République Algérienne Démocratique et Populaire
Ministère de l'enseignement et de la Recherche Scientifique
Université A. Mira- Bejaia
Faculté des Sciences Exactes
Département Informatique

Mémoire de fin de cycle

En vue d'Obtention du Diplôme de Master Professionnel en Informatique Option : Administration et Sécurité des Réseaux

Thème

Étude et mise en place de l'authentification RADIUS par certificat PEAP/TLS

Cas d'étude : SONATRACH

Réaliser par :

BEKKA Aimad

BENKHELLAT Oussama

Devant le jury composé de :

Le président	Dr	Farah Zoubeyr	U. A/Mira Bejaïa.
Examinateur	Dr	Bouchebbah Fatah	U. A/Mira Bejaïa.
Encadrant	Dr	Touazi Djoudi	U. A/Mira Bejaïa.

Année Universitaire : 2023-2024

REMERCIEMENTS

Tout d'abord, nous exprimons notre gratitude envers le bon Dieu, qui nous a accordé la force et le courage nécessaires pour mener à bien ce modeste travail.

Nous tenons également à exprimer notre profonde reconnaissance à Mr Touazi, notre promoteur, pour son aide précieuse et son accompagnement tout au long de cette expérience professionnelle. Ses conseils et ses encouragements nous ont été d'une grande aide pour mener à bien ce travail.

Nous remercions chaleureusement les membres du jury pour avoir accepté d'examiner et d'évaluer notre travail.

Notre gratitude s'étend à tous les enseignants qui ont assuré notre formation tout au long de notre cycle universitaire.

Nous adressons nos sincères remerciements à l'organisme d'accueil SONATRACH, qui nous a accueillis comme stagiaires et nous a offert l'opportunité de découvrir le monde professionnel.

Enfin, nous souhaitons exprimer notre profonde gratitude à nos chers parents et familles pour leurs sacrifices, leur soutien et leurs encouragements constants.

Tanmirt-nwen!

DEDICACE

Je remercie le Bon Dieu de m'avoir donné le courage, la santé et la volonté nécessaires pour mener à bien ce modeste travail.

Je le dédie particulièrement à mes très chers parents, qui sont ma raison de vivre, pour leurs sacrifices, leur patience, leur présence et leur soutien tout au long de mes études. Que Dieu les garde et les protège.

À la mémoire de mes chers grands-parents ;

À ma sœur Imane;

À mes tantes Zahia, Assia, Hassiba, Malika, Lamia, Chala et Hadjira ;

À mes cousins et cousines Salah, Samira, Amine, Fodil, Ryad, Dodo, Mehdi, Anis et Lina ;

À mon binôme Oussama et à sa famille ;

À mes amis et camarades Oussama, Rahim, Rabah, Sabrine et Amina ;

À tous les étudiants en 2ème année de Master Informatique de l'Université de Bejaïa.

Avec toute ma gratitude et mon affection.

Aimad

DEDICACE

Je remercie le Bon Dieu de m’avoir donné le courage, la santé et la volonté nécessaires pour mener à bien ce modeste travail.

Je dédie particulièrement ce travail à la mémoire de mon défunt père, qui restera à jamais vivant dans mon cœur, ainsi qu'à ma chère mère, ma raison de vivre. Leurs sacrifices, leur patience, leur présence et leur soutien tout au long de mes études ont été inestimables. Je vous serai à jamais reconnaissant.

À la mémoire de mes grands-parents décédés et en gratitude envers mes grands-parents vivants pour leur amour et leur soutien. Que Dieu les bénisse tous ;

À ma sœur S, mes frères Zakaria et Chems Eddine et à mon beau frère Salah;

À mes oncles et tantes;

À mes cousins et cousines;

À mon binôme Aimad et à sa famille;

À mes cousins et voisins Abiga, Zhayer, Rayane, Boutis, Moussa, Handal, Lmous, Khourou, HANI, Yelli, La suite;

À mes amis Nassim, Massi, Adnane, Houcine, Omar, Ahcen, Seifeddine, Raouf;

À mes camarades Sabrine, Amina, Massi, Cylia;

Et à tous ceux qui ont contribué de près ou de loin à la réalisation de ce projet, Thanmirth.

Oussama

Table des matières

Table des matières

Table des matières

Table des figures

Table des figures

LISTE DES TABLEAUX

Glossaire

AAA: Authentication, Authorization, and Accounting.

ACL : Access Control List.

AD : Active Directory.

AES : Advanced Encryption Standard.

BDD : Base de Données.

DES : Data Encryption Standard.

DHCP : Dynamic Host Configuration Protocol.

DOS : Denial of Service.

EAP : Extensible Authentication Protocol.

HTTP : Hypertext Transfer Protocol.

IA : Intelligence Artificielle.

IEEE : Institute of Electrical and Electronics Engineers.

IGMP : Internet Group Management Protocol.

IP : Internet Protocol.

IPSec : Internet Protocol Security.

IPv6 : Internet Protocol version 6.

IPS : Intrusion Prevention System.

JWT : JSON Web Token.

JSON : JavaScript Object Notation.

3LDAP : Lightweight Directory Access Protocol.

MAC : Media Access Control.

MFA : Multi-Factor Authentication.

MITM : Man-In-The-Middle.

MK : Master Key.

MS-CHAP : Microsoft Challenge-Handshake Authentication Protocol.

NAS : Network Attached Storage.

NAC : Network Access Control.

Glossaire

OAuth : Open Authorization.

PEAP : Protected Extensible Authentication Protocol.

PIN : Personal Identification Number.

PKI : Public Key Infrastructure.

PoE : Power over Ethernet.

Radius : Remote Authentication Dial-In User Service.

RFC : Request for Comments.

SHA : Secure Hash Algorithm.

SNMPv3 : Simple Network Management Protocol version 3.

SSH : Secure Shell.

SSL : Secure Sockets Layer.

SSO : Single Sign-On.

SONATRACH : Société Nationale pour la Recherche, la Production, le Transport, la Transformation et la Commercialisation des Hydrocarbures.

Tacacs : Terminal Access Controller Access-Control System.

TCP : Transmission Control Protocol.

TLS : Transport Layer Security.

TTLS : Tunneled Transport Layer Security.

UDP : User Datagram Protocol.

URI : Uniform Resource Identifier.

USB : Universal Serial Bus.

VLAN : Virtual Local Area Network.

VPN : Virtual Private Network.

VTP : VLAN Trunking Protocol.

WAF : Web Application Firewall.

Web : World Wide Web.

WIFI : Wireless Fidelity.

WPA : Wi-Fi Protected Access.

XTacacs : Extended Terminal Access Controller Access-Control System.

Introduction générale

Les réseaux informatiques constituent le fondement de l'infrastructure technologique au sein d'une entreprise, permettant une communication interne et externe entre les différents départements, employés et services. De plus, ils assurent une transmission sécurisée et une sauvegarde centralisée des données, garantissant ainsi le bon fonctionnement et la protection des activités de l'entreprise.

Les réseaux d'entreprise modernes englobent plusieurs types d'accès aux réseaux, suite à la variété des méthodes d'accès, les entreprises rencontrent des défis de gestion des identités et des droits d'accès et de détection des activités suspectes. En premier lieu, l'accès filaire nécessite une authentification robuste pour prévenir les intrusions physiques et les accès non autorisés à travers les points de connexion réseau. L'accès sans fil, quant à lui, introduit des vulnérabilités supplémentaires en raison de sa nature ouverte et facilement interceptable, en parallèle, l'accès à distance, qui pose des défis uniques en matière de vérification de l'identité sur les réseaux souvent non sécurisés.

Afin de garantir une bonne gestion des accès et limiter l'intrusion des entités non autorisées, les entreprises adoptent des stratégies de sécurité efficaces et mettent en place une politique gérante des différents matériaux et niveaux d'accès.

Notre objectif est donc de mettre en place une solution d'authentification permettant de sécuriser l'accès filaire des utilisateurs au réseau de l'Entreprise SONATRACH de Bejaia.

Pour atteindre cet objectif nous avons appliqué le protocole d'authentification RADIUS (Remote Access Dial In User Services) qui s'appuie à la fois sur le standard 802.1X dont l'objectif principale est de permettre l'accès physique à un réseau local après une phase d'authentification et le protocole PEAP (Protected Extensible Authentication Protocol) ainsi qu'une combinaison de plusieurs outils : Switch, pare-feu et serveur RADIUS intégrés sous Windows server 2022.

Notre mémoire est organisé en quatre chapitres comme suit :

Le premier chapitre nommé " présentation d'organisme d'accueil" aura pour but de fournir une meilleure compréhension de l'entreprise où nous avons effectué notre stage, sa structure hiérarchique, son réseau informatique et les différents matériels utilisés, ainsi que la problématique posée et la solution proposée pour la résoudre.

Le deuxième chapitre s'intitule "la sécurité des réseaux informatiques" consiste à définir les notions de bases da la sécurité.

Dans le troisième chapitre, nous effectuerons une analyse approfondie de la solution proposée ainsi que sa mise en œuvre concrète. Cette solution s'appuie sur l'utilisation du protocole 802.1x, associé à un serveur d'authentification RADIUS utilisant des certificats PEAP/TLS, dans le cadre d'un modèle AAA (Authentication, Authorization et Accounting).

Le quatrième chapitre, concerne la mise en pratique de ces concepts et détaille l'implémentation des mécanismes et protocoles choisis. Et nous avons conclus le travail en effectuant des tests afin de garantir l'efficacité de la solution implémentée.

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

Chapitre I :
Présentation de l'organisme d'accueil

I.1 Introduction

Analyser l'organisme d'accueil revêt une importance crucial servant à représenter les contraintes sous lesquelles se réalisera notre projet. Ainsi nous allons présenter l'entreprise SONATRACH et les différents départements qui la composent, fournir des informations clés pour notre travail tout en posant la problématique qui constituera le pivot de notre mémoire. Dans cette optique, nous pouvons concevoir une solution adéquate à implémenter.

I.2 Présentation générale de l'organisme d'accueil

SONATRACH est la Société Nationale pour la Recherche, la Production, le Transport, la Transformation et la Commercialisation des Hydrocarbures. Il s'agit de la principale entreprise publique algérienne opérant dans le secteur pétrolier et gazier. Fondée en 1963, SONATRACH est l'une des plus grandes sociétés pétrolières et gazières en Afrique et dans le monde.

Le logo de l'entreprise est sur la FIGURE 1.1 :

Figure 1.1: Logo de Sonatrach.

I.3 Historique, missions et activités de l'Entreprise

L'entreprise SONATRACH a été créé le 31 décembre 1963 par le décret n°63/491, les statuts ont été modifiés par le décret n°66/292 du 22 septembre 1966, et SONATRACH devient Société nationale pour la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures», cela a conduit à une restructuration de l'entreprise dans le cadre d'un schéma directeur approuvé au début de l'année 1981 pour une meilleure efficacité organisationnelle et économique, Ce qui a mené en 1986 à l'adoption d'une politique plus

ouverte aux relations d'association avec des partenaires étrangers et affiche son ambition de devenir un groupe pétrolier de dimension international.

Aujourd'hui Sonatrach est un acteur majeur de l'économie algérienne, contribuant largement au budget de l'État et au développement du pays, et s'engage également dans le développement durable et la responsabilité sociétale.

SONATRACH s'articule autour de trois activités principales pour concrétiser ses objectifs stratégiques :

- **Exploration et Production :**
  - **Objectif :** Découvrir et exploiter de nouveaux gisements d'hydrocarbures pour répondre à la demande croissante en énergie.
  - **Activités clés :** Exploration pétrolière et gazière, production d'hydrocarbures, optimisation des procédés de production, gestion des réservoirs.
- **Transport et transformation :**
  - **Objectif :** Acheminer, stocker et transformer les hydrocarbures pour les rendre commercialisables.
  - **Activités clés :** Gestion du réseau de transport, exploitation des infrastructures de stockage, raffinage du pétrole brut, liquéfaction de gaz naturel.
- **Commercialisation et développement :**
  - **Objectif :** Vendre les hydrocarbures et produits dérivés sur les marchés nationaux et internationaux, tout en diversifiant les activités et en investissant dans la recherche et le développement.
  - **Activités clés :** Commercialisation des hydrocarbures, négociation de contrats, diversification des activités, recherche et développement.

SONATRACH est divisée en cinq branches à l'échelle nationale, comme illustré dans la figure suivante :

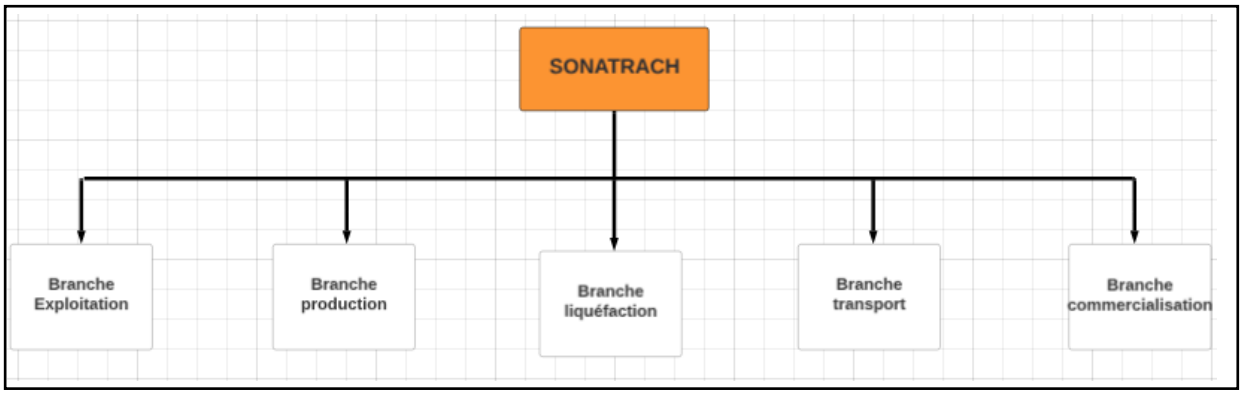

Figure 1.2: Les branches de Sonatrach.

I.4 Les directions régionales de transport de SONATRACH

SONATRACH possède cinq directions régionales de transport des hydrocarbures :

- La direction régionale Est (Skikda).
- La direction régionale Centre (Bejaïa).
- La direction régionale Ouest (Arzew).
- La direction régionale de Haoud-EL-Hamra.
- La direction régionale d'Ain Amenas.

I.5 Présentation de la RTC (Région Transport Centre)

La direction régionale de transport de Béjaïa, est l'une des cinq directions régionales de transport des hydrocarbures de la SONATRACH (RTC). Elle se charge de l'acheminement des hydrocarbures pétroles brut, gaz et condensat vers les ports pétroliers, les zones de stockages et les pays d'exploitation.

Parmi les missions qui lui sont affectées, on peut citer :

- L'entretien, la maintenance et la protection des ouvrages et canalisations.

- L'exploitation et la gestion des ouvrages et canalisations de transport d'hydrocarbures.
- La gestion de l'interface transport des projets internationaux du groupe ou en partenariat.

La direction régionale de Béjaïa est composée de plusieurs entités, comme illustré dans l'organigramme ci-dessous. Notre travail se concentre sur le centre informatique.

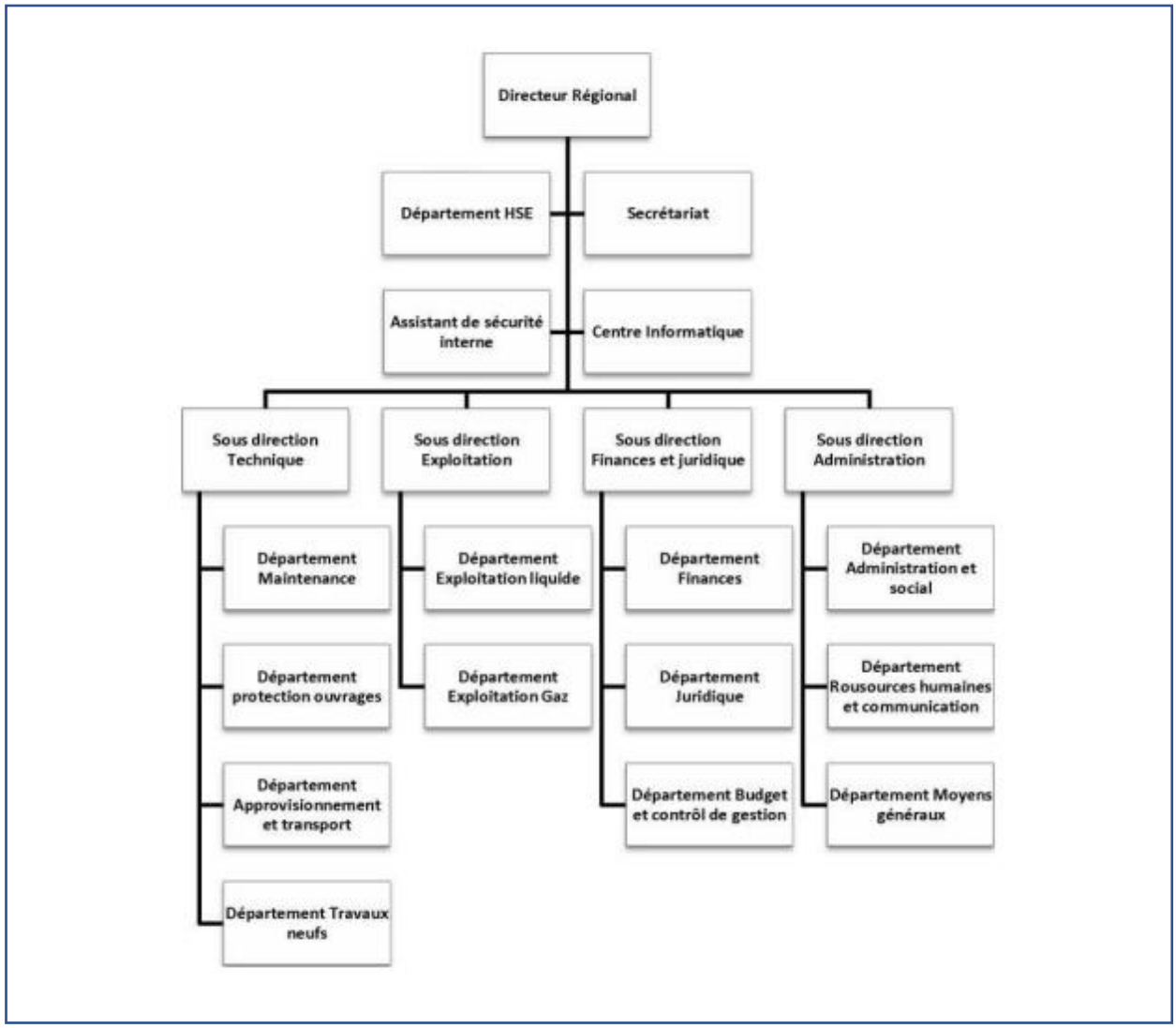

Figure 1.3: Organigramme de l'organisation de la direction régionale de Bejaïa.

I.6 Présentation du centre informatique

Le centre informatique joue un rôle essentiel dans la gestion et l'optimisation des systèmes informatiques et des données au sein de l'organisation. Il est constitué de trois services (service système et réseau, service base de données et logiciel et service support technique).

- **Fonctions principales d'un centre informatique**

  Parmi ces fonctions on peut citer **:**

  - **Hébergement et gestion des systèmes informatiques :** Abrite les serveurs, les ordinateurs centraux, les équipements de stockage et autres composants matériels qui supportent les applications et les systèmes d'information critiques.

  - **Stockage et sécurisation des données :** Assure le stockage sécurisé des données numériques, garantissant leur accessibilité, leur intégrité et leur confidentialité.

  - **Réseau et connectivité :** Gère le réseau informatique interne et les connexions externes, permettant aux utilisateurs d'accéder aux ressources informatiques et de communiquer entre eux.

  - **Sauvegarde et restauration des données :** Met en place des procédures de sauvegarde et de restauration régulières pour protéger les données contre les pertes ou les pannes système.

  - **Administration et maintenance :** Assure la surveillance continue des systèmes, la résolution des problèmes techniques et la mise à jour des logiciels et du matériel.

- Les services informatiques sont illustrés dans la figure suivante :

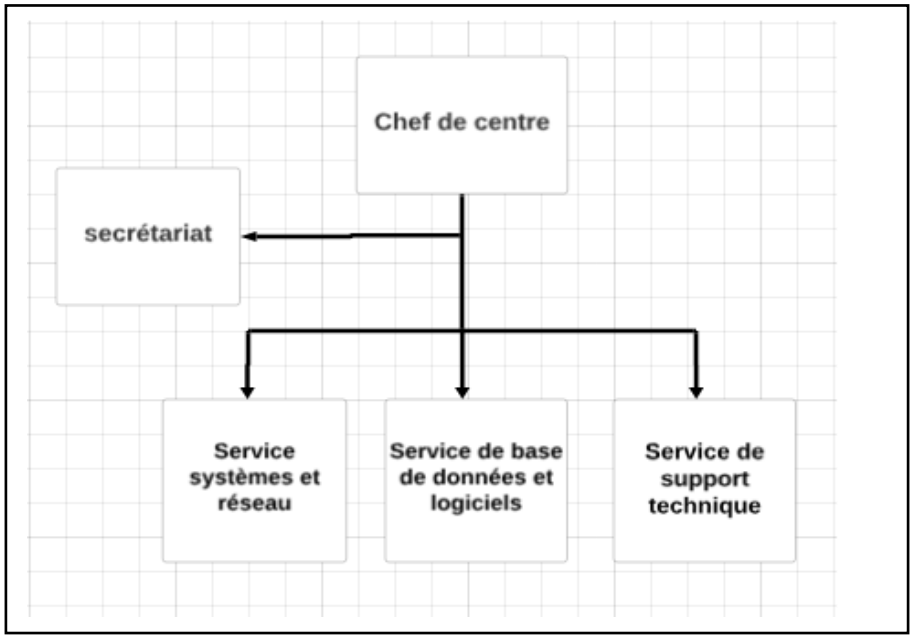

Figure 1.4: Les services du centre informatique de RTC.

I.7 Présentation du réseau de l'entreprise

L'entreprise SONATRACH RTC de Béjaïa utilise principalement des équipements de marque CISCO pour son infrastructure réseau. Cette préférence pour les produits CISCO s'explique par la réputation de fiabilité, de performance et de sécurité de cette marque dans le domaine des réseaux informatiques. Les équipements CISCO comprennent une gamme variée de commutateurs, de routeurs, de pare-feu et d'autres dispositifs réseau qui répondent aux besoins spécifiques de SONATRACH RTC en matière de connectivité, de gestion de réseau et de sécurité des données.

- **Les équipements utilisés dans le réseau de l'entreprise :**

a) **Catalyst Cisco 2950 :** sont des modèles autonomes, empilables et à configuration fixe, conçus pour fournir une connectivité Fast Ethernet et Gigabit Ethernet à vitesse filaire. Ils représentent une avancée en termes de performance et de fonctionnalités pour les réseaux locaux, avec des liaisons montantes 10/100/1000BaseT et un service IOS amélioré pour la gestion des données, de la voix et de la vidéo.

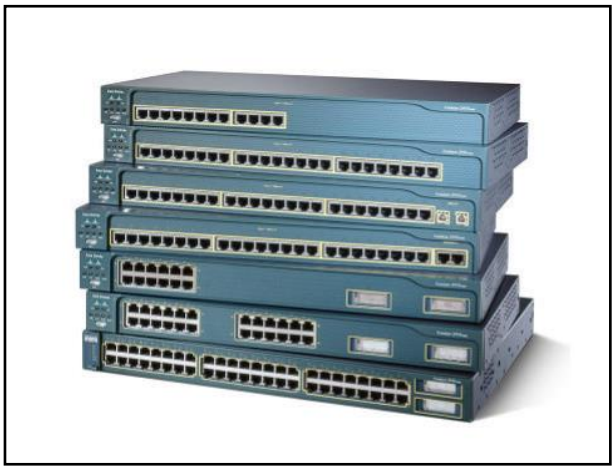

Figure 1.5: Commutateurs Catalyst Cisco 2950.

b) Catalyst Cisco 6500 : Ce commutateur, renommé pour sa fiabilité et sa robustesse, garantit une protection optimale des investissements en prenant en charge plusieurs générations de produits sur un même châssis. Il offre une évolutivité exceptionnelle, permettant l'ajout ou le remplacement de modules en fonction des besoins spécifiques du réseau.

Figure 1.6: Commutateurs Catalyst Cisco 6500.

c) Catalyst Cisco 3750 : Ce commutateur conçu pour les réseaux locaux d'entreprise. Avec sa capacité de gestion du trafic au niveau 2 et 3, il assure un contrôle précis et efficace des données au sein du réseau. Cette gamme de produits dispose de la technologie Cisco StackWiseTM, elle offre un Éventail étendue de fonctionnalités de sécurité, telles que l'authentification des utilisateurs et le contrôle d'accès, pour protéger les données sensibles contre les menaces potentielles.

Figure 1.7: Commutateurs Catalyst Cisco 3750.

d) Le pare-feu FortiGate : est un dispositif de sécurité réseau qui agit comme une barrière entre un réseau interne et des réseaux externes tels qu'Internet. Il filtre le trafic entrant et sortant en fonction de règles définies, telles que les adresses IP, les ports et les protocoles. Il intègre des fonctionnalités avancées telles que l'inspection des paquets, la prévention des intrusions (IPS) et la protection contre les logiciels malveillants. De plus, les modèles haut de gamme proposent des fonctionnalités supplémentaires comme le filtrage web, la protection contre les ransomwares et la gestion des identités et des accès.

➢ **Pourquoi FortiGate ?**

- **Intelligence Artificielle (IA) intégrée :** Certains modèles de FortiGate intègrent des fonctionnalités d'intelligence artificielle pour la détection et la prévention des menaces avancées, ce qui renforce encore la capacité de FortiGate à protéger les réseaux contre les attaques sophistiquées.
- **Gamme complète de fonctionnalités de sécurité :** FortiGate propose une suite complète de fonctionnalités de sécurité, y compris le pare-feu traditionnel, la prévention des intrusions (IPS), la détection des malwares, le contrôle d'accès réseau (NAC), la sécurité des applications Web (WAF), le VPN IPSec et SSL, et bien d'autres. Ces fonctionnalités sont soutenues par des protocoles de sécurité robustes tels que IPSec, SSL/TLS, et le protocole de gestion sécurisé SNMPv3.
- **Mises à jour logicielles gratuites :** Fournit des fonctionnalités de sécurité avancées sans frais supplémentaires.
- **Solution tout-en-un :** Intègre plusieurs fonctions de sécurité dans un seul appareil, réduisant ainsi les coûts d'acquisition et de maintenance.

I.8 Problématique

Le réseau de l'organisme Sonatrach est composé de nombreux postes informatiques reliés entre eux par un réseau local filaire et sans fil. Ce réseau permet aux collaborateurs internes de l'entreprise d'échanger des données et se connecter à l'internet. Cependant, la gestion des accès à ce réseau pose un certain nombre de défis.

Vu le grand nombre de postes informatiques possédé par les entreprises, il est important de prendre des mesures pour faire face aux défis rencontrer et essayer de les maitriser.

Parmi ces défis, citons :

Le manque de contrôle d'accès qui expose le réseau à des risques d'intrusions non autorisées, au vol de données et d'attaques malveillantes.

De plus, l'utilisation courante de l'authentification par mot de passe/nom d'utilisateur, une méthode connue pour sa vulnérabilité, en offrant une faible barrière de sécurité contre les attaques.

Parallèlement, l'absence de visibilité sur les activités des utilisateurs représente un autre défi majeur. Sans un système de supervision d'accès adéquat, il est difficile d'identifier et de tracer les actions des utilisateurs sur le réseau.

Enfin, le risque d'accès non autorisés reste une préoccupation constante. Les failles dans le contrôle d'accès et la configuration peuvent permettre à des individus malveillants d'exploiter les vulnérabilités sur le réseau afin d'accéder à des informations sensibles ou perturber le fonctionnement de système.

Compte tenu des obstacles auxquels nous faisons face, il est indispensable de mettre en place des solutions concrètes dans le but de renforcer le réseau d'entreprise et le rendre plus robuste.

I.9 Solutions proposées

Notre étude vise principalement à mettre en place une solution d'administration et d'authentification afin d'améliorer la gestion et la sécurité de l'accès aux services réseau de l'entreprise.

Pour garantir une authentification efficace et une gestion optimale des autorisations d'accès, ainsi que le suivi et l'enregistrement des activités des utilisateurs authentifiés, nous avons déployé le protocole RADIUS. Ce dernier centralise les informations d'identification des utilisateurs, simplifiant ainsi leur gestion. De plus, pour sécuriser l'accès aux réseaux, nous avons intégré le protocole 802.1x ainsi que la méthode PEAP-TLS. Cette approche utilise des certificats pour une authentification robuste et assure un transport sécurisé des données d'authentification.

I.10 Conclusion

Dans ce chapitre, nous avons abordé brièvement le fonctionnement du réseau de la RTC de Bejaia, cette étude nous a permis de maitriser les différentes structures informatiques de l'entreprise afin de mettre en place notre solution pour renforcer la sécurité du réseau.

Dans ce qui suit, nous étudieront les différentes techniques, méthodes et protocoles qui feront partie de notre étude.

Chapitre II :
Sécurité des réseaux informatiques

II.1 Introduction

De nos jours, la mise en réseau des équipements informatiques est devenue incontournable pour les entreprises. Quelle que soit la taille du réseau, la communication en temps réel et le partage d'informations sont essentiels pour améliorer l'efficacité opérationnelle. Cependant, cette connectivité accrue expose également les entreprises à des risques de sécurité croissants.

La sécurité des réseaux informatiques vise à protéger ces réseaux contre les menaces potentielles, telles que les cyberattaques, les intrusions et les violations de données. L'objectif de ce chapitre est de présenter les concepts clés de la sécurité des réseaux.

II.2 Définition de sécurité des réseaux informatiques

La sécurité des réseaux informatiques fait référence à un ensemble de mesures techniques(chiffrement), procédures (la politique de gestion des identifiants et des accès) et pratiques (la configuration et la gestion des pare-feu) misent en place dans le but de protéger les infrastructures, les systèmes et les données contre les fuites, intrusions et se prémunir contre les menaces croissantes du cyberespace.

La confidentialité, l'intégrité et la disponibilité sont les objectifs majeurs visés par la SRI afin de garantir le bon fonctionnement et la fiabilité des échanges au sein d'un réseau informatique.

II.3 Fondements de la sécurité des réseaux

La sécurité des réseaux informatiques constitue un pilier essentiel pour la protection des infrastructures et des données contre les menaces et les attaques malveillantes, garantissant ainsi la confidentialité, l'intégrité et la disponibilité des informations, des systèmes et des opérations critiques.

II.3.1 Principes fondamentaux de la sécurité des réseaux

Parmi ces principes on cite :

- **La confidentialité :** est la protection contre les accès non autorisés, tout en permettant aux utilisateurs autorisés d'accéder aux ressources sans obstruction. La confidentialité garantit que les données ne sont pas divulguées.
- **L'intégrité :** est la protection contre les modifications non autorisées, tout en permettant les modifications autorisées effectuées par des utilisateurs autorisés. L'intégrité garantit que les données restent cohérentes, tant en interne qu'en externe. Elle protège également contre les accidents et les modifications pirates par du code malveillant ou des logiciels écrits dans une intention malveillante. [1]
- **La disponibilité :** est la protection contre les temps d'arrêt, la perte de données et les accès bloqués, tout en fournissant une disponibilité constante, en protégeant les données et en prenant en charge l'accès autorisé aux ressources.
  La disponibilité garantit que les utilisateurs peuvent effectuer leur travail dans les délais et avoir accès aux ressources appropriées. [1]

II.3.2 Menaces et attaques informatiques

Une menace informatique se réfère à tout événement, acteur ou processus potentiellement nuisible ou malveillant qui vise à compromettre la sécurité, l'intégrité ou la disponibilité des systèmes informatiques, des réseaux ou des données. Tandis qu'une attaque informatique est une action malveillante exploitant les vulnérabilités d'un système, dans le but de compromettre leur sécurité, intégrité ou disponibilité, voici quelques exemples courants d'attaques informatiques :

a) Interception : L'attaque informatique par interception, également connue sous le nom d'attaque par homme du milieu (MitM), elle implique la capture de données en transit sur un réseau, cela peut se faire en exploitant des réseaux non sécurisés, en utilisant des outils de sniffing de paquets ou même des dispositifs d'écoute électronique. [2]

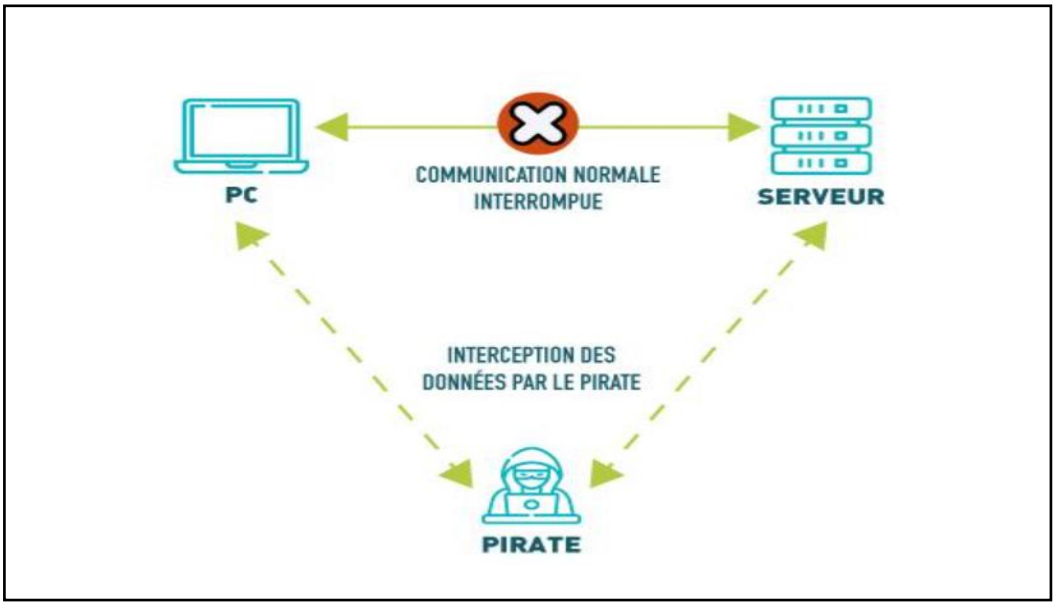

Figure 2.1: L'interception. [3]

b) Altération : une attaque informatique par altération implique la modification non autorisée de données, de fichiers ou de systèmes informatiques dans le but de servir des intérêts personnels, et cela en utilisant diverses techniques pour modifier les données, telles que l'injection de code malveillant, falsification et suppression de données, Altération de la configuration.

Tableau 2.1: La différence entre l'interception et l'altération.

Caractéristique	Attaque d'interception	Attaque d'altération
Cible	Communication entre deux parties.	Données stockées ou transmises.
Objectif	Vol, modification	Corruption ou falsification de données
Méthodes	Interception du trafic réseau, sniffing.	Logiciels malveillants, injection de code.
Conséquences	Perte de confidentialité, vol d'informations.	Dysfonctionnements,pertes financières.

c) **Attaque par déni de service (Dos) :** est un type de cyberattaque dans lequel un acteur malveillant vise à rendre un ordinateur ou un autre appareil indisponible pour ces utilisateurs prévus en interrompant le fonctionnement normal de l'appareil. Les attaques DoS fonctionnent généralement en submergent ou en saturant une machine ciblée de requête jusqu'à ce que le trafic normal ne puisse plus être traité ce qui entraîne un déni de service pour les utilisateurs légitimes. [3]

II.3.3 Modèle CIA

Les trois lettres de la « triade CIA » signifient Confidentialité, Intégrité et Disponibilité. La méthode CIA correspond à un modèle commun qui constitue la base du développement des systèmes de sécurité. Elle est utilisée pour identifier les vulnérabilités et les méthodes de création de solutions.

La triade CIA fournit une liste de contrôle de haut niveau simple et complète pour l'évaluation de vos procédures et outils de sécurité. [4]

II.4 Concepts de base en sécurité des réseaux

II.4.1 L'authentification et contrôle d'accès

a) **Authentification** : est le processus qui consiste à déterminer si quelqu'un ou quelque chose est, en fait, qui ou ce qu'il prétend être.

La technologie d'authentification permet de contrôler l'accès aux systèmes en vérifiant si les informations d'identification d'un utilisateur correspondent aux informations d'identification contenues dans une base de données d'utilisateurs autorisés ou dans un serveur d'authentification des données. Ce faisant, l'authentification garantit la sécurité des systèmes, des processus et des informations de l'entreprise, l'authentification à deux facteurs, l'authentification biométrique et l'utilisation de nom d'utilisateur et MDP sont les mécanismes d'identification les plus couramment utilisés. [5]

b) **Contrôle d'accès** : Le contrôle d'accès est le processus de détermination des autorisations dont dispose un utilisateur ou un appareil authentifié, il se basent sur des politiques qui définissent les ressources auxquelles chaque individu est autorisé à accéder et les actions qu'il est autorisé à effectuer.

II.4.2 La cryptographie

La cryptographie est une technique d'écriture où un message chiffré est écrit à l'aide de codes secrets ou de clés de chiffrement. La cryptographie est principalement utilisée pour protéger un message considéré comme confidentiel.

Il existe de nombreux algorithmes cryptographiques qui peuvent être utilisés pour chiffrer (et déchiffrer pour le destinataire) le message. Certains sont considérés comme basiques et d'autres offrent un niveau de sécurité presque absolu. [6]

- **Le chiffrement symétrique** : est une méthode de cryptage où la même clé est utilisée à la fois pour le chiffrement et le déchiffrement des données. On peut citer AES, Triple DES et RC4.

- **Le chiffrement asymétrique :** est une méthode de chiffrement qui utilise deux clés différentes pour chiffrer et déchiffrer des données où la clé publique est connue par tout le monde et sert à chiffrée les données, tandis que la clé privée doit être gardée secrète par le propriétaire et sert à déchiffrer les données. On peut citer l'algorithme de chiffrement RSA et DSA. [6]

II.4.3 Pare-feu :

Un pare-feu est un appareil ou un logiciel de protection du réseau qui contrôle et surveille le trafic entrant et sortant, et décide d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.

Les pare-feu constituent la première ligne de défense des réseaux. Ils établissent une barrière entre les réseaux internes sécurisés et contrôlés, qui sont dignes de confiance, et les réseaux externes tels qu'Internet. [7]

- **Type de pare-feu :**

Il existe plusieurs types de pare-feu, chacun conçu pour répondre à des besoins spécifiques en matière de sécurité réseau. Voici quelques types de pare-feu couramment utilisés :

- **Un pare-feu personnel** est conçu pour protéger un système unique ou un petit réseau, tel qu'un réseau SOHO. La plupart des pare-feu personnels offrent des interfaces conviviales qui peuvent être de nature Web ou graphique (c'est-à-dire une interface utilisateur graphique ou GUI). [8]
- **Un pare-feu commercial** est conçu pour assurer la protection d'un réseau d'entreprise de moyenne à grande taille. La plupart de ces pare-feu sont assez complexes et nécessitent souvent une formation et une certification spéciale pour tirer pleinement parti des fonctionnalités avancées.
- **Un pare-feu logiciel** est une application installée sur un hôte, il dépend du matériel et du système d'exploitation de l'hôte. Il ne peut protéger qu'un seul hôte contre les activités réseau malveillantes. Cette barrière de sécurité est uniquement capable de filtrer le trafic qui atteint l'interface réseau de son hôte. [8]

II.5 Mécanismes de sécurité des réseaux

II.5.1 VPN

Un réseau privé virtuel (VPN) est un mécanisme permettant d'établir une connexion d'accès à distance sécurisée sur un réseau intermédiaire, souvent Internet. Les VPN permettent un accès à distance, un contrôle à distance et des communications hautement sécurisées au sein d'un réseau privé. Les VPN utilisent le cryptage et l'authentification pour assurer la confidentialité, l'intégrité et la protection de la vie privée des communications réseau. [9]

- **Déploiement d'un VPN :**

Voici quelques figures illustrant le déploiement d'un VPN :

- **La Figure 2.2** décrit une configuration où un réseau local et un client distant ont chacun une connexion à Internet, ces connexions étant indépendantes. La connexion du réseau local est généralement permanente ou dédiée. Une fois que les deux points de terminaison sont connectés à Internet, le VPN peut être créé.
- **La Figure 2.3** illustre comment une nouvelle connexion réseau, à savoir le VPN, est établie entre le client distant et le réseau local via Internet. [9]

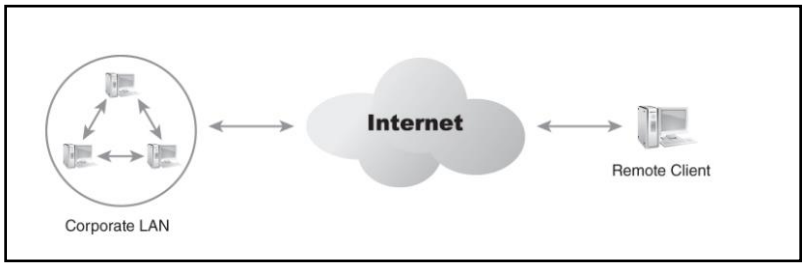

Figure 2.2: Avant avoir utilisé un VPN. [9]

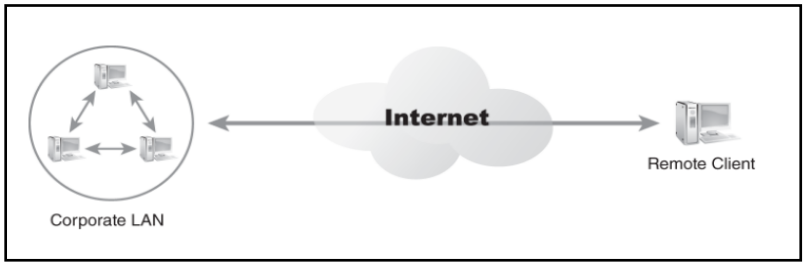

Figure 2.3: Après avoir utilisé un VPN. [9]

II.5.2 IDS (Intrusion Detection Systems) et IPS (Intrusion Prevention Systems)

Les IDS (Intrusion Detection Systems) : analysent et surveillent le trafic réseau pour détecter des signes indiquant que des hackers utilisent une cybermenace connue afin de s'infiltrer dans le réseau ou y voler des données. Les systèmes d'IDS comparent l'activité réseau en cours avec une base de données d'attaques connues afin de détecter divers types de comportements tels que les violations de la politique de sécurité, les malwares et les scanners de port.

Les IPS (Intrusion Prevention Systems) : agissent dans la même zone du réseau qu'un pare-feu, entre le monde extérieur et le réseau interne. Les IPS rejettent de façon proactive les paquets réseau en fonction d'un profil de sécurité si ces paquets représentent une menace connue. [10]

II.5.3 Sécurité sans fil

Désigne l'ensemble des mesures et techniques mises en œuvre pour protéger les réseaux et les appareils connectés sans fil contre les accès non autorisés, l'interception de données et autres menaces. [11]

- **Les protocoles de sécurité :**

  a) **WPA** (Wi-Fi Protected Access) est un protocole de sécurité sans fil lancé en 2003 pour résoudre les vulnérabilités de plus en plus importantes de son prédécesseur le WEP. Le protocole Wi-Fi WPA est plus sûr que le WEP, car il utilise une clé de chiffrement 256 bits, ce qui représente une nette amélioration par rapport aux clés 64 bits et 128 bits utilisées par le système WEP.

  b) **WPA2** (Wi-Fi Protected Access 2) est la deuxième génération de protocole de sécurité sans fil du WPA. Elle s'assure que les données envoyées et reçues sur le réseau sans fil sont bien chiffrées et que seules les personnes disposant du mot de passe réseau y ont accès. L'un des avantages du système WPA2 est qu'il a remplacé le système TKIP, assez vulnérable et utilisé dans le protocole WPA, par le système AES (Advanced Encryption System). [12]

  c) **WPA3** (Wi-Fi Protected Access 3) est le dernier des protocoles de sécurité de réseau sans fil, conçu pour chiffrer les données à l'aide d'un type de chiffrement fréquent et automatique appelé (Perfect Forward Secrecy) Il est plus sûr que son prédécesseur le WPA2. [12]

II.6 Protocoles de sécurité des réseaux

II.6.1 TLS/SSL

Un certificat SSL/TLS est un objet numérique qui permet aux systèmes de vérifier l'identité et d'établir ensuite une connexion réseau chiffrée avec un autre système.

Les certificats sont utilisés dans un système cryptographique appelé « infrastructure à clé publique » (PKI, Public Key Infrastructure). L'infrastructure PKI permet à une partie d'établir l'identité d'une autre partie à l'aide de certificats si elles font toutes deux confiances à un tiers appelé « autorité de certification ». Les certificats SSL/TLS font donc office de cartes d'identité numériques pour sécuriser les communications réseau. [13]

II.6.2 IPSEC

IPSec est un groupe de protocoles utilisés ensemble pour établir des connexions cryptées entre appareils. Il permet de sécuriser les données envoyées sur les réseaux publics. IPSec est souvent utilisé pour configurer des VPN et fonctionne en cryptant les paquets IP et en authentifiant la source d'où proviennent les paquets. [14]

II.6.3 TACAC+

TACACS+ signifie (Terminal Access Controller Access-Control System Plus), il s'agit d'un protocole qui a été développé comme une extension de l'ancien protocole TACACS, qui était principalement utilisé pour l'accès au terminal. TACACS+ utilise TCP comme protocole de couche transport et crypte l'intégralité du paquet. Il prend en charge les fonctions AAA et diverses méthodes d'authentification, telles que PAP, CHAP, EAP et Kerberos. [16]

II.7 Conclusion

La sécurité des réseaux informatiques est un défi permanent qui exige une vigilance et une adaptation constantes. Face à l'évolution permanente des menaces. Face à cette réalité, il est impératif pour les entreprises de rester vigilants, de mettre en place des mesures de protection robustes et de rester à jour avec les dernières avancées en matière de sécurité informatique. Dans ce chapitre, nous avons présenté quelques généralités sur la sécurité des réseaux informatiques.

Dans le prochain chapitre, nous explorerons en détail l'authentification, en examinant de près des concepts tels que RADIUS, AAA et 802.1X, afin de mieux comprendre leur importance et leur fonctionnement dans les systèmes informatiques modernes.

Chapitre III :
Les bases d'authentification Radius

III.1 Introduction

De nos jours, la sécurité joue un rôle considérable dans le monde numérique. Les réseaux sont devenus une priorité absolue. Les données sensibles et les ressources critiques doivent être protégées contre les accès non autorisés. L'authentification permet la gestion des accès et la protection des réseaux.

Dans ce chapitre nous explorons les concepts fondamentaux de l'authentification, en s'attardant sur les technologies Radius, AAA et 802.1X.

III.2 L'authentification

L'authentification est une procédure permettant de vérifier l'authenticité les identités des personnes ou d'un périphérique, en autorisant les personnes concernées à accéder à certaines ressources sécurisées.

Dans cette section, nous examinons en profondeur les fondements de l'authentification, ainsi que les différentes méthodes et protocoles utilisés pour renforcer la sécurité des systèmes informatiques.

III.2.1 Fondements d'authentification

III.2.1.1 Concepts fondamentaux de l'authentification

Ils reposent sur trois concepts clés qui garantissent la sécurité des systèmes informatiques : identification, vérification et l'authentification.

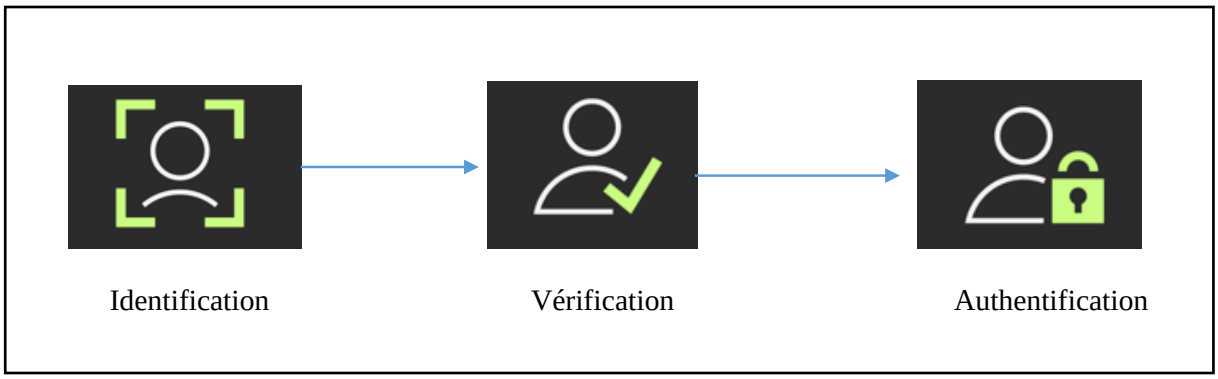

Figure 3.1: Concepts d'Authentification.

a) **L'identification :** Elle exige qu'un utilisateur ou un périphérique « s'identifie », généralement en indiquant une adresse e-mail, un numéro de téléphone ou un nom d'utilisateur. Il s'agit du processus par lequel une personne décline son identité par un identifiant unique.

b) **Vérification :** elle vérifie si l'identité est valide en s'appuyant sur des informations supplémentaires telles que : des mots de passe, des clés, des empreintes digitales.

Cette étape vise à valider que l'entité prétendant à l'identité est bien celle qu'elle prétend être.

c) **L'authentification :** Elle consiste à confirmer que l'utilisateur a réussi à prouver son identité en passant les étapes d'identification et de vérification. Une fois l'authentification réussie, l'utilisateur est autorisé à accéder aux ressources demandées.

III.2.1.2 Méthodes et technologies traditionnelles d'authentification

Il existe quatre facteurs d'authentification classiques qui peuvent être utilisés dans le processus d'authentification d'un utilisateur : [17]

- Une information que seul l'utilisateur connaît : mot de passe, numéro d'identification personnel.
- Une information unique que seul l'utilisateur possède : certificat d'immatriculation, carte d'identité, carte à puce, certificat électronique.
- Une information qui caractérise l'utilisateur dans un contexte donné : photo, caractéristique physique.
- Une information que seul l'utilisateur peut produire : signature.

a) **Nom d'utilisateur/Mot de passe :** Il s'agit d'une des méthodes les plus utilisées, avec laquelle les utilisateurs sont les plus familiers, voici commet l'Authentification par couple login/mot de passe se déroule :

- **Formulaire de connexion :** L'utilisateur saisit son login ainsi que son mot de passe dans un formulaire.
- **Requête HTTP :** Ces informations sont transmises au serveur via la requête HTTP.
- **Vérification du login :** Le serveur recherche d'abord si un utilisateur avec ce nom d'utilisateur/email existe en BDD.

- **Vérification du mot de passe :** Si c'est le cas, il compare ensuite le mot de passe saisi une fois haché avec le mot de passe stocké en base de données.
- **Autorisation :** Le serveur vérifie que l'utilisateur soit bien autorisé à accéder à la ressource. [17]

b) 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.

Afin de pouvoir accéder à un site ou une application nécessitant une authentification par certificat, vous devez vous enregistrer auprès d'une Autorité de Certification, L'Autorité de Certification vous émet un document électronique (le certificat d'authentification) qui contient vos informations vérifiées, ce certificat vous permet ensuite de vous identifier auprès d'un service. Lorsque vous essayez de vous connecter**,** le serveur vous demande de vous authentifier avec votre certificat**.** Si cette authentification est validée, il peut alors comparer les informations contenues dans votre certificat à celles contenues dans la liste des utilisateurs préalablement enregistrés**.** Il autorise la connexion dès qu'une correspondance est établie**.** [18]

c) Biométrie : L'authentification biométrique utilise les caractéristiques physiques ou les comportements uniques d'une personne pour vérifier son identité. Il s'agit notamment des empreintes digitales, de la reconnaissance faciale, de la voix, de l'iris et même des veines. [19]

Tableau 3.1: les avantages et Inconvénients des méthodes d'authentifications.

Méthodes	Avantages	Inconvénients
Mot de passe	• Facile à mettre en place. • Familiarité pour les utilisateurs. • Coût relativement bas.	• Vulnérabilité aux attaques par force brute. • Risque d'oubli ou de partage de mots de passe.
Certificat	• Authentification forte. • Sécurisé, car basé sur des clés cryptographiques.	• Mise à jour des certificats • Complexité pour les administrateurs et les utilisateurs finaux.
Biométrie	• Très sécurisé, car basé sur des caractéristiques uniques de l'utilisateur.	• Coût élevé pour la mise en place d'infrastructures biométriques.

III.2.1.3 Modèles d'authentification et de gestion des identités

Les modèles d'authentification déterminent les méthodes et les processus utilisés pour vérifier l'identité d'un utilisateur tentant d'accéder à un système ou des ressources.

La gestion des identités se concentre sur la création, la maintenance et la suppression des comptes utilisateurs, ainsi que sur la définition des droits et des permissions de chaque utilisateur.

a) Modèles d'authentification :

- **Authentification simple :** L'authentification simple repose sur un seul facteur d'authentification, tel qu'un mot de passe ou un code PIN. Bien que ce modèle soit le plus simple à mettre en place et à utiliser, il présente des vulnérabilités aux attaques telles que le phishing ou le vol de mot de passe.

- **Authentification forte :** L'authentification forte (Multi facteurs) : est une procédure permettant d'identifier un utilisateur. Elle nécessite la concaténation d'au moins deux facteurs d'authentification**.** Les facteurs d'authentification peuvent être classés en trois catégories :

  Ce que l'utilisateur sait **:** Mot de passe, code PIN.

  Ce que l'utilisateur possède **:** Clé USB, carte à puce, téléphone portable.

  Ce que l'utilisateur est **:** Empreinte digitale, reconnaissance faciale. [20]

- **Authentification unique :** L'authentification unique **SSO** (Single Sign-On) est un modèle qui permet aux utilisateurs de se connecter une seule fois pour accéder à plusieurs applications ou services, sans avoir besoin de saisir à nouveau leurs identifiants à chaque fois.

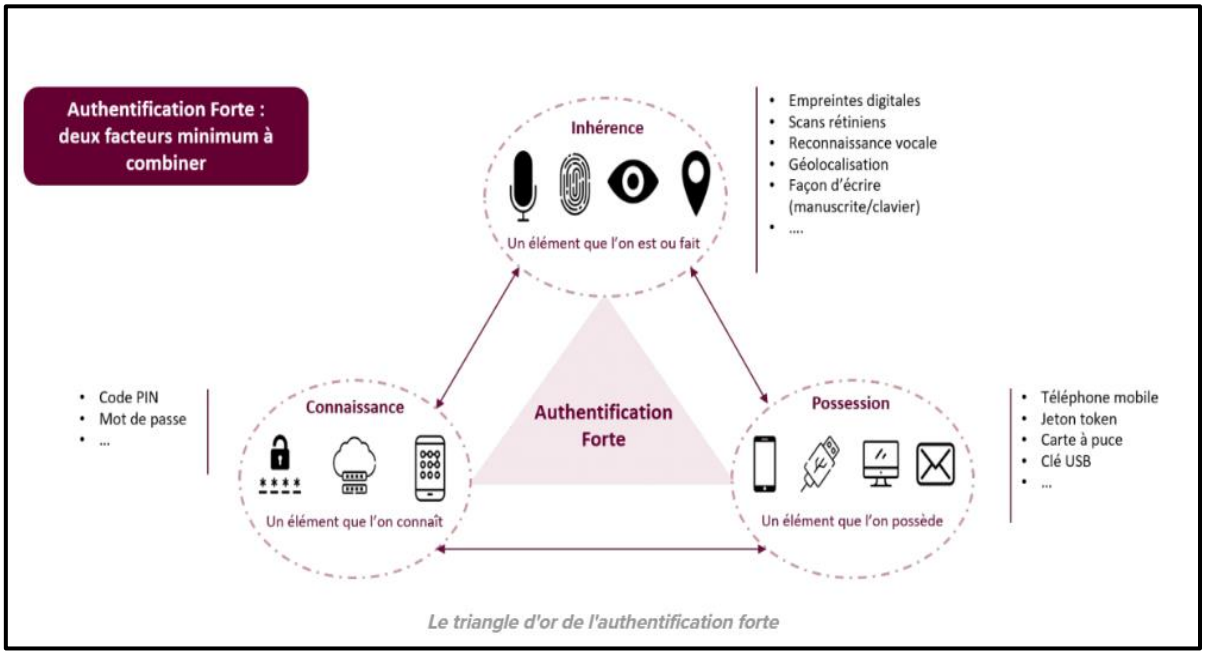

Figure 3.2: Authentification Forte. [21]

b) Les modèles de gestion des identités :

- **Gestion centralisée des identités :** elle s'appuie sur la collecte et le stockage des données d'identité des utilisateurs. Avec la gestion centralisée des identités, les utilisateurs peuvent accéder à toutes leurs applications, à leurs sites web et autres systèmes avec les mêmes identifiants. [22]

Ceci améliore l'expérience utilisateur car il suffit de saisir un nom d'utilisateur et un mot de passe, mais cela peut conduire à une vulnérabilité accrue si les identifiants sont compromis.

- **Gestion décentralisée des identités :** ce modèle distribue les informations d'identification et d'authentification sur plusieurs serveurs ou entités.

III.2.1.4 Evolution Des Technologies D'authentification

Face à l'augmentation des cybermenaces et la sophistication des attaques, les technologies d'authentification traditionnelles se révèlent de plus en plus insuffisantes. Les mots de passe et les codes PIN ne suffisent plus à protéger les données sensibles. C'est dans ce contexte que de nouvelles technologies d'authentification plus robustes, émergent et promettent de révolutionner la manière dont nous nous identifions et sécurisons nos accès.

L'avenir de l'authentification sera probablement marqué par une convergence de ces technologies. La biométrie, l'intelligence artificielle (IA) et la blockchain, entre autres, joueront un rôle crucial dans la création de systèmes d'authentification plus sûrs et plus pratiques.

III.3 Les protocoles d'authentification AAA, Radius et 802.1X

Dans cette section, nous explorerons en détail trois protocoles d'authentification majeurs qui constituent les fondements de notre approche pratique. Ces protocoles jouent un rôle essentiel dans la sécurisation des accès et des données au sein des réseaux informatiques.

III.3.1 Le protocole AAA

III.3.1.1 La définition de protocole AAA

L'authentification, l'autorisation et la traçabilité « AAA » est un ensemble de concepts primaires de sécurité informatique courants qui aide à contrôler l'accès aux réseaux. Ce modèle est utilisé quotidiennement pour protéger les données et les systèmes. C'est un moyen qui permet de contrôler les utilisateurs autorisés à accéder au réseau « authentification », ce qu'ils peuvent faire pendant qu'ils y sont « autorisation » et de vérifier les actions qu'ils ont effectués lors de l'accès au réseau « traçabilité ».

AAA est abordé dans plusieurs RFC. Le RFC 2903 traite de l'architecture générale d'AAA, il s'agit d'un RFC "expérimental", depuis lors, AAA a été plus clairement défini dans d'autres RFC. [25]

Les autres RFC pertinents incluent :

- RFC 2924 : Attributs de comptabilité et formats d'enregistrement
- RFC 2975 : Introduction à la gestion de la comptabilité.
- RFC 2989 : Critères d'évaluation des protocoles AAA pour l'accès au réseau
- RFC 3127 : Authentification, autorisation et comptabilité : Évaluation du protocole. [25]

III.3.1.2 Architecture AAA

AAA est une architecture Client-Serveur qui utilise de multiples technologies de réseaux et de plateformes pour que l'ensemble de ces fonctionnalités soient mise en services.

Les serveurs AAA permettent de gérer les utilisateurs et les clients AAA en se basant sur des outils, politiques et données nécessaires à l'authentification et sur l'autorisation des utilisateurs et à la comptabilisation des ressources utilisées.

Les clients AAA sont installés sur des routeurs ou des serveurs d'accès au réseau (NAS-Network Access Server). [27]

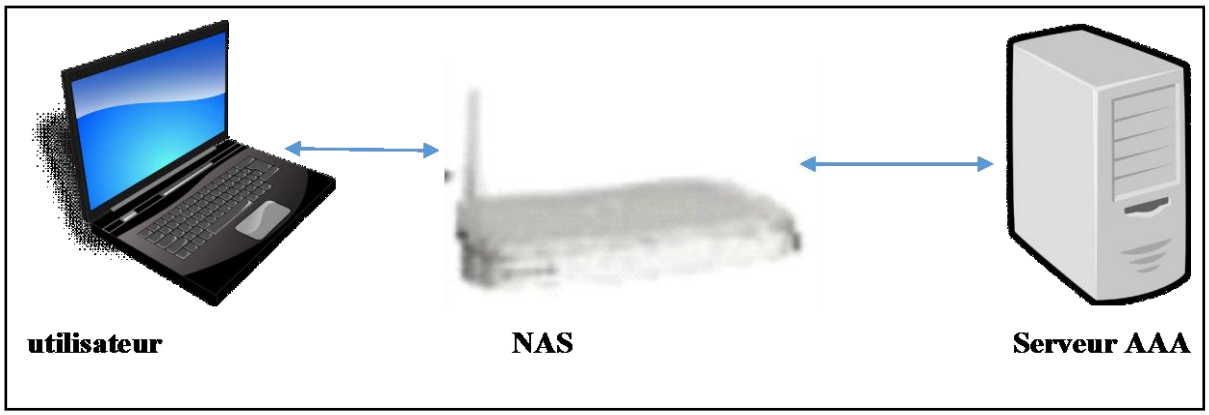

Figure 3.3: Architecture AAA.

III.3.1.3 Importance du protocole AAA dans les réseaux informatiques

AAA est un élément crucial de la sécurité réseau, car il limite les personnes ayant accès à un système et assure le suivi de leur activité. De cette manière, les acteurs malveillants peuvent être tenus à l'écart, et un acteur vraisemblablement bon qui abuse de ses privilèges peut faire l'objet d'un suivi de son activité, ce qui donne aux administrateurs des informations précieuses sur leurs activités**.**

III.3.1.4 Autorisation

Après l'authentification, le processus d'autorisation applique les politiques réseau, le contrôle d'accès granulaire et les privilèges utilisateur. Ce protocole détermine les ressources réseau spécifiques auxquelles l'utilisateur est autorisé à accéder, comme une application particulière, une base de données ou un service en ligne.[25]

III.3.1.5 Accounting

La comptabilité suit l'activité des utilisateurs pendant leur connexion à un réseau en suivant des informations telles que la durée de leur connexion, les données qu'ils ont envoyées ou reçues leur adresse IP (Internet Protocol), l'identifiant uniforme des ressources (URI) qu'ils ont utilisé et les différents services auxquels ils ont accédé.

AAA prend en charge six types de comptabilité :

- **Comptabilité réseau** : suit l'utilisation globale du réseau, comme le trafic entrant et sortant.
- **Comptabilité de connexion** : suit la création, la fermeture et la durée des sessions utilisateur.
- **Comptabilité EXEC** : suit l'activité de la ligne de commande de l'appareil.
- **Comptabilité système** : suit les événements liés au système lui-même, tels que les redémarrages et les changements de configuration.
- **Comptabilité des commandes** : suit l'exécution de commandes spécifiques sur l'appareil.
- **Comptabilité des ressources** : suit l'utilisation des ressources spécifiques, telles que la mémoire et le processeur**.** [25]

III.3.2 Protocole RADIUS

Dans le domaine de l'authentification, un client d'authentification, d'autorisation et de comptabilité (AAA) peut utiliser plusieurs protocoles pour communiquer avec un serveur AAA. Il s'agit des protocoles tels que TACACS, XTACACS, TACACS+ et RADIUS. Cette partie se concentre sur le protocole Remote Authentication Dial-In User Service (RADIUS). [24]

III.3.2.1 Présentation du protocole RADIUS

Le protocole RADIUS est un standard de l'IETF conçu pour fournir un système centralisé de gestion des accès réseau.

En utilisant le protocole AAA, RADIUS offre une solution complète pour l'identification des utilisateurs, l'autorisation de leurs activités réseau et le suivi de leurs actions. Fonctionnant sur un modèle client/serveur.

Il effectue à la fois l'authentification et l'autorisation simultanément, tandis que la comptabilité est gérée séparément. En utilisant le protocole UDP sur le port 1812 pour l'authentification, et le port 1813 pour la comptabilité, RADIUS garantit un échange efficace de données entre les clients et les serveurs. [27]

III.3.2.2 Origines et évolution du protocole radius

RADIUS a été créé pour répondre aux besoins d'une méthode centralisée d'authentification, d'autorisation et de comptabilité pour les utilisateurs accédant à des ressources informatiques.

- **Problème :** Merit Networks(Une organisation), un pionnier d'Internet, avait du mal à gérer les utilisateurs se connectant à son réseau commuté à l'aide de méthodes d'authentification spécifiques à chaque appareil.
- **Solution :** Merit a collaboré avec Livingston Entreprises pour développer RADIUS, un protocole permettant une authentification, une autorisation et une comptabilité centralisées.
- **Succès :** RADIUS est devenu un standard de l'industrie, adopté par les fournisseurs de serveurs et d'équipements réseau. Il est toujours largement utilisé aujourd'hui pour sécuriser les réseaux et les accès aux ressources. [26][31]

III.3.2.3 Principes de protocole RADIUS

a) **Architecture Radius :** L'architecture RADIUS repose sur un modèle client/serveur, avec deux acteurs principaux :

- **Client RADIUS (NAS) :** Il s'agit généralement d'un périphérique réseau tel qu'un routeur, un commutateur, un point d'accès sans fil ou un serveur VPN.
  Le NAS initie le processus d'authentification et d'autorisation en envoyant des requêtes RADIUS au serveur RADIUS.

- **Serveur RADIUS** : Il s'agit d'un serveur centralisé qui héberge le service RADIUS et interagit avec des bases de données externes (Active Directory, LDAP, etc.) pour vérifier les informations d'identification et les droits d'accès des utilisateurs. Le serveur RADIUS traite les requêtes RADIUS envoyées par les NAS, consulte les bases de données des utilisateurs et renvoie des réponses indiquant si l'accès doit être autorisé ou refusé.

b) Fonctionnement du protocole Radius : Le fonctionnement de RADIUS se déroule en plusieurs étapes : [27]

1. **Demande d'accès par l'utilisateur :**
   - Un utilisateur tente de se connecter à un périphérique réseau, comme un routeur ou un point d'accès sans fil.
   - L'utilisateur saisit ses identifiants (nom d'utilisateur et mot de passe).

2. **Transmission de la requête au serveur RADIUS :**
   - Le périphérique réseau (NAS), intercepte la demande d'accès de l'utilisateur.
   - Le NAS encapsule les informations d'identification de l'utilisateur dans un message RADIUS.
   - Le NAS envoie le message RADIUS à un serveur RADIUS.

3. **Authentification par le serveur RADIUS :**
   - Le serveur RADIUS extrait les informations d'identification de l'utilisateur du message RADIUS.
   - Le serveur RADIUS consulte une base de données d'utilisateurs stockée localement ou sur un serveur externe (Active Directory, LDAP, etc.) pour vérifier les informations d'identification de l'utilisateur.

4. **Réponse du serveur RADIUS :** En fonction du résultat de l'authentification, le serveur RADIUS envoie une réponse RADIUS au NAS.
   - **ACCEPT:** Si l'authentification est réussie, le serveur RADIUS envoie une réponse ACCEPT au NAS. Cela indique que l'utilisateur est autorisé à accéder au réseau.

- **REJECT:** Si l'authentification échoue, le serveur RADIUS envoie une réponse REJECT au NAS. Cela indique que l'utilisateur n'est pas autorisé à accéder au réseau.
- **CHALLENGE** Si le serveur RADIUS a besoin d'informations supplémentaires de l'utilisateur pour compléter l'authentification, il envoie une réponse CHALLENGE au NAS. La réponse CHALLENGE contient un "défi" spécifique.

5. **Traitement de la réponse par le NAS:**
   - Le NAS reçoit la réponse RADIUS du serveur RADIUS.
   - Si la réponse est ACCEPT, le NAS accorde l'accès à l'utilisateur au réseau.
   - Si la réponse est REJECT, le NAS informe l'utilisateur de l'échec de sa connexion et de la raison du rejet (mot de passe incorrect, compte désactivé, etc.).
   - Si la réponse est CHALLENGE, le NAS présente le défi à l'utilisateur et recueille sa réponse. [27]

c) Format d'un paquet RADIUS : Radius utilise quatre types de paquets pour assurer les transactions d'authentification. Tous les paquets ont le format général indiqué par la figure suivante :

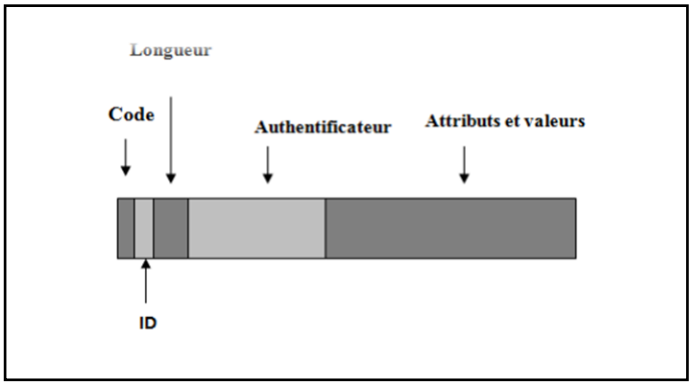

Figure 3.4: Format des paquets RADIUS. [27]

Tableau 3.2: Description du champ code.

Code	Type de message	Description
1	Access-Request	Ce message est généré par le NAS (client RADIUS) vers le serveur pour transmettre la demande depuis ou au nom d'un utilisateur
2	Access-Accept	Ce message est envoyé du serveur RADIUS au NAS pour indiquer la réussite de la demande.
3	Access-Reject	Ce message est envoyé par le serveur pour indiquer le rejet d'une demande.
4	Accounting-Request	Ce message est envoyé du client au serveur de comptabilité pour transmettre des informations comptables concernant le service fourni à l'utilisateur.
5	Accounting-Response	Ce message est envoyé par le serveur au client pour accuser réception de la réception des informations comptables envoyées par le client et indique le résultat de la fonction comptable effectuée par le serveur.
11	Access-Challenge	Ce message est envoyé du serveur RADIUS au client RADIUS (NAS) pour solliciter des informations supplémentaires pour l'autorisation du client.

- **Identifiant :** Ce champ, d'un seul octet, contient une valeur permettant au client Radius d'associer les requêtes et les réponses.
- **Longueur (taille) :** Champ de seize octets contenant la longueur totale du paquet.
- **Authentificateur :** Champ de seize octets a pour but de vérifier l'intégrité des paquets.
- **Attributs et valeurs :** ce champ est utilisé pour véhiculer toutes les informations nécessaires, il a pour format :

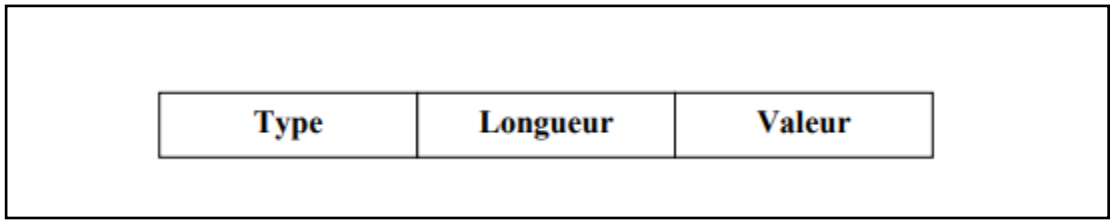

Figure 3.5: Format des attributs Radius. [27]

III.3.3 La norme 802.1X

III.3.3.1 Définition et origines de la norme 802.1X

Le protocole 802.1x est une solution standard de sécurisation de réseaux mise au point par l'IEEE, 802.1x permet d'authentifier un utilisateur souhaitant accéder à un réseau (câblé ou Wifi) grâce à un serveur central d'authentification.

Il ut nilise un protocole appelé EAP (Extensible Authentication Protocol) pour effectuer l'authentification. EAP est un protocole extensible qui peut prendre en charge une variété de mécanismes d'authentification, tels que PEAP (Protected Extensible Authentication Protocol), LEAP (Lightweight Extensible Authentication Protocol) et TTLS (Tunneled TLS).

III.3.3.2 Composants de la norme 802.1X

Voici la structure et les composants pour l'application de la norme :

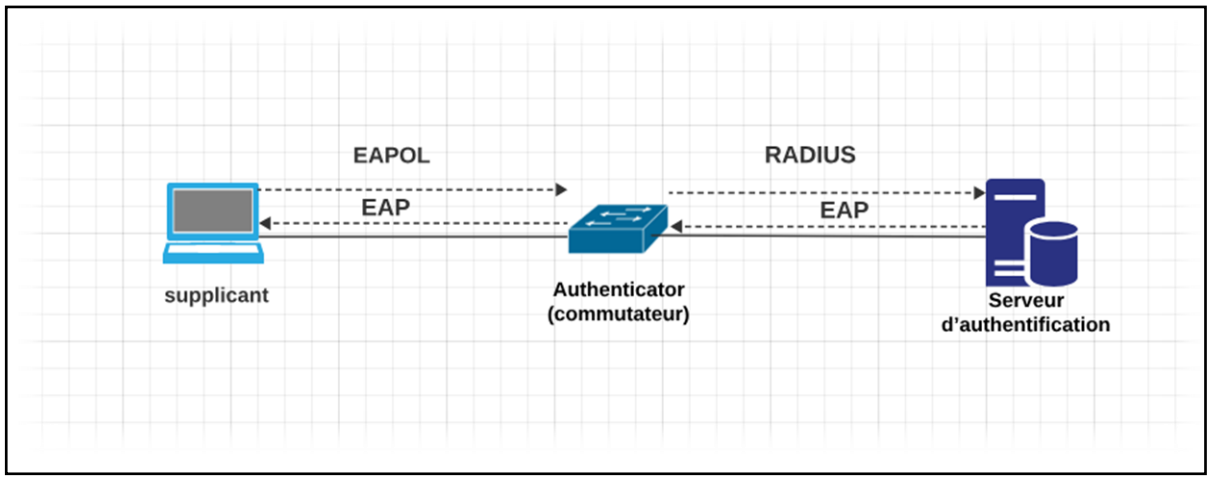

Figure 3.6: Composants 802.1x.

a) **Suppliant** (poste de travail) : est un client qui demande l'accès au réseau local et répond aux demandes du commutateur, tel qu'un ordinateur portable, un smartphone.
b) **Authenticator (**commutateur**) :** Il s'agit du périphérique réseau qui contrôle l'accès au réseau, tel qu'un commutateur Ethernet ou un point d'accès sans fil (PA).

c) **Serveur d'authentification :** Le serveur d'authentification valide l'identité du client et informe le commutateur si le client est autorisé à accéder au réseau local.

d) **EAPOL (**EAP over LAN Protocol**) :** Il s'agit d'un protocole qui transporte les messages EAP entre le supplicant et Authenticator, les paquets EAP sont encapsulés dans des trames EAPOL et sont délivrés au Authenticator**.**

e) **RADIUS :** Il agit comme un moyen de transport pour les messages EAP entre le client (le supplicant) et le serveur d'authentification, L'Authenticator encapsule les paquets EAP dans des paquets RADIUS et les envoie au serveur RADIUS pour traitement.

III.3.3.3 Fonctionnement de la norme 802.1X et les méthodes d'authentification

En 802.1X, dans la mesure où c'est le supplicant qui envoie les éléments d'authentification au server, 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, Tout se passe comme si chaque port était coupé en deux :

Port contrôlé : au départ, il est maintenu fermée par le commutateur.

Port non contrôlé : Par cette voie, le commutateur n'accepte que le protocole EAP. [25]

Comme l'indique la **figure 3.7**, au début de la connexion, le port est dans l'état non contrôlé. Seuls les paquets EAP permettant d'authentifier le client qui sont autorisés**.**

Et on peut le voir sur la **figure 3.8**, 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.

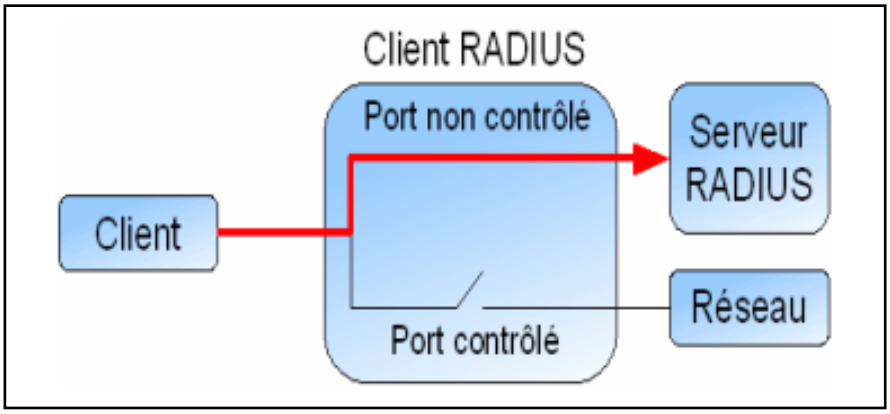

Figure 3.7: Accès avant authentification.

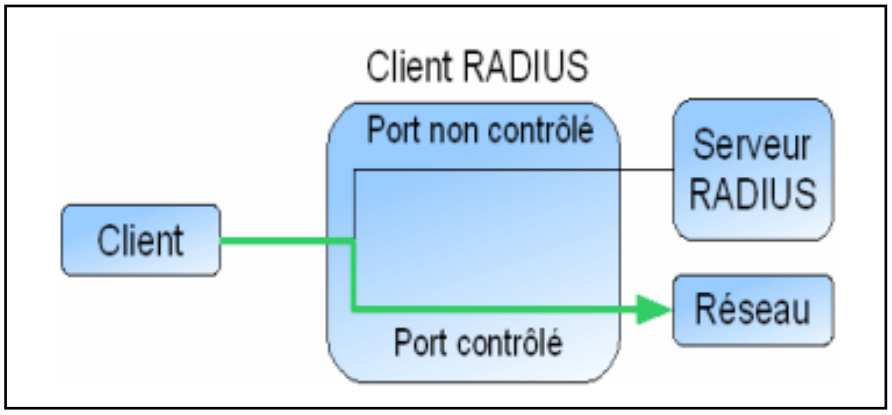

Figure 3.8: Accès après authentification.

III.3.3.4 Le protocole EAP

La communication entre l'équipement réseau (authenticator) et le serveur d'authentification est assurée par le protocole EAP (Extensible Authentication Protocol) ainsi que le transport des informations d'authentification et permet d'utiliser différentes Méthodes d'authentification

EAP spécifie que quatre types de messages peuvent être envoyés :

1. **Request (Demande) :** Envoyé par le serveur d'authentification pour demander des informations d'identification à l'entité d'authentification.
2. **Response (Réponse) :** Envoyé par le client en réponse à une demande, contenant les informations d'identification demandées.
3. **Success (Succès) :** pour indique que l'authentification a réussi.
4. **Failure (Échec) :** pour indique que l'authentification a échoué. [23]

- Les méthodes d'authentification associées à EAP :

EAP supporte une variété de méthodes d'authentification, telles que les identifiants de connexion (login/mot de passe), les certificats électroniques. Certaines méthodes combinent plusieurs critères pour renforcer la sécurité. Les méthodes d'authentification les plus fréquemment utilisées sont :

a. **EAP-TLS** : Le protocole EAP/TLS (Transport Layer Security) utilise le chiffrement pour sécuriser les échanges entre le client (supplicant) et le serveur lors du processus d'authentification. Avec EAP/TLS, l'authentification mutuelle se fait par certificat, où à la fois le client et le serveur s'authentifient en échangeant leurs certificats respectifs. [25]

b. **PEAP :** Le protocole PEAP (Protected Extensible Authentication Protocol) a été développé par Microsoft, Cisco et RSA Security pour résoudre le principal inconvénient d'EAP/TLS : la nécessité de distribuer des certificats à tous les utilisateurs ou machines, ce qui peut être une charge importante voire ingérable dans certains environnements. Dans le cas de PEAP, l'authentification est mutuelle entre le supplicant et le serveur, mais de manière asymétrique. Le serveur est authentifié par son certificat auprès du supplicant, tandis qu'il s'authentifie auprès du serveur en présentant un identifiant et un mot de passe. [25]

c. **TTLS :** TTLS (Tunneled Transport Layer Security) a été développé par Funk Software et Certicom dans le but de fournir un protocole d'authentification mutuelle entre le poste client et le serveur d'authentification, similaire à PEAP. Le client s'authentifie avec un identifiant et un mot de passe, tandis que le serveur s'authentifie avec un certificat.

   TTLS se distingue de PEAP à deux niveaux. Premièrement, les informations sont transportées au moyen de couples Attributs/Valeurs (AVP) compatibles avec ceux de Radius. Deuxièmement, la notion de serveur TTLS est introduite, agissant comme un intermédiaire entre l'équipement réseau et le serveur d'authentification. Ce serveur TTLS peut être distinct ou intégré au serveur d'authentification. [25]

III.3.3.5 Acheminement des protocoles utilisées :

Étape d'authentification : La norme 802.1X est utilisée dès le début du processus d'authentification. Elle définit le cadre pour le contrôle d'accès au réseau en exigeant que les périphériques se soumettent à une authentification avant d'être autorisés à communiquer sur le réseau. 802.1X utilise des protocoles EAP (Extensible Authentication Protocol) pour cette authentification.

Encapsulation sécurisée : PEAP est souvent utilisé après l'initiation via 802.1X pour encapsuler des protocoles EAP (comme EAP-TLS) dans une session TLS sécurisée. Cela garantit que les informations d'identification de l'utilisateur sont protégées pendant la transmission.

Le protocole AAA intervient principalement après que l'authentification initiale a été réalisée avec succès via PEAP et 802.1X.
ces derniers fournissent un mécanisme d'authentification sécurisé et une protection des données sensibles via un tunnel TLS.

Ensemble, ces protocoles permettent de sécuriser et de gérer efficacement l'accès au réseau, en garantissant une authentification forte, une autorisation appropriée et une traçabilité des activités réseau.

- **La relation entre le protocole 802.1X et AAA**

Le protocole 802.1x permet de gérer l'accès au réseau et cela en se basant sur l'état des ports. Au début le port est dans l'état non-contrôlé ce qui signifie que seuls les paquets EAP sont autorisés à passer, ces paquets transportent les informations d'identification du client.
Une fois ces informations arrivées au serveur Radius, il vérifie leurs authenticité et véracité en les comparant aux donnes contenues dans la base de données, et c'est là que commence le protocole AAA, plus précisément l'étape authentification, une fois cette étape validée le port passe à l'état contrôlé et permet ainsi l'accès au réseau et aux ressources.
Enfin, on passe aux deux autre étape (autorisation, accounting) du processus de gestion des accès et des ressources.

III.3.3.6 Fonctionnement de notre solution

Notre solution est basée sur l'authentification PEAP/TLS, offrant ainsi un niveau élevé de sécurité et d'authentification mutuelle entre les clients et les serveurs.

Avec PEAP/TLS l'authentification est asymétrique. Le serveur sera authentifié par son certificat auprès du supplicant qui, lui-même, s'authentifiera auprès du serveur par la présentation d'un identifiant et d'un mot de passe.

Comme l'indique la figure 3.9 l'authentification PEAP est décomposée en quatre étapes qui sont :

a) Étape « **Identité externe** ».

b) Étape « **Négociation de protocole** ».

c) Étape « **TLS handshake** ».

d) Étape « **TLS record** ».

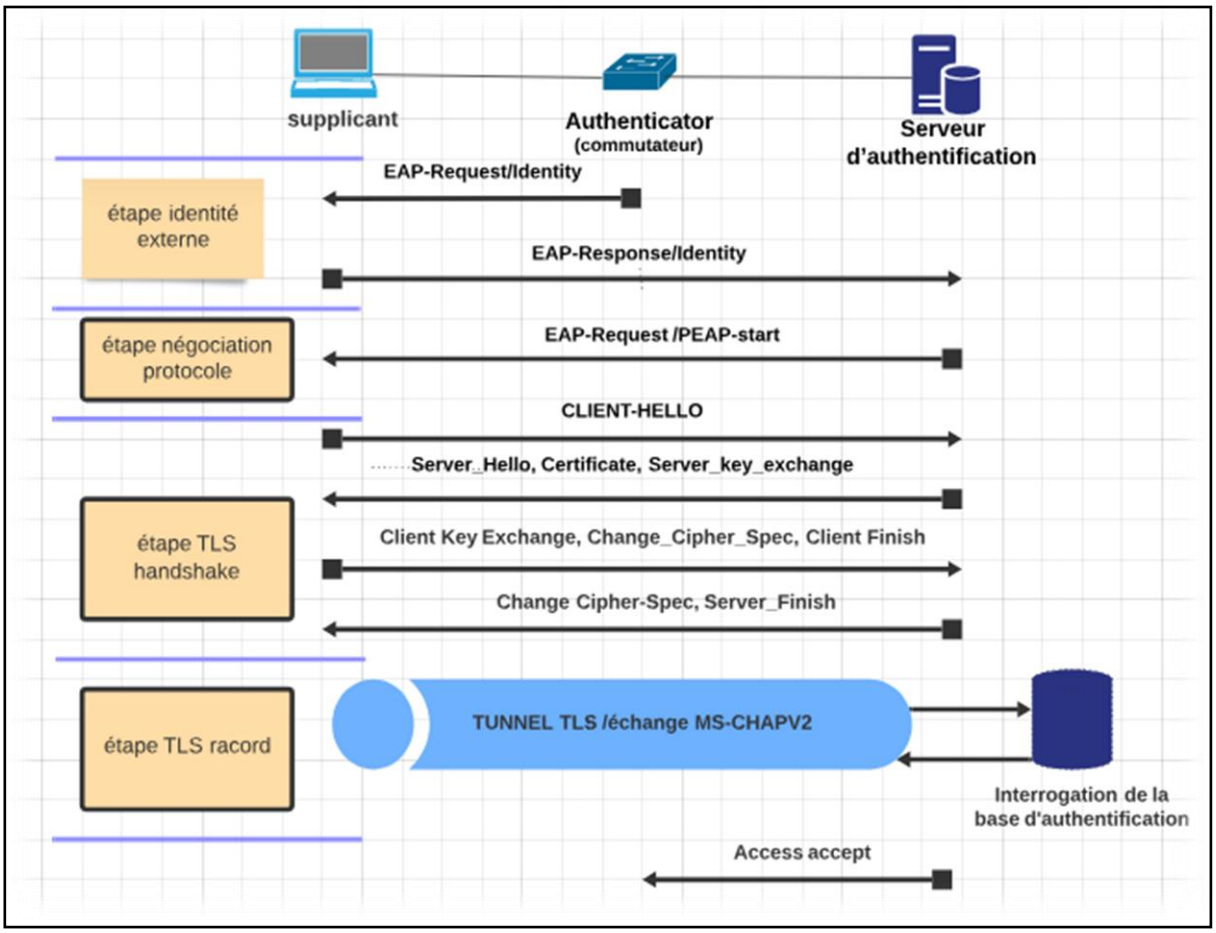

Figure 3.9: Authentification PEAP/TLS.

a) L'étape Identité externe :

- Le NAS envoie un paquet EAP de type **EAP-Request/Identity** pour demander au supplicant son identité.
- Le supplicant répond par un paquet de type **EAP-Response/Identity** contenant son identité.
- Le NAS fabrique un paquet RADIUS de type **Access-Request** dans lequel il écrit un en-tête puis un champ attributs et valeurs. À l'intérieur de celui-ci, il écrit l'attribut **EAP-Message** dans lequel il encapsule le paquet EAP venant du supplicant.
- Le NAS envoie le paquet **Access-Request** au serveur.

b) L'étape négociation de protocole :

- Le serveur reçoit le paquet Access-Request.
- Il construit un paquet RADIUS de type Access-Challenge dans lequel il écrit un attribut **EAP-Message** formé d'un paquet **EAP-Request** qui contient une proposition de protocole d'authentification **PEAP,** EAP-Type=PEAP (**PEAP-start**).
- Le NAS décapsule le paquet EAP contenu dans **EAP-Message** et le transfert vers le supplicant. Celui-ci répond par un paquet **EAP-Response**.

c) L'étape TLS handshake :

- Le supplicant envoie un message (**client_hello**) avec la liste des algorithmes de chiffrement qu'il est capable d'utiliser.
- Le serveur répond (**Serveur_Hello**) en transmettant l'algorithme qu'il a choisi parmi la liste qu'il a reçue. Il envoie son certificat et sa clé publique au supplicant.
- Le supplicant authentifie le certificat du serveur. Il génère la **Pré-Master Key**. Celle-ci est chiffrée avec la clé publique que vient de lui envoyer le serveur. À partir de cette clé, il calcule la clé principale **Master Key (MK).**
- **Le serveur** déchiffre **la Pré-Master Key** grâce à la clé privée de son propre certificat. Il est donc en mesure de calculer de son côté la même Master Key. Le serveur envoie au supplicant la notification de son changement de paramètre de chiffrement (Change_Cipher_Spec). Et un tunnel chiffré est établi entre eux.

d) L'étape TLS record :

Dans cette étape le serveur d'authentification utilise MS-CHAPv2 pour vérifier les informations d'identification fournies par le client.

MS-CHAPv2 est une méthode d'authentification par mot de passe qui permet au client de prouver son identité à un serveur d'authentification par l'utilisation un échange de défis et de réponses pour valider le mot de passe sans l'envoyer en clair sur le réseau.

- Le supplicant envoie son identifiant au serveur au moyen d'un nouveau paquet **EAP-identity**.
- Le serveur envoie une chaîne aléatoire, appelée challenge, au moyen d'un paquet **Access-Challenge**.
- Le supplicant génère une réponse calculée à partir d'une formule de hachage impliquant divers éléments, tels que le challenge, son identifiant et son mot de passe, puis envoie cette réponse au serveur via un paquet **Access-Request**.
- Le serveur effectue les mêmes calculs et compare le résultat à la réponse reçue. Si elles correspondent, le mot de passe est validé.
- Le supplicant envoie une requête **EAP-Response** vide pour signifier que les opérations sont terminées de son côté.
- Le serveur envoie un paquet **Access-Accept** au NAS pour lui commander d'ouvrir le port.

Conclusion

En conclusion, il est clair que l'avenir de l'authentification repose sur l'adoption de méthodes plus avancées qui offrent des niveaux de sécurité plus élevés. Cette évolution est cruciale pour répondre aux besoins croissants en matière de sécurité dans un monde numérique en constante évolution, où la protection des informations sensibles est une priorité absolue.

Au cours du prochain chapitre, nous entamerons la partie pratique de ce projet en implémentant les mécanismes de sécurité du modèle AAA et du protocole 802.1X étudiés théoriquement dans les chapitres précédents.

Chapitre IV :
Implémentation de la solution.

IV.1 Introduction

Dans ce chapitre, nous introduisons notre projet en détaillant ses architectures et son environnement de travail. Ensuite, nous mettons en œuvre notre solution d'authentification RADIUS par certificats, ainsi que les règles de pare-feu.

Enfin, nous présentons quelques tests pour mieux comprendre les politiques de sécurité mises en place et la solution proposée.

IV.2 Environnement de travail

IV.2.1 Les outils de travail

a) **GNS3** (Graphical Network Simulator) : est un logiciel open source qui permet aux utilisateurs de simuler, modéliser, configurer et tester des réseaux informatiques virtuels. En utilisant des images d'appareils réseau réels, les utilisateurs peuvent créer des topologies réseau complexes et expérimenter différentes configurations sans avoir besoin de matériel physique ou malmener les équipements. [28]

Figure 4.1: Logo de GNS3.

b) **VMware Workstation :** est un logiciel de virtualisation développé par VMware, il permet la création et la gestion efficace de machines virtuelles sur un seul ordinateur hôte.

Cette solution permet aux utilisateurs d'installer et d'exécuter simultanément plusieurs systèmes d'exploitation, tels que Windows, Linux, etc. Les ressources matérielles telles que la mémoire et le processeur peuvent être configurées pour chaque machine virtuelle, offrant ainsi une expérience similaire à celle d'une machine physique. Cela facilite le développement, les tests et l'isolement d'applications dans des environnements contrôlés avant leur déploiement sur des machines physiques. [29]

Figure 4.2: Logo de VMware Workstation.

c) **Wireshark** est un logiciel d'analyse de réseau open source qui permet aux utilisateurs de capturer et d'analyser le trafic réseau en temps réel. Il prend en charge une variété de protocoles et offre la possibilité de filtrer et rechercher des informations spécifiques dans le trafic capturé. Il est largement utilisé pour le dépannage et la sécurité réseau, le développement et la compréhension des protocoles de communication. [30]

Figure 4.3: Logo de Wireshark.

IV.3 Les équipements hard et soft

Pour implémenter ce système d'authentification, nous avons utilisés les équipements suivants :

- Des commutateurs de type **Cisco Catalyst 2960** prenant en charge le protocole 802.1X.IL joue le rôle du client RADIUS.
- Un pare-feu « **Fortigate** ».
- Des clients sous **Windows 10 :** Nous avons deux client Windows pour faire nos différents tests.
- **Windows Serveur 2022 :** est un système d'exploitation conçu pour répondre aux besoins spécifiques des serveurs informatiques, il prend en charge la gestion des ressources au sein de l'entreprise, le contrôle d'accès et les services du domaine Active Directory.

IV.4 Architecture proposée

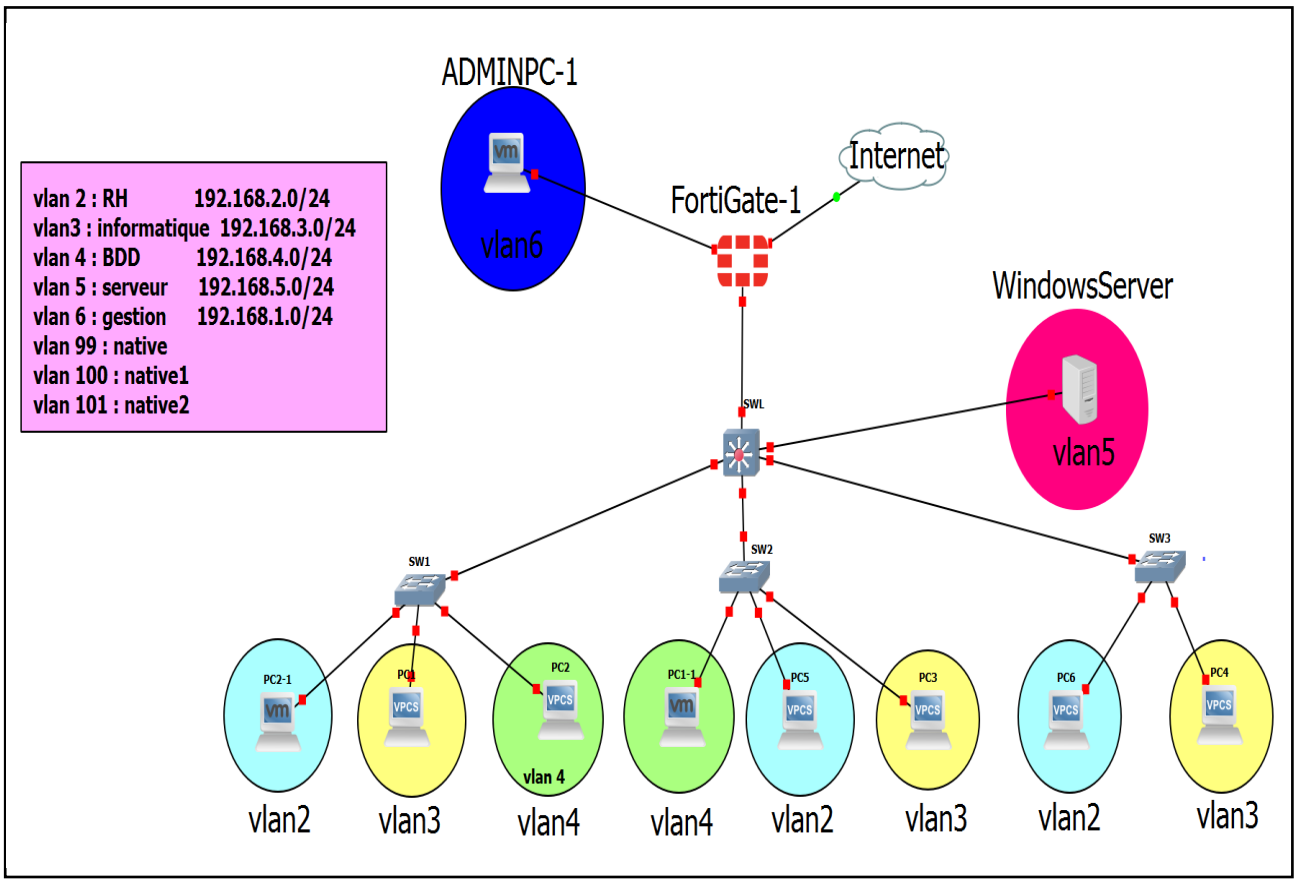

Figure 4.4 Architecture réseau proposée sur GNS3.

Nous avons intégré des switches Cisco prenant en charge la norme 802.1X pour le contrôle d'accès réseau. Pour renforcer la sécurité et gérer le routage inter-VLAN, nous avons déployé un pare-feu FortiGate dédié à la protection de l'accès à Internet. De plus, un serveur Windows centralise les services essentiels tels que DHCP, DNS, l'autorité de certification et le serveur RADIUS. Notre configuration inclut plusieurs PC clients nécessitant un accès sécurisé ainsi qu'un PC administrateur dédié à la gestion du réseau. Nous avons utilisé des VLANs pour segmenter le réseau en sous-réseaux logiques distincts, optimisant ainsi la gestion du trafic et la sécurité.

IV.5 Tableau d'adressage des VLANs

Le tableau suivant englobe les VLANs créés lors de notre configuration :

Tableau 4.1: les VLANs.

Nom du vlan	Id du vlan	Adresse IP	Masque	Passerelle
RH	2	192.168.2.0	255.255.255.0	192.168.2.254
Informatique	3	192.168.3.0	255.255.255.0	192.168.3.254
BDD	4	192.168.4.0	255.255.255.0	192.168.4.254
Server	5	192.168.5.0	255.255.255.0	192.168.5.254
Gestion	6	192.168.1.0	255.255.255.0	192.168.1.254

IV.6 Méthodologie de réalisation

Pour notre projet, nous avons suivi une méthodologie en sept étapes. Nous avons commencé par l'installation des machines virtuelles (Fortigate, Windows Server, Windows 10). Ensuite, nous avons effectué la configuration basique du réseau, y compris les trunks et le protocole VTP. Nous avons créé et configuré les VLANs et attribué les adresses et configuré le routage inter-VLANs. Puis, nous avons mis en place le pare-feu pour sécuriser le réseau et assuré l'accès à Internet. Après cela, nous avons configuré les services essentiels sur Windows Server, tels que DHCP, DNS, et Active Directory. Nous avons ensuite configuré le serveur RADIUS. Enfin, nous avons réalisé des tests pour vérifier la fiabilité et l'efficacité du système.

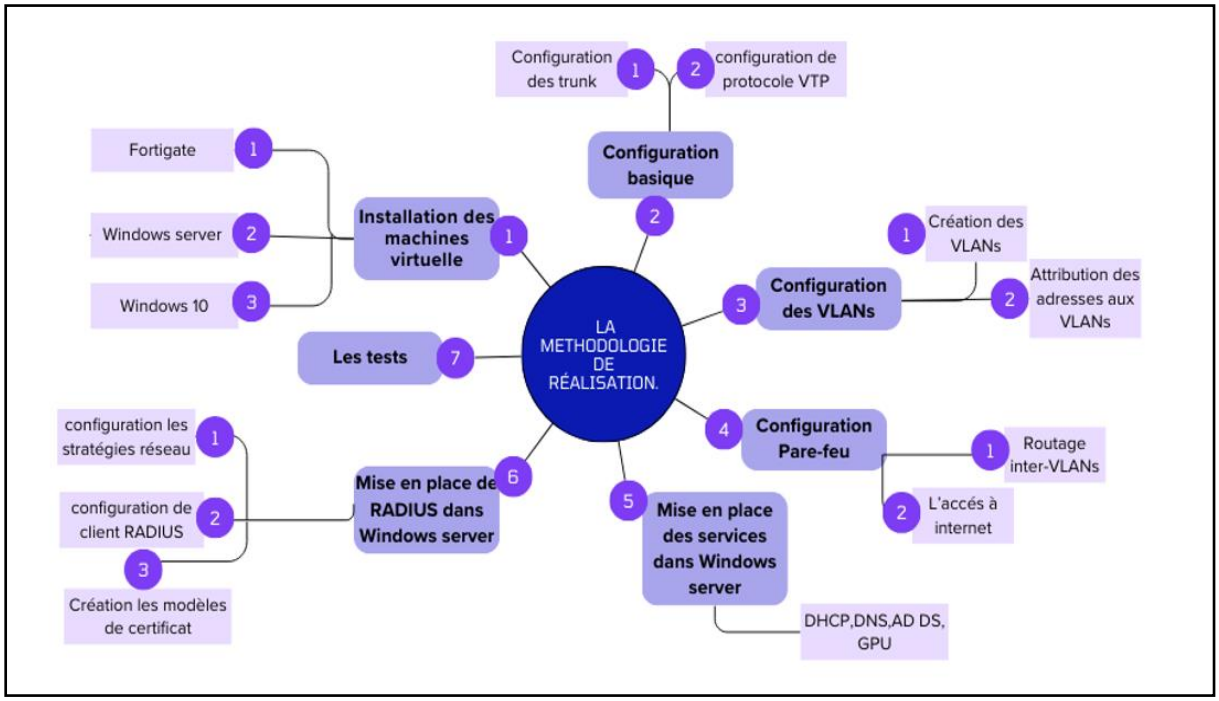

Figure 4.5 La méthodologie de réalisation.

IV.7 Réalisation

IV.7.1 Phase 1 : Installations des machines virtuelles

a) Windows 10

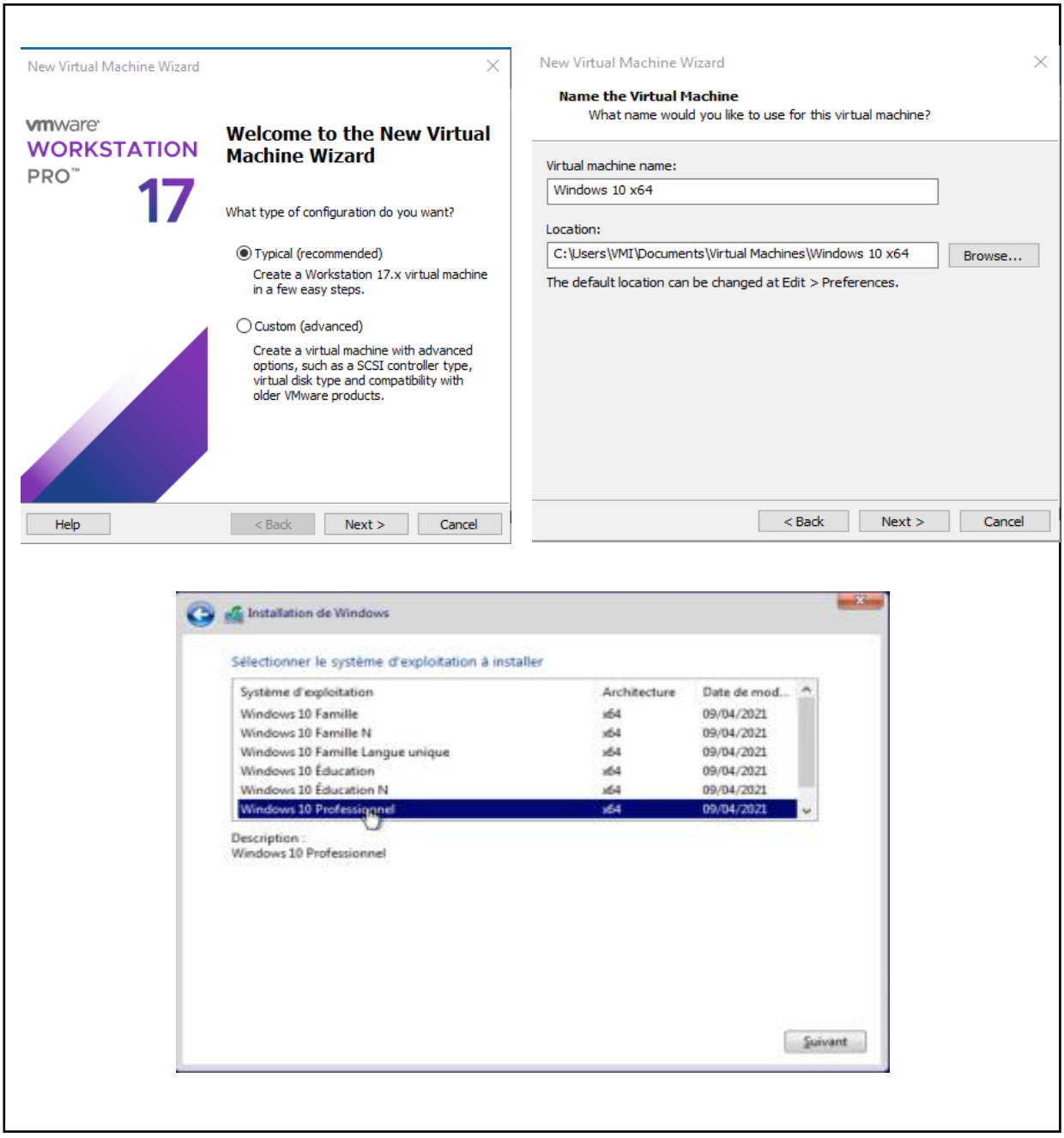

Figure 4.6: Installation du Windows 10.

b) Windows server 2022 :

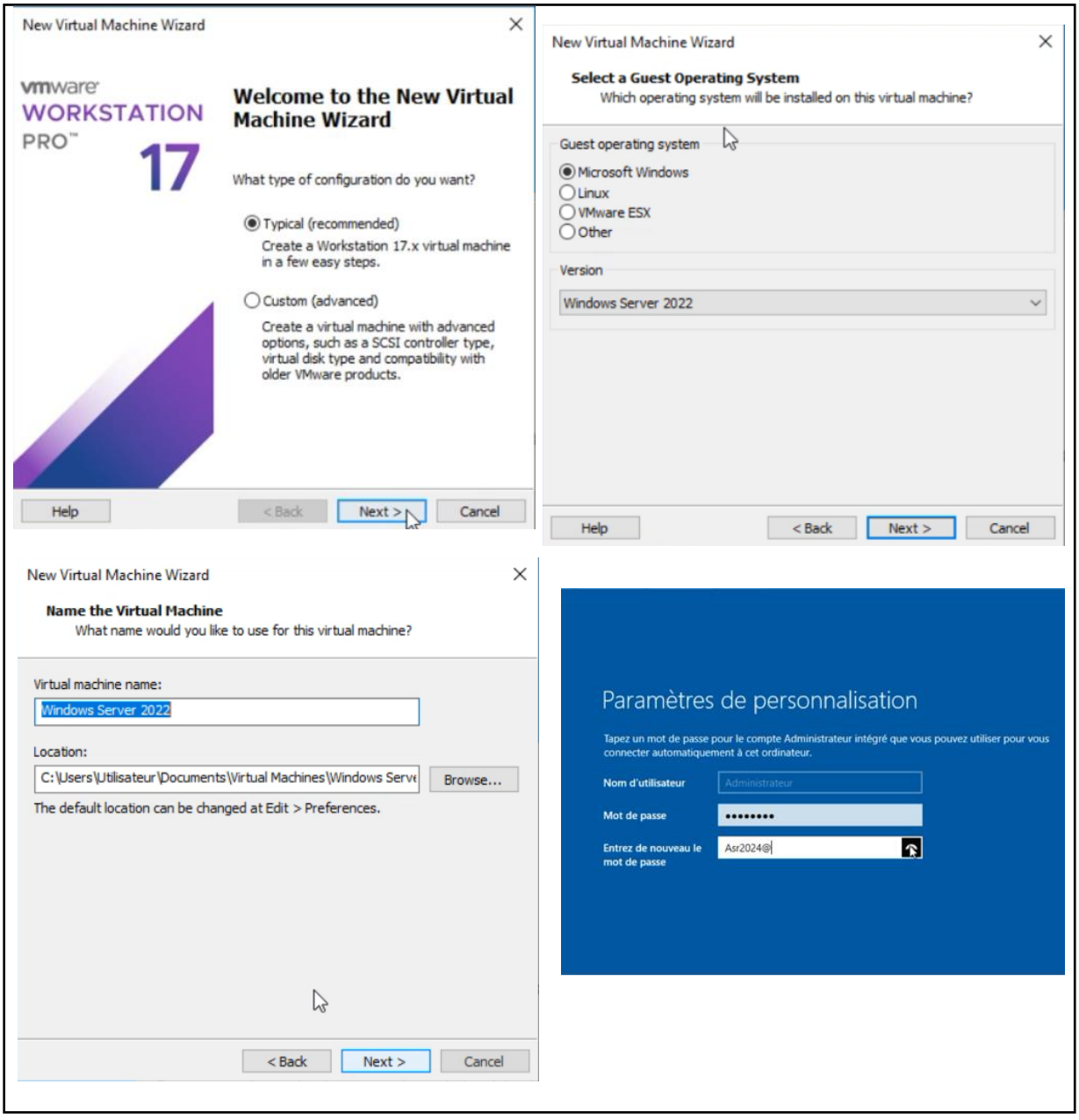

Figure 4.7: Installation du Windows server 2022.

IV.7.2 Phase 2 : Configurations

1) Configuration de pare-feu Fortigate

Tout d'abord, nous avons configuré l'interface de Fortigate, en attribuant un nouveau login, mot de passe, nom et une adresse IP comme les figures suivantes le montrent

Une fois les interfaces configurées, nous pouvons accéder à l'interface de gestion de FortiGate via le navigateur en utilisant l'adresse IP configurée sur l'une des interfaces.

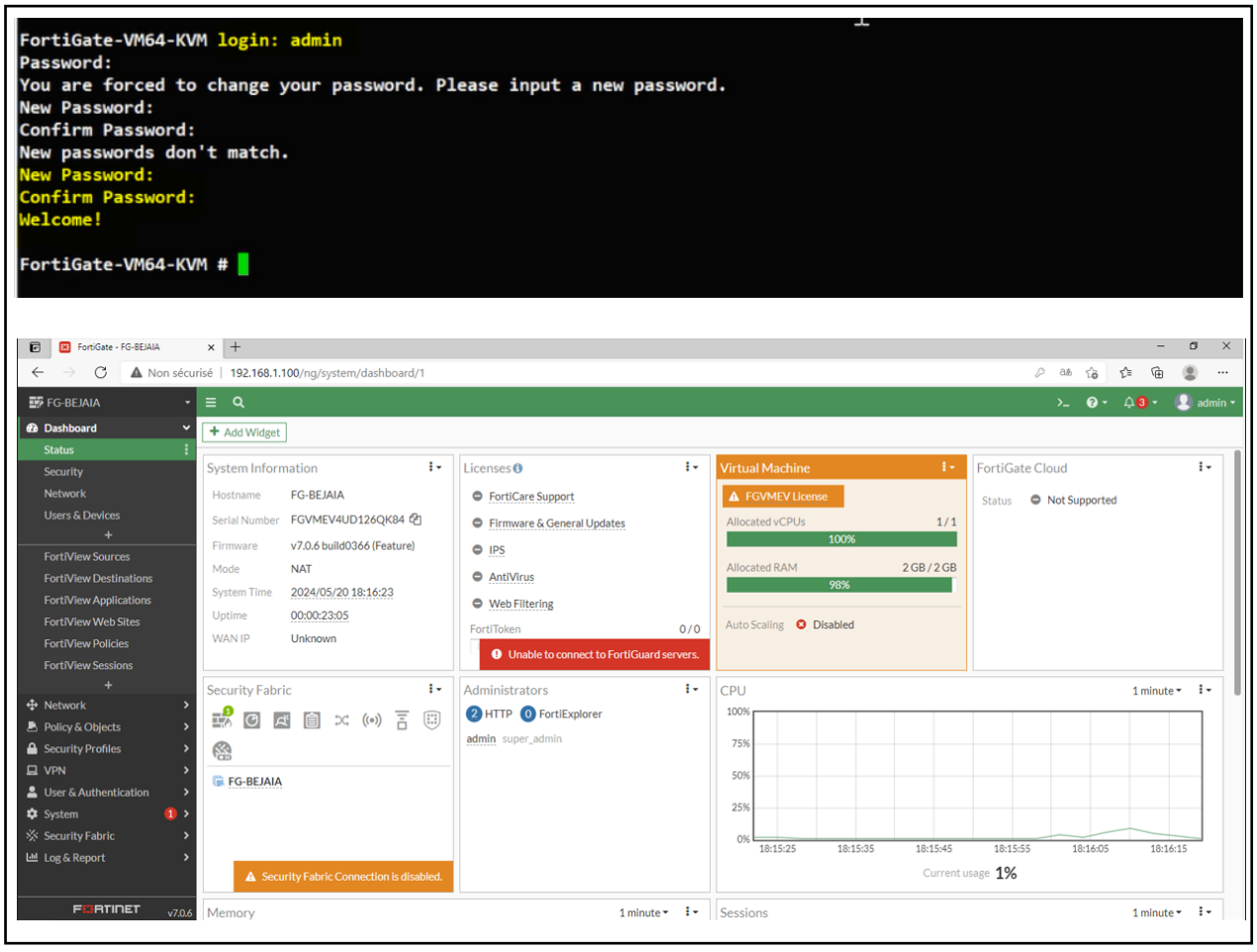

Figure 4.8: Configuration de l'interface de Fortigate.

Ensuite nous avons mis en place une route statique via la passerelle (@ 192.168.122.1) pour accéder à Internet :

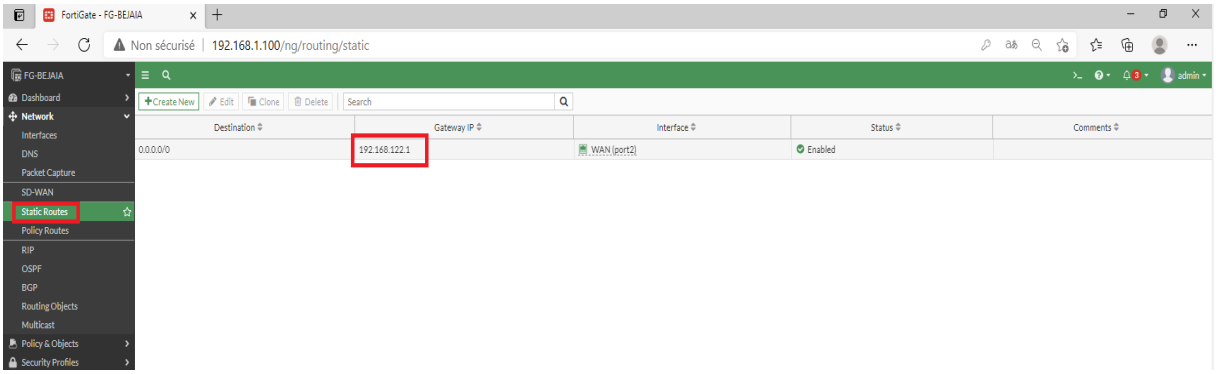

Figure 4.9: La création de la route statique.

Par la suite, nous avons créé les VLAN ainsi qu'une zone de routage pour le routage Inter-VLAN.

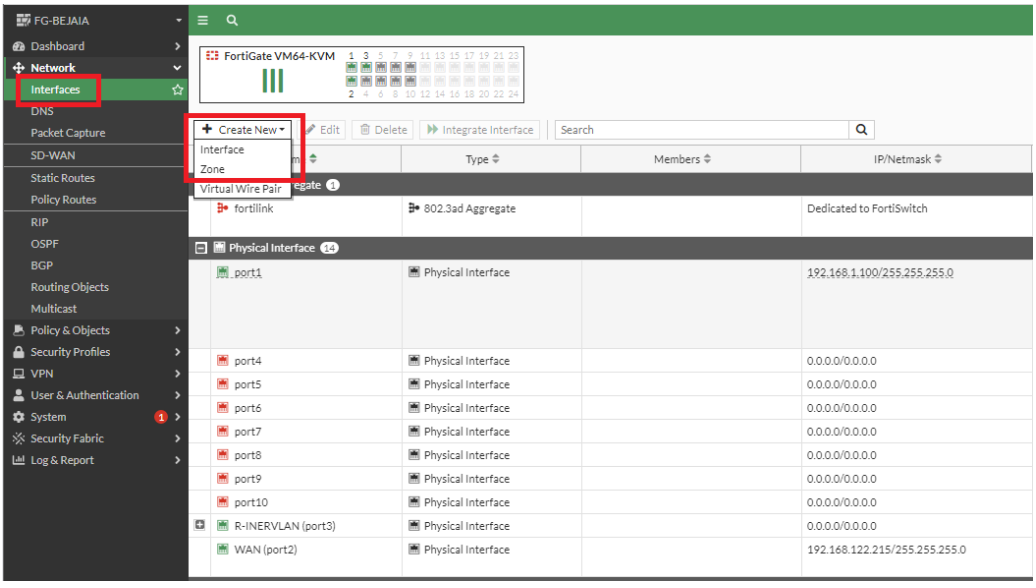

Figure 4.10: La création des interfaces.

Dans la création de VLAN, nous avons configuré une interface VLAN nommée BDD avec un ID VLAN de 4, et seul le PING est autorisé. De plus, un serveur DHCP a été configuré en mode relais avec un type "Regular" et une adresse IP de serveur DHCP définie à 192.168.5.200 (adresse IP de Windows server).

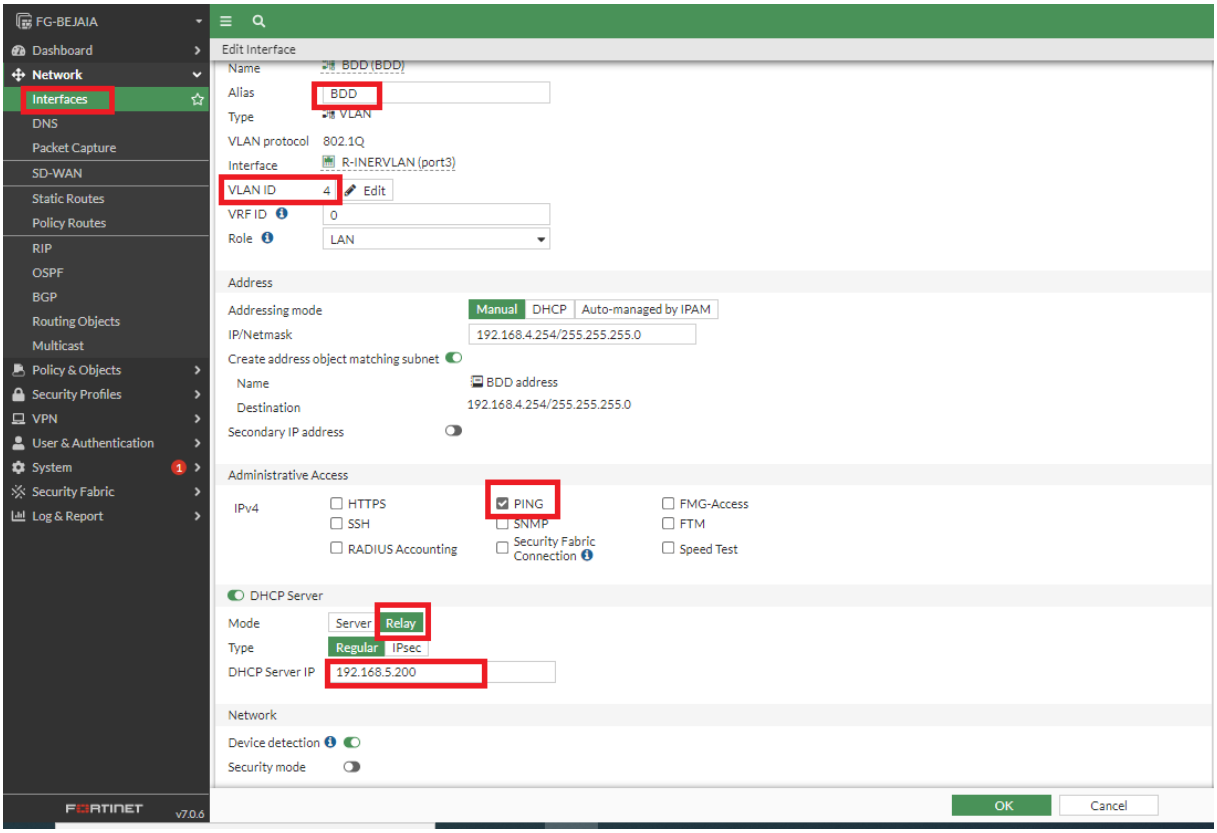

Figure 4.11: La configuration de VLAN BDD.

Nous avons suivi les étapes précédentes pour créer d'autres VLAN.

La figure suivante montre les VLAN déjà créer.

Figure 4.12: Les VLAN crée.

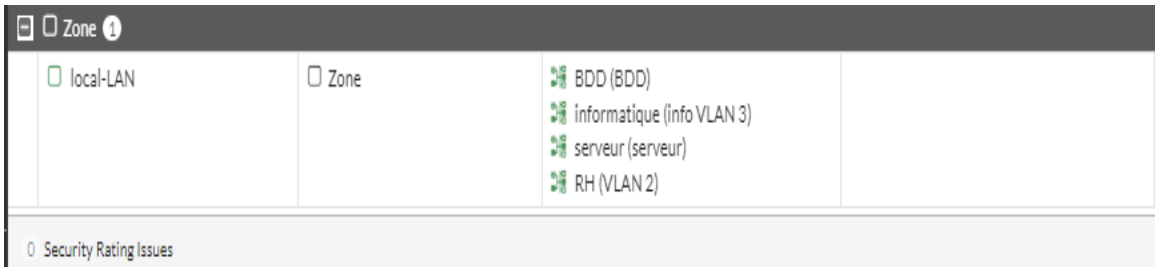

Figure 4.13: La création de la zone.

Maintenant les vlan peuvent se communiquer entre eux.

Après, nous avons défini une politique de pare-feu afin d'accéder à Internet en configurant une règle nommée "ACCES INTERNET". Cette règle permet au trafic provenant de l'interface entrante "local-LAN" de sortir par l'interface "WAN (port2)".

D'autres règles peuvent être configurées, telles que la limitation de la durée d'utilisation d'Internet en définissant des dates, des heures de début et de fin, ainsi que la possibilité d'activer l'antivirus pour filtrer les applications. D'autres options incluent la mise en place de politiques de filtrage des contenus pour bloquer l'accès à des catégories spécifiques de sites web, telles que les réseaux sociaux, les jeux en ligne ou les sites de streaming, pendant les heures de travail.

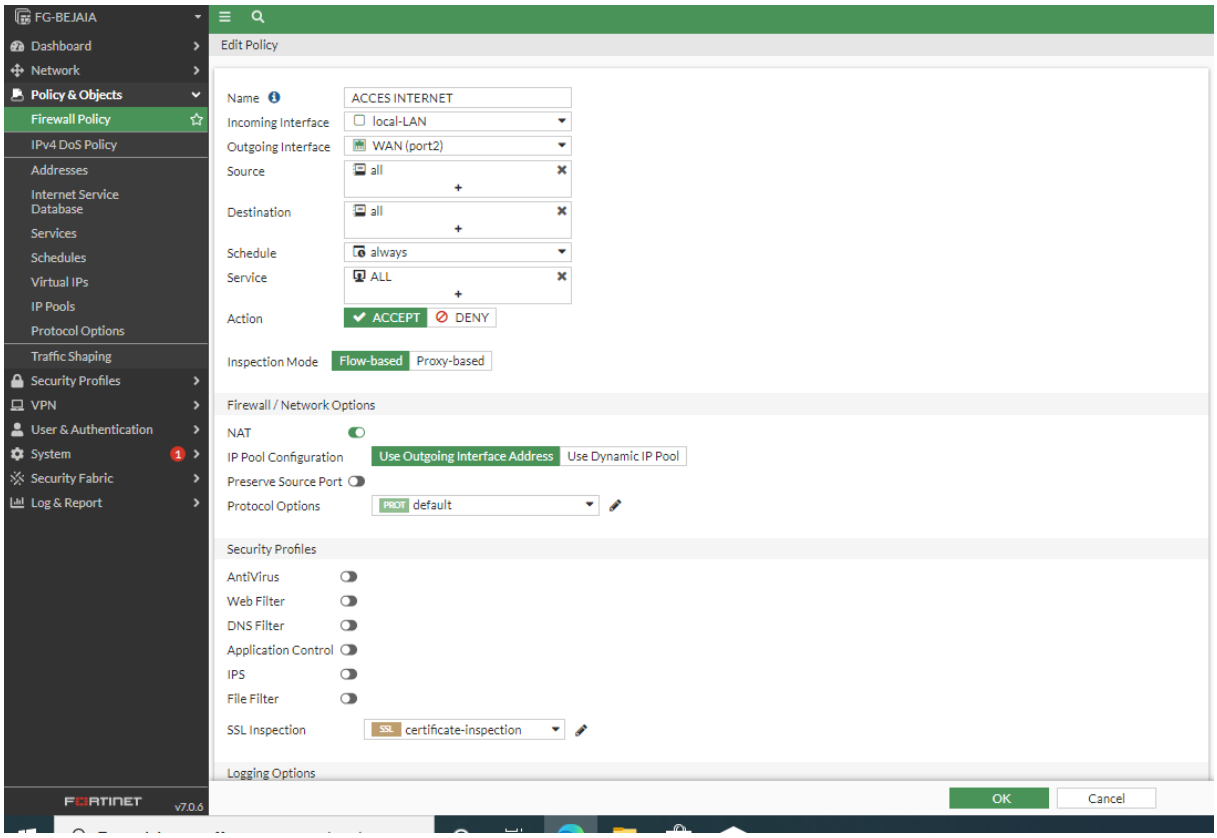

Figure 4.14: Autorisation de trafic.

2) Configuration de Windows server

a) Installation du rôle Active Directory : Après y avoir accéder au serveur, nous avons commencé par ajouter le rôle Active Directory (AD DS) au serveur local avec les rôles Serveur DNS, Serveur DHCP, Services de certificats Active Directory et Services de stratégie et d'accès réseaux.

- Dans le gestionnaire de serveur, nous allons cliquer sur « Ajouter des rôles et fonctionnalités ».

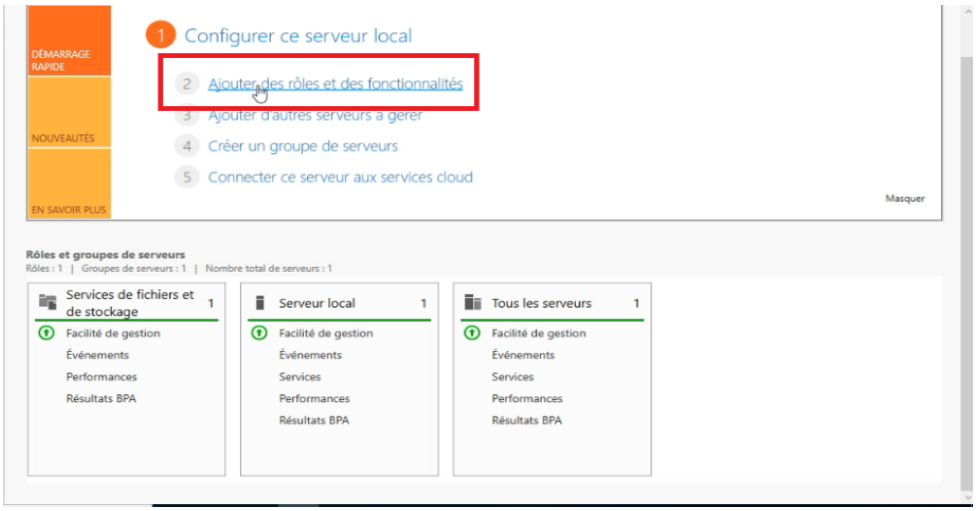

Figure 4.15: Ajouter des rôles et des fonctionnalités.

- Au niveau des rôles, choisir les rôles : Serveur AD DS, Serveur DNS, Serveur DHCP, Services de certificats, Active Directory et Services de stratégie et d'accès réseaux.

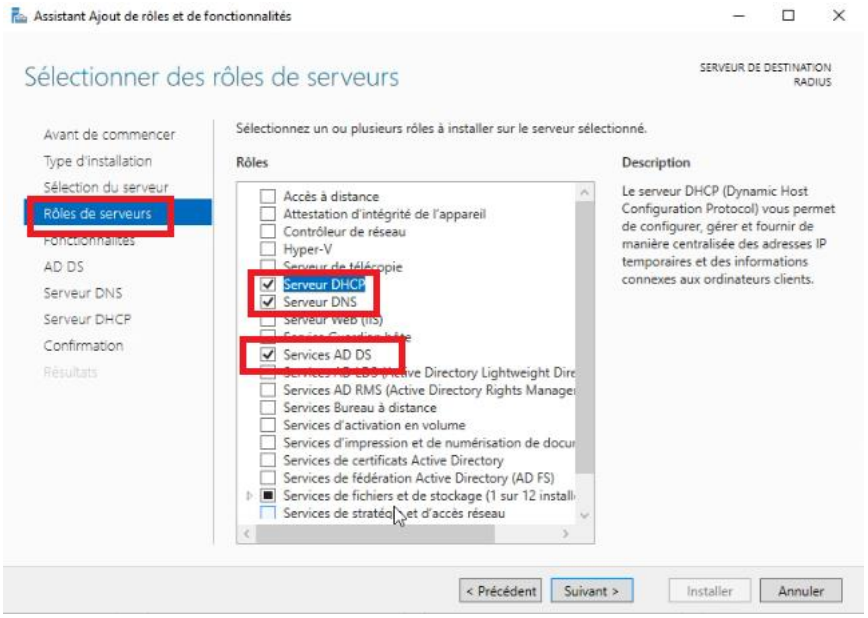

Figure 4.16: La sélection des rôles AD.

- Nous avons suivi les étapes de l'assistant d'installation pour terminer l'installation des rôles.

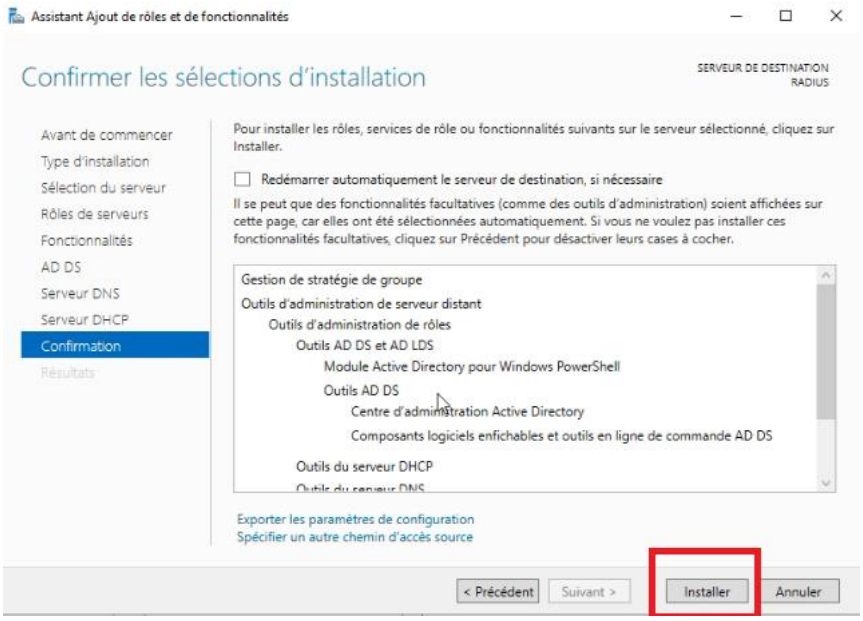

Figure 4.17: Installation les rôles sélectionner.

Une fois les rôles Active Directory sont bien installés nous allons entamer la Configuration.

b) Création de domaine des groupes et des utilisateurs : Pour créer un domaine, des groupes et des utilisateurs, nous allons commencer par la création d'une forêt nommée « SONATRACH.local ». À l'intérieur de cette forêt, nous établirons des groupes et des utilisateurs qui partageront des politiques de sécurité et des stratégies de groupe communes. Cela permettra une gestion centralisée des ressources et des permissions, assurant ainsi une administration efficace et sécurisée de l'ensemble de l'organisation. Les groupes permettront de simplifier la gestion des accès aux ressources, tandis que les stratégies de groupe garantiront que les paramètres de sécurité et les configurations sont appliqués de manière cohérente à tous les utilisateurs et ordinateurs au sein de la forêt SONATRACH.local.

- La création d'une nouvelle forêt en couchant sur « Ajouter une nouvelle forêt » et nous avons spécifié le nom de notre domaine « sonatrach.local ».

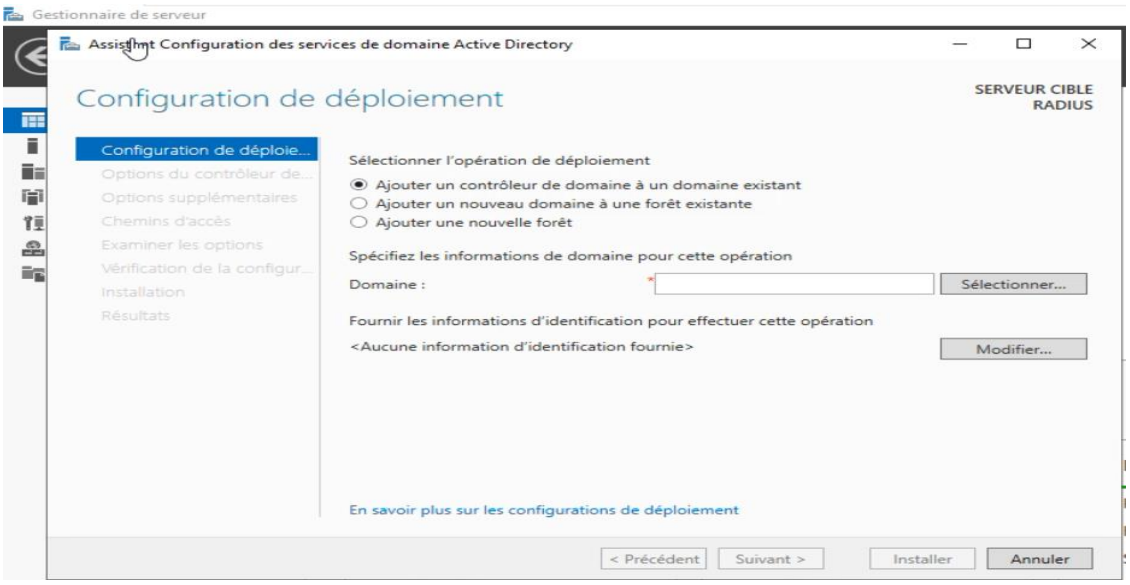

Figure 4.18: Création du domaine « sonatrach.local».

- Choisir le niveau fonctionnel de la forêt et du domaine.

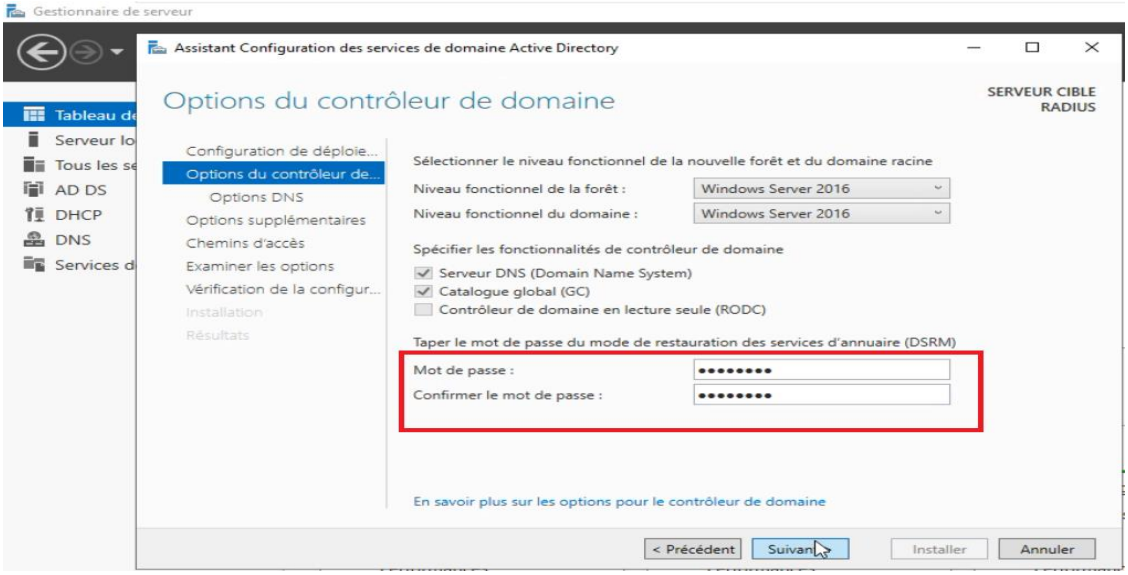

Figure 4.19: Niveau fonctionnel de la forêt et du domaine.

- Pour créer un groupe, un clic droit sur notre domaine "sonatrach.local", "new" puis "group .

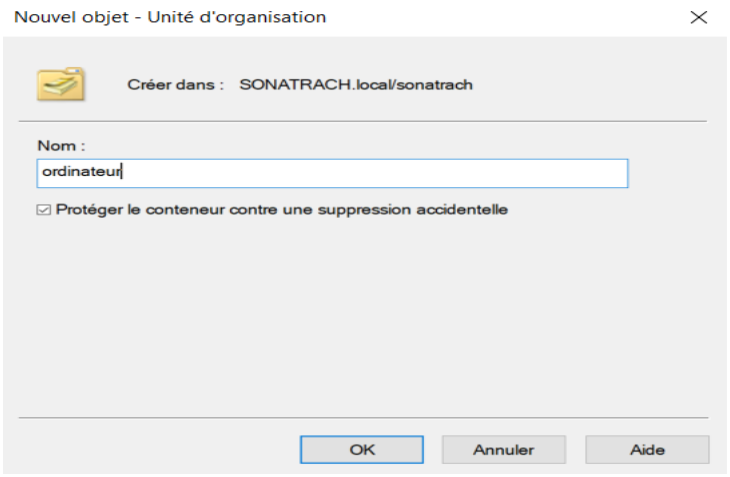

Figure 4.20: Création de groupe ordinateur.

- Pour créer un utilisateur, nous appuyons sur le clic droit sur le domaine "sonatrach.local" puis "New user"

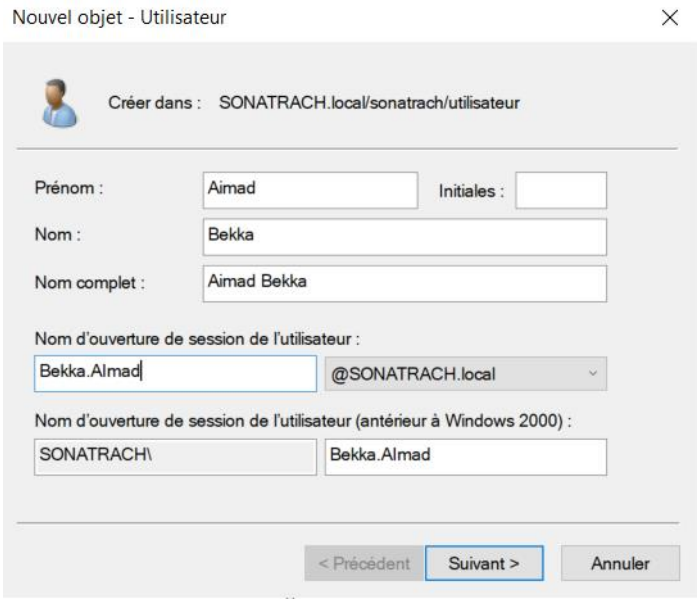

Figure 4.21 : Création d'un utilisateur.

c) **Configuration du service DHCP :** Lors de la configuration du serveur DHCP, il est nécessaire de spécifier un nom et un intervalle d'adresses, comme illustré dans la figure ci-dessous.

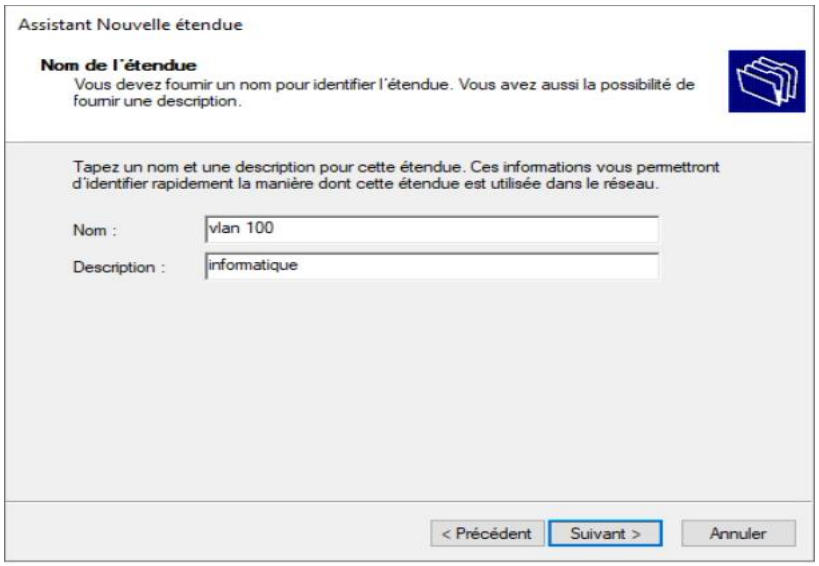

Figure 4.22 : Nom de l'étendue.

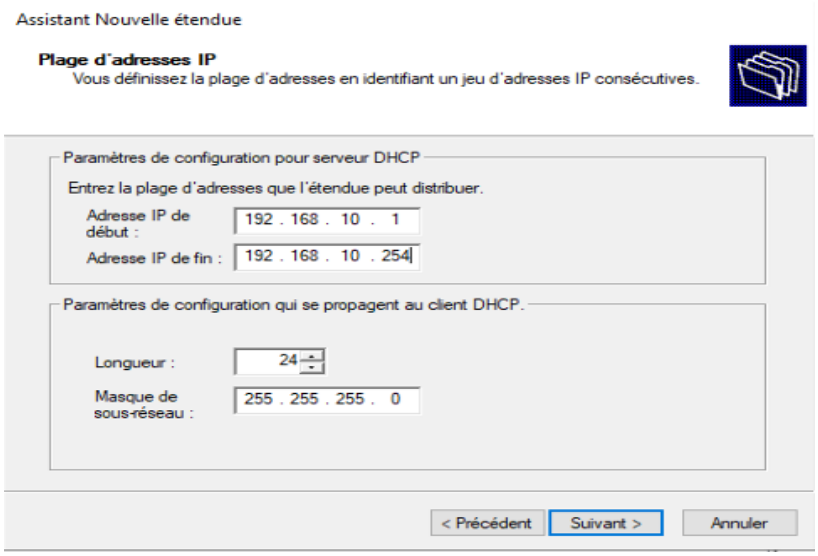

Figure 4.23: Configuration d'une plage d'adresse du serveur DHCP.

- Nous incluons l'adresse IP de la passerelle par défaut pour chaque étendue créée.

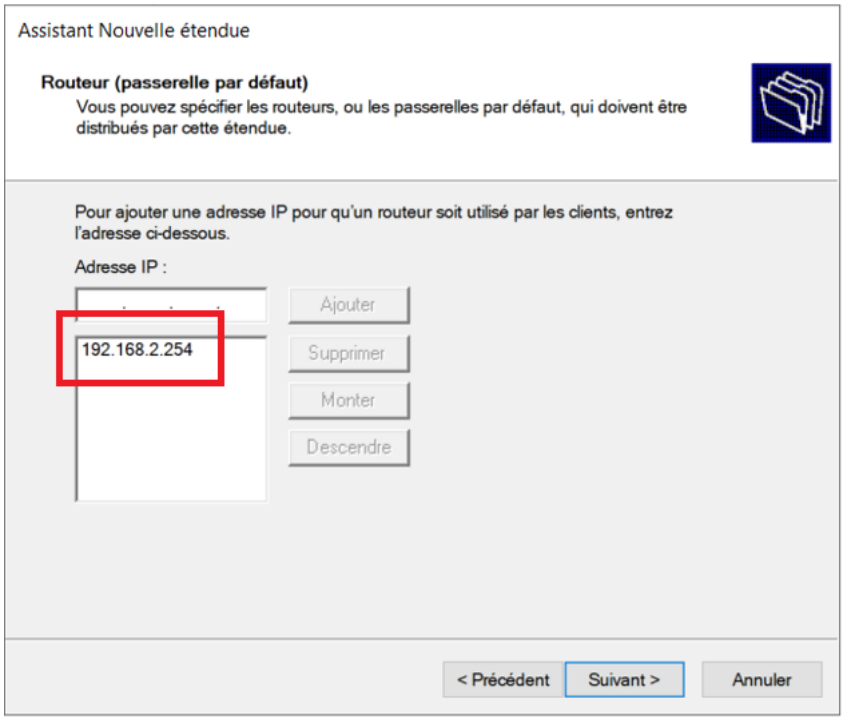

Figure 4.24: Ajout de l'adresse IP de la passerelle.

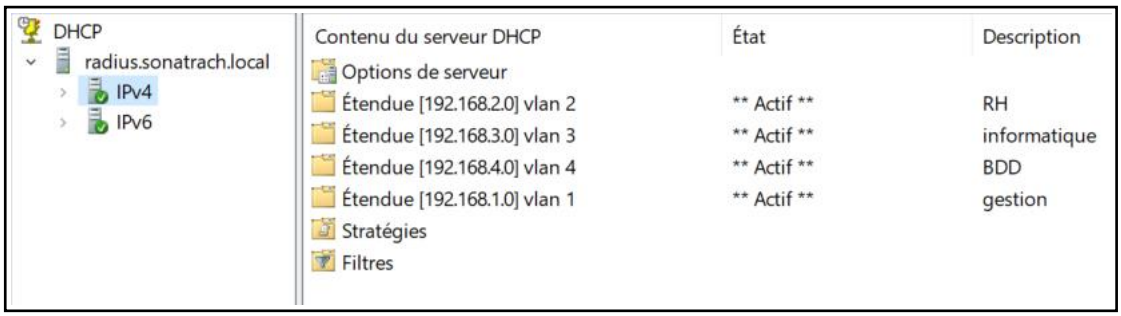

Figure 4.25: Ensemble des plages d'adressage.

d) **Configuration du RADIUS** : Le serveur NPS (Network Policy Server) est déployé en tant que serveur RADIUS. Cette configuration permet au serveur NPS d'assumer plusieurs rôles essentiels dans la gestion des connexions réseau. Tout d'abord, il assure l'authentification des utilisateurs qui tentent de se connecter au réseau, vérifiant leur identité selon les paramètres définis par l'administration. Ensuite, le serveur NPS gère également l'autorisation des connexions, en déterminant les niveaux d'accès appropriés pour chaque utilisateur ou groupe d'utilisateurs en fonction des politiques définies.

- Pour que le serveur NPS puisse accéder aux informations d'identification et aux utilisateurs finaux stockées dans Active Directory, il doit être enregistré dans ce dernier. Ce processus d'enregistrement établit une connexion entre le serveur NPS et Active Directory, permettant ainsi un accès sécurisé aux informations d'identification.

Figure 4.26: Inscrire NPS dans AD.

➢ **Configuration du client RADIUS :** Le client RADIUS (les switches) garantit la communication entre le serveur RADIUS et les utilisateurs finaux. Il agit comme une passerelle qui transmet les demandes d'authentification et d'autorisation des clients au serveur RADIUS, et renvoie les réponses correspondantes du serveur RADIUS aux clients.

- La configuration d'un client RADIUS nommé "SW1" avec l'adresse IP 192.168.5.50 et un secret partagé qui a été défini manuellement pour sécuriser les communications entre ce client et le serveur RADIUS.

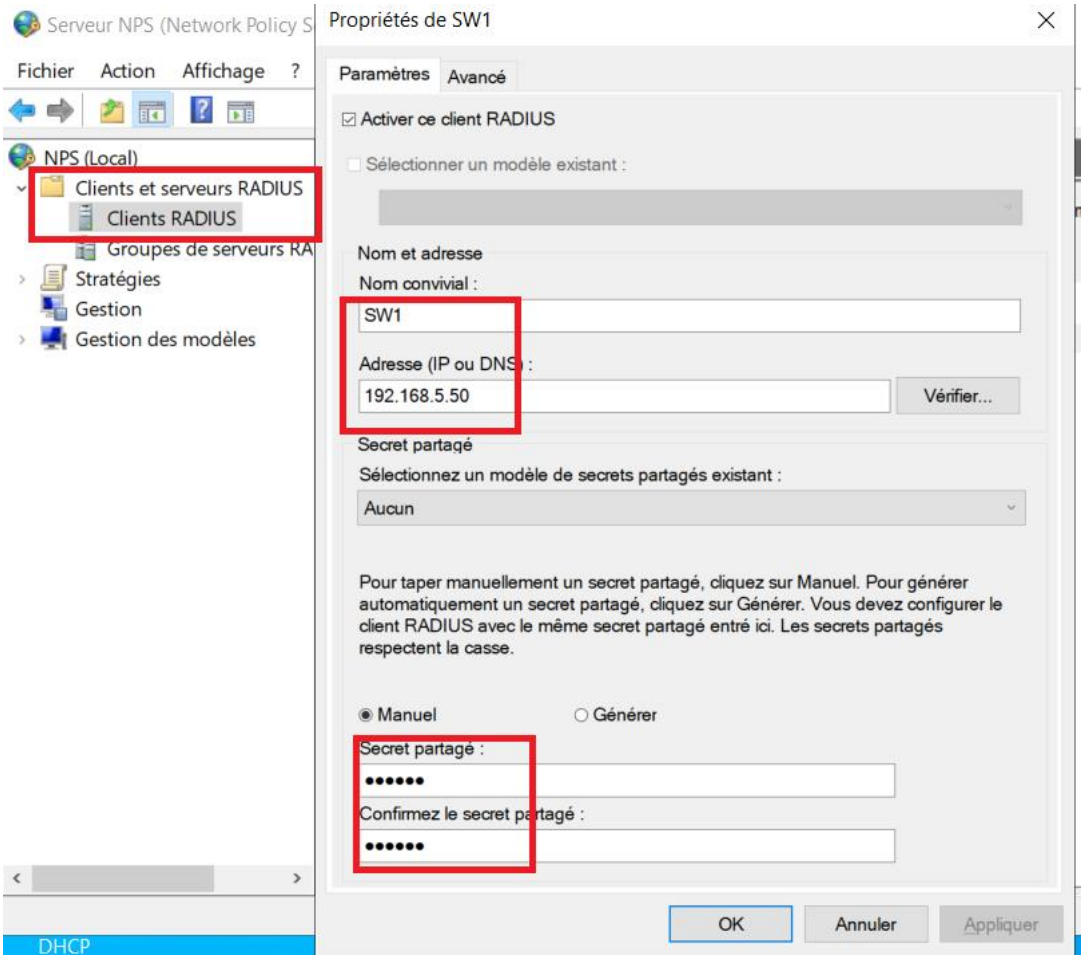

Figure 4.27: Création du client Radius.

e) Création et configuration des stratégies de groupe

➢ **Configuration de la 802.1x :** Pour configurer la norme 802.1X, nous avons suivi ces étapes :

- Nous avons choisi un scénario de configuration adapté à nos besoins : "Serveur RADIUS pour la connexion câblée ou sans fil 802.1

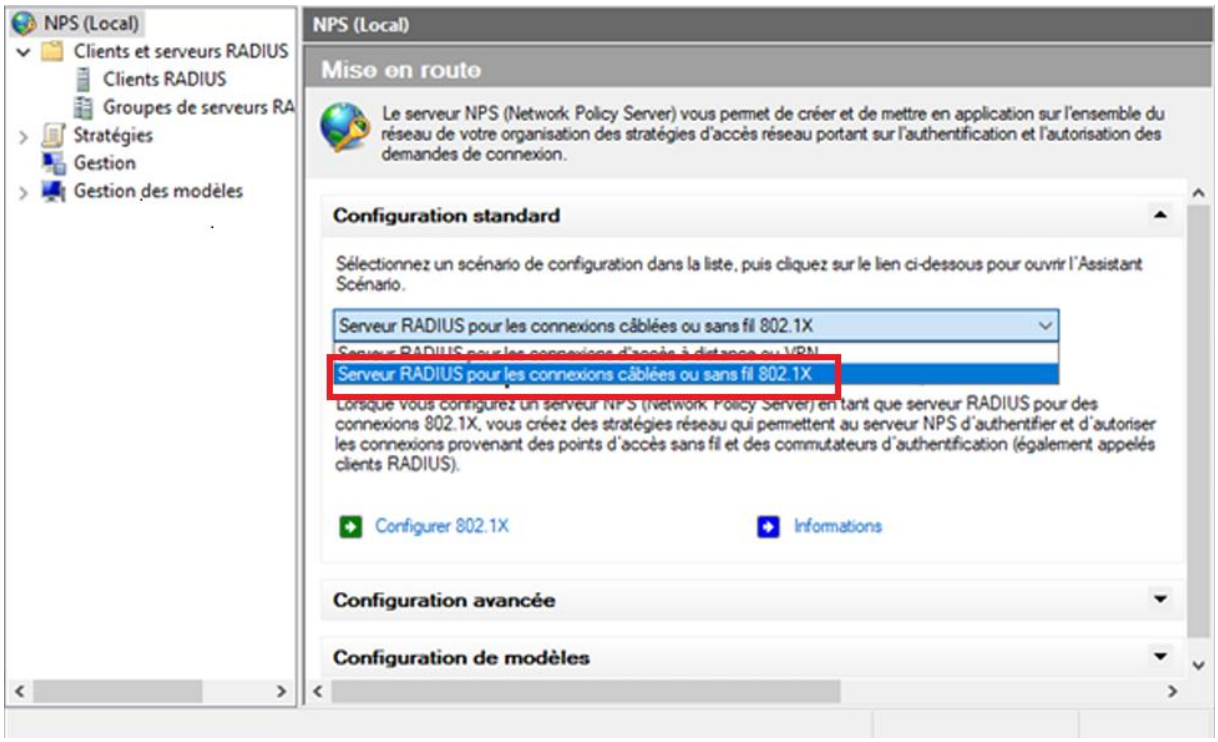

Figure 4.28: Sélection d'un scénario de configuration.

- Nous avons choisi le type d'authentification et de connexion à utiliser. Pour notre cas l'authentification par PEAP pour les réseaux câblés.

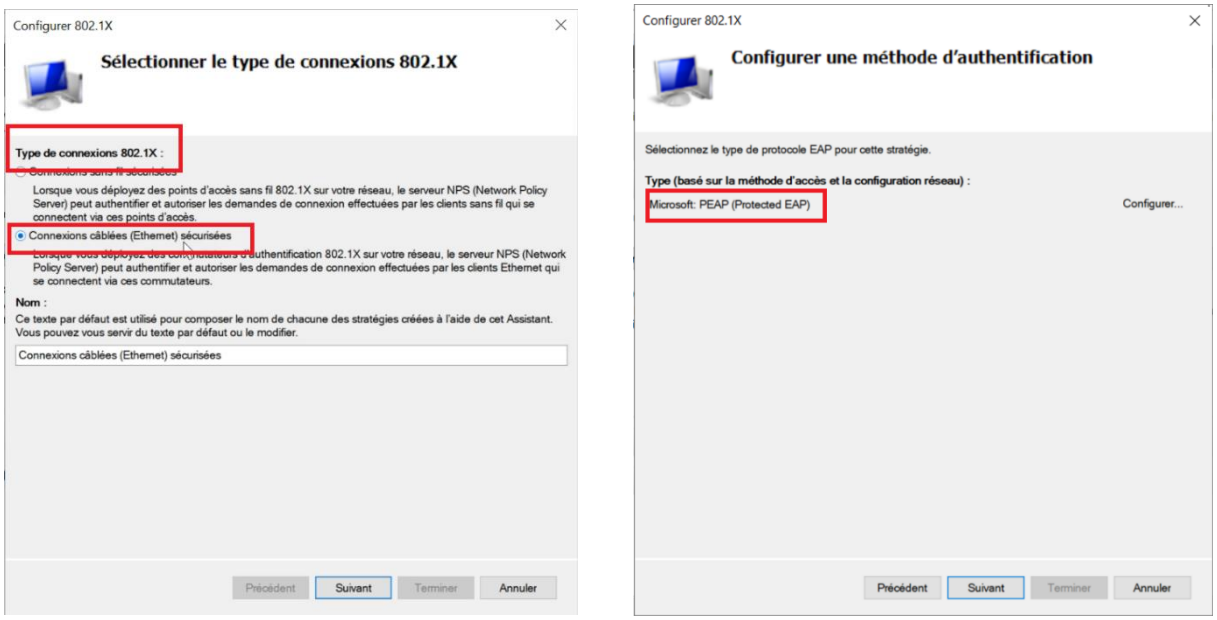

Figure 4.29: Type d'authentification deconnexion802.1X.

- Nous avons ajouté les clients Radius (les switches)

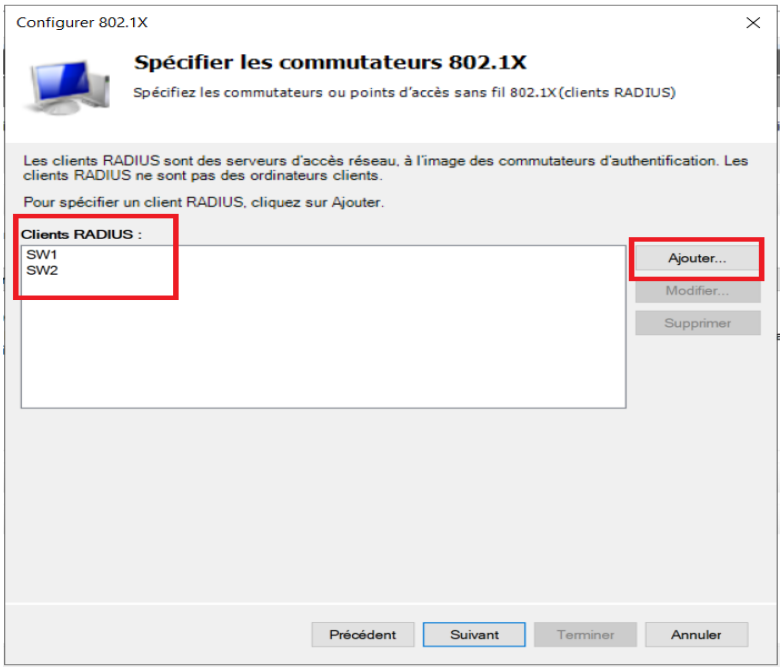

Figure 4.30: Ajout de client Radius.

➢ **Activer la distribution du certificat automatiquement** : nous allons activer la distribution automatique des certificats, un certificat sera délivré automatiquement pour chaque PC.

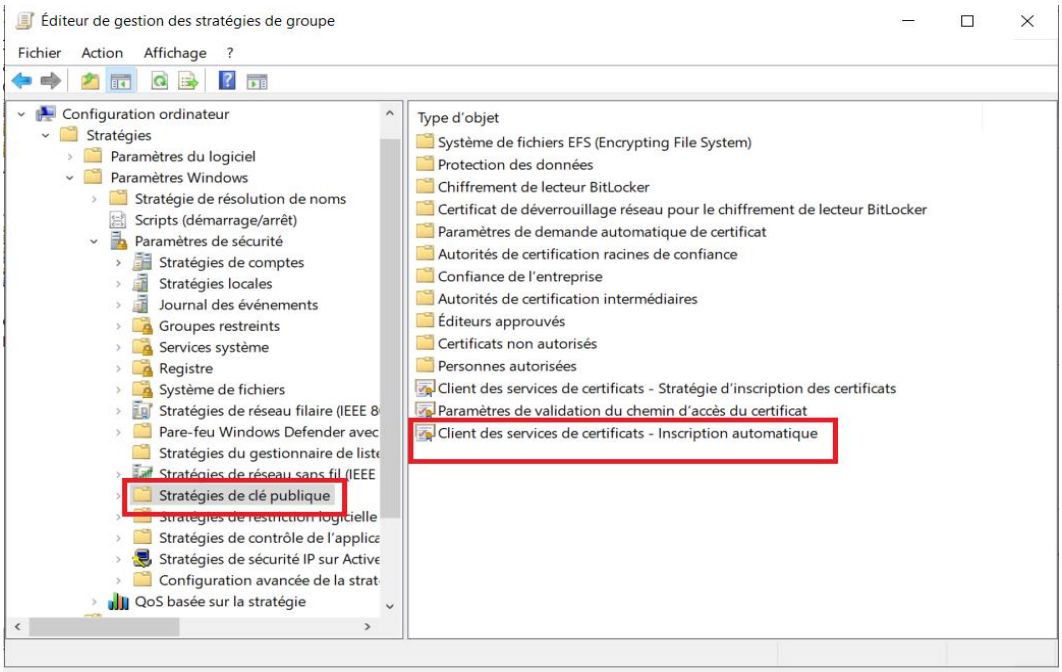

Figure 4.31: Activation de la stratégie inscription automatique.

➢ **Configuration de l'authentification sur le client-RADIUS :** La configuration Radius au niveau des switches clients sont comme suit :

- Nous avons activé le nouveau modèle AAA.

```
SW1(config)# aaaaaa new-model
```

- Nous avons créé une liste d'authentification "default" qui indique que L'authentification des utilisateurs se fera en 802.1x grâce au protocole Radius.

```
SW1(config)# aaa authentication dot1x default group radius
```

- L'autorisation d'accès au réseau par le serveur Radius.

```
SW1(config)# aaa authentication dot1x default group radius
```

- Nous avons activé la 802.1x sur le switch.

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

- Nous avons donné l'adresse de notre serveur RADIUS, ainsi que le mot de passe.

```
SW1(config)# radius server SERVER-RADIUS
SW1(config-radius-server)# address ipv4 192.168.5.200
SW1(config-radius-server)# key 0 RADIUS
SW1(config-radius-server)# exit
```

- Nous avons activé le 802.1X sur le port relié à l'utilisateur.

```
SW1(config)# interface eth0/0
SW1(config-if)# switchport mode access
SW1(config-if)# switchport nonegotiate
SW1(config-if)# authentication port-control auto
SW1(config-if)# dot1x pae authenticator
SW1(config-if)# authentication host-mode multi-domain
SW1(config-if)# exit
```

- Nous avons indiqué l'interface source du client RADIUS.

```
SW1(config)# ip radius source-interface Vlan 5
```

IV.7.3 Phase 3 : Testes

a) **Test DHCP :** Nous avons utilisé la commande « IP DHCP » sur plusieurs PC pour vérifier si la configuration des adresses IP a été correctement faite par le serveur DHCP.

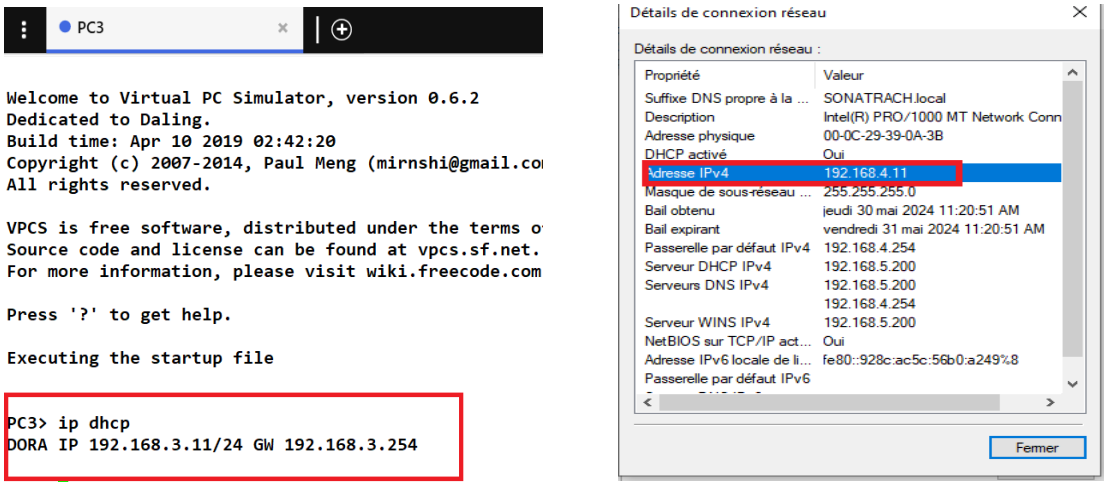

Figure 4.32: Test DHCP.

b) **Test routage inter-VLANs :** pour la vérification de routage inter-vlan, nous avons pris un exemple du vlan BDD au vlan Informatique, pour cela nous avons lancé un ping du PC1(192.168.4.11) vers le PC3 (192.168.3.11)

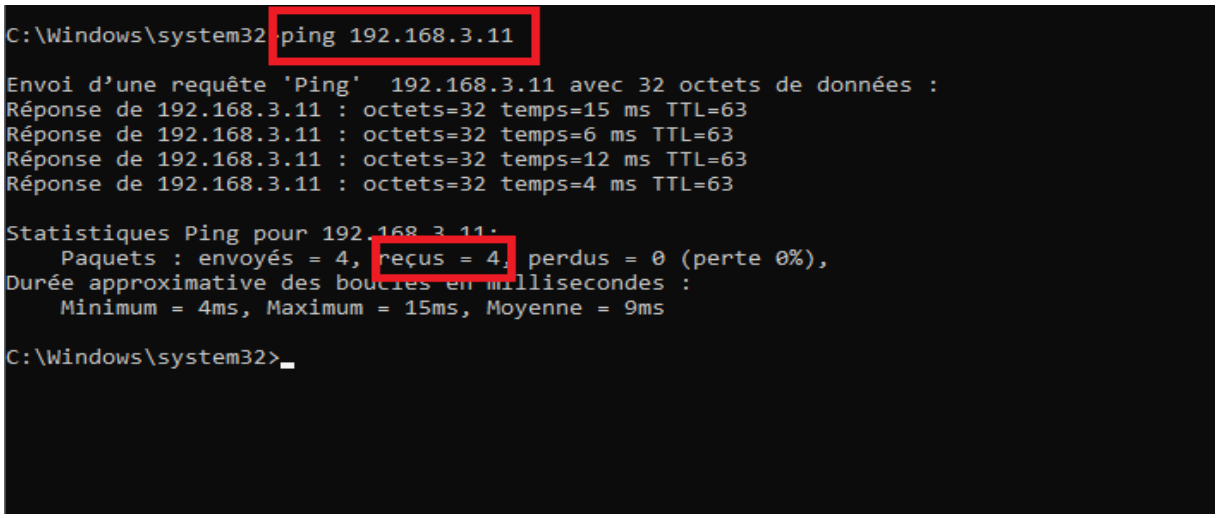

Figure 4.33: Test de routage.

c) **Test routage inter-VLANs :** pour la vérification de la connectivité entre le serveur-RADIUS (RADIUS) et le Client-RADIUS (SW1), nous avons lancé un ping sur l'invite commande (cmd) du serveur avec la commande (Ping adresse IP).

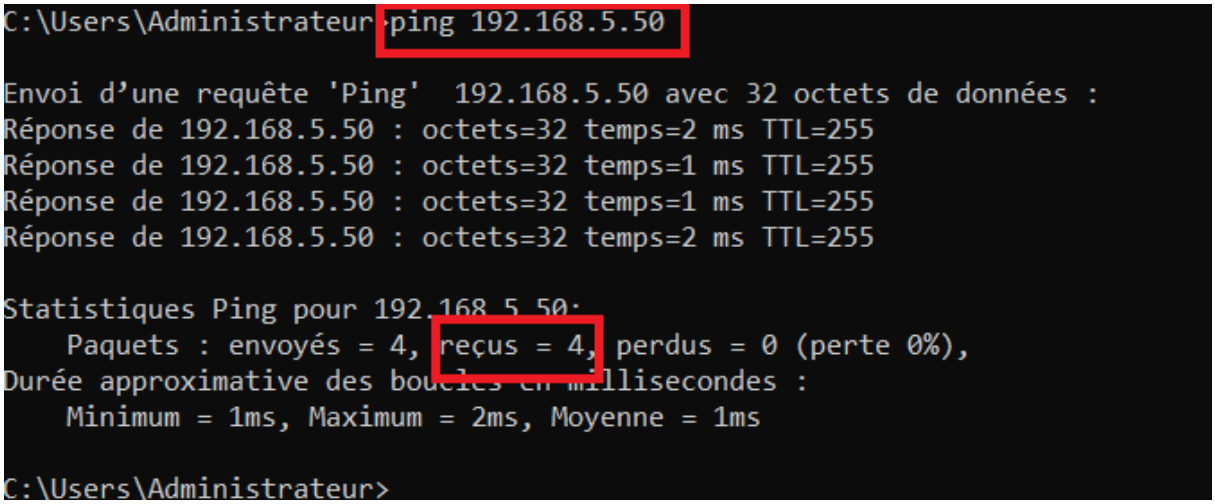

Figure 4.34: Test entre le client-RADIUS et le serveur-RADIUS.

e) **Test de l'authentification RADIUS :** Une fois la configuration de Radius est approuvée, ainsi que toutes les stratégies sont mises à jour, les ordinateurs et les utilisateurs sont rajoutés à leurs groupes, nous constaterons que les PC obtiendront des certificats.

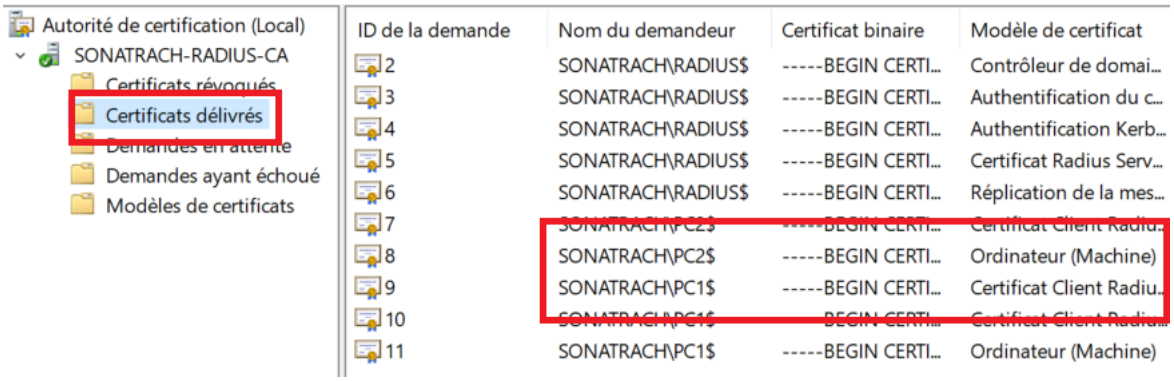

Figure 4.35: Obtention du certificat.

Pour l'authentification RADIUS nous avons deux cas :

1) **L'authentification réussie :** lorsque que le PC2 est ajouté dans le groupe vlan RH nous verrons sur wireshark que client (192.168.5.50) tente de s'authentifier auprès d'un serveur RADIUS (192.168.5.200), une demande d'accès (Access-Request) envoyée par le client et de défis d'accès (Access-Challenge) retournés par le serveur, où le serveur demande des informations supplémentaires. Finalement, le serveur accepte l'authentification (Access-Accept), indiquant que le client a fourni les informations correctes et que l'authentification a réussi.

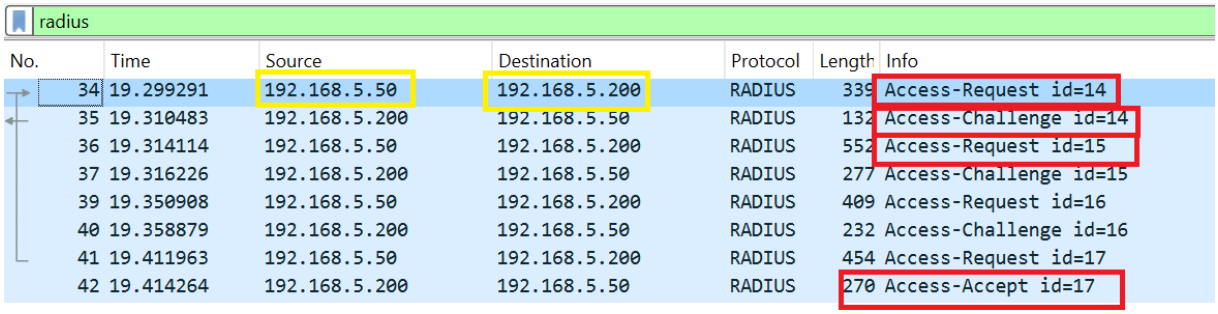

Figure 4.36: Authentification réussie sur Wireshark.

Au niveau du journal d'événement qui se trouve dans le serveur, nous allons voir que l'authentification du PC2 est faite avec succès.

Figure 4.37 : Journal d'événement.

Et sur la console du switch Client Radius à l'aide de la commande "show authentification sessions interface Ethernet 0/0 détail" nous verrons que l'authentification est faite avec succès.

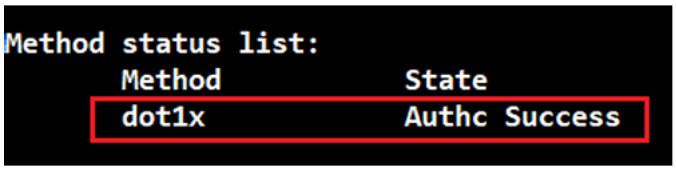

Figure 4.38: Authentification succès.

2) **L'authentification échouée :** Afin de garantir que le serveur RADIUS permet effectivement d'authentifier les hôtes des utilisateurs par un certificat, nous avons testé cela en éliminant "PC2" du groupe" vlan RH". PC2 n'aura plus la possibilité de s'authentifier au domaine "sonastrach.local" ni d'avoir un certificat et donc aucun accès au réseau local de l'entreprise.

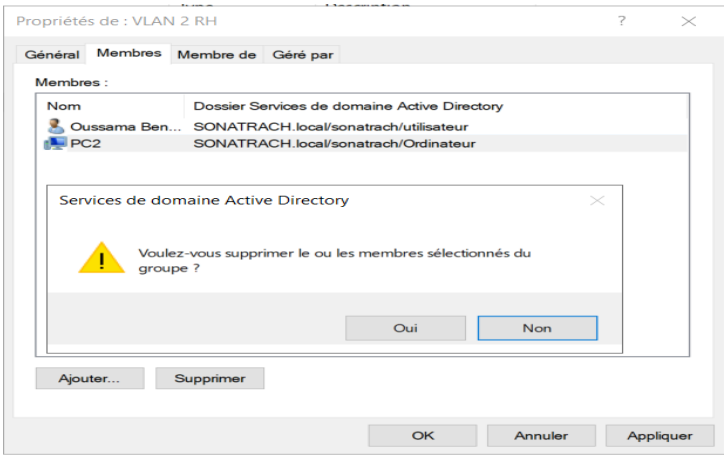

Figure 4. 39: Supprimer le PC2 du Vlan RH.

PC2 ne sera plus authentifié.

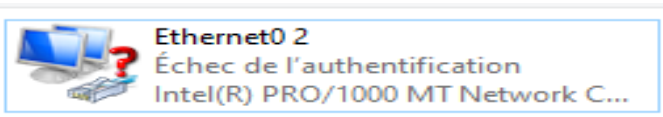

Figure 4.40: Echec d'authentification.

Sur Wireshark nous verrons que l'accès est rejeté.

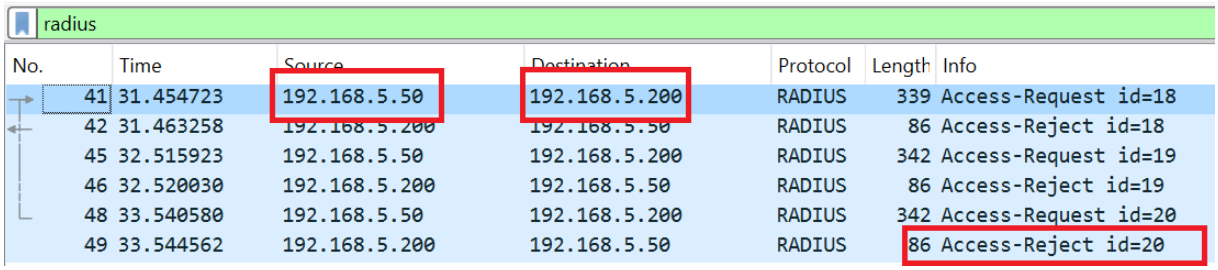

Figure 4.41: Authentification rejeté sur Wireshark.

Et au niveau du journal d'événement, nous verrons un échec d'authentification.

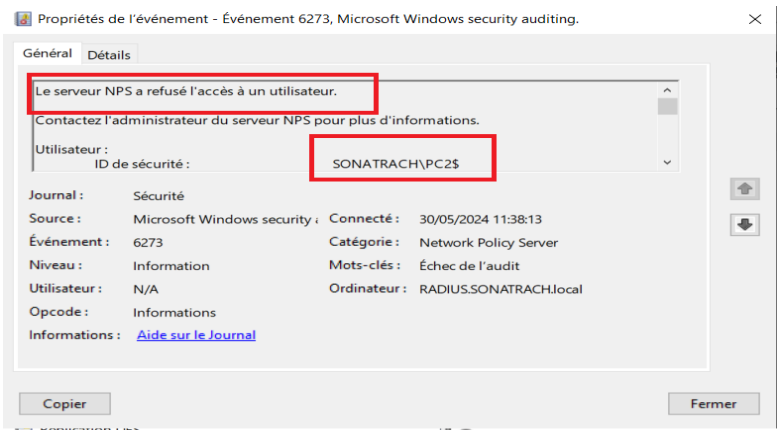

Figure 4.42: Journal d'événement.

IV.8 Conclusion

Dans ce chapitre, nous avons présenté notre environnement de travail, comme nous avons montré l'implémentation de notre solution d'authentification par certificats RADIUS. Le serveur de contrôle d'accès Radius offre une réponse pertinente aux difficultés de connexion au réseau local et améliore la gestion de l'accès au réseau. Sa simplicité d'installation constitue un avantage majeur.

En conclusion, notre étude met en évidence l'importance de l'authentification des utilisateurs par RADIUS pour accéder aux données d'un système.

Conclusion Générale

L'évolution rapide et significatif des technologies de l'information et de la communication incite continuellement à la recherche de nouveaux outils visant à faciliter la gestion et la sécurisation des données. Afin de réduire les risques de cyber-attaques et maintenir la sécurité de manière efficace les entreprises adoptent différentes stratégies et outils pour protéger leurs informations sensibles et assurer la continuité des opérations. Parmi ces outils les solutions de gestion des identités et des accès.

Dans ce mémoire, nous avons abouti à une solution permettant d'assurer une gestion centralisée des utilisateurs et des droits d'accès. Cette méthode repose sur l'authentification par RADIUS, qui s'appuie sur le protocole PEAP pour garantir une authentification sécurisée des utilisateurs, la norme 802.1X qui permet de contrôler les accès aux réseaux. Cette pratique facilite la gestion des accès pour l'administrateur et une meilleure flexibilité en s'adaptant facilement aux besoins changeants des entreprises.

Grâce à la réalisation de ce projet, nous avons pu tirer profit en approfondissant nos connaissances et améliorant notre expertise en matière de réseaux locaux et d'administration. De plus, nous avons eu la chance d'apprendre à utiliser Windows server, gérer les équipements et utilisateurs et en mettre en place des Stratégies de sécurité solides et efficaces.

Enfin comme perspective pour ce projet nous souhaitons également exploiter mieux les services qu'offre le protocole radius notamment l'authentification des utilisateurs pour les connexions réseau sans fil et l'accès à distance.

BIBLIOGRAPHIE

[1] Stewart, J. M., & Kinsey, D. (2020). **Network security, firewalls, and VPNs (**3rd ed.). Jones & Bartlett Learning.

[2] https://www.axis-solutions.fr/cyberattaques-les-5-types-les-plus-courants

[3] https://www.cloudflare.com/fr-fr/learning/ddos/glossary/denial-of-service

[4] https://www.fortinet.com/fr/resources/cyberglossary/cia-triad

[5] https://www.cyberuniversity.com/post/quest-ce-que-lauthentification-et-pourquoi-cest-crucial-en-matiere-de-securite-informatique

[6] https://blog.mailfence.com/fr/difference-chiffrement-symetrique-asymetrique/

[7] https://www.cisco.com/c/fr_fr/products/security/firewalls/what-is-a-firewall.html

[8] Stewart, J. M., & Kinsey, D. (2020). **Network Security, Firewalls, and VPNs** (3rd ed.). Jones & Bartlett Learning. ISBN: 978-1-284-18365-8

[9] Stewart, J. M., & Kinsey, D. (2020). **Network Security, Firewalls, and VPNs** (3rd ed.). Jones & Bartlett Learning.

[10] https://www.varonis.com/fr/blog/ids-et-ips-en-quoi-sont-ils-differents

[11] Chaouchi, H., & Laurent-Maknavicius, M. (2018). **Sécurité des réseaux sans fil et mobiles - Les 3 volumes** [Wireless and Mobile Network Security - The 3 Volumes]. Editions Eyrolles. ISBN: 978-2-7462-1697-6

[12] https://www.avast.com/fr-fr/c-wep-vs-wpa-or-wpa2

[13] https://aws.amazon.com/fr/what-is/ssl-certificate

[14] https://www.udemy.com/course/ipsec-vpn/

[15] https://www.fortinet.com/fr/resources/cyberglossary/radius-protocol

[16] https://fr.linkedin.com/advice/3/how-do-you-compare-radius-tacacs-protocols?lang=fr

[17] https://www.cybersecura.com/post/authentification-definition-et-methodes

[18] https://www.certigna.com/authentification-par-certificat

[19] https://www.fortinet.com/fr/resources/cyberglossary/authentication-token

[20] https://fr.wikipedia.org/wiki/Authentification_forte

[21] https://www.sia-partners.com/fr/publications/publications-de-nos-Experts/authentification-forte-un-defi-cle-a-relever-pour-les

[22] https://www.pingidentity.com/fr/resources/identity-fundamentals/identity-and-access-management/centralized- decentralized-identity-management.html

[23] Fanti, M. (2023**). Implementing Multifactor Authentication: Protect Your Applications from Cyberattacks with the Help of MFA**. Packt. ISBN : 978-1803246963.

[24] A. Mazouzi, « **Services d'Authentication et Annuaires** », UFR Informatique, UCB Lyon1, 14 décembre 2009.

[25] Carroll, Brandon. **Cisco Access Control Security : AAA Administration Services**. Cisco Press, 2004, ISBN : 978-1-58705-124-1.

[26] RADIUS par Jonathan Hassell, O'Reilly Media, Inc., octobre 2002, 206 pages.

[27] Bordères, S. (2006). **Authentification réseau avec Radius : 802.1x - EAP - FreeRadius**. Blanche. ISBN : 978-2-212-0073.

[28] https://docs.gns3.com/docs/

[29] https://docs.vmware.com/en/VMware-Workstation-Pro/index.html

[30] https://www.wireshark.org/docs/

[31] https://www.merit.edu/

Annexe

- **Configuration de base et administration de l'architecture proposée**

1) **Configuration du mode trunk** : utilisé sur les commutateurs réseau pour permettre le transport de plusieurs VLAN sur un seul lien physique, nous le configurons sur tous les ports actifs des commutateurs de la topologie.

```
IOU2(config)#interface eth
IOU2(config)#interface ethernet 0/3
IOU2(config-if)#sw
IOU2(config-if)#switchport trunk encap
IOU2(config-if)#switchport trunk encapsulation d
IOU2(config-if)#switchport trunk encapsulation dot1q
IOU2(config-if)#interface ethernet 0/3
IOU2(config-if)#switchport trunk encapsulation dot1q
IOU2(config-if)#switchport mode trunk
IOU2(config-if)#
*May 20 23:58:27.273: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to down
IOU2(config-if)#
*May 20 23:58:30.278: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to up
IOU2(config-if)#
```

Figure 1: Configuration mode trunk.

2) **Le protocole VTP :** utilisé pour la création, la suppression et la modification des VLANs à partir d'un switch central appelé serveur VTP, ce protocole assure la propagation automatique de ces modifications aux autres switches clients du réseau, garantissant ainsi une synchronisation cohérente des configurations de VLANs.

```
IOU1(config)#
IOU1(config)#
IOU1(config)#vtp mode server
Device mode already VTP Server for VLANS.
IOU1(config)#vtp password cisco
Setting device VTP password to cisco
IOU1(config)#vtp domain campusvtp
Changing VTP domain name from NULL to campusvtp
IOU1(config)#vtp ver
IOU1(config)#vtp version 2
IOU1(config)#end
```

Figure 2: Configuration VTP Server.

```
IOU1(config-vlan)#vlan 2
IOU1(config-vlan)#name RH
IOU1(config-vlan)#vlan 3
IOU1(config-vlan)#name informatique
IOU1(config-vlan)#vlan 4
IOU1(config-vlan)#name BDD
IOU1(config-vlan)#vlan 5
IOU1(config-vlan)#name serveur
IOU1(config-vlan)#vlan 6
IOU1(config-vlan)#name gestion
IOU1(config-vlan)#name 99
IOU1(config-vlan)#native
                    ^
% Invalid input detected at '^' marker.

IOU1(config-vlan)#vlan 99
IOU1(config-vlan)#name native
IOU1(config-vlan)#vlan 100
IOU1(config-vlan)#name native1
IOU1(config-vlan)#vlan 101
IOU1(config-vlan)#name native2
IOU1(config-vlan)#
```

Figure 3: Création des VLANs.

```
IOU2(config)#vtp mode client
Device mode already VTP Client for VLANS.
IOU2(config)#vtp password cisco
Password already set to cisco
IOU2(config)#vtp domain campusvtp
Domain name already set to campusvtp.
IOU2(config)#vtp version 2
```

Figure 4:Configuration VTP client.

```
IOU2(config-if)#interface ethernet 0/0
IOU2(config-if)#switchport mode access
IOU2(config-if)#switchport access vlan 2
IOU2(config-if)#exit
IOU2(config)#interface ethernet 0/1
IOU2(config-if)#switchport mode access
IOU2(config-if)#switchport access vlan 3
IOU2(config-if)#interface ethernet 0/2
IOU2(config-if)#switchport mode access
IOU2(config-if)#switchport access vlan
% Incomplete command.

IOU2(config-if)#switchport access vlan 4
IOU2(config-if)#
```

Figure 5: Attribution des ports aux VLANs.

Résumé

De nos jours, garantir la sécurité informatique est essentiel pour le bon fonctionnement des réseaux. Les administrateurs réseau jouent un rôle clé dans l'implémentation de diverses méthodes et mécanismes afin d'atteindre les objectifs de sécurité.

Notre projet vise à implémenter une solution d'authentification pour le réseau Ethernet. Pour ce faire, nous avons opté pour le protocole Radius, l'un des protocoles d'authentification les plus performants.

Dans le cadre de notre projet, nous avons débuté par une révision des concepts fondamentaux des réseaux et de la sécurité informatique. Ce qui nous a permis de mieux appréhender les fondements nécessaires pour aborder notre problématique. Afin d'implémenter notre solution, notre choix s'est porté sur Windows Server 2022. Ce système d'exploitation intègre un serveur d'authentification Radius ainsi qu'une base de données Active Directory, offrant ainsi une infrastructure robuste pour la gestion des comptes utilisateurs et les accès au réseau.

Mots clés : authentification, Ethernet, Radius, Windows Server 2022, Active Directory.

Abstract

Nowadays, ensuring IT security is essential for the proper functioning of networks. Network administrators play a key role in implementing various methods and mechanisms to achieve security objectives.

Our project aims to implement an authentication solution for the Ethernet network. To do this, we have opted for the Radius protocol, one of the most powerful authentication protocols.

As part of our project, we started with a review of the fundamental concepts of networking and IT security. This allowed us to better understand the foundations necessary to address our problem. In order to implement our solution, we chose Windows Server 2022. This operating system integrates a Radius authentication server and an Active Directory database, providing a robust infrastructure for user account management and network access.

Keywords: authentication, Ethernet, Radius, Windows Server 2022, Active Directory.