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

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

MÉMOIRE DE MASTER

En

Informatique

Option

Administration et Sécurité des Réseaux

Thème

Etude et mise en place de l'authentification RADIUS et la norme 802.1x sur un réseau filaire et sans fil Cas : SARL Collable

Présenté par : Mr BERRAH Salim
Melle CHABOUNI Chafia

Soutenu devant le jury composé de :

Président :	**Mr ZERARGA L.**	**M.C.B.**	**Univ. A. Mira Béjaia.**
Encadrant :	**Mr TOUAZI Dj.**	**M.C.B.**	**Univ. A. Mira Béjaia.**
Examinateur :	**Mr SALHI N.**	**M.A.A.**	**Univ. A. Mira Béjaia.**

Béjaïa, Juillet 2024

REMERCIEMENTS

En préambule de ce mémoire, nous tenons à remercier notre Dieu, le Tout Puissant, de nous avoir donné le bon sens et la grande volonté pour réaliser ce modeste travail.

Avec immense plaisir que nous souhaitons vivement remercier et exprimer notre grande gratitude :

A notre encadrant, en l'occurrence Dr TOUAZI, à qui nous sommes très reconnaissant pour ses remarques, ses conseils et surtout ses encouragements afin d'aboutir à notre objectif.

Au Directeur de Campus NTS et son client le gérant de la SARL Collable pour leurs orientations et leurs soutiens tout au long de la réalisation de ce projet.

Nos vifs remerciements vont également aux membres de jury qui ont acceptés d'évaluer notre travail.

Nos sincères remerciements s'adressent aussi en exprimant notre sincère gratitude à tous les enseignants de bonne foi qui nous ont accompagnés durant notre formation.

A nos collègues de travail et à toutes les personnes qui ont contribués de près ou de loin à l'aboutissement de ce travail.

Sans oublier de remercier chaleureusement nos familles qui ont sacrifiées leurs temps et leurs énergies avec une grande patience pour tenir tranquillement notre formation.

Dédicaces

الحمد لله رب العالمين

J’aimerais, avant tout exprimer ma reconnaissance à l’éternel mon Dieu pour ce que je suis, car une vraie réussite n’est possible sans Lui.

Je dédie ce modeste travail à :

À la mémoire de ma mère bien-aimée, dont la sagesse, la tendress et la générosité m’ont guidé tout au long de ma vie.

À ma femme bien-aimée, ensemble, nous continuerons à créer une vie remplie de joie et d'aventures.

À mes chers parents (mon père et ma belle mère), vous m'avez toujours soutenu et guidé. Merci d'être des modèles d'intégrité et de bienveillance.

À mes enfants chéris, Que cette œuvre soit un témoignage de mon amour inconditionnel. Puissiez-vous toujours briller de mille feux.

À mes frères et sœurs, merci d'avoir partagé avec moi les hauts et les bas de la vie. Votre complicité est un trésor inestimable.

À toute ma famille élargie, pour leur amour, leurs encouragements, et leur foi en moi.

À mes chers amis et collègues, votre présence a enrichi mon existence. Je suis reconnaissant pour votre soutien et votre amitié sincère.

A ma binôme et toute la promo ASR 2024.

Que cette dédicace exprime toute ma gratitude envers ceux qui comptent le plus à mes yeux.

SALIM

Dédicaces

الحمد لله رب العالمين

Le parcours n'a pas été court, et il ne devait pas l'être. Le rêve n'était pas proche, et le chemin n'était pas facile, mais grâce à Dieu puis au soutien de ma chère famille, l'espoir s'est réalisé et le but a été atteint.

Je dédie avec tout mon amour ce mémoire de fin d'études

À celle dont les prières constantes ont été le secret de ma réussite, celle qui a été une lumière dans mes moments les plus sombres, ma mère.

À la mémoire de mon père bien-aimé, dont la sagesse et la générosité m'ont guidé tout au long de ma vie.

Aucune dédicace ne saurait être assez éloquente pour exprimer ce que vous méritez pour tous les sacrifices que vous n'avez cessé de me donner depuis ma naissance. Rien au monde ne vaut l'assistance et les efforts fournis jour et nuit pour mon éducation et mon bien être.

À ceux dont il a été dit : « Nous raffermirons ton bras par ton frère », mes frères et sœurs. Que Dieu vous garde toujours comme un pilier solide pour moi.

À mes adorables neveux et nièces, votre présence constitue une grande force pour moi.

À mon binôme, chaque défi que nous avons surmonté ensemble et chaque succès que nous avons partagé sont des témoignages de notre travail acharné et de notre détermination.

À celles qui m'ont toujours inspiré courage et ont été des appuis constants dans mes moments de doute, mes amies.

À toutes les personnes qui ont, de près ou de loin, contribué à ma réussite, votre soutien, vos encouragements et votre aide m'ont permis de franchir chaque étape avec confiance et détermination. **CHAFIA**

Table des matières

Liste des abréviations

AAA ***A****uthentication* ***A****uthorization* ***A****ccounting*

AD ***A****ctive* ***D****irectory*

ARP ***A****ddress* ***R****esolution* ***P****rotocol*

CA ***C****erticate* ***A****uthority*

Campus NTS ***C****ampus* ***N****ew* ***T****echnology &* ***S****olutions*

CHAP ***C****hallenge* ***H****andshake* ***A****uthentication* ***P****rotocol*

DHCP ***D****ynamic* ***H****ost* ***C****onfiguration* ***P****rotocol*

DNS ***D****omain* ***N****ame* ***S****ystem*

EAP ***E****xtensible* ***A****uthentication* ***P****rotocol*

EAP-Fast ***E****xtensible* ***A****uthentication* ***P****rotocol-****F****lexible* ***A****uthentication via* ***S****ecure* ***T****unneling*

EAP-OL ***E****xtensible* ***A****uthentication* ***P****rotocol-****O****ver the* ***L****AN*

EAP-TLS ***E****xtensible* ***A****uthentication* ***P****rotocol-****T****ransport* ***L****ayer* ***S****ecurity*

EAP-TTLS ***E****xtensible* ***A****uthentication* ***P****rotocol-****T****unneled* ***T****ransport* ***L****ayer* ***S****ecurity*

FAI ***F****ournisseur d'****A****ccès* ***I****nternet*

GPO ***G****roup* ***P****olicy* ***O****bject*

IEEE ***I****nstitute of* ***E****lectrical and* ***E****lectronics* ***E****ngineers*

IDS ***I****ntrusion* ***D****etection* ***S****ystem*

IP ***I****nternet* ***P****rotocol*

IPSec ***I****nternet* ***P****rotocol* ***Sec****urity*

ISO ***I****nternational* ***S****tandard* ***O****rganization*

LAN ***L****ocal* ***A****rea* ***N****etwork*

LEAP ***L****ightweight* ***E****xtensible* ***A****uthentication* ***P****rotocol*

MAC ***M****edia* ***A****ccess* ***C****ontrol*

MD5 ***M****essage* ***D****igest 5*

MS-CHAP ***M****icrosoft* ***C****hallenge* ***H****andshake* ***A****uthentication* ***P****rotocol*

NAP ***N****etwork* ***A****ccess* ***P****rotection*

NAS ***N****etwork* ***A****ccess* ***S****erver*

NAT ***N****etwork* ***A****ddress* ***T****ranslation*

NPS ***N****etwork* ***P****olicy* ***S****erver*

OU ***O****rganization* ***U****nit*

OSI ***O****pen* ***S****ystem* ***I****nterconnection*

PAT ***P****ort* ***A****ddress* ***T****ranslation*

PC ***P****ersonnel* ***C****omputer*

POS ***P****ersonal* ***O****perating* ***S****pace*

PEAP ***P****rotected* ***E****xtensible* ***A****uthentication* ***P****rotocol*

RADIUS ***R****emote* ***A****uthentication* ***D****ial-****I****n* ***U****ser* ***S****ervice*

RH ***R****essources* ***H****umaines*

SARL ***S****ociété commerciale* ***A*** ***R****esponsabilité* ***L****imitée*

TCP ***T****ransmission* ***C****ontrol* ***P****rotocol*

UDP ***U****ser* ***D****atagram* ***P****rotocol*

VLAN ***V****irtual* ***L****ocal* ***A****rea* ***N****etwork*

VMware ***V****irtual* ***M****achine*

VPN ***V****irtual* ***P****rivate* ***N****etwork*

VTY ***V****irtual* ***T****erminal*

WAN ***W****ide* ***A****rea* ***N****etwork*

WEP ***W****ired* ***E****quivalent* ***P****rivacy*

WLAN ***W****ireless* ***L****ocal* ***A****rea* ***N****etwork*

WPA ***W****ifi* ***P****rotected* ***A****ccess*

Table des figures

Liste des tableaux

Introduction générale

Les réseaux informatiques sont essentiels et jouent un rôle central dans presque tous les aspects de notre vie moderne, de la communication à la gestion de l'information, en passant par le divertissement et la sécurité.

La sécurité des réseaux informatiques est une préoccupation majeure dans le monde numérique d'aujourd'hui. Avec la prolifération des appareils connectés et des échanges de données en ligne, la protection des réseaux contre les menaces potentielles est cruciale pour garantir la confidentialité, l'intégrité et la disponibilité des informations.

L'évolution constante des technologies et des attaques informatiques rend la sécurisation des réseaux un défi complexe et en constante évolution. Les entreprises, les organisations gouvernementales et les particuliers doivent mettre en œuvre des mesures de sécurité robustes pour contrer les menaces telles que les cyberattaques, les logiciels malveillants, les attaques par déni de service et les violations de données.

Les stratégies de sécurité des réseaux incluent généralement plusieurs couches de défense, telles que les pare-feu, les systèmes de détection et de prévention des intrusions (IDS/IPS), les systèmes de prévention des pertes de données (DLP) et les solutions de chiffrement des données. En outre, la sensibilisation à la sécurité et la formation des utilisateurs sont essentielles pour réduire les risques liés aux erreurs humaines et aux pratiques de sécurité négligentes.

L'authentification RADIUS (Remote Authentication Dial-In User Service) et la norme 802.1x sont deux technologies essentielles pour renforcer la sécurité des réseaux, qu'ils soient filaires ou sans fil. Ensemble, ces protocoles offrent un mécanisme robuste pour contrôler l'accès au réseau, en garantissant que seuls les utilisateurs autorisés puissent se connecter et accéder aux ressources.

D'autre part, l'authentification RADIUS est un protocole client-serveur largement utilisé pour l'authentification à distance, l'autorisation et la comptabilisation des utilisateurs qui se connectent et utilisent un réseau. Lorsqu'un utilisateur tente de se connecter à un réseau sécurisé, les informations d'identification sont transmises à un serveur RADIUS pour vérification.

Notre objectif dans ce projet est de mettre en place une solution d'authentification qui va permettre de sécuriser l'accès des utilisateurs au réseau de la SARL Collable client de Campus NTS.

Le mémoire est structuré comme suit :

Le premier chapitre a pour but de définir des généralités sur les réseaux informatiques et leur sécurité.

Le deuxième chapitre aborde la présentation de l'organisme d'accueil surnommé Campus NTS qui réalise des solutions aux problématiques des clients en leur apportant des solutions.

Le troisième chapitre consiste à étudier les solutions proposées en s'appuyant sur les protocoles tels que RADIUS, la norme 802.1x et le EAP.

Le quatrième chapitre est consacré à la mise en œuvre de service d'authentification pour le réseau du client SARL Collable proposé par Campus NTS.

Enfin, nous terminons ce mémoire par une conclusion générale dans laquelle nous décrivons les éléments essentiels qui ont été développés et quelques perspectives pour ce projet.

Chapitre 1 : Généralités sur les réseaux et sécurité informatique

Section 1 : Généralités sur les réseaux informatiques

1 Introduction

Un réseau est un moyen de communication qui permet à des individus ou à des groupes de partager des informations et des services. La technologie des réseaux informatiques constitue l'ensemble des outils qui permettent à des ordinateurs de partager des informations et des ressources.

Un réseau est constitué d'équipements appelés nœuds. Ces réseaux sont catégorisés en fonction de leur étendue et de leur domaine d'application, et pour communiquer entre eux, les nœuds utilisent des protocoles, ou langages, compréhensibles par tous.

2 Définition d'un réseau informatique

Un réseau peut être vu comme un ensemble de stations (hôtes) reliées entre elles par des nœuds de communication et des liens de communication (supports). La principale fonction des nœuds de communication est de relayer les paquets d'information vers les autres nœuds (routeur, pont, commutateur, etc.). Les liens de communication assurent le transfert des paquets entre deux nœuds. [1]

3 Topologie de réseaux informatiques [2]

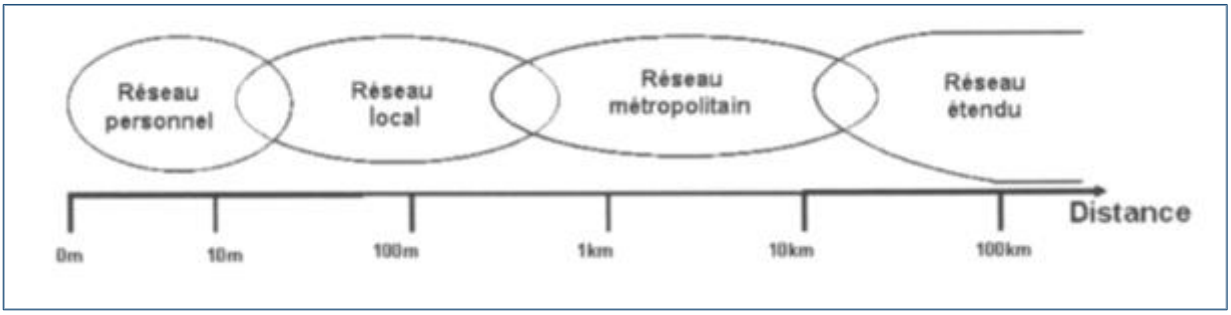


Figure 1.1 : *Topologie de réseaux informatiques*

3.1 Le réseau personnel

La plus petite étendue de réseau est nommée en anglais *Personal Area Network* (PAN). Centrée sur l'utilisateur, elle désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour de celui-ci, le *Personal Operating Space* (POS). Deux autres appellations de ce type de réseau sont : réseau individuel et réseau domestique.

3.2 Le réseau local

De taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, le Local Area Network (LAN), en français Réseau Local d'Entreprise (RLE), relie entre eux des ordinateurs, des serveurs … Il est couramment utilisé pour le partage de ressources communes comme des périphériques, des données ou des applications.

3.3 Le réseau métropolitain

Le réseau métropolitain ou Metropolitan Area Network (MAN) est également nommé réseau fédérateur. Il assure des communications sur de plus longues distances, interconnectant souvent plusieurs réseaux LAN. Il peut servir à interconnecter, par une liaison privée ou non, différents bâtiments distants de quelques dizaines de kilomètres.

3.4 Le réseau étendu

Les étendues de réseaux les plus conséquentes sont classées en Wide Area Network (WAN). Constitués de réseaux de type LAN, voire MAN, les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier.

Le WAN le plus célèbre est le réseau public Internet dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseau.

4 Equipements d'interconnexion

4.1 Carte réseau

La carte réseau constitue l'interface physique entre l'ordinateur et le support de communication. Pour qu'un ordinateur soit mis en réseau, il doit être muni d'une carte réseau.

4.2 Répéteur

Le répéteur appelé REPEATER en anglais, est un équipement qui sert à régénérer le signal entre deux nœuds pour le but d'étendre la distance du réseau. Il est à noter qu'on peut utiliser un répéteur pour relier deux supports de transmission de types différents. Le répéteur est un dispositif actif non configurable et fonctionne au niveau physique.

4.3 Concentrateur / Hub

Le concentrateur appelé HUB en anglais est un équipement physique à plusieurs ports. Il sert à relier plusieurs ordinateurs entre eux. Son rôle c'est de prendre les données reçues sur un port et les diffuser sur l'ensemble des ports. Il comprend généralement un agent SNMP (configurable) et il agit au niveau de la couche physique du modèle OSI.

4.4 Pont (Bridge)

Appelé BRIDGE en anglais est un équipement qui sert à relier deux réseaux utilisant le même protocole. Quand il reçoit la trame, il est en mesure d'identifier l'émetteur et le récepteur, comme ça il dirige la trame directement vers la machine destinataire. Son administration et filtrage configurable à distance (agent SNMP). Il travaille sur les trames au niveau liaison.

4.5 Commutateur

Appelé SWITCH en anglais, est un équipement multiport. Il sert à relier plusieurs équipements informatiques entre eux. Sa seule différence avec le hub, c'est sa capacité de connaitre l'adresse physique des machines qui lui sont connectées et d'analyser les trames reçues pour les diriger vers la machine de destination. Il fonctionne au niveau liaison de données du modèle OSI.

4.6 Routeur

Aussi appelé Router ou Gateway (Passerelle) dans Internet. Un routeur a pour objectif d'interconnecter des sous-réseaux co-localisés ou distants à travers des liaisons longues distances. Il fonctionne au niveau réseau (couche 3 du modèle OSI), c'est-à-dire avec des adresses logiques (administrées).

4.7 Coupe-feux

Aussi appelé pare-feux ou Firewall, il est placé en front d'accès extérieur de manière à protéger le(s) réseau(x) interne(s), il permet une sécurité accrue (Access Control List) en mettant en œuvre des fonctionnalités étendues entre la couche liaison Ethernet et la couche réseau IP par filtrage au niveau trame Ethernet et IP : vérifier si les règles de sécurité (définies par l'administrateur) autorisent le transfert du paquet vers le destinataire et filtrage des requêtes FTP, HTTP, et autres services.

4.8 Passerelle

La passerelle appelée GATEWAY en anglais est un système matériel et logiciel qui sert à relier deux réseaux utilisant deux protocoles et/ou architectures différentes, comme par exemple un réseau local et internet. La passerelle crée un pont entre les deux réseaux. Les informations ne sont pas directement transmises, elles sont plutôt traduites pour assurer la transmission tout en respectant les deux protocoles.

Section 2 : La sécurité des réseaux informatiques

1 Introduction

Depuis quelques années, prenant conscience de la prépondérance du système d'information dans leur fonctionnement les entreprises se montrent plus sensibles à la sécurité de leur réseau informatique. Si au départ le réseau local se trouvait protégé par les murs de l'entreprise, l'apparition des systèmes d'accès distants puis d'internet a radicalement modifié ce fait. Ainsi est apparue la nécessité d'un contrôle accru des accès. A cela s'ajoute désormais le nombre croissant d'entreprises disposant de réseaux Wifi qui augmente le risque d'intrusion.

L'information étant une ressource stratégique pour l'entreprise, sa protection est indispensable car elle permet de :

• Garantir la continuité d'activité de l'entreprise,

• Réduire les dommages éventuels sur l'activité de l'entreprise,

• Maximiser le retour sur investissement des systèmes d'information.

2 Objectifs de la sécurité [3]

Figure 1.2 : *Objectifs de la sécurité informatique*

4.9 Authentification :

Doit permettre de vérifier l'identité d'une entité pour pouvoir assurer son authentification, ainsi seules les personnes autorisées auront accès aux ressources.

4.10 Confidentialité :

La confidentialité des données peut être définie comme la protection des données contre une divulgation non autorisée.

4.11 Disponibilité :

Le bon fonctionnement des services, systèmes et données doivent être accessibles aux ayants droits en continu sans interruption, sans retard, ni dégradation.

4.12 Non-répudiation :

C'est le fait de ne pas pouvoir nier qu'un événement (actions, transactions) a eu lieu.

4.13 Intégrité :

Le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions et services) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle ou accidentelle.

5 Outils et systèmes d'authentification

Est un ensemble de processus et de mécanismes utilisés pour vérifier l'identité d'un utilisateur ou d'un système informatique. L'objectif principal de l'authentification est de garantir que seules les personnes autorisées ont accès à des données sensibles, des systèmes ou des services. Il existe différentes méthodes d'authentification, allant des simples (comme les mots de passe) aux plus complexes (comme la biométrie ou l'authentification par des cartes à puce). Nous allons citer quelques outils et méthodes couramment utilisés :

5.1 Les annuaires

Un annuaire est une bibliothèque mise à jour régulièrement qui regroupe des informations (nom, adresse, coordonnées) sur les membres d'une association, d'une entreprise ou d'un organisme professionnel [4].

5.2 Active Directory

Active Directory est un annuaire système hiérarchique. Il permet de localiser, rechercher et gérer des ressources représentées par des objets de l'annuaire. Il offre des mécanismes de sécurité pour protéger ses informations. Il permet de gérer des ressources liées à la gestion du réseau (domaines, comptes utilisateurs, stratégies de sécurité … etc).

La base de donnée d'AD est distribuée, ce qui lui permet d'améliorer la tolérance aux pannes. Certains produits Microsoft sont installés par défaut (ou fortement conseillés lors de l'installation) comme : DNS serveur web. Active Directory centralise l'authentification. Le contrôle d'accès peut être défini à la fois sur chaque objet de l'annuaire. [5]

5.3 Domaine Windows

Un domaine est l'ensemble d'objets : ordinateurs, utilisateurs et groupes définis par un administrateur réseau. Ces objets partagent une base de données d'annuaire et des stratégies de sécurité. [6]

5.4 Les protocoles d'authentification

Les protocoles d'authentification sont des systèmes et des règles utilisés pour vérifier l'identité des utilisateurs ou des dispositifs dans un réseau informatique. Ils sont essentiels pour la sécurité des systèmes informatiques, car ils permettent de garantir que seuls les utilisateurs autorisés peuvent accéder à des ressources spécifiques.

5.5 Protocole RADIUS (Remote Authentication Dial-In User Service)

Le protocole Radius, mis au point initialement par Livingston, est un protocole d'authentification standard, défini par un certain nombre de RFC **[7]**.

5.6 Ethernet

Ethernet désigne un protocole de réseau local (LAN). Celui-ci se base sur des commutations de paquets et sur des câbles en paires torsadées pour permettre de relier plusieurs machines entre elles. [8]

5.7 Serveur DHCP (Dynamic Host Configuration Protocol)

Le serveur DHCP permet la gestion et la distribution des adresses IP dynamiquement à un ordinateur qui se connecte sur un réseau, son but principal étant la simplification de l'administration d'un réseau. [9]

5.8 Le serveur DNS (Domaine Name System)

Le service DNS permet de faciliter et de standardiser le processus d'identification des ressources connectées aux réseaux informatiques, et il associe un nom à une adresse IP à chaque machine connectée au réseau. [9]

5.9 Politique de sécurité

Une politique de sécurité informatique est une stratégie visant à maximiser la sécurité informatique d'une entreprise. Elle est matérialisée dans un document qui reprend l'ensemble des enjeux, objectifs, analyses, actions et procédures faisant parti de cette stratégie. [10]

6 Méthodes de sécurité

Les méthodes de sécurité sont comme suit :

6.1 La protection par mot de passe :

Pour se connecter au réseau, l'utilisateur doit donner le mot de passe. Cette protection est également très simpliste. Il est facile pour un intrus de capturer le mot de passe et de l'utiliser par la suite pour se connecter au réseau.

6.2 La protection par adresse MAC :

Chaque adaptateur réseau possède une adresse physique unique appelée adresse MAC, représentée par douze chiffres hexadécimaux.

Les points d'accès permettent généralement dans leur interface de configuration, de gérer une liste de droits d'accès basée sur les adresses MAC des équipements autorisés à se connecter au réseau. Le filtrage MAC peut aussi être contourné. Une écoute passive du réseau permet de récupérer les adresses MAC reconnues par le réseau.

6.3 La protection par les certificats :

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

7 Sécurité renforcée

7.1 Mise en place d'un pare-feu

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

7.2 Mise en place d'un VPN

Le VPN permet de simuler un réseau privé via internet en cryptant les paquets entre deux points distant une fois que le tunnel est créé à travers le réseau public (internet), entre deux machines (réseaux), ces derniers peuvent s'échanger des données de manière sécurisée, 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 des lignes spécialisées pour créer le VPN.

7.3 Le cryptage

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

7.3.1 Cryptage symétrique :

Appelé aussi cryptage à clé secrète. Ce type de cryptage utilise la même clé pour crypter et décrypter le message. Le principal problème de cette technique est la distribution de la clé dans un réseau.

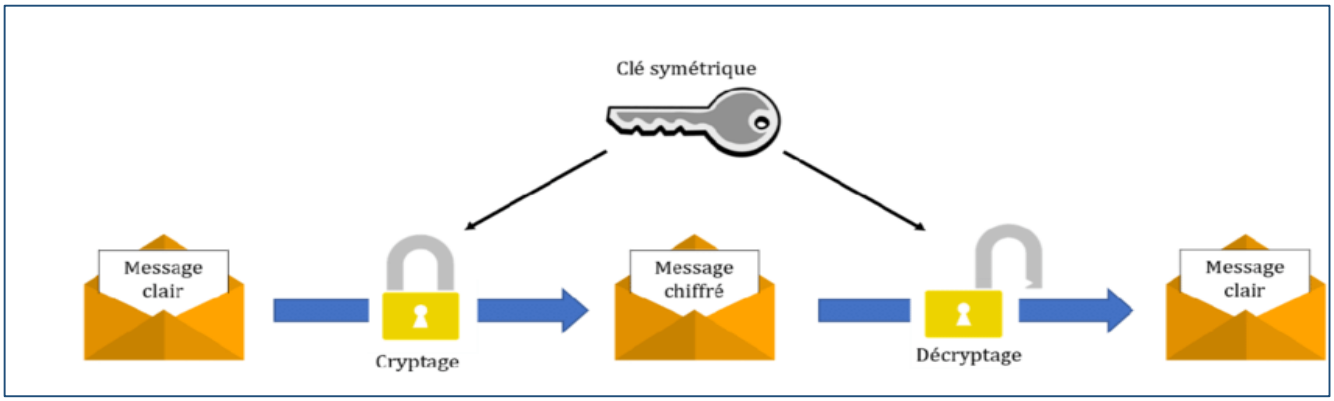


Figure 1.3 : *Cryptage symétrique*

7.3.2 Cryptage asymétrique :

Ce type de cryptage utilise deux clés différentes, une rivée et n'est connue que de son propriétaire et une autre publique et accessible par tout le monde.

Les deux clés (privée et publique) sont liées par l'algorithme de cryptage utilisée. Un message crypté par une clé publique ne peut être décrypté qu'avec la clé privée correspondante.

Le principal avantage de cette technique est de résoudre le problème de l'envoi de clé privée sur le réseau.

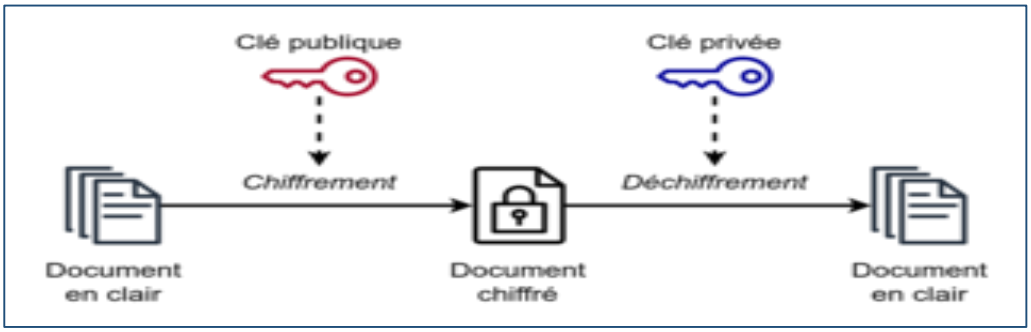


Figure 1.4 : *Cryptage asymétrique*

Conclusion

La dépendance des particuliers et des organisations aux réseaux informatiques et aux technologies internet amènent ces dernières à se confronter à différents degrés de vulnérabilités qui sont loin d'être négligeables. La maîtrise des nouvelles technologies par le grand public engendre un accroissement des menaces et une diversification d'outils d'attaques qui ne cessent de se perfectionner. Il devient donc impératif de mettre en place des mécanismes pour satisfaire au mieux les besoins de la sécurité.

Ce chapitre nous a permis d'avoir une vision globale sur les notions de base du réseau informatique, ainsi la sécurité informatique, ses mécanismes, l'ensemble des aspects qu'elle englobe. Vu que l'intérêt de ce travail est de mettre en place une politique de sécurité basée sur l'authentification, au cours du troisième chapitre, nous aborderons des généralités sur RADIUS et son principe de fonctionnement.

Chapitre 2 : Présentation de l'organisme d'accueil

Introduction

Ce chapitre sera réservé à la présentation de la SARL Collable de Béjaïa, client de l'entreprise Campus NTS (New Technology § Solutions), où nous effectuons notre stage. Dans un premier temps, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Nous étudierons ensuite l'architecture réseau de cette entreprise et ses composants afin de pouvoir suggérer des éventuelles améliorations.

Partie 1 : Présentation de l'entreprise « SARL Collable »

1 Création et évolution

Une entreprise algérienne établie à Béjaïa. Son expertise, dirigée par une équipe compétente, couvre les secteurs du service client, de la technologie, des services financiers, de la vente, du télémarketing et des ressources humaines. Réputés pour sa flexibilité, ses équipes qualifiées et ses infrastructures avancées, elle offre un service de qualité supérieure grâce à son engagement à long terme et à son expérience diversifiée. En tant que centre créé pour les agents, sa position géographique renforce son efficacité et son professionnalisme pour répondre aux besoins de ses clients.

2 Localisation de l'entreprise

Figure 2.1 : *Localisation de l'entreprise SARL Collable*

3 Fiche technique

Le tableau 2.1 ci-dessous représente quelques informations relatives à l'entreprise, dans laquelle, nous avons effectué notre stage de projet de fin d'étude.

Dénomination	SARL Collable
Logo	
Siège	Cité Rachid Aouchiche, Bloc A, route de Boukhiama Tazeboujt Béjaïa.
Secteur d'activités	Centres d´appel, hotline
Numéro de Téléphone	+213 552 478 722
E_mail	Contact@groupecollable.com
Site Internet	https://groupecollable.com/

***Tableau 2.1** : Identification sur SARL Collable*

4 Objectifs, Missions et activités de l'Entreprise

Les objectifs, les missions et les activités sont représentées dans la figure ci-dessus :

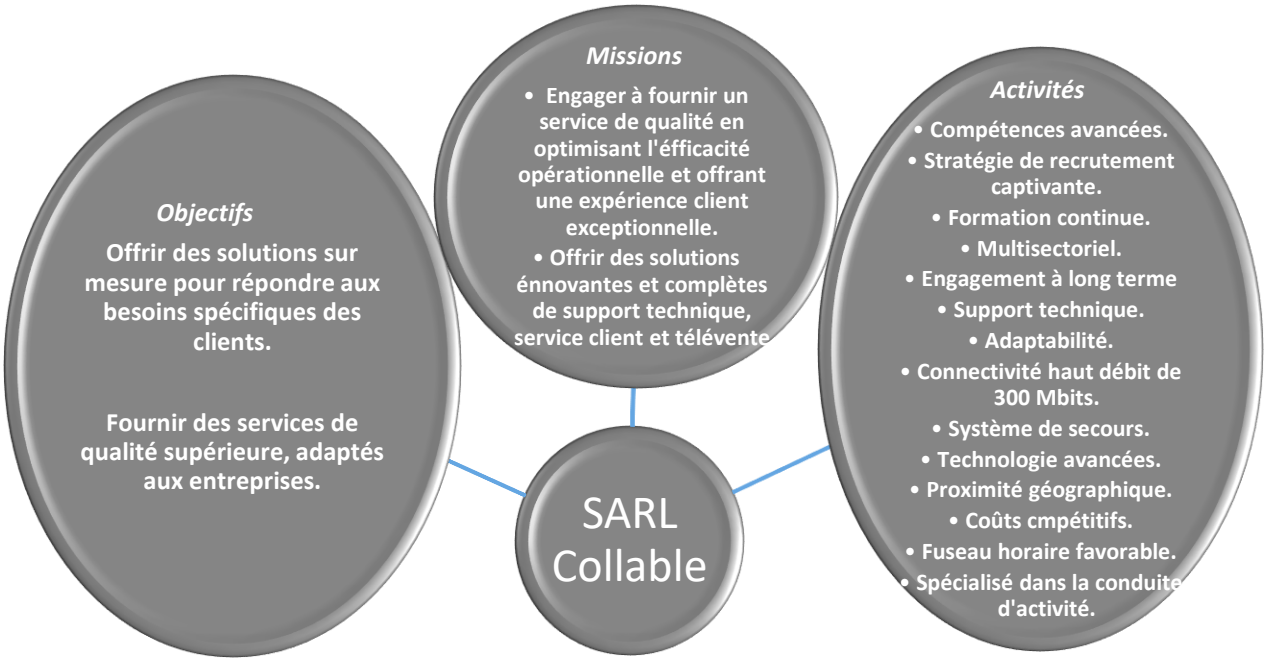


***Figure 2.2 :** Objectifs, missions et activités de SARL Collable*

5 Organigramme général de l'organisme d'accueil

Nous allons nous contenter de présenter ci-dessous la description de l'organigramme du campus NTS (voir la figure 3) dans lequel les apprentis effectuent le stage.

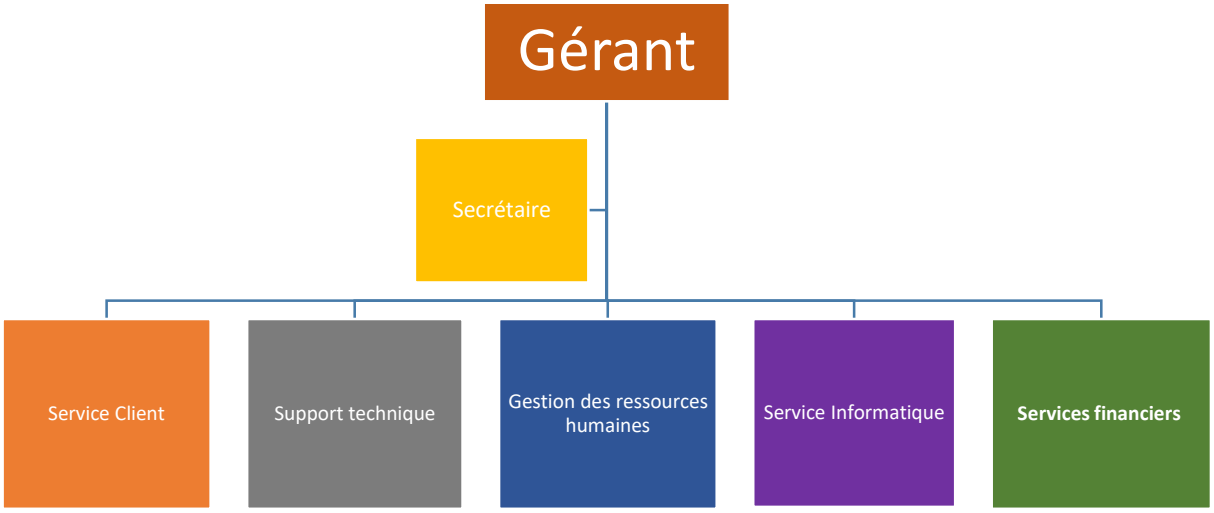


***Figure 2.3** : Organigramme de SARL Collable*

5.1 Service client

- Assistance multicanale 24/7.
- Gestion des plaintes et des retours.
- Formation continue du personnel.

5.2 Support technique

- Expertise technique pointue dans une variété de domaines.
- Dépannage rapide et précis.
- Mise en place de solutions de suivi et de surveillance …

5.3 Gestion des ressources humaines

- Recrutement stratégique et gestion RH.
- Développement professionnel continu.
- Tenue des livres précise et conforme aux normes locales et internationales.

5.4 Service informatique

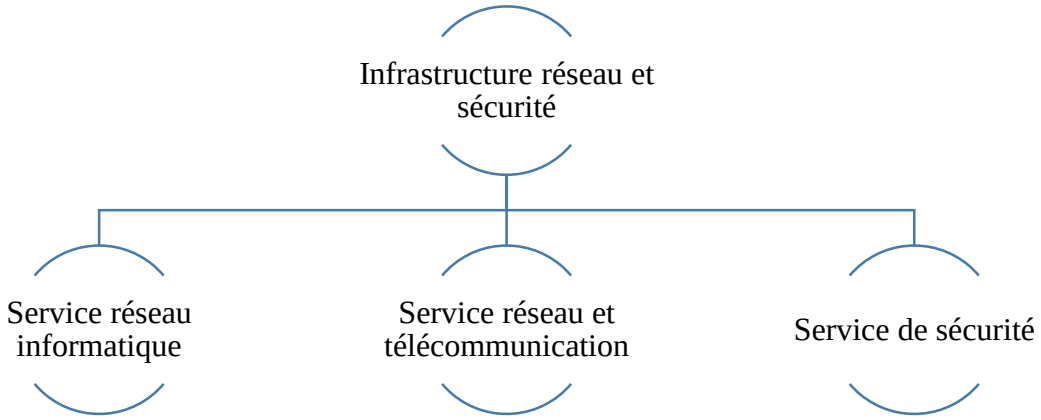


Figure 2.4 : *Organigramme de service d'accueil*

➢ **Service réseau**

Ce service contient 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

5.5 Services financiers

- Analyse financière approfondie.
- Assistance dans la planification budgétaire et fiscale.
- Comptabilité.

Partie 2 : État des lieux (SARL Collable)

1 Présentation du réseau SARL 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 de la SARL Collable :

1.1 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 :

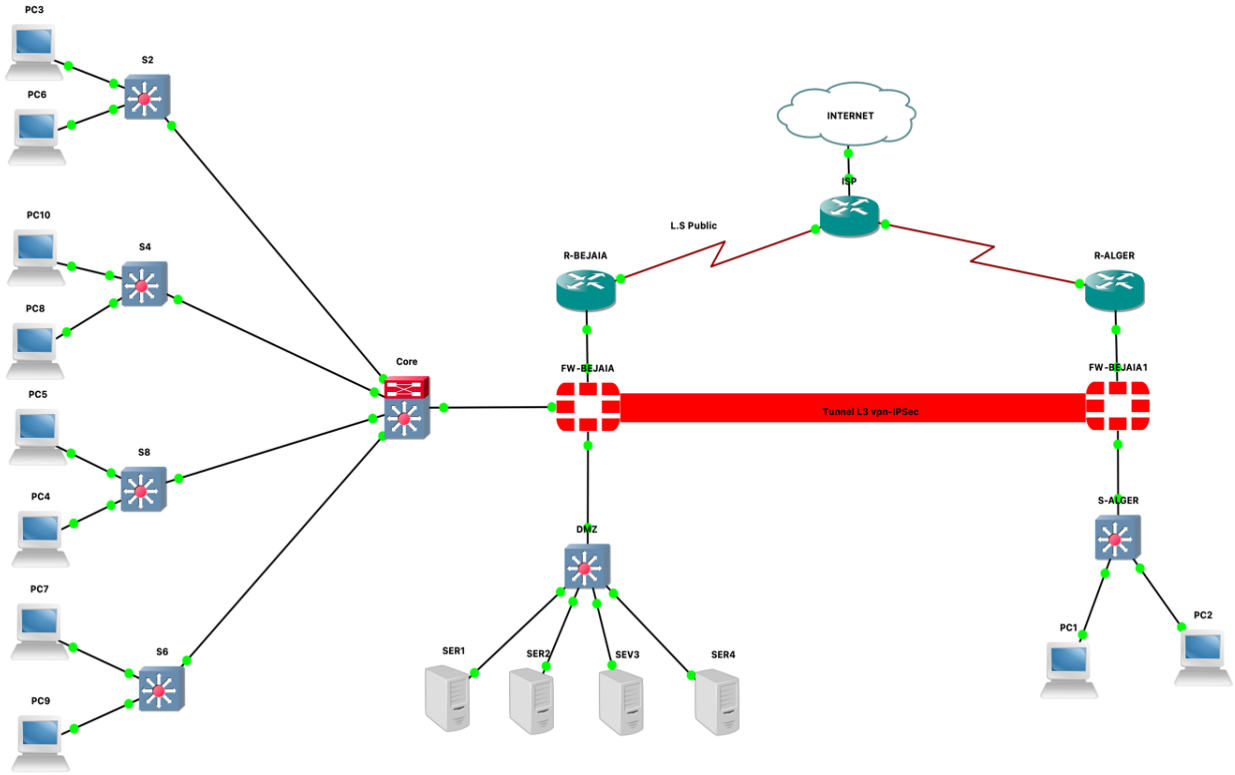


Figure 2.5 **:** *Architecture du réseau de la SARL Collable*

1.2 Analyse du parc informatique

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

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

Tableau 2.2 : *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
Serveur 	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)
Terminaux  	Dell IAER 35 R	• **AMD core :** i5 8th génération • **RAM :** 8GO • **Disque :** 256GO • **Ecran :** UHD Graphies 620 ($1920 \times 1080 \times 32b$)

Tableau 2.3 : *Détails des ressources disponibles de l'entreprise*

Partie 3 : Problématique et solution proposée

1 Problématique

Lors de notre stage à Bejaia entreprise NTS, nous avons constaté qu'il dispose d'un réseau local de diverses plates-formes, de différents services, nous avons pu mettre en évidence des pannes de réseau, à savoir :

- La plupart des ports de commutateur se trouve sur le VLAN Physique, ce qui risque d'augmenter les domaines de diffusion et de compromettre la sécurité. Contredit, l'objectif de l'utilisation des VLANs, qui est de micro-segmenter le réseau en petits domaines de diffusion.
- Les adresses IP attribuées dans les différents sites de l'entreprises ne sont pas masquées.
- L'entreprise s'étend à des sites distants et à plusieurs centres de distribution. Il dispose donc d'un réseau important et nécessite une interconnexion permanente fiable et privée entre ces différents sites.
- Absence de point de centralisation et de gestion des comptes et droit des accès systèmes.
- Absence de contrôle d'accès pour certains sites Web gourmands en bande passante qui réduit la vitesse à laquelle les employés travaillent.
- Pas d'accès à distance sécurisé aux équipements depuis l'intranet et l'extranet de l'infrastructure réseau.
- Les ports physiques sont ouverts qui permet d'avoir un accès facile au réseau.

2 Solution

Le principal défi d'une architecture de réseau sécurisée est de pouvoir réguler l'accès aux ressources réseau à partir du réseau local et de l'extérieur, tout en limitant autant que possible les vulnérabilités aux éventuelles attaques ou vol d'informations afin d'améliorer la sécurité du réseau local. Pour cela, nous avons proposé différentes solutions en se basant sur le modèle de référence OSI (Sécurités par niveau) :

- Niveau 01 (physique) :
  - Mise en place d'une salle technique pour les armoires, des contrôles d'accès, détection d'incendie, caméras de surveillance, câblage blindé et encastré.

- Niveau 02 (liaison de données) :
  - Mise en place du filtrage par adresse MAC en utilisant la technique ports Security
  - Authentification des ports physique via la norme 802.1x en utilisant l'authentification Radius par Certificat TLS et le protocole AAA (*Authentication, Authorization, Accounting/Auditing*).

- Niveau 03 (Réseau) :
  - Mise en place des VLANs pour améliorer la sécurité du réseau et réduire les tempêtes de diffusion ARP.
  - Mise en place d'un Canal sécurisé de bout en bout entre le site de Bejaia et celui d'Alger en utilisation le protocole IPSec (IP sécurisé) pour avoir la confidentialité, l'intégrité et l'authentification des données circulant sur le réseau internet.

- Niveau 04 (Transport) :
- Mise en place d'un firewall afin de contrôler, gérer et sécuriser les ports logiques ouverts sur le réseau externe.

- Niveau (05-06-07) (Application) :
- Mise en place du protocole VPN SSL pour sécuriser les accès à distance aux équipements d'interconnexion depuis l'externe
- Mise en place d'un Proxy (Hard) pour un filtrage des sites WEB et Applicatif.

Conclusion

Dans ce chapitre, nous avons donné un aperçu général de la SARL Collable, puis nous avons découvert des problèmes qui nous ont amenés à rechercher et à mettre en œuvre une nouvelle architecture de réseau sécurisée par l'authentification RADIUS. Enfin, l'application de la solution proposée fera l'objet du chapitre suivant.

Chapitre 3 : Radius et la norme 802.1x

1 Introduction

Le but de ce chapitre est de présenter les protocoles d'authentification RADIUS et la norme 802.1x qui permettent aux opérateurs d'authentifier des utilisateurs, de leur autoriser certains services et d'assurer la sécurité.

2 Protocole RADIUS

RADIUS avait tout d'abord pour objet de répondre aux problèmes d'authentification pour des accès distants, par liaison téléphonique, vers les réseaux des fournisseurs d'accès ou des entreprises. C'est de là qu'il tient son nom qui signifie « Remote Access Dial In User Service ». Au fil du temps, il a été enrichi et aujourd'hui il peut être utilisé pour authentifier les postes de travail sur les réseaux locaux, qu'ils soient filaires ou sans fil. Le protocole RADIUS est décrit dans la RFC 2865 de l'IETF (Internet Engineering Task Force).

RADIUS est un système client/serveur qui permet de sécuriser des réseaux contre des accès à distance non authorisés.il répond au modèle AAA résumant ses trois fonctions comme suit :

A = Authentication : authentifier l'identité du client ;

A = Authorization : accorder des droits au client ;

A = Accounting : enregistrer les données de comptabilité de l'usage du réseau par le client. [7]

3 Fonctionnement de RADIUS

Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau en utilisant le protocole UDP et les ports 1812 et 1813. Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, Active Directory, annuaire LDAP, etc.) et 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. [7]

Le scénario du principe de fonctionnement est le suivant :

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 » (en anglais « challenge ») ;
CHANGE PASSWORD : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

4 Format de l'en tête du paquet RADIUS

Code	Identifier	Length
Request authenticator		
/		
Response authenticator		
Attributes		

Code (1 octet):

1 : access-request
2 : access-accept
3 : access-reject
4 : accounting-request
5 : accounting-response
11 : access-challenge

Length (2 octets):

- Taille totale du message (de 20 à 4096 octets)

Identifier (1 octet) :

- Unique pour chaque authentification

Request Authenticator (16 octets):

- Identique pour une retransmission
- Un nombre aléatoire unique

Response Authenticator (16 octets):

MD5 (Code + ID + Length + RequestAuth + Attributes + Secret)

Les attributs :

Type	Length	Value
Type (1 octet):	**Length (1 octet):**	**Value (1 – 253 octets) :**
1 : User-Name	- Taille totale du message (max 254 octets)	text 1-253 octets
2 : User-Password		string 1-253 octets
3 : CHAP-Password		address 32 bits
4 : NAS-IP-Address		integer 32 bits
5 : NAS-Port		time 32 bits
6 : Service-Type …		

User-Password :

Le mot de passe est coupé en blocks de 16 octets : p1, p2,…

c1 = p1 XOR MD5(Secret + Request Authenticator)

c2 = p2 XOR MD5(Secret + c1)

Le mot de passe encodé est la concaténation de : c(1)+c(2)+..

5 Rôle de protocole RADIUS

- Authentifier et autoriser l'accès des utilisateurs à un réseau, qu'il soit distant ou sur site.
- Centraliser les données d'authentification de tous les utilisateurs dans le même serveur.
- Placer les machines dans des sous-réseaux virtuels.
- Assurer plusieurs moyens d'authentification.
- Initialiser les algorithmes de chiffrement des communications (WPA).

6 Caractéristiques de RADIUS

Les caractéristiques principales de Radius sont :

- Modèle client/serveur.
- Sécurité réseau.
- Mécanismes flexibles d'authentification.
- Protocole extensible.

6.1 Modèle client/serveur

Un serveur d'accès de réseau NAS fonctionne en tant que client Radius. Le client est responsable pour passer l'information de l'utilisateur vers les serveurs Radius, et puis d'effectuer les traitements en fonction de la réponse qui est retournée. Les serveurs Radius sont chargés de recevoir les demandes de connexion d'utilisateur, d'authentifier l'utilisateur, et puis de renvoyer toute l'information de configuration nécessaire pour que le client puisse fournir le service à l'utilisateur.

6.2 Sécurité réseau

Les transactions entre le client et le serveur Radius sont authentifiées par l'utilisation d'un secret partagé, qui n'est jamais envoyé en dehors du réseau. En outre, tous les mots de passe utilisateur sont envoyés chiffrés entre le client et le serveur, pour éliminer la possibilité que quelqu'un sur un réseau suffisamment sécurisé puisse espionner le transit réseau pour déterminer le mot de passe d'un utilisateur.

6.3 Mécanismes flexibles d'authentification

Le serveur Radius peut supporter une variété de méthodes pour authentifier un utilisateur. Quand on lui fournit le nom d'utilisateur et le mot de passe initial donnés par l'utilisateur, il peut supporter la procédure de connexion de PPP, PAP, CHAP, login Unix ou d'autres mécanismes d'authentification.

6.4 Protocole extensible

Toutes les transactions sont composées de triplets (Attribut, Longueur, Valeur), des nouvelles valeurs d'attribut peuvent être ajoutées sans perturber les implémentations existantes du protocole.

7 Avantages de RADIUS

- **Sécurité forte :** L'utilisation d'un certificat Radius permet de demander à toute personne souhaitant se connecter au réseau de s'authentifier, il consiste à faire présenter un certificat électronique dont la validité sera vérifiée par le serveur. Chaque utilisateur aura son propre certificat. La transaction entre un client radius et le serveur radius est cryptée.
- **Fiabilité :** La méthode d'authentification par certificat est très fiable.
- **Administré :** Radius permet de centraliser des données d'authentification.

8 Protocole RADIUS et la couche de transport UDP

Le protocole établit une couche applicative au-dessus de la couche de transport UDP.

Les ports utilisés sont :

• 1812 pour recevoir les requêtes d'authentification et d'autorisation.

• 1813 pour recevoir les requêtes de traçabilité.

Le Protocol Radius utilise le protocole UDP. Pourquoi UDP ?

• Il permet la réémission d'une demande d'authentification à un serveur secondaire si le serveur primaire ne répond pas.

• Radius est un protocole sans état.

• UDP simplifie la mise en œuvre du serveur.

9 Éléments d'authentification Radius

• **Authentification avec l'adresse Ethernet (adresse MAC)**

L'authentification par adresse MAC, appelée Radius-MAC, est la plus simple à mettre en œuvre. En revanche, c'est la moins sûre. La figure ci-dessous représente un réseau sur lequel est connecté un serveur Radius et un poste de travail par l'intermédiaire « commutateur ».

Les étapes du protocole sont :

1. Le poste de travail se branche sur un des ports du commutateur.

2. Le commutateur détecte cette connexion et envoie une requête d'authentification (Access-Request) au serveur Radius. Dans cette requête, l'adresse MAC du poste de travail fait office d'identifiant.

3. Le serveur reçoit ce paquet et utilise l'adresse MAC comme point d'entrée dans sa base de données.

4. Le serveur envoie sa réponse au commutateur. Si elle est négative (Access-Reject), le port du commutateur reste fermé et le poste n'est pas connecté au réseau. Si la réponse est positive (Access-Accept), elle contient le numéro de VLAN autorisé. Le commutateur ouvre alors le port sur ce VLAN et le poste peut commencer à travailler. Donc, dans ce type d'authentification, il n'y a pas de communication entre le poste de travail et le serveur Radius.

Tous les échanges interviennent entre le commutateur et le serveur.

Dans le cas des réseaux sans fil, le schéma est exactement le même. Certes, il n'y a pas de port physique, mais l'opération d'association est équivalente au "branchement " d'un poste sur la borne. Celle-ci crée alors un port virtuel et tout se passe ensuite comme en filaire. Le serveur dialogue avec la borne exactement comme avec un commutateur. [11]

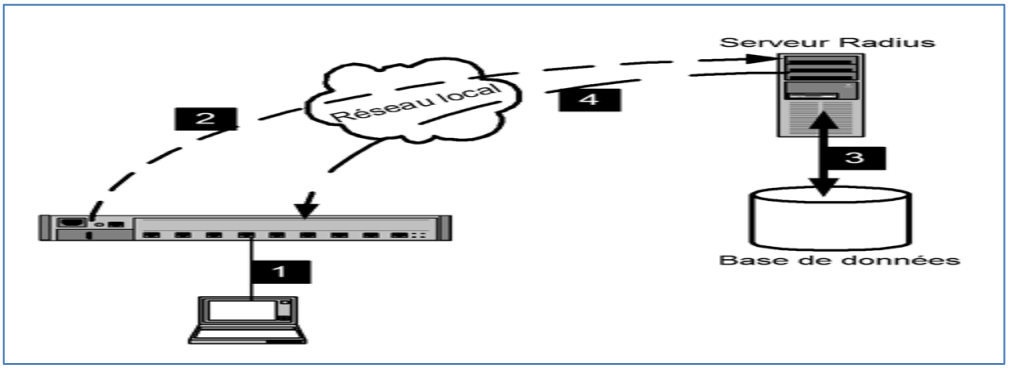


Figure 3.1 **:** *Principes de l'authentification Radius-Mac*

• Authentification avec 802.1x (EAP)

Le schéma général de l'authentification 802.1X ressemble à celui de Radius-MAC, les deux méthodes sont, en réalité, très différentes. L'authentification 802.1X est plus compliquée et délicate à mettre en œuvre.

Tout d'abord, la différence la plus importante est que, cette fois, un logiciel particulier sera indispensable sur le poste de travail. Ce logiciel est appelé supplicant. Suivant le schéma de la figure ci-dessous, c'est lui qui va envoyer (1) vers le serveur Radius les éléments d'authentification (certificat, identifiant, mot de passe. . .).

Cependant, il ne communique pas directement avec le serveur. C'est le commutateur qui va servir d'intermédiaire (2), car il connaît l'adresse du serveur.

Pour interroger sa base de données (3), le serveur Radius a besoin d'un identifiant qu'il utilise comme point d'entrée. Dans ce cas, il ne s'agira pas de l'adresse MAC. L'identifiant sera configuré et envoyé par le supplicant. [15]

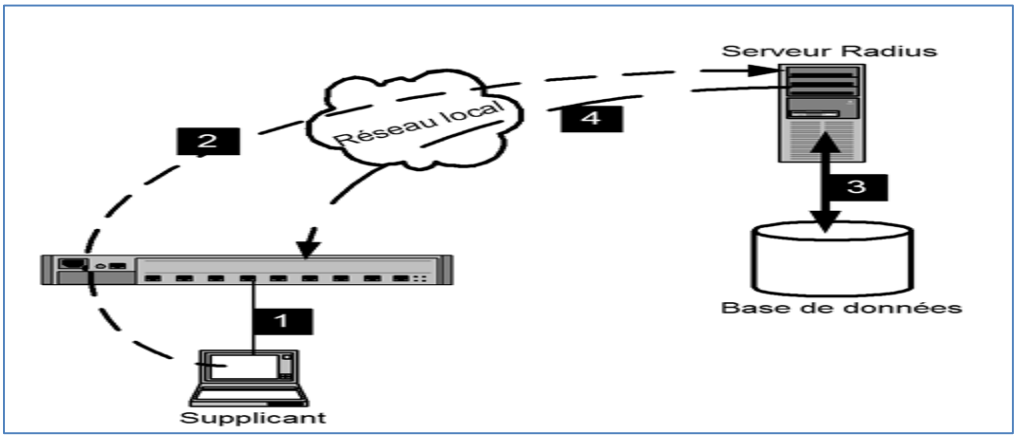


Figure 3.2 **:** *Principes de l'authentification 802.1x*

Comme précédemment, le serveur accepte ou refuse l'authentification et renvoie sa réponse au commutateur (4). Et celui-ci ouvre le port sur le VLAN commandé par le serveur. Mais l'opération est complètement différente du cas précédent.

Avec Radius-MAC, l'authentification est réalisée sans aucune communication entre le poste de travail et le serveur. En 802.1X, dans la mesure où c'est le supplicant qui envoie les éléments d'authentification, il y a bien une communication.

Or, comment peut-il y avoir une communication, et donc un trafic réseau, puisque le port du commutateur n'est pas ouvert et qu'il ne le sera que lorsque le poste aura été authentifié ?

C'est justement là que tient tout le protocole 802.1X. Les ports du commutateur seront configurés d'une façon particulière. Avant d'être complètement ouverts, ils ne laisseront passer qu'un seul type de protocole EAP. D'ailleurs, l'autre nom de 802.1X est « Port-Based Network Access Control » qui, traduit littéralement, signifie « Accès au réseau basé sur le contrôle de port ».

Tout se passe comme si chaque port était coupé en deux. Une moitié est appelée port contrôlé au départ, elle est maintenue fermée par le commutateur.

L'autre moitié est appelée port non contrôlé. Par cette voie, le commutateur n'accepte que le protocole EAP.

Dans notre cas, nous avons choisi l'authentification Radius 802.1x par identifiant et mot de passe. [11]

a. Port non contrôlé

Au début de la connexion, le port est dans l'état non contrôlé. Seuls les paquets 802.1X permettant d'authentifier le client qui sont autorisés (figure ci-dessous).

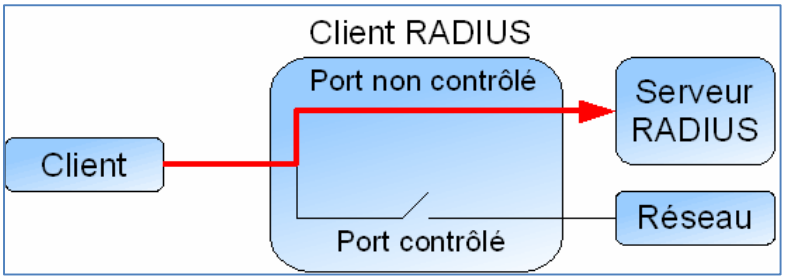


Figure 3.3 **:** *Etat du port avant la phase d'authentification*

b. Port contrôlé

Une fois l'authentification effectuée, le port passe dans l'état contrôlé. Alors, tous les flux du client sont acceptés et le client peut accéder aux ressources partagées (figure ci-dessous).

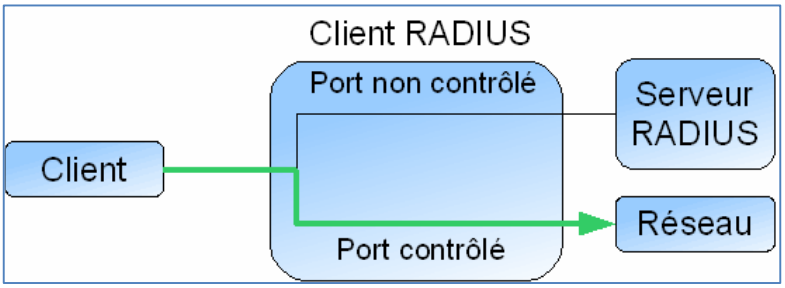


Figure 3.4 **:** *Etat du port après une authentification réussie*

10 La norme IEEE 802.1X

10.1 Définition

Le standard 802.1x est une solution de sécurisation, mise au point par l'IEEE en juin 2001. Il permet d'authentifier les équipements connectés sur un port avant d'accéder à un réseau (sans fils ou filaire) grâce à un serveur d'authentification. Il repose sur le protocole **EAP (Extensible Authentication Protocol).** [12]

Le 802.1x se base sur trois éléments :

- **Supplicant :** le client demande à s'authentifier avant de pouvoir accéder aux ressources du réseau.
- **Authenticator :** l'authentificateur est l'équipement réseau (commutateur, point d'accès…) auquel le client se connecte. Suivant la réponse du serveur d'authentification, le commutateur laissera passer ou non le trafic du client.
- **Authentication server :** le serveur d'authentification vérifie sur demande du commutateur si le demandeur peut ou non accéder aux ressources réseau LAN.

10.2 Les méthodes d'authentification de 802.1x

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

11 Le protocole EAP

La communication entre l'équipement réseau (authenticator) et le serveur d'authentification est assurée par le protocole EAP (Extensible Authentication Protocol) qui assure le transport des informations d'authentification et permet d'utiliser les différentes méthodes d'authentification d'où le terme '' Extensible''.

Le domaine d'application de ce protocole correspond donc à tous les modes de connexion pouvant être considérés comme des connexions dites point à point telles que: connexion réseau sans fil entre un poste utilisateur et une borne d'accès Wifi.

On distingue deux types de trafic EAP :

• **EAP over LAN (EAPOL) :** entre le système à authentifier et le point d'accès.

• **EAP over Radius :** entre le point d'accès et le serveur d'authentification.

11.1 Les méthodes associées à EAP

Le protocole EAP ne propose qu'une seule méthode d'authentification c'est-à-dire qu'il utilise ces différents éléments pour identifier un client :

- Le login / mot de passe
- Le certificat électronique
- La biométrie
- Une puce (SIM)

Certaines méthodes combinent plusieurs critères (certificat et login/mot de passe…). En plus de l'authentification, EAP gère la distribution dynamique des clés de chiffrement. Parmi les méthodes de l'authentification les plus communes sur EAP, on distingue :

• EAP-TLS (EAP Transport Layer Security)

EAP-TLS est implémenté chez de nombreux fabricants de matériel sans fil, il utilise deux certificats numériques, le serveur et le client s'authentifient mutuellement tout en cryptant les données échangées dans cette phase d'authentification. L'utilisation de clés publiques et privées des deux côtés permet de créer un tunnel sécurisé entre les deux parties, ce qui garantit l'intégrité des données. Avec ce principe le client ne fournit pas de mot de passe puisque le certificat permet l'authentification.

L'utilisation de certificat possède des avantages et des inconvénients. Ils sont souvent considérés comme plus sûrs que les mots de passe, cependant la distribution des certificats aux clients est une contrainte qu'il ne faut pas négliger.

• EAP-TTLS (EAP Tunneled Transport Layer Security) et EAP-PEAP (Protected EAP)

Ces deux méthodes sont assez similaires, elles s'appuient sur la confidentialité proposée par l'encapsulation dans un tunnel pour réaliser une authentification via login/mot de passe.

On distingue deux phases d'authentification :

Première phase : identification du serveur par le client en utilisant un certificat validé par une autorité de certification.

Deuxième phase : identification du client par le serveur par login/password.

À l'issue de la première phase, le tunnel TLS chiffré s'établit, garantissant une grande confidentialité des échanges pour la deuxième phase où le client transmet ses éléments

d'authentification (login/password) via le CHAP, PAP, MS-CHAP ou MS-CHAPv2 pour EAP-TTLS et MS-CHAPv2, token-card ou certificat (similaire à EAP-TLS) pour EAP-PEAP.

La différence entre EAP-PEAP et EAP-TTLS vient de la manière d'encapsuler les échanges lors de la deuxième phase. Pour EAP-PEAP, les données échangées entre le client et le serveur au travers du tunnel TLS sont encapsulées dans des paquets EAP. EAP-TTLS utilise des AVP (Attribute-Values Pairs) encapsulées dans des paquets EAP-TTLS.

L'avantage présenté par ces deux méthodes est que le client peut être authentifié par mot de passe, on supprime donc la complexité de gestion liée aux certificats caractéristique d'EAP-TLS, tout en proposant une authentification mutuelle.

• EAP-MD5 (EAP Message Digest 5-Challenge)

Cette méthode ne propose pas une authentification mutuelle, le client s'authentifie simplement en fournissant un couple login/mot de passe. Grace au mécanisme de challenge/réponse, le serveur envoie un challenge au client, celui-ci renvoie son mot de passe associé au challenge, le serveur compare le résultat avec le mot de passe qu'il détient dans sa base de données, si le résultat est identique alors l'accès est autorisé, sinon il est refusé.

Le problème majeur de cette méthode réside dans le fait que les échanges ne sont pas chiffrés, en outre EAP-MD5 ne gère pas la distribution dynamique des clés WEP.

Le seul avantage de cette méthode est la simplicité : il est relativement facile de mettre en place une structure d'authentification basée sur cette méthode, celle-ci est d'ailleurs beaucoup utilisée pour des réseaux filaires où la contrainte liée au chiffrage des échanges est moins forte que pour les réseaux wifi.

• LEAP (Light weight EAP)

C'est une implémentation assurant une authentification simple par mot de passe via une encapsulation sécurisée. Ce protocole est vulnérable aux attaques (cryptage MD5) sauf si l'utilisateur utilise des mots de passe complexes.

11.2 Les protocoles de transport sécurisés [12]

Un protocole de transport sécurisé permet de porter l'information d'un lieu à un autre suivant des règles prédéfinies sans que l'objet transporté ne soit en danger.

Étant donné que la majorité des réseaux utilisés à travers le monde sont de type TCP/IP et que le choix des entreprises se porte souvent vers ce type de réseau, nous présentons les protocoles sécurisés suivants :

11.2.1 Le protocole PPP

Le 802.1x est une pyramide de protocoles dont la base est l'EAP. Pour bien comprendre l'EAP, il faut revenir à son origine : quand on lance une connexion à Internet via un modem téléphonique classique, l'ordinateur commence par établir une connexion avec une centrale téléphonique composée d'une batterie de modems eux-mêmes reliés à Internet. Cette centrale, mise en œuvre par un Fournisseur d'Accès à Internet (FAI) s'appelle un point de présence (Point of Presence, PoP). La connexion entre notre modem et l'un des modems du PoP repose sur un protocole très répandu : le Protocole de Point à Point PPP (Point-to- Point Protocol).

Le PPP définit notamment comment un client doit s'identifier : un mot de passe est attribué par le FAI, et ce client doit prouver qu'il le connaît. Si c'est le cas, le PoP lui autorise l'accès vers Internet, sinon, la connexion est interrompue.

11.2.2 Le protocole PAP

Le Protocol PAP (Password Authentication Protocol), utilisé avec le protocole PPP, permet d'identifier un utilisateur auprès d'un serveur PPP en vue d'une ouverture de connexion sur le réseau. Après une phase de synchronisation entre le client et le serveur pour définir l'utilisation du protocole PPP et PAP, le processus d'authentification se fait en deux étapes :

- Le client envoie son nom PAP ainsi que son mot de passe en clair.
- Le serveur qui détient une table de noms d'utilisateurs et de mots de passe vérifie que le mot de passe correspond à l'utilisateur et valide ou rejette la connexion.

PAP est le plus simple des protocoles d'authentification car il est très facile à implémenter. Mais étant donné que le mot de passe circule en clair sur le réseau, c'est aussi le moins sécurisé et il est donc fortement déconseillé car il ne procure aucune sécurité. D'autre part, même si le mot de passe est crypté, il est toujours possible d'utiliser un sniffer afin de capturer la requête d'authentification.

11.2.3 Le protocole CHAP

Le protocole CHAP (Challenge Handshake Authentication Protocol) est défini dans la RFC 1994. Le serveur commence par envoyer un « défi » au client (16 octets aléatoires) ainsi qu'un compteur qu'il incrémente à chaque fois qu'il lance un défi. Le client doit passer le compteur, son mot de passe et le défi au travers de l'algorithme de hachage MD5. Le résultat est une séquence de bits pseudo-aléatoires appelé le « hash » de 16 octets. Cet hash est envoyé

au serveur, qui peut effectuer le même calcul et vérifier si son résultat concorde avec celui du client.

Cet algorithme permet d'éviter que le mot de passe soit transféré, et qu'un pirate ne répète une authentification réussie qu'il aurait enregistrée auparavant. Puisque le défi change à chaque authentification il ne permet pas au client de s'assurer de l'identité du serveur.

11.2.4 Le protocole MS-CHAP

Ce protocole, souvent appelé MS-CHAP-v1, a été défini par Microsoft dans la RFC 2433. Il s'agit d'une variante de CHAP destinée à améliorer la sécurité. L'un des problèmes de CHAP est qu'il faut stocker le mot de passe en clair sur le serveur : sinon, il est impossible de calculer le hash et de vérifier l'identité du client. Toute personne ayant accès à la base de données des utilisateurs peut donc voir les mots de passe de tout le monde. Pour éviter cela, MS-CHAP spécifie que le serveur ne doit pas stocker le mot de passe, mais le résultat d'un hash sur ce mot de passe (selon un algorithme propriétaire de Microsoft).

Lorsque l'utilisateur saisit son mot de passe, celui-ci doit d'abord passer au travers du même algorithme de hash avant de suivre la procédure habituelle de CHAP.

Malheureusement, MS-CHAP comporte des failles de sécurité dues au hash propriétaire de Microsoft, qui l'ont rendu rapidement obsolète : seuls quelques vieux systèmes Windows 95/98 l'utilisent encore.

11.2.5 Le protocole MS-CHAP-v2

Suite à la découverte des failles de sécurité dans MS-CHAP, Microsoft a réagi en concevant cette version 2, définie dans la RFC 2759. Plus robuste, ce protocole fournit notamment un mécanisme d'authentification mutuelle : le serveur s'assure de l'identité du client, et vice versa, ce qui n'est pas le cas avec les méthodes d'authentification précédentes.

Le MS-CHAP-v2 est largement utilisé dans les réseaux, Windows depuis la version Windows 2000.

Conclusion

L'authentification RADIUS est un élément clé de la sécurité des réseaux informatiques, offrant une gestion centralisée, des fonctionnalités de sécurité avancées et une interopérabilité étendue entre les équipements du réseau.

Chapitre 4 : Réalisation

1 Introduction

Ce chapitre consiste à mettre en œuvre les solutions proposées pour la réalisation de notre projet, en exposant les différentes configurations nécessaires à implémenter sur le LAN. Ces configurations entourent entre la configuration des VLANs, VTP et le routage inter vlan en suit on a configuré le serveur de gestion et administration (AD), DNS et DHCP, ensuite la partie VPN et VPN Mobile en se basant sur le logiciel open source GNS 3, l'hyperviseur VMware Workstation et l'application Open vpn. Pour présenter les configurations que nous avons réalisées, nous nous sommes servies des captures d'écran qui illustrent les étapes de la configuration afin d'éclaircir chaque composant de cette dernière et son fonctionnement. Enfin, des tests de validation sont effectués pour confirmer le bon fonctionnement du réseau seront réalisés.

2 Présentation de l'environnement de travail

2.1 Installation de GNS3 sous Windows :

GNS3 (Graphical Network Simulator 3) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques. [13]

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

Figure 4.1*: *GNS 3

2.2 Installation de VMware Workstation pro

VMware Workstation est un outil de virtualisation, il permet de créer de nouvelles machines virtuelles, transformer un PC en une machine virtuelle et effectuer un déploiement en masse.

Afin de créer les machines utilisateurs virtuelles au sein du même pc, nous sommes appelés à installer VMware Workstation en suivant les étapes d'installations jusqu'à la fin puis cliquer sur le bouton « terminer ». La figure 4.2 présente L'interface graphique de VMware Workstation pro.

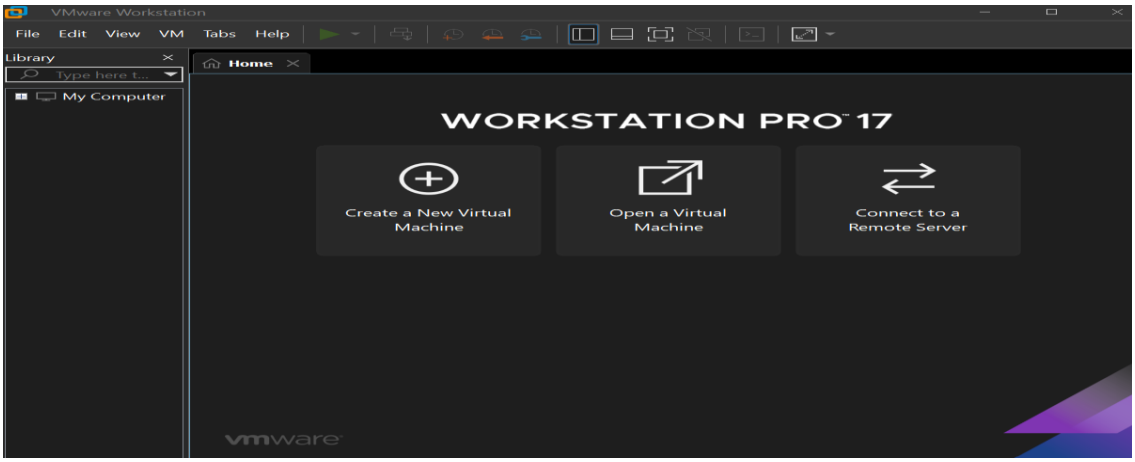


Figure 4.2: *Interface graphique de VMware Workstation pro 17*

2.3 Wireshark

C'est un outil de capture et d'analyse de paquets réseau Open Source destiné aux administrateurs réseau et aux développeurs, Wireshark est une référence en matière d'analyse des transactions réseau. Cet outil puissant supporte plusieurs centaines de protocoles et dispose de fonctions de filtrage avancées pour la capture et l'interprétation des données. [14]

La figure 4.3 présente l'interface graphique de Wireshark.

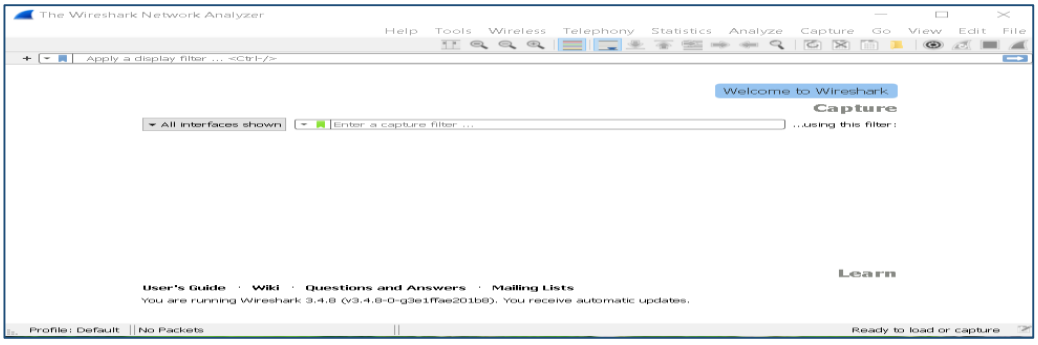


Figure 4.3 : *Interface graphique de Wireshark*

2.4 Les machines virtuelles

2.4.1 Le pfSense

PfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états Packet Filter ainsi que des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques.

Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise.

2.4.2 Windows server 2022

Windows Server 2022 est l'actuel système d'exploitation commercialisé par Microsoft et destiné aux serveurs. Le système offre une sécurité multicouche avancée, des fonctionnalités hybrides avec Azure et une plateforme d'application flexible.

2.4.3 Windows 10

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

3 Architecture proposée

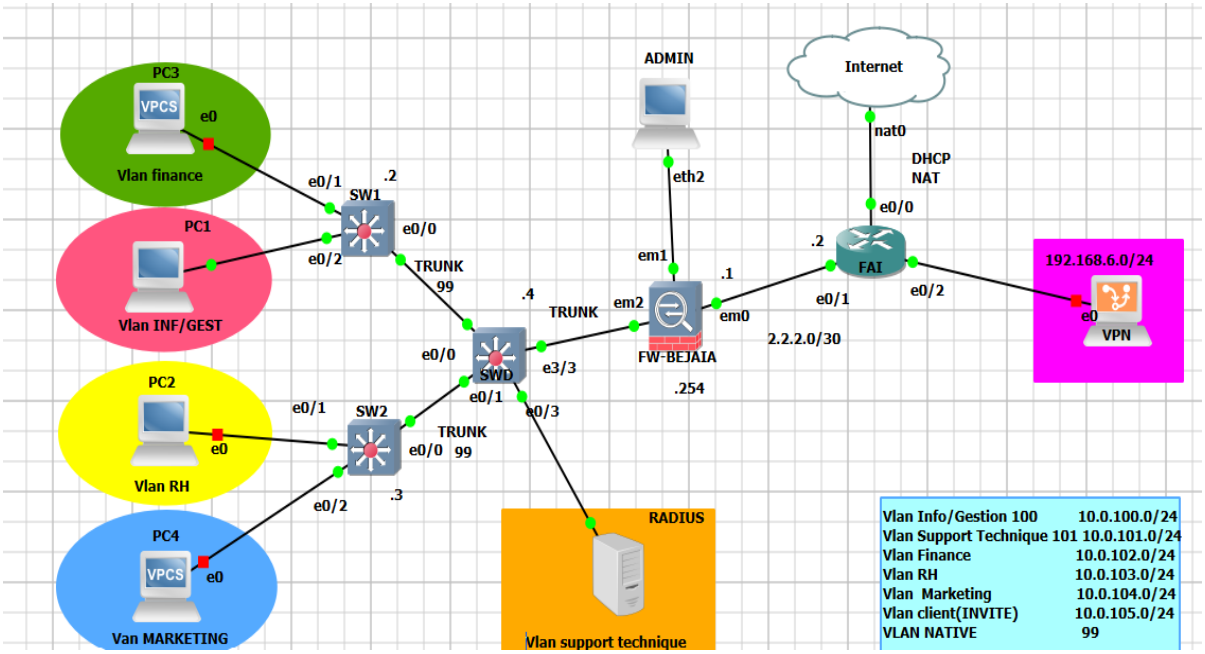


Figure 4.4 : *Architecture de réseau proposée*

4 La table des équipements

Equipement	Fournisseur	Nom d'équipement	Système
Routeur Cisco2911	Cisco	FAI	IOS
Switch Cisco2911	Cisco	Switch de distribution	IOS
Switch catalyst 2960	Cisco	Switch d'accès 1 et 2	IOS
Pfsense	Netgate	FW-Bejaia	FREE BSD
Serveur DELL R830	DELL	RADIUS	WINDOWS

Tableau 4.1 *: Les équipements utilisés*

5 La table d'adressage

Device	Interface	Adresse IP	Description	Passerelle
R-FAI	**E0/0**	**DHCP NAT**	**Connecté à Internet**	//
	E0/1	**2.2.2.2/30**	**Connecté au pfsense**	//
	E0/2	**192.168.6.0/24**	**Connecté au VPN**	//
Switch de distribution SWD	**E0/0**	**En mode trunk**	**Connecté au SW1**	//
	E0/1	**En mode trunk**	**Connecté au SWA2**	//
	E0/3	**VLAN 101**	**Connecté au Serveur**	//

	E3/3	**En mode trunk**	**Connecté au Pfsense**	**//**
Serveur RADIUS	**E0**	**10.0.101.200/24**	**Connecté au SWD**	**//**
Switch d'accès 1 SWA1	**E0/0**	**En mode trunk**	**Connecté au SWD**	**//**
	E0/1	**En mode accès**	**Connecté au vlan 102**	**//**
	E0/2	**En mode accès**	**Connecté au vlan 100**	**//**
Switch d'accès 2 SWA2	**E0/0**	**En mode trunk**	**Connecté au SWD**	**//**
	E0/1	**En mode accès**	**Connecté au vlan 103**	**//**
	E0/2	**En mode accès**	**Connecté au vlan 104**	**//**
Pfsense	**Em0**	**2.2.2.1/30**	**Connecté à FAI**	**//**
	Em1	**Sous interface**	**Connecté à ADMIN**	**//**
	Em2	**Sous interface**	**Connecté au SWD**	**//**
Client-VPN	**E0/1**	**Open vpn (internet)**	**Connecté à internet**	**//**

***Tableau 4.2** : Table d'adressage*

6 La table des VLANs

Nom VLANs	IP VLANs	Réseau/préfixe
Vlan Info/Gestion	100	10.0.100.0/24
Vlan Support physique	101	10.0.101.0/24
Vlan Finance	102	10.0.102.0/24
Vlan RH	103	10.0.103.0/24
Vlan Marketing	104	10.0.104.0/24
Vlan Invité	105	10.0.105.0/24
Vlan native	99	//////////////////

***Tableau 4.3 :** Table des Vlans*

7 Routage inter-Vlans sur pfsense

Créer une interface em2 pour le vlan. Et puis cliquer sur Vlans puis sur le bouton ADD pour créer les sous interfaces pour l'interface physique.

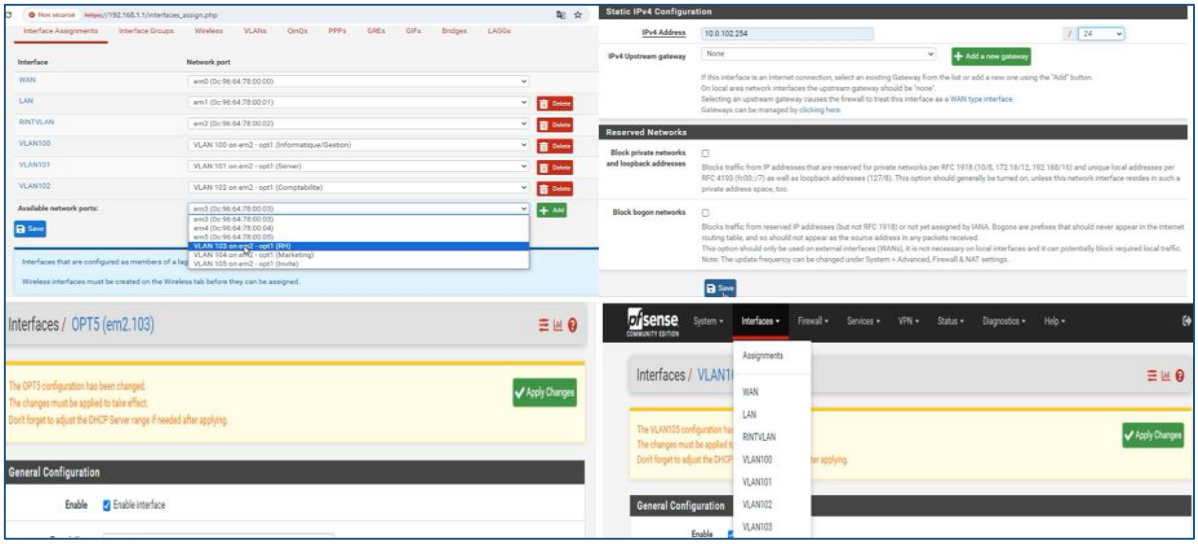


Figure 4.5 : *Routage inter-VLAN sur pfsense*

VLAN	NOM VLAN	GATEWAY
100	Informatique/gestion	10.0.100.254/24
101	Support physique	10.0.101.254/24
102	Finance	10.0.102.254/24
103	RH	10.0.103.254/24
104	Marketing	10.0.104.254/24
105	Invite	10.0.105.254/24

Tableau 4.4 : *Passerelles des VLANs*

8 Configuration de base sur le serveur

8.1 Attribution d'une adresse IP fixe (statique) au serveur

Accéder aux paramètres réseau, configurer les propriétés de la connexion réseau et faire entrer les paramètres IP statiques.

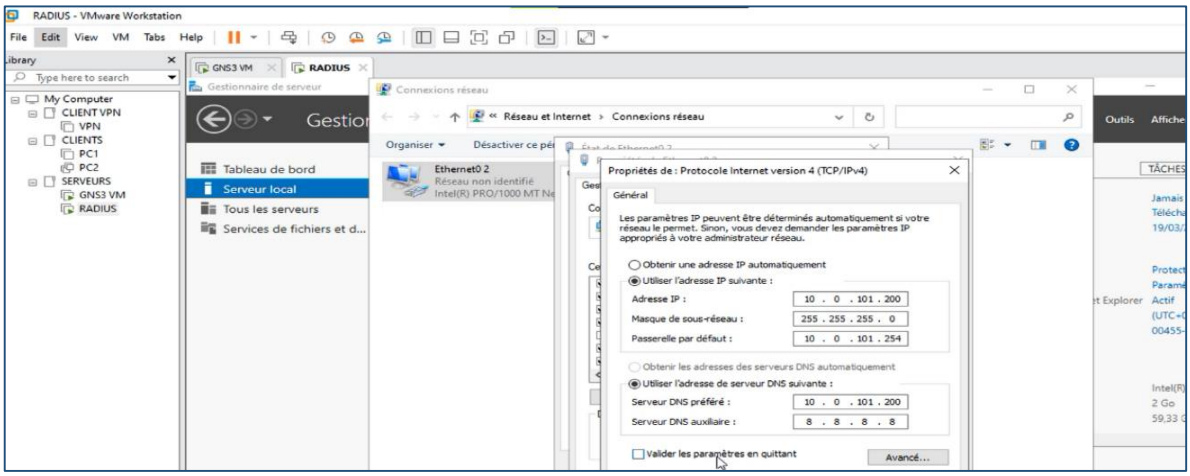


***Figure 4.6** : Attribution d'une @ IP fixe*

8.2 Installation de l'Active Directory dans le serveur

Vérifier que la machine Windows serveur 2022 dispose d'une adresse IP statique et d'un nom DNS valide. Ouvrir le gestionnaire de serveur : Connecter en tant qu'administrateur puis cliquer sur le bouton droit sur l'icône 'démarrer' et sélectionner 'gestionnaire de serveur'.

Commençant d'ajouter le Service de Rôle Active Directory.

- Assurer que le serveur Windows dispose des dernières mises à jour et que le pare-feu Windows est configuré pour permettre les communications nécessaires pour Active Directory.
- Ouvrir le Gestionnaire de serveur sur le serveur Windows. Cela peut être fait en cliquant sur Démarrer, puis en sélectionnant "Outils d'administration" puis "Gestionnaire de serveur".
- Dans le Gestionnaire de serveur, cliquer sur "Gérer" dans le coin supérieur droit, puis sélectionner "Ajouter des rôles et fonctionnalités".
- Suivre les instructions de l'assistant d'ajout de rôles et de fonctionnalités jusqu'à ce que vous atteigniez l'écran des rôles serveur. Cocher la case pour "Services de domaine Active Directory" et suivre les instructions pour terminer l'installation.

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

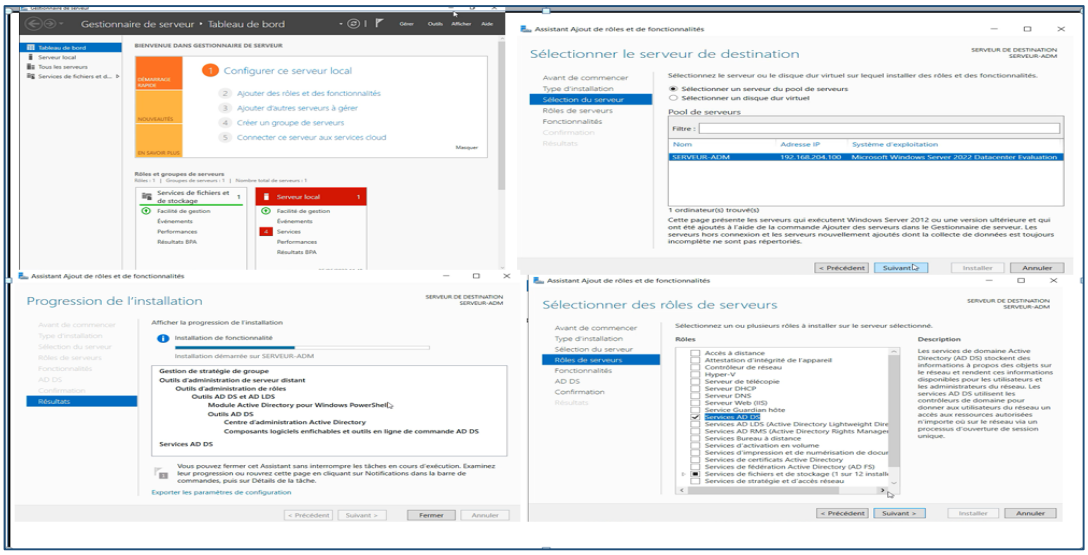


Figure 4.7 : *Installation de l'active directory*

8.3 Configuration d'Active Directory

- Une fois l'installation terminée, il faut configurer Active Directory en promouvant le serveur en contrôleur de domaine. Pour ce faire, ouvrir "Active Directory Domain Services Configuration Wizard" à partir du Gestionnaire de serveur et suivre les instructions pour promouvoir le serveur en contrôleur de domaine.
- Suivre les instructions de l'assistant pour spécifier le nom de domaine et les informations d'identification administratives pour le domaine. On a choisi ici nom de domaine « **collable.local** », on devra également choisir les options de réplication et de stockage de la base de données Active Directory.
- Une fois la promotion terminée, redémarrer le serveur pour appliquer les modifications.

A la fin de l'installation, on aura les deux rôles installés comme le montre la figure 4.8 :

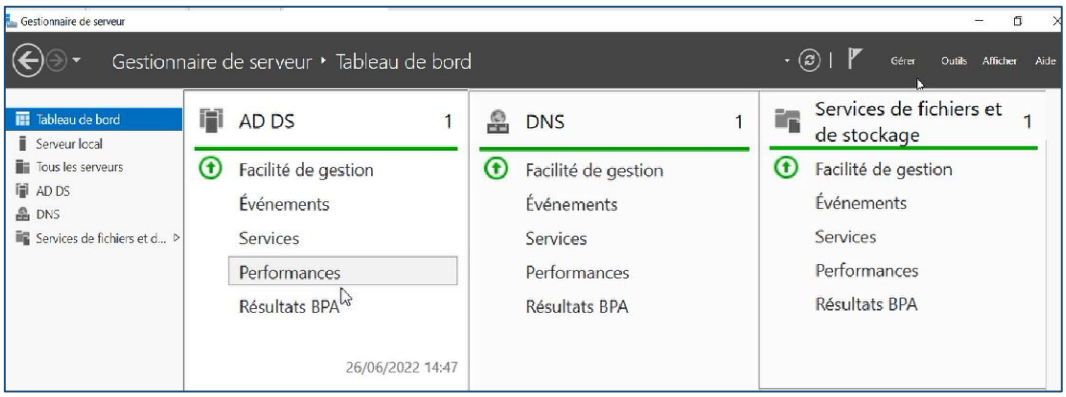


Figure 4.8 : *Rôles AD DS et DNS*

8.4 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 ajouter les fonctionnalités nécessaires.

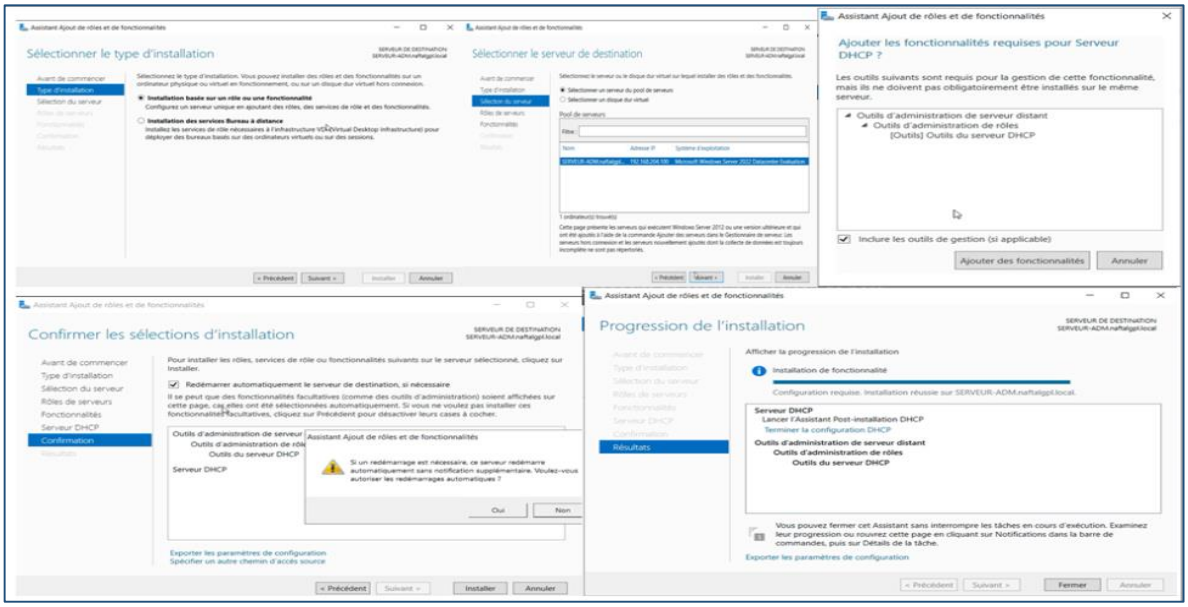


Figure 4.9 : *Installation de DHCP*

8.5 Configuration de DHCP

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

Etape 1 : fournir le nom et la description de chaque vlan pour identifier son étendue.

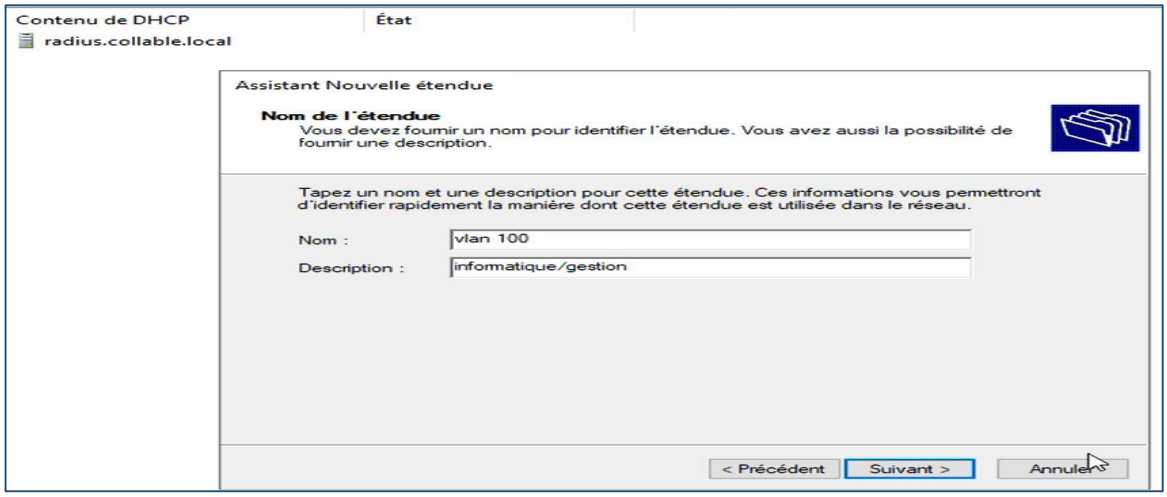


Figure 4.10 : *Nom et description de vlan*

Etape 2 : création de nos étendues DHCP à l'aide de la console d'administration DHCP qui a été lancée depuis le menu outils du gestionnaire de serveur.

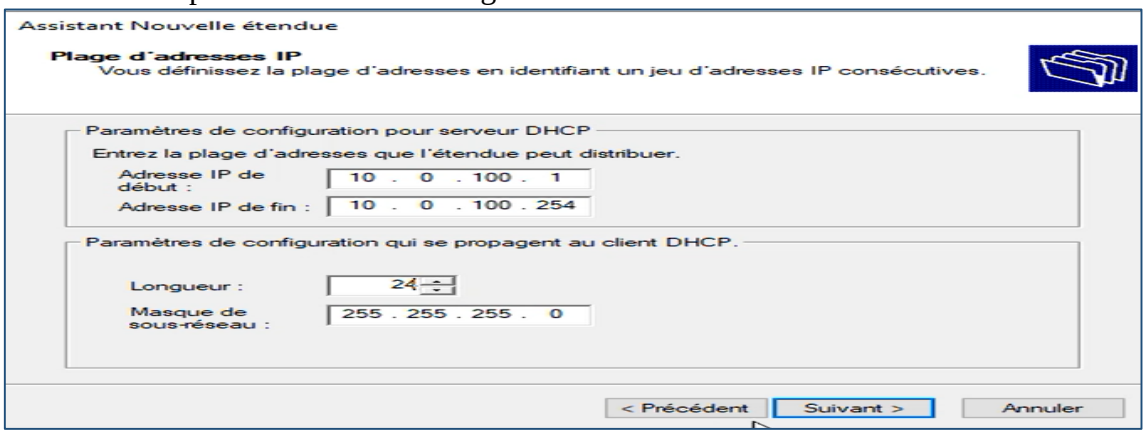


Figure 4.11 : *Paramétrage des adresses des Vlans*

Etape 3 : ajouter les exclusions des adresses ou des plages qui ne sont pas distribuées par le serveur afin de ne pas provoquer de conflit avec un périphérique qui serait configuré sur ces adresses.

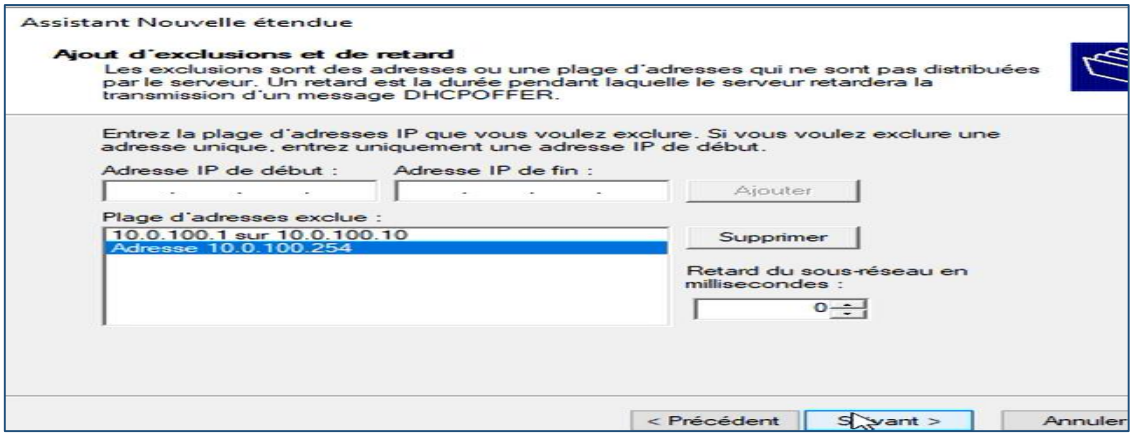


Figure 4.12*: Exclusion des 10 premières adresses plus la passerelle*

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

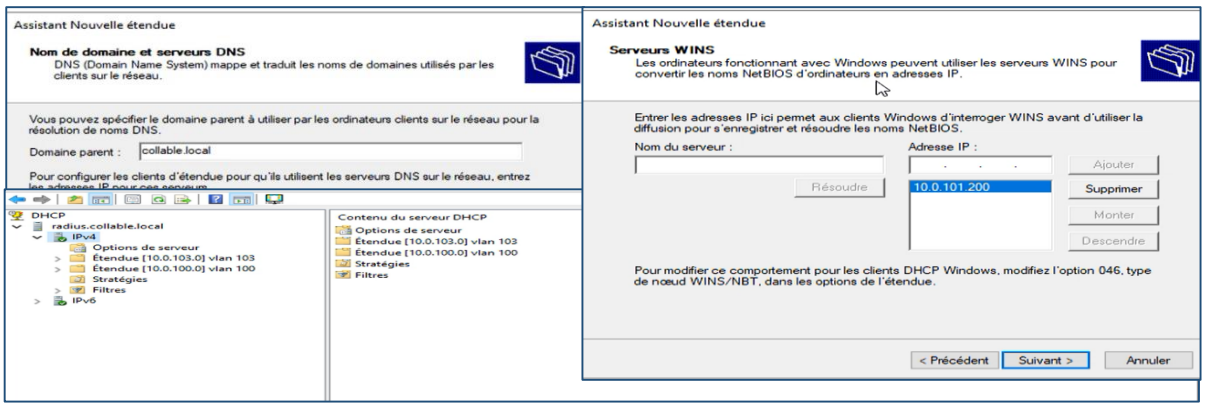


Figure 4.13 : *Les étendus des VLANs configurés*

8.6 Configuration d'unité d'organisation COLLABLE

Créer l'unité d'organisation collable dans laquelle on crée les utilisateurs.

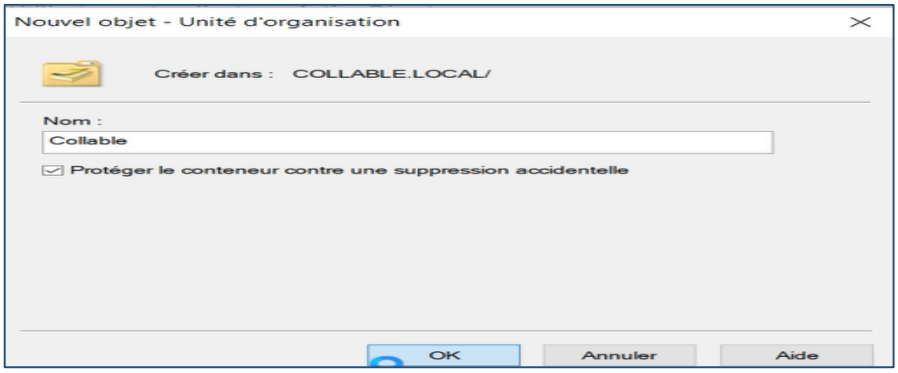


Figure 4.14: *Création d'une unité d'organisation*

Création des utilisateurs :

Pour créer un utilisateur, un clic sur le bouton droit sur le domaine "COLLABLE.local" puis "New user".

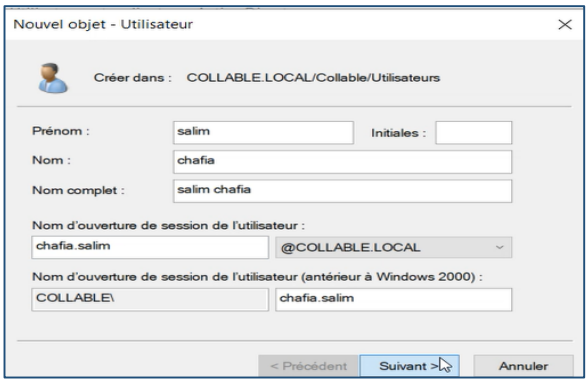


Figure 4.15: *Création d'utilisateur 1*

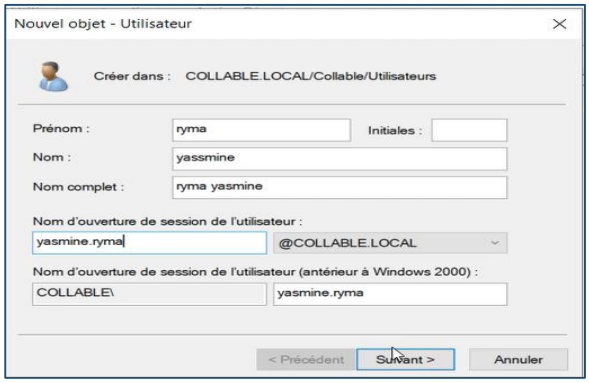


Figure 4.16: *Création d'utilisateur 2*

Création des groupes : Vlan 100 informatique gestion et Vlan 103 RH.

Pour ajouter des utilisateurs sur le groupe, un clic sur le bouton droit sur Vlan propriété, cliquer sur membre, ajouter, choisir l'emplacement collable, avancer puis sélectionner les utilisateurs. On a choisi chafia.salim pour Vlan 100 et aimed.oussama pour Vlan 103.

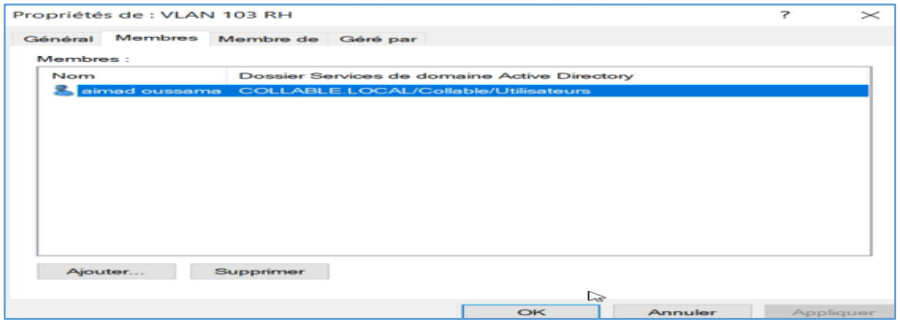


Figure 4.17 : *Ajout des utilisateurs dans un groupe*

8.7 Configuration des switchs

Configurer toutes les interfaces des switchs en mode trunk pour configurer de telle sorte que l'on peut y faire circuler des trames Ethernet modifiées comportant des informations relatives au VLAN sur lequel elles transitent.

8.7.1 Configuration de switch distribution

Lors de cette étape, nous allons configurer les interfaces des switchs client (SWA1, SWA2) qui sont reliés avec le switch de distribution en mode trunk.

```
SWD#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD(config)#interface range ethernet 0/0-1
SWD(config-if-range)#switchport trunk encapsulation dot1q
SWD(config-if-range)#switchport mode trunk
SWD(config-if-range)#switchport trunk native vlan 99
SWD(config-if-range)#
*Apr 21 10:08:56.447: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on E
thernet0/0 (99), with SWA1 Ethernet0/0 (1).
SWD(config-if-range)#switchport trunk allowed vlan 99-105
SWD(config-if-range)#end
SWD#w
*Apr 21 10:09:37.924: %SYS-5-CONFIG_I: Configured from console by console
SWD#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
```

Figure 4.18 : *Configuration de switch distribution*

8.7.2 Configuration de switch d'accès 1 (SW1)

La configuration du switch d'accès 2 (SW2) se fait de la même façon que le SW1. On change juste les interfaces nécessaires.

```
SWA1
SWA1#
SWA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA1(config)#interface ethernet 0/0
SWA1(config-if)#switchport trunk encapsulation dot1q
SWA1(config-if)#switchport mode trunk
SWA1(config-if)#end
SWA1#
```

Figure 4.19 : *Configuration de switch d'accès 1*

- **Configuration de Vlan Trunking 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 switchs d'accès.
- **Mode transparence :** Diffuser la configuration des switchs.

- **Configuration de VTP en mode serveur**

```
SWD#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD(config)#vtp mo
SWD(config)#vtp mode serve
SWD(config)#vtp mode server
Device mode already VTP Server for VLANS.
SWD(config)#vtp domain collable.vtp
Changing VTP domain name from NULL to collable.vtp
SWD(config)#vtp password collable123
Setting device VTP password to collable123
SWD(config)#vtp version 2
SWD(config)#vtp prun
SWD(config)#vtp pruning
Pruning switched on
SWD(config)#end
SWD#
SWD#
SWD#w
*Apr 21 10:14:04.822: %SYS-5-CONFIG_I: Configured from console by console
SWD#wr
Building configuration...
Compressed configuration from 1624 bytes to 962 bytes[OK]
SWD#
```

Figure 4.20 : *Configuration de VTP en mode serveur*

- **Configuration de VTP en mode client**

```
SWA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA1(config)#vtp mo
SWA1(config)#vtp mode cli
SWA1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SWA1(config)#vtp domain collable.vtp
Changing VTP domain name from NULL to collable.vtp
SWA1(config)#vtp password collable123
Setting device VTP password to collable123
SWA1(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
SWA1(config)#end
SWA1#wr
Building configuration...

*Apr 21 10:15:13.920: %SYS-5-CONFIG_I: Configured from console by consoleCompressed con
figuration from 1493 bytes to 905 bytes[OK]
```

Figure 4.21 : *Configuration de VTP en mode client*

- **Création des vlans sur le switch de distribution**

```
SWD#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD(config)#vlan 100
SWD(config-vlan)#name info/gestion
SWD(config-vlan)#vlan 101
SWD(config-vlan)#name server
SWD(config-vlan)#vlan 102
SWD(config-vlan)#name comptabilite
SWD(config-vlan)#vlan 103
SWD(config-vlan)#name RH
SWD(config-vlan)#vlan 104
SWD(config-vlan)#name Marketing
SWD(config-vlan)#vlan 105
SWD(config-vlan)#name invite
SWD(config-vlan)#end
SWD#
```

Figure 4.22: *Création des VLANs sur le switch de distribution*

- **Vérification des VLANs crées sur le switch de distribution**

Avec la commande **show vlan brief** permet d'afficher les vlans crées.

```
SWD#show  vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Et0/2, Et0/3, Et1/0, Et1/1
                                                   Et1/2, Et1/3, Et2/0, Et2/1
                                                   Et2/2, Et2/3, Et3/0, Et3/1
                                                   Et3/2, Et3/3
100  info/gestion                        active
101  server                              active
102  comptabilite                        active
103  RH                                  active
104  Marketing                           active
105  invite                              active
1002 fddi-default                        act/unsup
1003 trcrf-default                       act/unsup
1004 fddinet-default                     act/unsup
1005 trbrf-default                       act/unsup
SWD#
```

***Figure 4.23** : Vérification des VLANs crées*

- **Affectation des ports pour les Vlans en mode access**

```
SWA2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA2(config)#in
SWA2(config)#interface  eth
SWA2(config)#interface  ethernet 0/1
SWA2(config-if)#sw
SWA2(config-if)#switchport mo
SWA2(config-if)#switchport mode  acc
SWA2(config-if)#switchport mode  access
SWA2(config-if)#
SWA2(config-if)#sw
SWA2(config-if)#switchport acc
SWA2(config-if)#switchport access vl
SWA2(config-if)#switchport access vlan 103
SWA2(config-if)#exit
SWA2(config)#interface  ethernet 0/2
SWA2(config-if)#switchport mode  access
SWA2(config-if)#switchport access vlan 104
SWA2(config-if)#end
SWA2#
SWA2#
SWA2#w
```

***Figure 4.24** : Affectation des ports pour les Vlans en mode Access*

On suit les mêmes étapes pour la configuration du switch d'accès 2 (SW2) et le switch de distribution.

- **Activation de triple AAA :** sert à activer le service d'authentification Dot1X, avec triple (AAA) Authentication, Autorisation et Accounting et la deuxième commande définit le groupe de serveur à utiliser pour authentifier.

```
SW1(config)#aaa new-model
SW1(config)#aaa authen
SW1(config)#aaa authentication do
SW1(config)#aaa authentication dot1x de
SW1(config)#aaa authentication dot1x default gro
SW1(config)#aaa authentication dot1x default group ra
SW1(config)#aaa authentication dot1x default group radius
```

```
SW1(config)#radius server RADIUS
SW1(config-radius-server)#add
SW1(config-radius-server)#address ipv4 10.0.101.200
```

***Figure 4.25 :** Activation de service AAA*

7.3.3 Activation de la 802.1x pour le client

```
SW1(config)#dot1x system-auth-control
```

Port control auto : personne ne peut connecter sans authentification.

```
SW1(config-if)#authentication port-control auto
SW1(config-if)#dot1x pae authenticator
```

Spanning tree ne pas laisser la convergence sortir par le port pour éviter le piratage.

```
SW1(config-if)#spanning-tree bpduguard enable
```

Figure 4.26 : *Activation de la norme 802.1x*

8.8 Configuration du routeur

8.8.1 Configuration des interfaces

Comme tout périphérique joignable sur le réseau, les interfaces du routeur doivent posséder des adresses ipv4 et les masques, Nous avons attribué des adresses ip dhcp pour l'interface vers l'internet, l'adresse 2.2.2.2/30 pour l'interface vers le client collable et l'adresse 192.168.6.254/24 pour l'interface des clients X comme le VPN.

```
FAI(config)#interface ethernet 0/0
FAI(config-if)#no shu
FAI(config-if)#no shutdown
FAI(config-if)#description // interface vers client X  //
*Apr 21 10:39:45.268: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Apr 21 10:39:46.268: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
FAI(config-if)#description // interface vers internet  //
FAI(config-if)#ip add
FAI(config-if)#ip address dhcp
FAI(config-if)#end
```

```
FAI#
FAI#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
FAI(config)#in
FAI(config)#interface  eth
FAI(config)#interface  ethernet 0/1
FAI(config-if)#no shu
FAI(config-if)#no shutdown
FAI(config-if)#des
FAI(config-if)#description //
*Apr 21 10:36:30.451: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Apr 21 10:36:31.456: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
FAI(config-if)#description // interface vers client COLLABLEB //
FAI(config-if)#description // interface vers client COLLABLE //
FAI(config-if)#ip add
FAI(config-if)#ip address 2.2.2.2 255.255.255.252
FAI(config-if)#exit
FAI(config)#interface  ethernet 0/2
FAI(config-if)#description // interface vers client X  //
FAI(config-if)#no shu
FAI(config-if)#no shutdown
FAI(config-if)#ip add
FAI(config-if)#ip address 192.168.
*Apr 21 10:38:56.355: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*Apr 21 10:38:57.355: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to up
FAI(config-if)#ip address 192.168.6.254 255.255.255.0
FAI(config-if)#exit
```

Figure 4.27 : *Configuration des interfaces du routeur*

8.8.2 Vérification des adresses

```
FAI#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.122.118 YES DHCP   up                    up
Ethernet0/1                2.2.2.2         YES manual up                    up
Ethernet0/2                192.168.6.254   YES manual up                    up
Ethernet0/3                unassigned      YES NVRAM  administratively down down
Ethernet1/0                unassigned      YES NVRAM  administratively down down
Ethernet1/1                unassigned      YES NVRAM  administratively down down
Ethernet1/2                unassigned      YES NVRAM  administratively down down
Ethernet1/3                unassigned      YES NVRAM  administratively down down
Serial2/0                  unassigned      YES NVRAM  administratively down down
Serial2/1                  unassigned      YES NVRAM  administratively down down
Serial2/2                  unassigned      YES NVRAM  administratively down down
```

Figure 4.28 : *Vérification des adresses*

8.8.3 Configuration du NAT

Définir les interfaces internes.

```
FAI(config)#interface range ethernet 0/1-2
FAI(config-if-range)#ip nat in
FAI(config-if-range)#ip nat inside
```

Définir l'interface externe.

```
FAI(config)#interface  ethernet 0/0
FAI(config-if)#ip nat ou
FAI(config-if)#ip nat outside
FAI(config-if)#exit
```

Définir les adresses IP internes qui seront soumises à la traduction NAT.

```
FAI(config)#ip access-list standard NAT
FAI(config-std-nacl)#per
FAI(config-std-nacl)#permit 2.2.2.0 0.0.0.3
FAI(config-std-nacl)#per
FAI(config-std-nacl)#permit 192.168.6.0 0.0.0.255
FAI(config-std-nacl)#EXIT
```

```
FAI(config)#ip nat inside source list NAT interface  ethernet 0/0 overload
FAI(config)#end
```

Figure 4.29 : *Configuration du NAT*

8.8.4 Affichage de la translation

```
FAI#show  ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 192.168.122.118:123 2.2.2.1:123       162.159.200.1:123  162.159.200.1:123
udp 192.168.122.118:123 2.2.2.1:123       162.159.200.123:123 162.159.200.123:123
icmp 192.168.122.118:7026 2.2.2.1:7026    8.8.8.8:7026       8.8.8.8:7026
tcp 192.168.122.118:13341 2.2.2.1:13341   199.19.57.1:53     199.19.57.1:53
tcp 192.168.122.118:20176 2.2.2.1:20176   192.5.5.241:53     192.5.5.241:53
tcp 192.168.122.118:20548 2.2.2.1:20548   192.36.148.17:53   192.36.148.17:53
tcp 192.168.122.118:34888 2.2.2.1:34888   199.19.56.1:53     199.19.56.1:53
tcp 192.168.122.118:53093 2.2.2.1:53093   199.19.54.1:53     199.19.54.1:53
tcp 192.168.122.118:61137 2.2.2.1:61137   199.7.91.13:53     199.7.91.13:53
```

Figure 4.30 : *Affichage de la translation*

8.9 Configuration de base du Firewall

Première étape : Aller sur le navigateur et saisir 192.168.1.1. La fenêtre pfsense apparait comme elle est montrée dans la figure ci-dessous : saisir le nom d'administrateur et le mot de passe par défaut.

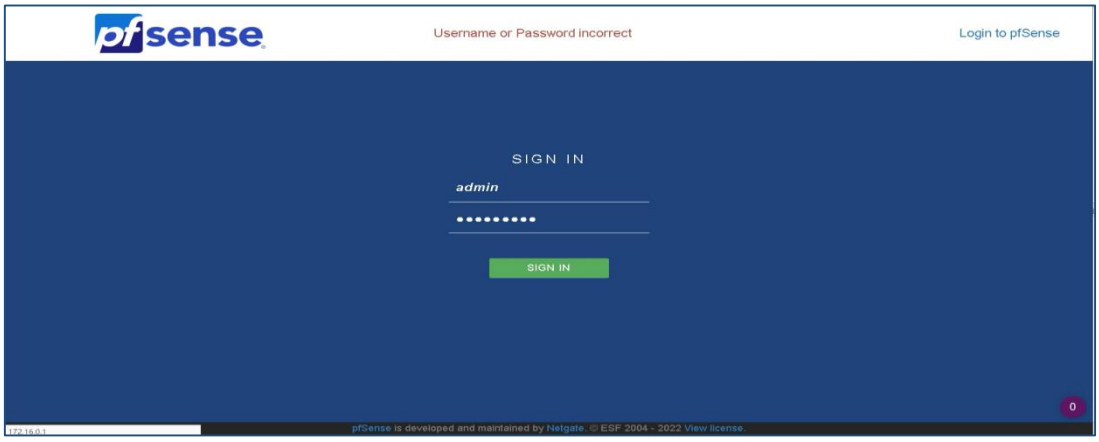


Figure 4.31: *Page d'accueil de pfsense*

Deuxième étape : La fenêtre qui vient juste après nous permet de donner un nom pour l'utilisateur et de changer son mot de passe, pour cela, on a choisi « admin » comme un nom d'utilisateur et « admin123 » comme mot de passe.

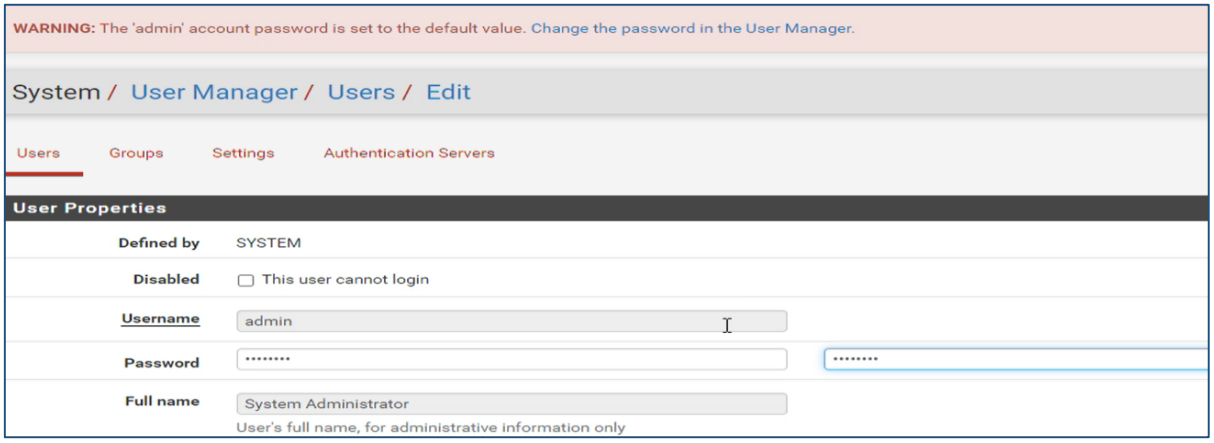


Figure 4.32 : *Changement de mot de passe*

8.9.1 Configuration de l'interface WAN (em0)

La configuration de l'interface WAN sur pfSense est une étape cruciale pour garantir que votre pare-feu peut se connecter à l'Internet ou à un autre réseau externe.

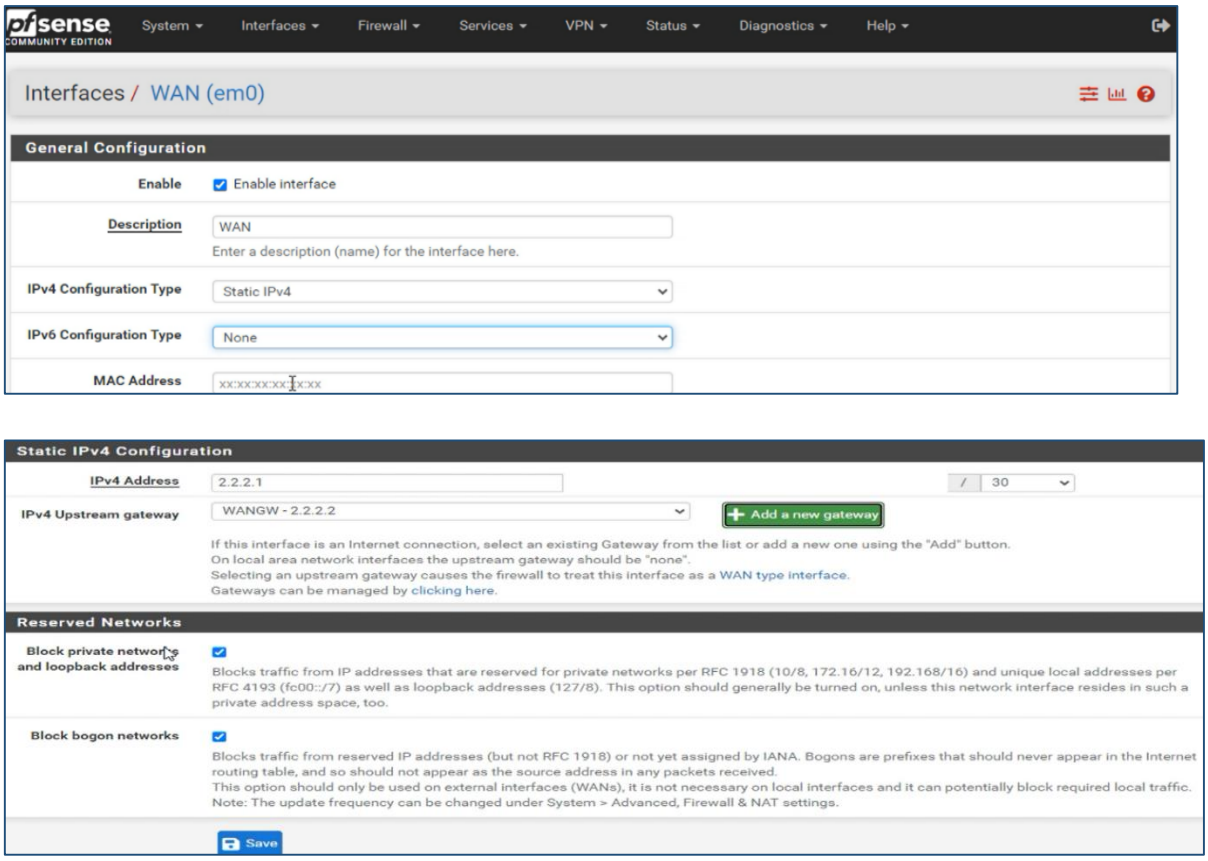


Figure 4.33 : *Configuration de l'interface WAN (em0)*

8.9.2 Création d'une interface pour les vlans (em2)

La configuration d'une interface physique sur pfSense permet de gérer plusieurs VLANs. Cette segmentation du réseau améliore la sécurité et facilite la gestion du réseau en assurant la configuration des règles de pare-feu appropriées pour chaque VLAN afin de contrôler le trafic réseau et maintenir la sécurité.

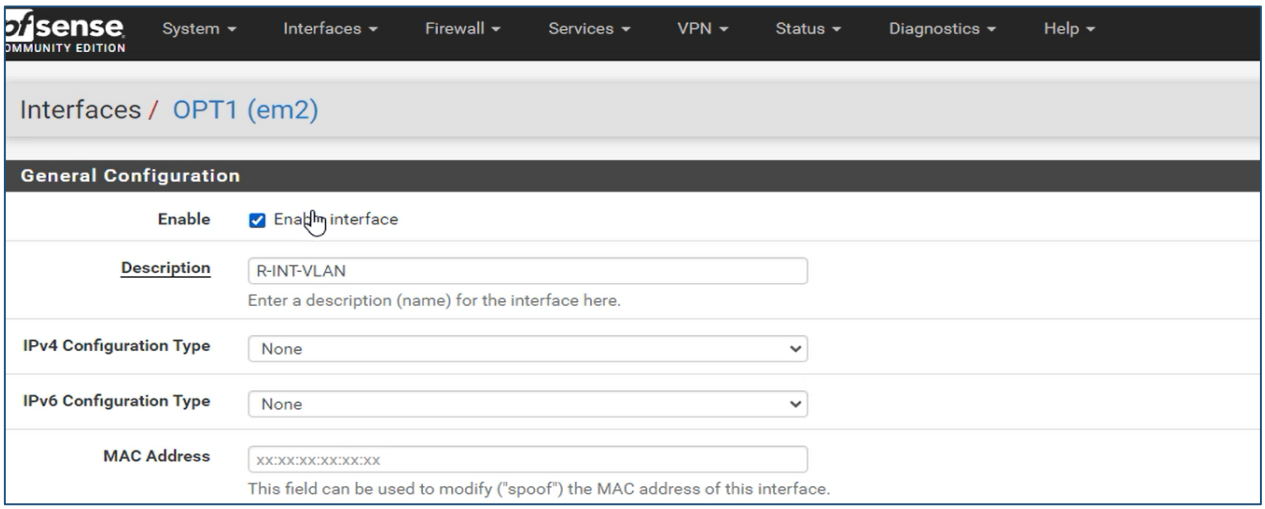


Figure 4.34 : *Création d'une interface em2 pour les vlans*

8.9.3 Création des sous interfaces dans l'interface physique

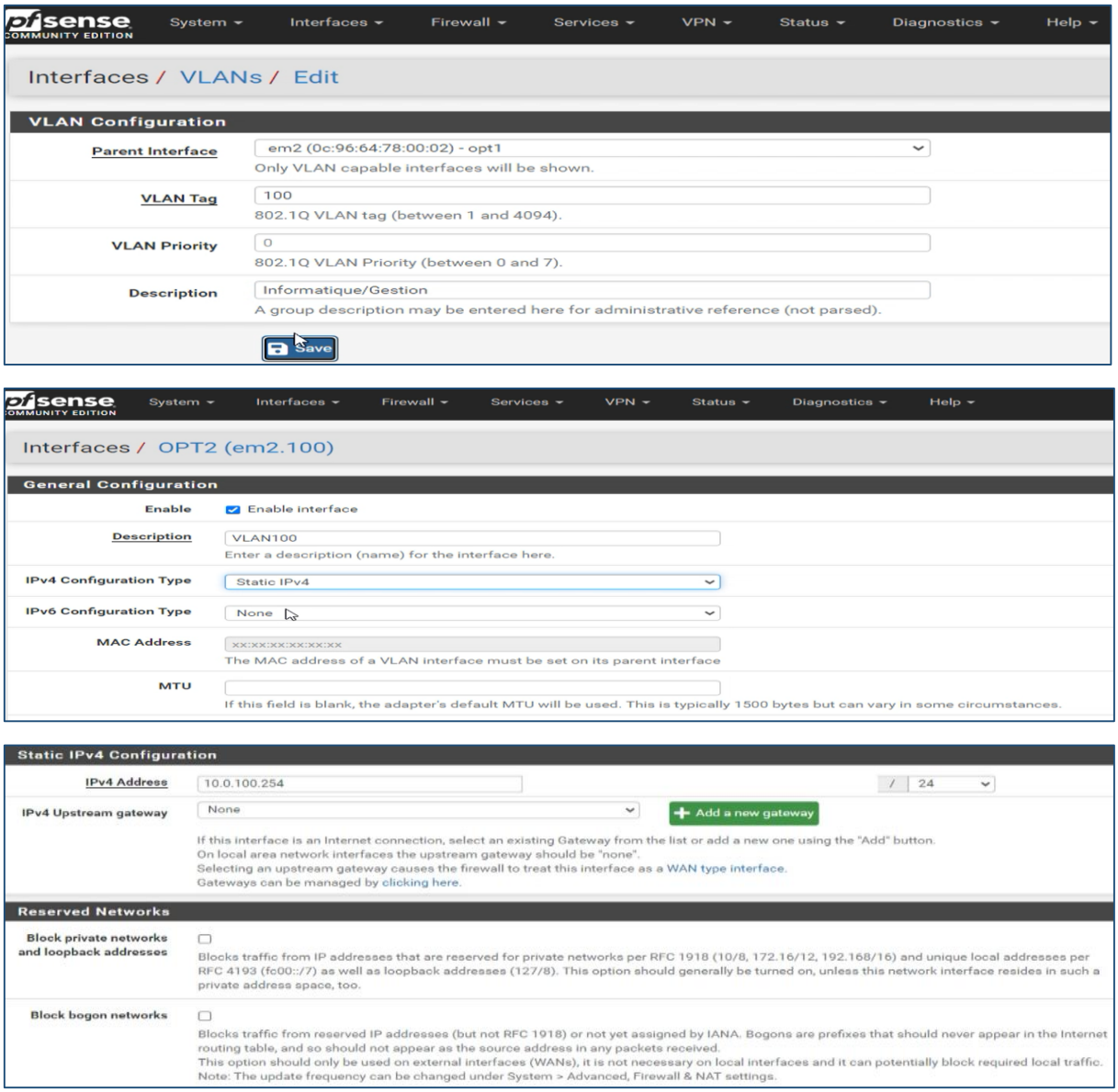


Figure 4.35 : *Création des sous interfaces dans l'interface physique*

8.9.4 Création des vlans

La création de VLANs sur pfSense est une étape importante pour segmenter le réseau en sous-réseaux logiques distincts, améliorant ainsi la gestion du réseau et la sécurité.

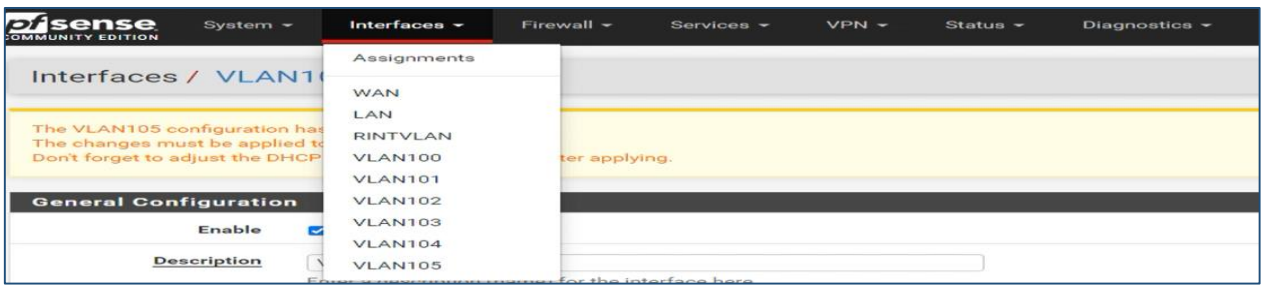


Figure 4.36 : *Création des VLANs*

Mentionner les vlans sur la partie firewall, ensuite on va autoriser le « IPV4 » puis on change la source au lieu de « Lan net » on met « Any ». Pour le vlan 100 et le vlan 103

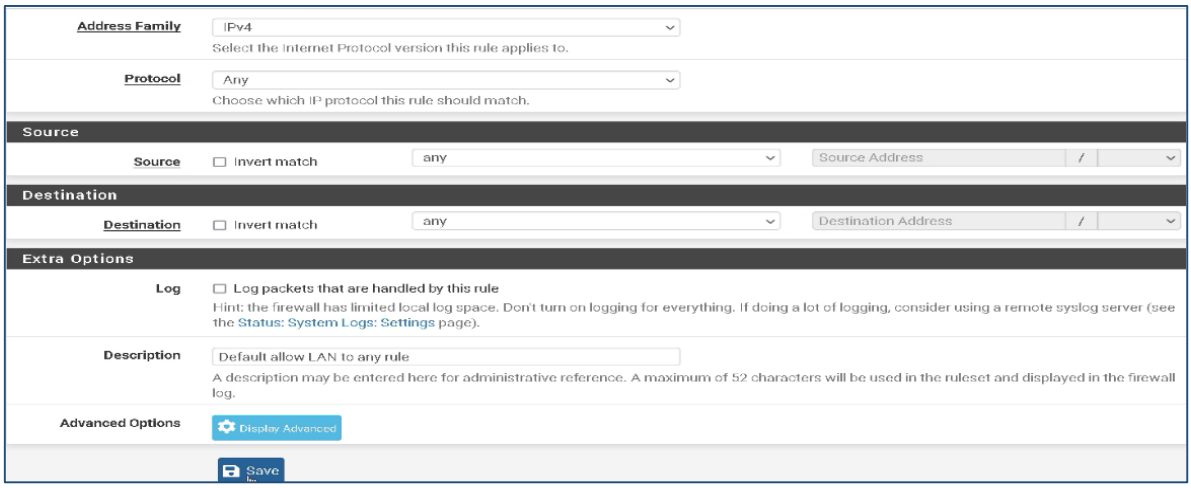


Figure 4. 37 : *Changement de la source de IPV4*

8.10 Configuration du certificat

8.10.1 Création des certificats RADIUS

Sur le serveur Radius, on clique sur l'icône utilisateurs et ordinateurs Active Directory on appuie sur Utilisateurs et avec le bouton droit, on choisit nouveau groupe puis nom certificat server radius.

Sur le groupe certificat radius, on clique sur Membre, Ajouter, Type d'objet, cocher sur les Ordinateurs, Rechercher, choisir Radius et enfin, on appuie sur Appliquer.

Mêmes étapes pour certificat client radius au lieu de choisir le serveur radius, on choisit PC1 et PC2.

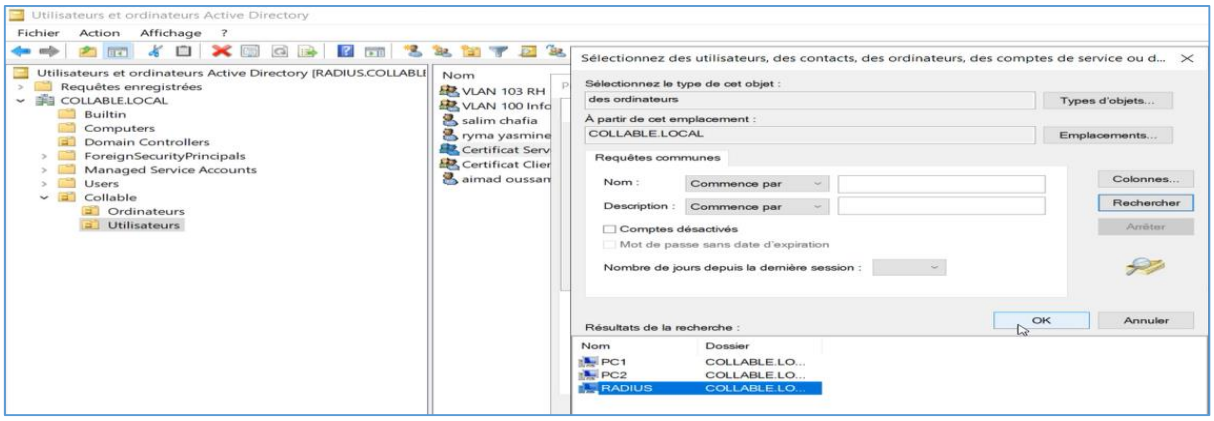


Figure 4.38 : *Création et configuration du groupe certificat server RADIUS*

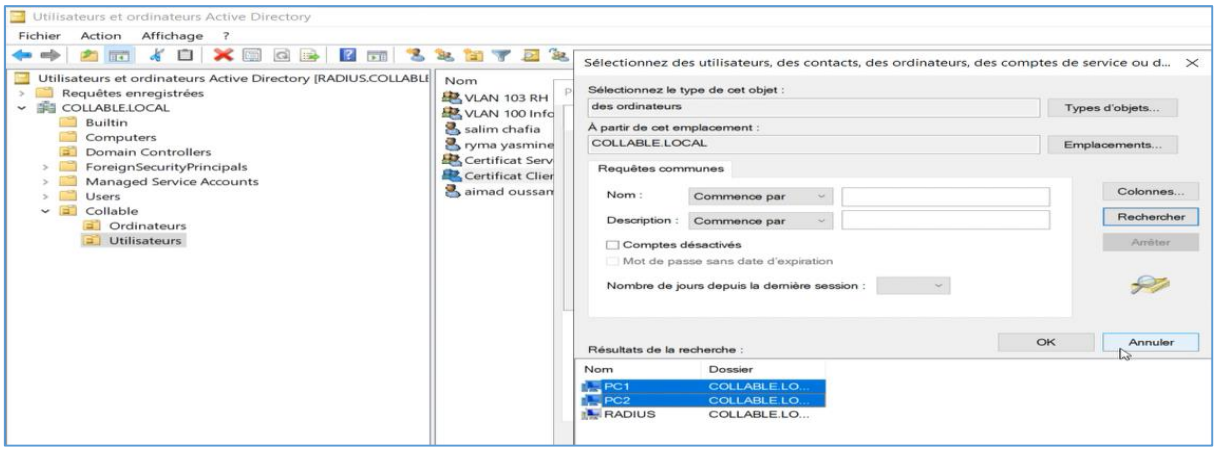


Figure 4.39 : *Création et configuration du groupe certificat client RADIUS*

8.10.2 Autorité de certificat

Aller sur modèle de certificat, avec le bouton droit sur gérer – choisir serveur RAS et IAS, appuyer sur le bouton droit et choisir dupliquer le domaine, changer le nom certificat radius server - choisir la validité 5 ans, renouvellement 6 semaines.

Sur compatibilité : pour autorité de certificat choisir Windows server 2016 et pour destinataire choisir Windows 10.

Sur sécurité : ajouter – certificat - vérifier – choisir certificats server radius cocher inscrire automatiquement – appliquer.

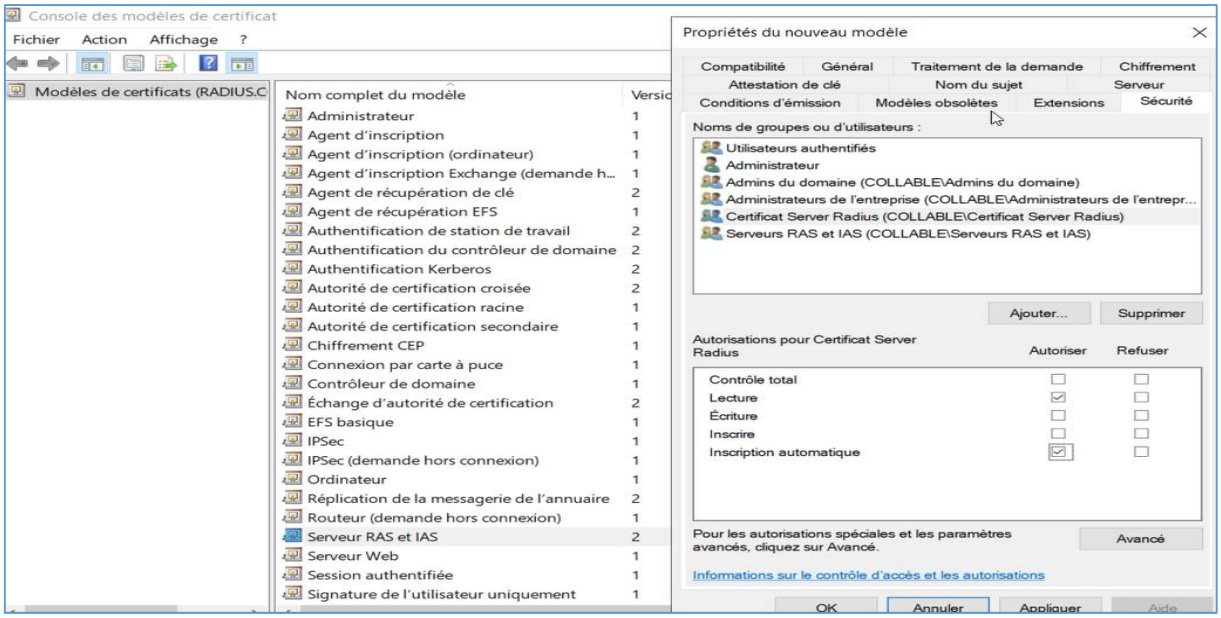


Figure 4.40 : *Modèles de certificat : Serveur RAS et IAS*

8.10.3 Authentification des stations de travail

On clique sur le bouton droit sur dupliquer le modèle et on choisit modèle server 2016 et Windows 10, sur général donner le nom certificat client radius, sur généralité ajouter certificat client radius et cocher inscription automatique et appliquer.

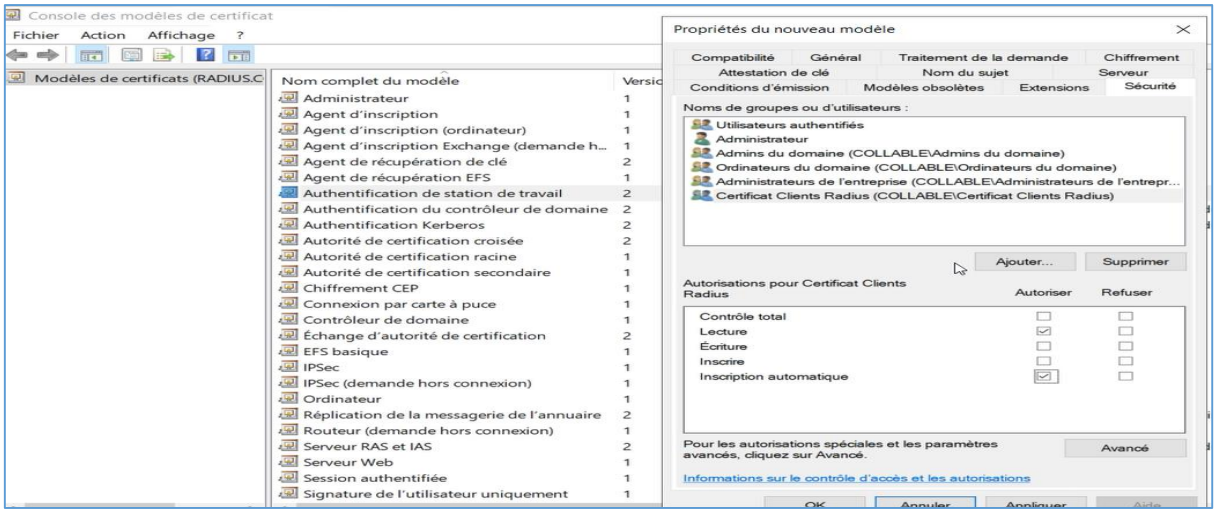


Figure 4.41 : *Modèles de certificat : Authentification de station de travail*

Ajouter les 2 groupes de certificats dans modèle de certificat en cliquant avec le bouton droit sur nouveau – modèle de certificat à délivrer, choisir certificat server radius et certificat client radius et appuyer enfin sur le bouton Ok.

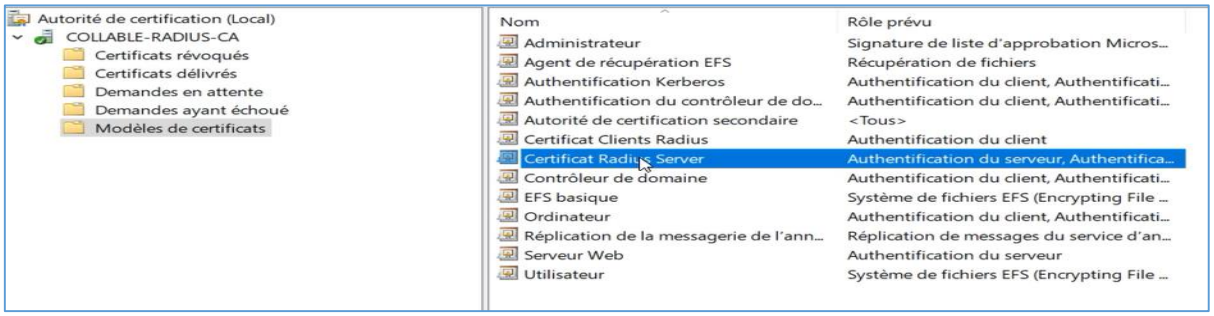


Figure 4.42 : *Ajout des certificats Radius server et client dans modèles de certificats*

8.10.4 Création d'une GPO

Pour activer la norme 802.1x et délivrer les certificats automatiquement : Sur Gestion de stratégie de groupe – domaine – collable.local - default domain policy bouton droit modifier - stratégie – paramètres Windows – paramètres de sécurité - stratégie de clé publique – client des services de certificat inscription automatique - propriétés modèle configuration activé, cocher mettre à jour les certificats - appliquer - ok. Certifier tout le monde

Pour certifier les ordinateurs : Sur objet de stratégie de groupe - bouton droit – nouveau nom : st-radius-filaire - ok

Sur la stratégie st-radius-filaire, bouton droit – modifier stratégie – paramètres Windows - paramètres sécurité- service system-configuration automatique de réseau câblé - définir ces paramètres de stratégie, sélectionner automatique et appuyer sur appliquer.

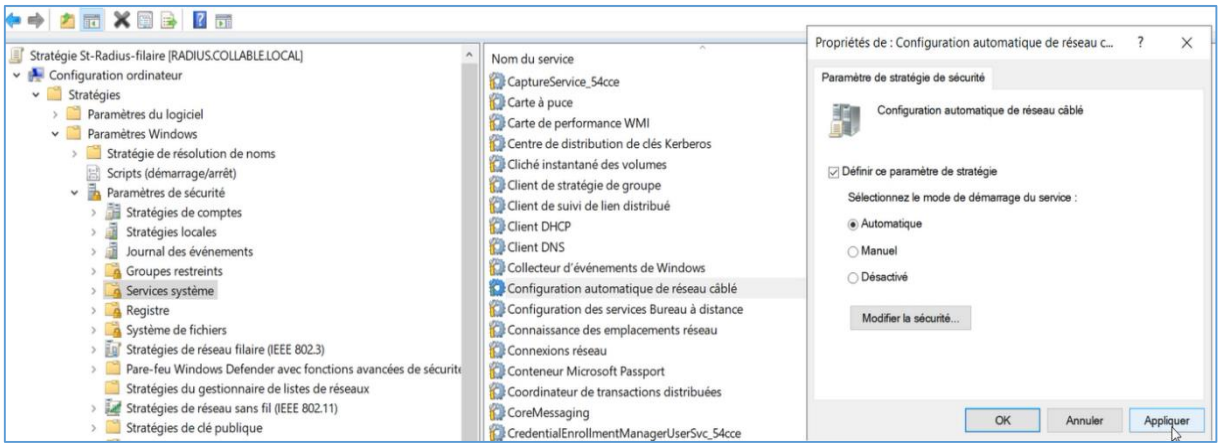


Figure 4.43 : *Certification des ordinateurs dans le réseau câblé*

Sur la stratégie de réseau filaire, cliquer avec le bouton droit choisir créer une stratégie de réseau câblé puis aller sur sécurité ensuite choisir les ordinateurs uniquement dans mode d'authentification et choisir 3 pour nombre d'authentifications. Sur propriétés EAP, cocher COLLABLE-RADIUS-CA et sélectionner la méthode d'authentification, choisir carte à puce ou autre certificat configurer cocher COLLABLE-RADIUS-CA et appuyer sur appliquer.

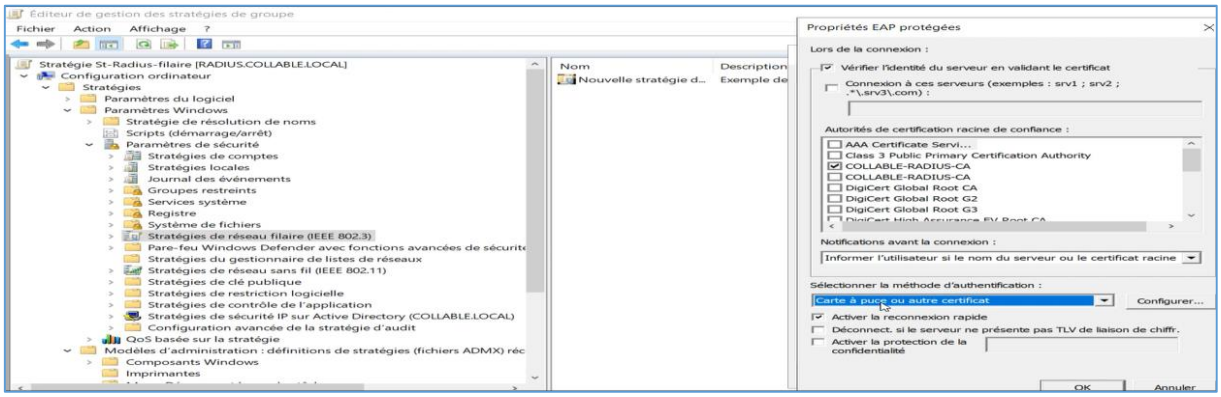


Figure 4.44 : *Stratégie de réseau filaire avec la norme 802.1x*

Création d'un modèle de certificat pour faciliter la tâche aux utilisateurs : Aller sur stratégie de clé publique – paramètres de demande automatique de certificat – appuyer sur le bouton droit de la souris et choisir nouveau – demande automatique certificat – suivant - cliquer sur ordinateur – suivant - ok.

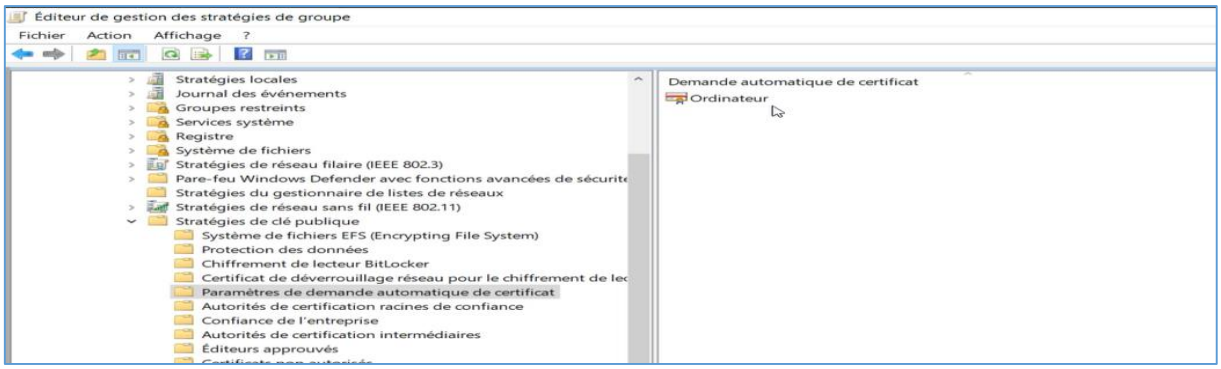


Figure 4.45 : *Demande automatique de certificats pour les ordinateurs*

Sur St-Radius-filaire : Aller sur paramètres et appuyer sur ajouter puis sur fermer.

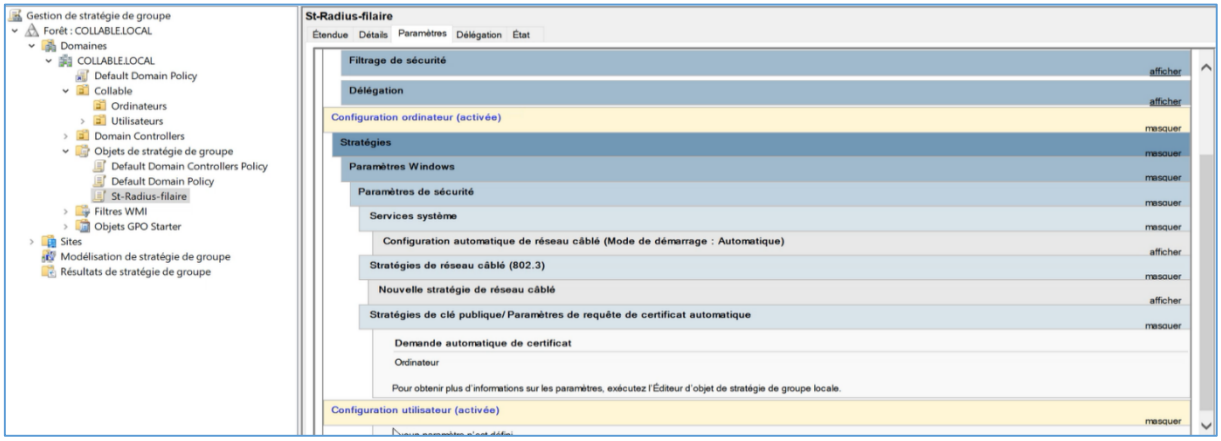


Figure 4.46 : *Vue globale de la stratégie Radius-filaire*

Mise à jour de la stratégie : sur la commande Windows PowerShell : gpupdate

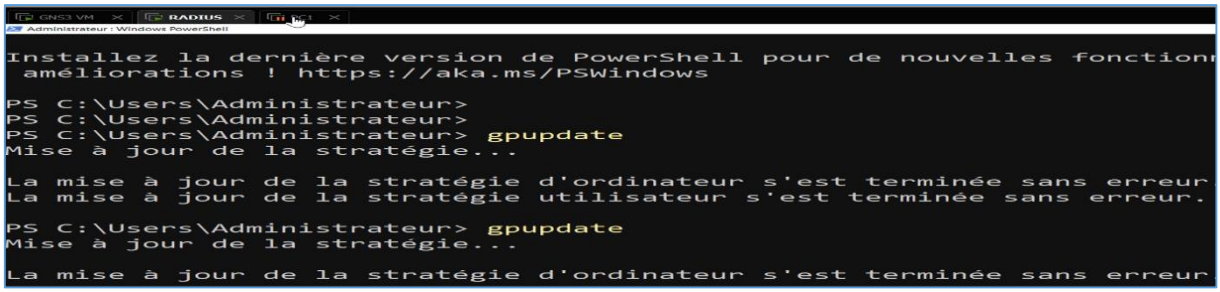


Figure 4.47 : *Mise à jour de la stratégie*

Mise des stratégies en ordre : sur ordinateurs, cliquer sur le bouton droit de la souris et cliquer sur lier un objet de la stratégie de groupe existant.

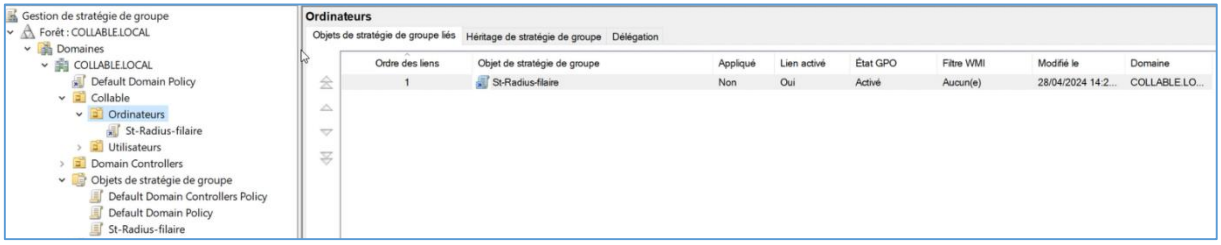


Figure 4.48 : *Liaison d'un ordinateur avec la stratégie de groupe*

8.11 Installation Open VPN

8.11.1 Création d'un client VPN

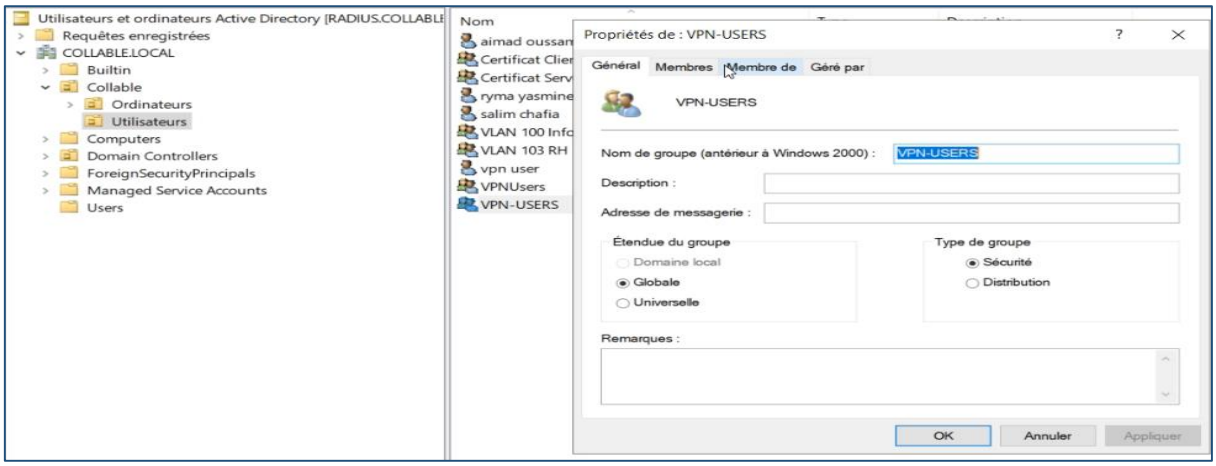


Figure 4.49 : *Création d'un client VPN*

8.11.2 Création de l'autorité de certificat

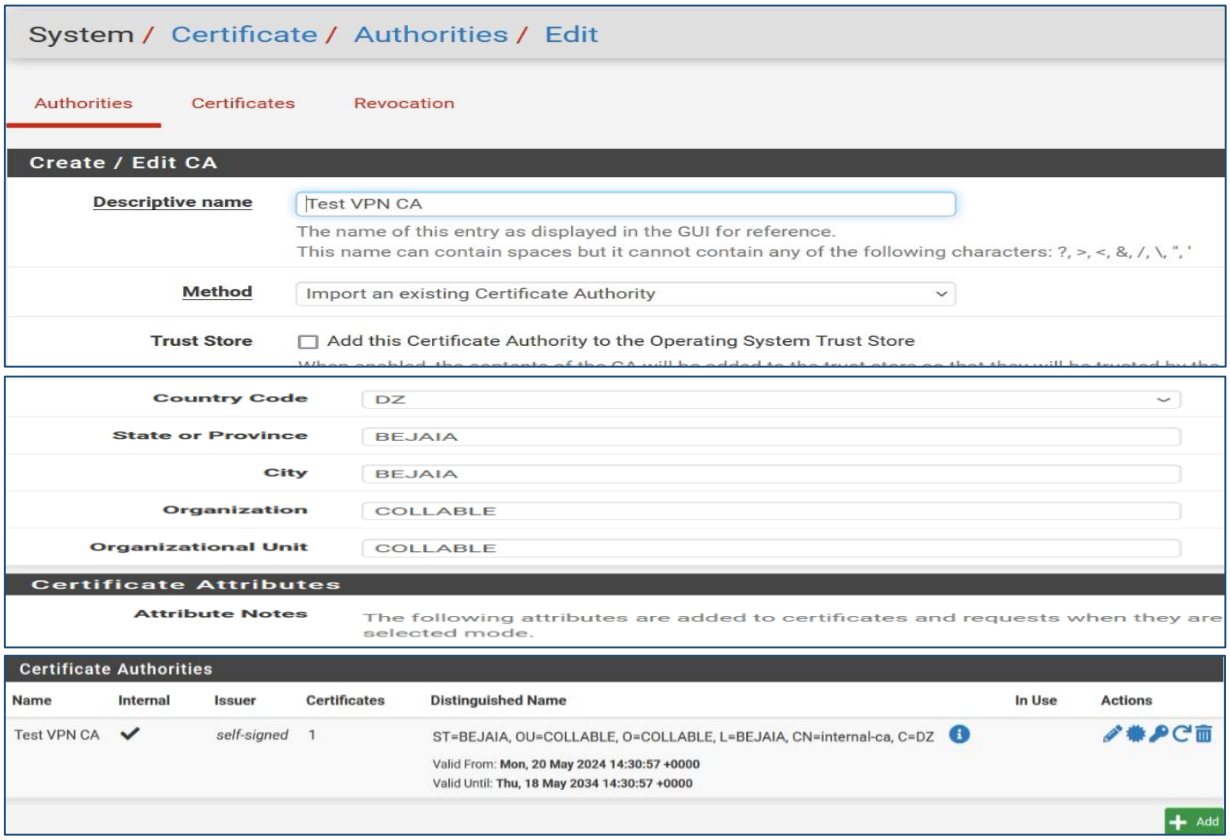


Figure 4.50 : *Autorité de certificat*

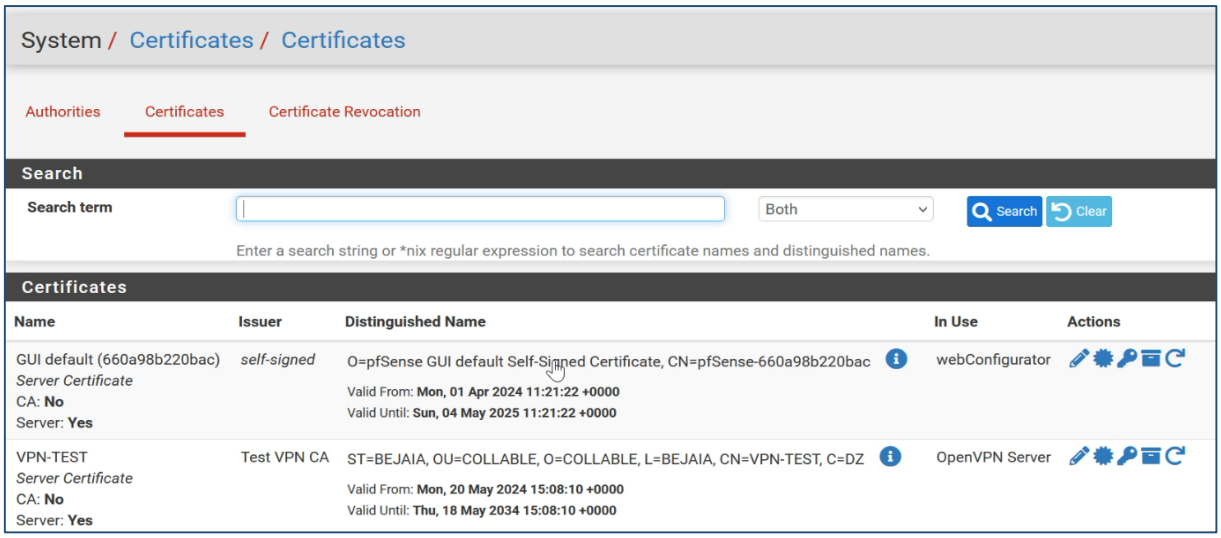
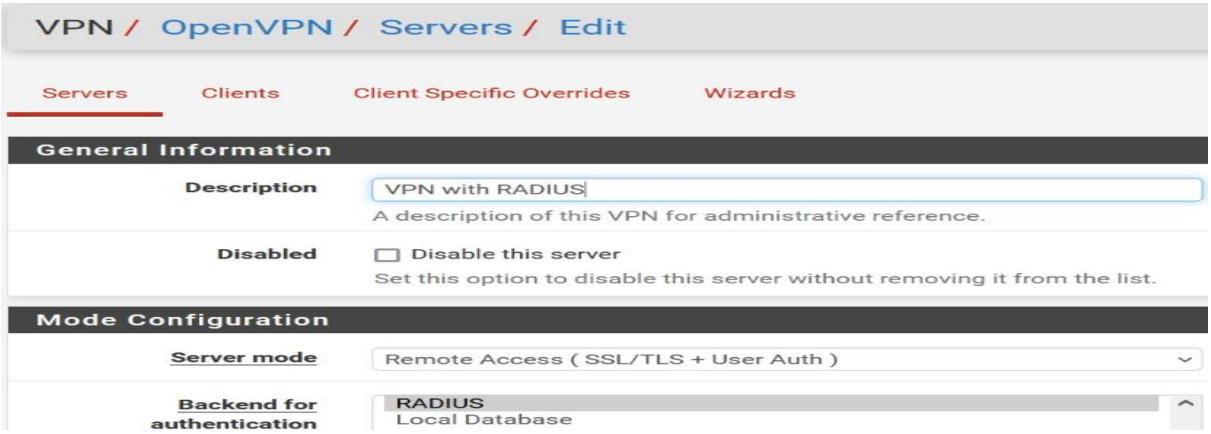


Figure 4.51 : *Création de certificat*

8.11.3 Création d'un VPN pour le serveur



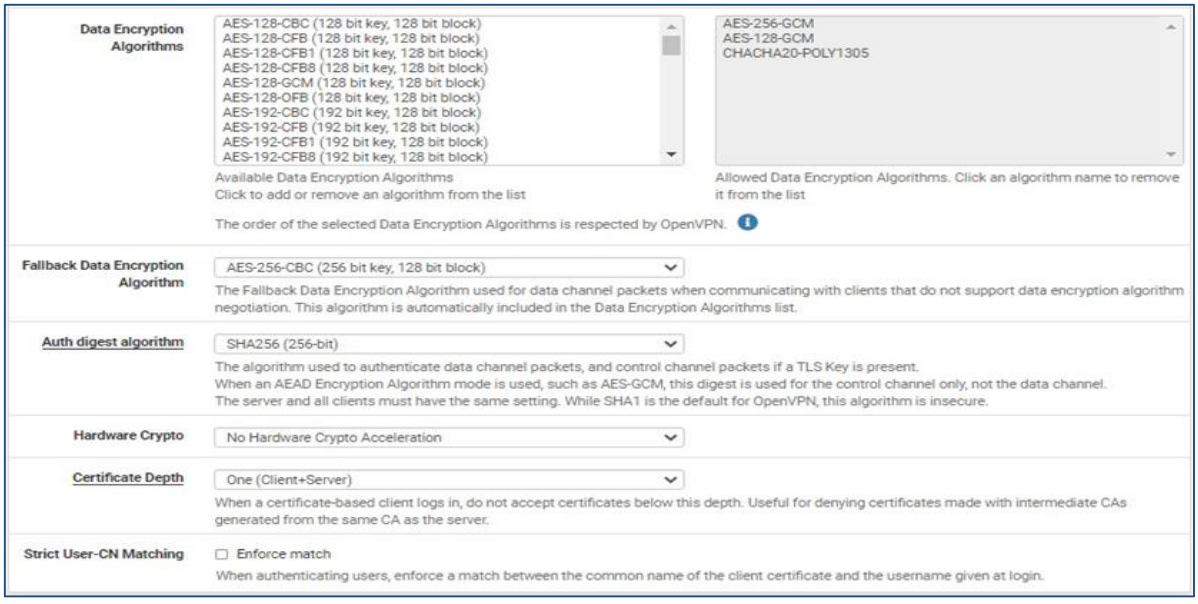


Figure 4.52 : *Création d'un server VPN*

8.11.4 Téléchargement du package pour les clients open VPN

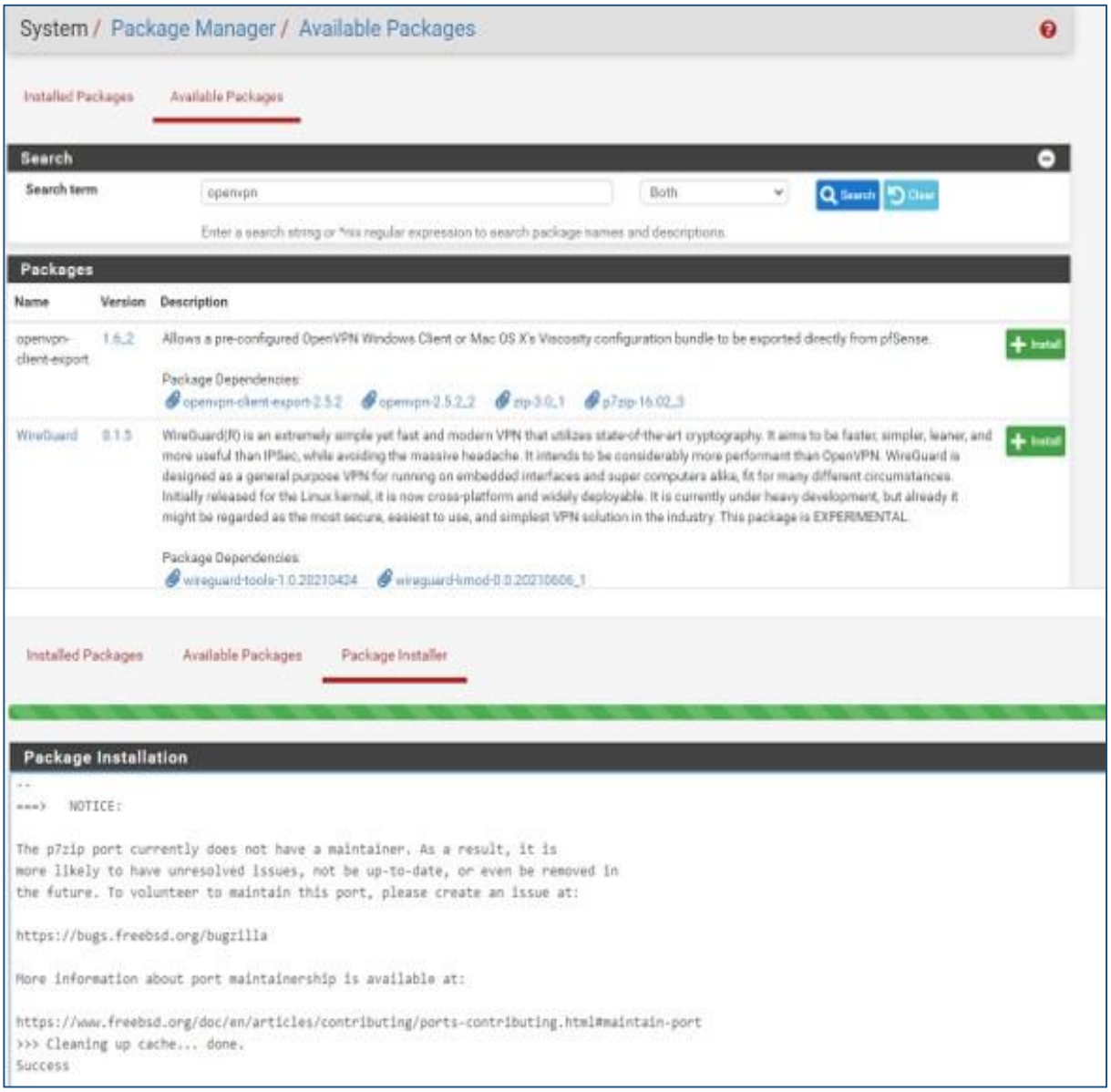


Figure 4. 53 : *Téléchargement de package pour les clients open VPN*

8.11.5 Exportation de la configuration Open VPN

- Exporter la configuration open VPN :

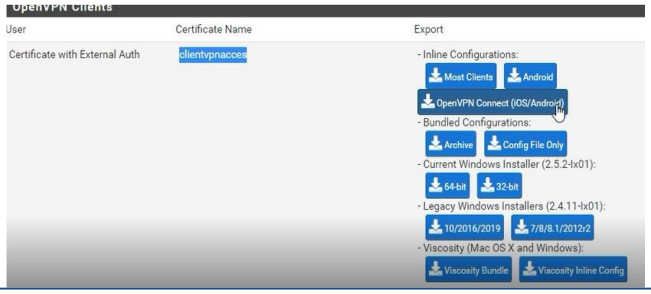


Figure 4.54 *: Exporter la configuration open VPN*

9 Tests

9.1 Tests de connectivité

9.1.1 Tests d'affectation des ports au VLANs

```
SWA2#show  vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/3, Et1/0, Et1/1, Et1/2
                                                 Et1/3, Et2/0, Et2/1, Et2/2
                                                 Et2/3, Et3/0, Et3/1, Et3/2
                                                 Et3/3
100  info/gestion                      active
101  server                            active
102  comptabilite                      active
103  RH                                active    Et0/1
104  Marketing                         active    Et0/2
105  invite                            active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
SWA2#
```

```
SWA1#show  vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/3, Et1/0, Et1/1, Et1/2
                                                 Et1/3, Et2/0, Et2/1, Et2/2
                                                 Et2/3, Et3/0, Et3/1, Et3/2
                                                 Et3/3
100  info/gestion                      active    Et0/2
101  server                            active
102  comptabilite                      active    Et0/1
103  RH                                active
104  Marketing                         active
105  invite                            active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
SWA1#
```

```
SWD#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/2, Et1/0, Et1/1, Et1/2
                                                 Et1/3, Et2/0, Et2/1, Et2/2
                                                 Et2/3, Et3/0, Et3/1, Et3/2
                                                 Et3/3
100  info/gestion                      active
101  server                            active    Et0/3
102  comptabilite                      active
103  RH                                active
104  Marketing                         active
105  invite                            active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
SWD#
```

Figure 4.55 : *Tests d'affectation des ports au VLANs*

9.1.2 Résultats des différents tests de connectivité

- **Ping de PC1 vers l'internet et la Gateway**

```
C:\Users\PC1>ping 8.8.8.8

Envoi d'une requête 'Ping'  8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=331 ms TTL=125
Réponse de 8.8.8.8 : octets=32 temps=359 ms TTL=125
Réponse de 8.8.8.8 : octets=32 temps=413 ms TTL=125
Réponse de 8.8.8.8 : octets=32 temps=411 ms TTL=125
```

```
C:\Users\PC1>ping 10.0.100.254

Envoi d'une requête 'Ping'  10.0.100.254 avec 32 octets de données :
Réponse de 10.0.100.254 : octets=32 temps=1771 ms TTL=64
Réponse de 10.0.100.254 : octets=32 temps=2227 ms TTL=64
Réponse de 10.0.100.254 : octets=32 temps=1784 ms TTL=64
Réponse de 10.0.100.254 : octets=32 temps=3507 ms TTL=64
```

Figure 4.56 : *Ping de PC1 vers l'internet et la Gateway*

- **Test de serveur vers Internet, Gateway et Switch d'accès 1**

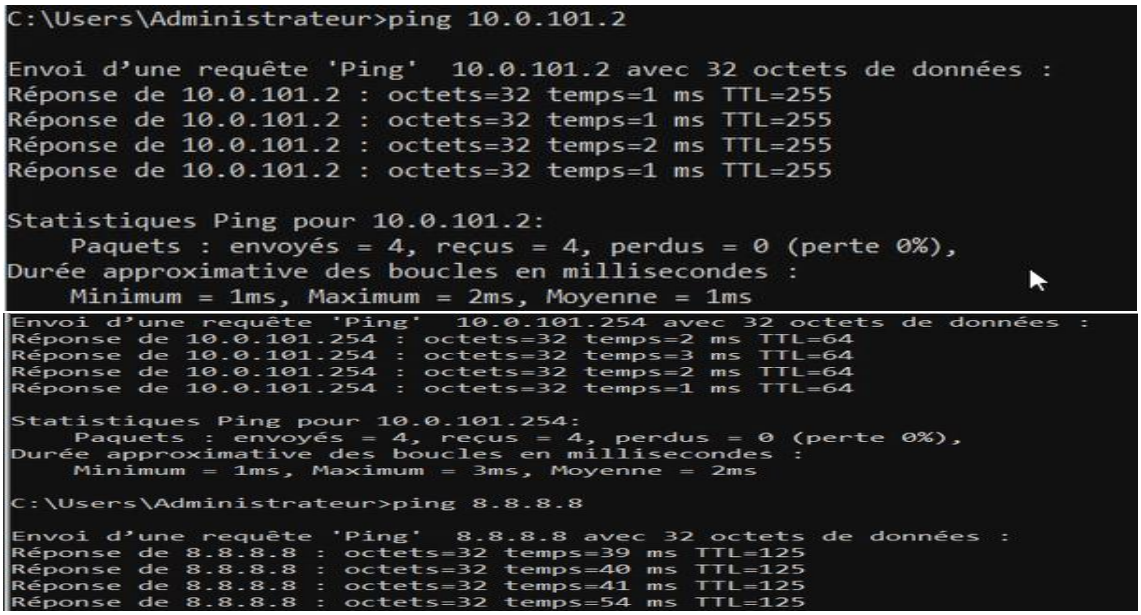


Figure 4.57 : *Ping de serveur vers l'internet, la Gateway et switch d'accès 1*

- **Test DHCP**
  - **Supprimer l'adresse IP de PC1**

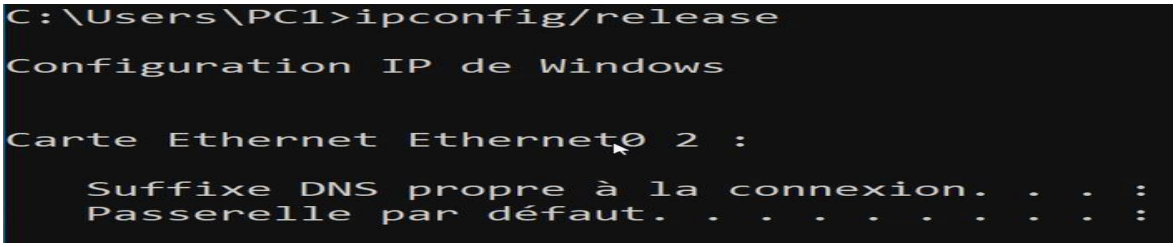


Figure 4.58 : *Test DHCP : Supprimer l'@ IP de PC1*

  - **Demander une adresse IP de PC1**

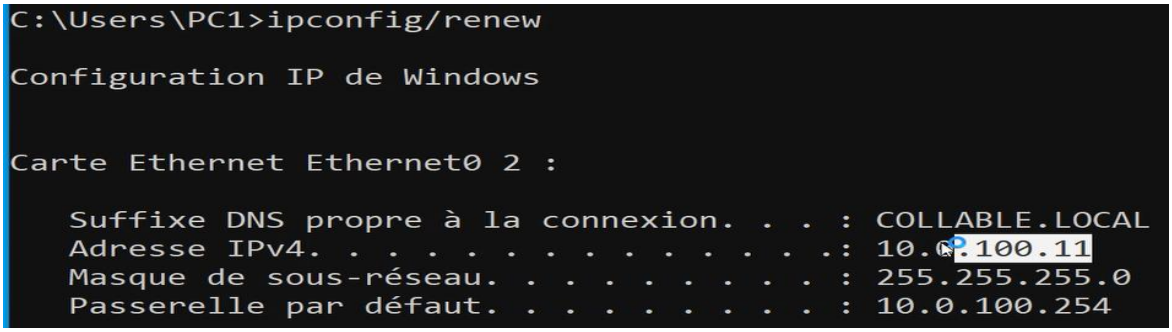


Figure 4.59 : *Test DHCP : Demander l'@ IP de PC1*

- **Dernière étape :** aller sur server et vérifier l'adresse IP de PC1.

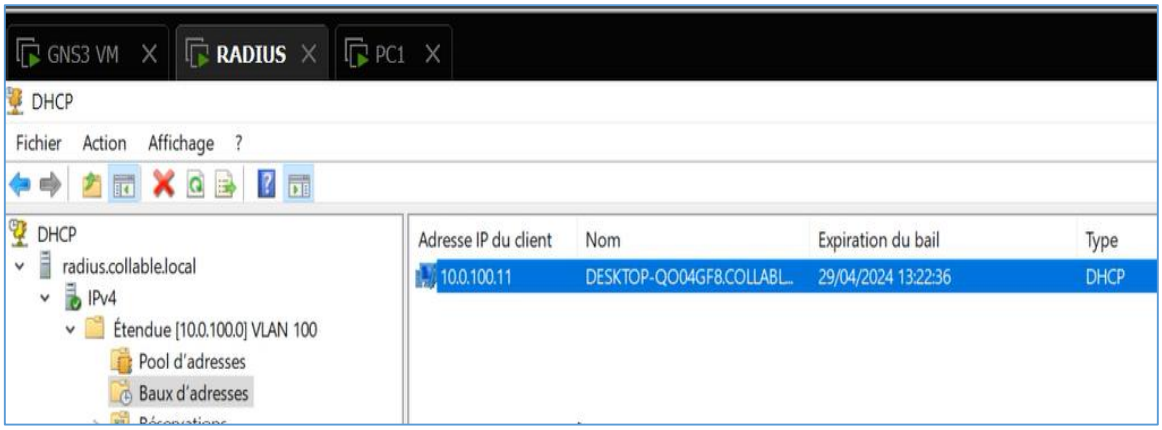
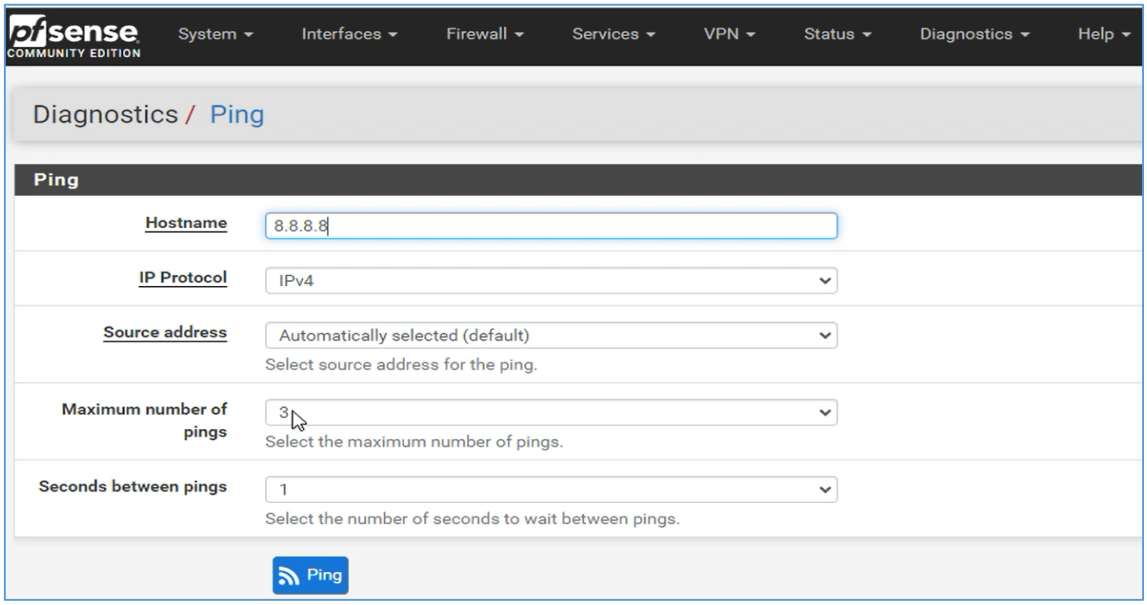


Figure 4.60 : *Vérification de l'@ IP de PC1 dans le serveur*

- **Test PfSense**



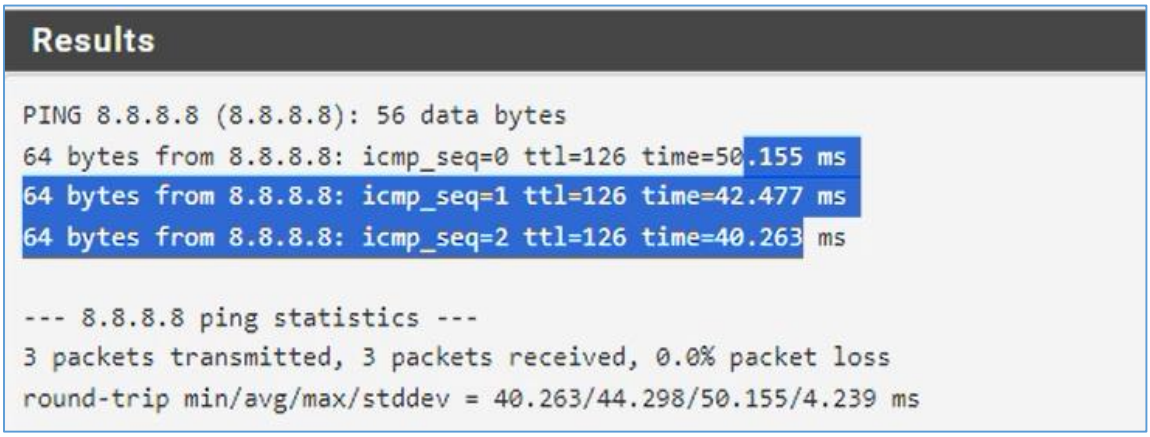


Figure 4.61 : *Test de pfsense*

9.2 Test d'authentification par certificat

9.2.1 Cas autorisé (authentification réussie)

Sur la console du switch Client Radius à l'aide de la commande show authentification sessions interface Ethernet 0/2, nous allons voir si la 802.1x est Configuré, et à l'aide de la commande show authentification sessions interface Ethernet 0/2 détail nous verrons que l'authentification est faite avec succès même sur wireshark.

```
Compressed configuration from 2116 bytes to 1244 bytes[OK]
SW1#show authentication sessions interface ethernet 0/2 details
            Interface:  Ethernet0/2
          MAC Address:  000c.2933.2949
         IPv6 Address:  Unknown
         IPv4 Address:  10.0.100.11
            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:  0A006502000000C00032762
     Acct Session ID:  Unknown
              Handle:  0x31000001
      Current Policy:  POLICY_Et0/2

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

Server Policies:
          Vlan Group:  Vlan: 100

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

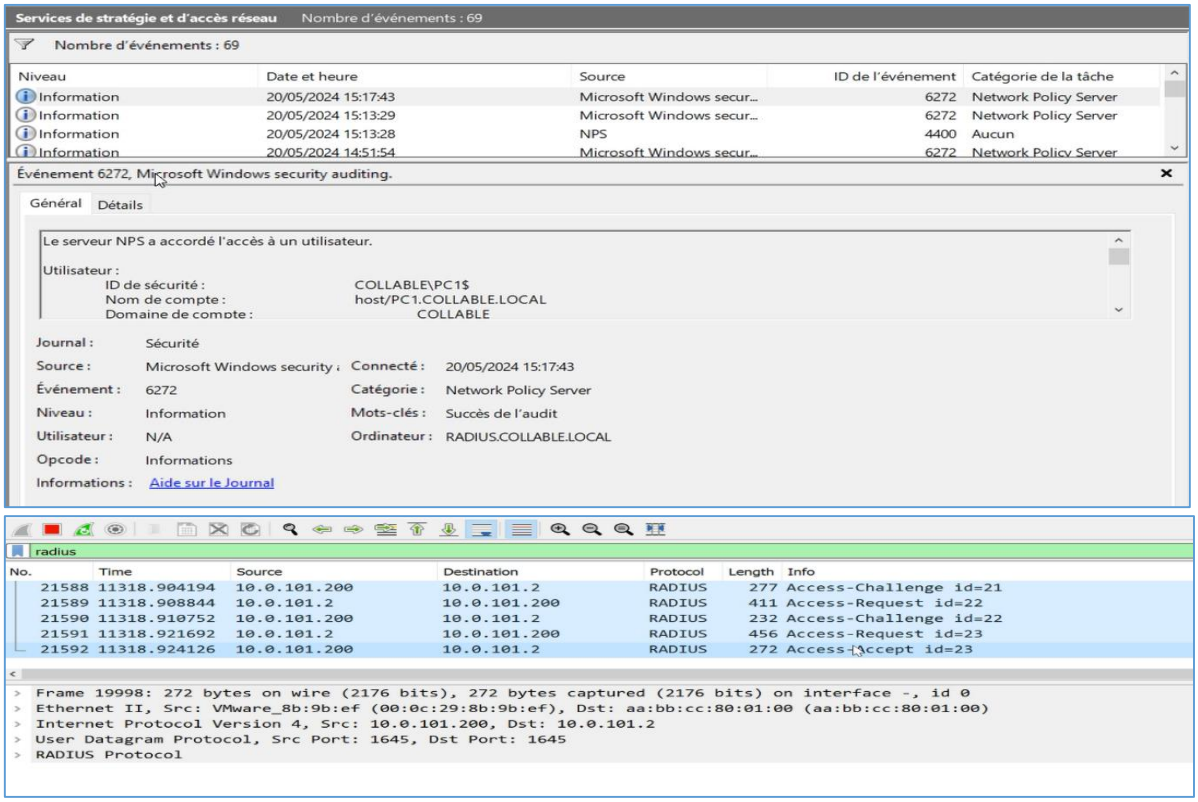


Figure 4.62 : *Résultats d'authentification par certificat : Cas autorisé*

9.2.2 Cas non autorisé

Dans le cas où l'authentification a échoué, nous observons qu'il y a un échec d'authentification comme le représente la figure 4.57.

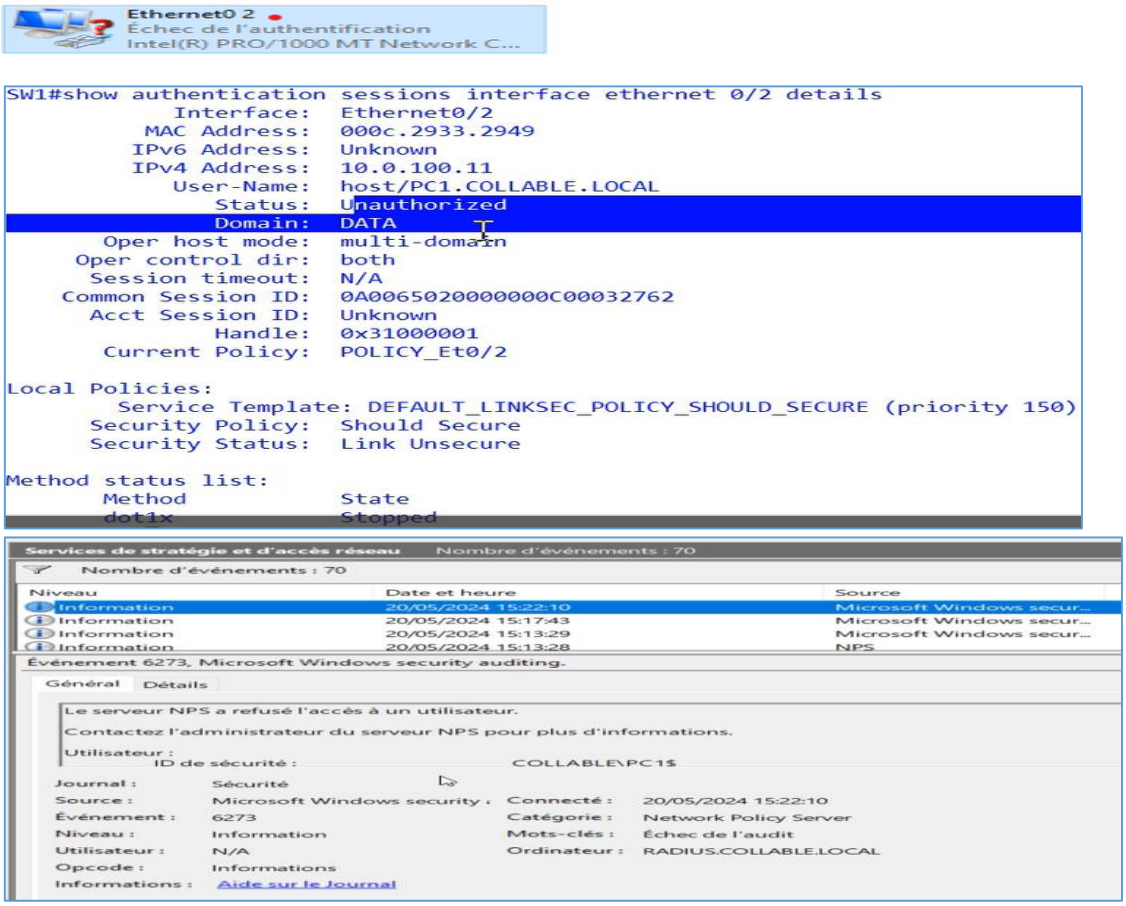


Figure 4.63 : *Résultats d'authentification par certificat : Cas non autorisé*

9.3 Test VPN

Ouvrir l'application OpenVPN pour tester l'accès à distance du client.

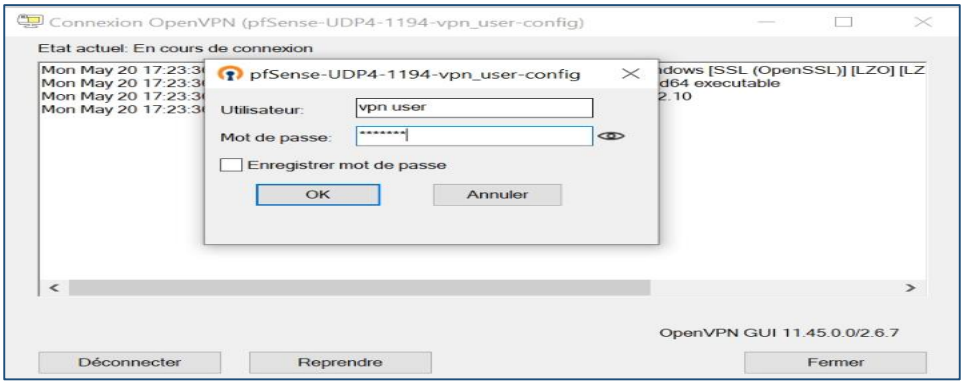


Figure 4.64 : *Test VPN*

Conclusion

Le Serveur de contrôle d'accès Radius constitue une réponse aux problématiques de connexion au réseau local et permet de mieux contrôler l'accès au réseau. Radius présente l'avantage d'être simple à installer. De plus, le fait qu'il reconnait les comptes déjà existants dans Active Directory, l'administrateur réseau ne va pas recréer ces comptes une deuxième fois sur équipement. Parvenu au terme de notre étude, on peut retenir qu'après l'identification des utilisateurs, leur Authentification est nécessaire pour accéder aux données d'un système.

Cette authentification, se fait par l'intermédiaire d'un serveur d'authentification, chargé d'autoriser ou de refuser l'accès aux données. Afin de permettre le service d'authentification, ce serveur nécessite une configuration de ses composants, ce fut là le but de notre travail.

Conclusion générale

La Direction de la SARL Collable souhaitait améliorer la sécurité de son réseau informatique en s'assurant de l'identité des utilisateurs et des ordinateurs accédant à son Système d'Information.

Une analyse exhaustive des besoins et des contraintes de l'entreprise, qui a souligné la difficulté de sécuriser l'accès au réseau local, nous a conduit à la conclusion que seule l'utilisation du protocole d'authentification RADIUS et la norme 802.1x permettaient de répondre à la problématique.

La réalisation de ce projet a été très enrichissante que ce soit au niveau technique par la découverte du protocole RADIUS et des différentes technologies mises en œuvre, mais aussi au niveau de la gestion d'un projet. Loin de devoir nous focaliser sur des questions purement techniques, il nous a été nécessaire de prendre du recul afin d'avoir une vision globale pour bien prendre en compte les contraintes de l'entreprise et mesurer les impacts des choix à faire. La bonne conduite d'un projet est exigeante en termes d'organisation et de communication.

La réalisation de ce mémoire a été une occasion plus particulière de mettre en application les connaissances acquises durant notre formation.

Nous avons également eu beaucoup de plaisir à apprendre et à nous familiariser avec le Windows server 2022 pour mieux gérer la sécurité de notre architecture réseau.

Pour conclure ce mémoire, nous souhaiterions rajouter qu'il faut garder à l'esprit que la sécurité totale n'existe pas. Il s'agit d'un compromis entre les contraintes qui peuvent être supportées.

BIBLIOGRAPHIE

[1] M. Yazid, « *Cours Administration des réseaux*», Cours de Master 2 en informatique, Université de Bejaïa, 2024.

[2] J. Dordoigne, « *Réseaux informatiques, notions fondamentales (protocoles, architectures, réseaux sans fil, virtualisation, sécurité, IP v6 …* » 6ème Edition, 2002.

[3] S. Ghernouati-Hélie, « *Sécurité informatique et réseaux* », Dunod, 3éme édition, 2008.

[4] M. Rizcallah, « *Annuaire LDAP* », EYROLLES, édition 2002.

[5] G. Mathieu, « *Tester la sécurité de son annuaire Active Directory V2* », version du 30 janvier 2016.

[6] D. Lachiver, « *Utilisation du réseau pédagogique* », édition 2013.

[7] S. Bordères, « *Authentification réseau avec Radius* », EYROLLES, édition 2006.

[8] W. Simpson, « *PPP Challenge Handshake Authentication Protocol (CHAP)* », édition 1996.

[9] M. Chateau, « *Windows Server 2008 R2 administration avancée* », 2ème édition, Eni édition, 2011.

[10] J. Delduca, «*La sécurité informatique en mode projet-organisez la sécurité du SI de votre entreprise*», ENI, 2010.

[11] S. Bordères, « *Authentification réseau avec Radius* », EYROLLES, édition 2000.

[12] S. Bouaziz, N. Farez « *Sécuriser un réseau Wifi en implémentant le protocole d'authentification 802.1x sur le serveur RADIUS* », mémoire fin d'études, Univ. Tizi-Ouzou 2012/2013.

[13] G. Pujolle, « *Les réseaux* », EYROLLES, Paris, 8éme édition, 2014.

[14] J. Sebban, « *Analyseur de paquets réseau pour les pros* », édition 1997.

Résumé

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

L'objectif de la présente étude consiste à étudier l'authentification des utilisateurs du réseau filaire ou sans fil qui se base sur le protocole RADIUS et la norme 802.1x.

Pour l'implémentation de ce travail, nous avons choisi Windows Server 2022 qui inclut le serveur d'authentification RADIUS pour la gestion des utilisateurs.

Mots-clés : IEEE 802.1x, Authentification, RADIUS, Windows Server 2022, cas: SARL Collable.

Abstract

This document is part of our final year project for obtaining the master's degree in Computer Science, specializing in Network Administration and Security at ABDERRAHMANE Mira University in Béjaïa. It describes our work during our internship at SARL Collable.

The objective of this study is to study the authentication of wired or wireless network users based on the RADIUS protocol and the 802.1x standard.

For the implementation of this work, we chose Windows Server 2022 which includes the RADIUS authentication server for user management.

Keywords: IEEE 802.1x, Authentication, RADIUS, Windows Server 2022, case: SARL Collable.