République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin d'études

En vue d'obtention du diplôme de Master en Informatique
Spécialité : Réseaux et Sécurité

Thème

Mise en place de la norme 802.1X sur un réseau filaire en jonction avec radius-certificate

Stage au niveau : Campus NTS-Bejaia

Réalisé par :

SABRACHOU Numidia et SAIDI Serine

Evalué le 26/06/2023 devant le jury composé de :

Président	**Dr SADI Mustapha**	**U. A/Mira Béjaia**
Examinateur	**Dr OUZEGGANE Redouane**	**U. A/Mira Béjaia**
Encadrant	**Dr KABYL kamal**	**U. A/Mira Béjaia**

Année universitaire 2022/2023

Remerciements

Avant tout, il semble approprié d'entamer ce mémoire par Des remerciements, d'abord au bon dieu de nous avoir accordé la force et le courage de mener à terme ce travail.

Un grand merci à l'organisme d'accueil CAMPUS NTS, qui nous a acceptées comme stagiaires et qui nous a donné l'opportunité de découvrir le domaine professionnel.

Nous tenons à remercier vivement M.KABYL Kamal, pour nous avoir honorés par son encadrement, pour sa disponibilité, ses orientations, ses précieux conseils et ses encouragements qui nous ont permis de mener à bien ce

travail.

Nos remerciements vont pareillement aux membres du jury pour avoir accepté d'examiner et de juger notre travail.

Nous remercions toute l'équipe pédagogique du département d'informatique de l'université

ABDERRAHMANE MIRA.

Que tous ceux qui, de près ou de loin ont contribué, par leurs conseils, leurs encouragements ou leur amitié à l'aboutissement de ce mémoire, trouvent ici l'expression de

notre profonde reconnaissance.

Enfin, nous remercions infiniment nos parents et nos frères et sœurs d'avoir toujours été présents à nos côtés. Et nous-mêmes davoir été courageuses, patientes et déterminées tout au long de ce parcours.

Dédicaces

Je dédie ce travail aux personnes qui nous sont les plus chères :

A ma chère mère qui nous a quitté trop tot,cette dédicace est pour toi, ma mère, en signe de mon amour éternel et de ma gratitude infinie. Que ton âme repose en paix.

A mon cher père,tu as été constamment présent à mes côtés, me soutenant et m'encourageant à poursuivre mes aspirations.

A ma belle mère.

A ma chère soeur,Tina.

A mes chers freres, Mouloud,Mazigh,Ghiles et Islem.

A ma belle-soeur,Meriem.

A mes grands parents.

A mes meilleures amies,Mouamina et Imene.

A ma binome et ma copine Serine et sa famille.

Numidia

Dédicaces

Je dédie ce travail :

À la femme de ma vie, ma plus belle étoile dans l'univers, mon modèle inégalé, mon soutien inconditionnel, ma source de bonheur et de réconfort. En signe d'amour et de reconnaissance pour tout le soutien et les sacrifices dont elle a fait preuve à mon égard. À celle qui n'a jamais cessé de mencourager et de se sacrifier pour que je puisse franchir tous les obstacles tout au long de ma vie.

Que Dieu te garde pour nous, maman.

À l'homme de ma vie, mon exemple étendu, mon soutien moral et ma source de joie et de bonheur. A celui qui s'est toujours sacrifier pour me voir réussir, qui

éclair mon chemin et m'illumine de douceur et d'amour.

Que dieu te garde pour nous, papa.

À mes chers frères ,Iles ,et Karim, ainsi qu'à ma sœur Nouara , qui ont toujours été là pour moi, partageant des moments précieux et étant mes complices et confidents. Leur soutien inébranlable et leur présence réconfortante

sont des trésors inestimables.

Que notre lien fraternel continue de grandir et de s'épanouir.

À mes chères copines, Numidia,Dalia,Farah et Anaïs celles qui ont illuminé ma vie de rires, de complicité et de précieux souvenirs.

Que notre amitié perdure a jamais.

Merci d'être toujours là pour moi.

Serine

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AAA	Authentication Authorization Accounting.
AD	Active Directory .
CHAP	Challenge Handshake Authentification Protocol.
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name Server.
EAP	Extensible Authentication Protocol.
GNS3	Graphical Network System 3.
GPO	Group Policy Object.
GTC	Generic Token Card .
ID	Identifiant.
IP	Internet Protocol.
LAN	Local Area Network.
NPS	Network Policy Server.
NAS	Network Access Server.
NAT	Network Address Translation
PPP	Point to Point Protocol
PEAP	Protected Extensible Authentication Protocol.
RADIUS	Remote Access Dial In User Service.
SSH	Secure shell.
SHA-1	Secure Hash Algorithm 1.
SHA-2	Secure Hash Algorithm 2.
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network.
VPN	Virtuel Private Network.
VTP	Understand VLAN Trunk Protocol.
VTY	Virtual Terminal.
WAN	Wide Area Network.

Introduction générale

La sécurité des entreprises est une préoccupation majeure dans le monde numérique d'aujourd'hui. Les attaques informatiques sont devenues de plus en plus sophistiquées, mettant en péril la confidentialité, l'intégrité et la disponibilité des données et des systèmes d'information. Les entreprises sont confrontées à divers types de menaces, tels que l'usurpation d'identité, l'accès non autorisé, l'interception de données sensibles et bien d'autres.

Face à ces défis, il est crucial pour les entreprises de mettre en place des mesures de sécurité pour protéger leurs réseaux et leurs ressources. C'est dans ce cadre que nous avons été accueillies à Campus NTS pour mettre en œuvre une mise en place de la norme 802.1X sur un réseau filaire qui capte n'importe quel service demandé et n'autorise le passage de ces services que si la personne répond aux critères de sécurité demandé. Ces besoins dépassent aujourd'hui la logique d'un pare feu classique Pour ce faire nous avons opté pour l'utilisation de la norme 802.1X en conjonction avec le protocole RADIUS et l'utilisation de certificats numériques. En utilisant GNS3, VMware et Windows10.

Cette mise en place permet de contrôler l'accès aux réseaux filaires en vérifiant l'identité des utilisateurs et des périphériques avant de les autoriser à se connecter. Elle fournit un mécanisme de port d'accès contrôlé (Port-Based Network Access Control) qui nécessite une authentification préalable avant d'autoriser la communication avec un port réseau. Donc avec cette solution les entreprises peuvent renforcer la sécurité de leurs réseaux filaires. Cela permet de prévenir les attaques telles que l'usurpation d'identité, l'accès non autorisé et l'interception de données sensibles. Les utilisateurs et les périphériques doivent fournir des informations d'identification valides et être authentifiés avant d'être autorisés à accéder au réseau.

Pour mener à bien notre projet nous avons d'abord procédé, dans notre premier chapitre à une brève présentation des concepts de base sur la sécurité des systèmes d'information. Le deuxième chapitre consiste à la présentation l'organisme d'accueil. Le troisieme chapitre présente la solution RADIUS et la norme 802.1X. Enfin dans le dernier chapitre nous avons réalisé la norme 802.1X en utilisant les services AD+DNS, DHCP, certificat et le serveur NPS.

Enfin, nous donnons une conclusion et quelques perspectives.

Chapitre 1

Quelques concepts de base sur la sécurité des systèmes d'information

1.1 Introduction

Dans ce chapitre nous allons présenter quelques concepts de base relatifs à la sécurité informatique et ses caractéristiques. par la suite on va définir et expliquer les différents types d'attaques qui peuvent y avoir lieu. En dérnier lieu nous allons aborder quelques mécanismes de sécurités à utiliser pour se protéger contre les attaques définies précédemment.

Définition de la sécurité des SI

La sécurité informatique fait référence à l'ensemble des mesures techniques, organisationnelles et humaines visant à protéger les systèmes informatiques, les réseaux, les données et les informations contre les menaces accidentelles ou attentionnelles. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des informations, ainsi que la continuité des activités[1].

1.2 Objectifs de la sécurité

Comme objectifs de la sécurité nous avons :

a) **Intégrité :** C'est le critère qui permet d'assurer que les informations sont exactes et complètes, et qu'elles n'ont pas été modifiées de manière non autorisée lors de leur transmission entre les entités[2].

b) **Confidentialité :** C'est la propriété qui permet de limiter la diffusion des données aux seules entités autorisées[2].

c) **Disponibilité :** Cet objectif s'agit d'assurer l'accessibilité des entités authentifiées du système d'information aux ressources de ce système au moment où elles en ont besoin[2].

d) **Authentification :** Doit permettre de vérifier l'identité d'une entité qui accède aux informations pour pouvoir assurer son authentification, ainsi seules les personnes autorisées auront accès aux ressources[2].

La figure 1.1 présente les différents objectifs de la sécurité.

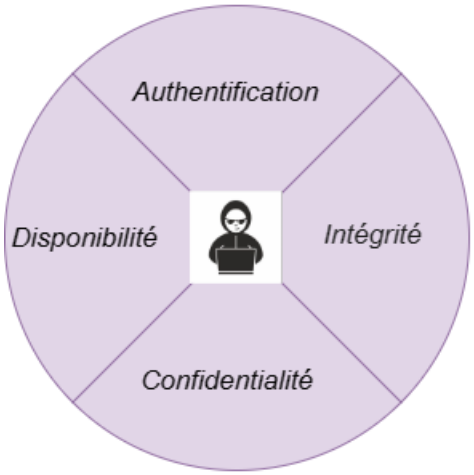


FIGURE 1.1 – Objectifs de la sécurité.

1.3 Services réseaux essentiels pour la sécurité

1.3.1 Service DHCP

Le protocole DHCP est conçu pour permettre à un ordinateur de se connecter à un réseau et d'obtenir automatiquement sa configuration réseau, sans faire appel à l'intervention de l'utilisateur. En spécifiant simplement l'utilisation du protocole DHCP, l'ordinateur peut obtenir une adresse IP sans efforts particuliers.

Le rôle principal du protocole DHCP est de distribuer des adresses IP sur un réseau, simplifiant ainsi l'attribution et la gestion des adresses pour les ordinateurs connectés.

Le fonctionnement du protocole DHCP repose sur l'échange de différents types de paquets entre le client et le serveur DHCP :

-DHCPDISCOVER : Dans ce cas le client envoie ce paquet pour localiser les serveurs DHCP disponibles sur le réseau.

-DHCPOFFER : Dans ce cas le serveur répond avec ce paquet contenant les premiers paramètres et une adresse IP proposée.

-DHCPREQUEST : Dans ce cas le client envoie cette requête pour valider l'adresse IP proposée par le serveur.

-DHCPACK : Dans ce cas le serveur envoie ce paquet pour confirmer l'attribution de l'adresse IP au client.[3]

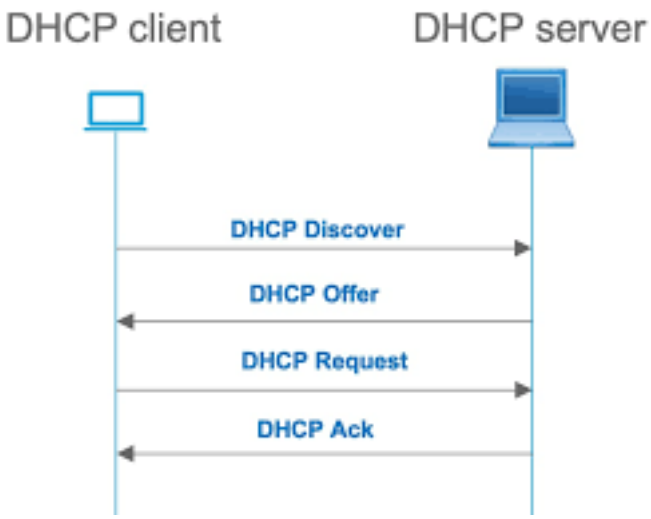


FIGURE 1.2 – Fonctionnement DHCP.

1.3.2 Service DNS

Le protocole DNS permet aux clients de réseau d'accéder à une base de données contenant des informations sur les machines et les services associés. Son rôle principal est de traduire les noms de domaine en adresses IP, agissant ainsi comme un répertoire téléphonique. Il facilite également l'obtention d'informations à partir d'un nom de domaine spécifique[4].

La figure 1.3 illustre le fonctionnement de DNS.

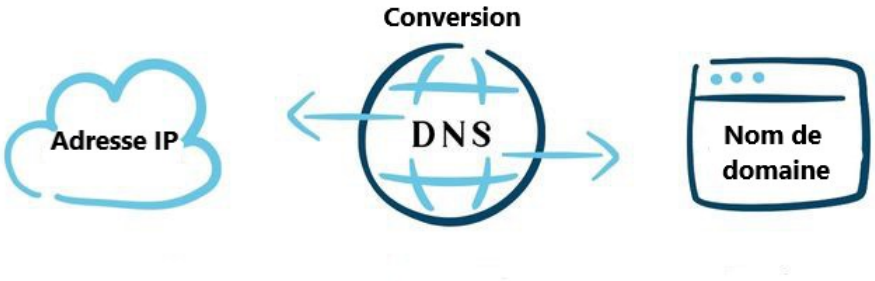


FIGURE 1.3 – Fonctionement de DNS.

1.3.3 Service RADIUS

Le protocole RADIUS est un service de communication entre un client (généralement un serveur d'accès à distance) et un serveur RADIUS. Il utilise le protocole UDP qui est un protocole réseau pour l'envoi de datagrammes non fiables et sans connexion pour la transmission des données.

Le serveur RADIUS est chargé de l'authentification des utilisateurs et de la fourniture des informations de configuration nécessaires au client pour offrir les services appropriés. Le protocole RADIUS fonctionne sans établir de connexion persistante et gère les problèmes de disponibilité du serveur et les délais d'attente. Il permet d'assurer l'authentification et l'autorisation des utilisateurs dans les réseaux en établissant une communication standardisée entre le client et le serveur RADIUS[5].

1.4 Virtual Local Area Network

Un VLAN (Virtual Local Area Network) Ethernet est un réseau local virtuel qui utilise Ethernet comme support. Son objectif principal est de regrouper des éléments du réseau tels que des utilisateurs, des périphériques, etc., en fonction de critères logiques tels que la fonction, le partage de ressources ou l'appartenance à un département. Contrairement aux contraintes physiques telles que le câblage inapproprié, un VLAN permet de rassembler ces éléments sans limitation liée à leur emplacement physique. Ainsi, les VLANs offrent une flexibilité et une adaptabilité accrues dans la gestion et la segmentation du réseau.

1.4.1 Avantages des VLANs

Les VLANs présentent plusieurs avantages, on peut citer :

a) **Flexibilité de la segmentation du réseau :** Possibilité de regrouper des utilisateurs et des ressources en fonction de leurs besoins de communication, indépendamment de leur emplacement physique.

b) **Simplification de la gestion du réseau :** Ajout ou déplacement rapide d'éléments sans manipulation des connexions physiques.

c) **Amélioration des performances du réseau :** Segmentation du trafic réseau et limitation des diffusions (broadcast).

d) **Utilisation plus efficace des serveurs réseau :** Possibilité pour un serveur d'appartenir à plusieurs VLAN simultanément, réduisant ainsi le trafic routé (trafic IP).

e) **Renforcement de la sécurité du réseau :** Les frontières virtuelles des VLANs ne peuvent être franchies que par le biais d'un routage, ce qui limite les accès non autorisés.

1.4.2 Méthodes d'implémentation des VLANs

Voici quelques-unes des méthodes d'implémentation couramment utilisées pour les VLANs dans un réseau :

a) **Par port (niveau 1) :** Les VLANs par port sont une méthode de configuration des VLANs de niveau 1 (physique) où chaque port du commutateur est associé à un VLAN spécifique. Cette approche est simple à mettre en œuvre et a été largement utilisée depuis l'apparition des commutateurs. Cependant, les VLANs par port manquent de souplesse car tout déplacement d'une station nécessite une reconfiguration des ports. De plus, toutes les stations connectées à un même port via un concentrateur appartiennent au même VLAN. La propagation des VLANs d'un commutateur à un autre reste une question à résoudre dans ce contexte.

b) **Par adresse MAC (niveau 2) :** Les VLANs par adresse physique sont des VLANs de niveau 2 où les adresses MAC des stations sont associées à chaque VLAN. Cette approche permet une indépendance de la localisation, ce qui signifie qu'une machine peut être déplacée sans avoir à reconfigurer le VLAN, car son adresse physique reste la même. Les VLANs configurables avec l'adresse MAC sont particulièrement adaptés à l'utilisation de stations portables. Cependant, la configuration peut être fastidieuse car elle nécessite une table de correspondance VLAN-MAC contenant toutes les adresses MAC des machines de l'entreprise, et cette table doit être partagée et propagée sur tous les commutateurs.

c) **Par protocole (niveau 3) :** Un VLAN par protocole, également appelé VLAN de niveau 3, est créé en associant un réseau virtuel à un type de protocole réseau spécifique, tels que TCP/IP, etc. Avec cette approche, on peut créer des réseaux virtuels distincts pour chaque protocole. Cependant, la configuration de ce type de VLAN repose sur l'apprentissage des commutateurs, ce qui peut entraîner une performance moins optimale car les commutateurs doivent analyser les trames pour identifier le protocole utilisé.

d) **Par sous réseau (niveau 3) :** Un VLAN par sous-réseau, également connu sous le nom de VLAN de niveau 3, utilise les adresses IP pour associer un réseau virtuel à chaque sous-réseau IP. Grâce à cette configuration, les commutateurs sont capables d'apprendre la configuration VLAN, ce qui permet de déplacer une station sans avoir à reconfigurer le VLAN. Cette solution présente de nombreux avantages, bien que l'analyse des informations puisse entraîner une légère dégradation des performances de commutation[17].

1.5 Notion de trunk

Un trunk est une connexion physique qui permet de transmettre le trafic de plusieurs réseaux virtuels. Les trames qui circulent à travers le trunk sont complétées avec un identificateur de réseau local virtuel (VLAN ID ou tag), ce qui permet de maintenir les

trames regroupées dans un même VLAN (ou domaine de diffusion) et de les acheminer vers un autre équipement. Les trunks peuvent être utilisés dans différentes configurations, notamment entre deux commutateurs pour la distribution des réseaux locaux, entre un commutateur et un hôte capable de supporter le trunking pour analyser le trafic de tous les VLANs, et entre un commutateur et un routeur pour permettre l'accès aux fonctions de routage et l'interconnexion des réseaux virtuels par le routage inter-VLAN[17].

1.6 VTP ou VLAN Trunking Protocol

VTP est un protocole Cisco qui permet la configuration et l'administration des VLANs sur les équipements. Il offre trois modes de propagation (client, server, transparent). Les modifications faites en mode server sont distribuées à l'ensemble du domaine VTP via les trunks. En mode transparent, les modifications restent locales. Les switches en mode client appliquent automatiquement les changements reçus si leur numéro de révision est plus élevé[17].

La figure 1.4 illustre le fonctionnement du protocole VTP.

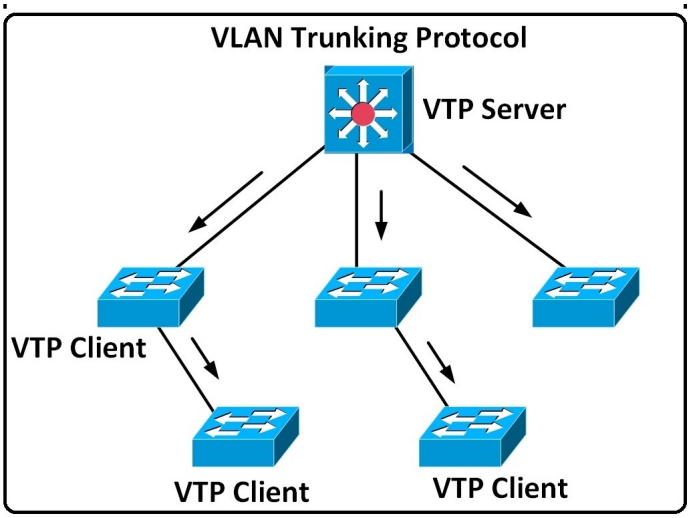


FIGURE 1.4 – Fonctionnement du protocole VTP.

1.7 Protocoles d'authentification

Les protocoles d'authentification jouent un rôle essentiel dans la sécurisation des communications réseau. Voici un aperçu des principaux protocoles, tels que PAP, CHAP, MS-CHAP, MS-CHAP-V2, GTC et TLS, qui offrent différents niveaux de sécurité et de fonctionnalités pour l'authentification des utilisateurs.

a) **PAP (PasswordAuthentication Protocol) :** Un protocole de négociation deux voies utilisé avec PPP, mais il n'est pas sécurisé.

b) **CHAP (Challenge Handshake Authentication Protocol) :** Un protocole de négociation trois voies considéré comme plus sûr que PAP.

c) **MS-CHAP (MD4) :** Une version Microsoft du protocole de négociation-réponse RSA Message Digest 4, utilisé uniquement sur les systèmes Microsoft et permet le chiffrement des données.

d) **MS-CHAP-V2 :** Une version améliorée de MS-CHAP qui permet la modification de mot de passe si nécessaire.

e) **GTC (Generic Token Card) :** Utilise des cartes à jetons pour l'authentification basée sur un certificat numérique. Il offre également une confidentialité supplémentaire en masquant les noms d'utilisateur pendant l'authentification.

f) **TLS (Transport Layer Security) :** Un protocole de sécurisation et d'authentification des communications sur les réseaux publics par le chiffrement des données. Ces protocoles offrent différentes méthodes d'authentification et de sécurité pour les communications réseau[18].

la figure 1.5 montre les différents Protocoles d'authentification.

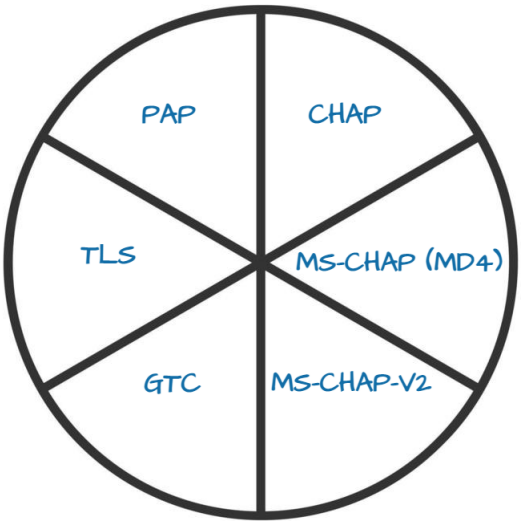


FIGURE 1.5 – Protocoles d'authentification.

1.8 Authentification réseau sécurisée

L'EAP (Extensible Authentication Protocol) est une méthode d'authentification avancée utilisée avec le protocole 802.1x pour assurer la sécurité des connexions réseau et garantir un accès sécurisé. D'autres méthodes d'authentification spécifiques peuvent également être utilisées pour renforcer la sécurité et protéger les connexions réseau.

1.8.1 Méthodes associées à EAP

a) **EAP-TLS (EAP Transport Layer Security) :** Est utilisé avec des cartes à puce ou des certificats, EAP-TLS peut être déployé en tant que méthode interne pour PEAP ou en tant que méthode EAP autonome.

b) **EAP-MD5 (EAP Message Digest 5-Challenge) :** L'utilisateur est authentifié à l'aide de son identifiant et de son mot de passe, mais ce dernier n'est pas transmis en clair sur le réseau. Le serveur envoie un défi au client, qui renvoie le mot de passe associé au défi. Le serveur compare le résultat avec le mot de passe stocké dans sa base de données, en tenant compte du défi. Si le résultat correspond, l'accès est autorisé, sinon il est refusé.

c) **LEAP (Lightweight EAP) :** Est une implémentation propriétaire d'EAP développée par Cisco Systems, qui permet une authentification simple par mot de passe via une encapsulation sécurisée. Cependant, ce protocole est vulnérable aux attaques, sauf si l'utilisateur utilise des mots de passe complexes.

d) **PEAP :** Est un protocole propriétaire développé par Microsoft, Cisco et RSA Security. Seul le serveur d'authentification possède un certificat numérique, qu'il transmet au client pour l'authentifier. Un tunnel sécurisé TLS est alors établi entre les deux parties. Le client s'authentifie via une encapsulation sécurisée. Toutefois, ce protocole est également vulnérable aux attaques, sauf si l'utilisateur utilise des mots de passe complexes.

e) **EAP-FAST (EAP-Flexible Authentication via Secure Tunneling) :** Une proposition de Cisco Systems visant à remédier aux faiblesses de LEAP en offrant une flexibilité d'authentification via une encapsulation sécurisée. Ces méthodes sont utilisées pour sécuriser les processus d'authentification dans les réseaux[19].

la figure 1.6 montre les différentes méthodes associées à EAP.

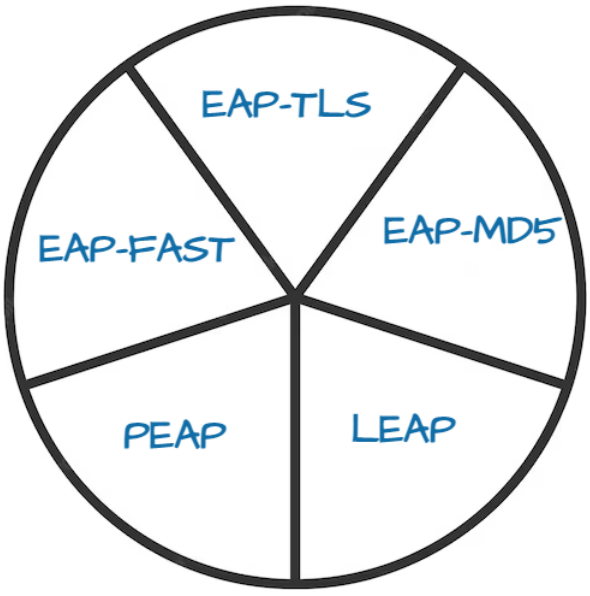


FIGURE 1.6 – Méthodes associées à EAP .

1.9 Active Directory

Active Directory est un service développé par Microsoft qui permet la gestion des identités et des accès. Principalement utilisé dans les environnements Windows, il centralise et administre les ressources réseau telles que les utilisateurs, les ordinateurs, les groupes et les politiques de sécurité.

Active Directory offre aux administrateurs un contrôle et une gestion de l'accès aux ressources du réseau, comme les fichiers, les imprimantes, les applications et les services. Il propose également des fonctionnalités de sécurité telles que l'authentification des utilisateurs, la gestion des autorisations et la mise en œuvre de stratégies de groupe.

Comme composants essentiels de l'Active Directory nous présentons :

a) **Annuaire :** Il s'agit de la base de données centrale qui stocke les informations sur les objets du réseau, tels que les utilisateurs, les ordinateurs, les groupes.

b) **Domaine :** Un domaine est une unité d'organisation logique dans Active Directory. Il regroupe un ensemble d'objets et fournit une frontière de sécurité pour l'administration.

c) **Contrôleur de domaine :** C'est un serveur qui exécute Active Directory et qui gère l'authentification des utilisateurs, la réplication des données et fournit les services d'annuaire aux clients.

d) **Stratégies de groupe :** Active Directory permet de définir des stratégies de groupe qui peuvent être appliquées aux utilisateurs et aux ordinateurs pour gérer leurs paramètres et leurs droits d'accès.

1.10 Menaces et vulnérabilités

Une menace est un événement ou une action qui pourrait causer une perte ou un dommage à un système informatique. Les menaces peuvent provenir d'attaquants malveillants tels

que des pirates informatiques, des virus ou des logiciels malveillants, mais aussi de facteurs naturels comme les catastrophes naturelles ou les pannes de courant.

Une vulnérabilité est une faille de sécurité le plus souvent cachée, touchant une infrastructure informatique. Ce terme est fréquemment associé aux logiciels mais il regroupe plus généralement toute faiblesse quelle qu'en soit la nature. Une erreur de configuration d'un équipement réseau constitue une vulnérabilité tout comme un mot de passe vide ou trivial.

1.10.1 Types de vulnérabilités des systèmes

—**Vulnérabilités humaines :** Négligence, manque de compétences.

—**Vulnérabilités de mise en œuvre :** Mauvaises configuration, mauvaise manipulation.

—**Vulnérabilités technologiques :** Hardware, logiciel et réseau, Mauvaise conception, erreur d'implémentation (Bugs).

—**Vulnérabilités organisationnelles :** Manque de documents formels, de procédures, de manuels de travail de validation et de maintenance suffisamment détaillés pour faire face aux problèmes de sécurité.

Il est important de comprendre les menaces et les vulnérabilités auxquelles un système informatique est exposé afin de mettre en place des mesures de sécurité appropriées pour les prévenir ou les atténuer[6].

1.10.2 Types d'attaques

Les informations ou les systèmes d'informations d'une entreprise peuvent subir des dommages de plusieurs façons : certains intentionnels (malveillants), d'autres par accident. Ces événements seront appelés des " attaques ".[9]

Les attaques peuvent se classer en deux catégories : celles qui visent à prendre connaissance d'informations soit pour les exploiter soit pour les altérer et celles qui visent à paralyser voire détruire les systèmes[7].

Il existe quatre catégories principales d'attaques :

—**L'accès :** Une attaque d'accès est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information.

—**La modification :** Une attaque de type " modification " consiste, pour un attaquant à tenter de modifier des informations. Ce type d'attaque est dirigé contre l'intégrité de l'information.

—**Le déni de service :** Les attaques par saturation sont des attaques informatiques qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes. Cette technique est assez simple à réaliser et jugée comme de la pure malveillance. Elle ne fait que bloquer l'accès aux sites, sans en altérer le contenu.

—**La répudiation :** La répudiation est une attaque contre la responsabilité. Autrement dit, la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soient réellement passé.

Comme buts des attaques nous avons [8] :

—**Interruption :** Vise la disponibilité des informations.

—**Interception :** Vise la confidentialité des informations.

—**Modification :** Vise l'intégrité des informations.

—**Fabrication :** Vise l'authenticité des informations.

1.10.3 Mécanismes de défense

Parmis les mécanismes de défense on cite :

a) **Signature numérique :** La signature numérique est un mécanisme permettant d'authentifier l'auteur d'un message électronique autrement dit de prouver qu'un message provient bien d'un expéditeur donné, à l'instar d'une signature sur un document papier. Son principe est par exemple que A veut signer numériquement un message destiné à B. Pour ce faire, A utilise sa clé privée pour chiffrer le message, puis il envoie le message accompagné de sa clé publique, étant donné que la clé publique de A est la seule clé qui puisse déchiffrer ce message, le déchiffrement constitue une vérification de signature numérique[9].

b) **Certificats :** Ce sont des structures de données qui sont numériquement signées par une autorité de certification (CA : Certificate authority) en qui les utilisateurs peuvent faire confiance. Ils contiennent une série de valeurs, comme le nom du certificat et son utilisation, des informations identifiant le propriétaire et la clé publique ainsi que la clé publique elle même, la date d'expiration et le nom de l'organisme du certificat. La CA utilise sa clé privée pour signer le certificat. Si le récepteur connait la clé publique du CA, il peut vérifier que le certificat provient vraiment de l'autorité concernée et assurée que le certificat contient une clé publique valide[10].

c) **Cartes à puces :** Une carte à puce est un petit dispositif électronique de la taille d'une carte de crédit. Elle est utilisée pour stocker et traiter des informations numériques, telles que des identifiants de compte, des clés d'authentification et des données personnelles. La carte à puce contient une puce intégrée qui peut communiquer avec un lecteur de carte à puce. La communication entre la carte et le lecteur est sécurisée et nécessite une authentification pour accéder aux informations stockées sur la carte. Les cartes à puce sont utilisées dans de nombreux domaines, tels que les systèmes de paiement électronique, les identités numériques, la santé électronique, le contrôle d'accès et la sécurité informatique en général.

1.11 Sécurité renforcée

Pour renforcer la sécurité on utilise :

1.11.1 VPN

Un VPN est un réseau privé virtuel, qui est une extension d'un réseau privé (intranet) sur un réseau public (internet). Le VPN établit un réseau privé virtuel en chiffrant les données échangées entre deux points distants. Une fois que le tunnel est créé à travers le réseau public (Internet) entre deux machines ou réseaux, ces derniers peuvent communiquer de manière sécurisée, comme s'ils étaient sur le même réseau local. Les VPN permettent aux entreprises de bénéficier d'une connexion sécurisée à moindre coût. Ils peuvent également utiliser des lignes spécialisées pour créer le VPN[20].

1.11.2 Pare-Feu

Un pare-feu (firewall en anglais) est un logiciel ou un matériel qui assure le respect de la politique de sécurité du réseau en déterminant les types de communications autorisées sur ce réseau informatique. Il effectue la prévention des applications et des paquets. Sa principale fonction consiste à contrôler le trafic entre différentes zones en filtrant les flux de données entrants et sortants, dans le but de fournir une connectivité contrôlée et maîtrisée entre ces différentes zones.

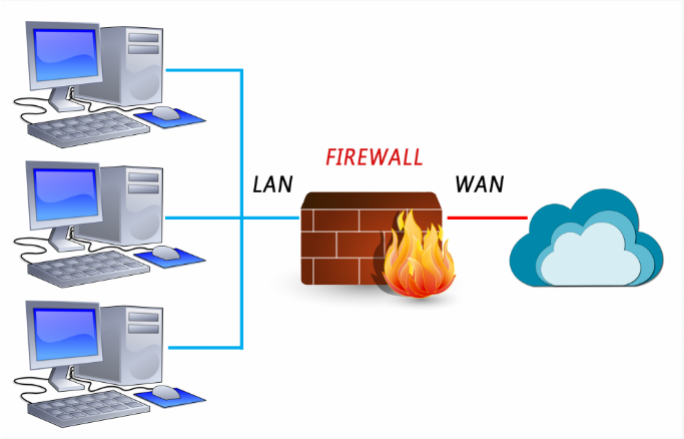


FIGURE 1.7 – Pare-Feu.

1.12 Conclusion

Ce chapitre est consacré à la présentation des concepts fondamentaux de la sécurité informatique y compris les mécanismes de protections. Ces éléments nous permettent d'analyser notre sujet en profondeur.

Chapitre 2

Présentation de l'organisme d'accueil

2.1 Introduction

Ce chapitre sera réservé à la présentation du campus NTS (New Technology § Solutions) où nous effectuons notre stage. Dans un premier temps, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Nous étudierons ensuite l'architecteur réseau de cette entreprise et ses composantes afin de pouvoir suggérer d'éventuelles améliorations.

2.2 Présentions de l'entreprise ■ Campus NTS ■

2.2.1 Création et évolution

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

Air Algérie, Retelem Alger, Poste d'Algérie, Adèle, RATP ALJAZAIR, la technologie, Morsi, Université de Bejaïa, Cité universitaire à Bejaïa (targaouzamour, 17 octobre...etc), SARL Alphas Bejaïa, Providentia Béjaïa.

2.2.2 Situation géographique

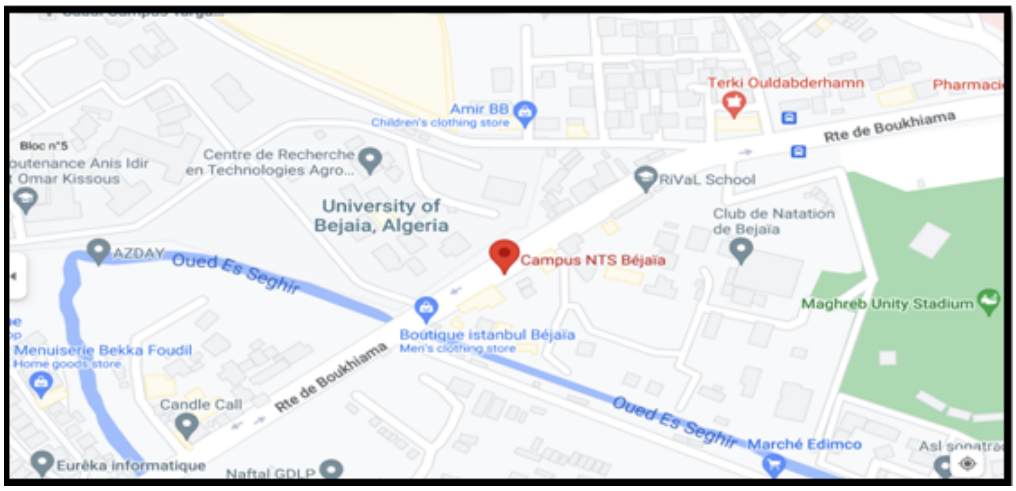


FIGURE 2.1 – Situation géographique.

2.2.3 Fiche technique

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

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

TABLE 2.1 – Identification sur campus NTS.

2.2.4 Objectifs, Missions et activités de l'Entreprise ■ N.T.S ■

Les objectifs, les missions et les activités sont représentées dans la figure 2.2 :

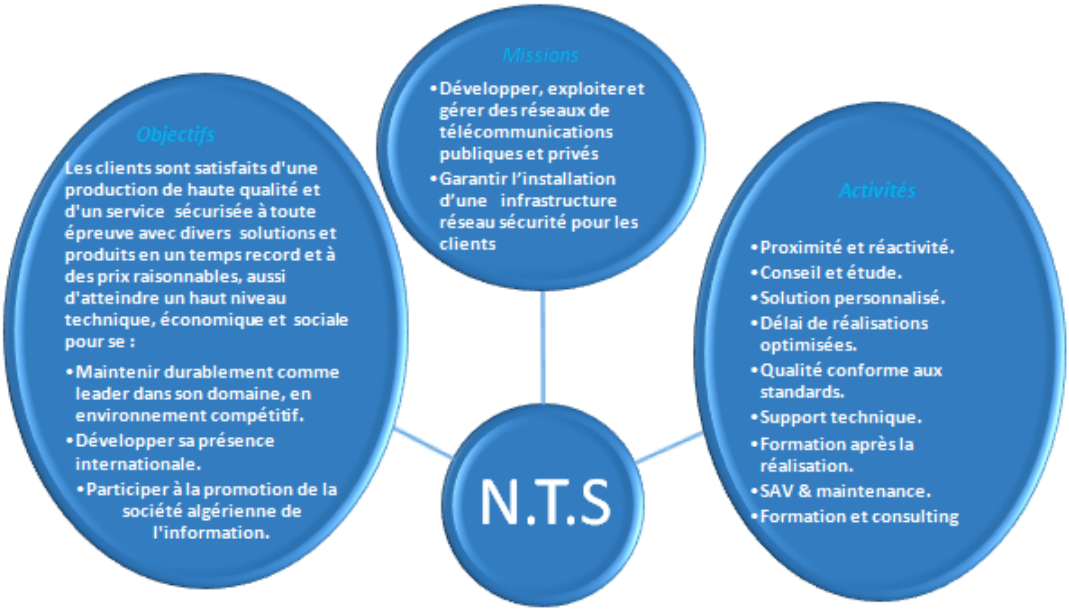


FIGURE 2.2 – Objectifs, Missions et Activités de l'NTS.

2.2.5 Organigramme général de l'organisme d'accueil

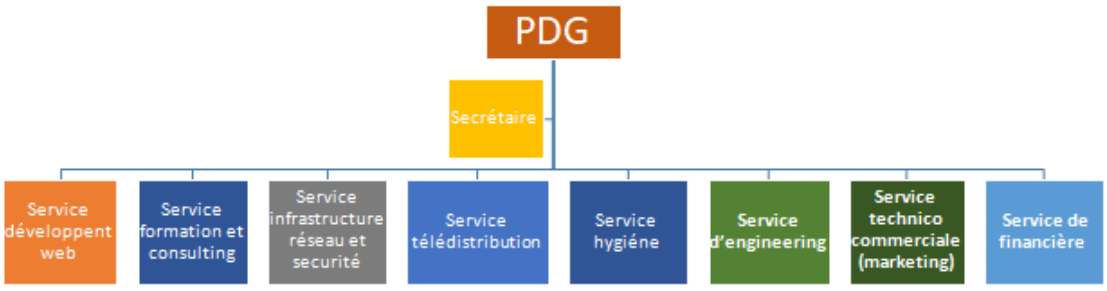


FIGURE 2.3 – Organigramme de campus NTS.

Nous allons nous contenter de présenter ci- dessous la description de l'organigramme du campus NTS (voir la figure 2.3) dans lequel cet apprentissage termine le stage :

1. **Service développement web** Il est responsable de la création des sites web, des applications pour internet, applications mobiles ou des solutions logicielles adaptées aux besoins des clients utilisant des langages de programmation informatique tels

que : HTML5, CSS, JavaScript ou PHP. En général, il représente les tâches liées au développement du site Web en améliorant son positionnement sur les moteurs de recherche qui seront hébergés sur Internet.

2. **Service formation et consulting** Ce secteur a été créé par le campus NTS pour offrir des stages et des formations professionnelles dans les domaines suivants :
   - Installation et configuration des réseaux informatiques.
   - Administration et sécurité des réseaux et système.
   - Installation et configuration des firewalls (pfsense, Sophos, fortigate, palo alto...).
   - Installation et configuration des réseaux sans fil professionnel.
   - Installation et configuration des caméras de surveillance analogique et numérique.
   - Fibre optique les réseaux d'accès FTTH/FTTX.
   - Création des sites web.
   - Electricités Bâtiments et industriels.
   - Virtualisation.
   - Microsoft server, SQL.
   - Cyber sécurité.

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

3. **Service d'accueil**

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

   L'infrastructure réseau est au cœur des opérations commerciales dans la plupart des industries. Il peut être considéré comme le centre sensible de toute l'organisation

informatique car il centralise les données, simplifie les échanges de données et facilite la communication entre les employés. A ce titre, il est un outil important pour le fonctionnement normal de l'entreprise et nécessite une attention constante en matière de sécurité. Ceci afin d'empêcher le nombre croissant et l'affectation des attaques externes et internes.

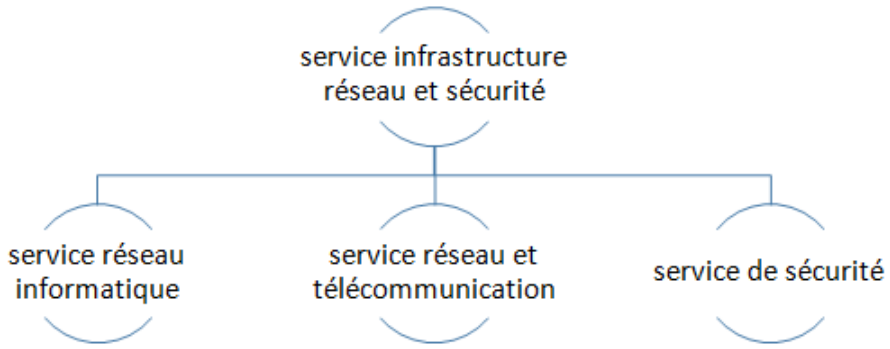


FIGURE 2.4 – Organigramme de service d'accueil.

➞**Service réseau informatique :** Ce service représente tous les appareils et périphériques au sein d'une entreprise qui sont physiquement ou virtuellement connectés les uns aux autres à partir d'un wifi professionnel ou d'autre méthodes afin de partager des ressources ou des informations. En fait, l'infrastructure réseau offre un large éventail de fonctionnalités pour les clients de services et les producteurs de services, telles que : Limitation de débit, analyse, vérification, surveillance et enregistrement et sécurisation du réseau de cette entreprise.

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

- Pose de fibre optique.

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

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

Les services qu'elle réalise sont les suivants :

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

4. **Service télédistribution** Ce service est spécialisé dans la transmission de données par câble (fibre optique, paire torsadée et onde horizontale) ou autres systèmes de distribution (paraboles collectif, télévision numériques terrestre et audiovisuelle). Son objectif principal est de garantir l'installation de ces supports de transmission à haut débit. Enfin, les services de télédistribution ont été appelés à jouer un rôle majeur dans l'émergence des nouveaux médias tel que :
   - •Rediffusion de programmation par satellite.
   - •Transmission de chaînes de télévision par abonnement.
   - •Services interactifs.
   - •Programmation locale.
5. **Service d'engineering :** Il est constitué d'une équipe multidisciplinaire d'experts dont la mission est de rechercher et d'analyser les besoins des clients pour trouver la meilleure solution spécifique à leur projet.

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

survenir auparavant. Cette équipe est composée :

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

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

6. **Service technico commerciale (marketing) :** Leurs offres ne se limitent pas à de simples fournitures standards. Ils disposent d'une équipe qui s'assure de répondre aux besoins et au confort de ses précieux clients dans le but de développer les services de cette entreprise. Par ailleurs, ce service commercialise aussi les services proposés par campus NTS.
7. **Service financier :** Le service financier situé au cœur de l'entreprise, représente l'ensemble des personnes chargées de la fonction comptable. Il intervient pour faire de bons investissements en prévenant d'éventuels risques de perte. Ce service contient un ensemble de tâches et rôles au sein de la société NTS :

→Les tâches principales du Service des finances :

•Assurer une saine gestion des ressources financières de l'entreprise par la planification.

•La coordination et le contrôle de toutes les politiques et procédures requises pour la protection des actifs.

•La production des informations financières exactes et pertinentes afin que le gestionnaire puisse prendre la décision éclairée.

→Le rôle du service financier :

•préparation et du suivi des budgets de fonctionnement et d'investissement.

•La préparation des états financiers.

•La gestion de la trésorerie et de des encaissements.

•rémunération des employés, des comptes à payer.

•De l'acquisition des biens et services pour l'ensemble de l'entreprise, des projets de recherche.

•La réception des marchandises et du courrier.

8. **Service hygiène :**

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

• Des actions de prévention des risques professionnels et de la pénibilité au travail.

• La mise en place d'une organisation et de moyens adaptés.

2.3 Conclusion

Ce chapitre nous a permis de présenter l'organisme d'accueil de campus NTS. L'étude de l'existant nous a permis de nous familiariser avec le réseau actuel de campus NTS, et de comprendre son fonctionnement.

Chapitre 3

Solution Radius et la norme 802.1X

3.1 Introduction

L'objectif de ce chapitre est de présenter le protocole RADIUS, ses composants avec leurs caractéristiques, suivi de la définition du protocole 802.1x et de ses fonctionnalités pour l'accès aux réseaux.

3.2 Protocole RADIUS

Le protocole RADIUS (Remote Authentication Dial-In User Service) a été développé en 1991 par Livingston Entreprises. C'est un protocole client-serveur largement utilisé pour la gestion centralisée de l'authentification, de l'autorisation et de la comptabilité (AAA) pour les connexions réseau. Il permet également la gestion de comptes d'utilisateurs distants, tels que l'ajout, la suppression et la modification des comptes d'utilisateurs. Selon RFC 2865, qui définit le protocole RADIUS, il est utilisé pour transporter les informations d'authentification pour les connexions de service d'accès distant, ainsi que pour les connexions de service de communication électronique à travers une passerelle d'accès. Le protocole RADIUS permet de vérifier les informations d'identification des utilisateurs auprès d'un serveur centralisé plutôt que de stocker ces informations localement sur chaque périphérique[11].

3.2.1 Fonctionnement du protocole RADIUS

Le protocole RADIUS fonctionne selon un modèle client/serveur, dans lequel les serveurs d'accès au réseau, tels que les points d'accès sans fil ou les passerelles VPN, agissent en tant que clients et envoient des demandes d'authentification à un serveur RADIUS centralisé. Le serveur RADIUS contient les informations d'authentification des utilisateurs, ainsi que les autorisations qui leur sont accordées. RADIUS utilise le modèle AAA (Authentification, Autorisation et Comptabilisation) pour offrir un accès sécurisé aux réseaux. En dautres termes, RADIUS est un protocole qui s'appuie sur le modèle AAA

pour authentifier les utilisateurs, autoriser leur accès et enregistrer leurs activités.

- **Authentification :** Lorsqu'un utilisateur tente de se connecter au réseau, son nom d'utilisateur et son mot de passe sont envoyés au serveur RADIUS pour authentification.
- **Autorisation :** Si l'authentification est réussie, le serveur RADIUS envoie une réponse au client contenant les informations d'autorisation pour l'utilisateur, telles que les droits d'accès au réseau.
- **Comptabilisation :** Pendant la session, le serveur RADIUS peut également envoyer des messages de comptabilisation pour enregistrer les détails de l'utilisation du réseau par l'utilisateur, tels que la durée de la session et la quantité de données transférées.

  Il convient de noter que le protocole RADIUS est souvent utilisé en combinaison avec d'autres protocoles, tels que le protocole 802.1X pour le contrôle d'accès au réseau ou le protocole de chiffrement EAP (Extensible Authentication Protocol) pour sécuriser les échanges d'informations d'identification. Le protocole RADIUS fonctionne selon le scénario suivant : un utilisateur envoie une demande de connexion à distance au NAS, qui transfère cette demande au serveur RADIUS. Le serveur RADIUS vérifie l'identité de l'utilisateur en consultant une base de données d'identification pour connaître le type de scénario d'authentification requis. Le serveur RADIUS renvoie une des quatre réponses suivantes : ACCEPT, REJECT, CHALLENGE, ou CHANGE PASSWORD. Après l'authentification réussie, une phase d'autorisation commence où le serveur RADIUS retourne les autorisations aux utilisateurs[12].

  La figure 3.1 montre le fonctionnement du protocole RADIUS.

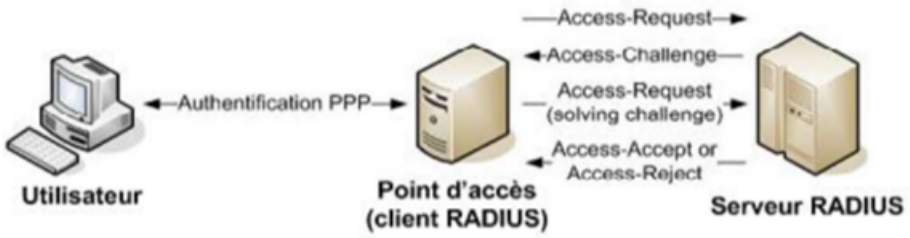


FIGURE 3.1 – Fonctionnement du protocole RADIUS.

3.2.2 Format de l'entête du paquet RADIUS

Le protocole RADIUS utilise des paquets pour communiquer entre les clients RADIUS et les serveurs RADIUS. Chaque paquet RADIUS est composé d'un en-tête et d'attributs. L'en-tête du paquet RADIUS est composé des cinq champs suivants.

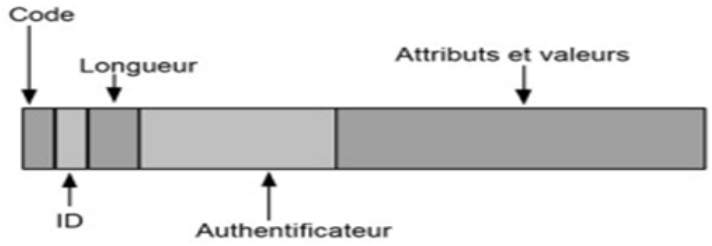


FIGURE 3.2 – Entête du paquet RADIUS.

— **Code :** Ce champ indique le type de paquet RADIUS et est codé sur un octet. Il peut prendre l'une des valeurs suivantes :

- **Access-Request**
- **Access-Accept**
- **Access-Reject**
- **Access-Challenge**

— **Identifiant :** Ce champ, qui ne fait qu'un octet, permet au client Radius d'associer les requêtes et les réponses en contenant une valeur spécifique pour chaque paquet émis.

— **Longueur :** Champ de seize octets contenant la longueur totale du paquet.

— **Authentificateur :** Ce champ est un champ de 16 octets utilisé pour l'authentification et pour vérifier l'intégrité des paquets RADIUS. On distingue : l'authentificateur de requête et l'authentificateur de réponse.

— **Attributs et valeurs :** Ce champ du paquet est de longueur variable et contient la charge utile du protocole, c'est-à-dire les attributs et leur valeur qui seront envoyés soit par le NAS en requête, soit par le serveur en réponse[13].

3.2.3 Elément d'authentification RADIUS

a) **Authentification RADIUS par identifiant et mot de passe :** Ce type d'authentification repose sur l'utilisation d'un identifiant et d'un mot de passe pour vérifier l'authenticité de l'utilisateur. Le serveur RADIUS interroge une base de données pour valider les informations fournies par l'utilisateur. Cependant, pour des raisons de sécurité, il est recommandé de ne pas stocker les mots de passe en clair dans la base de données. Des protocoles comme EAP/PEAP ou EAP/TTLS peuvent être utilisés pour résoudre ce problème.

b) **Authentification par certificat électronique X509 :** Ce type d'authentification nécessite la présentation d'un certificat électronique par le client. Ce certificat peut être celui de l'utilisateur ou celui de la machine à laquelle il est connecté. Le serveur RADIUS vérifie ensuite la validité du certificat présenté en s'appuyant sur une Infrastructure for Key Management (IGC ou PKI). L'authentification par certificat est considérée comme plus sécurisée que l'authentification par mot de passe.

c) **Authentification avec l'adresse Ethernet (adresse MAC) :** L'authentification basée sur l'adresse MAC repose sur l'utilisation de l'adresse MAC de l'appareil comme nom d'utilisateur et mot de passe pour l'authentification. Lorsque l'adresse MAC est stockée dans la base de données du serveur RADIUS et que les configurations sont effectuées sur le contrôleur, l'appareil peut accéder à Internet sans avoir à saisir de nom d'utilisateur et de mot de passe. Les appareils dont les adresses MAC ne sont pas dans la base de données seront refusés. Cette méthode d'authentification est utile pour les appareils qui ne disposent pas d'une interface utilisateur pour entrer des informations d'identification[14].

3.2.4 Rôle du protocole RADIUS

Le rôle principal du protocole RADIUS est de permettre l'authentification centralisée des utilisateurs ou des équipements réseau souhaitant accéder à un réseau. Il fonctionne selon un modèle client-serveur, où le client RADIUS (par exemple un routeur ou un

commutateur) envoie une demande d'authentification au serveur RADIUS. Le serveur RADIUS vérifie ensuite l'identité de l'utilisateur ou de l'équipement en comparant les informations d'identification fournies avec celles stockées dans sa base de données d'authentification. En plus de l'authentification, le protocole RADIUS peut également être utilisé pour l'autorisation d'accès réseau, où le serveur RADIUS peut fournir des informations de configuration spécifiques à l'utilisateur ou à l'équipement pour réguler l'accès et le comportement dans le réseau. Il peut également être utilisé pour la comptabilité, où le serveur RADIUS enregistre les informations de connexion et de déconnexion de l'utilisateur ou de l'équipement, ce qui permet aux administrateurs de superviser et de contrôler l'utilisation du réseau. En résumé, le protocole RADIUS joue un rôle crucial dans la gestion d'authentification et d'autorisation d'accès réseau en permettant l'authentification centralisée, l'autorisation d'accès et la comptabilité. Cela permet aux administrateurs de contrôler efficacement l'accès au réseau et d'assurer la sécurité des données et des ressources[11].

3.2.5 Avantages du protocoles RADIUS

Le protocole RADIUS présente plusieurs avantages, notamment :

1. Centralisation de l'authentification : Le protocole RADIUS permet d'authentifier les utilisateurs ou les équipements de manière centralisée, ce qui facilite la gestion de l'accès au réseau et assure une plus grande sécurité.

2. Flexibilité : Le protocole RADIUS est compatible avec différents types d'équipements réseau, ce qui le rend facilement adaptable aux besoins de diverses organisations.

3. Gestion de l'autorisation d'accès : En plus de l'authentification, le protocole RADIUS permet de réguler l'accès des utilisateurs et des équipements au réseau, en fournissant des informations de configuration spécifiques à chaque utilisateur ou équipement.

4. Comptabilité : Le protocole RADIUS permet également l'enregistrement des informations de connexion et de déconnexion des utilisateurs ou des équipements, ce qui facilite la supervision et le contrôle de l'utilisation du réseau.

5. Sécurité : Le protocole RADIUS utilise des méthodes de chiffrement pour assurer la sécurité des informations d'identification des utilisateurs lors des échanges entre le client RADIUS et le serveur RADIUS.

6. Authentification forte : Le protocole RADIUS permet l'utilisation de méthodes d'authentification forte, telles que les certificats numériques, pour renforcer la sécurité de l'authentification.

7. Redondance : Le protocole RADIUS permet la mise en place de serveurs RADIUS redondants pour assurer la continuité de service en cas de panne d'un serveur.

En résumé, le protocole RADIUS est une solution flexible, évolutive et sécurisée pour l'authentification et la gestion de l'accès au réseau, adaptée aux besoins des grandes organisations[11].

3.3 Protocole 802.1X

Le protocole 802.1X est un standard de sécurité réseau établi par l'IEEE en 2001, appartenant au groupe des protocoles IEEE 802.1. Il permet l'authentification des utilisateurs qui cherchent à accéder à un réseau câblé ou sans fil via un serveur central d'authentification. Aussi connu sous le nom de "Port-based Network Access Control" ou "User Based Access Control", 802.1X renforce la sécurité d'accès à la couche 2 (liaison de données) du réseau.

Avec 802.1X, tous les utilisateurs, internes ou externes, doivent s'authentifier avant de pouvoir accéder au réseau. Si un utilisateur ne parvient pas à s'authentifier, certains équipements réseau compatibles avec 802.1X peuvent les placer dans un VLAN "guest" qui les isole du reste du réseau.

802.1X utilise le protocole EAP (Extensible Authentication Protocol) pour le transport de différentes méthodes d'authentification dans les réseaux câblés ou sans fil. Pour fonctionner, 802.1X requiert la présence d'un serveur d'authentification tel qu'un serveur RADIUS (Microsoft, Cisco, FreeRADIUS) ou un serveur TACACS (dans le monde des

équipements Cisco).
Un port sur un commutateur en mode 802.1X peut être dans deux états : ”contrôlé” si l'authentification auprès du serveur RADIUS est réussie, ou ”non contrôlé” si elle a échoué.
Le succès ou l'échec de l'authentification détermine si le port est ouvert ou fermé à la communication. Par exemple, un port ouvert permet à un client final d'obtenir une adresse IP auprès d'un serveur DHCP. Dans certaines implémentations, le serveur RADIUS peut indiquer le VLAN dans lequel placer le client final[15].

3.3.1 Fonctionnement et compatibilité :

Le protocole 802.1X est un standard de sécurité réseau utilisé pour authentifier les utilisateurs qui souhaitent accéder à un réseau câblé ou sans fil. Il fonctionne en exigeant que les utilisateurs s'authentifient avant d'être autorisés à accéder au réseau. Voici comment le protocole 802.1X fonctionne :

1. Lorsqu'un utilisateur se connecte à un port de commutateur configuré en mode 802.1X, le port est considéré comme ”non contrôlé” jusqu'à ce que l'utilisateur s'authentifie via un serveur d'authentification, généralement un serveur RADIUS.

2. Si l'authentification réussit, le port est considéré comme ”contrôlé” et l'utilisateur peut accéder au réseau.

3. Si l'authentification échoue, le port reste ”non contrôlé” et l'utilisateur n'a pas accès au réseau.

Le protocole 802.1X utilise le protocole EAP pour transporter différentes méthodes d'authentification. Il nécessite la présence d'un serveur d'authentification compatible, comme un serveur RADIUS ou TACACS.
Le protocole 802.1X est compatible avec de nombreux équipements réseau, tels que les commutateurs, les points d'accès sans fil, les routeurs et les pare-feu. Il est également pris en charge par de nombreux systèmes d'exploitation, tels que Windows, MacOS et Linux, ainsi que par de nombreux clients VPN.

3.3.2 Composants du protocole 802 .1X

Les principaux composants du protocole 802.1X sont :

1. **Supplicant :** Le périphérique client qui tente de se connecter au réseau. Il envoie des informations d'identification au serveur d'authentification via le port de commutateur configuré en mode 802.1X.
2. **Authenticator :** Le commutateur qui contrôle l'accès au réseau. Il transmet les informations d'identification du supplicant au serveur d'authentification et contrôle l'accès au réseau en fonction des résultats de l'authentification.
3. **Serveur d'authentification :** Le serveur qui vérifie les informations d'identification du supplicant et renvoie une réponse au commutateur authenticator. Les serveurs d'authentification les plus couramment utilisés sont les serveurs RADIUS et TACACS+.

   Ces trois composants travaillent ensemble pour fournir une authentification sécurisée des utilisateurs qui tentent d'accéder au réseau[16].

3.3.3 Etapes d'authentification du protocole 802.1X

Le protocole 802.1X est un protocole de sécurité réseau qui fournit une méthode d'authentification d'un utilisateur ou d'un dispositif qui demande l'accès à un réseau local ou à un réseau étendu. Le processus d'authentification du protocole 802.1X comprend les étapes suivantes :

1.Initiation de la connexion : Le client envoie une demande d'accès (EAP Start) au point d'accès ou commutateur réseau. Le point d'accès ou commutateur répond en indiquant que l'authentification est requise en envoyant un paquet "EAP Request Identity".

2.Authentification : Le client envoie ses informations d'identification (nom d'utilisateur et mot de passe) au serveur d'authentification, qui peut être un serveur RADIUS ou un autre serveur d'authentification. Le serveur vérifie les informations d'identification

et renvoie une réponse d'acceptation ou de rejet. Si le serveur renvoie une demande de certificat, le client doit envoyer un certificat au serveur pour prouver son identité.

3.Attribution de la session : Si le client est authentifié avec succès, le point d'accès ou commutateur réseau envoie une requête d'attribution de session au serveur d'attribution de session (Session-Attribute Server), qui renvoie une clé de session au point d'accès ou commutateur réseau. Cette clé est ensuite transmise au client pour établir une connexion sécurisée.

4.Contrôle d'accès : Le point d'accès ou commutateur réseau utilise la clé de session pour contrôler l'accès du client aux ressources du réseau. Le client peut alors accéder aux ressources du réseau.

Si l'authentification échoue à l'une de ces étapes, le client ne sera pas autorisé à accéder aux ressources du réseau. Le protocole 802.1X est souvent utilisé en conjonction avec d'autres protocoles de sécurité tels que WPA2 (Wi-Fi Protected Access 2) pour assurer la sécurité des réseaux sans fil[16].

Les différentes étapes de l'authentification sont illustrées dans la figure 3.3.

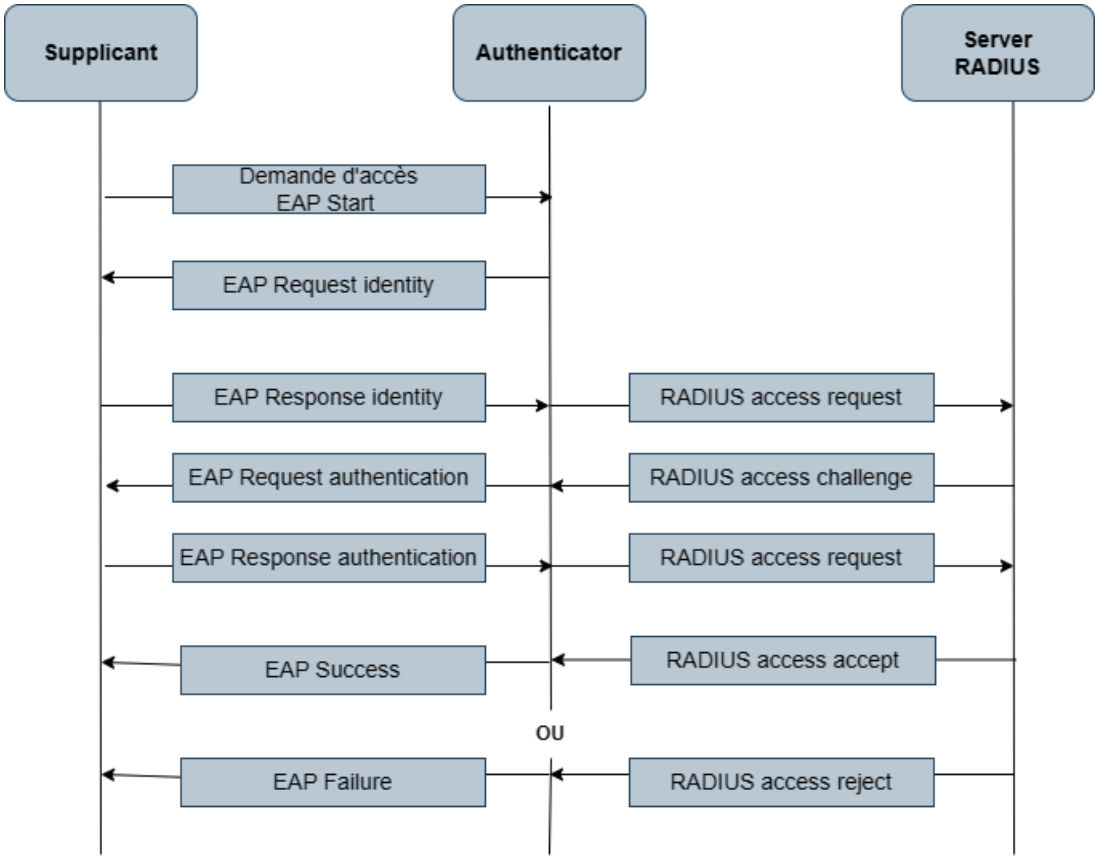


FIGURE 3.3 – Etapes d'authentification du protocole 802.1X .

3.3.4 Protocole EAP

Le protocole EAP (Protocole d'authentification extensible) est un protocole simple avec une seule fonction. Il est utilisé pour transporter et gérer les informations d'authentification entre le Supplicant et le serveur d'authentification dans le cadre du processus d'authentification 802.1X.

Le protocole EAP n'est pas responsable de la transmission sécurisée des données, mais simplement du transport et de la gestion des informations d'authentification entre les parties.

Le processus d'authentification commence lorsque l'authenticator envoie une demande d'identification (Request-Identity) au supplicant, qui répond avec un message d'identification (Response). L'authenticator retire toute encapsulation du paquet, ré-encapsule le

message EAP et le transfert au serveur d'authentification.

Le serveur d'authentification traite les données et répond en conséquence. Ce processus se poursuit jusqu'à ce que le serveur d'authentification déclare le succès ou l'échec de l'authentification.

EAP est capable de supporter différents types d'authentification tels que MD5, OTP, l'utilisation de cartes à puce, etc. L'architecture du protocole permet d'ajouter des modules d'authentification sans affecter le mécanisme de transport.

Le protocole EAP ne comprend pas de mécanismes de sécurité intégrés, mais utilise un processus de verrouillage pour garantir l'ordre des échanges de paquets[16].

La figure 3.4 montre le fonctionnement du protocole EAP.

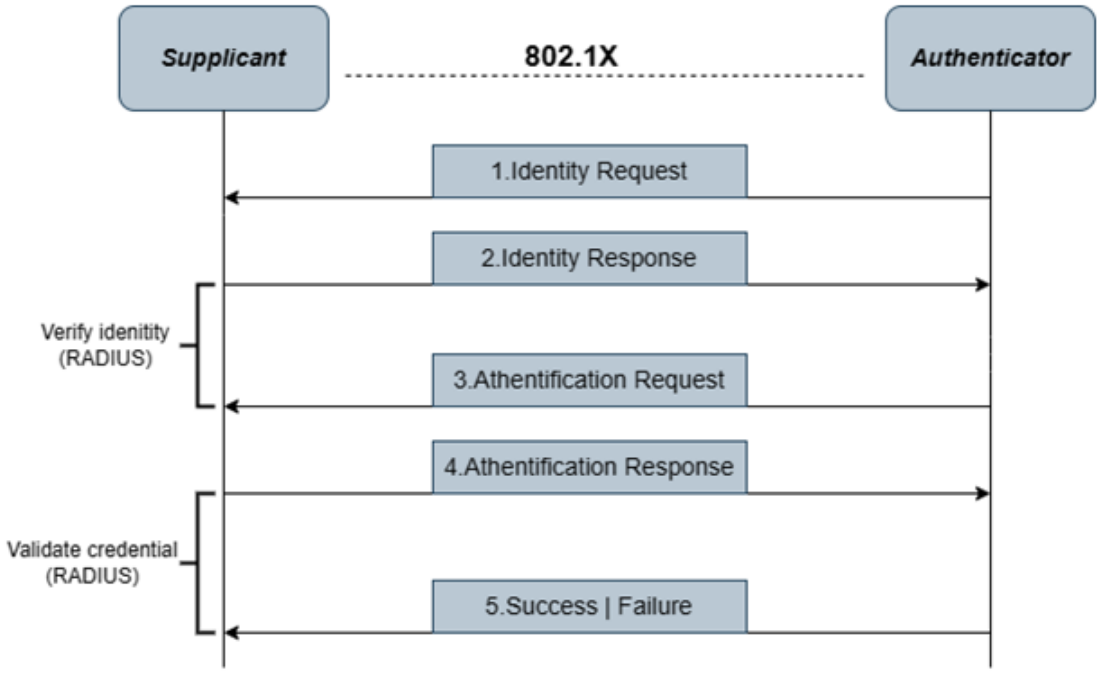


FIGURE 3.4 – Protocole EAP.

3.4 Conclusion

Ce chapitre a été consacré à une description détaillée du protocole RADIUS, qui est conforme à la norme 802.1X.

Chapitre 4

Mise en place d'un protocole d'authenfication

4.1 Introduction

Ce chapitre consiste à la présentation de notre protocole d'authentification basé sur la norme 802.1x en jonction avec RADIUS et Certificat et les différents pré requis et étapes de configurations utilisés dans le but de la mise en place de la norme 802.1x au sein de l'entreprise NTS afin de sécuriser le Réseau.

4.2 Environnement de travail

Les pré requis utilisés dans notre travail sont GNS3 et WMware définis et installés comme suit :

4.2.1 Installation de GNS3

GNS3 est une solution open-source qui permet d'émuler des équipements informatiques (routeur, switch, PC...) et qui permet de simuler leurs fonctionnements. Le GNS3 est très utile pour maquetter avant une mise en production, afin de préparer des déploiements en limitant au maximum les impacts. La figure 4.1 montre le logo de GNS3.

FIGURE 4.1 – Logo de GNS3.

Pour procéder à l'installation de GNS3, il est nécessaire de suivre les étapes suivantes : Tout d'abord aller sur https ://gns3.com/ , télécharger le fichier exécutable, puis le lancer

et suivre les instructions d'installation jusqu'à leur terme. Enfin, cliquer sur le bouton "Terminer" pour finaliser le processus. La figure 4.2 illustre l'interface de GNS3.

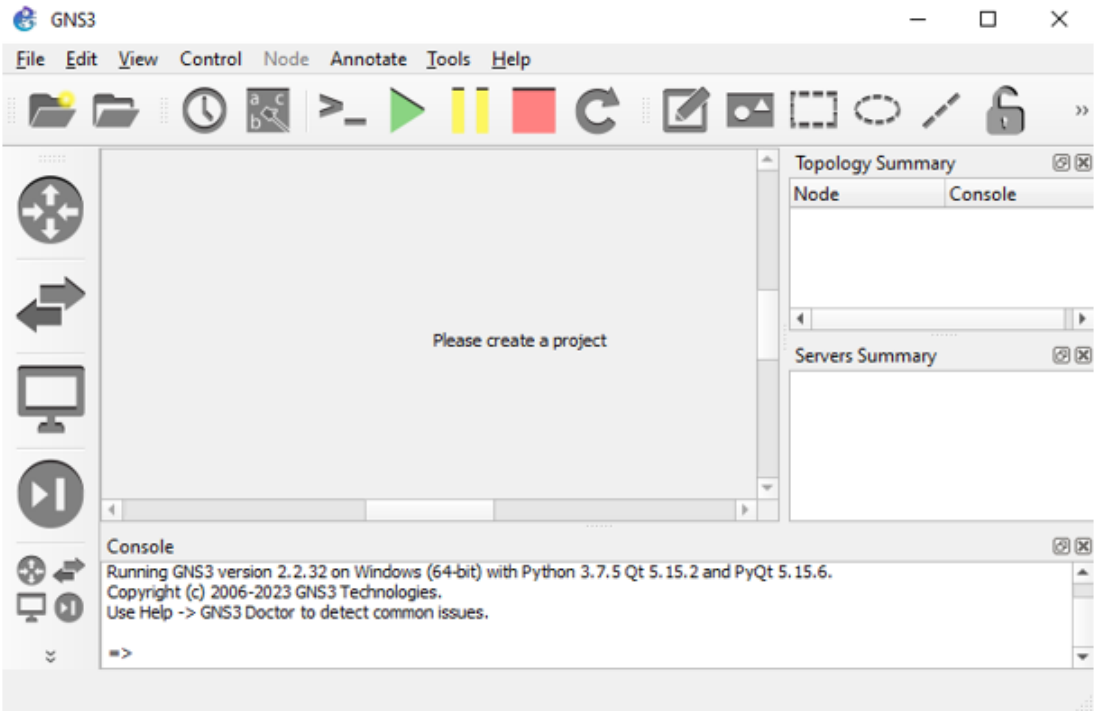


FIGURE 4.2 – Interface de GNS3.

4.2.2 Installation de VMware workstation version 16.2.1

VMware est un logiciel développé par VMware Inc qui permet la virtualisation des machines.Ce logiciel est utilisé dans la création de plusieurs instances d'un même système d'exploitaion ou d'exécuter les différents systèmes d'exploitation sur une seule machine X86 d'une manière simultanée.VMware prend aussi en charge une variété de systèmes d'exploitation pouvant être exécutés sur un PC Windows ou Linux. De plus, il propose des outils de déploiement tels que VMware ACE permettant de stocker de stocker le bureau d'un utilisateur sur une clé USB pour faciliter le transport. VMware consiste également à la création des environnements virtuels complets conprenant des serveurs du stockage et des réseaux.Son utilisation contribue à réduire les coûts liés à l'informatique tout en améliorant l'efficacité et l'agilité des opérations. La figure 4.3 montre le logo de VMware.

FIGURE 4.3 – Logo de VMware.

Pour créer des machines virtuelles sur un même ordinateur, nous devons procéder à l'installation de VMware Workstation en suivant les étapes illustrées dans la figure 4.4.

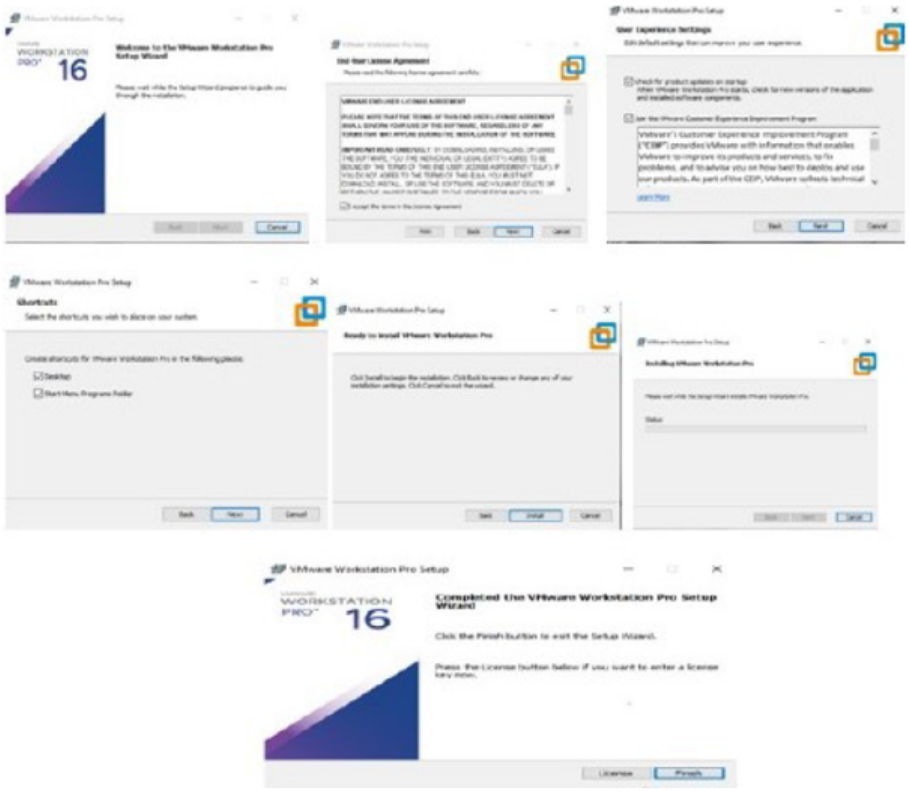


FIGURE 4.4 – Etapes d'installation de VMware.

Une fois VMware est installé, une page d'accueil s'affichera (comme le montre la figure 4.5).

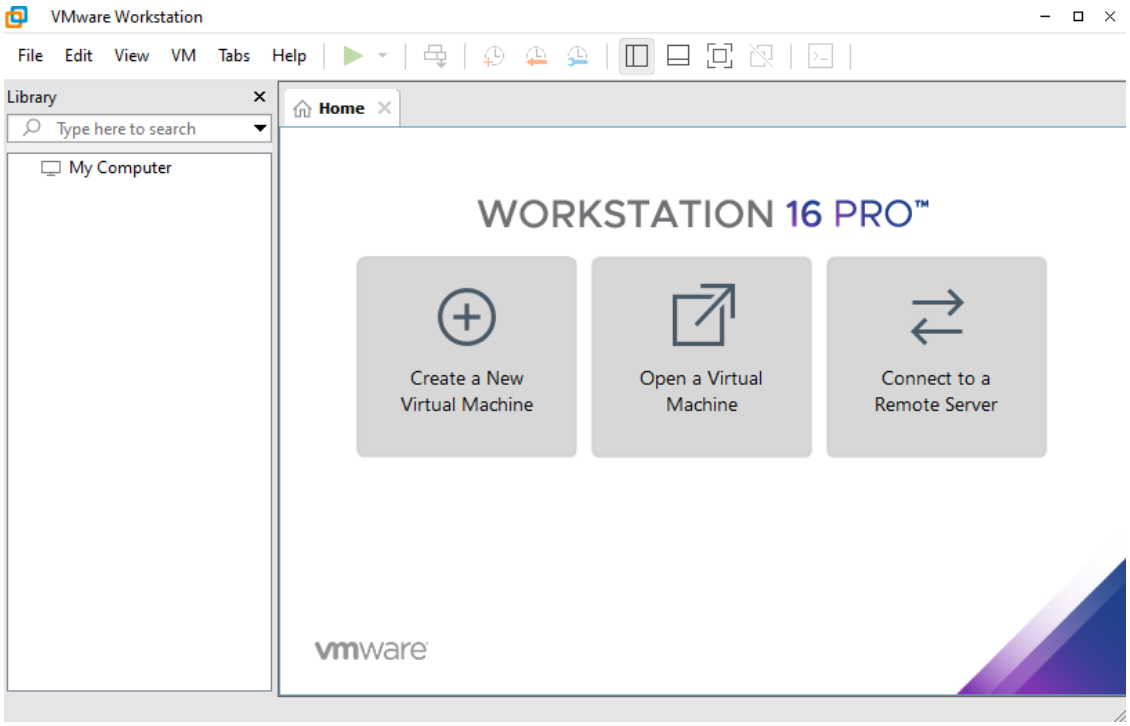


FIGURE 4.5 – Page d'accueil de VMware.

Dans le cadre de l'interprétation des données et la gestion des connexions à distance des clients nous allons utiliser les logiciels suivant :

•**Wireshark** : C'est un logiciel Open Source, conçu pour les administrateurs réseau et les développeurs, et sert à capturer et analyser les paquets de données d'un réseau. Il est largement reconnu comme une référence en matière d'analyse des transactions réseau. Doté d'une grande puissance, Wireshark prend en charge des centaines de protocoles différents et offre des fonctionnalités de filtrage avancées pour faciliter la capture et l'interprétation des données.

• **Putty** : C'est un logiciel client open-source, populaire et largement utilisé pour les connexions à distance via des protocoles tels que SSH. Il offre une interface simple et conviviale qui permet aux utilisateurs de se connecter à des serveurs distants et de gérer ces connexions de manière sécurisée. Putty est disponible pour les systèmes d'exploitation Windows et Linux, et il est souvent utilisé par les administrateurs système, les développeurs et les professionnels de l'informatique pour l'administration à distance des serveurs

et des dispositifs réseaux.

4.3 Architecture proposée

Notre solution implémentée sous GNS3 est montrée dans la figure 4.6.

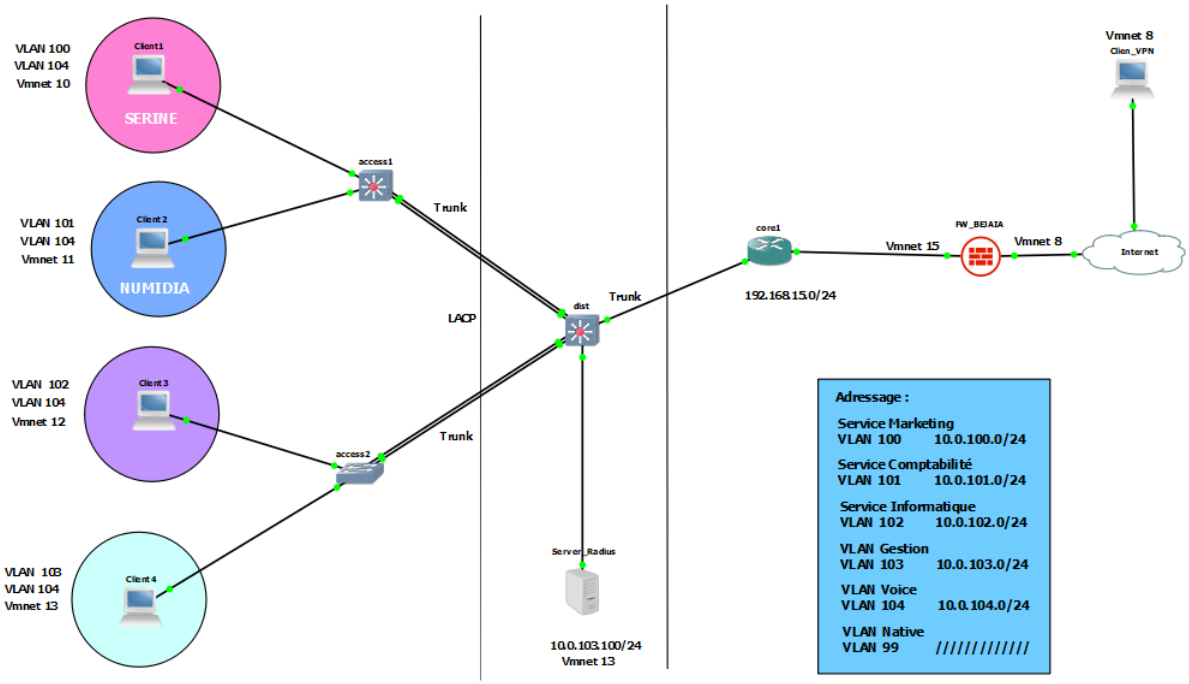


FIGURE 4.6 – Architecture proposée :

4.4 Installation et configuration de l'Active Directory AD+DNS

La figure 4.7 illustre les étapes à suivre dans l'ordre pour effectuer la configuration AD+DNS.

FIGURE 4.7 – Etapes de la configuration AD+DNS.

4.4.1 Installation de AD + DNS

Pour installer le rôle Service de domaine Active Directory, on ouvre le gestionnaire de serveur et on accède à l'option "Ajouter des rôles et des fonctionnalités". On sélectionne les rôles "Serveur DNS" et "Service AD DS" dans la liste, on coche les cases correspondantes, puis on suit les instructions pour finaliser l'installation. Une fois terminée, le rôle Service de domaine Active Directory sera installé sur notre serveur. La figure 4.8 montre l'installation de AD+DNS.

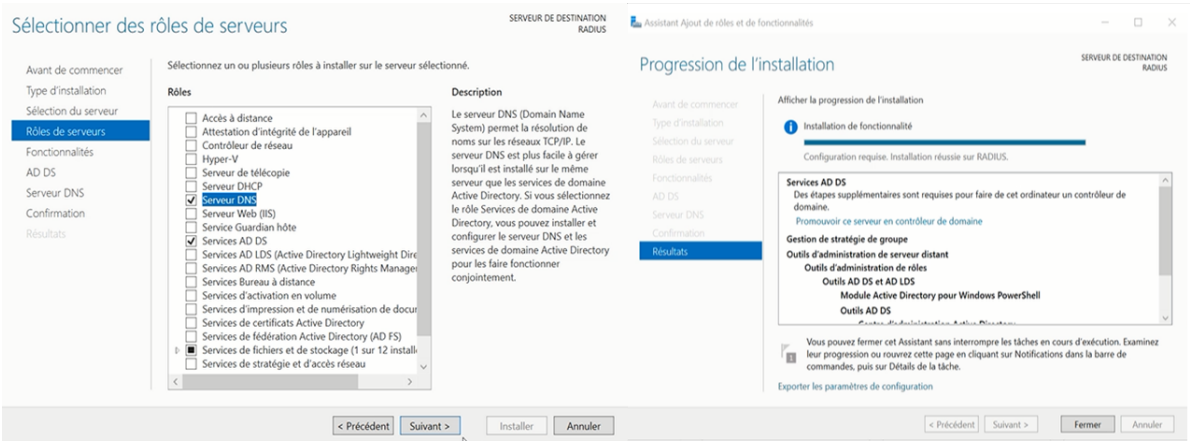


FIGURE 4.8 – Installation de AD + DNS.

4.4.2 Création de Contrôleur de domaine

Une fois que les fonctionnalités d'AD DS sont installées, on doit promouvoir ce serveur en tant que contrôleur de domaine afin de créer le domaine. Pour le nouveau domaine, on choisit "Ajouter une nouvelle forêt" et on spécifie le nom du domaine "campusnts.local". La figure 4.9 illusttre la création du nom de domaine.

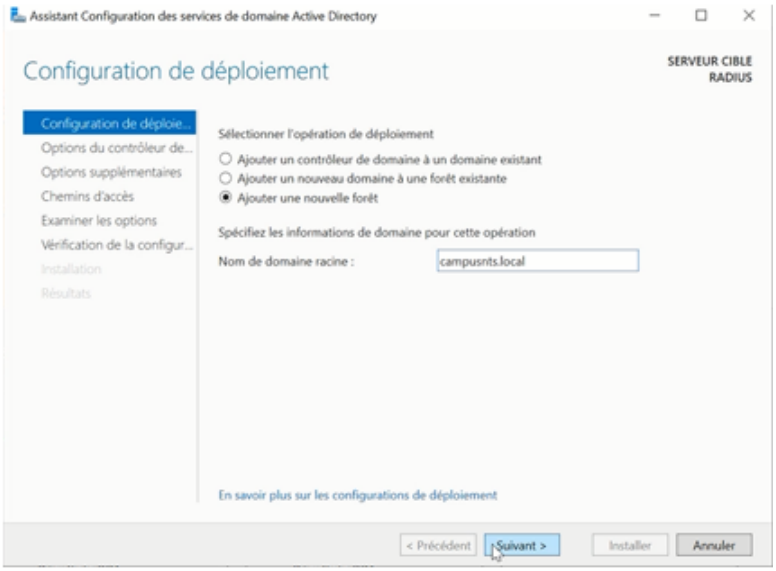


FIGURE 4.9 – Création de nom de domaine.

Ensuite, on sélectionne le niveau fonctionnel de la forêt et du domaine "Windows server 2016", et on définit un mot de passe de restauration des services d'annuaires. La figure 4.10 montre la création du nom de domaine.

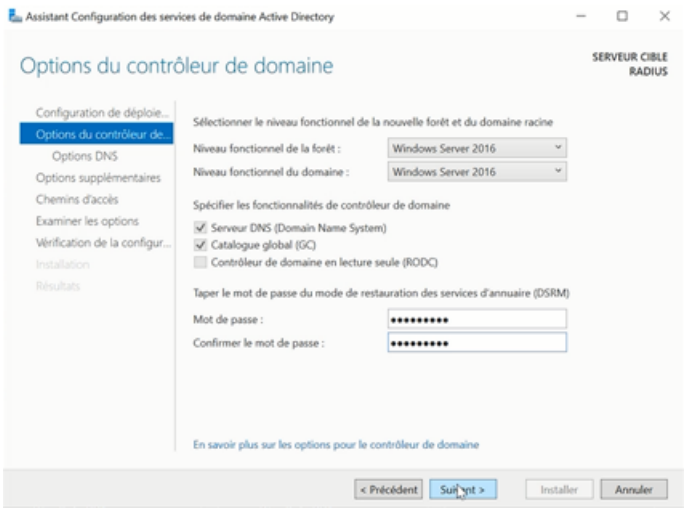


FIGURE 4.10 – Option du controleur de domaine.

On continue l'installation en cliquant sur "Suivant" après avoir vérifié le nom NetBIOS du domaine "CAMPUSNTS". La figure 4.11 montre des options supplémentaires.

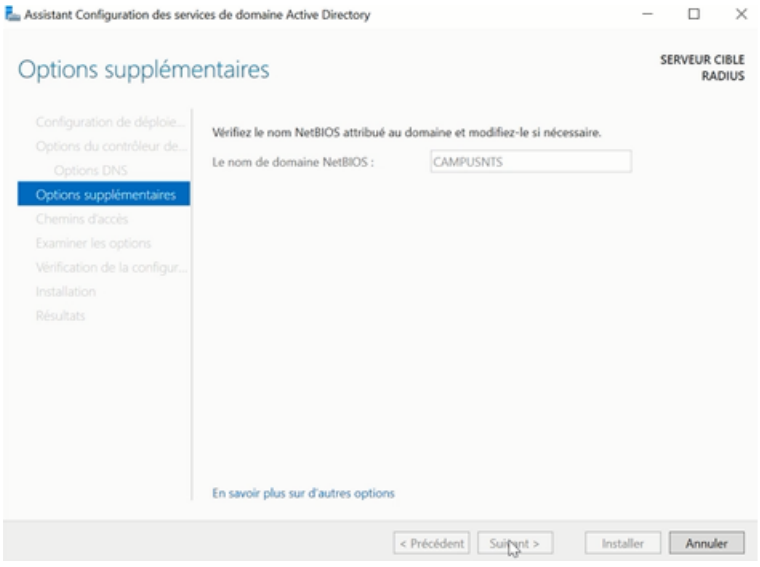


FIGURE 4.11 – Options supplémentaires.

Ensuite, on spécifie les dossiers qui abriteront la base de données du contrôleur de domaine Active Directory. Windows peut proposer des options supplémentaires, comme l'installation d'un serveur DNS compatible avec notre Active Directory. La figure 4.12 illustre la vérification de la configuration requise.

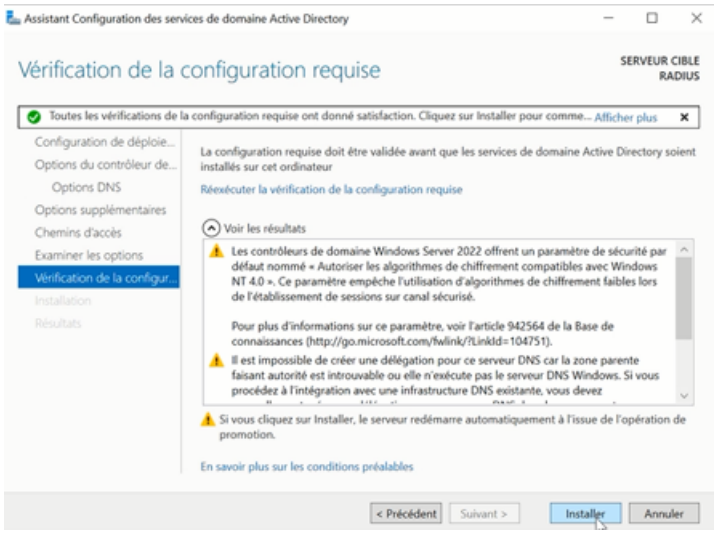


FIGURE 4.12 – Vérification de la configuration requise.

Après avoir configuré et installé tous les services nécessaires, il est possible que le système demande un redémarrage pour appliquer les modifications.

4.4.3 Création de l'unité d'organisation

On commence la création d'une nouvelle unité d'organisation. Pour cela, on se rend dans "Outils" puis "Utilisateurs et ordinateurs AD". Ensuite, on sélectionne le nom de notre domaine "campusnts.local" et on fait un clic droit avec la souris. On choisit "Nouveau" puis "Unité d'organisation". On donne un nom à cette unité d'organisation, qui sera "Site Bejaia" dans notre cas. Dans cette unité "Site Bejaia", on va aussi créer d'autres unités d'organisation. Pour cela, on fait un clic droit sur l'unité "Site Bejaia" et on choisit "Nouveau" puis "Unité d'organisation". On attribue ensuite un nom à cette nouvelle unité d'organisation. Dans notre cas, nous avons créé les unités d'organisation "Ordinateurs" et "Utilisateurs". Voir la figure 4.13.

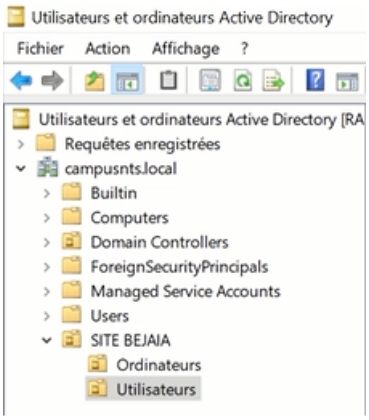


FIGURE 4.13 – Unité d'organisations

4.4.4 Création des Groupes

Une fois que l'unité d'organisation "Utilisateur" a été créée, nous allons procéder à la création de groupes et d'utilisateurs à l'intérieur de celle-ci. La figure 4.14 montre les groupes crées.

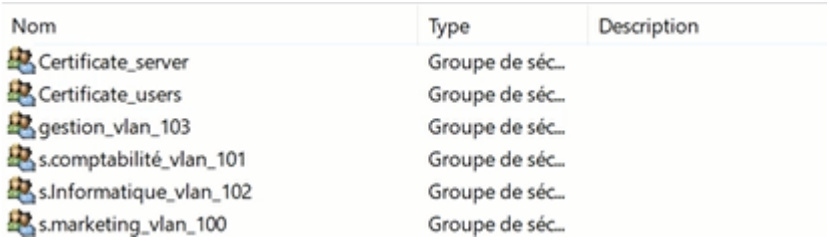


FIGURE 4.14 – Groupes crées.

Pour créer un utilisateur dans Active Directory, on fait un clic droit sur l'unité d'organisation "Utilisateur", puis on sélectionne "Nouveau" et enfin "Utilisateur". Dans notre cas, nous allons créer deux utilisateurs : Saidi Serine et Sabrachou Numidia, et les affecter à différents services de l'entreprise. Nous allons d'abord créer l'utilisateur Saidi Serine et l'ajouter au service marketing. Saidi Serine aura ainsi accès aux informations et aux fonctionnalités liées au marketing. Ensuite, nous allons créer l'utilisateur Sabrachou Numidia et l'affecter au service comptabilité. Sabrachou Numidia aura donc accès aux informations liées à ce service. Les deux figure 4.15 et 4.16 montrent respectivement la

création de l'utilisateur Saidi Serine et l'utilisateur sabrachou numidia.

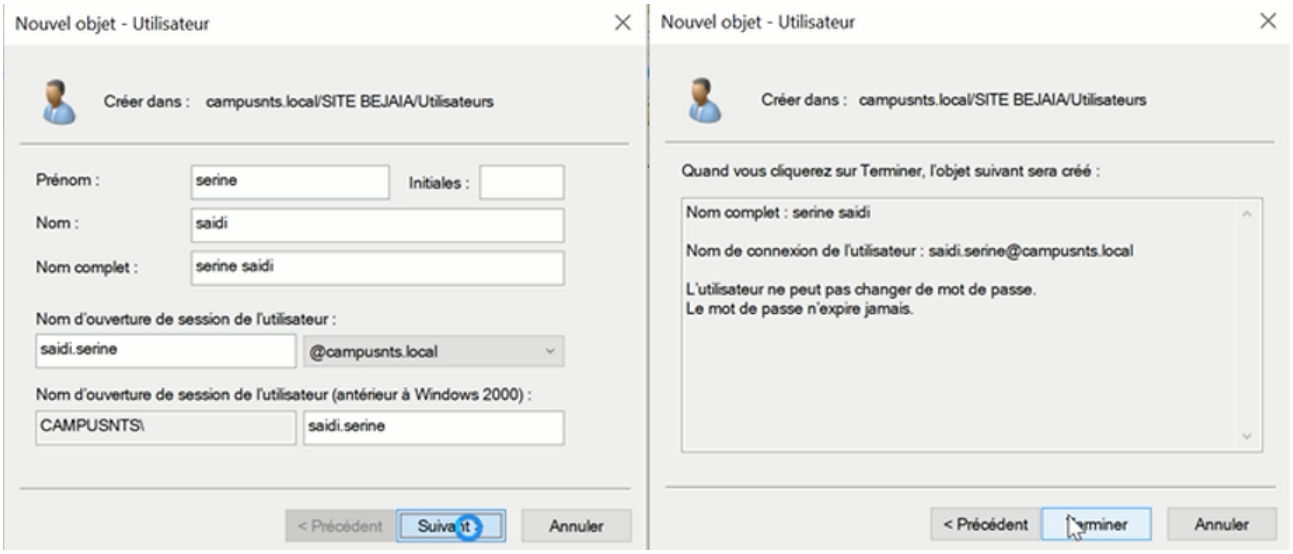


FIGURE 4.15 – Création de l'utilisateur Saidi Serine.

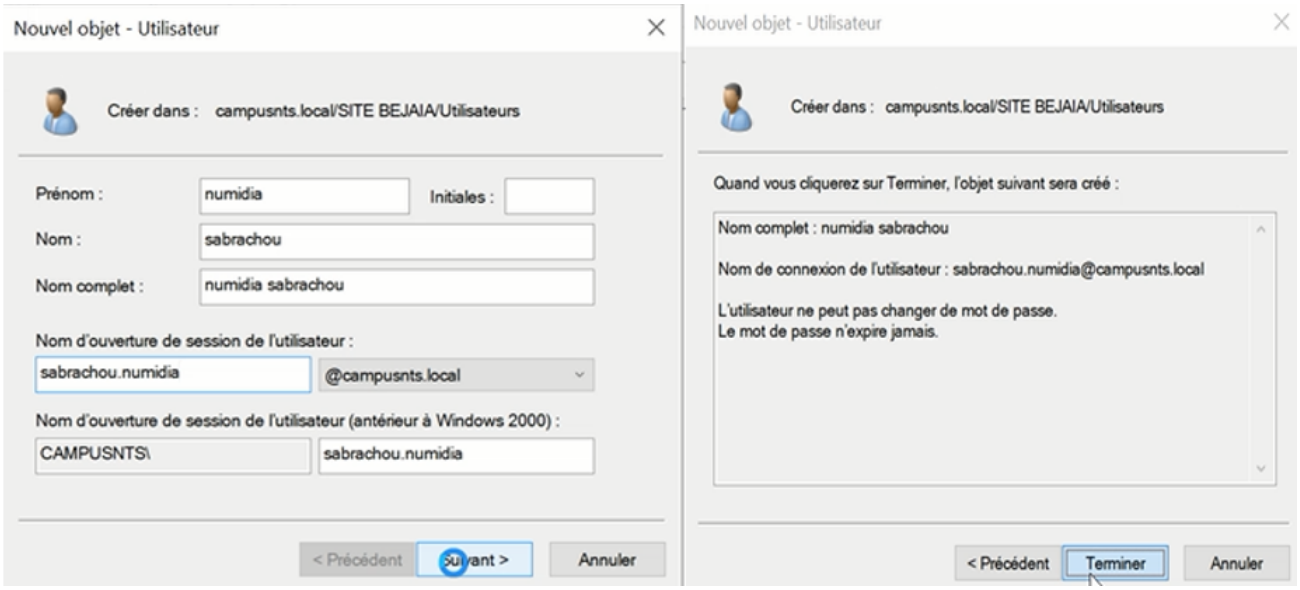


FIGURE 4.16 – Création de l'utilisateur Sabrachou Numidia.

L'affectation chaque utilisateur des figure 4.15, 4.16 à son service est montré dans la figure 4.17.

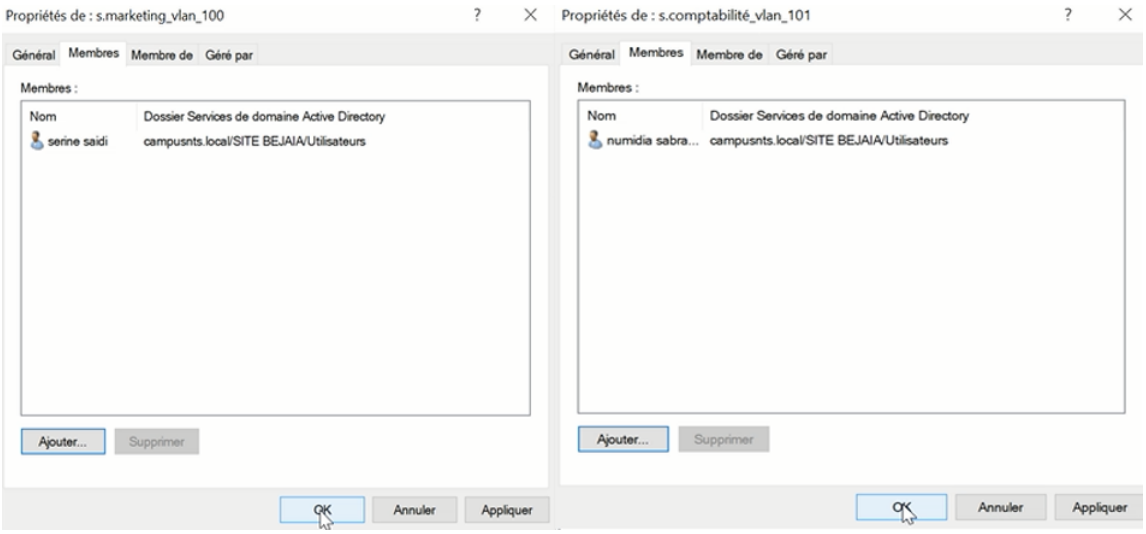


FIGURE 4.17 – Ajouter Saidi Serine au service Marketing et Ajouter Sabrachou Numidia au service comptabilité.

4.4.5 Création de la GPO pour RADIUS

Après avoir créé les groupes et les utilisateurs, il est temps de passer aux GPO (Group Policy Objects), qui sont des outils de gestion de stratégies de groupe utilisés dans Active Directory pour configurer et appliquer des paramètres sur les utilisateurs et les ordinateurs d'un réseau Windows. Pour créer les GPO, nous allons accéder au menu Démarrer, puis aux Outils d'administration, et enfin cliquer sur Gestion des stratégies de groupe. Dans cette étape, nous allons créer une GPO nommée "st_radius" et l'appliquer à l'unité d'organisation "Ordinateur". Comme indiqué dans les figures 4.18 et 4.19.

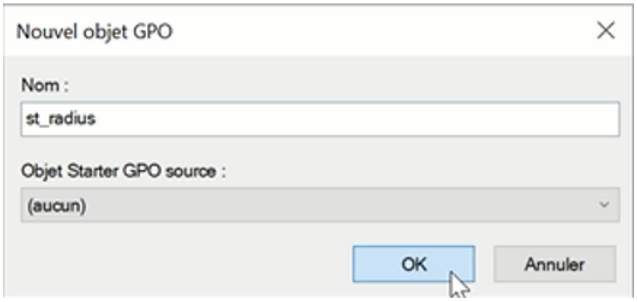


FIGURE 4.18 – Création d'une nouvelle GPO.

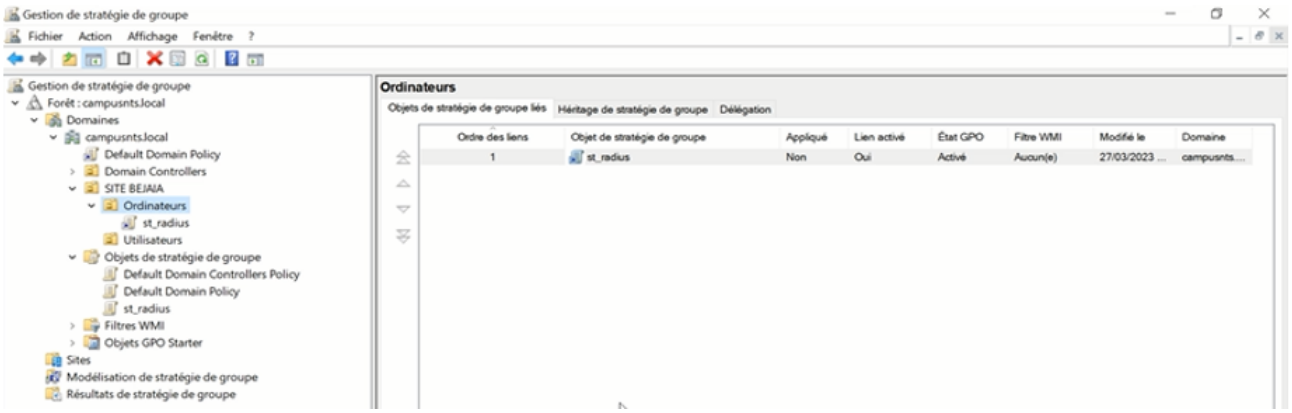


FIGURE 4.19 – GPO crée dans l'unité d'organisation Ordinateur.

Dans notre travail nous considérons les réseaux filaire.Pour configurer la GPO afin d'automatiser la configuration du réseau câblé, nous accédons aux "Objets de stratégie de groupe", puis nous recherchons et sélectionnons l'objet "st_radius". Ensuite, nous modifions la stratégie en cliquant sur "Modifier" et en accédant à "Paramètres Windows", "Paramètres de sécurité", "Services et systèmes" et enfin "Configuration automatique de réseau câblé". Nous sélectionnons l'option "Automatique" pour finaliser la configuration. Les différentes étapes que nous avons utilisés sont résumés dans les figures 4.20 et 4.21.

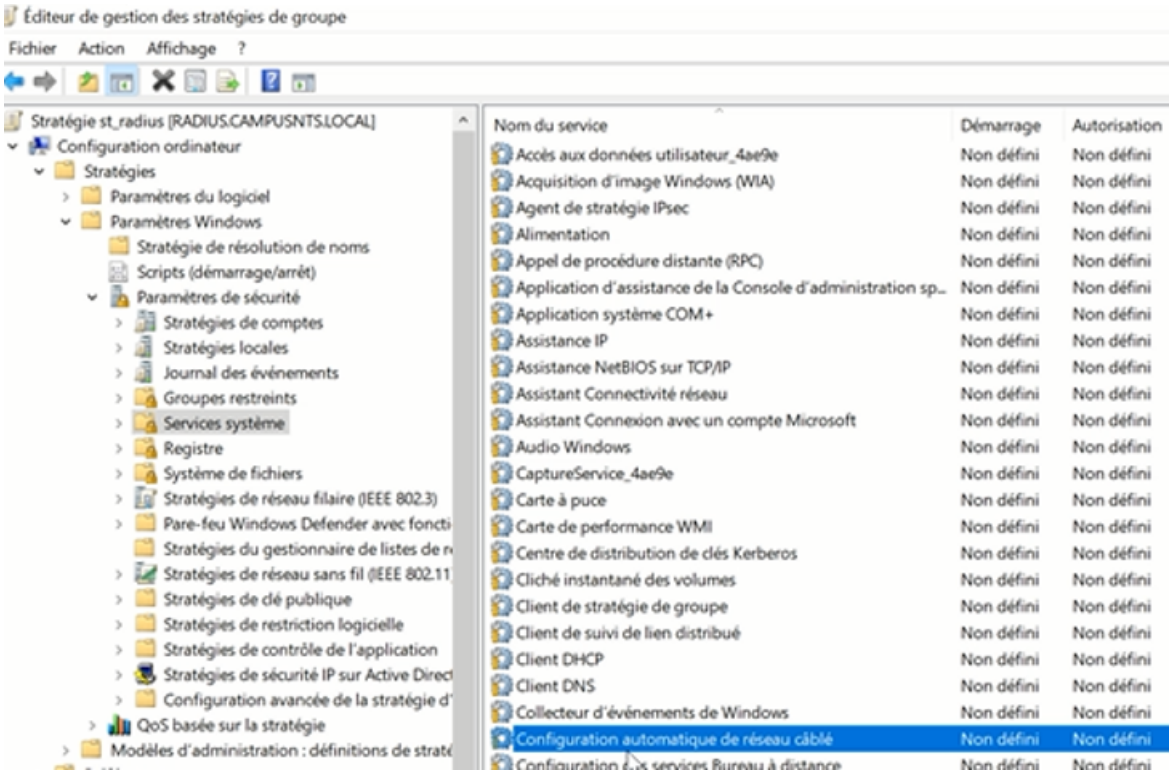


FIGURE 4.20 – Configuration de la GPO.

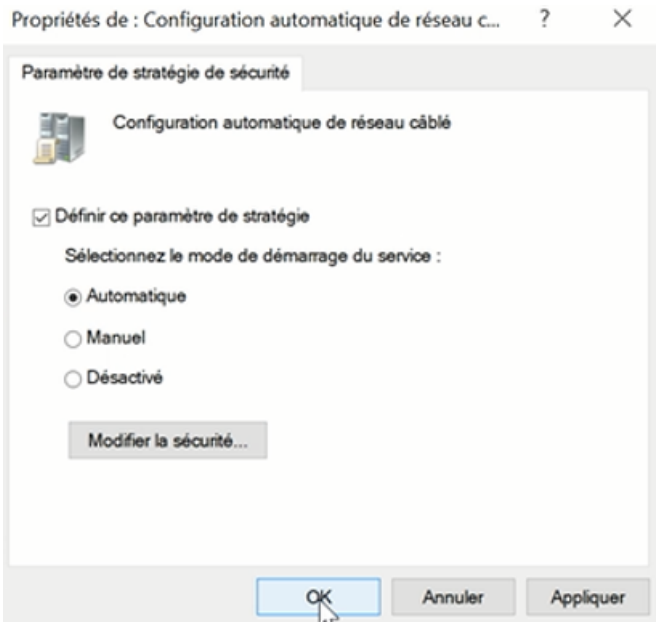


FIGURE 4.21 – Activation automatique des services.

4.5 Installation de Dynamic Host Configuration Protocol (DHCP)

Pour une installation de DHCP nous suivons les étapes montrées dans la figure 4.22.

FIGURE 4.22 – Etapes de la configuration DHCP.

4.5.1 Installation de service DHCP

Afin de permettre la communication entre les PC et les serveurs, il est essentiel de leur assigner une adresse IP, un masque de sous-réseau, une passerelle et un serveur DNS, qui doit être un DNS d'Active Directory. Dans l'assistant de gestion des rôles, sélectionnez le rôle de serveur DHCP en cochant la case correspondante, puis cliquez sur "Suivant" jusqu'à l'installation. Enfin, cliquez sur "Installer" pour terminer. Comme l'indique la figure 4.23.

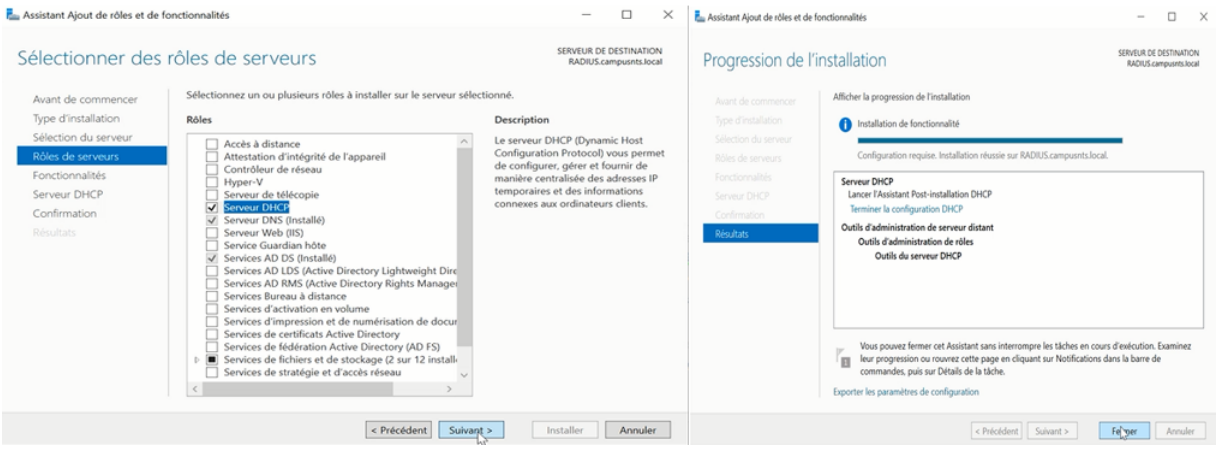


FIGURE 4.23 – Installation de DHCP.

4.5.2 DHCP relais

La figure 4.24 illustre la façon de lier le serveur DHCP avec Active Directory (AD) et les informations d'identification à utiliser pour autoriser le serveur DHCP dans le service AD.

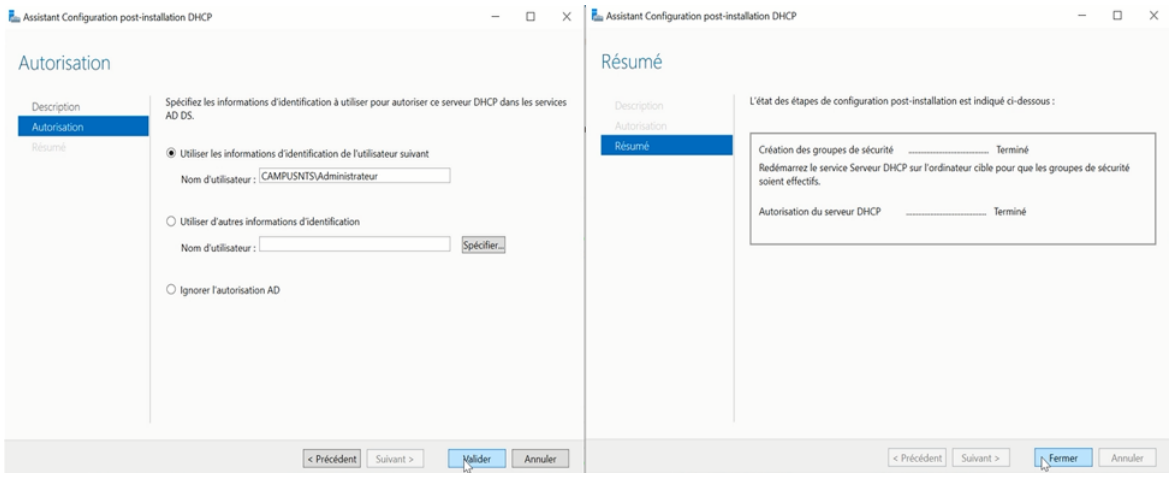


FIGURE 4.24 – DHCP relais.

Pour créer nos étendues DHCP, nous utilisons la console d'administration DHCP accessible depuis le menu "Outils" du gestionnaire de serveur. À l'aide de cette console, nous configurons les étendues en définissant les paramètres nécessaires tels que les plages d'adresses IP, les masques de sous-réseau, les passerelles par défaut, etc. Cela nous permet

d'attribuer des adresses IP aux clients dans chaque étendue de manière appropriée. Voir la figure 4.25 .

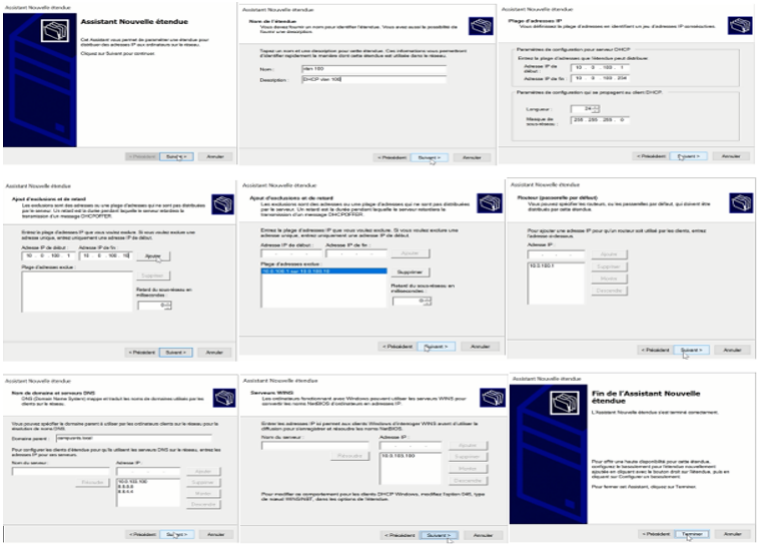


FIGURE 4.25 – Création de l'étendue.

La figure 4.26 illustre l'ensemble des étendues que nous avons créées.

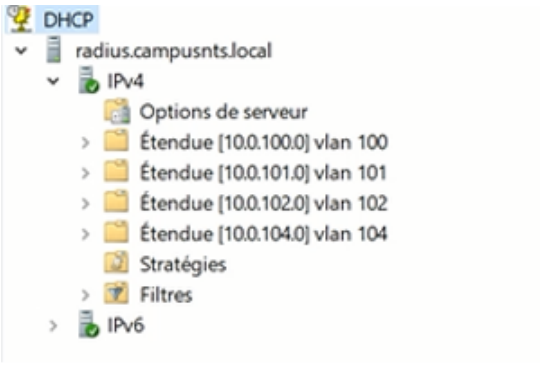


FIGURE 4.26 – Ensemble des étendues.

4.5.3 Configuration DHCP sur le routeur core1

La figure 4.27 illustre la configuration éffectuée sur le routeur Core1.

```
core1(config)#
core1(config)#interface ethernet 0/1.100
core1(config-subif)#encapsulation dot1Q 100
core1(config-subif)#ip address 10.0.100.1 255.255.255.0
core1(config-subif)#ip helper-address 10.0.103.100
core1(config-subif)#
core1(config-subif)#interface ethernet 0/1.101
core1(config-subif)#encapsulation dot1Q 101
core1(config-subif)#ip address 10.0.101.1 255.255.255.0
core1(config-subif)#ip helper-address 10.0.103.100
core1(config-subif)#
core1(config-subif)#interface ethernet 0/1.102
core1(config-subif)#encapsulation dot1Q 102
core1(config-subif)#ip address 10.0.102.1 255.255.255.0
core1(config-subif)#ip helper-address 10.0.103.100
core1(config-subif)#end
```

FIGURE 4.27 – Configuration DHCP sur le router.

4.6 Installation de serveur de certificat

Pour une installation de serveur de certificat nous suivant les étapes montrées dans la figure 4.28 .

FIGURE 4.28 – Etapes de l'installation dU serveur de certificat.

4.6.1 Installation de serveur Certificat

Afin d'installer le serveur de certificats sur la machine Windows Server, nous devons tout d'abord ajouter les services de certificats Active Directory. Ensuite, nous procédons au lancement de l'installation et à l'ajout des fonctionnalités requises. La figure 4.29 montre l'ajout des services de certificats Active Directory.

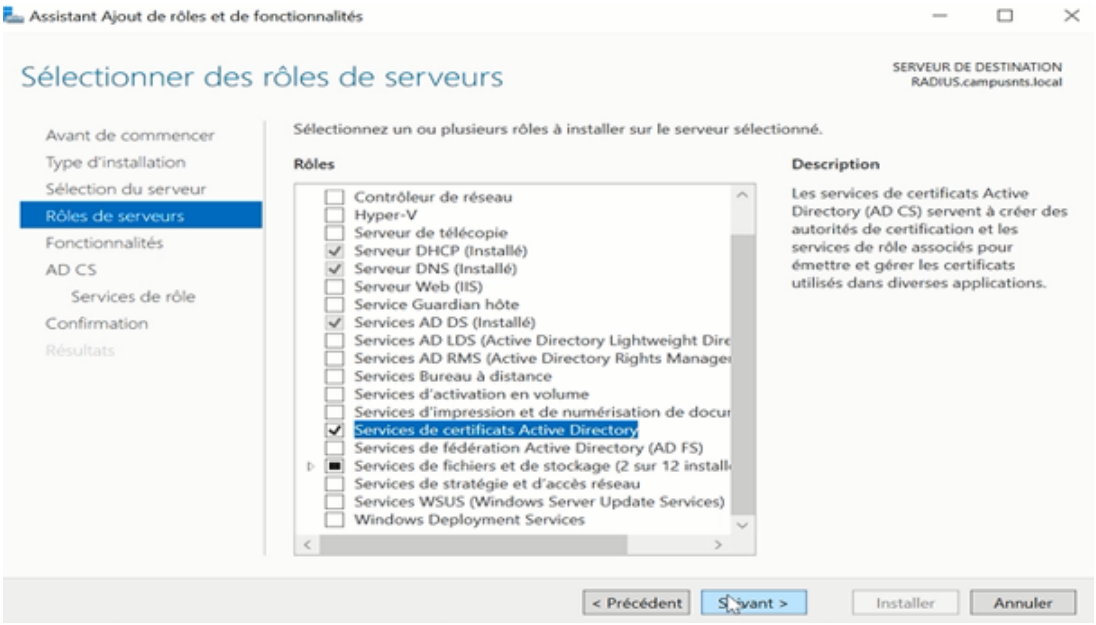


FIGURE 4.29 – Ajout des services de certificats Active Directory.

4.6.2 Création de l'autorité de certificat

À partir du gestionnaire de serveur, nous cliquons sur l'icône de notification, puis sur "Configurer les services de certificats Active Directory" pour ouvrir l'assistant de configuration.Nous fournissons les informations d'identification (CAMPUSNTS /administrateur), cochons l'autorité de certificat et choisissons le type "Autorité de certification d'entreprise". Ensuite, nous sélectionnons une clé privée, configurons le chiffrement de la clé et validons les informations fournies. La figure 4.30 illustre l'installation de l'autorité de certificat.

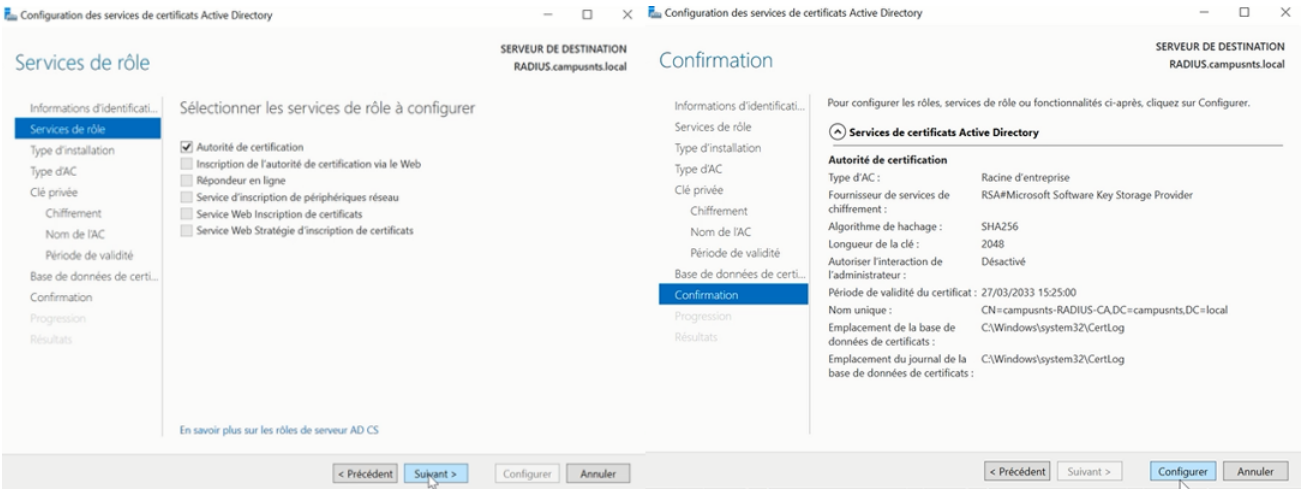


FIGURE 4.30 – Installation de l'autorité de certificat.

4.6.3 Création de Certificat "Client"

Pour créer une autorité de certification, on accède d'abord à l'outil de gestion des certificats. On sélectionne "campusnts-RADIUS-CA"Ensuite, En faisant un clic droit sur le"modèle de certificat", on choisit l'option "Gérer". Une fois dans les propriétés du modèle, on sélectionne "Authentification de station de travail ", puis on effectue un clic droit pour le dupliquer. Comme le montre la figure 4.31.

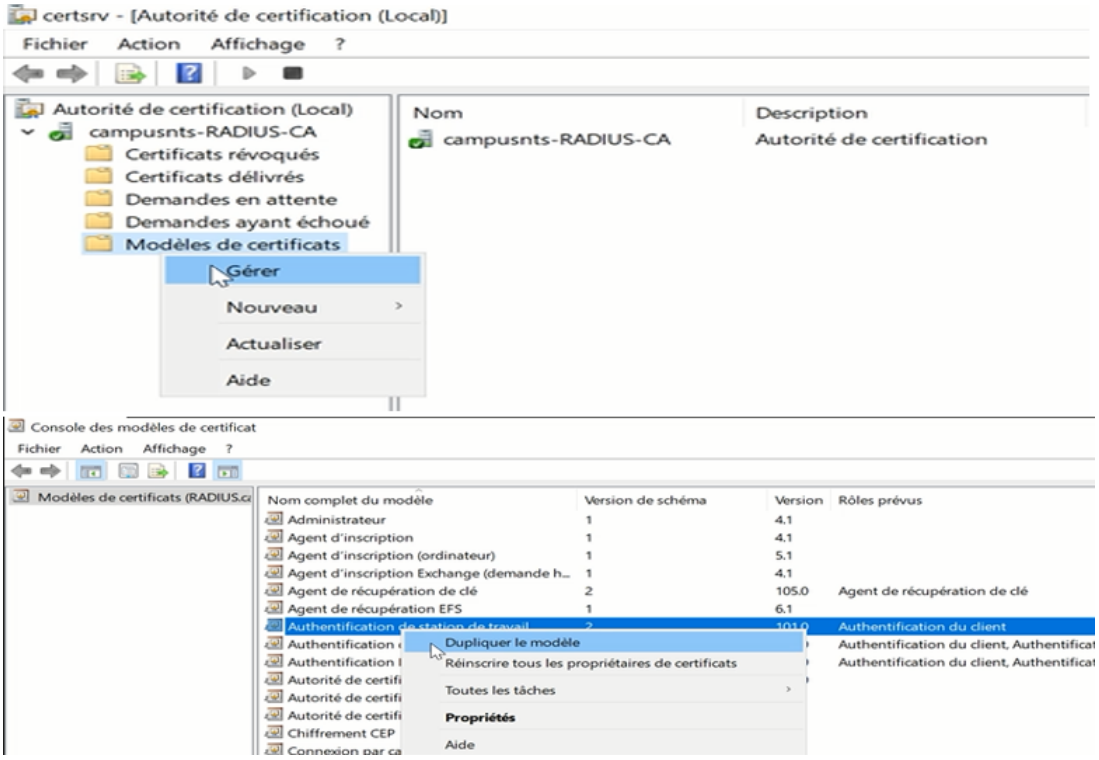


FIGURE 4.31 – Création de certificat "Client".

Dans les propriétés du nouveau modèle, on détermine les différentes propriétés requises, et notamment le nom du modèle, qu'on définit sur "Certificate_client_radius". Par la suite on clique sur le bouton "Appliquer" pour enregistrer les modifications. Comme indiqué dans la figure 4.32.

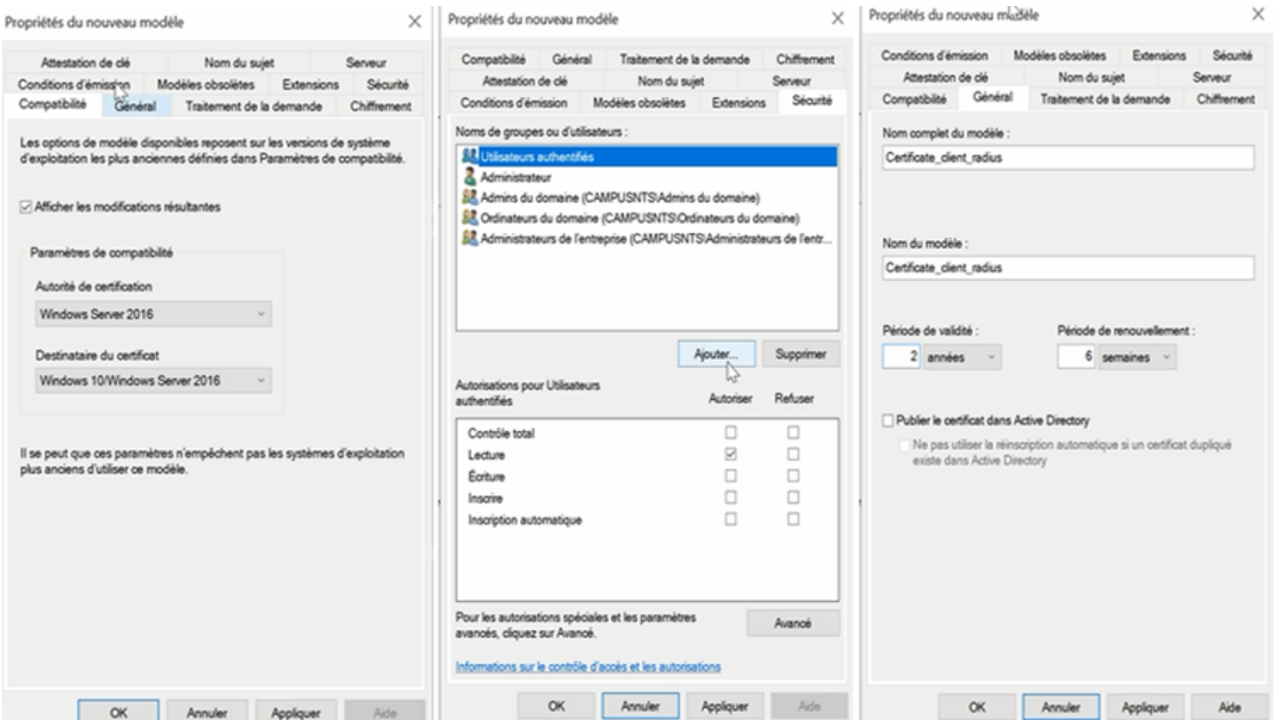


FIGURE 4.32 – Certificate_client_radius.

Une fois le certificat clients créé, nous procédons à la configuration du modèle de certificat par défaut qui sera délivré aux clients. La figure 4.32 présente le modèle de certificat à délivrer aux clients.

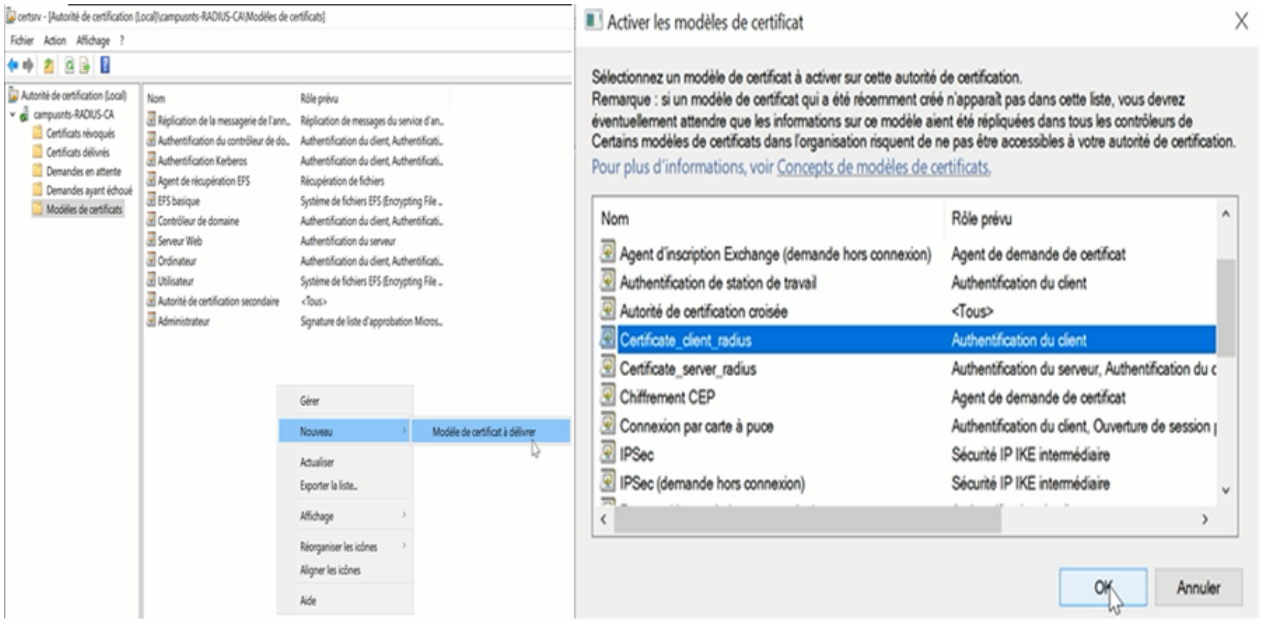


FIGURE 4.33 – Modèle de certificat client.

4.6.4 Création de certificat "Server"

Dans cette étape, on a dupliqué le modèle de certificat"serveur RAS et IAS" dans "Modèles de certificats" et on l'a renommé "Certificate_server_radius".

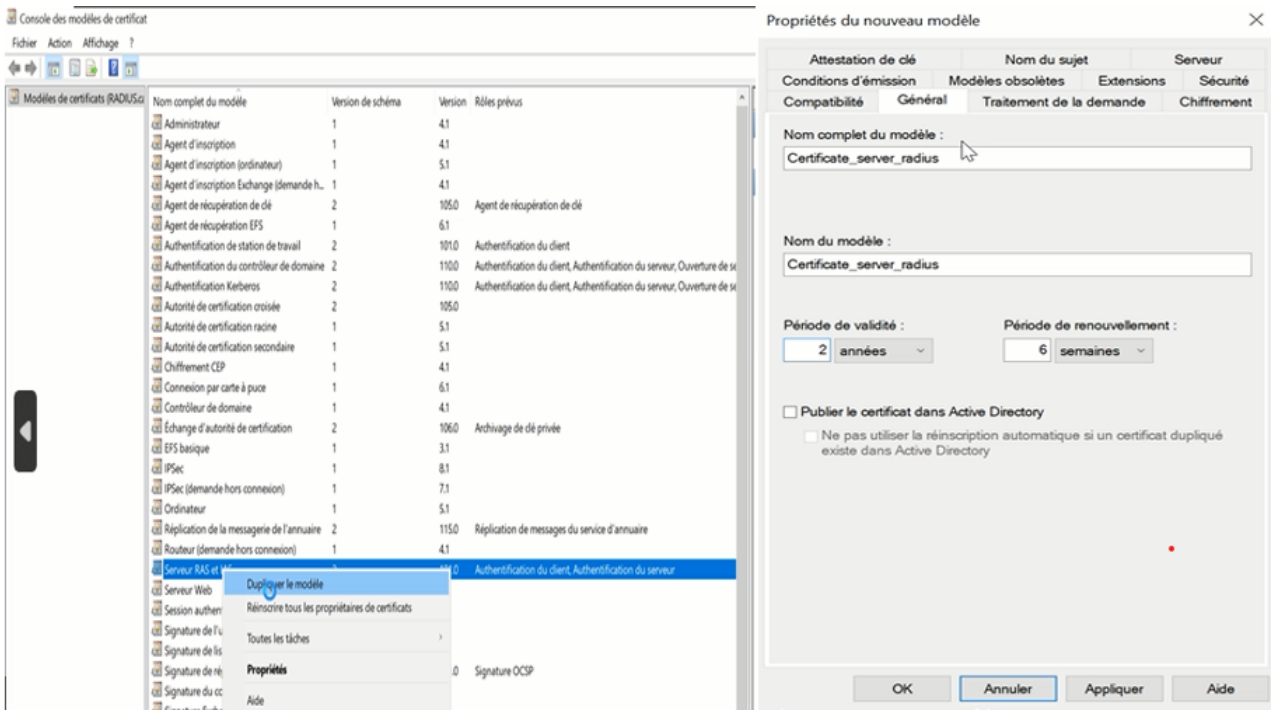


FIGURE 4.34 – Certificate_server_radius.

Une fois le certificat server créé, nous procédons à la configuration du modèle de certificat par défaut qui sera délivré au serveur. Comme illustré dans la figure 4.35.

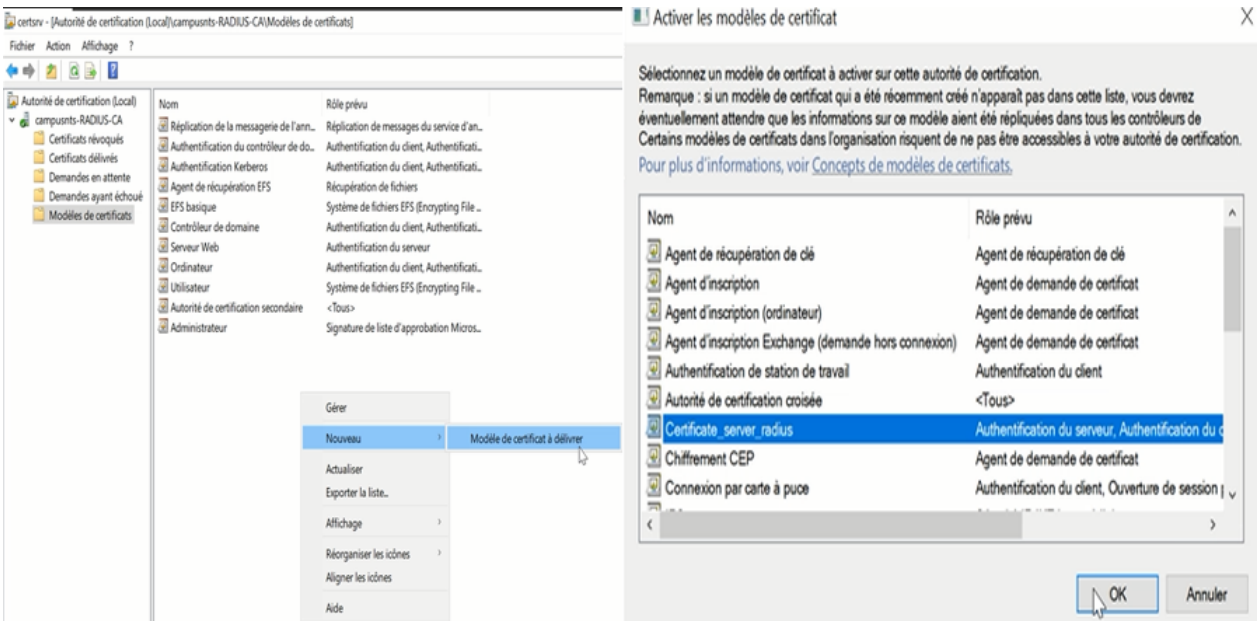


FIGURE 4.35 – Modèle de certificat server.

4.6.5 Création de Groupe Policy Object

• **Activation de l'inscription automatique des certificats par le serveur :** Nous allons activer la distribution automatique des certificats, pour cela nous accédons à l'objet de stratégie de groupe, en particulier à la stratégie "Default domain policy". Une fois dans les paramètres de sécurité, on se rend dans les stratégies de clé publique et on active l'option d'inscription automatique. Voir la figure 4.36.

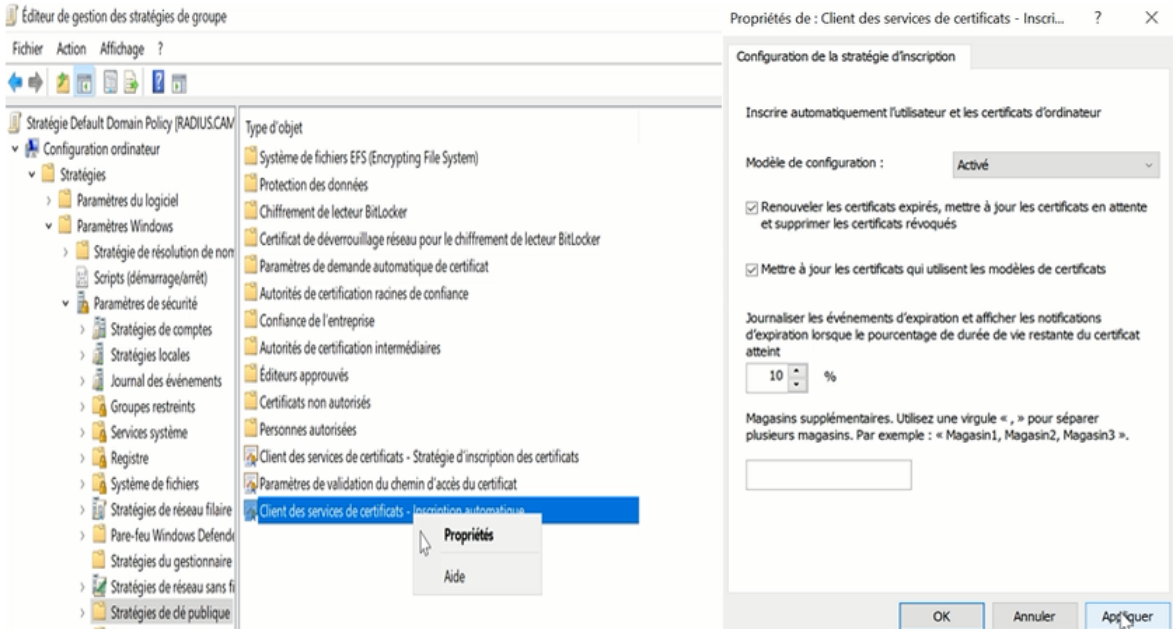


FIGURE 4.36 – Activation automatique des certificats.

• **Création d'une nouvelle stratégie des réseaux filaires :** Pour créer la stratégie globale des réseaux câblés, on clique sur "Stratégie de réseau filaire" et on sélectionne l'option "Créer" (st-radius-filaire). Ensuite, on choisit la méthode d'authentification réseau, et on opte pour PEAP (EAP), uniquement pour les ordinateurs. Une fois les paramètres configurés, on clique sur "Appliquer" puis sur "OK" pour valider les modifications. La figure 4.37 montre la création de la stratégie pour réseau filaire.

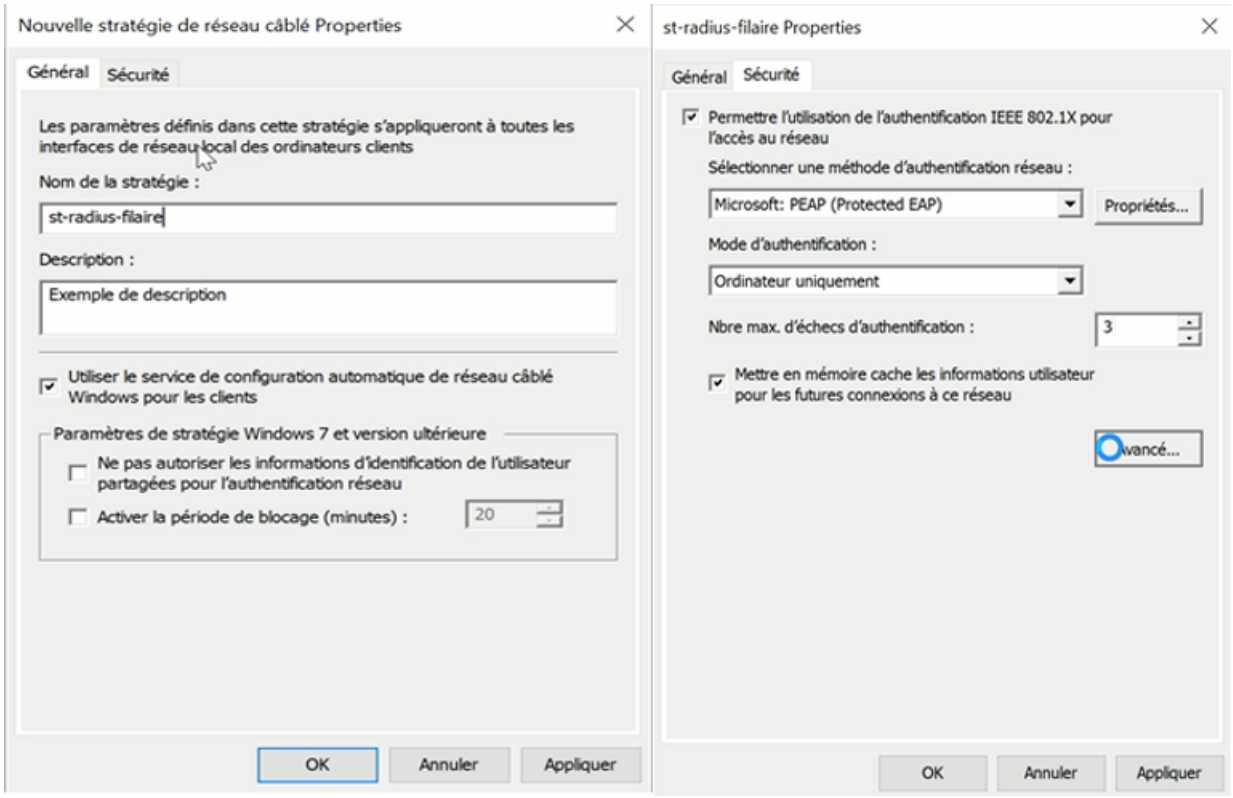


FIGURE 4.37 – Stratégie pour réseau filaire.

4.7 Installation et configuration de serveur NPS RADIUS

Pour permettre à notre protocole d'authentifier les clients nous allons installer le serveur NPS RADIUS en tenant compte des étapes illustrées dans la figure 4.38.

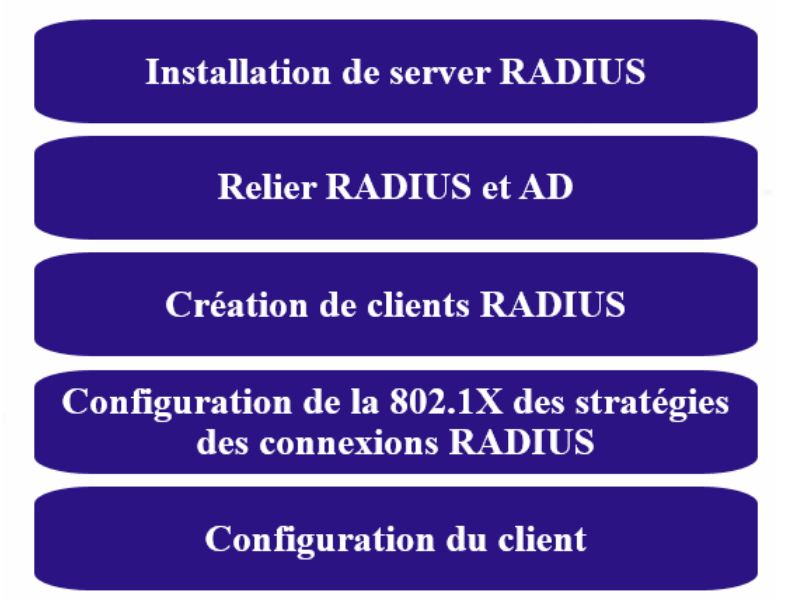


FIGURE 4.38 – Etapes de la configuration du serveur NPS RADIUS.

4.7.1 Installation de serveur RADIUS

Pour installer NPS Server (Network Policy Server) sur la machine Windows Server, on commence par ajouter le Service de NPS Server. Ensuite, on lance l'installation et on ajoute les fonctionnalités nécessaires. Comme le montre la figure 4.39.

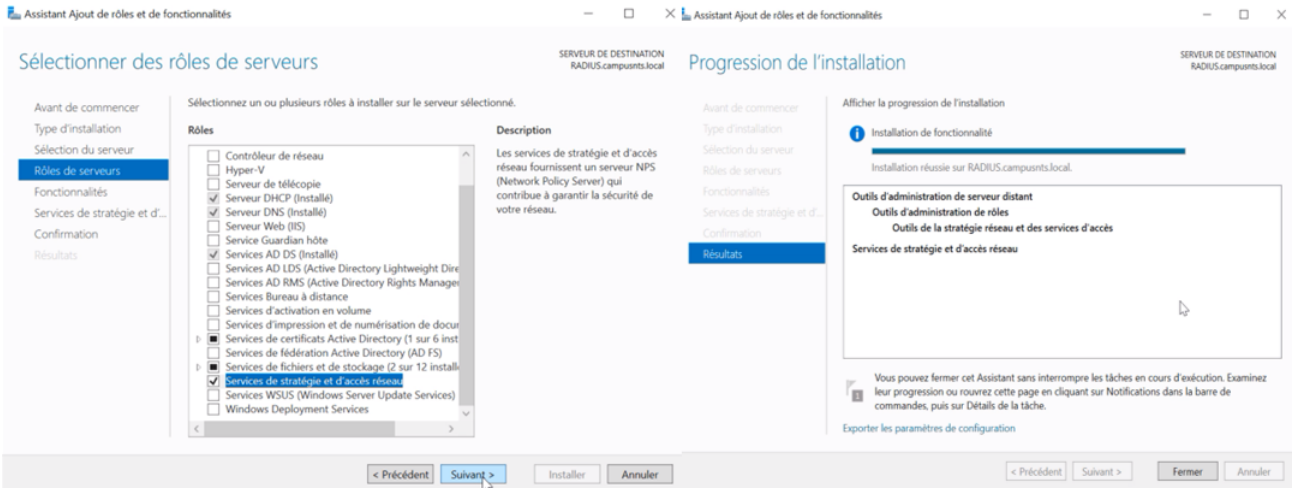


FIGURE 4.39 – Installation de server Radius.

4.7.2 Relier RADIUS et AD

Pour permettre à NPS d'accéder à distance aux informations d'identification et aux propriétés d'accès distant des comptes d'utilisateurs dans Active Directory, il est nécessaire d'inscrire le serveur NPS dans AD (Active Directory). On effectue un clic droit sur NPS (local) et on sélectionne "Inscrire un serveur dans Active Directory". Cela permet de lier le serveur NPS à Active Directory. Comme indiqué dans la figure 4.40.

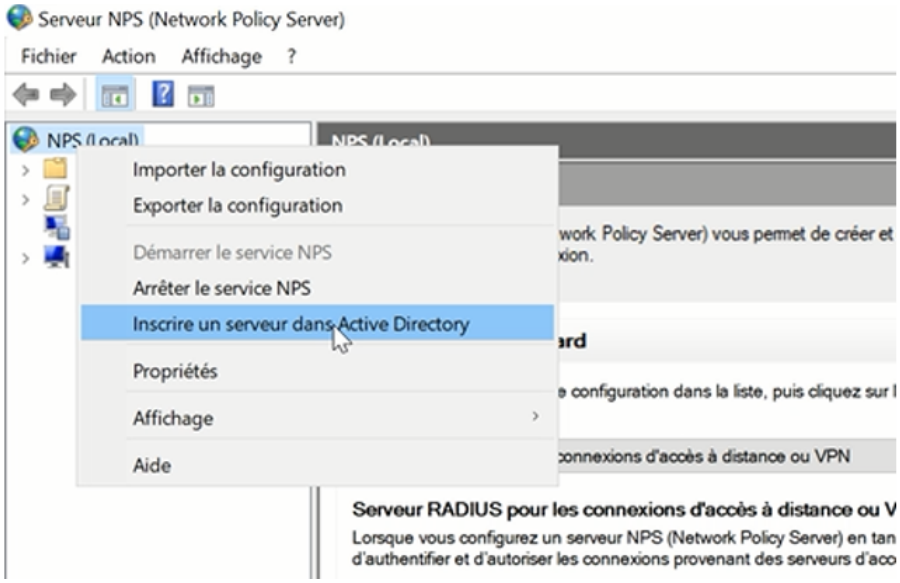


FIGURE 4.40 – Inscription du serveur NPS dans Active Directory.

4.7.3 Création des clients RADIUS

Les clients RADIUS jouent un rôle d'intermédiaire entre le serveur RADIUS et le client (utilisateur).

Pour créer des clients RADIUS, on accède à NPS, puis on se rend dans la section "Clients et serveurs RADIUS". Ensuite, on fait un clic droit sur "Client RADIUS" et on sélectionne l'option "Nouveau". Dans la fenêtre qui s'affiche, on saisit un nom, une adresse IP et une clé partagée.

L'étape de la création du client Radius est montrée dans la figure 4.41.

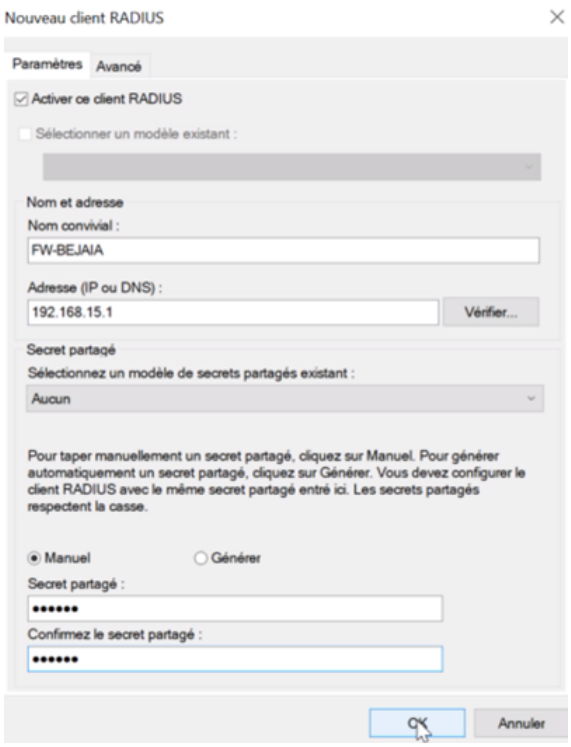


FIGURE 4.41 – Création d'un client radius.

L'ensemble des clients radius crées sont illustrés dans la figure 4.42.

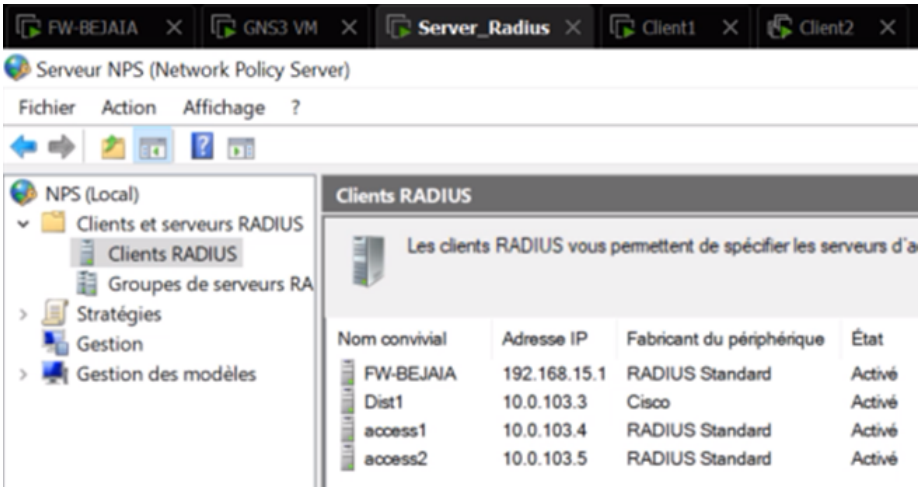


FIGURE 4.42 – Ensemble de clients.

La table 4.1 représente le clients Radius et leur adresses IP.

CLients RADIUS	Adresse IP
access1	10.0.103.4
access2	10.0.103.5
Core1	10.0.103.1
FWBEJAIA	192.168.15.1

TABLE 4.1 – Clients Radius et leurs adresses IP.

4.7.4 Configuration de la 802.1X des stratégies des connexions RADIUS

Pour configurer la norme 802.1X, on accède à NPS et on sélectionne le scénario de configuration "Serveur RADIUS pour la connexion câblée ou sans fil 802.1X". Ensuite, on clique sur "Configurer 802.1X" pour procéder à la configuration spécifique de cette norme. Voir la figure 4.43.

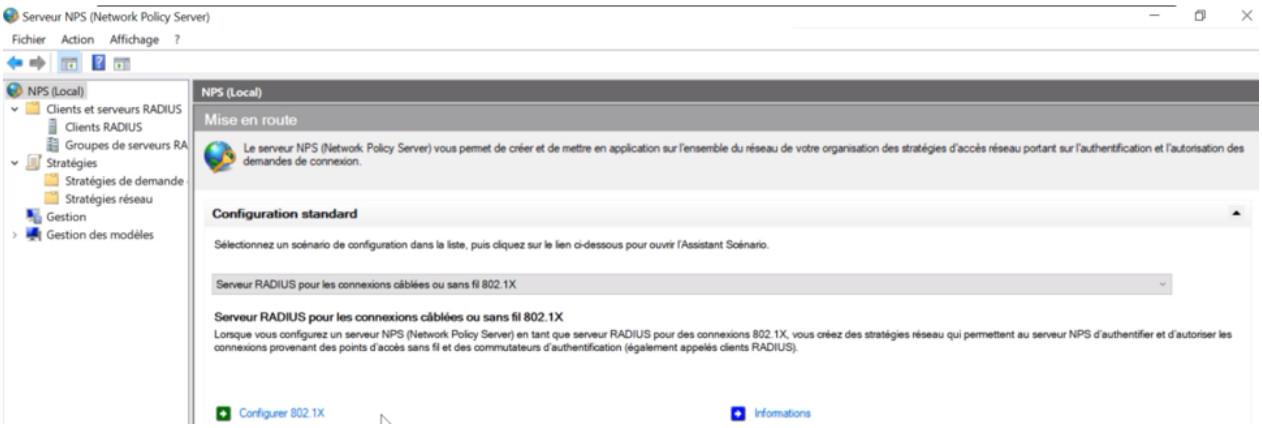


FIGURE 4.43 – Sélection d'un scenario de configuration.

Dans la figure 4.43, on choisit le type de connexion 802.1X, puis on coche la case correspondant aux "Connexions câblées (Ethernet) sécurisées". Ensuite, on donne un nom à la politique que nous avons créée, On commence par le Vlan 100. et enfin, on clique sur le bouton "Suivant" montré dans la figure 4.44.

FIGURE 4.44 – Type de connexion 802.1X.

Nous ajoutons nos clients RADIUS en cliquant sur ajouter. comme le montre la figure 4.45.

FIGURE 4.45 – Ajout de client Radius.

Pour le type de protocole EAP de cette stratégie, on sélectionne "Microsoft : PEAP (Protected EAP)". Ensuite, on clique sur "Configurer" et on ajoute la méthode d'authentification "Carte à puce ou autre Certificat". Enfin, on appuie sur "Suivant" pour continuer. Voir la figure 4.46.

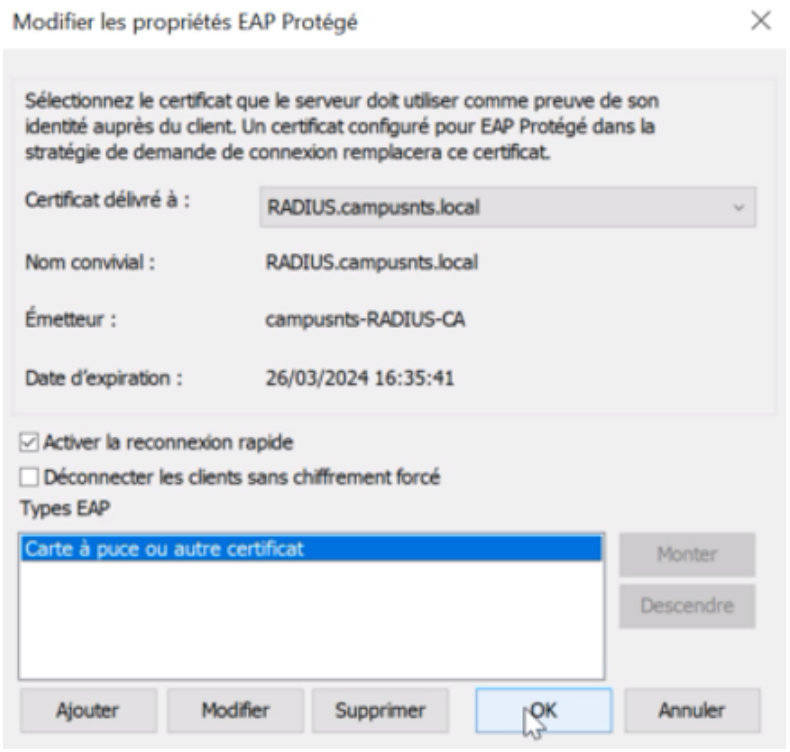


FIGURE 4.46 – Méthode d'authentification pour cette stratégie.

La figure 4.47 montre l'étape de l'ajout de Vlan100.

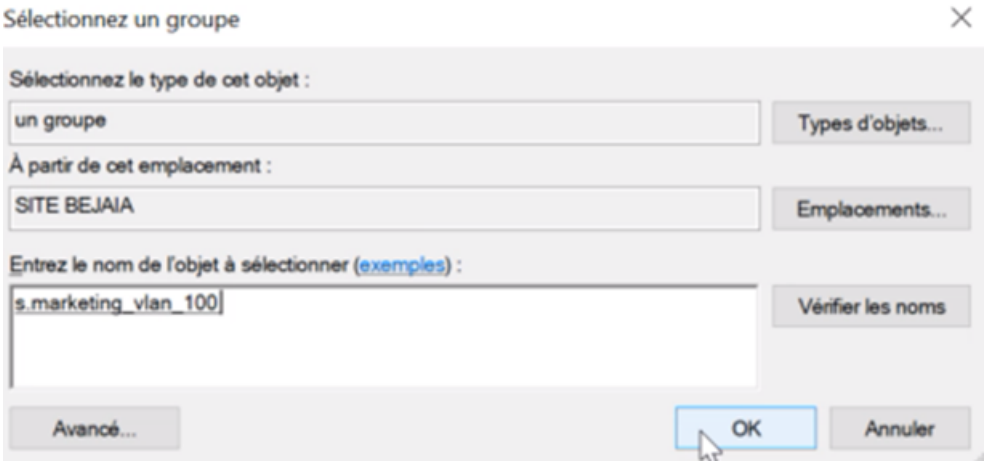


FIGURE 4.47 – Ajout de Vlan 100.

La figure 4.48 montre la configuration des attributs RADIUS.

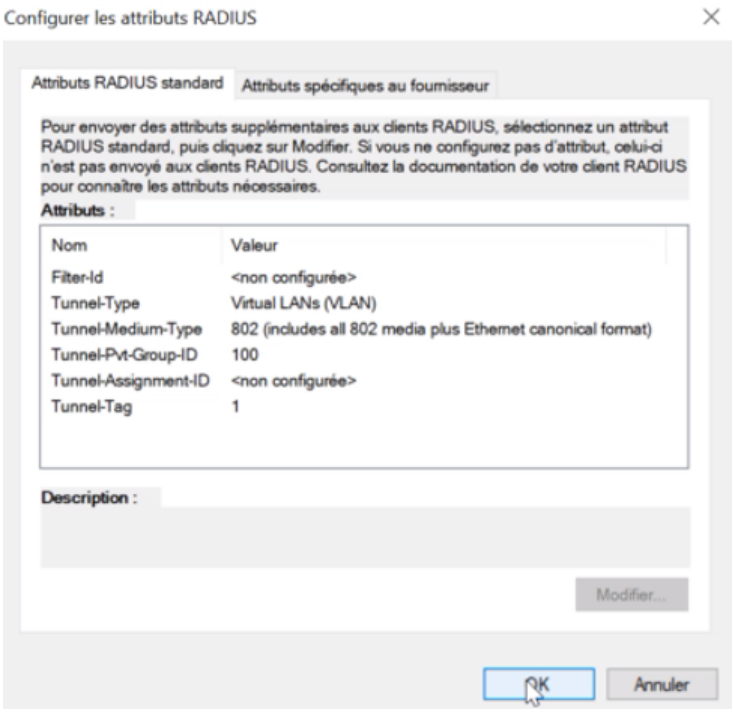


FIGURE 4.48 – Configuration des attributs RADIUS.

Dans NPS, nous accédons aux stratégies, puis aux stratégies de demande de connexion. Ensuite, nous sélectionnons les connexions câblées. Nous allons dans les conditions et choisissons le type de port NAS. Nous appuyons sur "Ajouter" pour ajouter les adresses de nos clients NAS, en ajoutant l'adresse 10.0.103.4 et l'adresse 10.0.103.5. Enfin, nous cliquons sur "OK" puis sur "Appliquer" pour valider les modifications. Voir la figure 4.49.

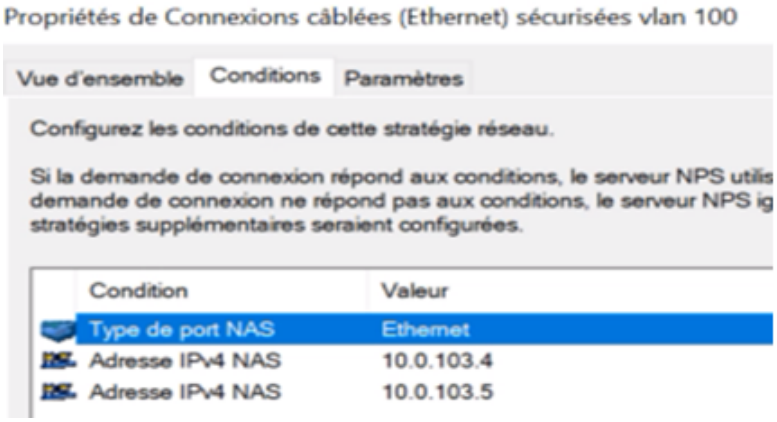


FIGURE 4.49 – Client NAS.

Une fois que nous avons créé notre stratégie réseau pour le VLAN 100, nous procédons à la duplication de cette stratégie pour les autres VLANs 101, 102, et 103. Pour chaque duplication, nous renommons la stratégie de manière appropriée et effectuons les modifications nécessaires. Cela inclut l'ajout des VLANs correspondants à chaque stratégie. Les différentes stratégies réseaux ajoutées sont montrées dans la figure 4.50.

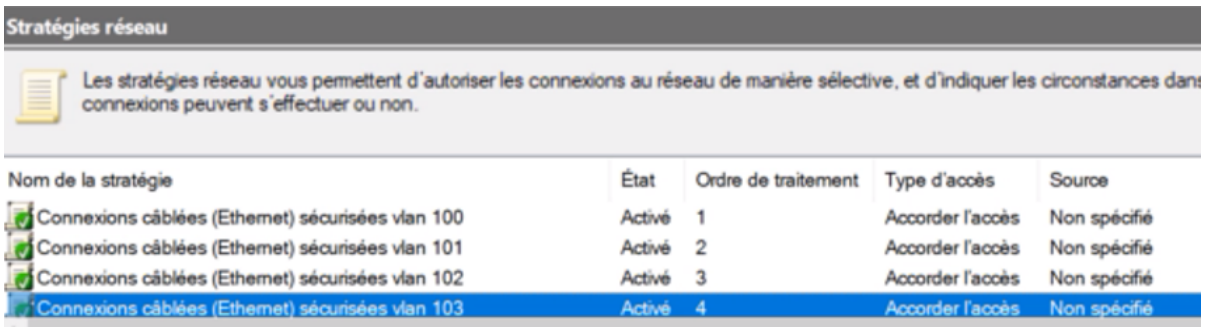


FIGURE 4.50 – Ensemble des stratégies réseaux.

Voici un tableau récapitulatif des stratégies que nous avons créées et les utilisateurs correspondants :

Nom de la stratégie	Utilisateurs coresspondant
connexion cablées(Ethernet) sécurisées Vlan 100	S.Marketing_Vlan_100
connexion cablées(Ethernet) sécurisées Vlan 101	S.Comptabilité_Vlan_101
connexion cablées(Ethernet) sécurisées Vlan 102	S.Informatique_Vlan_100
connexion cablées(Ethernet) sécurisées Vlan 103	Gestion_Vlan_103

TABLE 4.2 – Différentes stratégies et leur groupes assiciés.

Ce tableau résume les différentes stratégies que nous avons configurées, en associant chaque stratégie à un groupe spécifique d'utilisateurs.

4.7.5 Configuration du client

Pour la configuration du client nous allons procéder comme suit :

•**Activation de AAA** : En utilisant "aaa new-model", nous activons les commandes AAA et configurons le serveur RADIUS. Ensuite, nous définissons le groupe de serveurs pour l'authentification et attribuons des autorisations aux utilisateurs. Comme suit :

```
S1(config)#aaa new-model
S1(config)#aaa authentication dot1x default group radius
S1(config)#aaa authorization network default group radius
S1(config)#
```

FIGURE 4.51 – Configuration AAA.

•**Connexion serveur** : Sur le switch, nous allons activer l'authentification par mot de passe. La figure suivante illustre le processus d'activation de l'authentification sur le switch.

```
S1(config)#radius server RADIUS
S1(config-radius-server)#address ipv4 10.0.103.100
S1(config-radius-server)#key 0 RADIUS
S1(config-radius-server)#end
```

FIGURE 4.52 – Connexion server.

•**Activation DOT1X sur switch** : Pour activer le contrôle des ports en vue de l'authentification 802.1x. On va formuler la commande suivante :

```
S1(config-if-range)#dot1x system-auth-control
```

FIGURE 4.53 – Activation DOT1X sur switch.

•**Configuration de port** : L'activation de l'authentification 802.1X sur le port est représentée par la figure 4.54.

```
S1(config)#interface range ethernet 3/2-3
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport nonegotiate
S1(config-if-range)#authentication port-control auto
S1(config-if-range)#authentication open
S1(config-if-range)#dot1x pae authenticator
S1(config-if-range)#end
```

FIGURE 4.54 – Configuration de port.

4.8 Configurations OpenVPN

Nous avons suivi les étapes illustrées dans la figure 4.55 pour configurer l'accès à distance avec OpenVPN.

FIGURE 4.55 – Etapes de la Configurations OpenVPN.

4.8.1 Ajout du server

Dans pfSense, on accède à la section "VPN" et on choisit "OpenVPN". Ensuite, on va sur "wizard" et on sélectionne le type de serveur "RADIUS" en lui donnant le nom "radi". On specifie l'adresse correspondante et on conserve les ports par défaut. Enfin, on définit un mot de passe.La figure 4.56 montre l'ajout du server.

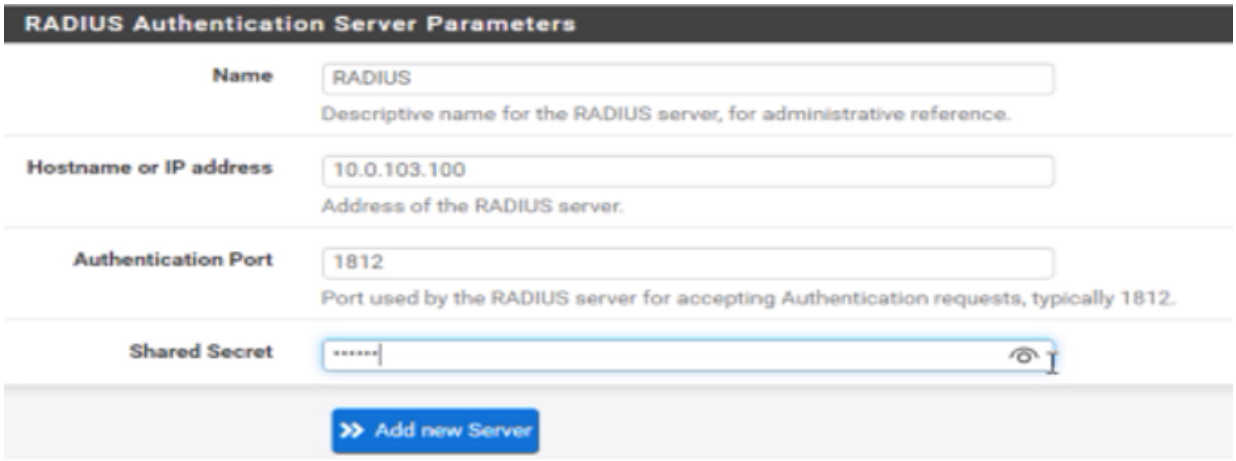


FIGURE 4.56 – Ajout du server.

4.8.2 Création de l'autorité de certificat

Ensuite, nous avons créé une autorité de certificat que nous avons nommée "CA_CONNEXION_VPN". La figure 4.57 indique la création de l'autorité de certificat.

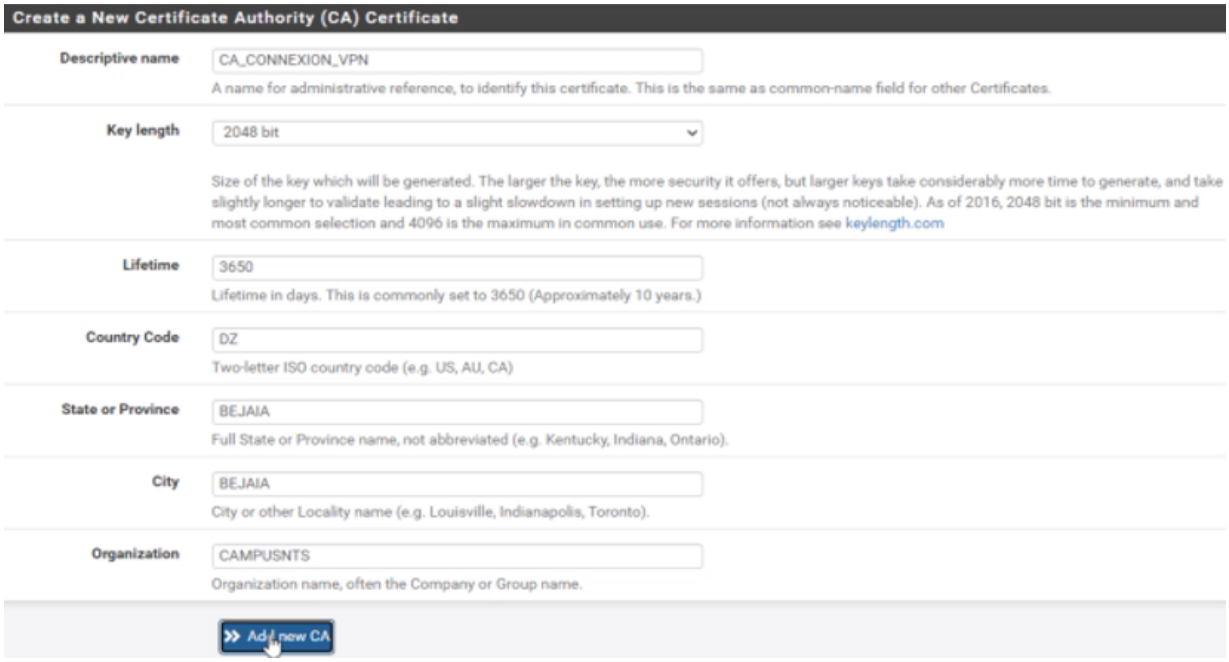


FIGURE 4.57 – Création de l'autorité de certificat.

4.8.3 Création de certificat server

Après cela, nous avons créé un certificat de serveur que nous avons nommé "certificate_server_vpn-radius". La figure 4.58 illustre la création de certificat server.

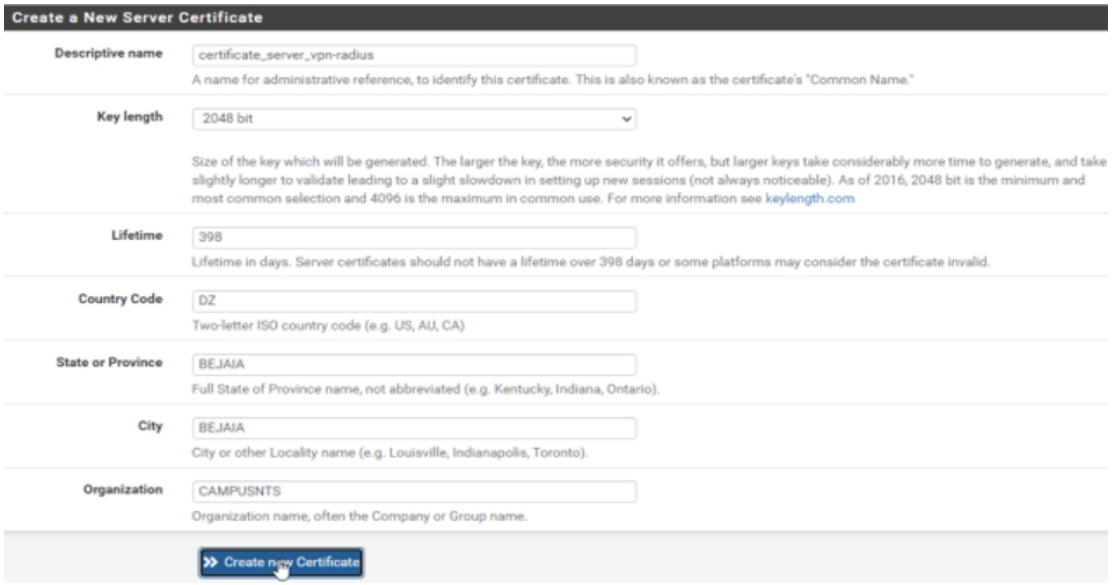


FIGURE 4.58 – Création de Certificat server.

4.8.4 Création de server VPN

Nous avons poursuivi les configurations jusqu'à la fin, et voilà, notre serveur VPN est maintenant créé avec succès. La figure 4.59 montre le server VPN crée.

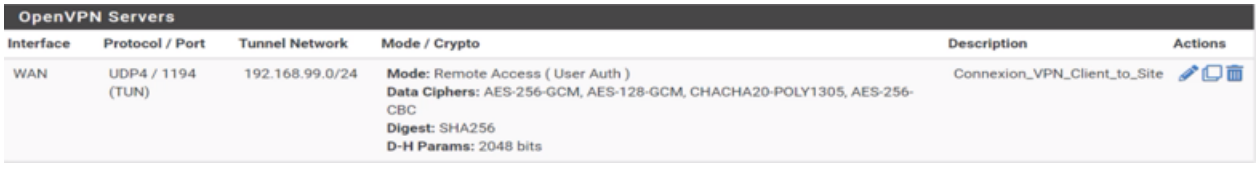


FIGURE 4.59 – Server VPN crée.

Configurer les utilisateurs orienté vers server RADIUS. Voir la figure 4.60.

FIGURE 4.60 – Server d'authentification .

4.8.5 Installation de OpenVPN

Nous procédons à l'installation d'OpenVPN. Commme indiqué dans la figure 4.61.

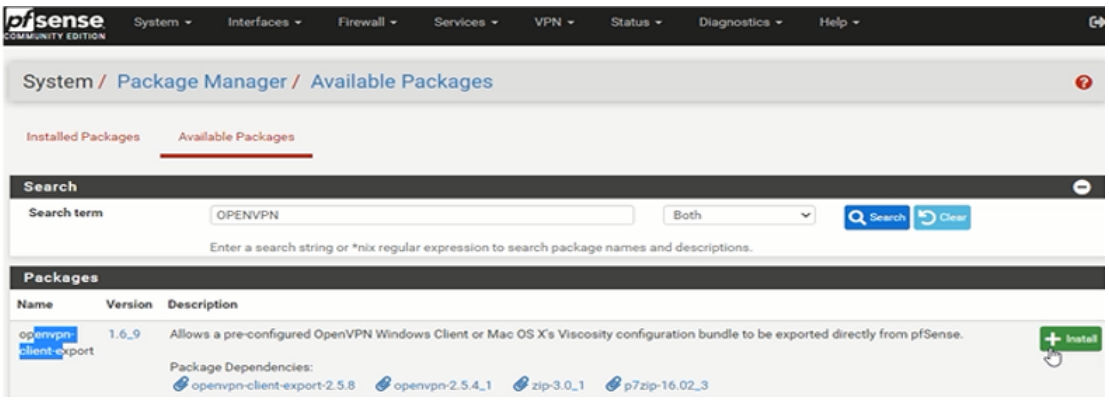


FIGURE 4.61 – Installation OpenVPN.

Ensuite, nous procédons à l'installation d'OpenVPN sur la machine. Voir la figure 4.62.

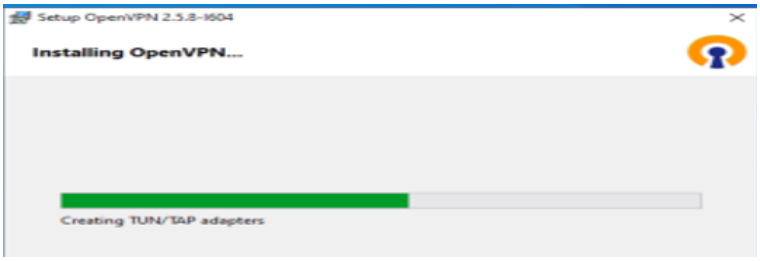


FIGURE 4.62 – Installation OpenVPN sur la machine.

4.8.6 Création de groupe VPN

Pour créer un nouveau groupe d'utilisateurs dans Active Directory, on accède à la console "Utilisateurs et groupes d'Active Directory". Ensuite, on sélectionne l'unité d'organisation "SITE BEJAIA". On fait un clic droit sur "Utilisateurs", on choisit "Nouveau" puis "Groupe". On donne un nom au groupe "Acces VPN". Comme le montre la figure 4.63.

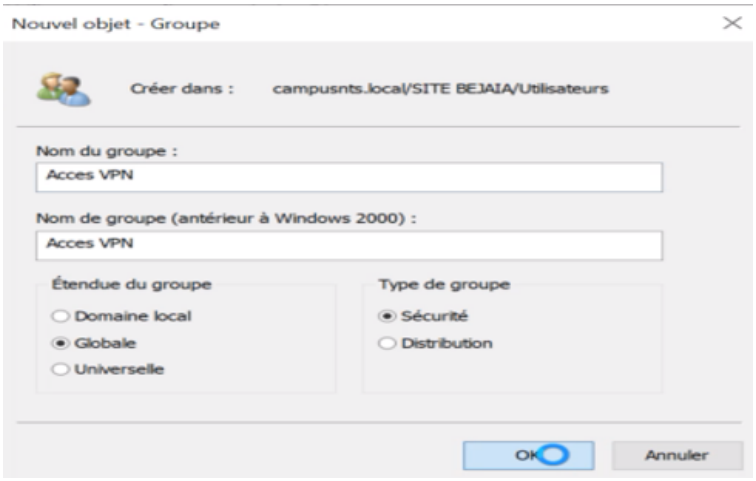


FIGURE 4.63 – Création groupe accès VPN.

Nous ajoutons Saidi Serine et SabrachouNumidia en tant que membres de ce groupe que nous venons de créer. Voir la figure 4.64.

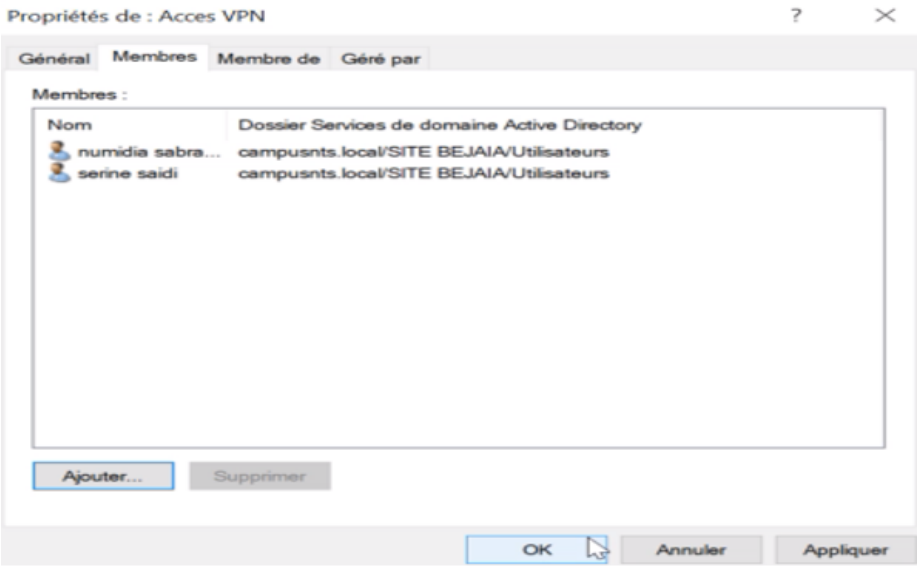


FIGURE 4.64 – Ajout de membres au groupe.

4.8.7 Configuration de la 802.1X pour VPN

Sur NPS, nous sélectionnons le type de connexion 802.1X, puis nous activons l'option "Connexions câblées (Ethernet) sécurisées". Nous attribuons un nom à la politique que nous avons créée, "accès VPN". Comme indiqué dans la figure 4.65.

FIGURE 4.65 – Stratégie accès VPN.

Ensuite, nous ajoutons "FW-BEJAIA". Voir la figure 4.66.

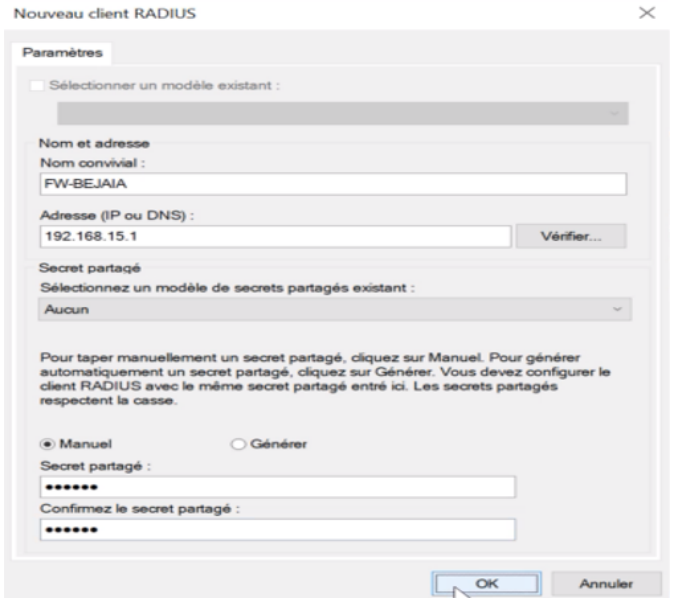


FIGURE 4.66 – Ajout de "FW-BEJAIA".

La figure 4.67 montre la méthode d'authentification que nous avons choisi.

FIGURE 4.67 – Méthode d'authentification.

Ensuite, on ajoute le groupe "Acces VPN". Comme le montre la figure 4.68.

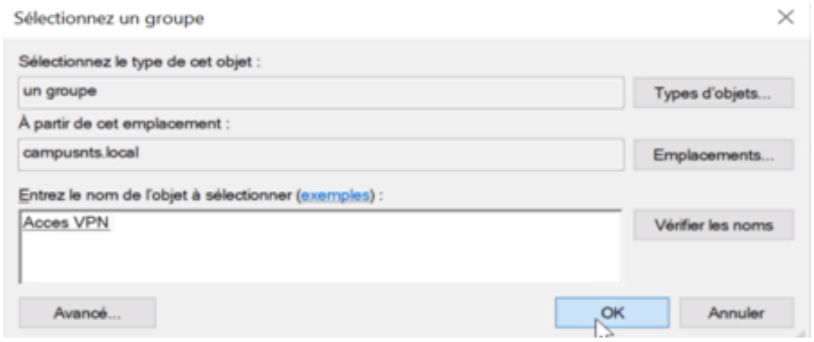


FIGURE 4.68 – Ajout du groupe "Acces VPN".

FIGURE 4.69 – Fin de la configuration.

Voilà, la stratégie "accès VPN" a été créée avec succès.

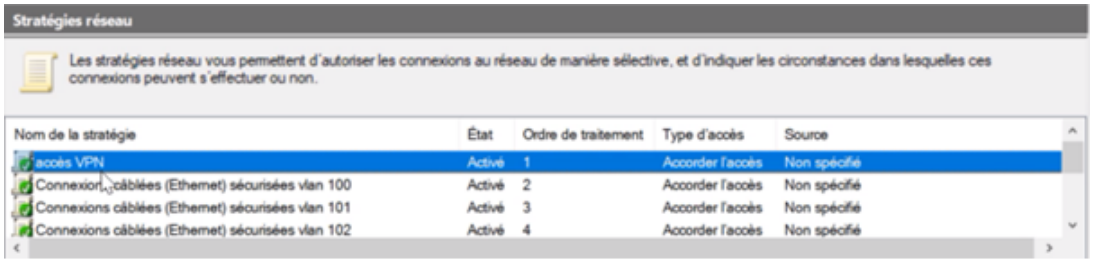


FIGURE 4.70 – Stratégie "accès VPN".

Ensuite, on procède à la configuration de notre stratégie en utilisant l'option "login", puis

on applique les paramètres en cliquant sur "OK". Voir la figure 4.71.

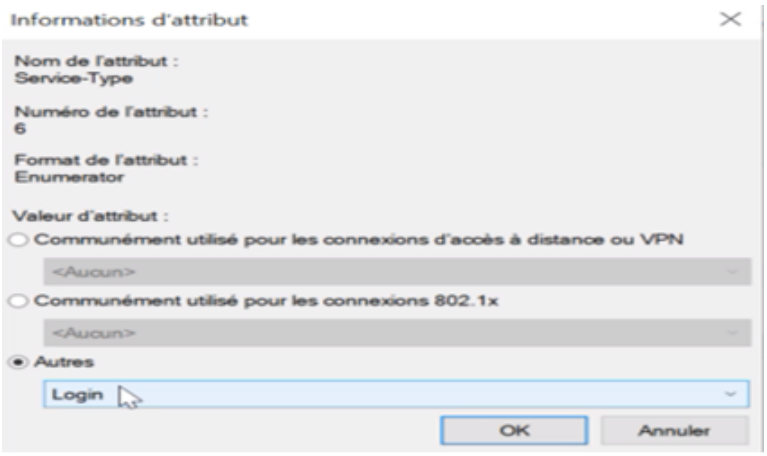


FIGURE 4.71 – Attribut LOGIN.

4.9 Configurations de SSH

Les étapes nécessaires pour configurer SSH sont illustrées dans la figure 4.72.

FIGURE 4.72 – Etapes de la Configurations de SSH.

4.9.1 Création de Groupe SSH

La figure 4.73 montre la création de groupe accès SSH.

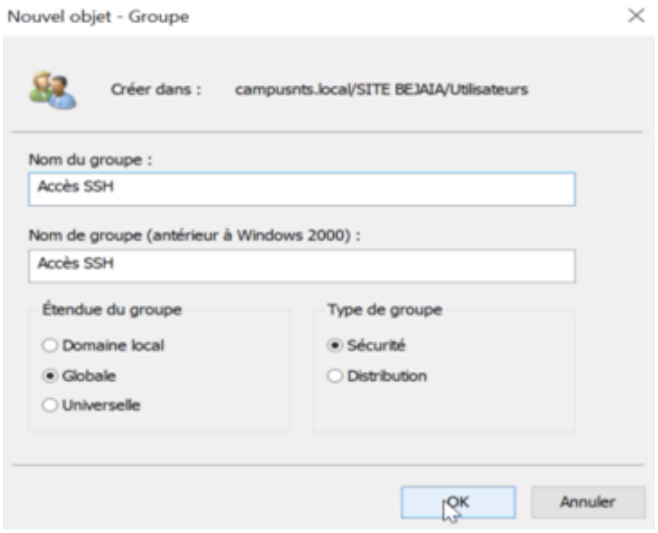


FIGURE 4.73 – Création de groupe accès SSH.

Nous ajoutons Saidi Serine et Sabrachou Numidia en tant que membres de ce groupe que nous venons de créer comme l'indique la figure 4.74.

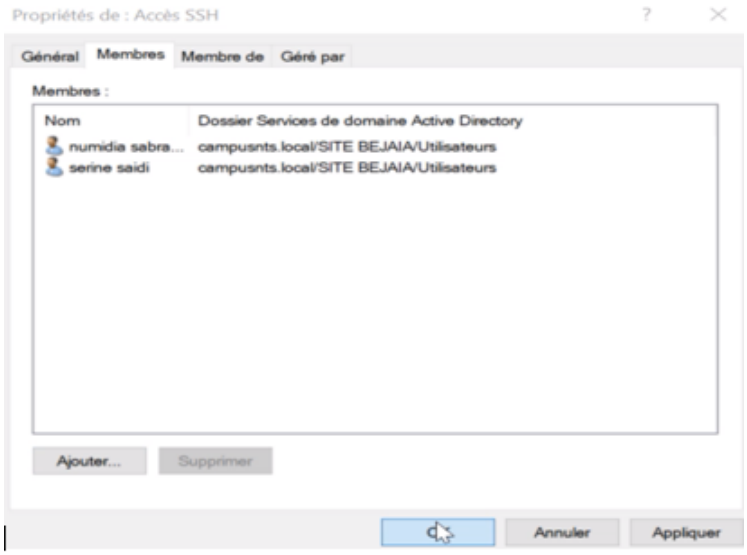


FIGURE 4.74 – Ajout de membres au groupe.

4.9.2 Configuration de la 802.1X pour SSH

Dans NPS, nous allons créer une stratégie SSH comme suit :

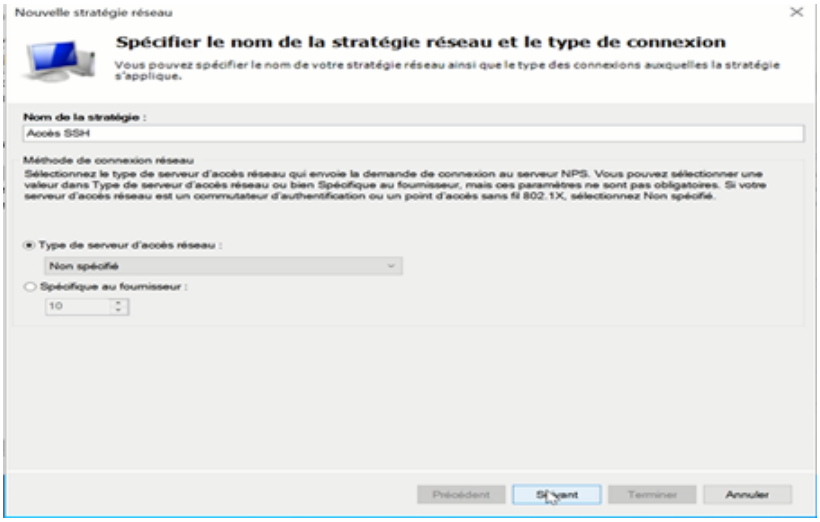


FIGURE 4.75 – Stratégie accès SSH.

Ensuite, nous ajoutons "Core1". Comme indiqué dans la figure 4.76.

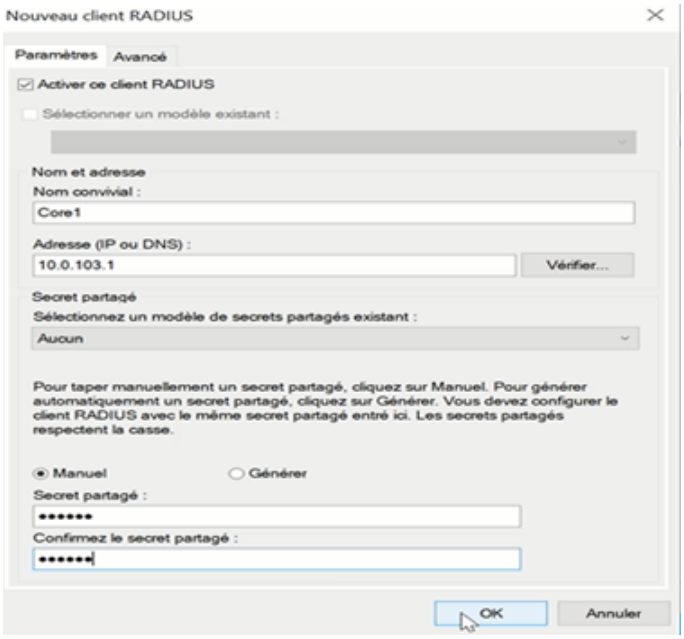


FIGURE 4.76 – Ajout de "Core1".

On sélectionne la méthode d'authentification avec mot de passe, puis, on ajoute le groupe

"Acces SSH". Voir la figure 4.77.

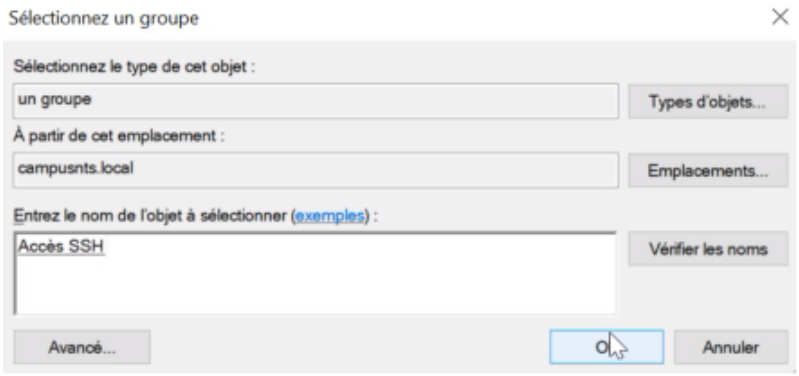


FIGURE 4.77 – Ajout du groupe "Acces SSH".

La stratégie "accès SSH" a été créée avec succès. Voir la figure 4.78.

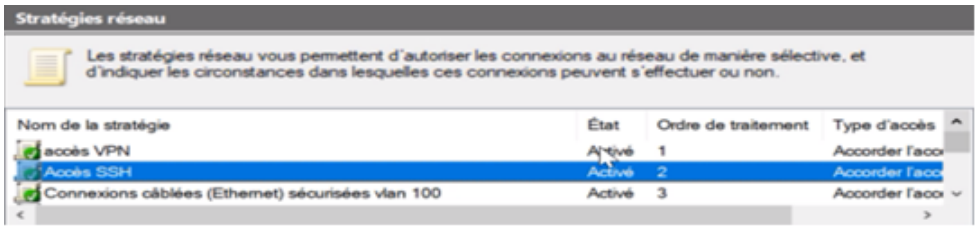


FIGURE 4.78 – La stratégie "accès SSH".

4.9.3 Configuration AAA sur le routeur core1

Pour configurer le protocole AAA, on utilise les commandes suivantes :

aaa new-model : Est utilisée pour activer la fonctionnalité AAA sur Core1.

aaa authorization exec default group radius local : Cette commande est utilisée pour configurer les règles d'autorisation pour les sessions d'exécution (exec) sur Core1.

aaa authentication login default enable : Est utilisée pour configurer la méthode d'authentification par défaut pour les connexions de login sur Core1.

aaa authorization network default group radius local : Est utilisée pour configurer les règles d'autorisation pour les connexions réseau sur Core1. La figure 4.79 montre la configuration AAA sur retour core1.

```
core1(config)#
core1(config)#aaa new-model
core1(config)#aaa authorization exec default group radius local
core1(config)#aaa authentication login default enable
core1(config)#aaa authorization exec default group radius local
core1(config)#aaa authorization network default group radius local
core1(config)#
```

FIGURE 4.79 – Configuration AAA sur le routeur core1.

4.9.4 Connexion routeur sur RADIUS

```
core1(config)#
core1(config)#radius server RADIUS
core1(config-radius-server)#address ipv4 10.0.103.100
core1(config-radius-server)#key RADIUS
core1(config-radius-server)#
core1(config-radius-server)#
```

FIGURE 4.80 – Connexion routeur sur RADIUS .

4.9.5 Configuration SSH

Pour configurer le protocole SSH sur Core1, on utilise les commandes suivantes :

ip domain-name capmusnts.ssh : Configure le nom de domaine pour Core1, dans notre cas le nom du domaine est campusnts.ssh.

crypto key generate rsa modulus 1024 : Est utilisée pour générer une paire de clés RSA d'une taille de 1024 bits pour Core1.

ip ssh version 2 : Est utilisée pour configurer la version du protocole SSH sur Core1.

line vty 0 4 : Est utilisée pour accéder aux lignes virtuelles de type vty qui sont utilisées pour permettre l'accès à distance à l'équipement via des protocoles tels que SSH, dans notre cas les lignes vty de 0 à 4 sont configurées.

transport input ssh : Est utilisée pour spécifier le protocole de communication autorisé sur lignes de 0 à 4 de type vty, dans notre cas on a autorisé le protocole SSH.

login authentication default : Est utilisée pour configurer la méthode d'authentification par défaut sur Core1.La figure 4.81 présente la configuration SSH.

```
core1(config)#
core1(config)#ip domain-name campusnts.ssh
core1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: core1.campusnts.ssh

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

core1(config)#
*May 19 19:33:32.240: %SSH-5-ENABLED: SSH 1.99 has been enabled
core1(config)#
core1(config)#ip ssh version 2
core1(config)#line vty 0 4
core1(config-line)#transport input ssh
core1(config-line)#login authentication default
core1(config-line)#exit
core1(config)#
```

FIGURE 4.81 – Configuration SSH.

4.9.6 Téléchargement et instalation putty

Pour télécharger PuTTY, il faut se rendre sur le site officiel de PuTTY. Une fois sur le site, on peut trouver la section de téléchargement et choisir la version de PuTTY adaptée à notre système d'exploitation. Voir la figure 8.82.

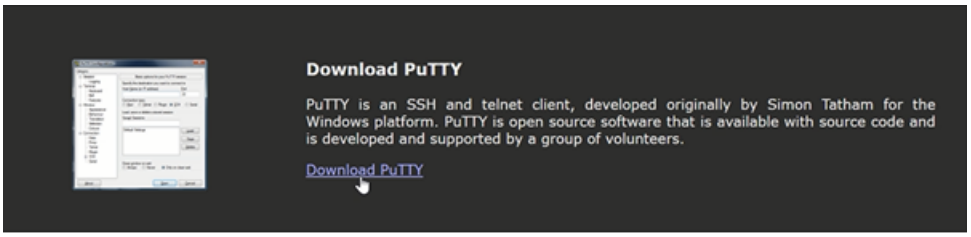


FIGURE 4.82 – Téléchargement Putty.

Une fois que le fichier de PuTTY a été téléchargé, on peut exécuter le programme d'installation en double-cliquant dessus. Cela lancera le processus d'installation de PuTTY. Comme l'indique la figure 4.83.

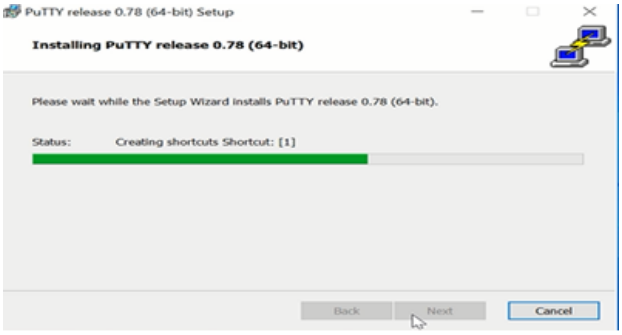


FIGURE 4.83 – Installation Putty.

4.9.7 Configuration putty

Une fois PuTTY installé, on peut procéder à sa configuration. Cela implique de spécifier les paramètres nécessaires tels que l'adresse IP du serveur, le port et le type de connexion ainsi que d'autres options de personnalisation selon nos besoins. Une fois la configuration terminée, on est prêt à utiliser PuTTY pour établir des connexions SSH. La figure 4.84 montre la configuration Putty.

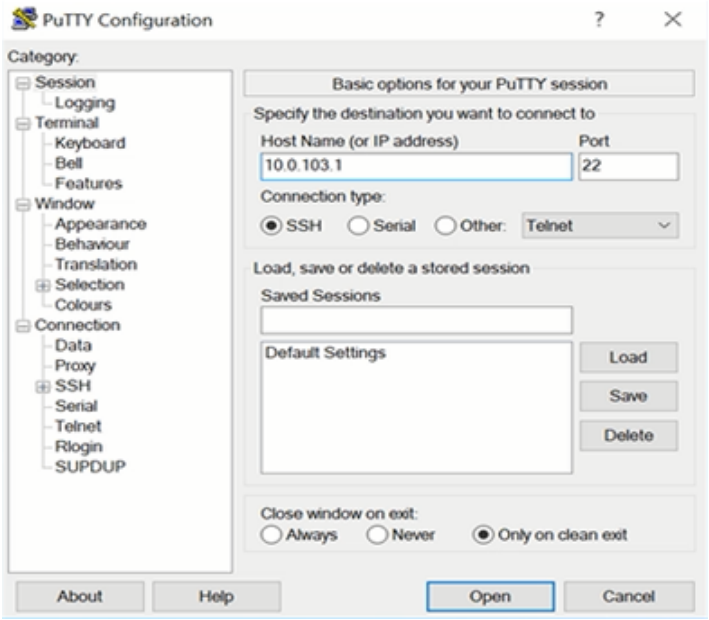


FIGURE 4.84 – Configuration Putty.

4.10 Tests

Dans cette phase de test, nous allons effectuer une série de tests. Tout d'abord, nous allons tester le DHCP à partir d'un PC, puis nous procéderons à la vérification de la stratégie depuis les clients 1 et 2. Ensuite, nous effectuerons des tests sur le VPN, et enfin, nous effectuerons des tests sur le SSH.

4.10.1 Tester DHCP depuis un PC

Pour tester le service DHCP,on verifie l'obtention des adresses IP pour chaque client.

On observe que le client1 a obtenu une adresse IP dans la plage réservée au VLAN 100 qu'on a créé,comme le montre la figure 4.85.

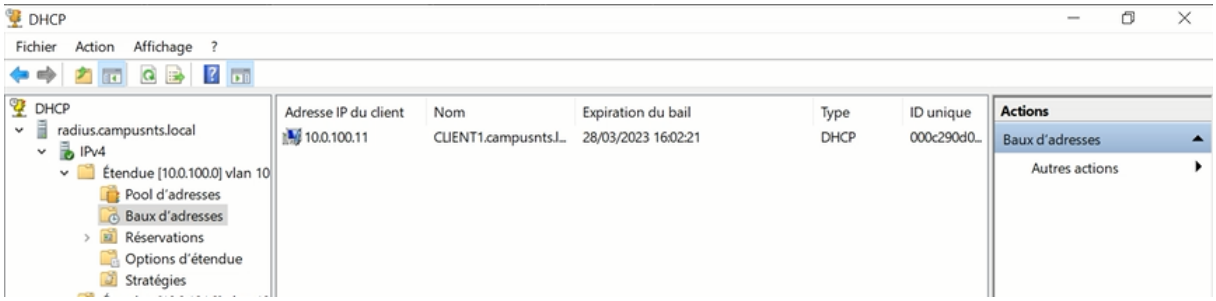


FIGURE 4.85 – Obtention de l'adresse IP pour client1 de VLAN 100.

On observe que le client2 a obtenu une adresse IP dans la plage réservée au VLAN 101 qu'on a créé,comme le montre la figure 4.86.

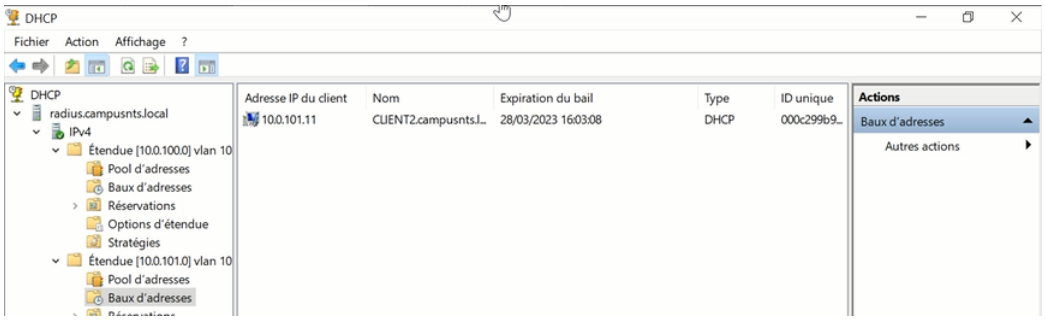


FIGURE 4.86 – Obtention de l'adresse IP pour client2 de VLAN 101.

4.10.2 Tester la stratégie depuis les client1 et client2

Pour savoir si le serveur RADIUS nous donnera l'acces, nous avons suivi les étapes suivantes

On a activé la carte réseau du client 1 comme le montre la figure 4.87.

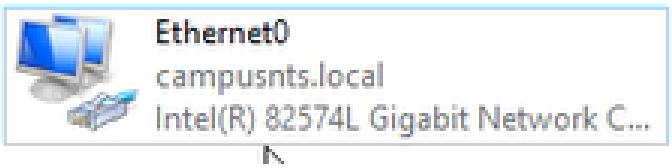


FIGURE 4.87 – Activation de la carte réseau du client1.

La figure 4.88 montre les détails de la réussite d'authentification du client1 en utilisant la commande "show athentification session interface ethernet 3/3".

```
access1#
access1#show  authentication sessions interface  ethernet 3/3 details
            Interface:  Ethernet3/3
          MAC Address:  000c.297a.4d97
         IPv6 Address:  Unknown
         IPv4 Address:  10.0.100.11
            User-Name:  host/CLIENT1.campusnts.local
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-domain
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0A00670400000000B00006988
      Acct Session ID:  Unknown
               Handle:  0xA0000001
       Current Policy:  POLICY_Et3/3

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

Server Policies:
          Vlan Group:  Vlan: 100

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

FIGURE 4.88 – Activation de la carte réseau du client1.

La figure 4.89 montre que RADIUS a accordé l'accès pour le client1.

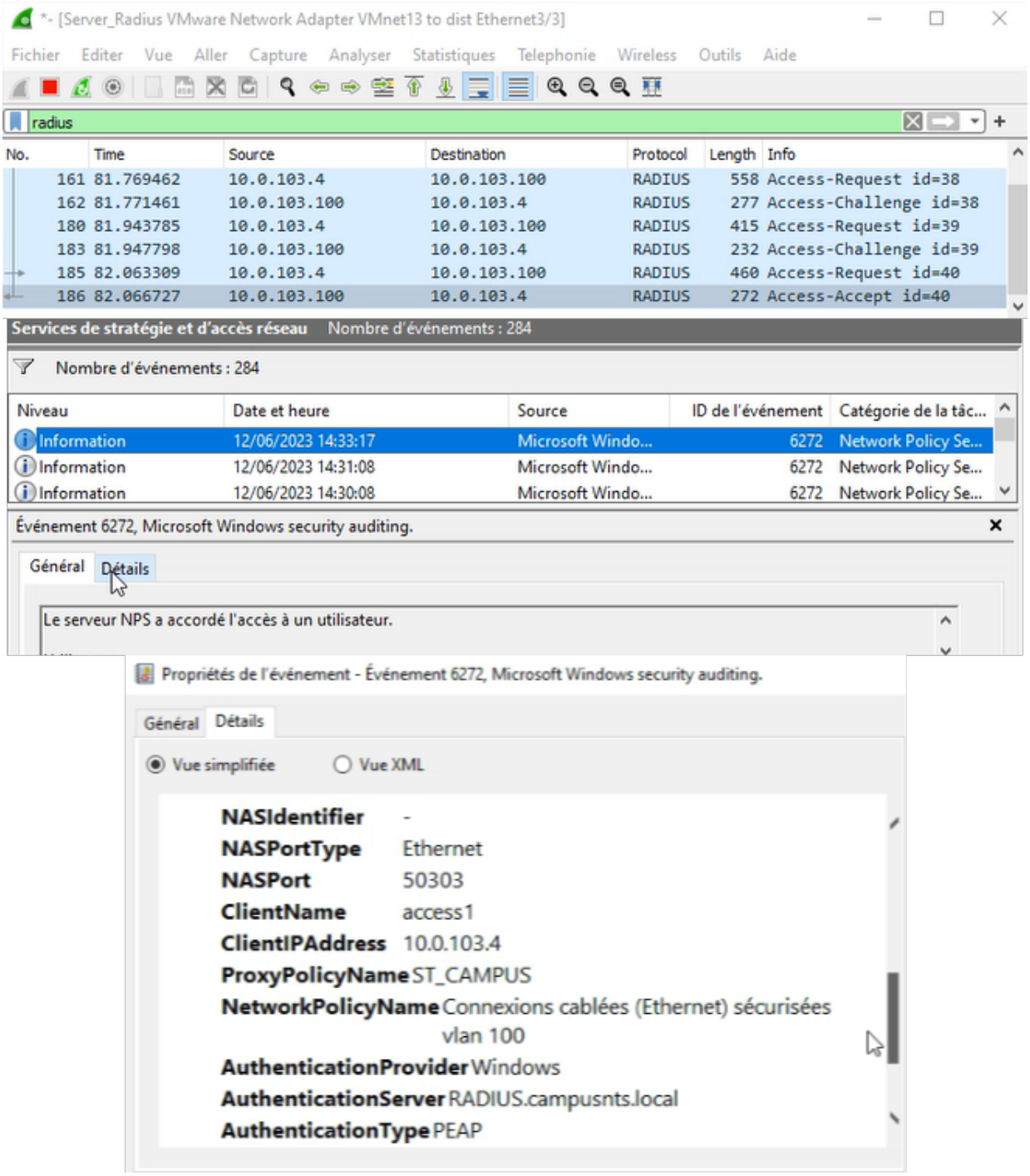


FIGURE 4.89 – RADIUS a accordé l'accès pour le client1 .

Nous nous rendons chez le client 2 qui est associé au VLAN101, nous le retirons et nous essayons de nous authentifier avec le VLAN100 à partir du client 2 (nous échangeons les VLAN). on observe dans la figure 4.90 que RADIUS a accordé l'accès pour le client 2 à partir du VLAN100.

```
access1#
access1#show  authentication sessions interface  ethernet 3/3 details
            Interface:  Ethernet3/3
          MAC Address:  000c.2946.da0c
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  host/CLIENT2.campusnts.local
               Status:  Authorized
               Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  0A0067040000000E0012533D
     Acct Session ID:  Unknown
               Handle:  0x87000003
      Current Policy:  POLICY_Et3/3

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

Server Policies:
          Vlan Group:  Vlan: 101

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

FIGURE 4.90 – RADIUS a accordé l'accès pour le client2 .

La figure 4.91 montre les détails de l'authentification du client2 à partir du VLAN100.

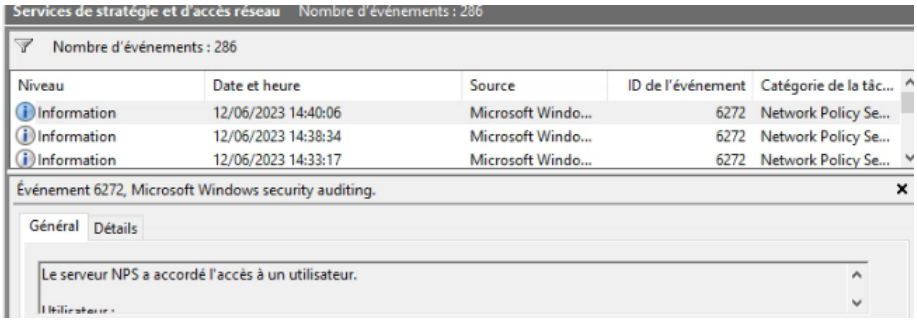


FIGURE 4.91 – Détails de l'authentification du client2 à partir du VLAN100.

Lorsque nous retirons le client 2 du service comptabilité, il sera bloqué lors de sa tentative d'authentification, ce qui entraînera un échec de l'authentification. La figure 4.92 montre l'échec d'authentification du client2 après sa suppression du service de comptabilté.

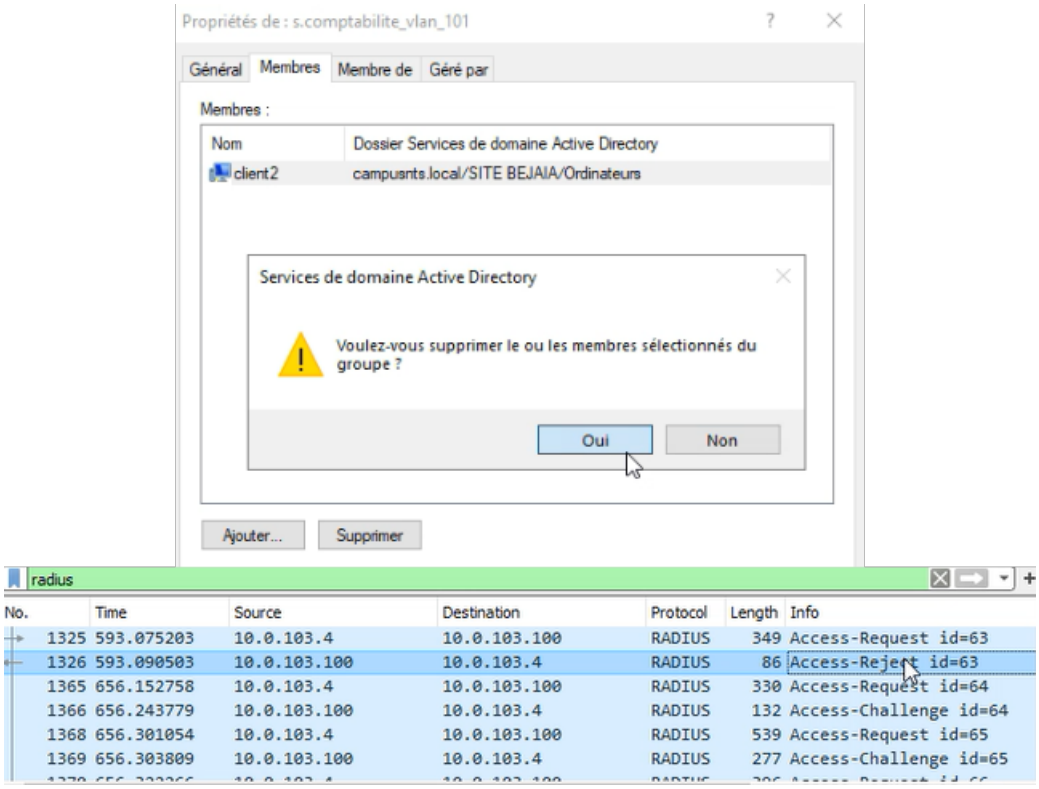


FIGURE 4.92 – Echec d'authentification du client2 après sa suppression .

4.10.3 Test VPN

Pour tester l'authentification des cleints VPN, nous exécutons une commande ping en direction du serveur RADIUS. Comme le montre la figure 4.93.

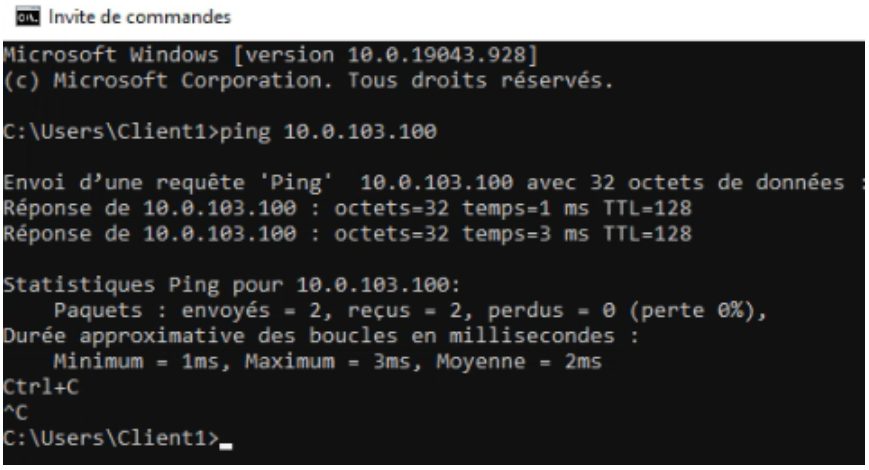


FIGURE 4.93 – PING vers le serveur RADIUS.

la figure 4.94 montre les étapes de connexion de l'utilisateur VPN "saidi serine" qui a réussi à s'auhthentifier.

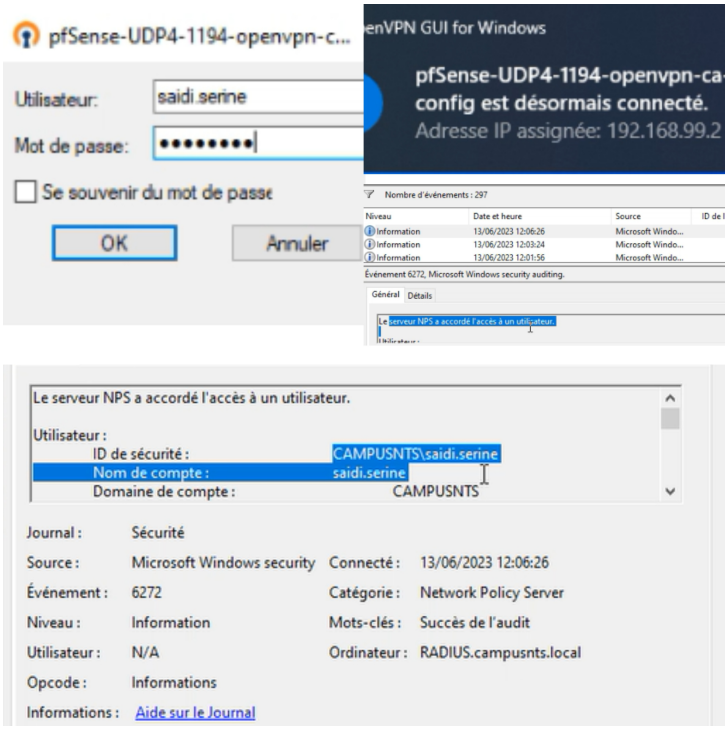


FIGURE 4.94 – Connexion réussie.

la figure 4.95 montre les étapes de connexion de l'utilisateur VPN "sabrachou numidia " qui a réussi à s'auhthentifier.

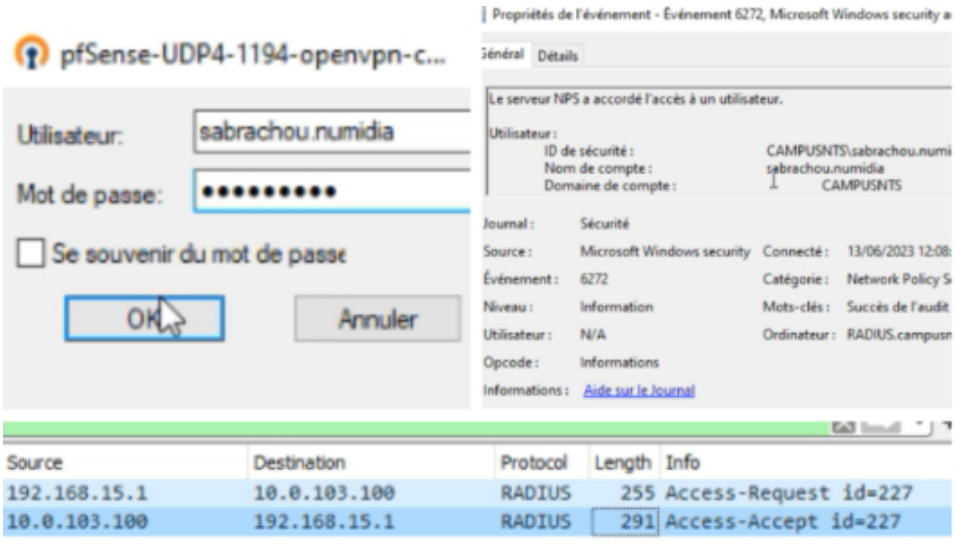


FIGURE 4.95 – Connexion réussie.

4.10.4 Test SSH

On peut accéder au routeur en utilisant un client SSH tel que PuTTY comme le montre la figure 4.96.

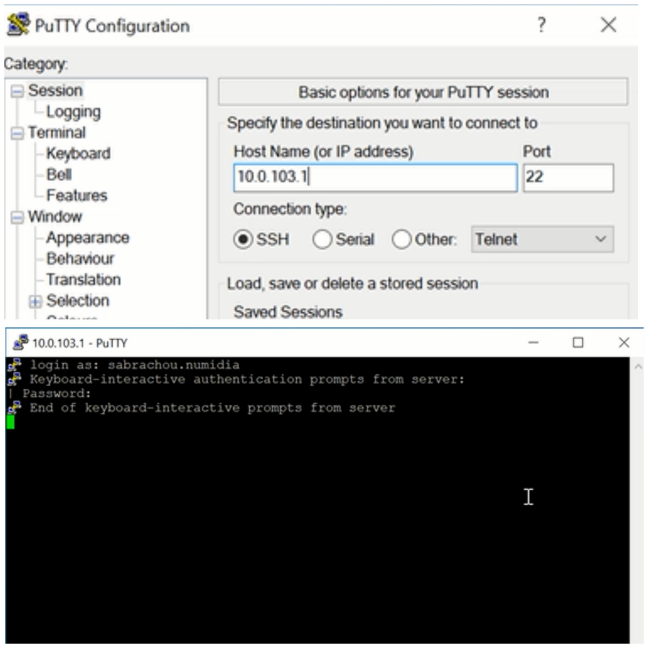


FIGURE 4.96 – Accéder au routeur Core1 par l'outil putty.

La figure 4.97 montre que le serveur RADIUS nous a donné un accès pour le client SSH "sabrachou numidia".

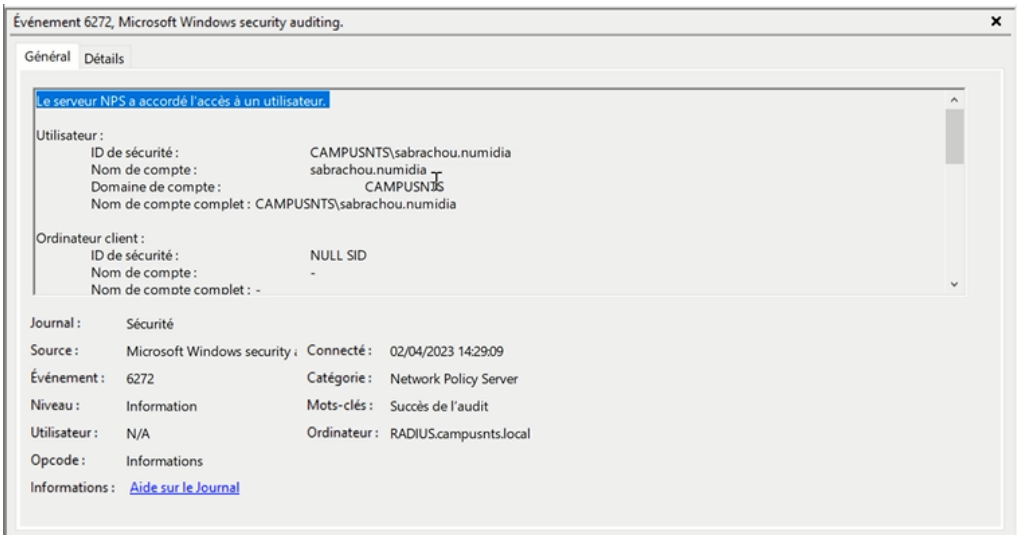


FIGURE 4.97 – Le serveur RADIUS a accordé l'accès à un l'utilisateur SSH "sabrachou numidia".

Conclusion générale

Le réseau informatique d'une entreprise est crucial car il permet l'échange de données entre les différents objets connectés. Cependant, il est essentiel de garantir la validité et la sécurité de ce réseau pour préserver l'activité de l'entreprise et éviter tout risque de perte d'authenticité.

Dans notre travail, nous avons proposé une solution une solution d'authentification pour le réseau Ethernet de l'entreprise Campus NTS. Pour cela, nous avons utilisé le protocole RADIUS, qui est reconnu comme l'un des protocoles d'authentification les plus efficaces. Par la suite nous avons segmenté le réseau en plusieurs VLANs pour une meilleure gestion.

Pour réaliser ce travail, nous avons utilisé l'environnement de simulation GNS3 pour configurer et tester la solution, ainsi qu'une machine virtuelle VMware sur laquelle nous avons installé une machine Windows 10 et un serveur Windows Server 2022.

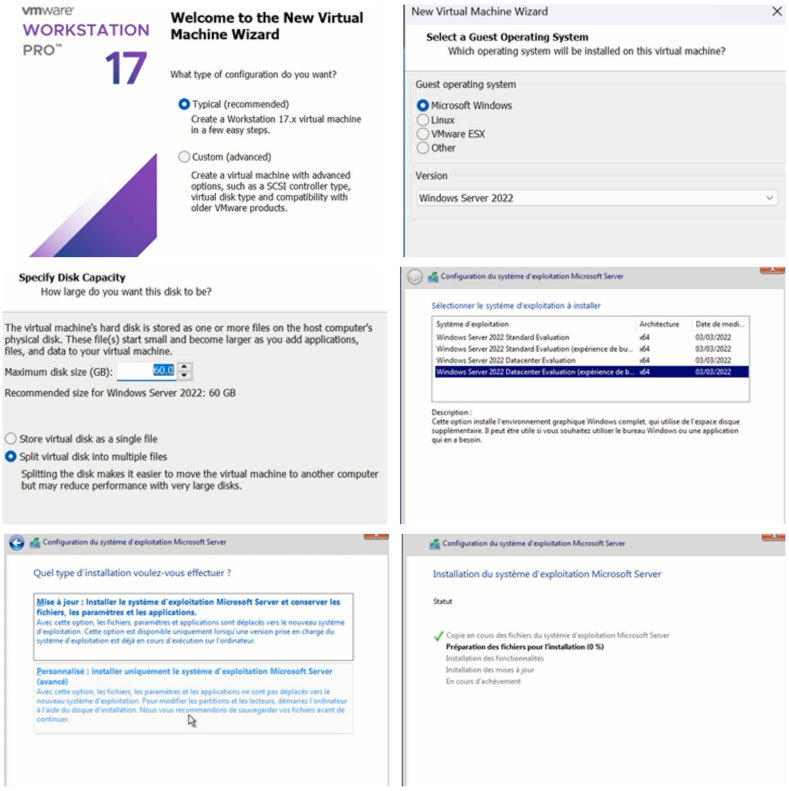
L'objectif final de notre travail était de mettre en place une solution d'authentification basée sur la norme 802.1X, en utilisant RADIUS et des certificats, pour sécuriser le réseau filaire de l'entreprise Campus NTS.

Annexes

Création des machines virtuelles

Installation du windows server sur vmware workstation

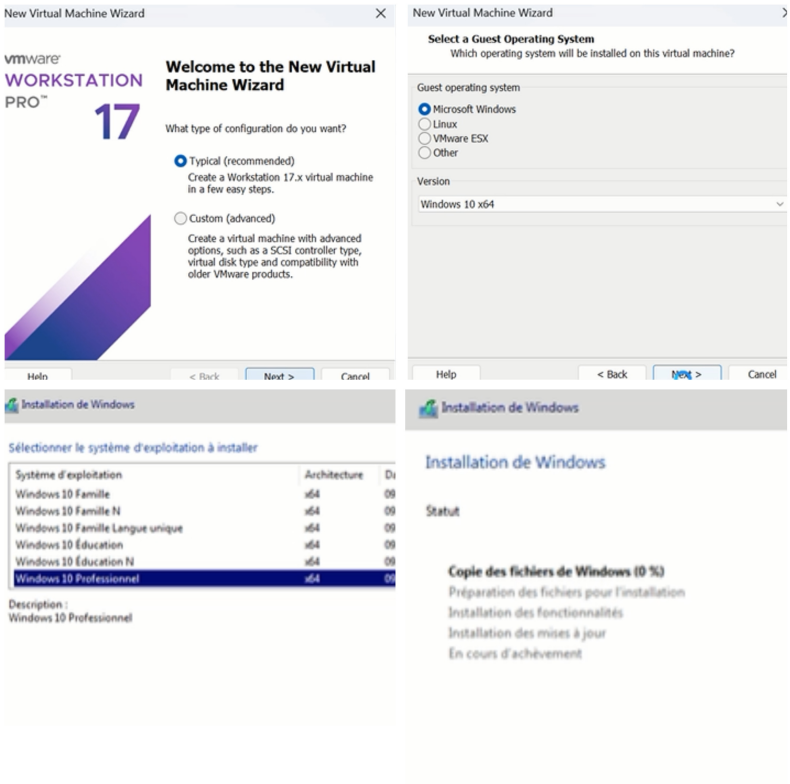
la figure suivante montre les étapes d'installation de Windows server 2017 sous le nom "server_Radius" avec les caractéristiques qu'on a attribué au serveur :



Etapes d'installation du Windows server 2017.

Installation de la machine virtuelle Windows 10

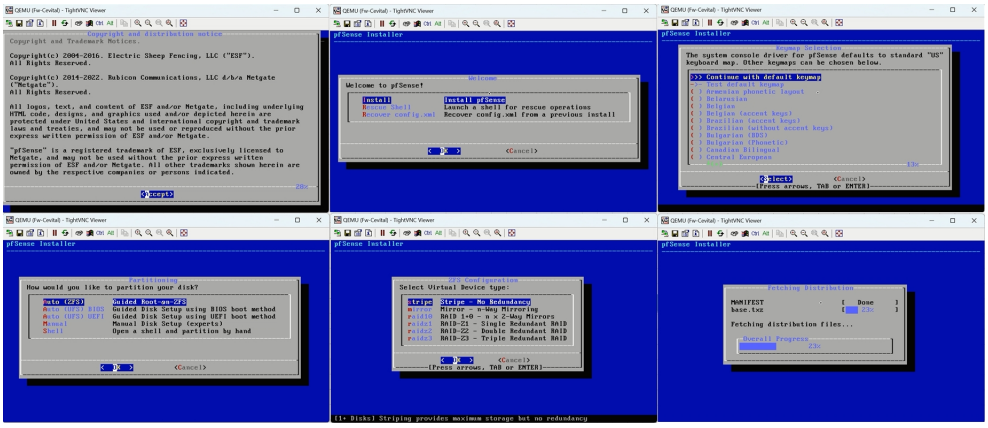
la figure suivante montre les étapes d'installation dU Windows 10 avec les caractéristiques qu'on a attribué :



Etapes d'installation de la machine virtuelle Windows 10.

Installation du pare-feu PfSense

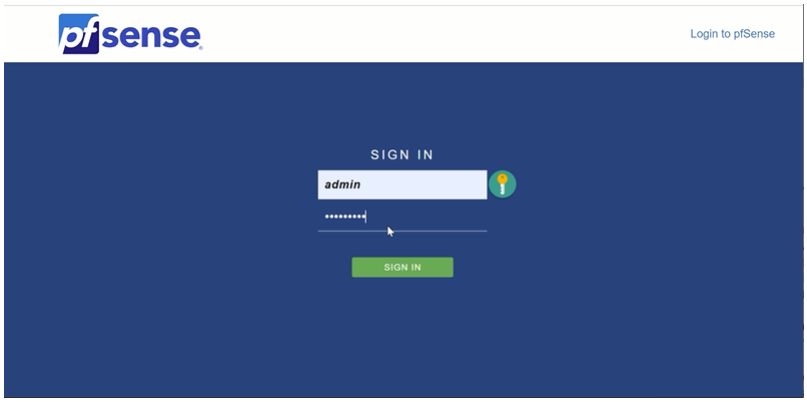
Tout d'abord, nous allons procéder à la création d'une machine virtuelle PFsense sur VMware, puis nous lancerons le processus d'installation.



Etapes d'Installation du pare-feu PfSense.

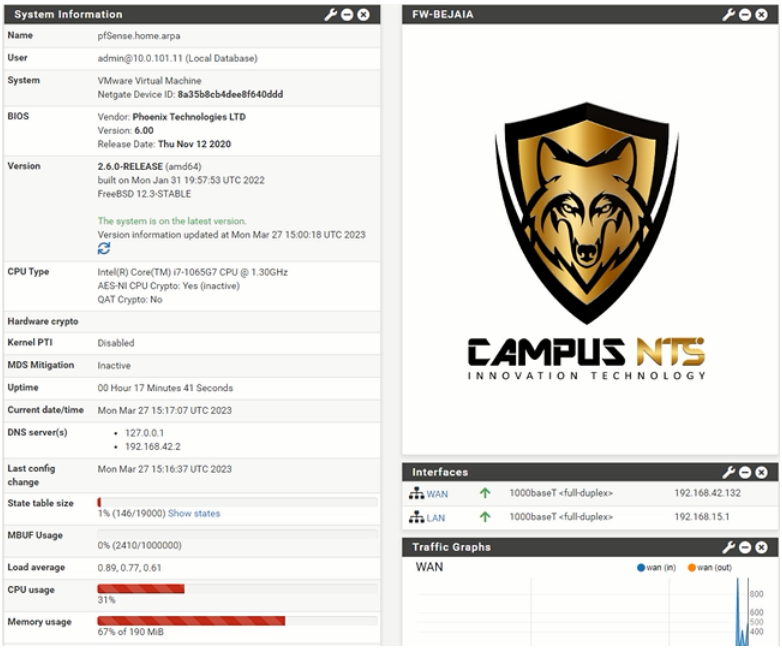
Une fois l'installation terminée, nous nous rendons sur le navigateur web afin de nous

connecter à l'interface de configuration Web de PfSense. Pour ce faire, nous utilisons l'adresse IP de l'interface LAN, à savoir https ://192.168.15.1 La figure suivante illustre la page d'identification.



Page d'authentification de Pfsense.

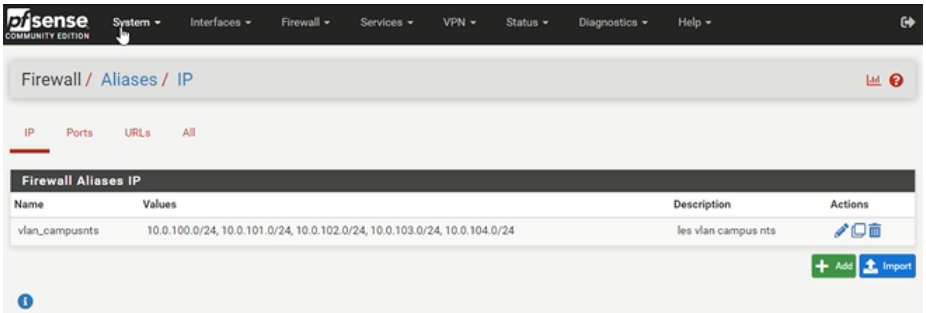
Après avoir introduit le mot de passe et le nomd'utilisateur(s'authentifier) l'interface d'accueil s'affichera comme l'illustre la figure ci-dessous :



Interface web d'accueil de Pfsense.

Ajout des vlans sur le pare-feu

Nous avons créé un alias appelé "vlan_campusnts" pour regrouper tous les VLAN sur le pare-feu. La Figure ci-dessous présente l'alias que nous avons créé pour cette configuration.



Ajout des VLANs sur PFsense.

Bibliographie

[1] Mr Farah, Cour introduction à la sécurité Master1 informatique, université de Bejaia.

[2] Solange Ghernaouti-Hélie, Livre "Sécurité informatique et réseaux", Dunod 3e édition 2008 .

[3] university of new southwales le protocole dhcp. Consultez le : https ://web.maths.unsw.edu.au/ lafaye/CCM/internet/dhcp.htm

[4] Qu'est-ce que le DNS ? sur le site cloudFlare. Consultez le : https ://www.cloudflare.com/fr-fr/learning/dns/what-is-dns/

[5] Fonctionnement de radius sur le site Cisco. Consultez le : https ://www.cisco.com/c/fr_ca/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.pdf

[6] Mr Mihoubi Mohamed et Mr Medjani Nacer, Thèse master 2 en électronique UMMTO,"Sécurisation d'une infrastructure lan/wan base d'équipement cisco", 2015.

[7] Claude Servin, Livre "Réseaux et télécom" 4e édition.

[8] Cour 3eme année licence académique en informatique.

[9] Co lyonnais, politique de certification, édition 2001.

[10] M. OMAR , Cours de sécurité informatique, Université de Bejaia, 2013.

[11] RFC 2865 RemoteAuthentication Dial In User Service (RADIUS).

[12] Mémoire de fin d'étudesMaster II en Informatique Option : Réseaux, Mobilité et systèmes embarqués. Thème : ■ Mise en place d'un système de sécurité basé sur l'authentification dans un réseau IP ■ l'université mouloud mammeritiziouzou 2014/2015.

[13] Serge Bordères, Livre "Authentification réseau avec radius : 802.1x - eap - freeradius".

[14] Mémoire de Fin d'Etudes de MASTER ACADEMIQUE Spécialité : Réseau, Mobilitè et Système Embarqué Thème :■ Étude et mise en place d'un serveur d'authentification RADIUS la norme 802.1X ■ au sein de département informatique à l'université mouloud mammeritiziouzou 2021/2022.

[15] Rapport de Stage Université de la Réunion Département de Mathématiques et Informatique M2 INFORMATIQUE 2014-2015 SAUTRON Nick Mise en production du service eduroam.

[16] Edwin Lyle Brown, Livre "802.1X Port-BasedAuthentication".

[17] Eric Leclercq et Marinette, Chapitre X reseau virtuels (VLANS) de Savonnet departement IEM université Bourgogne. Consultez le :
https ://ufrsciencestech.u-bourgogne.fr/licence3/SystemesEtReseaux2/SupportsCours/ch10.pdf

[18] Protocoles d'authentification sur le site support.elmark. Consultez le :
http ://support.elmark.com.pl/rgd/drivery/u12c/wlan/win7/Docs/FRA/overview.htmauthprots

[19] K.J,GUIDE DE MISE EN PLACE D'UNE SOLUTION D'AUTHENTIFICATION NIVEAU 2,´edition 2010.

[20] Jean-Paul Archier, Les VPN fonctionnement, mise en œuvre et maintenance, collection Expert IT dirigée par Joëlle MUSSET.

Résumé

L'objectif de notre travail est de mettre en place une solution d'authentification basée sur la norme 802.1X, en utilisant RADIUS et des certificats, afin de sécuriser le réseau filaire de l'entreprise Campus NTS. Cette solution permet de contrôler l'accès des utilisateurs au réseau Ethernet de l'entreprise, en garantissant leur authenticité et en empêchant l'accès non autorisé. En combinaisant avec la solution d'authentification basée sur la norme 802.1X, RADIUS et les certificats, nous avons segmenté le réseau en plusieurs VLANs pour avoir une gestion plus précise des utilisateurs, des services et des ressources, tout en limitant la propagation des problèmes de sécurité du réseau.

Mots clés : RADIUS, 802.1X, AUTHENTICATION, AUTHORIZATION, ACCOUNTING, EAP, SSH, CLIENT NAS, SUPPLICANT, VLAN, DNS, DHCP, NPS, PEAP.

Abstract

The objective of our work is to implement an authentication solution based on the 802.1x standard, using RADIUS and certificates, in order to secure the wired network of Campus NTS company. This solution enables the control of user access to the company's Ethernet network by ensuring their authenticity and preventing unauthorized access. In conjunction with the authentication solution based on the 802.1x standard, RADIUS, and certificates, we have segmented the network into multiple VLANs to achieve more precise management of users, services, and resources, while limiting the propagation of security issues and facilitating network management.