parvenir à cette conclusion de mon cycle.

Dans cet espace je souhaiterai dédier ce travail à mes très chers parents

En premier lieu mes dédicaces vont droit à ma chère mère,

Tes encouragements et tes prières ont été d'un grand soutien pour moi, je ne serai te remercier comme il se doit ton affection, ta bienveillance et ta présence à mes coté a toujours été ma source de force pour affronter les différents obstacles, que dieu te garde pour moi.

A mon cher père,

Ta présence dans ma vie, tes précieux conseils, ton soutien fut une lumière dans tout mon parcours, ce modeste travail est le fruit de tous les sacrifices que tu as déployés pour mon éducation et ma formation, j'espère avoir réussi à te rendre fière chose que je tâcherai de continuer à faire, que dieu te garde pour moi.

A mon unique cher Frère Mehdi,

Prunelle de mes yeux tu as toujours été à mes cotes pour me soutenir et m'encourager, je suis fière de toi, je t'aime très fort, je te souhaite toute la réussite et le bonheur dans ton parcours ainsi que ta vie et que Dieu te préserve inshallah

A mes chers sœurs Assia et Amel,

Que je porte dans mon cœur, je vous aime très fort, je ne vous souhaite que de la réussite et que Dieu vous protège inchallah

A toute ma famille, a tous ceux qui ont veillé à mon instruction

Avec l'expression de tous mes sentiments et mon respect,

Yasmine MADI

Dédicace

À mes très chers parents,

Ma raison de vivre, pour leurs sacrifices inlassables et leur soutien indéfectible tout au long de mes études. Que Dieu les garde et les protège.

À mon cher frère Ismaël,

Tu es celui sur qui je peux toujours compter. Ce mémoire est dédié à la force de notre lien. Merci d'être toujours là, pour moi.

À mon cher mari Saïd,

Ta force et ton soutien indéfectible sont le roc sur lequel je m'appuie.

À mon petit ange, Aris,

Chaque sourire est un rayon de lumière dans ma vie. Que Dieu te garde en parfaite santé.

À mon beau-frère Ayoub et ma belle-sœur Salma,

Votre présence dans ma vie est une bénédiction que je chéris profondément.

Ryma ZADIR

TABLE DES MATIERES

Liste des figures

Liste des tableaux

Liste des abréviations

AAA Authentication Authorization Accounting AD Active Directory

CA Certificate Authority

CHAP Challenge Handshake Authentication DHCP Dynamic Host Configuration

DNS Domain Name System

EAP Ertensible Authentication

GPO Group Policy Object

NAS Network Access Server

NPS Network Policy Server, OSI Open Systems Interconnection

PC Personnel Computer PEAP Protected Ertensible Authentication Protocol

RADIUS Remote Authentication Dial-In User Serunce

TCP Transmission Control Protocol

VLAN Virtual Local Area Network OU Organization Unit VMwar Virtual Machine

VPN Virtual Private Network

WAN Wide Area Network

PAP Password Authentication Protocol

MS-CHAP Microsoft Challenge Handshake Authentication Protocol

Introduction générale

De nos jours, la plupart des entreprises possèdent un nombre considérable de postes informatiques interconnectés via un réseau local. Ce réseau permet l'échange de données essentielles entre différents collaborateurs au sein de l'entreprise. Dans ce contexte, renforcer la sécurité devient indispensable pour garantir la confidentialité, l'intégrité et le contrôle d'accès au réseau, réduisant ainsi les risques d'attaques potentielles.

Le centre d'appels Collable ressent le besoin urgent d'adopter des solutions de sécurité réseau avancées, en particulier des systèmes de contrôle d'accès robustes. Dans cette optique, notre travail vise à mettre en place un système d'authentification par certificat, où chaque ordinateur de l'entreprise recevra un certificat d'authentification. Pour atteindre cet objectif, nous avons opté pour une solution basée sur le serveur RADIUS.

Ce mémoire est structuré en quatre chapitres : Le premier chapitre offre une introduction aux réseaux informatiques, exposant brièvement les concepts théoriques essentiels pour une compréhension approfondie des éléments nécessaires à la résolution de notre problématique. Le deuxième chapitre traite des systèmes d'authentification et de la norme 802.1x. Le troisième chapitre présente l'environnement spécifique dans lequel notre projet s'est déroulé. Enfin, le quatrième chapitre détaille l'installation du serveur RADIUS et décrit le déploiement simulé de la solution d'authentification avec GNS3, suivi d'un test de validation pour assurer la configuration optimale des processus de sécurisation.

La norme 802.1X joue un rôle crucial dans notre approche de sécurité réseau pour Collable. En établissant un cadre standardisé pour le contrôle d'accès au réseau, elle permet une authentification sécurisée des utilisateurs et des périphériques avant qu'ils n'accèdent aux ressources réseau. En intégrant cette norme dans notre solution, nous assurons une protection renforcée contre les accès non autorisés et les attaques potentielles, tout en offrant une gestion centralisée et efficace des droits d'accès. Ainsi, en combinant un système d'authentification par certificat avec la norme 802.1X, nous visons à garantir à Collable un environnement réseau fiable, sécurisé et conforme aux meilleures pratiques de sécurité actuelles.

CHAPITRE I :
Généralités sur les réseaux et la sécurité informatique

1.1. Introduction

La problématique de sécurité est omniprésente lorsque l'on évoque les systèmes d'informations et elle devient fondamentale lorsque l'on parle des réseaux. Comme tous les êtres humains, les usagers d'un réseau ressentent le besoin de sécurité et cela est dû à la grande place qu'occupe le réseau dans leurs vies. Les données transmises se rapportant à des biens personnels et professionnels nécessitent la confidentialité des échanges, l'authentification des sources, la garantie de leur intégrité, etc.

Ces apports ne peuvent, par ailleurs, être fournis sans la garantie de la disponibilité du réseau et des services associés. On ne peut en effet concevoir la sécurité sans la sûreté de fonctionnement.

1.2. Définition des réseaux informatiques

Un réseau informatique est un ensemble de périphériques (ordinateurs, tablettes, imprimantes, Serveurs, commutateurs, routeurs, etc.). Reliés par divers moyens matériels (médias) fibre optique, paire torsadée, ondes radio, Bluetooth, etc.) et logiciels (ex. Protocoles et applications réseau pour échanger des informations (données, images, vidéo, voix) etc.) et offrir des services aux utilisateurs.

Un réseau informatique peut servir :

- Facilitent notre travail avec le partage de fichiers, d'applications et de ressources.
- La communication entre personnes (grâce au courrier électronique, la discussion en direct,).
- La communication entre processus (entre des machines industrielles).
- La garantie de l'unicité de l'information (bases de données).
- Facilitent l'apprentissage avec la création de classes virtuelles, la diffusion vidéo, les espaces d'apprentissage collaboratifs, l’apprentissage sur appareils mobiles.
- Permettent de réduire considérablement les coûts d'infrastructure
- Facilitent le divertissement : les jeux en ligne, la messagerie instantanée, etc.

1.3. Classification des réseaux

On peut distinguer différents types de réseaux selon plusieurs critères tel que : leurs étendues, leurs architectures et leurs topologies.

1.3.1. Classification selon l'étendue géographique

[1] Voir la Figure 1.1

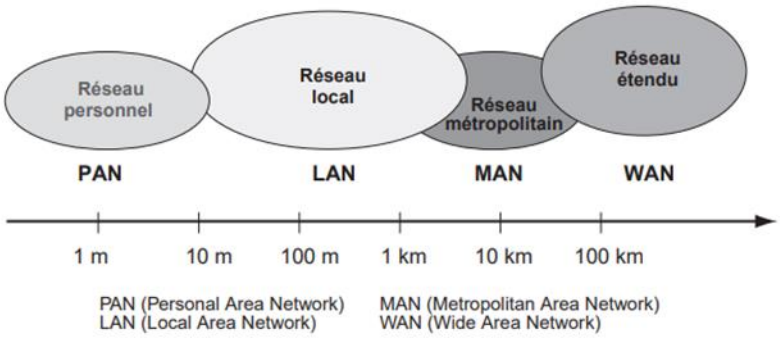

Figure I.1 : catégories de réseaux informatiques.

a. PAN (Personale Area Network)

Ces réseaux personnels, appelés aussi réseaux domestiques, interconnectent sur quelques mètres (généralement sur 10m ou moins) les équipements personnels (tel que les téléphones portables, PDA, oreillettes, terminaux GSM, organiseurs, domotique, etc.) d'une seule personne ou d'un très petit nombre de personne.

b. LAN (Local Area Network)

Ce sont des réseaux de taille plus ou moins modeste (quelques dizaines à quelques centaines de mètres correspondent par leur taille aux réseaux intra-entreprise, d'un campus, d'une salle informatique, d'un bâtiment ou équivalents. L'infrastructure est privée et est gérée localement. Ils sont couramment utilisés pour le partage de ressources commune comme des périphériques (imprimantes), des données ou des applications.

c. Réseaux MAN (Métropolitain Area Network)

Les réseaux métropolitains permettent l'interconnexion de plusieurs réseaux locaux répartis sur différents sites dans une ville (sur une distance comprise environ entre 5Kms et 50Kms). Ces réseaux peuvent être placés sous une autorité publique ou privée comme le réseau intranet d'une entreprise, d'une université ou d'une ville. Il permet donc pour une société, une ville, de contrôler elle-même son réseau. Ce réseau est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits qui utilise généralement des fibres optiques, Mais aussi des lignes téléphoniques**.**

d. Réseaux WAN (Wide Area Network)

Les réseaux longue distance WAN ou réseaux étendus, sont destinés comme leurs noms l'indiquent, à assurer la transmission des données sur une très grande distance géographique. Ils

permettent l'interconnexion entre LANs ou MANS à l'échelle d'un pays, d'un continent voire de la planète.

Leurs supports de transmission sont variés (lignes téléphoniques, ondes hertziennes, fibre optique, satellite, etc.). L'infrastructure est en général publique.

Le plus grand et connu réseau WAN est le réseau InterNet (Inter Networking ou interconnexion de réseaux).

1.3.2. Classifications selon l'architecture

Il existe deux catégories de réseaux LAN

- Réseau peer-to-peer (poste à poste)
- Réseau avec serveurs dédiés **[2]**.

a) Réseaux LAN poste à poste ou égal à égal (Peer to Peer)

Chaque poste ou station agit en tant que client et serveur.

Le grand avantage de tels systèmes est le faible coût (postes de travail, cartes réseau, Switch, câbles).

Par contre, si le réseau commence à comporter plusieurs machines (>10 postes) il devient impossible à gérer.

b) Réseaux LAN avec serveur dédié (client/serveur)

C'est un peu comme un réseau peer-to-peer, mais avec un poste plus puissant destiné a des taches bien précises : **le serveur**

Le serveur centralise les données liées au bon fonctionnement du réseau. Dans l'exemple précédant, c'est lui qui contient tous les mots de passe. Ainsi les comptes utilisateurs et mots de passe ne se trouvent plus qu'à un seul endroit, il est donc plus facile pour l'administrateur du réseau de faire des modifications ou des créations.

L'avantage de ce type est de facilité de gestion d'un nombre important de postes. Voir la Figure 1.2.

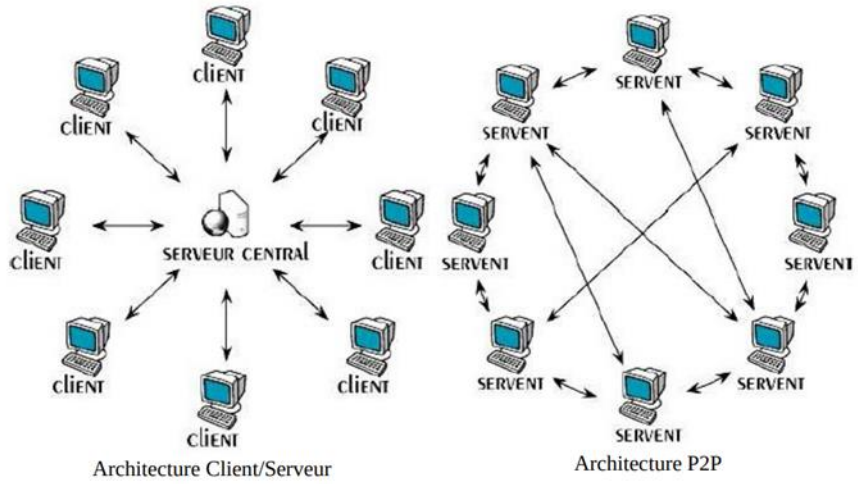

Figure 1.2 : Classification selon l'architecture

1.3.3. Classifications selon la topologie

Dans les réseaux, nous distinguons différents types de topologies que l'on peut classer en deux grandes catégories :

La topologie physique : relative au plan du câblage, elle désigne l'organisation ou la disposition physique (l'architecture d'un réseau) des nœuds (un ordinateur, une imprimante, un équipement d'interconnexion, etc.) du réseau. (Définit la manière dont les équipements sont reliés entre eux). Voir la Figure 1.3

Parmi les topologies physiques, on trouve :

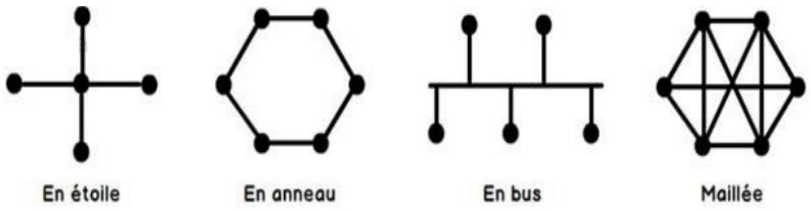

Figure 1.3: Topologies Physiques

La topologie logique : typologie d'échange, précise la façon dont les informations circulent au plus bas niveau. (Définit le chemin que prennent les signaux de données à travers la topologie physique)

Une topologie logique définit comment les données sont transmises. Tandis que la topologie physique consiste à définir des périphériques réseau et du câblage

1.4. Modèle de communication

1.4.1 OSI

Le modelé OSI (open system interconnexion ou interconnexion de système ouverts) a été mise en place par l'ISO (international Organization for Standardization Organisation internationale de normalisation, http://www.iso.org) afin de normaliser les communications entre les ordinateurs d'un réseau. En effet, aux origines des réseaux chaque constructeur avait un système propre (système propriétaire) et de nombreux réseaux incompatibles coexistaient. Ce modèle a permis de standardiser la communication entre les machines afin que les différents constructeurs puissent mettre au point des produits (logiciels ou matériels) compatibles (pour peu qu'ils respectent scrupuleusement le modèle OSI).

Le modèle OSI est un modèle qui comporte 7 couches, tandis que le modèle TCP/IP n'en comporte que 4. En réalité le modèle TCP/ IP a été développé à peu près au même moment que le modèle OSI, c'est la raison pour laquelle il s'en inspire sans être conforme à ses spécifications **[3]**. Voir la Figure 1.4.

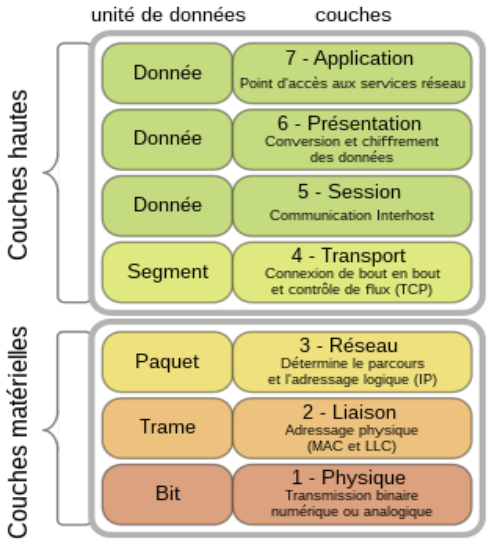

Figure1.4 : Modèle OSI

Les rôles des différentes couches sont les suivants :

- **La couche Physique** définit la façon dont les données sont physiquement converties en signaux numériques ou analogiques sur le média de communication (impulsions électriques, modulation de la lumière, etc.).
- **La couche Liaison de données** définit l'adressage physique : l'interface avec la carte réseau (par son adresse MAC) et le partage du média de transmission.

- **La couche Réseau** permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau (adresse IP).
- **La couche Transport** est chargée du transport des données, de leur découpage en paquets et de la gestion des éventuelles erreurs de transmission : ports, TCP et UDP.
- **La couche Session** gère les sessions de communication entre les différentes applications.
- **La couche Présentation** définit le format des données manipulées par le niveau applicatif (leur représentation éventuellement leur compression et leur chiffrement) indépendamment du système.
- **La couche Application** assure l'interface avec les applications : c'est le niveau le plus proche des utilisateurs, le point d'accès aux services réseau géré directement par les logiciels.

1.4.2. TCP/IP

Le modèle TCP/IP reprend l'approche modulaire du modèle OSI (utilisation de modules ou de couches) mais ne contient, lui, que quatre couches. Ces couches ont des tâches beaucoup plus diverses étant donné qu'elles correspondent à plusieurs couches du modèle OSI.

Les rôles des différentes couches sont les suivants :

- **La couche Accès réseau** spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.
- **La couche Internet** est chargée de fournir le paquet de données (datagramme).
- **La couche Transport** assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission.
- **La couche Application** englobe les applications standards du réseau. Voir la Figure 1.5

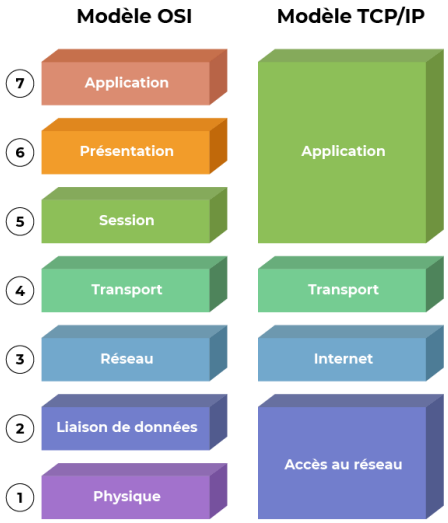

Figure 1.5: Comparaison des modèles OSI et TCP IP

1.5. Routage IP [4].

Parmi les fonctionnalités principales de la couche IP, on trouve le routage IP qui consiste à déterminer la manière d'acheminer les datagrammes IP à travers les différents réseaux d'un internet. Chaque réseau se compose d'un ou de plusieurs machines, et est relié aux autres réseaux par des routeurs. La fonction du routeur est de transmettre les paquets IP d`un réseau à un autre selon un algorithme de routage prédéfini. On peut distinguer deux types de routage

- **Le routage direct :** Permet de transférer directement un datagramme d'une machine à une autre, et peut être utilisé par deux machines si elles sont reliées directement au même système de transmission physique (Ethernet).
- **Le routage indirect :** Permet de transmettre les datagrammes d'un réseau à un autre, ainsi il est nécessaire de déterminer vers quel routeur envoyer un datagramme IP en fonction de sa destination finale.

Dans le cas du routage indirect le choix du routeur vers lequel va être envoyé le datagramme IP se fait à l'aide des tables de routages. Ces tables contiennent les informations relatives aux différentes destinations possibles et à la façon de les atteindre. Machines et routeurs possèdent tous des tables de routage.

D'un point de vue fonctionnel une table de routage contient des paires d'adresses du type (D, R) où D est l'adresse IP d'un réseau destination et R l'adresse IP du routeur suivant sur le chemin menant à cette destination. Tous les routeurs mentionnés dans une table de routage doivent bien sûr être directement accessibles à partir du routeur considéré. Cette technique, dans laquelle un

routeur ne connaît pas le chemin complet menant à une destination, mais simplement la première étape de ce chemin, est appelée routage par sauts successifs (next-hop routing).

Il existe deux modes de routages bien distincts lorsque nous souhaitons aborder la mise en place d'un protocole de routage, il s'agit du routage statique et du routage dynamique.

a) Routage statique : Dans le routage statique, les administrateurs vont configurer les routeurs un à un au sein du réseau afin d'y saisir les routes (par l'intermédiaire de port de sortie ou d'IP de destination) à emprunter pour aller sur tel ou tel réseau. Concrètement, un routeur sera un pont entre deux réseaux et le routeur d'après sera un autre pont entre deux autres réseaux.

b) Routage dynamique : : Le routage dynamique permet quant à lui de se mettre à jour de façon automatique. La définition d'un protocole de routage va permettre aux routeurs de se synchroniser et d'échanger des informations de façon périodique ou événementielle afin que chaque routeur soit au courant des évolutions du réseau sans intervention manuelle de l'administrateur du réseau. Concrètement, le protocole de routage fixe la façon dont les routeurs vont communiquer mais également la façon dont ils vont calculer les meilleures routes à emprunter.

1.6. Adressage [1]

IP Une adresse IP (IPv4) ou adresse logique est un numéro d'identification de 32, soit 4 octets. L'adresse IP est le plus souvent écrite en notation décimale pointée : les octets sont séparés par des points et chaque octet représente un nombre décimal compris entre 0 et 255.

- **La partie réseau** (NET-ID) : une sous-séquence qui désigne l'adresse (l'identifiant) d'un réseau
- **La partie hôte** (HOST-ID) : une sous-séquence qui désigne l'adresse (l'identifiant) d'une machine sur le réseau désigné par le net-ID.

1.6.1. Classe d'adresse IP

Les adresses IP sont réparties en cinq classes Les champs NET-ID et HOST-ID ont des longueurs variables, qui dépendent de la classe de l'adresse IP

Classe A. (grands réseaux)

Les adresses de classe A sont attribuées aux réseaux comportant un nombre élevé d'hôtes. Le NET- ID est alors codé sur le premier octet et les trois derniers octets représentent le HOST-ID.

Classe B. (réseaux moyens)

Les adresses de classe B sont attribuées à des réseaux de taille moyenne à grande. Le NET-ID alors codé sur 2 octets et l'HOST-ID est codé sur les deux autres octets.

Classe C. (Petits réseaux)

Les adresses de classe C sont généralement employées pour de petits réseaux locaux. Le NET-ID est alors codé sur les 3 premiers octets et le HOST-ID sur le dernier octet.

Classe D. (Multicast)

La classe D ne peut pas être utilisée pour adresser des équipements individuels, mais elle est utilisée pour la diffusion d'un message à un groupe de nœud IP Dans cette classe.

Classe E. (Classe réservée)

Ce sont les adresses dont les cinq bits de poids fort sont 1111 C'est une classe réservée pour des usages futurs.

1.6.2. Adresse IP privée

Les adresses IP privées représentent toutes les adresses IP de classe A, B et C non routable sur internet (elles sont masquées pour Internet et tous les autres réseaux) donc jamais attribuées par un FAI (fournisseurs d'accès à Internet), et que l'on peut utiliser librement en interne dans un réseau privé (Particulier, entreprise, LAN, etc.).

Les réseaux privés se sont développés en réaction à deux évolutions d'Internet : la mauvaise utilisation et la pénurie de de l'adressage IPv4, et les besoins de sécurisation des réseaux d'entreprises. Ainsi des réseaux privés différents peuvent utiliser les même adresses IP privées à condition que les hôtes qui les utilisent soient visibles uniquement à l'intérieur de ces réseaux. Les adresses IP publiques sont celles qui sont exposées à Internet.

Les classes d'adresse A, B et C comprennent chacune une plage d'adresses IP privées à l'intérieur de la plage globale. Pour créer son propre réseau local en TCP/IP, on utilise ce type d'adresses.

1 .7. La sécurité informatique

La sécurité informatique est les mécanismes utilisés pour la protection de l'information contre les menaces et les attaques informatiques **[5]**.

Consiste généralement en cinq principaux objectifs :

- L'intégrité : garantir que les données sont bien celles que l'on croit être.
- La disponibilité : maintenir le bon fonctionnement du système d'information.
- La confidentialité : rendre l'information inintelligible `a 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 **[6]**.

1.8. Les menaces

Une menace est une violation potentielle de la sécurité, c'est-à-dire un signe qui laisse prévoir un danger **[7]**.

1.9. Les attaques

Une attaque est l'exploitation d'une vulnérabilité d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) par des actions que ce soit accidentelles, malveillantes ou intentionnelles **[8]**.

1.9.1. Type d'attaque

Les attaques peuvent ˆêtre regroupées en trois familles différentes **[8]** :

• Les attaques directes

C'est la plus simple des attaques. Le hacker attaque directement sa victime `a partir de son ordinateur. En effet, les programmes de hack qu'ils utilisent ne sont que faiblement paramétrable.et un grand nombre de ces logiciels envoient directement les paquets a la victime Voir la Figure 1.6

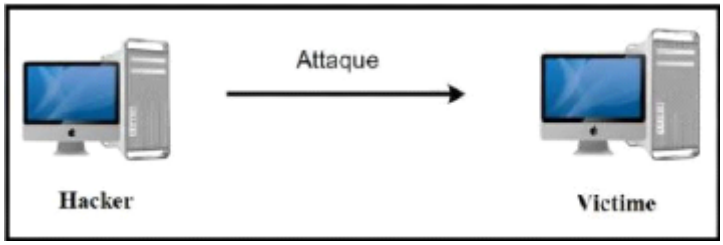

Figure 1.6 : Les attaques directes

•Les attaques indirectes par rebond

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :

- Masquer l'identité (l'adresse IP) du hacker.
- Utiliser les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante) pour réaliser son attaque.

Le principe en lui-même, est simple : les paquets d'attaque sont envoyés à l'ordinateur intermédiaire, qui répercute l'attaque vers la victime. D'où le terme de rebond. Voir la Figure 1.7

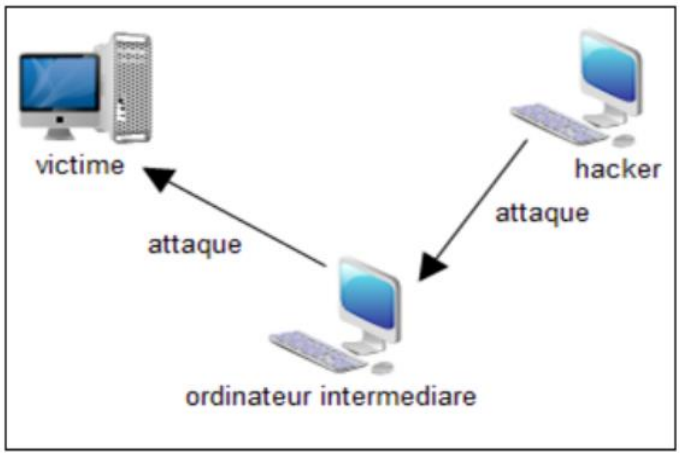

Figure 1.7 : Les attaques indirectes par rebond

•Les attaques indirectes par réponse

Cette attaque est une dérive par rebond. Elle offre les mêmes avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête et c'est cette réponse à la requête qui va être envoyé à l'ordinateur victime Voir la Figure 1.8

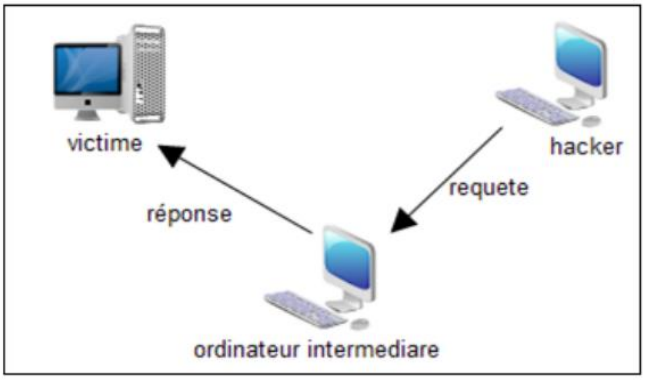

Figure1.8 : Les attaques indirectes par réponse

1.9.2. Descriptions de quelques attaques

- **L'attaque Man In The Middle**

L'attaque man-in-the-middle (Homme au milieu) est une technique de piratage informatique consistant à intercepter des échanges cryptés entre deux personnes ou deux ordinateurs A et B pour décoder les messages. L'attaquant doit donc être capable de recevoir les messages des deux parties et d'envoyer des réponses à une partie en se faisant passer pour l'autre **[7]**. Voir la Figure 1.9

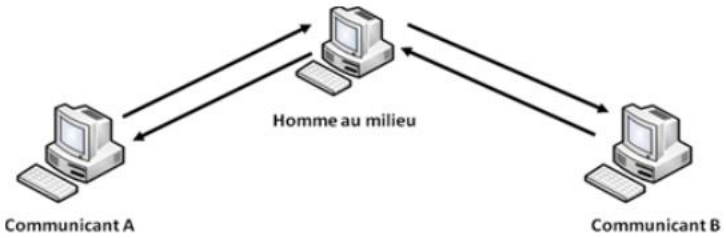

Figure 1.9: Attaque Man In The Middle

- **Les attaques par saturation (déni de service)**

Cette technique d'attaque consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs dont le but de paralyser un site pendant quelques heures, et d'en bloquer ainsi l'accès aux internautes. Il existe différentes attaques par saturation, parmi ces attaques **[10]** :

- **Le flooding**

Cette attaque consiste à envoyer `a une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.

- **Le smurf**

Le smurf est une attaque qui s'appuie sur le ping (Packet Internet Groper) et les serveurs de broadcast. On falsifie d'abord son adresse IP pour se faire passer pour la machine cible. On envoie alors un ping sur un serveur de broadcast. Il le fera suivre `a toutes les machines qui sont connectées qui renverront chacune une réponse au serveur qui fera suivre à la machine cible. Celle-ci sera alors inondée sous les paquets et finira par se déconnecter

1.10 Quelque logiciel malveillant [7]

- **Virus**

Un virus est un fragment de code qui se propage à l'aide d'autres programmes.

- **Vers**

Un ver est un programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellement besoin d'un support physique ou logique pour se propager.

- **Trojans**

Le trojan est un logiciel de très petite taille qui est dissimulé au sein d'un autre programme (c'est l'hôte) que vous utilisez. En lançant ce dernier, vous activez par la même occasion, le trojan

caché qui ouvre alors une ou plusieurs portes virtuelles (ports) sur votre machine. Le trojan devient autonome, même si vous quittez le programme qui lui a permis de s'activer.

- **Backdoor**

Un programme backdoor (littéralement porte arrière mais traduit par porte dérobée) est un petit bout de code introduit en général par un pirate informatique pour pouvoir ouvrir un accès dérobé sur un système informatique et ainsi prendre le contrôle de celui-ci quand il le désire.

1.11. Quelque mécanisme de défense

- **Le VPN [6]**

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

- **Un pare-feu [6]**

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

- **IPS/IDS**

Un IPS (Système de Prévention d'Intrusion) et un IDS (Système de Détection d'Intrusion) sont des outils de sécurité réseau qui surveillent le trafic en temps réel à la recherche de comportements suspects ou de signatures connues d'attaques.

IDS : Il détecte les intrusions en analysant le trafic réseau et génère des alertes en cas d'activité suspecte, mais n'intervient pas pour arrêter l'attaque.

IPS : Il agit de manière proactive en plus de détecter les intrusions. Il peut bloquer ou arrêter automatiquement le trafic réseau jugé malveillant.

I.12. Conclusion

Dans ce chapitre, nous avons exploré les concepts fondamentaux des réseaux et de la sécurité informatique. Le prochain chapitre sera consacré à la présentation des systèmes d'authentification

CHAPITRE II
Les systèmes d'authentification

II.1. Introduction

Dans ce chapitre, nous explorerons l'état de l'art des systèmes d'authentification, un aspect crucial de la sécurité informatique. Nous passerons en revue différentes techniques, telles que les mots de passe, la biométrie et la cryptographie, ainsi que les protocoles couramment utilisés, tels que PAP, CHAP, et RADIUS. L'objectif est de fournir un aperçu des options disponibles pour sécuriser l'accès aux systèmes et aux réseaux, en mettant en lumière leurs avantages et leurs limitations respectifs.

II.2 Définition de système d'authentification

Le système d'authentification est un ensemble de méthodes et de processus utilisés pour vérifier l'identité d'un utilisateur ou d'un système informatique. Cela garantit que seules les personnes autorisées peuvent accéder aux ressources ou services d'information.

II.2.1 Les techniques d'authentification faibles

Les techniques d'authentifications faibles, sont souvent basées sur des méthodes d'identification qui offrent un niveau de sécurité bas ; telles que les mots de passe simples, les questions de sécurité triviales. Ces techniques sont vulnérables aux attaques et peuvent être compromises facilement par des attaquants expérimentés, mettant ainsi en danger la sécurité des systèmes et des données.

II.2.2 Les techniques d'authentification fortes

Les techniques d'authentification forte exigent deux types de preuves différents pour confirmer l'identité d'un utilisateur, ce qui augmente le niveau de sécurité.

II.3 La cryptographie

La cryptographie est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données. La cryptographie vous permet de stocker des informations sensibles ou de les transmettre à travers des réseaux non surs (comme internet) de telle sorte qu'elles ne puissent être lues par personne a l'exception du destinataire convenu **[12]**.

II.3.1 Cryptages symétriques

La cryptographie symétrique (ou le cryptage des clés symétrique) est une classe d'algorithme de cryptographie qui utilisent les mêmes clés cryptographiques pour le cryptage du texte claire et le décryptage de texte chiffré.

Voir la Figure II.1 **[12]**.

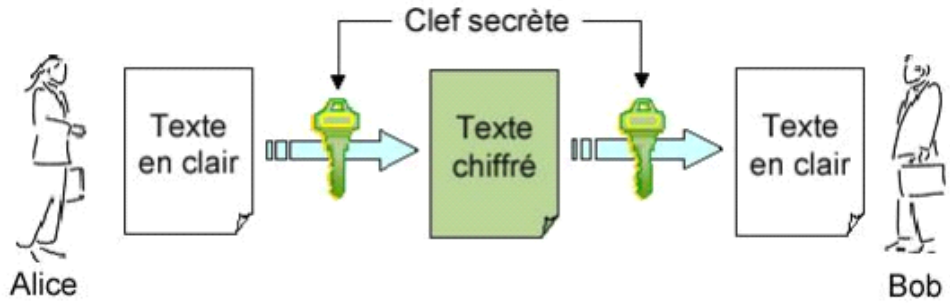

Figure II.1 : Modèle opérationnel de la cryptographie symétrique.

II.3.2 Cryptages asymétriques

La cryptographie a clé publique (PKC), également appelée cryptographie asymétrique, se réfère à un algorithme cryptographique qui nécessite deux clés distinctes m dont l'une est secret (ou privées) et l'autre public. bien que différentes, les deux parties de cette paire de ces sont liées mathématiquement. Voir la figure II.2 **[12]**.

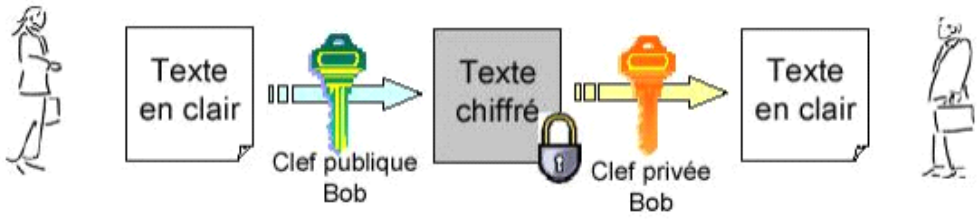

Figure II.2 : Modèle opérationnel de la cryptographie asymétrique (PKC)

II.3.3 Le cryptage a clé mixte

Le cryptage à clé mixte utilise à la fois le cryptage symétrique et asymétrique pour sécuriser les données. Les données sont d'abord cryptées avec une clé symétrique, puis cette clé est elle-même cryptée avec la clé publique du destinataire.

II.4. Les certificats numériques

Un certificat numérique fournit un moyen de prouver l'identité de quelqu'un dans les transactions electronique.la fonction de celui-ci pourrait être considère comme un passeport. Ou un permis de conduire dans les interactions en face à face **[12]**.

II.5. L'authentification par mot de passe à usage unique

L'authentification par mot de passe à usage unique génère des mots de passe uniques pour chaque connexion, renforçant ainsi la sécurité en ligne. Ces mots de passe sont temporaires et générés dynamiquement.

II.6. La biométrie

La biométrie est un système d'identification basé sur des caractéristiques distinctives du corps ou du comportement, comme les empreintes digitales ou la voix, utilisé pour sécuriser l'accès aux systèmes informatiques ou aux lieux.

II.7. Les Protocoles d'authentification

Les protocoles d'authentification sont des règles et des procédures utilisées pour vérifier l'identité d'un utilisateur ou d'un système avant de lui accorder l'accès à des ressources. Ils garantissent que seules les entités autorisées peuvent interagir avec un réseau ou un service. On peut citer :

- **PAP :** PAP est un protocole réseau bidirectionnel ayant lieu en deux étapes et qui n'utilise pas le chiffrement : les noms d'utilisateur et mot de passe sont envoyés en clair dans le réseau informatique. S'ils ont accepté, la connexion est autorisée. L'authentification a lieu une seule fois **[3]**.
- **CHAP :** Le protocole CHAP utilise un mécanisme de défi-réponse pour authentifier les utilisateurs. Lorsqu'une connexion est établie, le serveur envoie un défi à l'utilisateur, qui doit alors générer une réponse en utilisant un mot de passe. Le serveur vérifie ensuite cette réponse pour confirmer que le mot de passe est correct. Étant donné que le mot de passe n'est jamais envoyé en texte clair sur le réseau.
- **MS-CHAP :** MS-CHAP est un protocole d'authentification développé par Microsoft. Il utilise un mécanisme de défi-réponse similaire à CHAP pour authentifier les utilisateurs, mais il est spécifiquement conçu pour les environnements Microsoft.

II.8. Le Protocole 802.1x

Le protocole 802.1X est un protocole d'authentification au niveau Ethernet mis au point par l'IEEE (Institute of Electrical and Electronics Engineers) [4]. Il implémente l'authentification basée sur les ports. Un port d'un commutateur réglé en mode 802.1X peut se trouver dans deux états distincts :

- État "contrôlé" : Ce statut indique que l'authentification auprès du serveur RADIUS a réussi. Dans cet état, le port est ouvert à toute communication.
- État "non contrôlé" : Ce statut indique que l'authentification a échoué. Dans cet état, le port est fermé à toute communication **[3]**.

La réussite ou l'échec de l'authentification détermine donc l'ouverture ou la fermeture du port.

De plus, le protocole EAP (Extensible Authentication Protocol) est une norme de l'IETF (Internet Engineering Task Force) qui définit une infrastructure permettant aux clients d'accès réseau et aux serveurs d'authentification de communiquer.

Microsoft Windows utilise EAP pour authentifier l'accès réseau dans le cadre des connexions PPP (Point-to-Point Protocol), notamment pour l'accès distant, le réseau privé virtuel, ainsi que pour l'accès réseau basé sur IEEE 802.1X aux commutateurs Ethernet et aux points d'accès sans fil [3

II.9. PEAP

PEAP (Protected Extensible Authentication Protocol) est un protocole de sécurité utilisé pour l'authentification des utilisateurs dans les réseaux informatiques. Dans PEAP, seul le serveur dispose d'un certificat numérique. Lorsqu'un utilisateur se connecte, le serveur lui envoie ce certificat pour vérification. Ensuite, un tunnel sécurisé est créé entre le serveur et l'utilisateur pour protéger les échanges d'informations. L'utilisateur peut alors s'authentifier en utilisant une méthode quelconque, comme un nom d'utilisateur et un mot de passe, tout en bénéficiant de la sécurité du tunnel.

II.10. Protocoles d'authentification utilisant un serveur d'application

II.10.1. Kerberos

Kerberos est un protocole d'authentification développé par le MIT (Massachusetts Institue of Technology). Il a été conçu afin de fournir une authentification unifiée pour les applications de type client/serveur sur des réseaux qualifies de non surs à l'aide de chiffrement symétrique. L'authentification repose sur une tierce partie de confiance nommée Key Distribution Center (KDC) pour l'attribution de tickets permettant l'accès aux différents services du réseau **[1]**. Son fonctionnement est présente sur la Figure II.3 .

Kerberos utilise la notion de (ticket) pour éviter à un utilisateur de devoir s'authentifier constamment aux différents serveurs auxquels il se connecte. L'utilisateur s'authentifie sur le KDC puis utilise un ticket pour s'authentifier sur chaque service demande **[2]**. Le protocole Kerberos sépare le rôle du KDC en deux services.

- AS (Authentification Service) : il s'agit du service sur lequel l'utilisateur s'authentifie. Il délivre un ticket en cas d'authentification réussie. Ce ticket est en fait une demande d'accès au TGS.
- TGS (Ticket Granting Service) : ce service fourni les tickets d'accès aux différents services du réseau. On les appelle TS (Ticket Service) **[3]**.

II.10.2. Les étapes de fonctionnement de l'authentification dans Kerberos

1. Le client envoie au serveur d'authentification le message 1< KRB AS REQ> : ou il précise son nom et demande un ticket qui va le présenter ensuite au TGS afin de contacter le destinataire.
2. Le serveur d'authentification lui répond avec le message 2 <KRB AS REP > : le serveur d'authentification cherche le client dans sa base de données. S'il le trouve, il engendre une clé de session qui devra être utilisée entre le client et le TGS. Cette clé est chiffrée avec la clé secrète du client : c'est la première partie du message. Ensuite, il crée un ticket pour le client afin qu'il puisse s'authentifier auprès du TGS, ce ticket est chiffre avec la clé secrète du TGS. Le client ne pourra pas le déchiffrer mais pourra le présenter tel quel est à chaque requête au TGS. Dans ce cas particulier, le ticket est appelé TGT.
3. Ensuite, avec le message 3 <KRB TGS REQ> le client s'authentifie auprès de TGS et demande le ticket de service qu'il souhaite avoir accès. Pour cela, le client fourni au TGS d'une part le nom du serveur qu'il souhaite contacter, d'autre part le ticket TGT et un identificateur qui possède des informations crypte avec la clé de session cet identificateur est vérifiable à partir du ticket par le TGS.
4. Grace a sa clé secrète, le TGS déchiffré le ticket, et récupère la clé de session et peut ainsi déchiffrer l'identificateur. Il compare le contenu de l'identificateur avec les informations contenues dans le ticket et si tout concorde (le client est authentifiée), il peut engendrer une clé de session (qui sera utilisée entre le client et le service souhaite à avoir accès) qu'il chiffre avec la clé de session et un nouveau ticket que le client devra présenter au service. Ces deux derniers seront la réponse de TGS au client contenant dans le message 4< KRB TGS REP>. Apres réception de ce message et déchiffrement, le client dispose donc en plus de la clé de session et de TGT (qu'il conserve jusqu'à expiration du ticket pour dialoguer avec TGS) déjà obtenue par le AS, d'une nouvelle ce de session et d'un nouveau ticket qu'il pourra utiliser avec service à accéder.
5. Le message 5 <KRB AP REQ >correspond à la demande de service souhaite par le client, il s'authentifier auprès de ce service de la même manière qu'avec le TGS (message 3(KRB TGS REQ)).
6. Et le message 6<KRB AP REP> correspond à la réponse à la demande. De son cote, le service accède s'authentifie en prouvant qu'il a pu déchiffrer le ticket reçu par le client et donc, il possède la clé de session. Pour cela, il faut qu'il renvoie une information vérifiable par le client et chiffrée avec cette clé **[14]** voir la figure 2.3

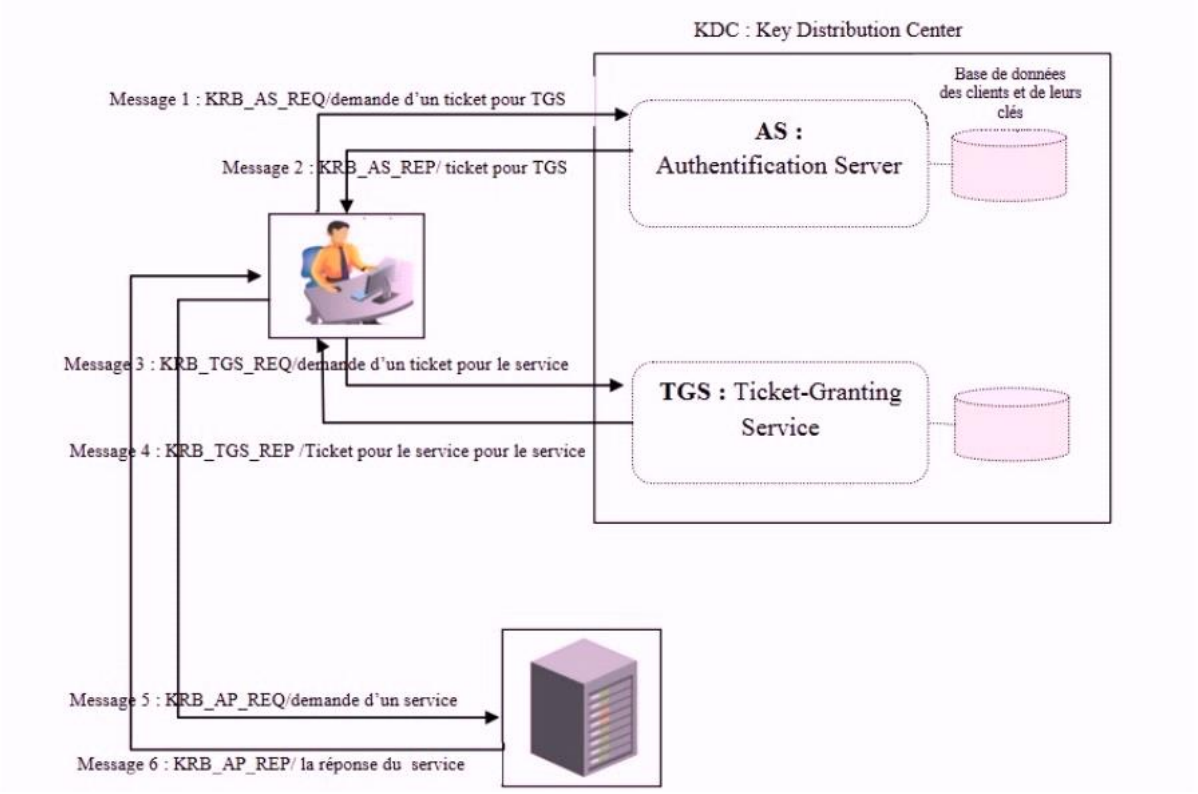

Figure II.3– L'authentification dans Kerberos **[14]**.

II.10.3. Les points faibles de Kerberos

Kerberos est un protocole conçu pour être sur même lorsqu'il est exécuté sur un réseau peu sur.

- Kerberos garantit l'intégrité des données, leur confidentialité, la non répudiation et l'authentification mutuelle des clients services.
- Les transmissions sont chiffrées avec une clé secrète appropriée, l'attaquant ne peut pas avoir un ticket valide pour gagner l'accès non autorisé à un service sans compromettre une clé de cryptage.
- Diminue le nombre de bugs d'implémentation **[13]**.

II.10.4. Les points faibles de Kerberos

Il n'y a pas de système parfait et il s'agit d'être bien conscient des limitations de ce système. Les grandes lignes des faiblesses du système Kerberos sont :

- Kerberos chiffre uniquement la phase d'authentification, il ne chiffre pas les données qui seront transmises lors de la session.
- Tous les services du réseau doivent être < Kerberisé >, c'est-à-dire compatible avec le protocole Kerberos. Les services doivent être capables de comprendre le système de ticket, sinon aucune authentification ne sera possible.

- Si l'AS de Kerberos est compromis, un attaquant pourra accéder a tous les services avec un unique login **[13]**.

II.11. Le protocole AAA

II.11.1. Définition de AAA

Le terme "AAA" est Utilisé pour décrire un ensemble de processus d'authentification, d'autorisation et de comptabilité qui aident à contrôler l'accès des utilisateurs au réseau et aux ressources informatiques. "AAA" signifier :

- **Authentification (Authentication) :** L'authentification est un processus de vérification de l'identité d'un utilisateur est généralement réalisé en utilisant des données d'identification telles que Nom/Mot de passe, des informations biométriques, etc.
- **Autorisation (Authorization) :** L'autorisation est le processus de contrôle et de gestion des droits d'accès et des privilèges d'un utilisateur une fois que l'authentification a été effectuée avec succès.
- **Comptabilité (Accounting) :** la comptabilité consiste à enregistrer l'utilisation des ressources par les utilisateurs.

Parmi les protocoles AAA connus nous citons :

II.11.1.1. Le protocole RADIUS (Remote Authentication Dial-In User Service)

Le protocole Radius est un protocole client -serveur qui repose principalement sur :

- Un 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 est chiffré et authentifié grâce à un secret partagé.

II.11.1.1.1. Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci

1. Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;
2. Le NAS achemine la demande au serveur RADIUS.
3. 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 »

• **GHANGE PASSWORD** : le serveur RADIUS demande à

L'utilisateur un nouveau mot de passe **[7]**.

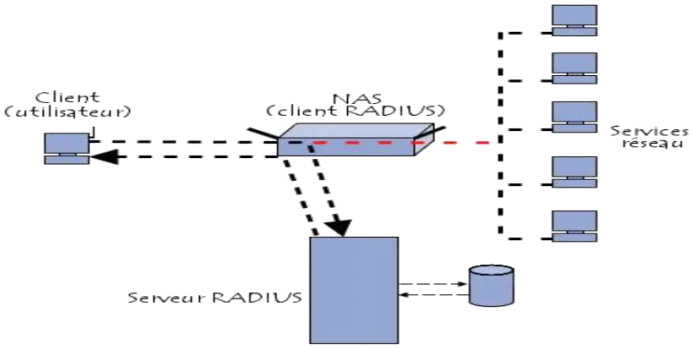

Figure II.4: Fonctionnement RADIUS

II.11.1.2. Le protocole DIAMETER [15]

DIAMETER est un protocole permettant à des domaines administratifs différents de collaborer pour réaliser les fonctionnalités AAA. Il est constitué d'un protocole de base qui définit le format des messages, comment ils sont transportés, les messages d'erreurs ainsi que les services de sécurité que toutes les implémentations doivent supporter. À ce protocole de base s'ajoutent les applications : Mobile IP, NAS et CMS.

- L'application Diameter Mobile IPv4 : permet d'appliquer le triple-A avec un utilisateur Mobile sur le protocole IPv4.
- L'application Diameter NAS : permet l'accès au réseau via PPP/EAP, il s'agit de l'amélioration de RADIUS.
- L'application Diameter CMS : permet de protéger les échanges Diameter au niveau applicatif entre serveurs ou entre un serveur et son client.

Diameter a été conçu dans l'idée d'être facilement extensible.

II.11.1.3. Le protocole TACACS [15]

TACACS (Terminal Access Controller Access-Control System) est un protocole d'authentification distant utilisé pour communiquer avec un serveur d'authentification, généralement utilisé dans des réseaux UNIX. TACACS permet à un serveur d'accès distant de communiquer avec un serveur d'authentification dont l'objectif est de déterminer si l'utilisateur a le droit d'accéder au réseau. Sa définition complète est faite dans la RFC 1492.

II.11.1.4 Le protocole TACACS+

TACACS+ (Terminal Access Controller Access-Control SystemPlus) est la dernière version du protocole TACACS. Développé à l'origine par BBN puis repris par Cisco, il a été étendu une première fois avec XTACACS (eXtended TACACS).

TACACS+ utilise le protocole TCP et le port 49 pour son transport, contrairement à TACACS qui s'appuie sur UDP. Il gère séparément les trois fonctions AAA (Authentication, Authorization, Accounting) :

- **Authentification :** TACACS+ hérite des méthodes d'authentification du protocole PPP, c'est-à-dire PAP, CHAP et EAP, incluant pour la dernière méthode la possibilité d'utiliser des cartes, ou tokens. Les échanges d'authentification sont élémentaires. Ils s'appuient sur des demandes d'authentification de la part du client et des réponses d'authentification de la part du serveur. Une base de données située sur le serveur d'accès distant sur lequel s'exécute le serveur TACACS+ gère l'ensemble des utilisateurs.
- **Autorisation :** Les échanges d'autorisation sont également élémentaires, Ils s'appuient sur des demandes d'autorisation de la part du client AAA et des réponses de la part du serveur TACACS+. Un profil d'autorisation sur des ressources réseau contient à la fois la liste des équipements autorisés à l'accès et les commandes autorisées à exécuter pour les configurations (Degré de privilèges). Il s'agit d'une option très importante pour attribuer des droits de lecture sans possibilité de modification. Les profils sont stockés sur le système hébergeant le serveur TACACS+.
- **Journalisation des événements :** Le serveur TACACS+ enregistre Les informations concernant les demandes d'authentification afin d'ouvrir une session, les fermetures de session ainsi que les actions exécutées durant une session donnée. Si plusieurs serveurs TACACS+ sont déployés, une consolidation des journaux d'activité doit être réalisée afin de corréler les événements entre eux. Les transactions entre un client TACACS+ et un serveur TACACS+ sont authentifiées par le biais d'un secret partagé, qui n'est jamais transmis sur le réseau. Les données échangées lors de ces transactions sont chiffrées à l'aide d'une fonction XOR appliquée sur les données et une empreinte calculée à l'aide du secret partagé. Ces protections ne s'appliquent pas entre le client d'accès distant et le point d'accès réseau si c'est ce dernier qui exécute le client TACACS+.

II.12.2 Comparaison entre le protocole RADIUS et TACACS+

	TACACS+	RADIUS
Protocole de transmission	Protocole de couche transport orienté connexion TCP, transmission de données en full-duplex fiable.	Utilise le protocole UDP orienté non-connexion, échange de datagramme sans accusés de réception ou de livraison garanti.
Ports utilisés	49	Authentification et autorisation: ports 1645 et 1812 Accounting: 1646 et 1813.
Chiffrement	Cryptagedu paquet entier.	Chiffre seulement les mots de passe jusqu'à 16 octets.
AAA Architecture	La commande séparée de chaque service: l'authentification, l'autorisation et la comptabilité.	Authentification et autorisation combinées en un seul service.
Rôles principal	la gestion des périphériques.	contrôle d'accès des utilisateurs.

Tableau II.1 : Comparaison entre le protocole RADIUS et TACACS+

II.13 Conclusion

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

CHAPITRE III
Présentation de l'organisme d'accueil

III.1 Introduction

Ce chapitre est consacré à la présentation du campus NTS (New Technology § Solutions) organisme d'accueil pour notre stage. Dans un premier temps, nous abordons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Dans un second temps, nous procéderons à une analyse approfondie de l'architecture réseau de l'entreprise COLLABLE qui fera l'objet de notre cas d'étude, en examinant minutieusement chacune de ses structures réseaux. Cette démarche rigoureuse nous permettra de formuler des propositions d'optimisation concrètes et pertinentes, c'est pourquoi elle constitue une étape essentielle de notre travail.

III.2 Présentation de l'entreprise « Campus NTS »

III.2.1 Création et évolution

NTS est une jeune entreprise axée sur la recherche, la conception et la mise en œuvre de solutions, d'intégration de systèmes de sécurité, d'importation et de la distribution d'équipements et de matériels de sécurité des réseaux et des télécommunications, de la formation et le conseil. Elle a été créée en 2020 à Bejaia par Yassine DJEBBARI, qui a de nombreuses d'années d'expérience et a réalisé d'importants projets dans différents secteurs et régions du pays, comme référence :

- Air Algérie.
- Retelem Alger.
- Poste d'Algérie.
- Adèle.
- RATP ALJAZAIR.
- Géant de l'électronique BBR.
- Morsi.
- Université de Bejaïa.
- Cité universitaire à Bejaïa (targa ouzamour, 17 octobre...etc).
- SARL Alphas Bejaïa.
- Providentia Béjaïa.

III.2.2 Localisation de l'entreprise

Voir la figure 3.1.

Adresse : Bâtiment A les beaux quartiers, Résidence Universitaire Targa Ouzemour, Béjaïa 06000

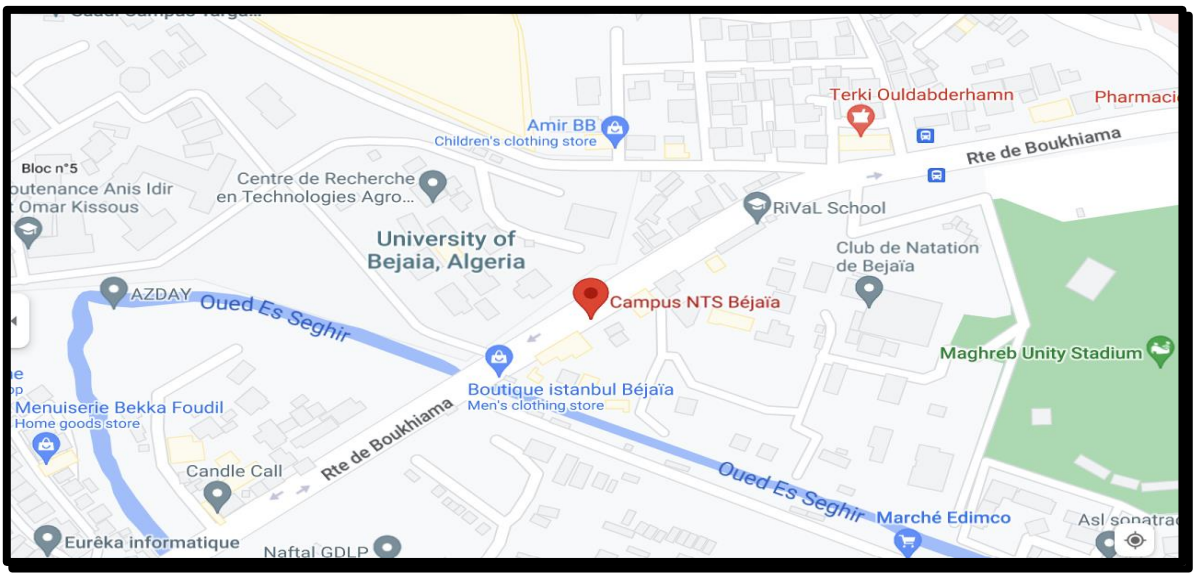

Figure3.1 : Localisation de l'entreprise NTS.

III.2.3 Fiche technique

Le tableau 1 ci-dessous représente quelques informations relatives à l'entreprise dans laquelle nous avons effectué notre stage de projet de fin d'étude.

Dénomination	**Campus NTS**
Logo	
Siège	Bâtiment A les beaux quartiers Targa Ouzemour, Béjaïa 06000
Secteurs d'activités	Informatique et télécommunication
Numéros de FAX	044 204 400
Numéros de Téléphone	0770446101
Email	contact@campus-nts.com
Site Internet	http://www.campus-nts.com/

Tableau III.1 *:* Identification sur campus NTS

III.3 Objectifs, Missions et activités de l'Entreprise « N.T.S »

Les objectifs, les missions et les activités sont représentées dans la figure 3.2 :

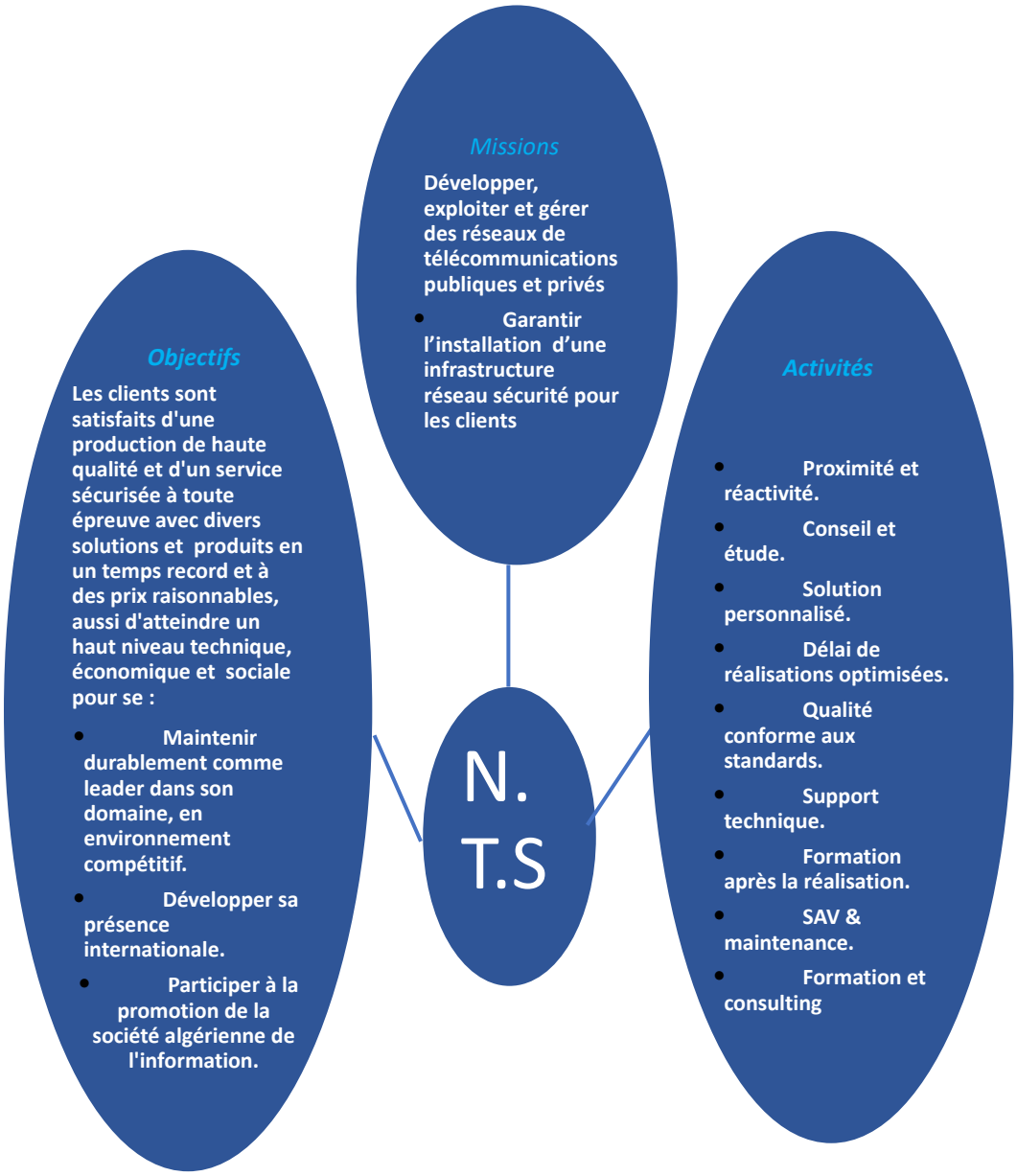

Figure III.2 : Objectifs, Missions et Activités de l'NTS

III.4 Organigramme général de l'organisme d'accueil

voir la figure 3.3

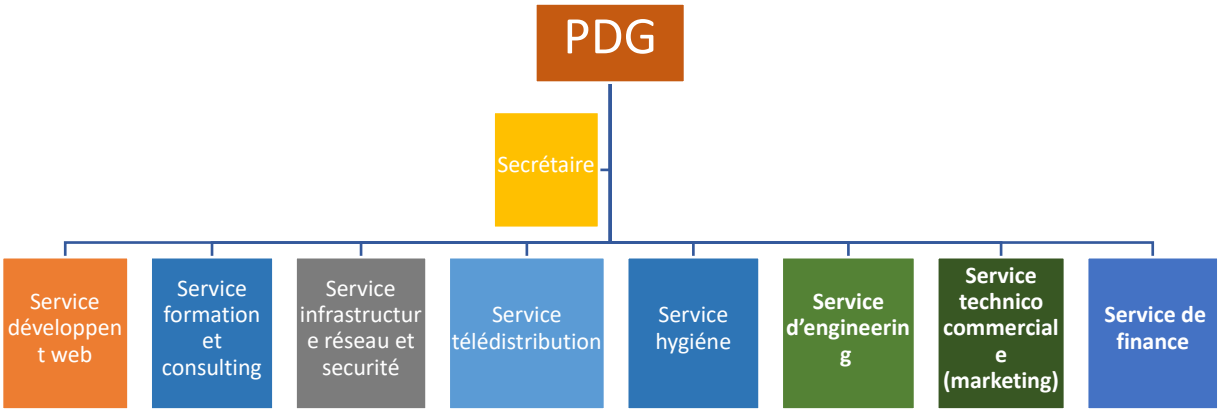

Figure III.3 : L'organigramme de campus NTS.

Dans la suite, nous mettons l'accent sur le service concerné par notre stage qui est le service Infrastructure réseau et sécurité

A. Service développement web

Il est responsable de la création des sites web, des applications pour internet, applications mobiles ou des solutions logicielles adaptées aux besoins des clients utilisant des langages de programmation informatique tels que : HTML5, CSS, JavaScript ou PHP. En général, il représente les tâches liées au développement du site Web en améliorant son positionnement sur les moteurs de recherche qui seront hébergés sur Internet.

B. Service formation et consulting

Ce secteur a été créé par le campus NTS pour offrir des stages et des formations professionnelles dans les domaines suivants :

- Installation et configuration des réseaux informatiques.
- Administration et sécurité des réseaux et système.
- Installation et configuration des firewalls (pfsense, Sophos, fortigate, palo alto…).
- Installation et configuration des réseaux sans fil professionnel.
- Installation et configuration des caméras de surveillance analogique et numérique.
- Fibre optique les réseaux d'accès FTTH/FTTX.
- Création des sites web.
- Programmation (C, C++, C#, Java, Python…etc.).
- Electricités Bâtiments et industriels.
- Formation Cisco CCNA, CCNP S&R.
- Virtualisation.

- Microsoft server, SQL.
- Cyber sécurité.

Ces stages s'adressent aux étudiants, ouvriers, entreprises en fin de projet et à tous ceux qui apprécient le terrain pour développer leurs compétences en sécurité, acquérir des qualifications supérieures et leur expérience en entreprise. NTS repose sur la capacité des ressources et des structures à délivrer à ses clients et à ses partenaires (Alhua, Hikvision, Cisco, Legend, Mikrotik, Zkteco, Commax, D-link, Alcatel-Lucent, Synology, Microsoft, Apollo, Panasonic, Huawei).

C. Service infrastructure réseau et sécurité

Notre stage a été effectué au niveau du service infrastructure réseau et sécurité.

- **Présentation de service infrastructure réseau et sécurité**

L'infrastructure réseau est au cœur des opérations commerciales dans la plupart des industries. Il peut être considéré comme le centre sensible de toute l'organisation informatique car il centralise les données, simplifie les échanges de données et facilite la communication entre les employés. A ce titre, il est un outil important pour le fonctionnement normal de l'entreprise et nécessite une attention constante en matière de sécurité. Ceci afin d'empêcher le nombre croissant et l'affectation des attaques externes et internes.voir la figure 3.4

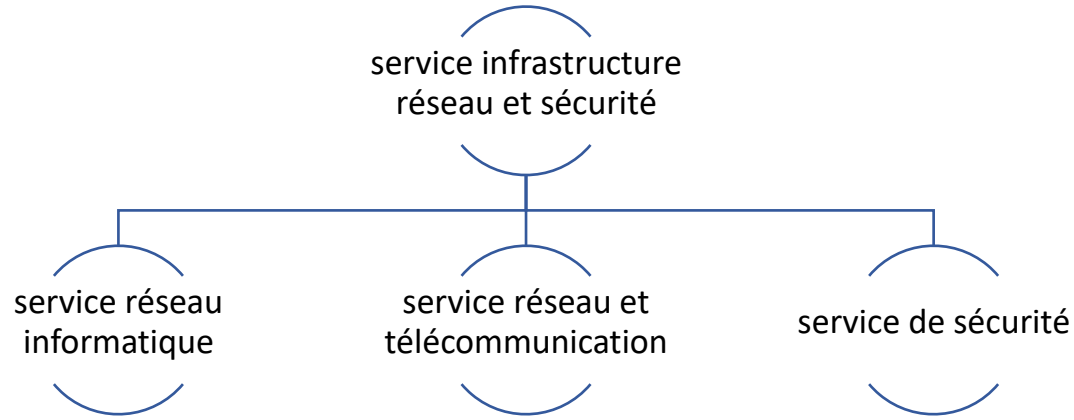

Figure III.4 : organigramme de service d'accueil

➢ **Service réseau informatique :**

Ce service représente tous les appareils et périphériques au sein d'une entreprise qui sont physiquement ou virtuellement connectés les uns aux autres à partir d'un wifi professionnel ou d'autre méthodes afin de partager des ressources ou des informations. En fait, l'infrastructure

réseau offre un large éventail de fonctionnalités pour les clients de services et les producteurs de services, telles que :

Limitation de débit, analyse, vérification, surveillance et enregistrement et sécurisation du réseau de cette entreprise.

- **Service réseau et Télécommunication**

Les services de télécommunications sont conçus pour transmettre des informations en un temps réel (synchronisation des informations) sous forme analogique ou numérique à l'exception de la radio et de la télévision. La plupart de ces services peuvent aider les clients à identifier leurs besoins en matière d'infrastructure de télécommunications. Voici des exemples de services d'infrastructure de télécommunications :

- Pose de fibre optique.
- Emplacement du site de la tour cellulaire.
- Test d'antenne radio.
- Installation d'équipements téléphoniques standards et réseau de données.
- Téléphonie standard

- **Service de sécurité**

Cette entreprise NTS accomplit à la fois le gardiennage et l'installation des systèmes de sécurité électroniques. Aussi elle fournit aux clients des solutions complètes et fiables pour protéger leurs ressources.

Les services qu'elle réalise sont les suivants :

- Caméras de surveillance
- Alarme anti- intrusion
- Détection incendie
- Pointeuse et Contrôles d'accès
- Vidéophonie

D. Service télédistribution

Ce service est spécialisé dans la transmission de données par câble (fibre optique, paire torsadée et onde horizontale) ou autres systèmes de distribution (paraboles collectif, télévision numériques terrestre et audiovisuelle). Son objectif principal est de garantir l'installation de ces supports de transmission à haut débit. Enfin, les services de télédistribution ont été appelés à jouer un rôle majeur dans l'émergence des nouveaux médias tel que :

- Rediffusion de programmation par satellite.
- Transmission de chaînes de télévision par abonnement.

- Services interactifs.
- Programmation locale.

E. Service d'engineering

Il est constitué d'une équipe multidisciplinaire d'experts dont la mission est de rechercher et d'analyser les besoins des clients pour trouver la meilleure solution spécifique à leur projet.

L'équipe de campus NTS n'hésite pas à se circuler sur le terrain pour consulter l'état d'avancement du projet afin de faire face à d'éventuelles difficultés qui auraient pu survenir auparavant. Cette équipe est composée :

- D'ingénieurs en télécommunications.
- D'informaticiens en gestion et sécurité des réseaux.
- D'administrateurs de systèmes d'information.
- D'informaticiens en programmation.
- De techniciens fibre.
- De techniciens supérieurs en informatique.

Leurs propositions sont en recherche informatique et sécurité et leurs cotations est dans la recherche sur les réseaux et les systèmes de télécommunication.

F. Service technico commerciale (marketing)

Leurs offres ne se limitent pas à de simples fournitures standards. Ils disposent d'une équipe qui s'assure de répondre aux besoins et au confort de ses précieux clients dans le but de développer les services de cette entreprise. Par ailleurs, ce service commercialise aussi les services proposés par campus NTS.

G. Service de financière

Le service financier situé au cœur de l'entreprise, représente l'ensemble des personnes chargées de la fonction comptable. Il intervient pour faire de bons investissements en prévenant d'éventuels risques de perte. Ce service contient un ensemble de tâches et rôles au sein de la société NTS :

➢ Les tâches principales du Service des finances :

- Assurer une saine gestion des ressources financières de l'entreprise par la planification.
- La coordination et le contrôle de toutes les politiques et procédures requises pour la protection des actifs.
- La production des informations financières exactes et pertinentes afin que le gestionnaire puisse prendre la décision éclairée.

- Le rôle du service financier :
  - La préparation et du suivi des budgets de fonctionnement et d'investissement.
  - La préparation des états financiers.
  - La gestion de la trésorerie et de des encaissements.
  - La rémunération des employés, des comptes à payer.
  - De l'acquisition des biens et services pour l'ensemble de l'entreprise, des projets de recherche.
  - La réception des marchandises et du courrier.

H. Service hygiène

La sécurité et la santé occupent une place prépondérante dans les conditions de travail. L'employeur est en effet responsable de la santé et de la sécurité de ses salariés. Il coordonne ses différentes équipes et attribue les moyens nécessaires tel que :

- Des actions de prévention des risques professionnels et de la pénibilité au travail.
- La mise en place d'une organisation et de moyens adaptés.

III.5 Cas d'étude : Client Collable

III.5.1 Présentation du réseau collable

L'entreprise a une architecture en couches et, pour assurer la communication entre ses différents services, elle connecte ces vlans à une connexion L.S (Ligne Spécialisée publique symétrique) en fibre optique fournie par Algérie télécom, Le schéma ci-dessous nous montre l'infrastructure du réseau Collable :

A. Présentation de l'architecture réseau existant dans l'entreprise

Collable construit un réseau en choisissant une topologie arborescente pour connecter ses différents appareils, comme illustré dans la figure suivante : voir figure 3.5

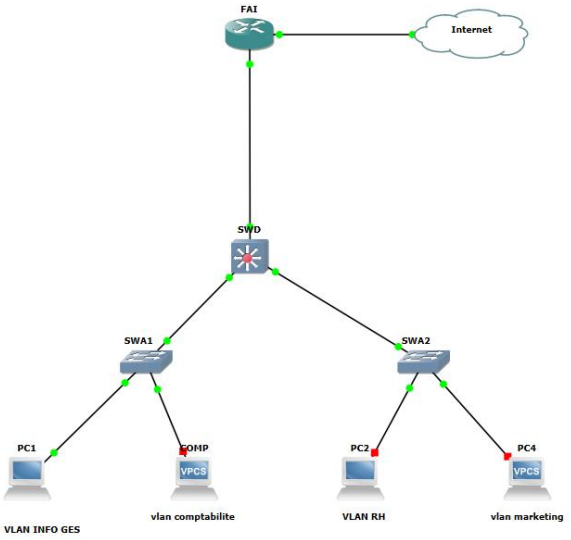

Figure III.5 : Architecture de réseau Collable

B. Analyse du parc informatique

➢ **Présentation d'environnement hard et soft :**

Nom de l'équipement	**Le hardware (hard)**	**Software (soft)**
Routeur	ISR 4331	IOS (International Organisation For Standardisation)
Pare-feu	PfSense	FREEBSD
Switch	• HPE 1820-24G Managed L2 • HPE 1920-24G Managed L3	LINUX
Server	ESHP ProLiant DL380P génération 10	• ESXI • GOAUTODIAL • SERVER WINDOWS 2022
PC portable	Dell IAER 35 R	Windows 10

Tableau III.2 : L'environnement hardware et le software

➢ **Les caractéristiques des équipements par niveaux**

Nom de l'équipement	**Modèle**	**Caractéristique**
Router	ISR 4331	• **RAM:** 4 G0 (installé) /16 GO (maximum) • **Mémoire Flash :**4000 MO • **Débit :**100 Mb/s • **Protocole de liaison de données :** Ethernet, fast Ethernet et gigabit-ethernet
Pare-feu	PFSENSE	• **Débit :** 4000 Mbit/s • **Débit IPS :** 2700Mbit/s • **Débit VPN IP sec :** 560 Mbit/s • **@ IP/Numéro de port**
Switch	**HPE 1920**	• **Ports :** 24 ports • **Mémoire Flash :** 16MO • **Mémoire RAM :** 128MO • **Capacité de commutation :** 32 Gbit/s
Switch	**HPE 1820**	• **Ports :** 24 ports • **Mémoire Flash :** 128MO • **Mémoire RAM :** 512MO • **Capacité de commutation :** 56 Gbit/s
server	HP ProLiant DL380P génération 10	• Processor Intel Xeon • Silver 4110 (Octo-Core 2.1 GHZ / 3.0 GHZ Turbo-16 Threads-cache 11Mo) • 16 G0 DDR4 RDIMM (1x 16 GO -12 slots)
PC portable	Dell IAER 35 R	• **AMD core :** i5 8th génération • **RAM :** 8GO • **Disque :** 256GO • **Ecran :** UHD Graphies 620 ($1920 \times 1080 \times 32b$)

Tableau III.3 : Détails des ressources disponibles de l'entreprise

III.6 Problématiques

Les réseaux informatiques, en facilitant la communication entre divers appareils, contribuent à enrichir l'environnement numérique. Cependant, ils exposent également les systèmes à des risques majeurs, notamment les accès non autorisés, qui représentent l'un des principaux dangers. À l'ère numérique, les mots de passe sont souvent la première ligne de défense contre les cyberattaques. Cependant, le piratage de mots de passe demeure l'un des moyens les plus simples pour les cybercriminels d'accéder à des informations sensibles

III.7 Solutions

Pour renforcer la sécurité des réseaux contre les risques liés aux mots de passe, une stratégie efficace consiste à utiliser des certificats pour l'authentification. Les certificats numériques permettent d'établir une authentification mutuelle sécurisée entre les serveurs et les clients. Dans ce processus, non seulement le serveur vérifie l'identité du client, mais aussi le client peut vérifier l'identité du serveur.

En utilisant des certificats pour l'authentification, les réseaux peuvent bénéficier d'un niveau de sécurité plus élevé et réduire les risques de violation de sécurité. Cela garantit également que seuls les utilisateurs et les serveurs légitimes peuvent accéder aux ressources du réseau, renforçant ainsi la protection des données sensibles et la confidentialité des communications.

III.8 Conclusion

Dans ce chapitre, nous avons donné un aperçu de l'infrastructure de client collable du fournisseur de solution IT campus NTS, puis nous avons découvert un problème qui nous a amenés à rechercher et à mettre en œuvre une nouvelle architecture de réseau sécurisée. Enfin, l'application de la solution proposée fera l'objet du chapitre suivant.

CHAPITRE IV
Implémentation et réalisation

IV.1 Introduction

Après avoir analysé la sécurité du réseau de Collable et décrit la nécessité d'une solution robuste d'authentification, nous nous penchons dans ce chapitre sur le développement de l'authentification par certificat avec RADIUS en conformité avec la norme IEEE 802.1X. Cette approche permet de sécuriser les accès réseau en vérifiant de manière centralisée l'identité des clients et des serveurs à l'aide de certificats numériques. Tout en intégrant les principes de contrôle d'accès définis par la norme 802.1X.

Nous explorerons la génération des certificats, leur attribution aux entités dynamiques du réseau de Collable, ainsi que la configuration détaillée du serveur RADIUS pour orchestrer ce processus d'authentification. Cette méthodologie vise à renforcer la sécurité tout en simplifiant la gestion des accès, assurant ainsi une intégrité robuste de l'infrastructure réseau de Collable.

IV.2 Présentation de l'environnement de travail

Pour la réalisation de notre solution nous avons utilisé un ensemble d'outils et de solutions : GNS3, VMware Workstation pro, Wireshark

IV.2.1 GNS3

GNS3, abrégé de Graphical Network Simulator, est un logiciel open source qui permet de simuler des réseaux informatiques. Pour l'installer, commencez par télécharger le fichier exécutable. Ensuite, lancez-le et suivez les instructions d'installation jusqu'à la fin. Une fois l'installation terminée, cliquez sur le bouton "Finish". Ci-dessous, vous trouverez le logo de GNS3

Figure IV.1: GNS3

IV.2.2 VMware Workstation pro

VMware Workstation est un programme de virtualisation qui permet de créer de nouvelles machines virtuelles, de convertir un ordinateur en machine virtuelle et de déployer des configurations en grand nombre. Pour l'installer, il vous suffit de suivre les étapes d'installation jusqu'à la fin, puis de cliquer sur le bouton "Terminer". Voici l'interface graphique de VMware Workstation Pro, illustrée dans la figure IV.2

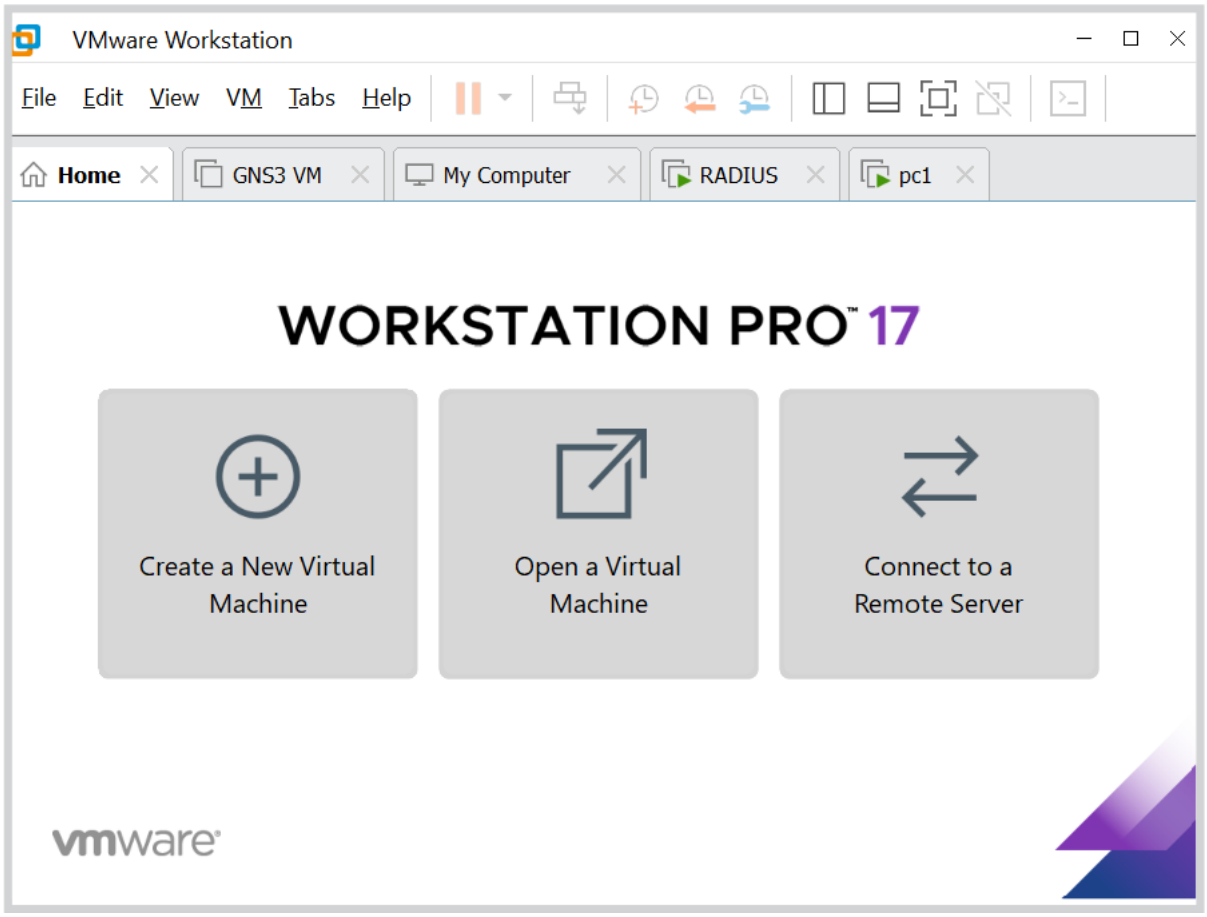

Figure IV.2: L'interface graphique de VMware Workstation pro 17

IV.2.1.3 Wireshark

Wireshark est un analyseur de protocole réseau gratuit et open source qui permet aux utilisateurs de parcourir de manière interactive le trafic de données sur un réseau informatique. La figure IV.3 présente l'interface graphique de Wireshark.

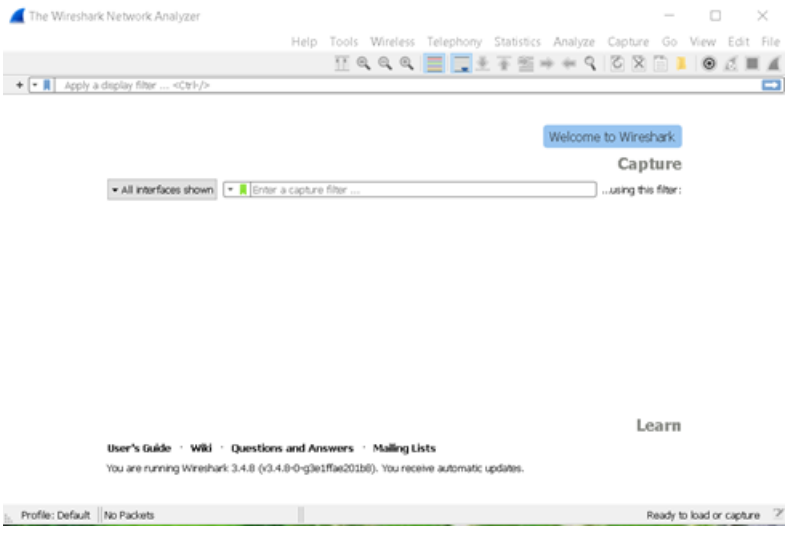

Figure IV.3 : L'interface graphique de Wireshark

IV.3 Les machines virtuelles

IV.3.1 Le pfsense

pfsense est un système d'exploitation open source construit sur FreeBSD, spécialement conçu pour fonctionner comme un routeur et un pare-feu. Il utilise le pare-feu à états Packet Filter, ainsi que des fonctionnalités de routage et de NAT pour connecter divers réseaux informatiques entre eux. pfsense offre une solution libre aux fonctionnalités présentes généralement sur les routeurs professionnels propriétaires

IV.3.2 Windows serveur 2022

Windows Server 2022 est le dernier système d'exploitation de Microsoft conçu spécifiquement pour les serveurs. Il propose des mesures de sécurité avancées sur plusieurs niveaux, des fonctionnalités hybrides intégrées avec Azure, et une plateforme d'application flexible.

IV.3.3Windows 10

Windows 10 est un système d'exploitation de la famille Windows NT développé par la société américaine Microsoft.

IV.4 Architecture proposée

L'architecture proposée est détaillée dans la figure IV.4

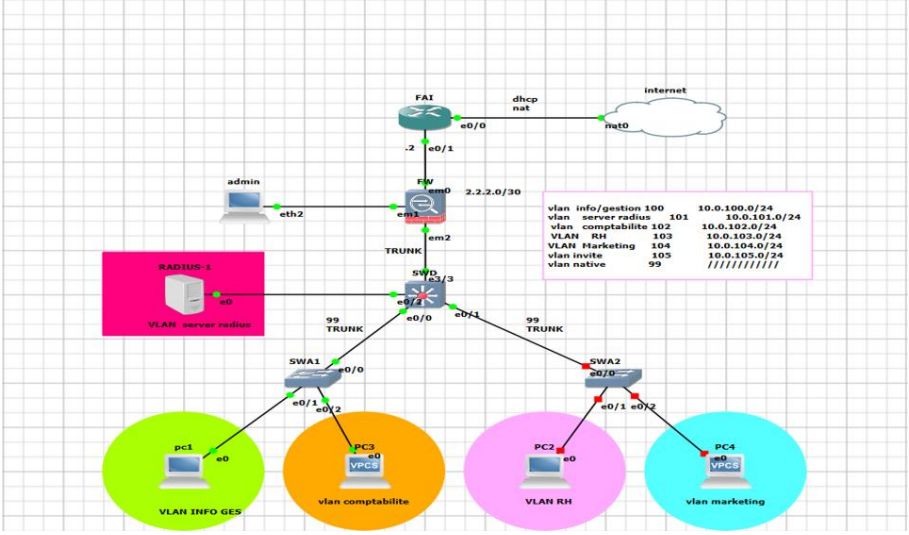

Figure IV.4 : Architecture de réseau proposée

IV.5 La table des équipements :

Equipement	Fournisseur	Nom équipement
Routeur Cisco2911	Cisco	FAI
Switch Cisco2911	Cisco	Switch distribution
Switches 2960	Cisco	Switch accès 1 et 2
Pfsense	Netgate	FW
Serveur DELL R830	DELL	Serveur ADM

Table IV.1 : Les équipements

IV.6 La table des Vlans

Nom vlans	**IP vlans**	**Réseau/préfixe**
Informatique et gestion	100	10.0.100.0/24
Server	101	10.0.101.0/24
Comptabilité	102	10.0.102.0/24
RH	103	10.0.103.0/24
Marketing	104	10.0.104.0/24
Vlan native	99	//////////////////

Table IV.2 : Table de Vlan

IV.7 Configuration de base sur le serveur

Notre solution suit les étapes suivantes

IV.7.1 Distribuer une adresse IP fixe au serveur

Attribuer une adresse IP statique au serveur voir la figure IV.5

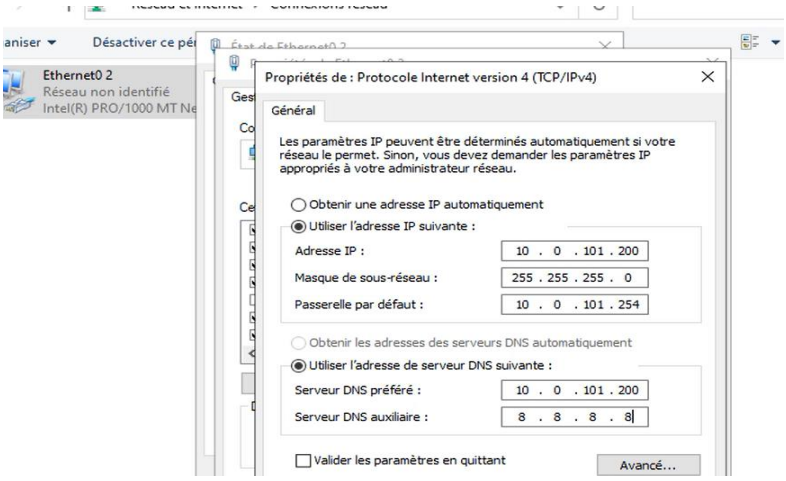

Figure IV.5 : Configuration de serveur

IV.7.2 Installer l'active directory dans le serveur

Sur la machine Windows serveur 2022 nous avons installé un contrôleur de domaine dont le nom de domaine est COLLABLE.LOCAL

Pour commencer l'installation, il va falloir ajouter le Service de Rôle Active Directory.

Lancer l'installation et ajouter les fonctionnalités qui nous manquent.

Voici les étapes d'installation active directory

- Dans la gestionnaire de serveur on choisit ajouter des rôles et fonctionnalités.
- Sélectionné le serveur destination.
- Choisi le rôle active directory.
- Lancer l'installation.

Le DNS sera installé automatiquement en parallèle avec l'active directory.

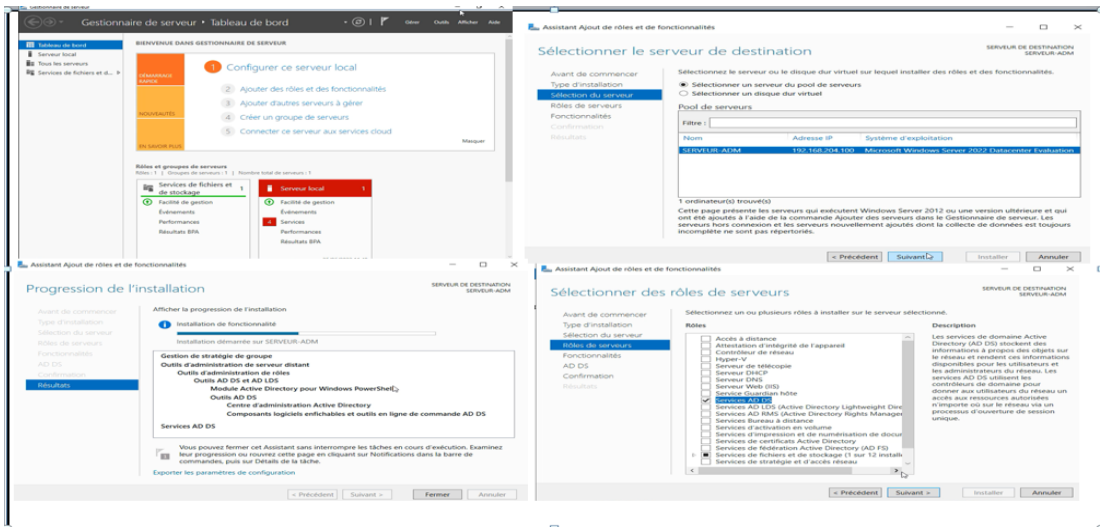

Figure IV.6 : L'installation active directory

IV.7.3 Configuration d'Active Directory

Maintenant nous allons commencer la configuration de Active Directory.

La première étape consiste à créer une nouvelle foret, nommé collable.local Le nom affecté, Windows nous demande de choisir le niveau fonctionnel de notre foret Active Directory.

Dans notre exemple, nous mettrons un niveau fonctionnel 2016. Windows nous propose ensuite d'installer des options supplémentaires, tel qu'un serveur DNS compatible avec notre Active Directory. Le domaine créé collable.local est notre premier contrôleur de domaine catalogue global activé. Lorsque les services seront installés et configurés, cliquant sur FIN le système devra redémarrer. A la fin de l'installation on aura les deux rôles installés AD DS et DNS

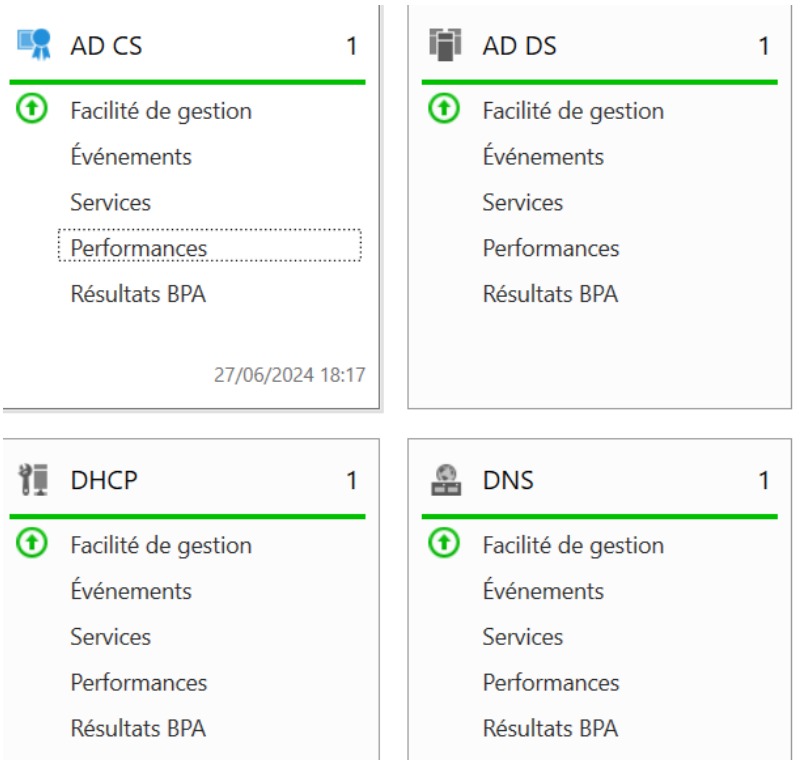

Figure IV.7 : Les rôles AD DS et DNS

IV.7.4 Installation de DHCP

Nous avons installé DHCP server sur la machine Windows server 2022 Pour commencer l'installation, il va falloir ajouter le Service de DHCP Server et ajouté les fonctionnalités nécessaires.

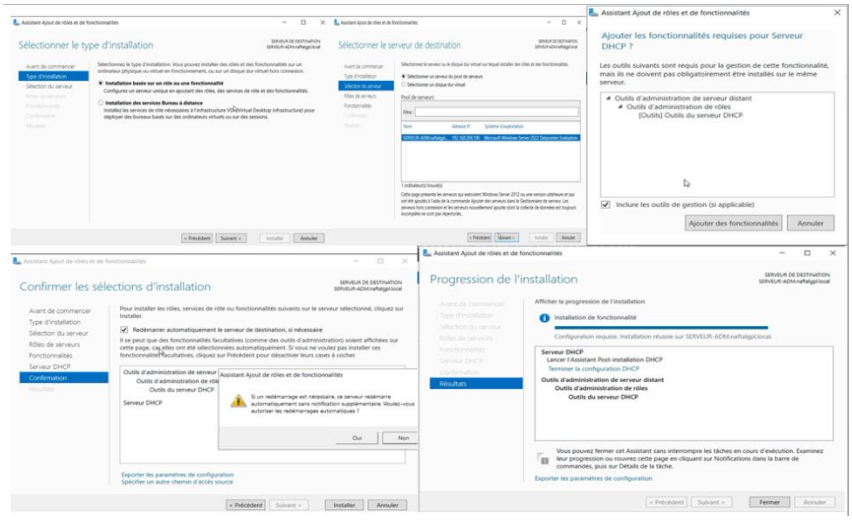

Figure IV.8 : Installation de DHCP

Pour relier le DHCP avec l'active directory il suffit de valider le nom d'utilisateur pour autorise la relation. Voir la figure IV.9.

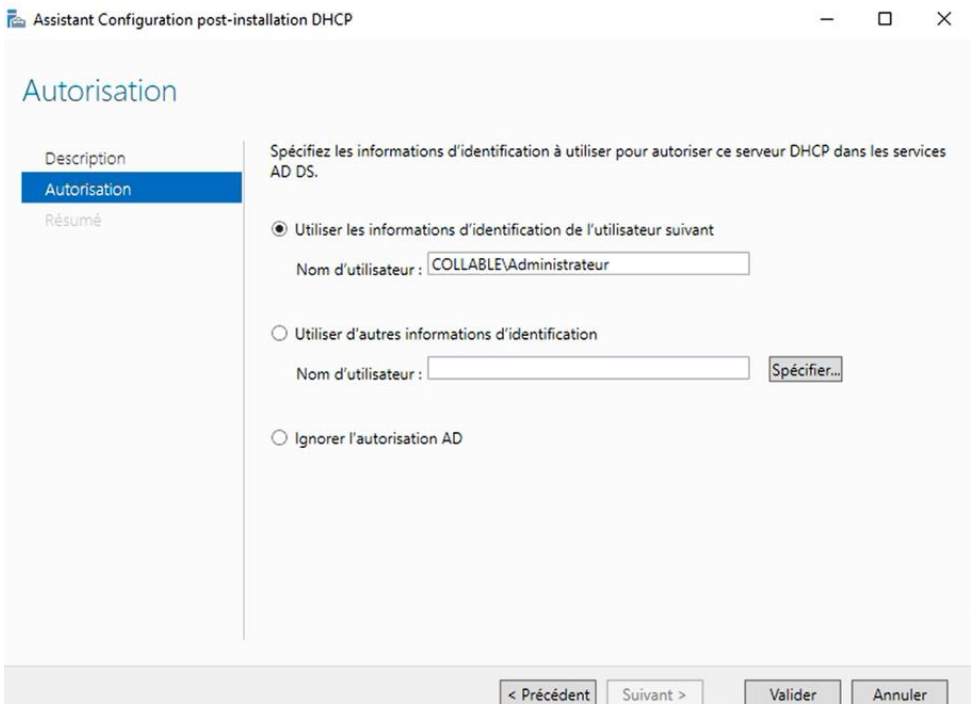

Figure IV.9 : Relier DHCP avec l'actif directory

IV.7.5 Configuration du DHCP

Pour créer un pool d'adresse pour chaque Vlan (distribution des adresses pour chaque vlan) on clique sur IPV4.

Etape1 : donner le nom et la description de vlan

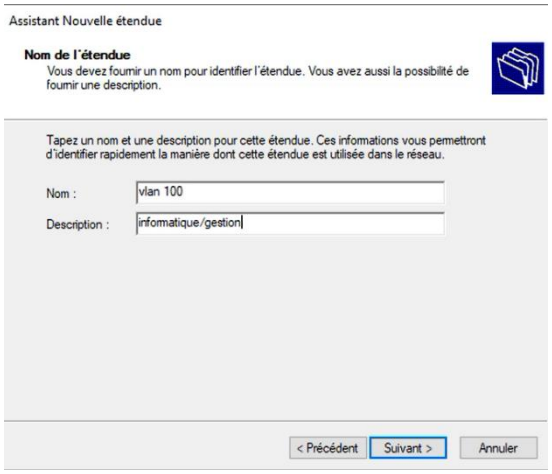

Figure IV.10: nom et description de vlan

Etape2 : distribution des adresses pour les vlans voir la figure IV.11

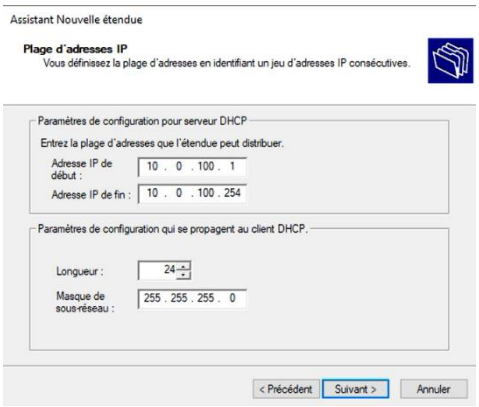

Figure IV.11: paramétrer les adresses des Vlan

Etape3 : On va exclure les 10 premières adresses et la passerelle voir la figure IV.12

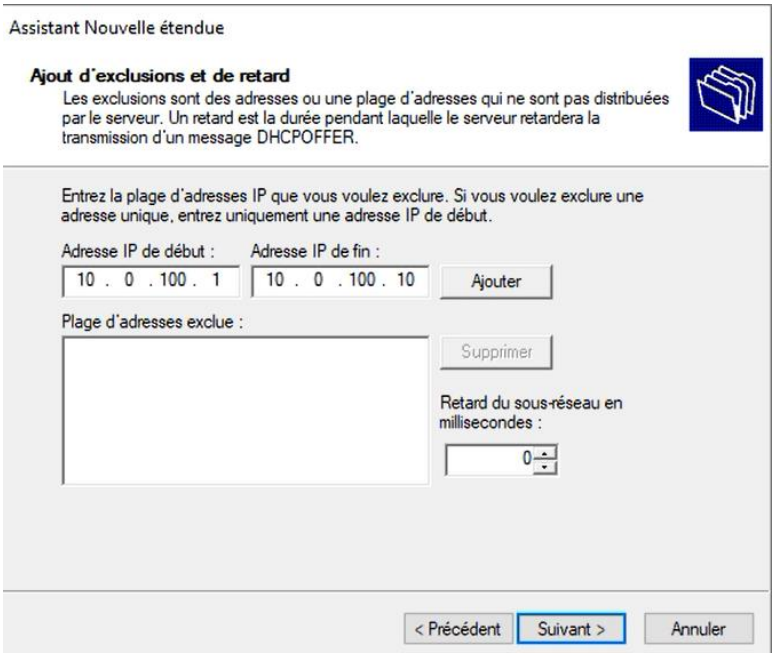

Figure IV.12: Exclusion des 10 premières adresses

Ensuit on active l'étendu et configurer des étendus des vlans voir la figure IV.13

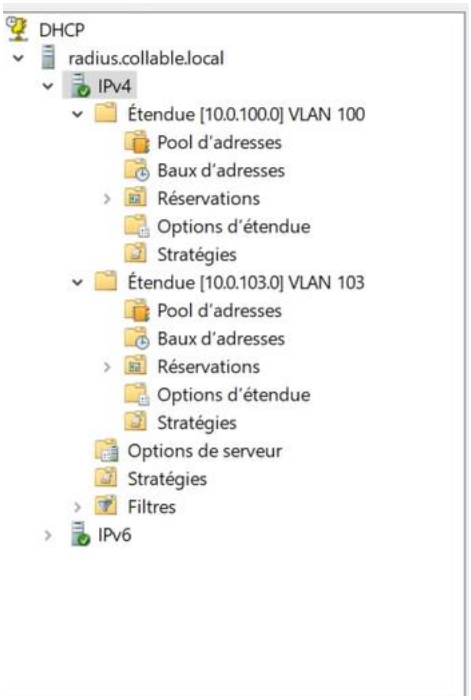

Figure IV.13: Les étendus des vlans configurer

IV.7.6 Configuration unité d'organisation collable

Créer unité d'organisme collable dans laquelle en criée les utilisateurs. Voir la figure IV.14

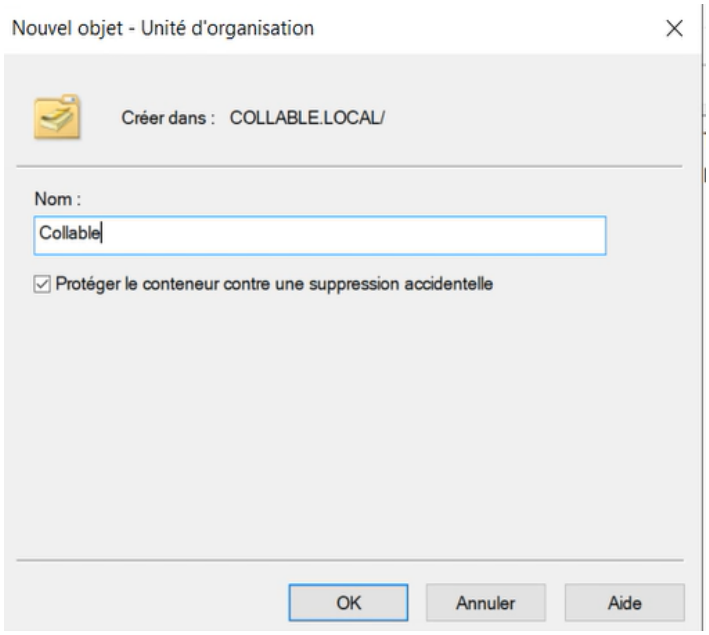

Figure IV.14: création d'utile d'organisation

La création des utilisateurs par le serveur active directory voir les deux figure IV.15 et la figure IV.16

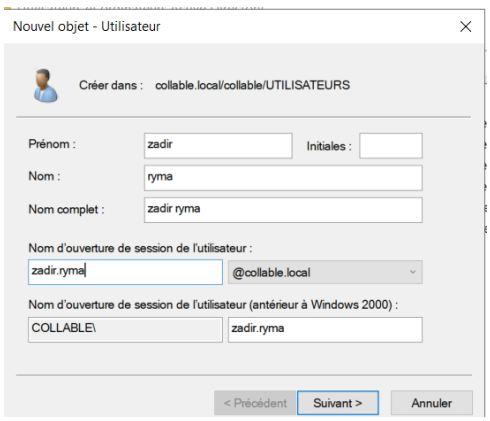

Figure IV.15: Création d'utilisateur 1

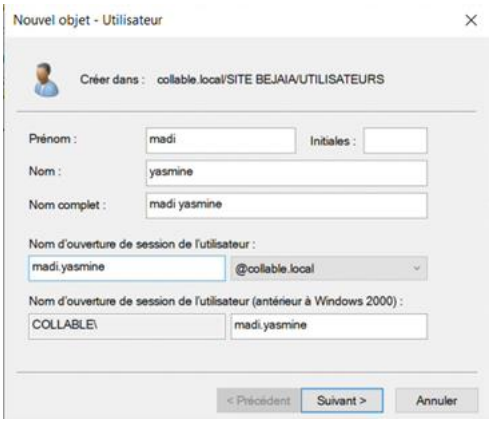

Figure IV.16: Création d'utilisateur 2

Créer les groupes de l'entreprise comme groupes informatiques et gestion

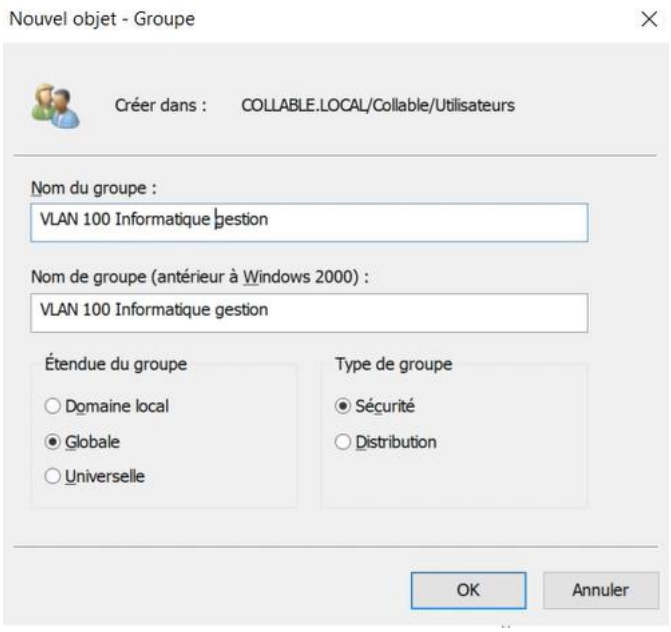

Figure IV.17: Création de groupe informatique et gestion

On va créer les autres groupes de la même façon.

IV.7.7 Configurations des switches

Pour la configuration des switches, on commence par les switches de distribution après les switches d'accès1 et switches d'accès2.

IV.7.7.1 Configuration de switch distribution

Les commandes sont lancées dans le terminal voir la figure IV.18

Figure IV.18: Configuration de switch distribution

IV.7.7.2 Configuration de switch d'accès 1

Les commandes sont lancées dans le terminal Voir la figure IV.19

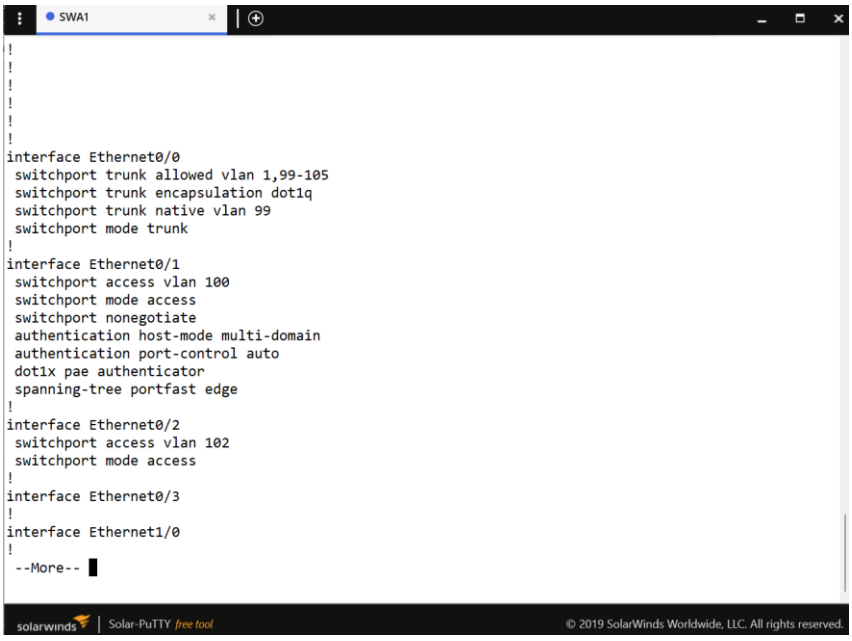

Figure IV.19: Configuration de switch d'accès 1

IV.7.7.3 Configuration de switch d'accès 2

Les commandes sont lancées dans le terminal voir la figure IV.20

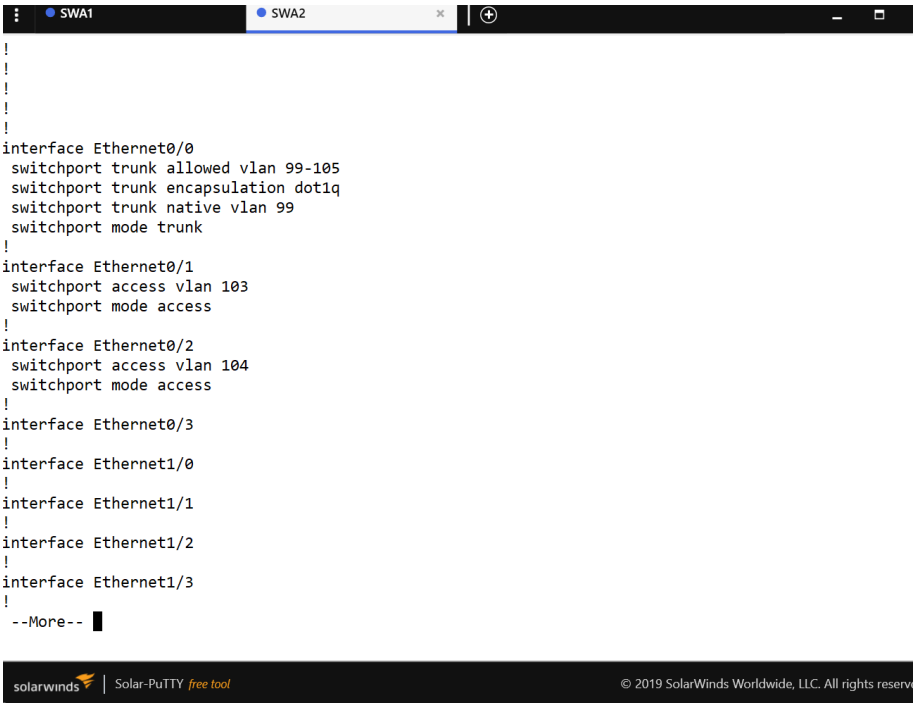

Figure 4.20: Configuration de switch d'accès 2

IV.8 Configuration du Protocol VTP

Le VTP facilite la gestion des VLANs, il a trois modes de configuration :

- **Mode serveur :** Centraliser les commandes dans le switch de distribution.
- **Mode client :** Appliquer la configuration dans les switches d'accès.
- **Mode transparence :** diffuser la configuration des switches.

Configuration de VTP en mode serveur

Les commandes sont lancées dans le terminal voire la figure IV.21

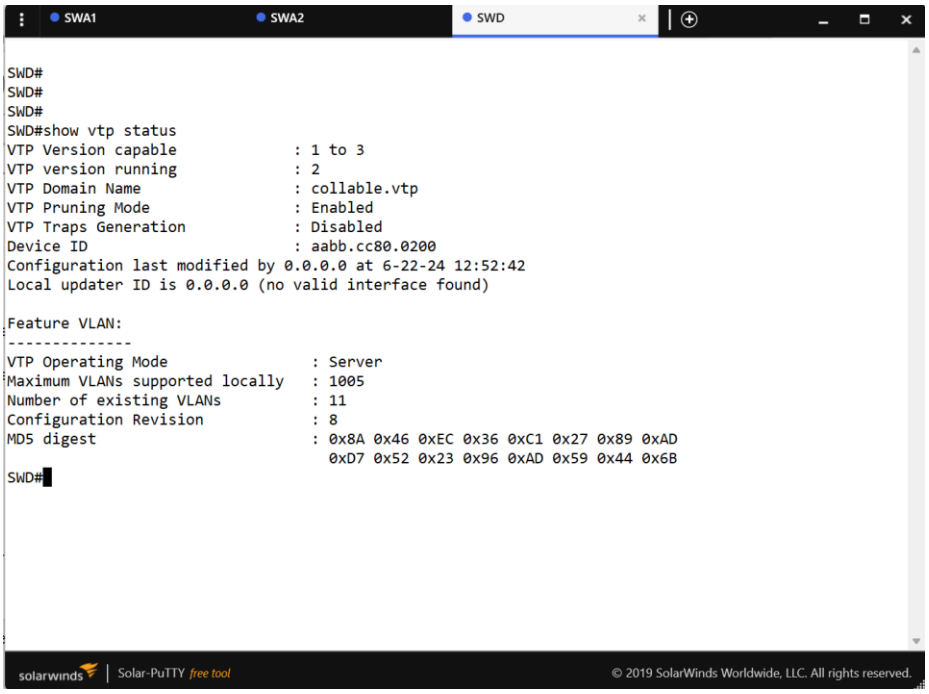

Figure IV.21: Configuration de VTP en mode serveur

Configuration de VTP en mode client

Les commandes sont lancées dans le terminal voir la figure IV.22

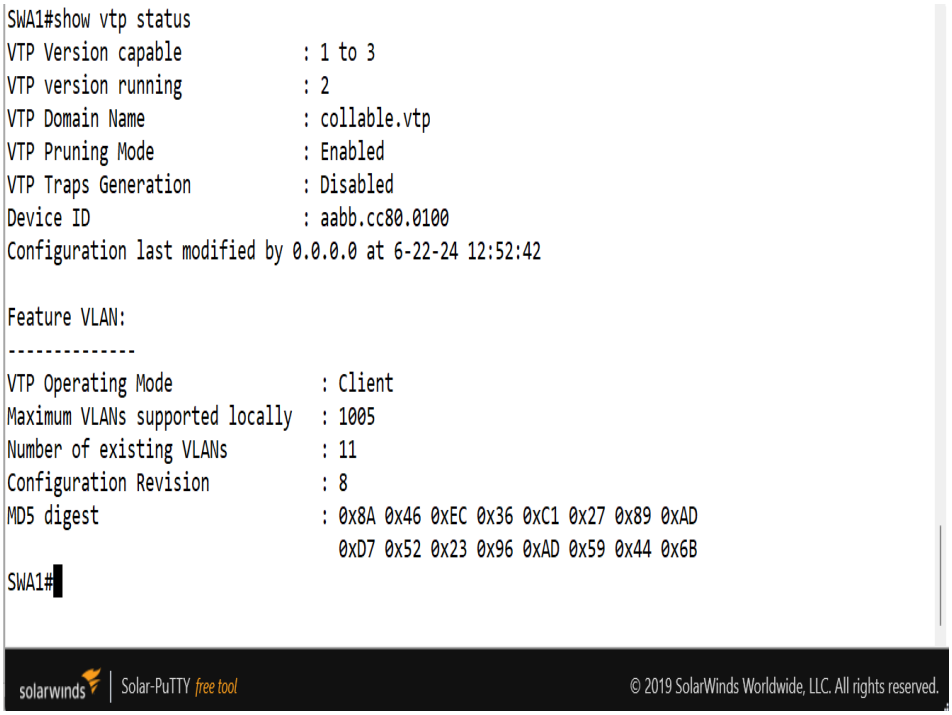

Figure IV.22: Configuration de VTP en mode client

IV.9 Créer les vlans sur le switch distribution.

Les commandes sont lancées dans le terminal voir la figure IV.23

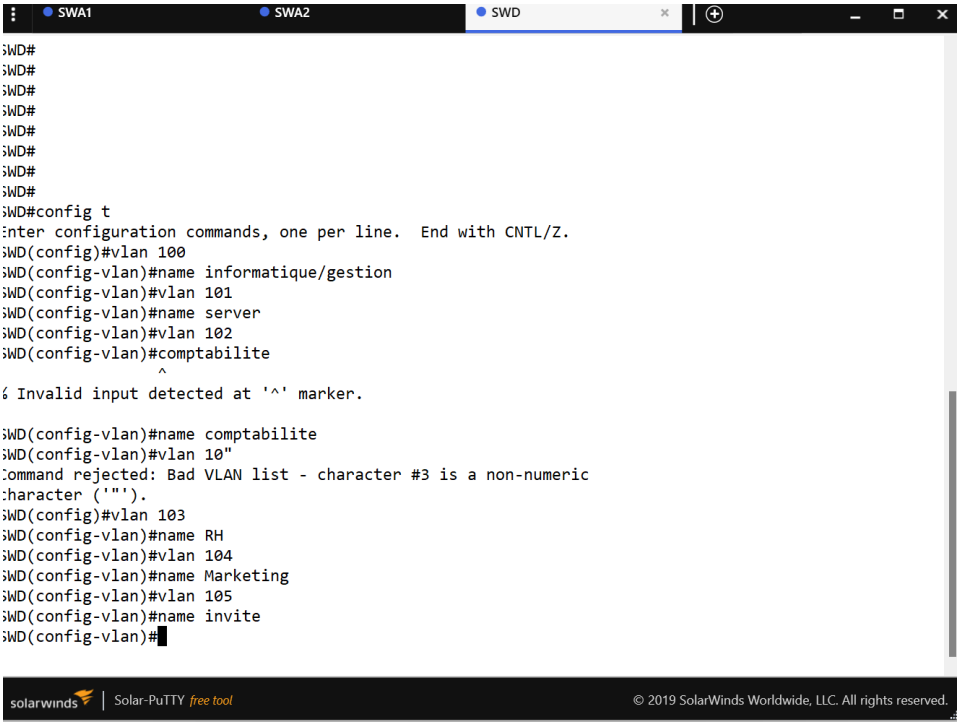

Figure IV.23: Création des vlans

IV.9.1 La vérification des vlans crée sur le switch distribution

Dans cette étape, on vérifie que tous les vlans ont reçu la configuration voir dans la figure IV.24.

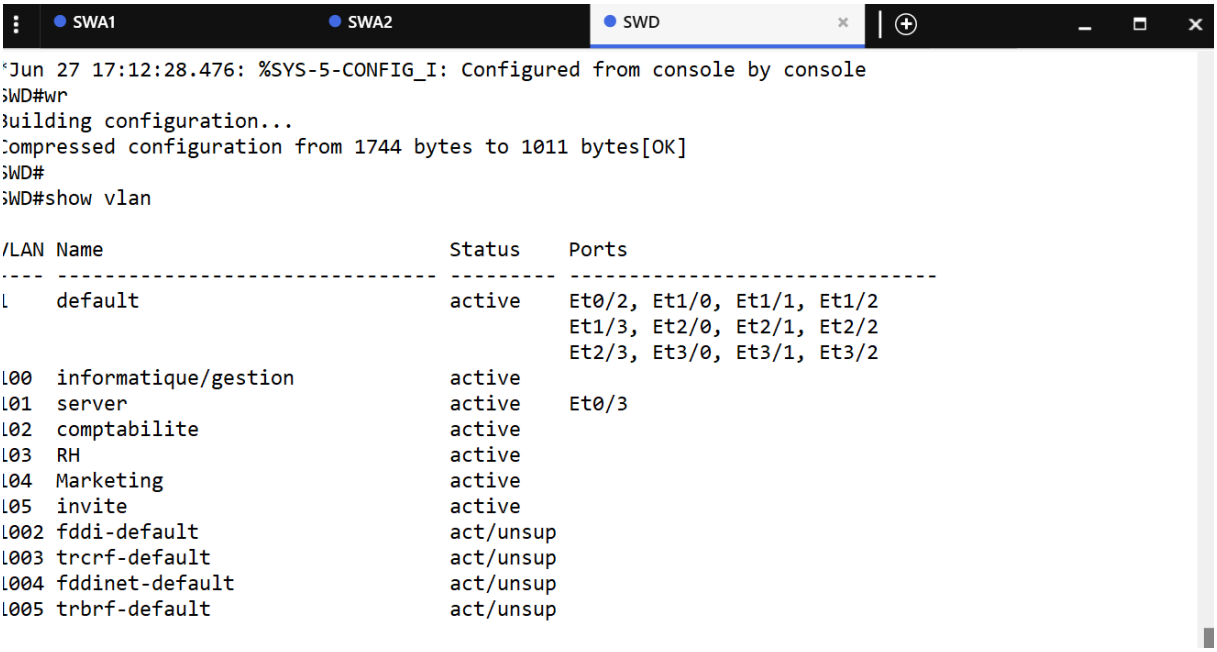

Figure IV.24: Vérification des vlans créés

IV.10 Le routage inter VLAN

Étape 1 : Connexion à pfsense

Accès à l'interface de pfsense et saisie du nom d'utilisateur et du mot de passe.voir la figure IV.25

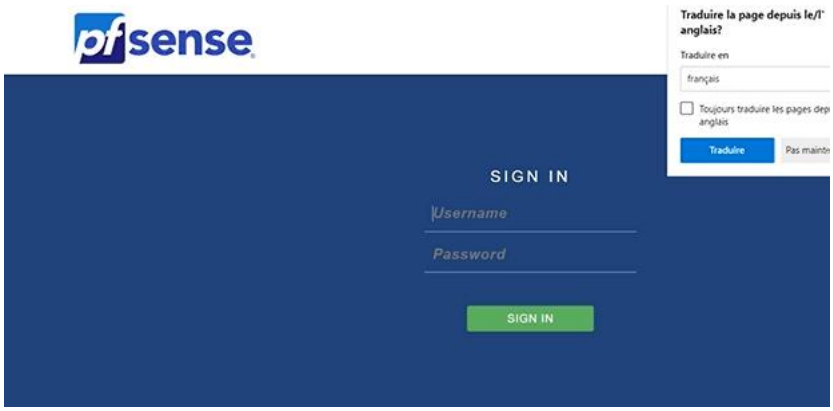

Figure IV.25: Page d'accueil de pfsense

Étape 2 : Changement du mot de passe de pfsense

Modification du mot de passe par défaut de pfsense pour des raisons de sécurité voir la figure IV.26

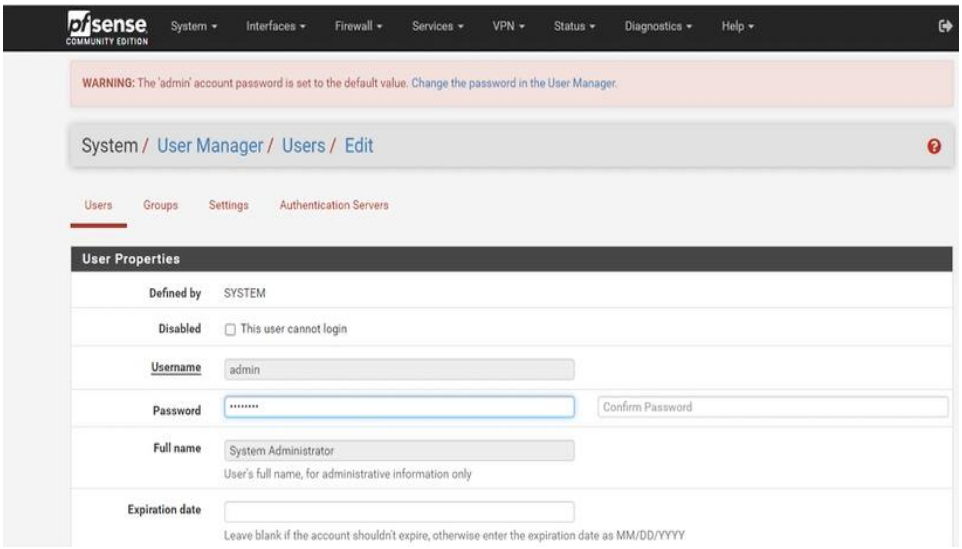

Figure IV.26: Changement de mot de passe

Étape 3 : Configuration des sous-interfaces VLAN

Création des sous-interfaces pour chaque VLAN et déclaration des VLAN sur pfsense. Voir la figure IV.27

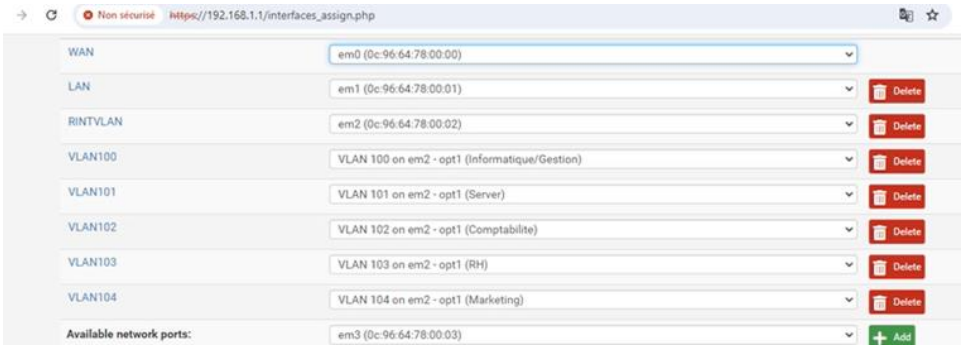

Figure IV.27: Création des sous interfaces

IV.11 Configuration de l'accès Internet avec pfsense et liaison au routeur du fournisseur d'accès (FAI)

IV.11.1 Configuration de l'accès Internet sur pfsense

Etape1 : Configuration de l'interface WAN

Configurer l'interface WAN ainsi que la passerelle pour établir la connexion vers Internet. Voir la figure IV.28 et la figure IV.29

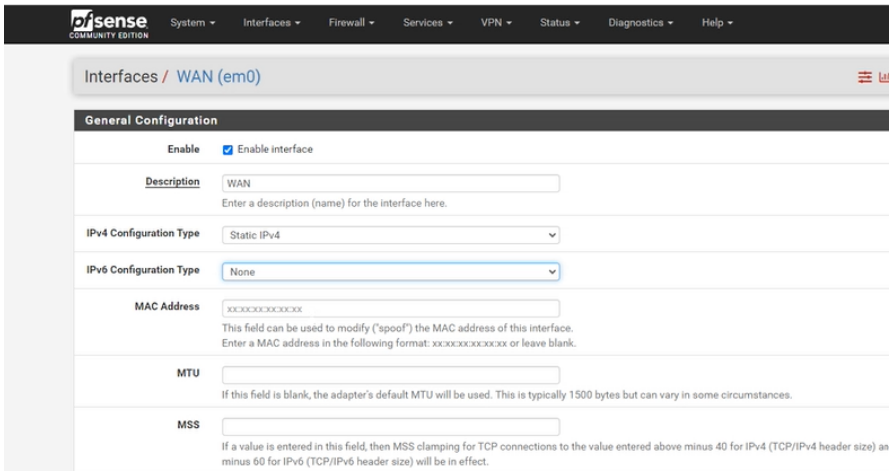

Figure IV.28: Configuration l'interface wan

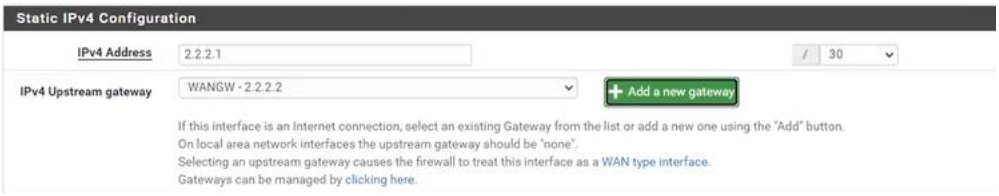

Figure IV.29: Configuration de la passerelle

Étape 2 : Autorisation du trafic vers Internet

Configuration des règles de pare-feu pour permettre le trafic sortant vers Internet. voir la figure IV.30

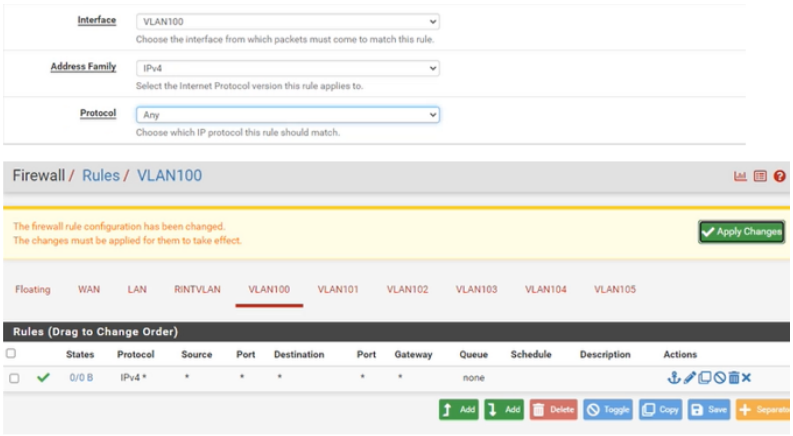

Figure IV.30: Configuration de la passerelle

4.11.2 Configuration de l'accès Internet sur le routeur du fournisseur

Les commandes sont lancées dans le terminal. Voir la figure IV.30

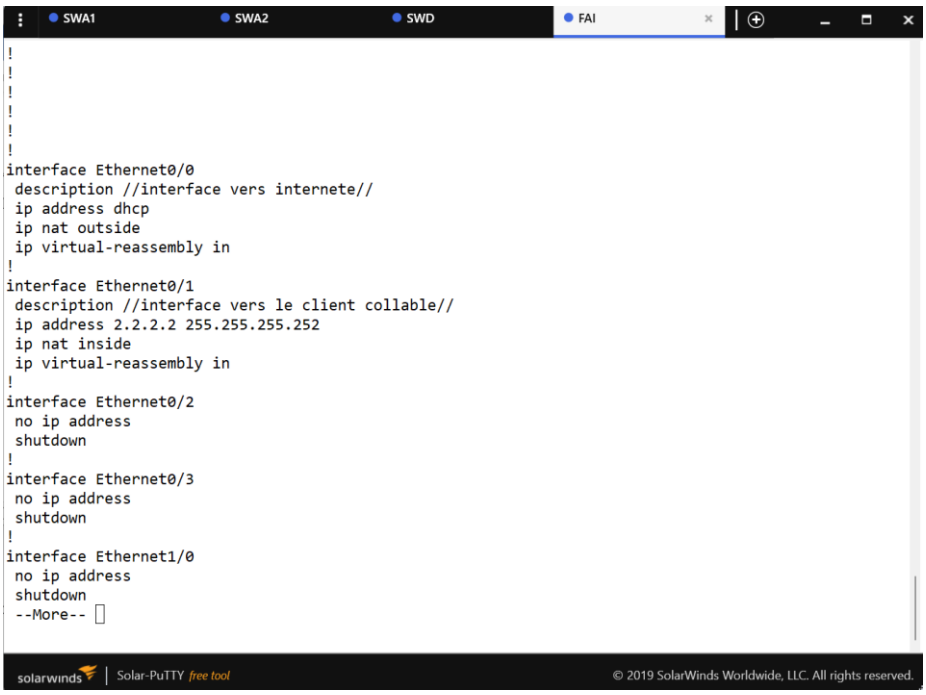

Figure IV.30 Interface eth0 /1

4.12 Ajouter l'utilisateur au domaine

Voir la figure IV.34

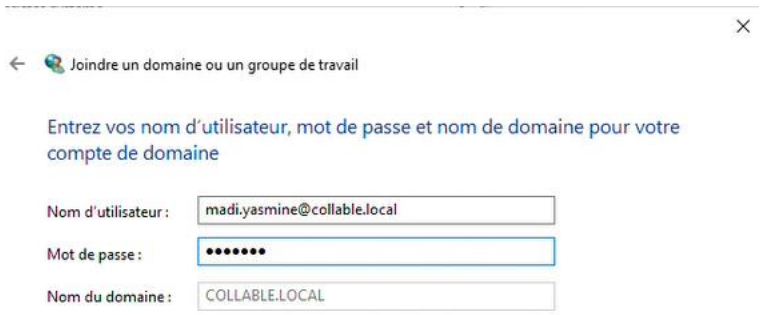

Figure IV.31 : Joindre domaine

4.13 Création de certificat autorité (CA)

Pour une authentification plus sécurisée on utilise une authentification par certificat. Voir la figure IV.32

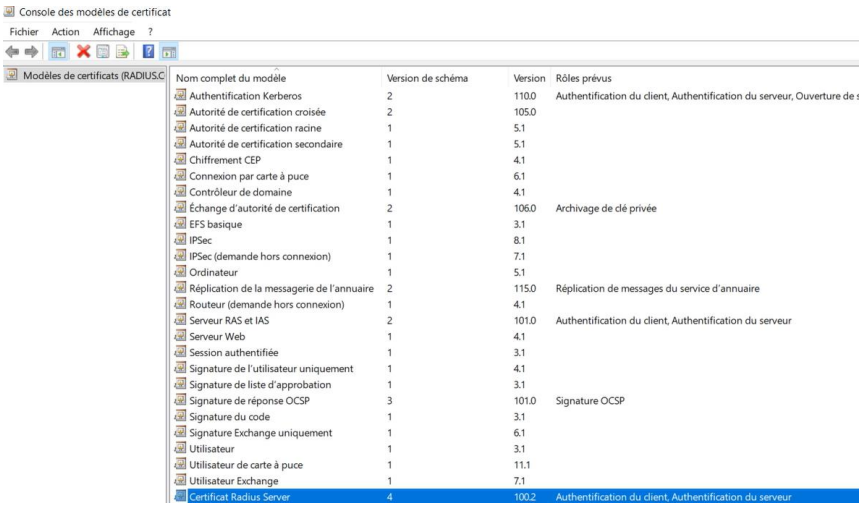

Figure IV.32 : Création de certificat autorité

Étape 1 : Création du certificat pour le serveur RADIUS

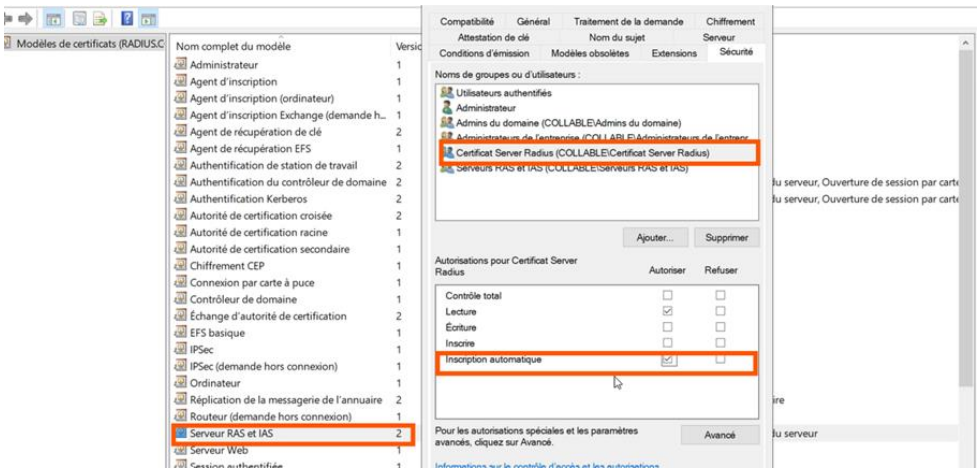

Figure IV.33: Création du certificat pour serveur

Étape 2 : Création du certificat pour le client RADIUS

Voir la figure IV.34

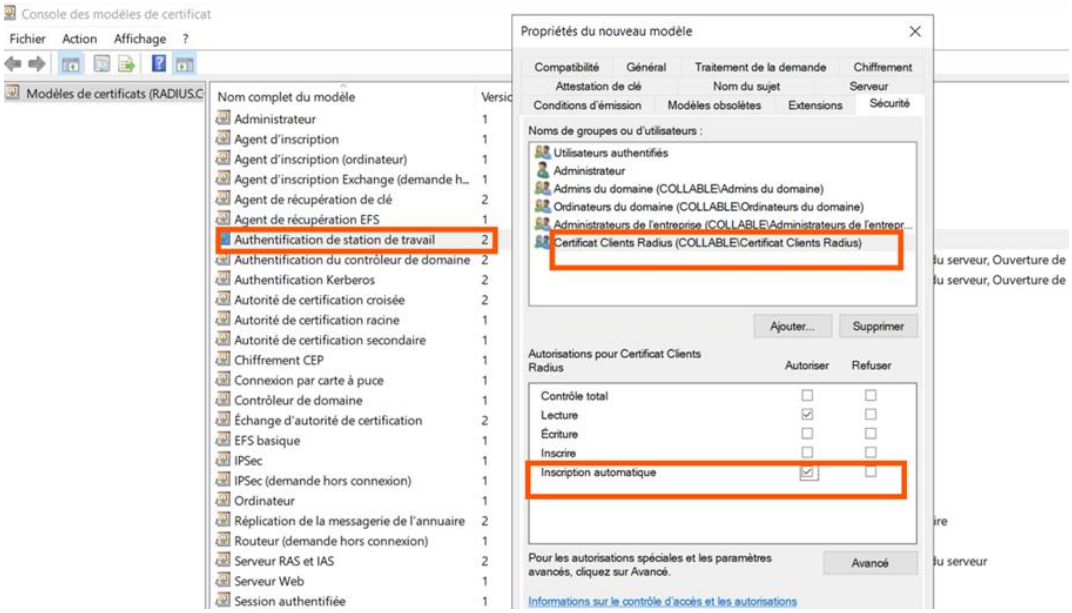

Figure IV.34: Création du certificat pour client

Étape 3 : Ajouter ces certificats au modèle de certificat

Voir la figure IV.35

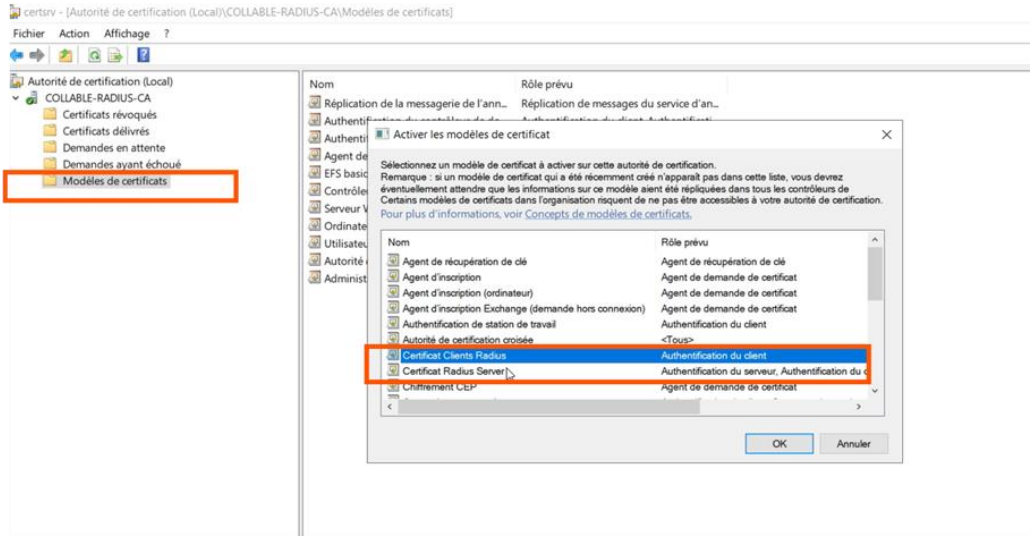

Figure IV.35 : Les certificats ajouter au modèle de certificat

IV.14 Configuration de l'Inscription Automatique au Certificat via les Stratégies de Groupe (GPO)

Etapes 1 : Certification Globale :

Indique l'aspect global de la configuration des certificats voir la figure IV.36

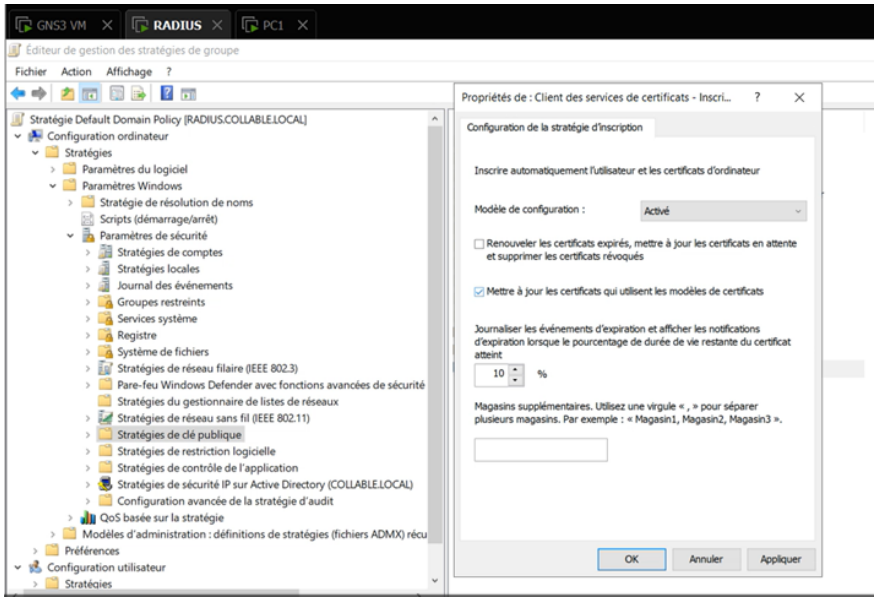

Figure IV.36 : Certification globale

Etape 2 : l'Inscription Automatique au Certificat

Voir la figure IV.37

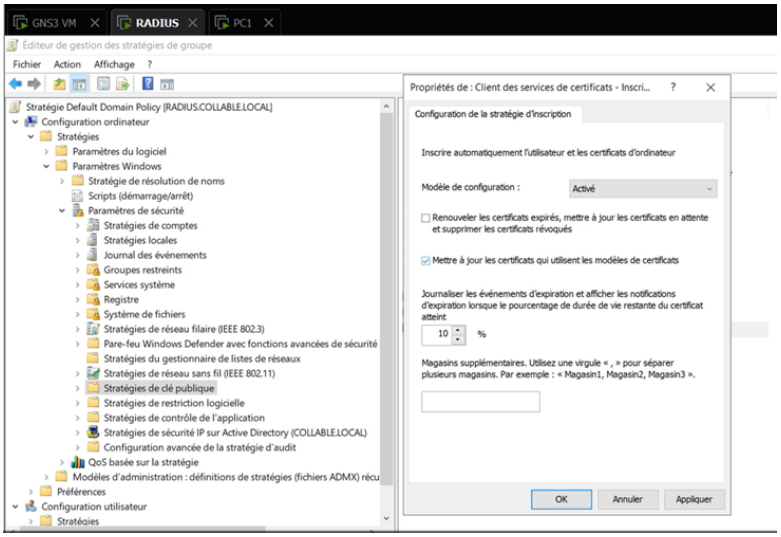

Figure IV.37 : Inscription automatique

Etape 3 : Création d'une Stratégie 802.1X Réseau Câblé

Voir la figure IV.38

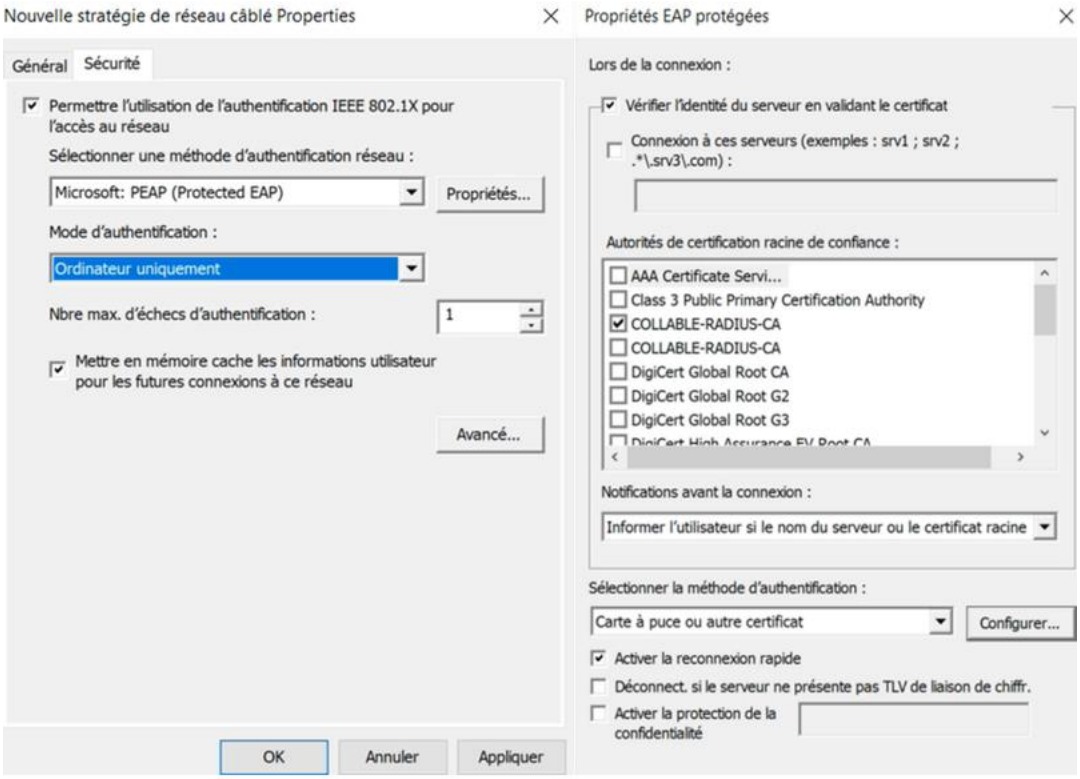

Figure 4.38 : Création d'une Stratégie 802.1X Réseau Câblé

- Configuration des Politiques RADIUS après Sélection du Client

Voir la figure IV.39

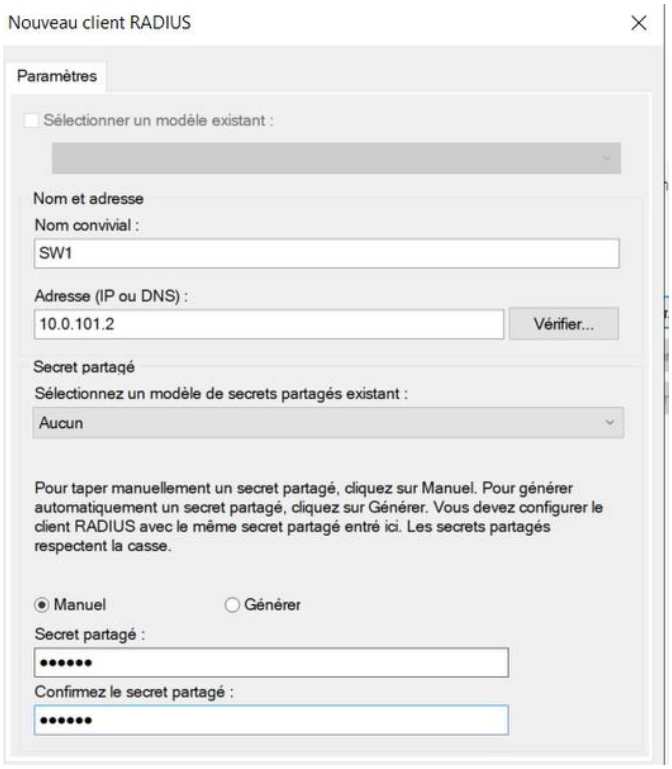

Figure IV.39 : Création de clients radius

Activation du Service AAA et Configuration du Service RADIUS sur client switch1

aaa new-model

aaa authentication dot1x default group radius

aaa authorization network default group radius

radius server RADIUS

address ipv4 10.0.101.200

key CCNP

- Configuration configuration dauthentification dot1x

SWA1#show running-config interface ethernet 0/1

interface Ethernet0/1

switchport access vlan 100

switchport mode access

switchport nonegotiate

authentication host-mode multi-domain

authentication port-control auto

dot1x pae authenticator

spanning-tree portfast edge

IV.15 Configuration de commutateur CLIENT-RADIUS pour l'accès SSH

Secure Shell (SSH) est un protocole réseau qui permet d'établir une connexion d'émulation de terminal sécurisée avec un routeur ou un autre périphérique réseau. SSH chiffre toutes les informations qui transitent via la liaison réseau et assure l'authentification de l'ordinateur distant. Il est en train de remplacer rapidement Telnet en tant qu'outil de connexion à distance de prédilection des professionnels réseau. Ce protocole est très souvent utilisé pour se connecter à une machine distante et exécuter des commandes.

hostname SWA3

aaa new-model

aaa authentication login default group radius local

aaa authorization exec default group radius local

radius-server host 10.0.101.200

radius-server key CCNP

ip domain-name collable.ssh

ip ssh version 2

line vty 0 15

login authentication default

transport input ssh

IV.16 LES TEST

1.Vérification de la Réception du Certificat sur l'Ordinateur

Voir la figure IV.40

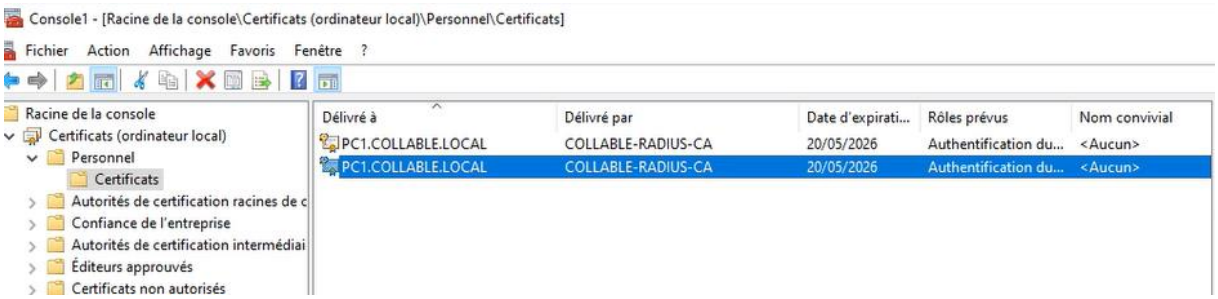

Figure IV.40 : la réception du certificat

Test authentification

Voir la figure IV.41

```
SWA1#
SWA1#show  authentication sessions interface  ethernet 0/1 details
            Interface:  Ethernet0/1
          MAC Address:  000c.298f.0393
         IPv6 Address:  Unknown
         IPv4 Address:  10.0.100.12
            User-Name:  host/pc1.collable.local
               Status:  Authorized
               Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
    Common Session ID:  0A00650200000000C00545733
      Acct Session ID:  Unknown
               Handle:  0xBC000001
      Current Policy:  POLICY_Et0/1

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

Server Policies:
          Vlan Group:  Vlan: 100

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

Figure IV.41 : Test d'authentification sur le switch

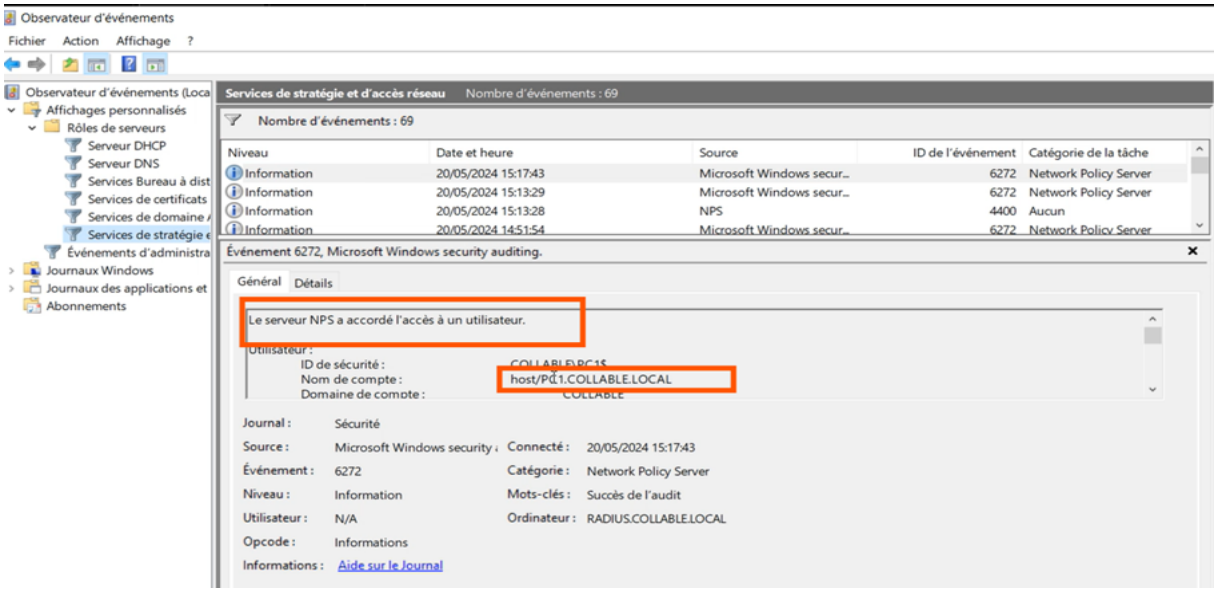

Figure IV.42 : Vérification d'authentification

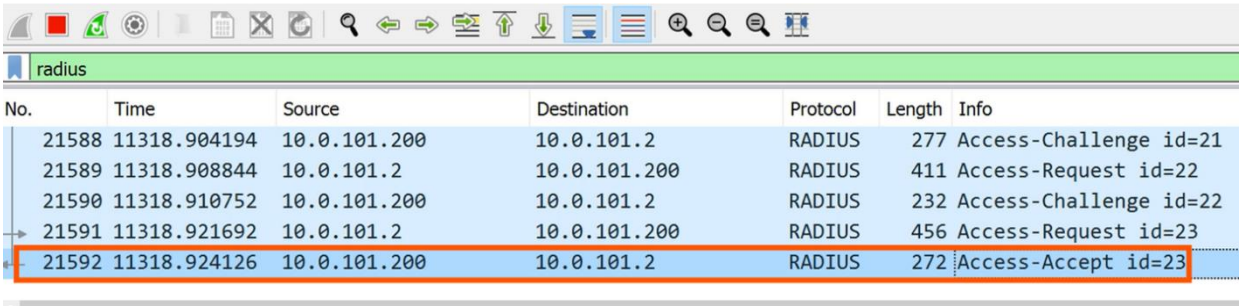

Figure IV.43 : Verification d'accès sur wirechak

Teste non authentification

Nous supprimons le PC du groupe associé à la stratégie RADIUS. Voir la figure IV.48

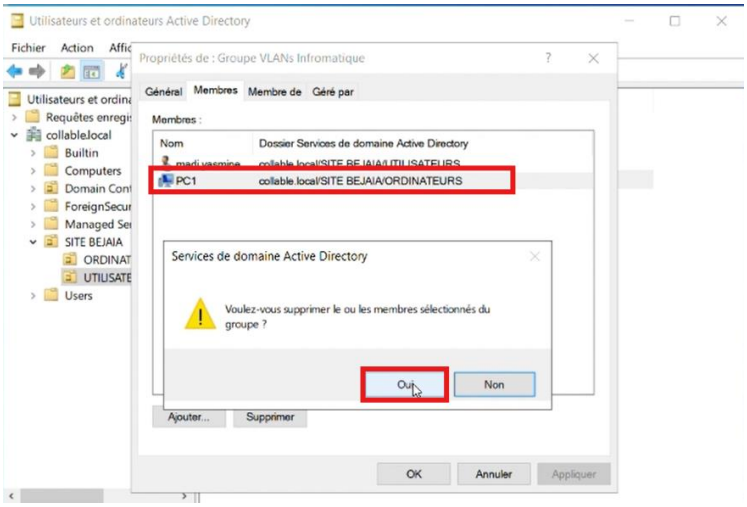

Figure IV.44 : Suppression le pc du groupe

```
SWA1#show  authentication sessions interface  ethernet 0/1 details
            Interface:  Ethernet0/1
          MAC Address:  000c.298f.0393
         IPv6 Address:  Unknown
         IPv4 Address:  10.0.100.12
            User-Name:  host/pc1.collable.local
               Status:  Unauthorized
               Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  0A0065020000000C00545733
     Acct Session ID:  Unknown
              Handle:  0xBC000001
      Current Policy:  POLICY_Et0/1

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

Method status list:
       Method           State
       dot1x            Stopped
```

Figure 4.45 : Test non authentification

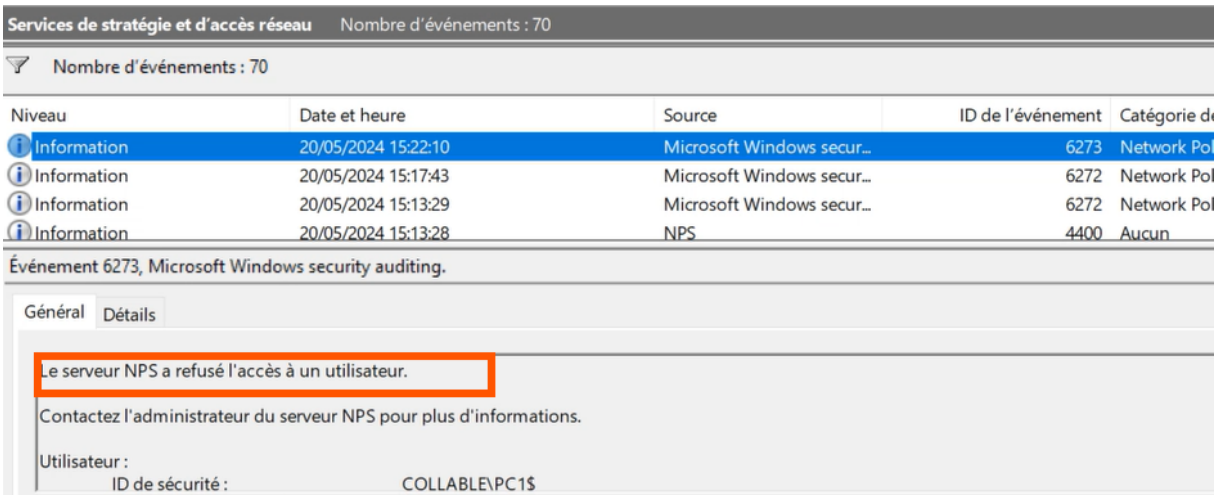

Figure 4.46: vérification de non authentification

IV.17 Conclusion

Ce chapitre a démontré l'efficacité de l'authentification par certificat et RADIUS pour sécuriser les communications réseau. En attribuant des certificats aux clients et serveurs dynamiques, nous avons renforcé la gestion des accès tout en améliorant la sécurité globale de notre infrastructure. Les tests d'authentification réussis et de non-authentification soulignent l'importance cruciale de ces méthodes pour garantir des normes élevées de sécurité et de gestion des accès.

Conclusion générale

Dans ce mémoire, nous avons mis en œuvre une technique de sécurisation d'accès aux réseaux informatiques afin de mieux garantir l'authentification l'intégrité et la confidentialité des données.

Cette technique de sécurisation s'agit en fait de la mise en place d'une solution d'authentification RADIUS, pour la réalisation nous avons utilisé Windows server 2020 qui inclut le serveur d'authentification Radius, et qui fait appel à des services de domaine Active Directory permettant d'avoir des contrôles de domaines.

La mise en œuvre de ce projet, nous a permis d'apporter une contribution au centre d'appel COLLABLE, et aussi d'acquérir de nouvelles connaissances sur le protocole authentification RADIUS grâce à une étude sur son fonctionnement.

Références Bibliographique

[1] M zidane cour de réseau informatique université de Bejaia

[2]http://math.univlyon1.fr/irem/Formation_ISN/formation_reseau/reseaux_generalites/generalites.html, consulté le 04/2023

[3] jean-francois pillou Fabrice lemainque, tout sur les réseaux et internet 5émé edition

[4] http://www.iro.umontreal.ca/kropf/ift-6052/exercices/applets/applet5/introduc.htm ,site internet.

[5] Tighilt, D., & Hamoudi, A. (2013). Mise en place d'une solution d'authentification RADIUS Cas : Cevital de Bejaia

[6] Djidjeli, A., & Ikhlef, L. (2021). Mise en place de la norme de sécurité 802.1X au sein du réseau de SONATRACH

[7] M.HAMZA.Cours de sécurité informatique. Université de Bejaia

[8] https://www.securiteinfo.com/; site internet .

[9] BOUGHAZI, Manal & LAKHAL, Asma. (2017). Attaque de l'homme du milieu dans les réseaux sociaux 4G. Mémoire de fin d'études, Université de 8 Mai 1945 – Guelma.

[10] TINA DEGHEN 6 Cédric Bertrand. Focus sur les attaques les plus courantes

[11] Une Introduction à la Cryptographie (news :fr.misc.cryptologie,1998).

[12] Benidris, F.Z. (2020). Cryptographie : Polycopie de cours et exercices corrigés. Université de Mostaganem.

[13] https ://connect.ed-diamond.com/misc/misc-054/attaque-sur-le-protocole-kerberos, consulte le 05/04/2024.

[14] LEO GONZALES. Kerberos : Principe de fonctionnement. 18 JUILLET 2018.

[15] BRAHAMI Nabila BOUFOUDI Siham. La sécurité des réseaux informatique à base de Kerberos, Université de Bejaïa, Mémoire de Master. 2014-2015.

Résumé De nos jours, la sécurité informatique est essentielle au bon fonctionnement des réseaux, qu'ils soient câblés ou sans fil. Les administrateurs réseau en entreprise doivent donc déployer des mécanismes de sécurité efficaces. Notre projet vise à mettre en place une solution d'authentification pour le réseau local du groupe collable de Bejaïa, assurant ainsi le contrôle d'accès des utilisateurs. Pour ce faire, nous avons opté pour la norme 802.1x avec certificats, en utilisant le protocole RADIUS, reconnu comme l'un des plus performants en matière d'authentification.

Dans cette étude, nous avons tout d'abord revisité les concepts de base des réseaux et de la sécurité informatique afin de bien appréhender les principes nécessaires à notre projet. Pour l'implémentation de notre solution, nous avons choisi Windows Server 2022, qui intègre un serveur RADIUS pour l'authentification, ainsi que la base de données Active Directory pour la gestion des comptes utilisateurs et les services de stratégies d'accès.

Mots clés : 802.1x, RADIUS, Windows Server 2022, Active Directory.

Abstract Nowaday’s, computer security is indispensable for the smooth operation of both wired and wireless networks. To achieve this, network administrators in organizations must deploy effective security measures.

Our project focuses on implementing an authentication solution for the local network of the group callable Bejaia, ensuring robust user access control. For this purpose, we opted for the 802.1x standard with certificates, using the RADIUS protocol, recognized as one of the most efficient in terms of authentication.

To undertake this initiative, we began with a review of fundamental networking concepts and computer security principles to address the challenges at hand. For the implementation phase, we opted for Windows Server 2022, leveraging its built-in RADIUS authentication server, Active Directory for user account management, and access policy services.

Keywords: 802.1x, RADIUS, Windows Server 2022, Active Directory.