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 de cycle.

En vue de l'obtention du diplôme de Master en Informatique.
Spécialité : Adminstration et Sécurité des Réseaux.

Thème

Mise en place d'un VPN SSTP avec ADCS sous windows serveur 2022 pour les clients mobiles via l'authentification radius

---

Réalisé par :

Mlle. AMAOUCHE Djida

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

Président :	**Dr.ATMANI Mouloud**	**U. A/Mira Béjaïa.**
Examinateur	**Dr. BOUZIDI Zair**	**U. A/Mira Béjaïa.**
Encadrant	**Dr. BOUDRIES Abdelmalek**	**U. A/Mira Béjaïa.**

Année universitaire 2022/2023

Remerciements

Je tiens à remercier toutes les personnes qui ont contribué à la réalisation de ce projet fin d'etude. Tout d'abord, je voudrais exprimer ma gratitude envers professeur Mr Boudries pour son soution, ses conseils et son expertise tout au long de ce projet.

Je remercie également tous les enseignants qui ont partagé leurs connaissances avec moi tout au long de mon parcours académique. Je tiens à exprimer mes reconnaissances envers tous mes collègues et amis pour leur soutien moral et leur encouragement tout au long de cette expérience. Votre présence a été une source de motivation pour moi.

Enfin, je voudrais remercier ma famille pour leur soutien inconditionnel, leurs amours et leurs encouragements tout au long de mes études.

Dédicaces

Avec gratitude et amour, je dédie humblement ce travail à mes parents qui m'ont soutenu et sacrifié pour me voir réussir. Merci infiniment pour vos efforts. Je suis reconnaissante et fière d'être votre fille. Que Dieu vous garde.

Je remercie également mon frère Naim pour son soutien, ainsi que mes sœurs Kanza et Wissam pour leur encouragement durant mon travail. Merci aussi à Aissam pour tout ce qu'il fait pour moi malgré la distance qui nous sépare.

Je tiens à exprimer ma reconnaissance envers mes amis Imane, Imad, L'hadi, Lynda, Cherif, Sarah, Mourad, Sousou, Nedjet, Dyhia et Sihem, ainsi qu'à tous ceux qui m'aiment et que j'aime.

Enfin, je dédie ce travail à la mémoire de mon cher ami Fouad CH.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AD	Active Directory.
ADDS	Active Directory Domain Services.
ADCS	Active Directory Certificate Services.
ADFS	Active Directory Federation Services.
AD RMS	Active Directory Rights Management Services.
CA	Autorité de certification.
CCNA	Cisco Certified Network Associate.
CCNP	Cisco Certified Network Professional.
CSS	Cascading Style Sheets.
EAP	Extensible Authentication Protocol.
FTTH	Fiber To The Home.
GRE	Generic Routing Encapsulation.
HTML	(pour HyperText Markup Language.
HTTPS	Hypertext Transfer Protocol Secure.
IPsec	Internet Protocol Security.
LAN	Local Area Network.
L2F	Layer 2 Forwarding.
L2TP	Layer 2 Tunneling Protocol.
MAN	Metropolitan Area Network.
MMC	Microsoft Management Console.
MPLS	Multiprotocol Label Switching.
NAT	Network Address Translation.
NPS	Network Policy Server.
NTS	New Technology § Solutions.
OSI	Open Systems Interconnection.
OU	Unité d'organisation.
PAN	Personal Area Network.
PEAP	Protected Extensible Authentication Protocol.
PPTP	Point-to-Point Tunneling Protocol.
PSI	La politique de sécurité informatique.
RADIUS	Remote Authentication Dial-In User Service.
SSH	Secure Shell.
SSL/TLS	Secure Sockets Layer/Transport Layer Security.
SSTP	Secure Socket Tunneling Protocol.
TCP/IP	Transmission Control Protocol/Internet Protocol.
VPN	Virtual Private Network.
WAN	Wide Area Network.

INTRODUCTION GÉNÉRALE

La mise en place d'un VPN SSTP (Secure Socket Tunneling Protocol) avec ADCS (Active Directory Certificate Services) sous Windows Server 2022 pour les clients mobiles via l'authentification RADIUS est un sujet d'étude crucial dans le domaine de la sécurité informatique. Avec la prolifération des appareils mobiles et la nécessité de protéger mes données sensibles lors de leur transmission, il est essentiel que je mette en place des mécanismes de sécurité fiables. Ce mémoire se propose donc d'explorer la mise en place d'un VPN SSTP avec ADCS afin de garantir une connexion sécurisée pour mes clients mobiles. L'utilisation de l'authentification RADIUS ajoute une couche supplémentaire de sécurité en s'assurant de mon identité et en contrôlant mon accès au réseau.

Dans ce mémoire, je vais tout d'abord présenter les concepts fondamentaux relatifs aux réseaux privés virtuels (VPN) et au protocole SSTP. Je vais également expliquer le rôle crucial d'ADCS dans la gestion des certificats nécessaires à l'établissement d'une connexion sécurisée.

Ensuite, je vais détailler les différentes étapes nécessaires à la mise en place d'un VPN SSTP avec ADCS sous Windows Server 2022. Je vais examiner la configuration du serveur VPN, l'installation et la configuration d'ADCS, ainsi que l'intégration de l'authentification RADIUS pour les clients mobiles.

Je vais également étudier les aspects de sécurité liés à cette configuration, en mettant l'accent sur la protection des certificats, la gestion des accès et la surveillance du réseau. Je vais examiner les meilleures pratiques de sécurité pour assurer l'intégrité et la confidentialité de les données lors de la communication entre les clients mobiles et le réseau privé.

En conclusion, ce mémoire offre une vision complète de la mise en place d'un VPN SSTP avec ADCS sous Windows Server 2022 pour les clients mobiles via l'authentification RADIUS. Il met en évidence l'importance de ces mécanismes de sécurité dans un environnement de plus en plus mobile et connecté, et souligne l'importance de protéger les données sensibles lors de leur transmission. Ce mémoire vise à fournir des recommandations pratiques pour les professionnels de la sécurité informatique afin d'améliorer la sécurité des réseaux et de garantir la confidentialité des informations échangées.

Chapitre 1

Généralités sur les réseaux et la sécurité informatique

1.1 Introduction

Les réseaux informatiques sont nés pour relier des terminaux distants à un site central, connecter des ordinateurs et des stations de travail à leur serveur. Ils permettent le partage de ressources entre des ordinateurs, tels que des données ou des périphériques.
Avant d'aborder les infrastructures de réseaux, il est important de revoir quelques notions de base sur les réseaux informatiques en général.

1.2 Généralité sur les réseaux informatique

Dans cette section, j'ai abordé des notions théoriques essentielles en matière de réseaux et de sécurité informatique. j'ai débuté par la définition du concept de réseau informatique, pour ensuite, j'ai penché sur les modèles OSI et TCP/IP.

1.2.1 Réseaux informatiques

a) Définition :

Un réseau informatique désigne un ensemble d'équipements informatiques reliés entre eux grâce à des supports de communication qui peuvent échanger des données et partager des ressources entre eux

b) Intérêt :

Un réseau informatique peut servir à plusieurs buts distincts [1] :

— Le partage de ressources telles que fichiers, applications ou matériels.

— La communication entre personnes via le courrier électronique ou les discussions en direct.

— Garantie de l'unicité de l'information.

1.2.2 Classification des réseaux

Il existe plusieurs façons de classer les réseaux informatiques en fonction de leur taille, de leur portée géographique et de leur architecture. Voici les principales classifications :

a) **Réseau personnel (PAN) :** Le plus petit réseau étendu, qui représente l'interconnexion de dispositifs informatiques, tels qu'une souris sans fil, un clavier et un ordinateur dans un rayon de 10 mètres autour de l'utilisateur [2].

b) **Réseau local (LAN) :** De taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, est un groupe d'appareils informatiques connectés dans un lieu physique donné, tels qu'un bâtiment, un bureau ou une maison [2].

c) **Réseau étendu (MAN) :** Repose sur plusieurs réseaux locaux sur une grande zone géographique, mais qui est plus petit qu'un WAN. les réseaux métropolitains permettent à deux machines distantes de communiquer comme si elles faisaient partie du même réseau local [2].

d) **Réseau métropolitain (WAN) :** Qui s'étend sur une grande zone géographique et repose sur plusieurs réseaux plus petits. Il peut être composé de VPN, de réseaux cellulaires et de réseaux privés. les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier [2].

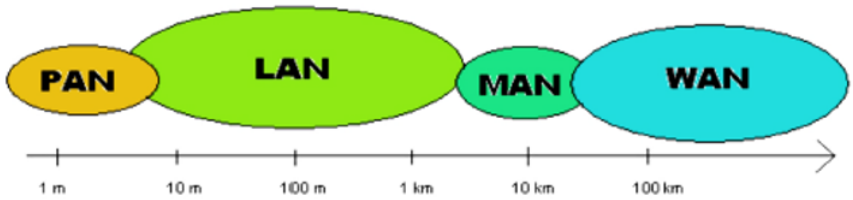


FIGURE 1.1 – Classification des réseaux

1.2.3 Mode d'acheminement des messages

Il existe plusieurs types de Mode d'acheminement, dont les principes sont [3] :

a) **La commutation de circuits :** C'est une technique de transmission de données où un circuit dédié est établi entre deux points de communication avant que les données ne soient transmises. Une fois le circuit établi, les données sont transmises sans interruption jusqu'à ce que le circuit soit terminé.

b) **La commutation de messages :** C'est une technique de transmission de données où les données sont transmises sous forme de messages individuels. Chaque message est transmis de manière indépendante et peut emprunter différents chemins pour atteindre sa destination.

c) **La commutation de paquet :** C'est un mode de transmission de données dans lequel les packet switching sont divisées en trames de taille fixe, qui sont ensuite envoyées individuellement à leur destination. Chaque trame peut suivre un chemin différent pour atteindre sa destination.

1.2.4 Architecture des réseaux

On distingue :

a) Poste à poste :

Est un modèle de réseau décentralisé dans lequel chaque ordinateur peut agir à la fois comme client et comme serveur [5].

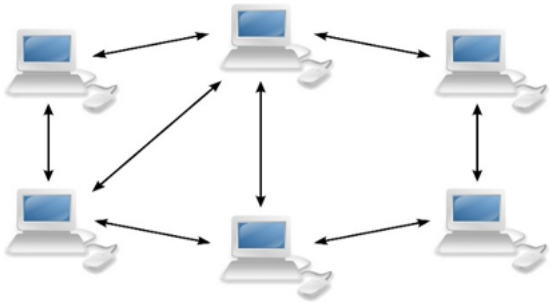


FIGURE 1.2 – Architecture Poste à poste.

b) Client/serveur : Est un modèle centralisé dans lequel les clients dépendent des serveurs pour accéder aux services. [**5**]

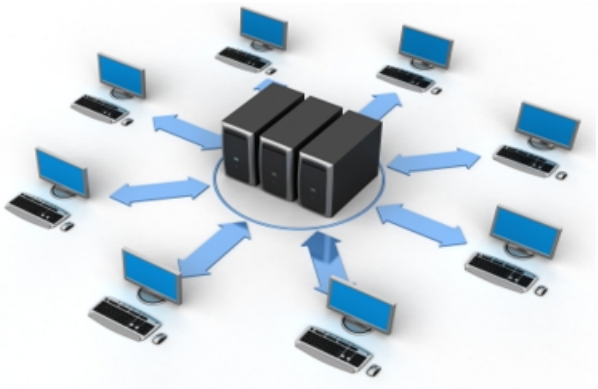


FIGURE 1.3 – Architecture Client serveur/

1.2.5 Topologies des réseaux

On distingue :

a) Topologie en bus : Dans cette topologie, chaque périphérique est connecté à un câble commun, appelé bus. Les données circulent le long du câble et chaque périphérique reçoit toutes les données, mais ne traite que celles qui lui sont destinées [6].

b) Topologie en anneau : Dans cette topologie, chaque périphérique est connecté à ses voisins, de sorte que les données circulent dans un cercle [6].

c) Topologie en étoile : Dans ce type de réseau, chaque périphérique est connecté à un commutateur central, qui coordonne les communications entre eux [6].

d) Topologie en maillage : Dans cette topologie, chaque périphérique est connecté à tous les autres périphériques du réseau [6].

e) Topologie en arbre : Cette topologie est une combinaison de la topologie en étoile et en bus. Les périphériques sont connectés à des commutateurs qui sont à leur tour connectés à d'autres commutateurs [6].

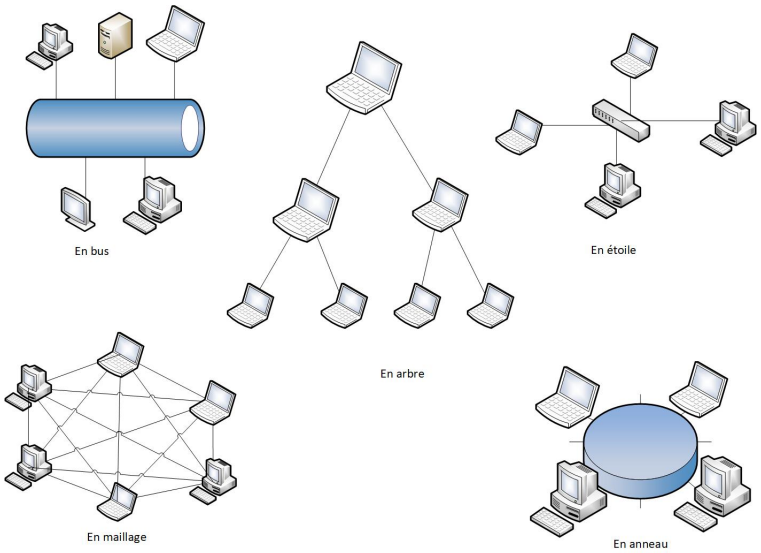


FIGURE 1.4 – Topologies des réseaux.

1.2.6 Modèles de références

a) Modèle OSI :

Le modèle OSI (Open Systems Interconnection) est un cadre conceptuel utilisé pour décrire les fonctions d'un système de mise en réseau. Il se décompose en sept couches, chacun responsable d'un aspect de la communication, et permet aux divers systèmes de communiquer entre eux [4].

1. **La couche physique :** Elle décrit les caractéristiques physiques du support de transmission (câble, fibre optique, etc.) et les signaux électriques, optiques ou électromagnétiques utilisés pour transférer les données.
2. **La couche de liaison de données :** Elle assure la fiabilité de la communication en détectant et en corrigeant les erreurs de transmission.
3. **La couche réseau :** Elle permet d'acheminer les paquets de données à travers différents réseaux et de trouver le meilleur chemin possible pour les transférer.
4. **La couche transport :** Elle assure la fiabilité de la transmission en gérant les flux de données et en vérifiant l'intégrité des données envoyées.
5. **La couche session :** Elle permet l'établissement, la gestion et la terminaison des sessions de communication entre les ordinateurs.
6. **La couche présentation :** Elle gère la présentation des données à l'utilisateur final en s'occupant de leur formatage, leur codage et leur compression.
7. **La couche application :** Elle fournit les services de communication de haut niveau, tels que le courrier électronique et le partage de fichiers.

7 Couche Application (Applications utilisant le réseau).
6 Couche Présentation (Formate les données en fonction de l'application).
5 Couche Session (Répartit les données suivant les applications).
4 Couche Transport (Détection et correction des erreurs).
3 Couche Réseau (S'occupe de la connexion sur le réseau).
2 Couche Liaison (Transfert de données fiable sur le lien physique).
1 Couche Physique (Définie les caractéristiques physiques du média).

TABLE 1.1 – Le modèle de référence OSI.

Le tableau TABLE 1.1 Table représente l'empilement des sept couches du modèle OSI avec leurs noms et fonctions respectives.

b) Modèle TCP/IP :

Le modèle TCP/IP est une architecture réseau à quatre couches [7].

1. **La couche hôte réseau :** Est responsable de l'adressage, du routage et de la transmission des données à travers les réseaux. Elle assure également la fiabilité de la transmission des données en utilisant des protocoles de contrôle de flux et de correction d'erreurs.
2. **La couche internet :** Est responsable de la transmission des paquets de données entre les différents réseaux d'un système.
3. **La couche transport :** Est responsable de l'acheminement des données de bout en bout entre les applications sur des systèmes hôtes différents.
4. **La couche application :** Cette couche est responsable de l'interaction directe avec les utilisateurs finaux et fournit une interface pour l'accès aux services de communication offerts par les applications.

1 Couche Application (Applications utilisées sur le réseau).
2 Couche Transport (Assure le transfert d'un site à un autre).
3 Couche Internet (Définie les datagrammes et leur routage).
4 Couche Physique (Ensemble de routines d'accès au média).

TABLE 1.2 – Architecture utilisant le protocole TCP/IP.

Le tableau TABLE 1.2 représente l'empilement des quatre couches du modèle TCP/IP avec leurs noms et fonctions respectives.

1.3 généralités sur la sécurité informatique

1.3.1 Critères de la sécurité

a) La confidentialité : Se réfère à la protection des informations contre toute personne non autorisée. Elle garantit que les informations ne sont accessibles qu'aux personnes qui ont les droits nécessaires pour y accéder [8].

b) L'intégrité : Est la garantie que les informations ne sont pas altérées ou modifiées de manière non autorisée [8].

c) La disponibilité : Est la garantie que les ressources nécessaires sont accessibles et utilisables lorsque cela est nécessaire [8].

d) La non-répudiation : Est la capacité à prouver qu'une personne a bien effectué une action ou une transaction. Elle empêche les utilisateurs de nier avoir effectué une action ou d'avoir envoyé une communication [8].

e) L'authentification : Est la vérification de l'identité d'un utilisateur ou d'un système. Elle garantit que l'utilisateur est bien la personne qu'il prétend être et qu'il a les autorisations nécessaires pour accéder aux informations ou effectuer une action [8].

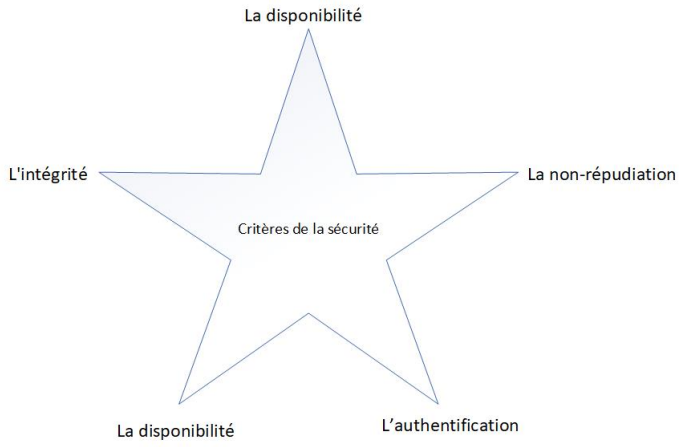


FIGURE 1.5 – Critères de la sécurité

1.3.2 Politique de sécurité informatique

La politique de sécurité informatique (PSI) est un ensemble de règles, procédures et pratiques mises en place par une organisation pour protéger ses systèmes informatiques, ses données et ses informations confidentielles contre les menaces internes et externes [9].

1.3.3 Menaces

Une menace en informatique fait référence à tout événement ou action qui a le potentiel de causer des dommages ou des perturbations à un système informatique, à des données ou à des utilisateurs [11].

Types de menaces

a) **Menaces graves :** Ce sont les menaces classiques qui ont la capacité d'accomplir des actions destructrices et illégales de manière autonome. Les malwares, tels que les vers, virus et Chevaux de Troie, font partie de cette catégorie. Ils constituent des dangers pour les systèmes informatiques [12].

b) **Menaces mineures :** Sont considérées moins dangereuses, mais peuvent être exploitées par des tiers pour des actions malveillantes. Les experts en sécurité informatique les appellent "logiciels gris" ou "logiciels potentiellement non sollicités", tels que les adwares, dialers, canulars, riskwares et hacktools. Toute présence de ces menaces doit être prise au sérieux [12].

1.3.4 Attaque

Est une tentative d'accéder illégalement à un système informatique, à des données ou à des informations stockées dans un ordinateur, un réseau ou un dispositif connecté.

Types de attaques

Il existe plusieurs types d'attaques informatiques, tels que [13] :

a) Attaque par rebond : Consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter à lui.

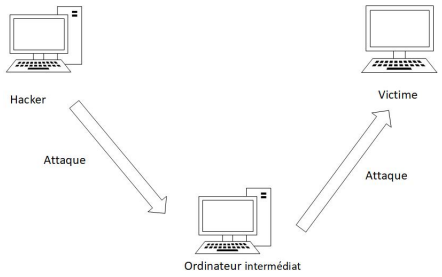


FIGURE 1.6 – Attaque par rebond

b) Attaque de l'homme du milieu : Le pirate se positionne entre deux ordinateurs et se fait passer pour l'un d'eux afin d'obtenir le mot de passe de l'autre. Il peut ensuite utiliser ce mot de passe valide pour attaquer le premier ordinateur.

c) Déni de service : Une attaque cherchant à rendre un ordinateur hors service en le submergeant de trafic inutile. Par exemple, un serveur entièrement occupé à répondre à de fausses requêtes de connexion. Des machines peuvent être à l'origine de l'attaque généralement à l'insu de leur propriétaire.

1.3.5 Mécanismes de sécuirté

A) La cryptographie

Est un domaine mathématique qui vise à assurer la sécurité des communications en convertissant les messages en un code secret compréhensible uniquement par les destinataires autorisés. Cette méthode est employée afin de préserver la confidentialité et l'intégrité des informations échangées [14].

Notions sur la cryptographie

Depuis plus de dix ans, la cryptographie est devenue un outil incontournable pour protéger les informations qui circulent sur les réseaux, qu'ils soient fermés ou ouverts comme Internet. Cette science, également connue sous le nom de "science du chiffrement", vise à assurer la confidentialité des messages en veillant à ce qu'ils ne soient compréhensibles que par leurs auteurs et incompréhensibles pour toute autre personne [17].
La cryptographie peut être divisée en deux grandes catégories [14] :

1. **Le cryptage symétrique :** Une clé secrète est partagée entre l'expéditeur et le destinataire, et cette clé est utilisée pour chiffrer et déchiffrer le message.

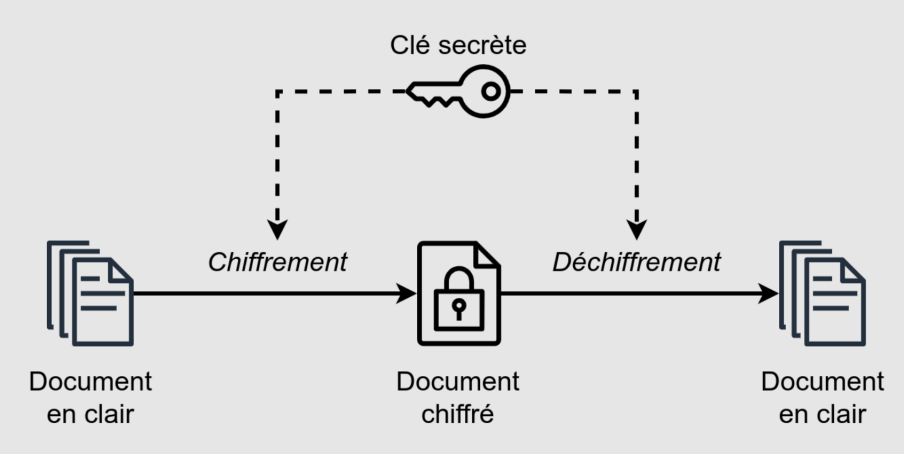


FIGURE 1.7 – Le cryptage symétrique

2. **Le cryptage asymétrique :** Chaque utilisateur possède une paire de clés, une clé publique et une clé privée. La clé publique peut être partagée avec n'importe qui, tandis que la clé privée doit être conservée secrète. Les messages sont chiffrés avec la clé publique du destinataire et ne peuvent être déchiffrés qu'avec sa clé privée.

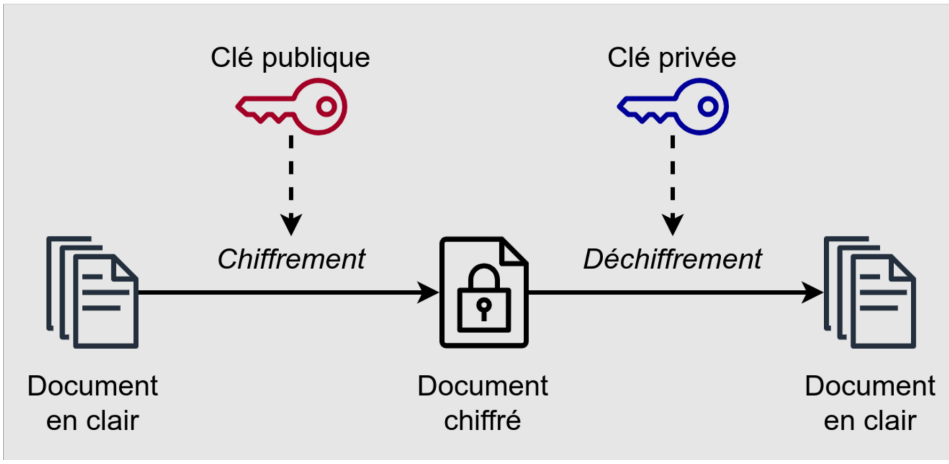


FIGURE 1.8 – Le cryptage asymétrique

B) La signature

1. **La signature numérique :** C'est un mécanisme de sécurité utilisé dans les environnements électroniques pour garantir l'intégrité et l'authenticité des données échangées [15].
2. **Les certificats :** C'est un outil numérique qui permet de confirmer l'identité d'une personne, d'un site web ou d'une organisation en ligne, émis par une autorité de certification (CA). Il est utilisé pour assurer la sécurité des communications en ligne, notamment pour les transactions financières et les échanges de données sensibles [15].

1.4 Conclusion

Ce chapitre a couvert les réseaux informatiques de manière générale, en présentant leurs différentes topologies, modes de cheminement, architectures, classifications, le modèle de référence OSI et le mode TCP/IP. Il a également abordé la sécurité informatique dans ces différents domaines.

Chapitre 2

Présentations de l’organisme d’accueil

2.1 Introduction

ce chapitre représente le campus NTS (New Technology § Solutions). Tout d'abord, je vais donner un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Ensuite, j'analyserai l'architecture réseau de cette entreprise et ses composantes afin de proposer d'éventuelles améliorations.

2.2 Présentions de l'entreprise « Campus NTS »

2.2.1 Création et évolution

NTS est une entreprise émergente spécialisée dans la recherche, la conception et la mise en œuvre de solutions d'intégration de systèmes de sécurité, ainsi que dans l'importation et la distribution d'équipements et de matériels de sécurité pour les réseaux et les télécommunications, la formation et le conseil.
Fondée en 2020 à Béjaïa par Yassine Djebbari, qui bénéficie d'une expérience de nombreuses années et a mené à bien des projets d'envergure dans divers secteurs et régions du pays, notamment pour Air Algérie, Retelem Alger, la Poste d'Algérie, Adèle, RATP ALJAZAIR, la technologie, Géant de l'électronique BBR, Morsi, l'Université de Bejaïa, la cité universitaire à Bejaïa (Targa Ouzamour, 17 octobre...etc), SARL Alphas Bejaïa et Providentia Béjaïa.

2.2.2 Localisation de l'entreprise

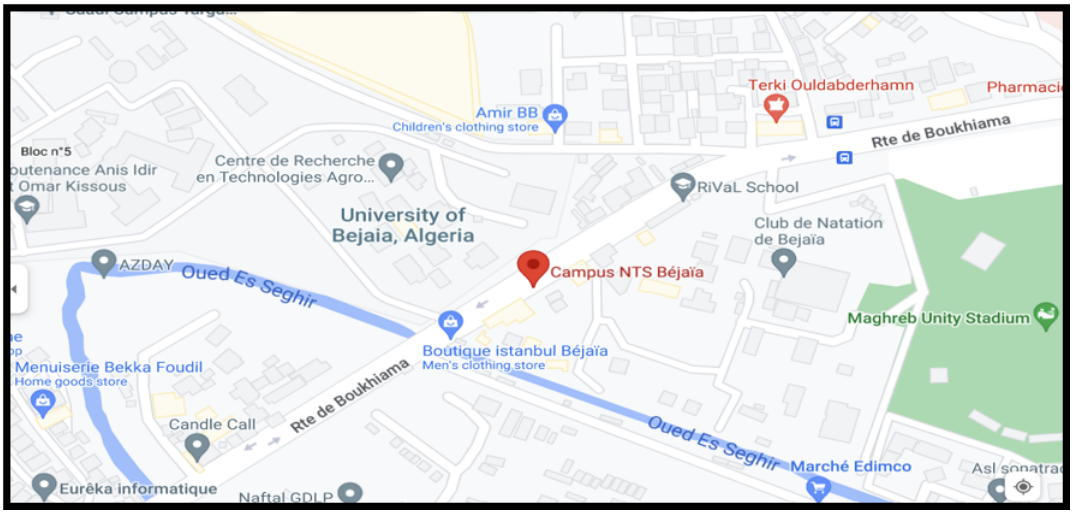


FIGURE 2.1 – Localisation de l'entreprise NTS.

2.2.3 Fiche technique

Le tableau TABLE 2.1 résume les informations relatives à l'entreprise NTS.

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

TABLE 2.1 – Identification sur campus NTS

2.2.4 Objectifs, missions et activités de l'Entreprise « Campus NTS »

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

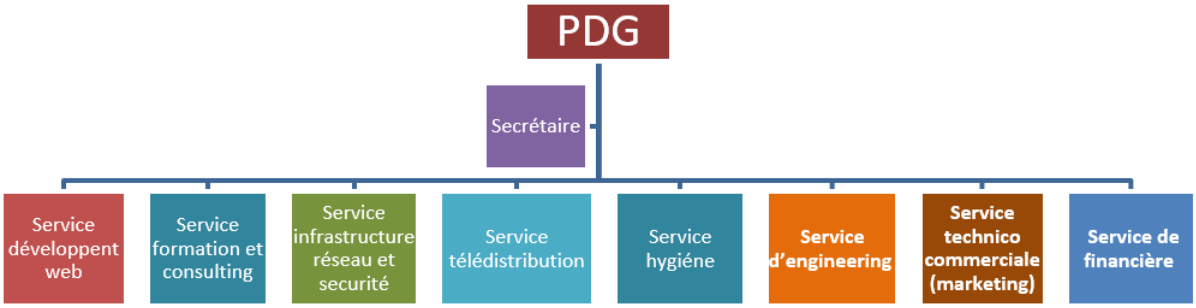


FIGURE 2.3 – L'organigramme de campus NTS.

Je vais me contenter de vous présenter ci-dessous la description de l'organigramme du campus NTS (voir la figure 2.3) dans lequel j'ai effectué mon stage de fin d'apprentissage.

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.
   • Programmation (C, C++,C#, Java, Python…etc.).
   • Electricités Bâtiments et industriels.
   • Formation Cisco CCNA, CCNP S&R.
   • Virtualisation et cyber sécurité.
   • Microsoft server, SQL.

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

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.

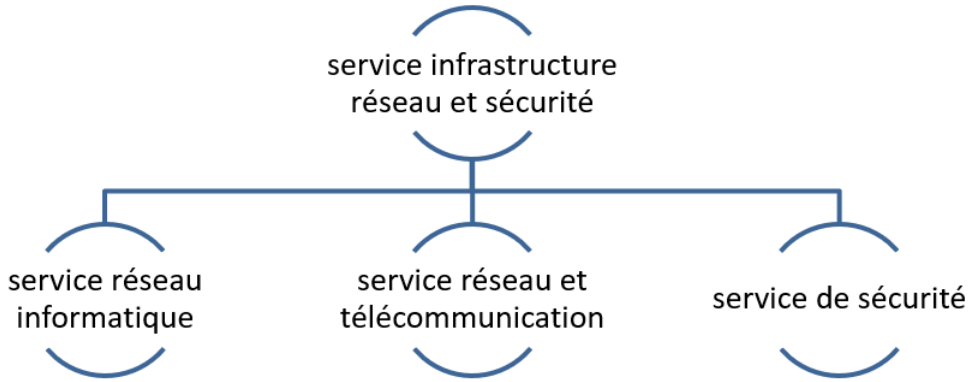


FIGURE 2.4 – Organigramme de service d'accueil.

a) **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.

b) **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.

c) **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 :**

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

• La préparation des états financiers.

• La gestion de la trésorerie et de des encaissements.

• La rémunération des employés, des comptes à payer.

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

• La réception des marchandises et du courrier.

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 Etat des lieux

2.3.1 Présentation du réseau campus NTS :

L'entreprise a une architecture en couches et pour assurer la communication entre ses différents services, elle connecte son LAN à une connexion FTTH fournie par un fournisseur d'accès Internet. Le schéma ci-dessous nous montre l'infrastructure du réseau NTS :

a) Présentation de l'architecture réseau existant dans l'entreprise

NTS construit un réseau en choisissant une topologie arborescente pour connecter ses différents appareils, comme illustré dans la figure de la page suivante :

Les caractéristiques des équipements par niveaux :

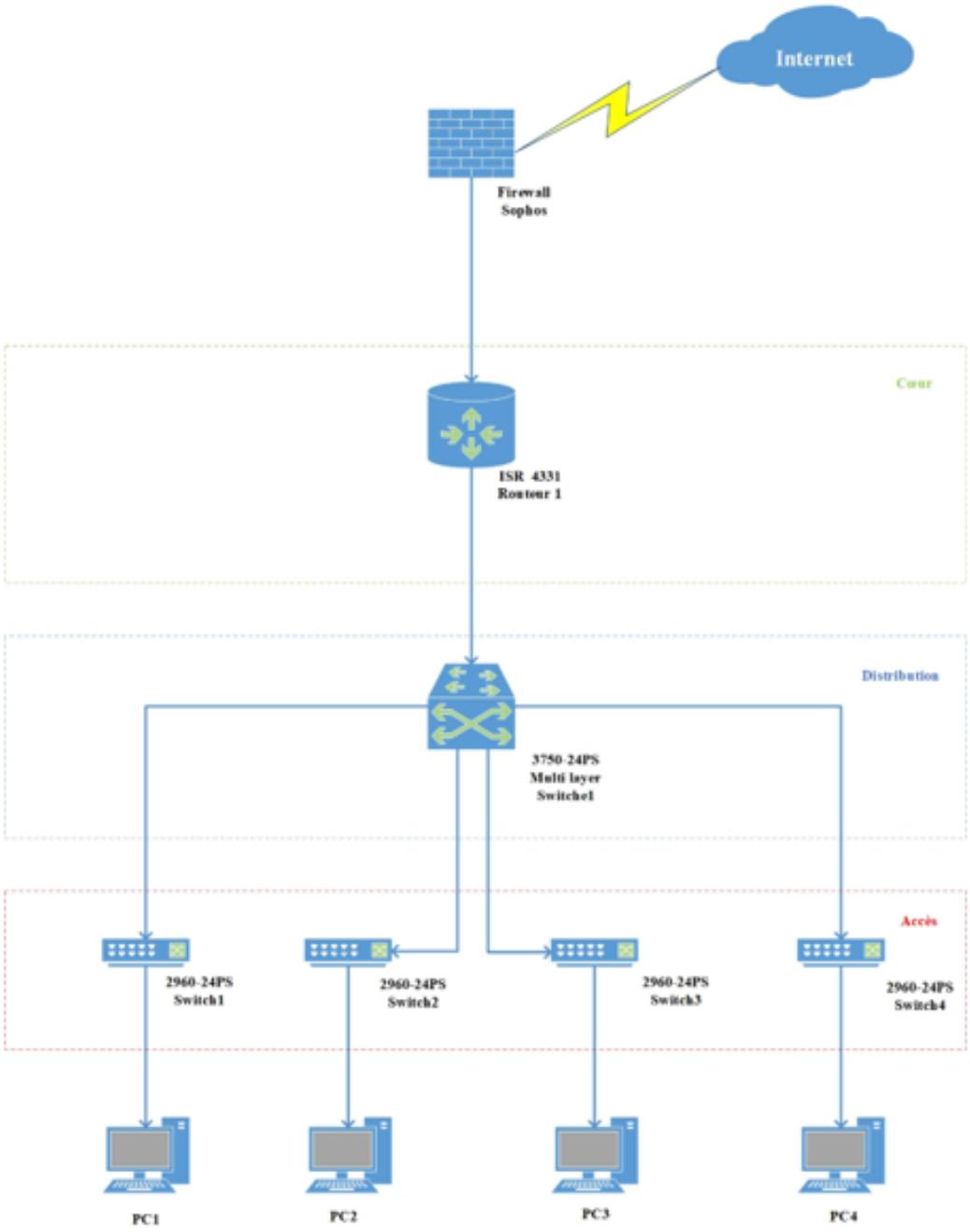


FIGURE 2.5 – Architecture de réseau (NTS).

b) Analyse du parc informatique

— **Présentation de l'environnement hardware et software :**

Nom de l'équipement	Le hardware (hard)	Software (soft)e
Routeur	ISR 4331	IOS (International Organisation For Standardisation)
Pare-feu	SOPHOS XG	Linux
Switch	• Cisco Catalyst 3750-24PS • Cisco Catalyst 2960-24PS	IOS (International Organisation For Standardisation)
server	HP ProLiant DL380P génération 10	Windows server 2012
PC portable	Dell IAER 35 R	Windows 10

TABLE 2.2 – L'environnement hardware et le software

— **Les caractéristiques des équipements par niveaux :**

Nom de l'équipement	Modèle	Caractéristique
Router 	ISR 4331	• **RAM :** 4 G0 (installé) /16 GO (maximum) • **Mémoire Flash :** 4000 MO • **Débit :**100 Mb/s • **Protocole de liaison de données :** Ethernet, fast Ethernet et gigabit-ethernet
Pare-feu 	SOPHOS XG	• **Débit :** 4000 Mbit/s • **Débit IPS :** 2700Mbit/s • **Débit VPN IP sec :** 560 Mbit/s • **@ IP/Numéro de port**
Switch 	Cisco Catalyst 3750-24PS Switch	• **Ports :** 24 ports • **Mémoire Flash :** 16MO • **Mémoire RAM :** 128MO • **Capacité de commutation :** 32 Gbit/s
Switch 	Cisco Catalyst 2960-24PS Switch	• **Ports :** 24 ports • **Mémoire Flash :** 128MO • **Mémoire RAM :** 512MO • **Capacité de commutation :** 56 Gbit/s
server 	HP ProLiant DL380P génération 10	Processeur Intel Xeon Silver 4110 (Octo-Core 2.1 GHZ / 3.0 GHZ Turbo-16 Threads-cache 11Mo) 16 G0 DDR4 RDIMM (1x 16 GO -12 slots) s
PC portable 	Dell IAER 35 R	• **AMD core :** i5 8th génération • **RAM :** 8GO • **Disque :** 256GO • **Ecran :** UHD Graphies 620 (1920×1080×32b)

TABLE 2.3 – Détails des ressources disponibles de l'entreprise

2.3.2 Problématiques et solutions proposées.

A) Problématiques

Après avoir étudié le parc informatique de l'organisme d'accueil NTS, j'ai identifié certains besoins critiques auxquels leur infrastructure réseau n'a pas accordé suffisamment d'importance. Ces besoins comprennent :

1. Le besoin d'accéder aux applications en temps réel pour le télétravail et le monitoring.
2. Le besoin d'une infrastructure réseau qui lui permettra d'assurer la disponibilité, l'extensibilité, l'évolutivité et la sécurité pour les applications.
3. Le besoin de renforcer l'authentification en utilisant les technologies suivantes :
- Technologies Microsoft serveur 2022.
- Le protocole SSTP.
- Active Directory.
- Le protocole Radius.

B) Solutions

Le principal défi d'une architecture de réseau sécurisée est de pouvoir réguler l'accès aux ressources réseau à partir du réseau local et de l'extérieur, tout en limitant autant que possible les vulnérabilités aux éventuelles attaques ou vol d'informations afin d'améliorer la sécurité des accès à distance. Je propose différentes solutions :

1. VPN SSTP : pour établir une connexion VPN chiffrée entre un client et un serveur et garantir la confidentialité des données pendant la transmission.

2. Authentification par certificat (TLS/EAP) : offre un haut niveau de sécurité grâce à l'utilisation de TLS et des certificats numériques. Les données échangées entre le client et le serveur sont chiffrées, ce qui protège leur confidentialité.
3. Le protocole Radius : est utilisé pour l'authentification et l'autorisation des utilisateurs dans les réseaux informatiques. Il offre une solution centralisée pour gérer l'accès aux services réseau, ainsi qu'une sécurité et une compatibilité étendues.

2.4 Conclusion

Dans ce chapitre, j'ai donné un aperçu général de l'entreprise du campus NTS, puis j'ai découvert un problème qui m'a amené à rechercher et à mettre en œuvre une nouvelle architecture de réseau sécurisée.

Chapitre 3

Administration avancée sur les VPNs

3.1 Introduction

Avec la généralisation d'Internet, les entreprises demandent à leurs employés de se connecter à leurs réseaux depuis des sites éloignés via des technologies de réseau privé virtuel (VPN).

Les VPN permettent une connexion sécurisée au réseau local de l'entreprise via un réseau public, offrant des opportunités commerciales telles que l'administration à distance et les applications à haute sécurité. L'utilisation de VPN est devenue incontournable pour de nombreux utilisateurs et groupes commerciaux nécessitant un accès régulier et fiable aux réseaux locaux d'entreprise.

3.2 Notion de base sur les VPNs

3.2.1 Définition

Un VPN (Virtual Private Network) est un réseau privé virtuel qui permet de créer une connexion sécurisée entre un ordinateur ou un appareil mobile et un réseau privé, tel que l'Internet ou un réseau d'entreprise [21].

3.2.2 Topologie

Nous pouvons distinguer deux grandes catégories de VPN [20] :

a) VPN d'entreprise :

— Le VPN d'entreprise site à site (ou VPN inter-sites) est une solution de connectivité de réseau privé qui permet à deux ou plusieurs réseaux entreprise de communiquer entre eux de manière sécurisée via Internet. Il relie les différents sites de l'entreprise, comme les bureaux, les filiales et les partenaires, pour leur permettre de partager des ressources et de la communication avec le même réseau local.

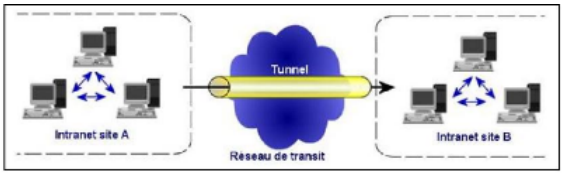


FIGURE 3.1 – VPN site à site

— Le VPN d'entreprise poste à site permet aux employés distants de se connecter à distance au réseau privé de l'entreprise à partir de leur poste de travail. Cette solution permet aux employés de travailler à distance tout en ayant accès aux outils et aux données nécessaires pour effectuer leur travail.

— Le VPN d'entreprise poste à poste permet aux employés de communiquer de manière sécurisée et privée entre deux postes distants situés à différents endroits géographiques en utilisant un protocole VPN. Cette solution permet aux employés de communiquer et de partager des fichiers de manière transparente, comme s'ils étaient sur le même réseau local.

b) VPN opérateur :

— Un VPN opérateur site à site permet aux entreprises de connecter leur réseau local à un autre réseau distant situé dans un autre emplacement géographique. Les réseaux distants peuvent être des filiales d'une même entreprise, des fournisseurs, des partenaires commerciaux ou tout autre réseau disposant d'une adresse IP publique.

— Un VPN nomade vers un réseau est un type de VPN qui permet à un utilisateur de se connecter à un réseau privé à distant (par exemple, un réseau d'entreprise) en utilisant Internet comme support. Ce type de VPN est souvent utilisé par des employés nomades qui ont besoin d'accéder aux ressources de leur entreprise tout en travaillant à distance.

3.2.3 Fonctionnements

Le VPN fonctionne grâce à une technique appelée tunneling. Une fois que l'émetteur et le destinataire sont authentifiés, les données sont encapsulées et acheminées à travers un tunnel sécurisé.
Le processus d'encapsulation implique de placer les données à transmettre dans un en-tête qui sera ajouté aux trames dans le tunnel.
Le tunneling est donc un ensemble de mécanismes qui assurent le transport sécurisé des données ainsi que leur désencapsulation à la réception [19].

3.2.4 Avantages

Les VPN offrent de nombreux avantages, que ce soit pour les particuliers ou pour les entreprises. Voici quelques-uns des principaux avantages des VPN [21] :

— Sécurité : Les VPN offrent une connexion sécurisée et chiffrée qui permet de protéger les données de l'utilisateur contre les pirates informatiques, les interceptions de données et la surveillance en ligne.

— Travail à distance : Les VPN permettent aux employés de travailler à distance en toute sécurité en se connectant au réseau privé de leur entreprise

— Économies : Les VPN permettent d'économiser sur les coûts liés aux lignes de communication dédiées, car ils peuvent être utilisés pour connecter des bureaux distants ou des partenaires commerciaux via Internet

— Contrôle d'accès : Les VPN permettent de contrôler l'accès au réseau privé, en limitant l'accès aux utilisateurs autorisés et en offrant des options de gestion des droits d'accès.

3.2.5 Protocoles

Les principaux protocoles de tunneling VPN sont les suivants :

a)Niveau 2

1. **PPTP (Point-to-Point Tunneling Protocol) :** Est un protocole de tunneling qui permet de connecter des ordinateurs distants à un réseau privé en utilisant des connexions Internet. PPTP encapsule les paquets de données dans des paquets PPP (Point-to-Point Protocol) pour les transmettre à travers le tunnel VPN. PPTP est considéré comme un protocole VPN obsolète en raison de ses vulnérabilités de sécurité connues [22].

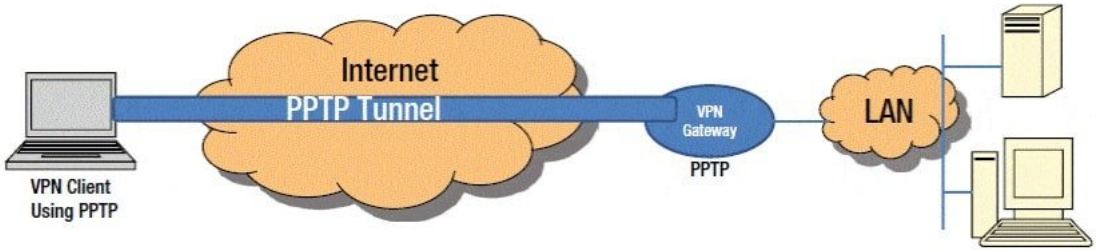


FIGURE 3.2 – Le protocole PPTP

2. **L2F (Layer 2 Forwarding) :** Il s'agit d'un protocole permettant aux utilisateurs distants de se connecter à des réseaux privés via Internet [24].
3. **L2TP (Layer 2 Tunneling Protocol) :** Il s'agit d'une extension du protocole PPTP (Point-to-Point Tunneling Protocol) utilisé par les fournisseurs de services Internet pour permettre des connexions virtuelles. Bien que le protocole L2TP ne fournisse pas de chiffrement en lui-même, il peut être combiné avec d'autres protocoles pour offrir une sécurité supplémentaire [22].

b) Niveau 2.5

1. **MPLS (Multiprotocol Label Switching) :** Utilisé pour la commutation de paquets dans les réseaux de télécommunication, Il permet notamment de créer des connexions VPN sécurisées à travers des réseaux publics comme Internet [33].

c) Niveau3 et plus

1. **IPsec (Internet Protocol Security) :** Est un ensemble de protocoles utilisés pour sécuriser les communications entre deux équipements en utilisant des clés de chiffrement et d'authentification pour protéger les données qui transitent entre eux [26].

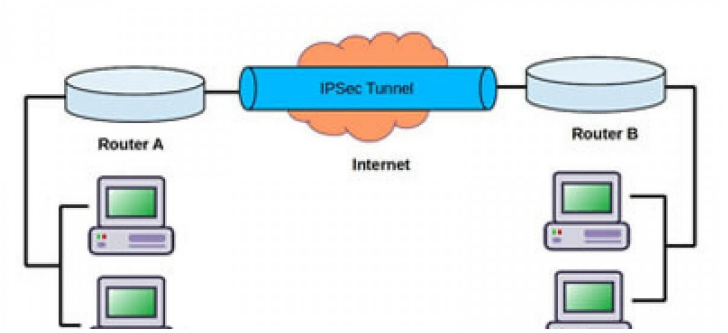


FIGURE 3.3 – Protocole IPsec

2. **GRE (Generic Routing Encapsulation) :** Est un protocole de tunneling qui permet de transporter des paquets de données de différents protocoles à travers un réseau IP. GRE encapsule les paquets de données dans des paquets IP pour les transmettre à travers le réseau. GRE est souvent utilisé en conjonction avec d'autres protocoles VPN pour fournir des fonctionnalités de routage et de commutation supplémentaires [25].
3. **SSL/TLS (Secure Sockets Layer) / (Transport Layer Security) :** Sont des protocoles de sécurité cryptographique qui permettent une communication sécurisée sur un réseau informatique. Le TLS est le protocole successeur de SSL, offrant un fonctionnement similaire basé sur le chiffrement pour la protection des données transmises sur un réseau. Ces deux protocoles sont couramment utilisés pour chiffrer les données et garantir des connexions sécurisées entre les serveurs Web et les clients [18].

4. **SSH (Secure Shell) :** Le protocole SSH est utilisé pour établir une connexion cryptée et sécurisée entre deux points sur un réseau non sécurisé. Il fournit une méthode fiable pour se connecter à des services réseau en toute sécurité et de manière confidentielle [23].

3.2.6 VPN poste à site

Le VPN poste à site permet à un utilisateur distant de se connecter à un réseau d'entreprise de manière sécurisée via Internet. Cela se fait grâce à un logiciel client VPN qui établit un tunnel sécurisé entre le poste de travail de l'utilisateur et le réseau d'entreprise.
Le VPN poste à site est souvent utilisé pour permettre aux employés de travailler à distance tout en accédant aux ressources et aux applications de l'entreprise, ainsi que pour permettre aux partenaires ou aux sous-traitants d'accéder aux ressources internes de l'entreprise de manière sécurisée et contrôlée.
Un VPN poste à site permet aux entreprises de bénéficier de nombreux avantages, notamment une meilleure flexibilité et productivité des employés, une réduction des coûts liés à la communication et une meilleure sécurité des données. Cependant, il est important de garantir une sécurité appropriée pour éviter toute violation de la sécurité du réseau [20].

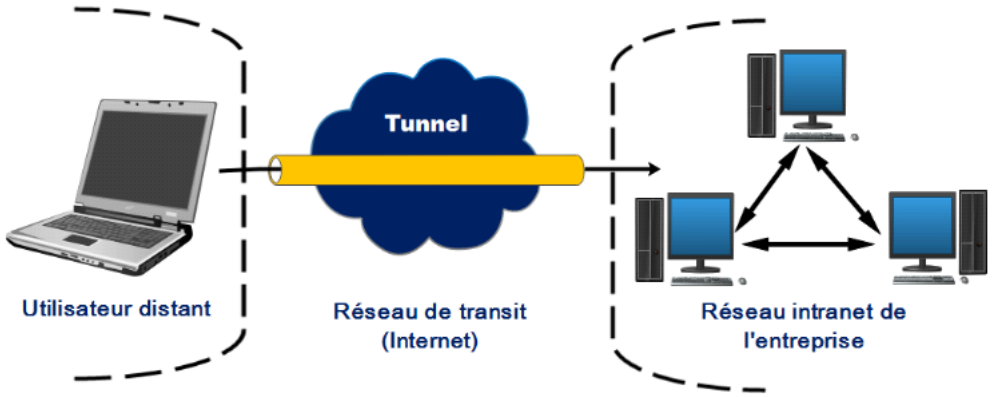


FIGURE 3.4 – VPN poste à site

3.2.7 Protocole SSTP

1. **Protocole SSTP(Secure Socket Tunneling Protocol) :** Est un protocole VPN qui a été développé par Microsoft. Il est basé sur le protocole SSL/TLS et permet de créer des tunnels VPN sécurisés entre des ordinateurs distants en utilisant le port TCP 443 (HTTPS). SSTP est conçu pour offrir un accès distant sécurisé aux ressources de réseau privé, tout en offrant une protection contre les attaques de type "man in the middle" [22].

   a) L'utilité de SSTP : L'utilité de SSTP réside dans sa capacité à fournir une connexion VPN sécurisée pour les utilisateurs distants qui travaillent à distance ou qui se connectent à leur réseau d'entreprise depuis l'extérieur. SSTP utilise le protocole SSL/TLS (Secure Sockets Layer/Transport Layer Security) pour créer un tunnel crypté entre les deux ordinateurs, ce qui garantit la confidentialité des données transmises [30].

   b) Fonctionnement de SSTP : SSTP fonctionne en encapsulant les paquets de données dans une connexion SSL/TLS. Cela permet aux données de traverser le réseau public (Internet) sans être exposées à des tiers malveillants. Le protocole utilise également le port 443, qui est généralement utilisé pour les connexions HTTPS, pour masquer le trafic VPN [30].

c) Avantages de SSTP :

SSTP présente plusieurs avantages en tant que protocole de tunneling VPN [28] :

— Sécurité renforcée : SSTP utilise le protocole SSL/TLS pour crypter les données et garantir la sécurité des communications entre les ordinateurs distants. Cela rend le protocole particulièrement utile pour les connexions VPN à des réseaux d'entreprise sensibles.

— Compatibilité avec le pare-feu : SSTP utilise le port 443, qui est souvent utilisé pour les connexions HTTPS, ce qui permet au protocole de contourner les restrictions de pare-feu qui bloquent généralement les connexions VPN.

— Facilité de configuration : SSTP est relativement facile à configurer par rapport à d'autres protocoles VPN, ce qui le rend accessible aux utilisateurs qui ne disposent pas d'une expertise technique approfondie.

— Disponibilité sur plusieurs systèmes d'exploitation : SSTP est pris en charge sur plusieurs systèmes d'exploitation, notamment Windows, Linux et macOS.

— Haute performance : SSTP est conçu pour offrir des performances élevées, même sur des connexions Internet à faible bande passante, ce qui en fait un choix idéal pour les utilisateurs distants qui ont besoin d'un accès rapide et fiable à leurs réseaux d'entreprise.

2. **La relation entre le protocole SSTP et L2TP :**

Les protocoles VPN SSTP (Secure Socket Tunneling Protocol) et L2TP (Layer 2 Tunneling Protocol) sont utilisés pour créer des connexions sécurisées entre les clients et les serveurs sur Internet. SSTP est un protocole de propriété de Microsoft qui fonctionne de manière optimale sur Windows, tandis que L2TP est disponible plus largement et facile à utiliser sur différents systèmes d'exploitation.

Les deux protocoles utilisent des méthodes de chiffrement pour protéger les données transmises sur Internet. Toutefois, L2TP utilise le protocole IPSec qui possède des algorithmes de cryptage plus sécurisés, ce qui en fait une option plus fiable que PPTP. SSTP peut être employé en remplacement d'autres protocoles VPN tels que PPTP et L2TP.

3.3 Administration et sécurité avancée dans les VPNs

3.3.1 Active Directory et Active Directory Certificate Services

a) **Définition AD :** Est un service d'annuaire développé par Microsoft pour centraliser la gestion des ressources informatiques d'une entreprise. Il permet de stocker et de gérer les informations relatives aux utilisateurs, groupes, ordinateurs et autres ressources réseau. Il facilite également l'authentification et l'autorisation des utilisateurs et des ordinateurs dans un environnement windows [29].

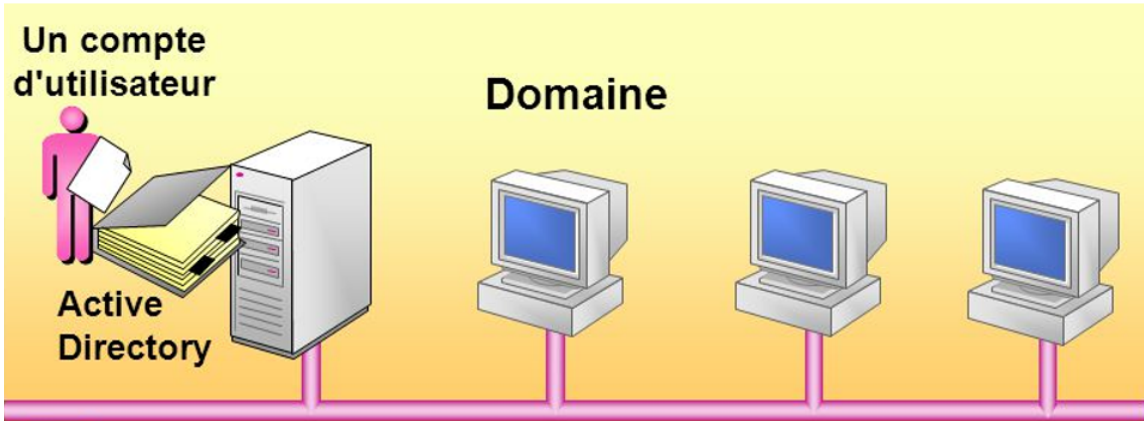


FIGURE 3.5 – Active Directory

b) Les différentes composant de AD :

Voici quelques composants importants d'un Active Directory [29] :

• Contrôleur de domaine : un serveur qui exécute le service Active Directory et qui gère les informations d'identification et les autorisations pour les ressources du domaine.

• Domaine : Un groupe de ressources informatiques, telles que des ordinateurs, des utilisateurs et des groupes, qui sont gérées en tant qu'unité dans un Active Directory.

• Unité d'organisation (OU) : Est un conteneur logique utilisé pour regrouper des objets Active Directory, tels que des ordinateurs, des utilisateurs et des groupes.

• Forêt : Est un ensemble de domaines qui partagent une structure de noms commune et une relation d'approbation. Une forêt peut également contenir des domaines qui n'ont pas de relation d'approbation .

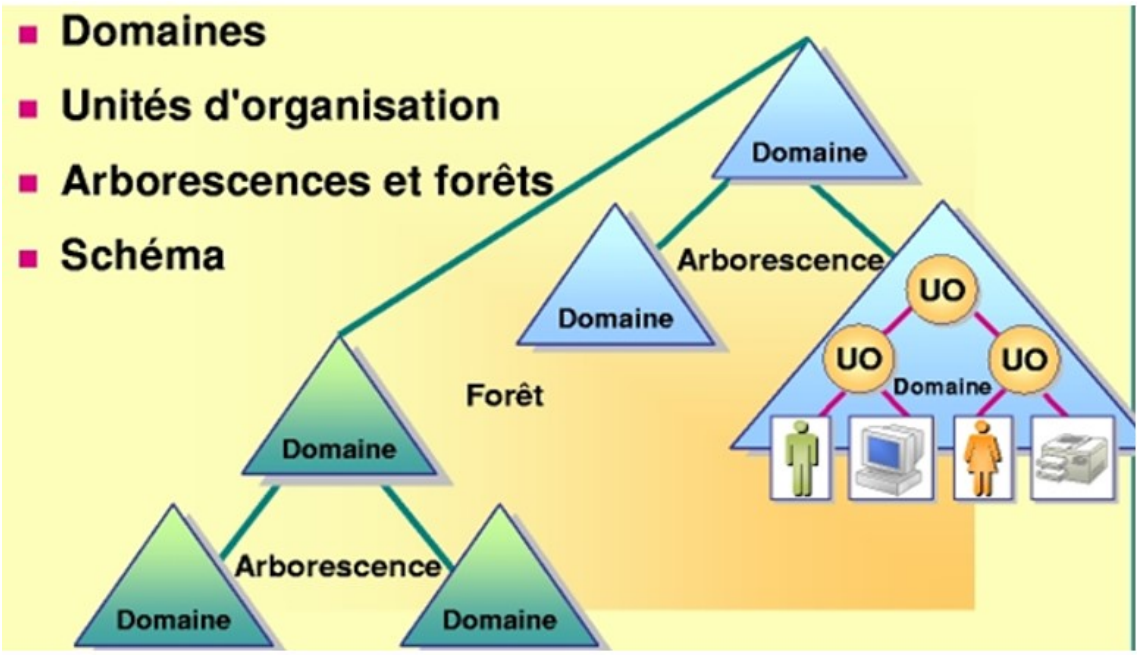


FIGURE 3.6 – Structure logique d'active directory

c) Types d'Active Directory : Il existe plusieurs types d'Active Directory, notamment [31] :

1. **Active Directory Domain Services (AD DS) :** C'est la forme la plus courante d'Active Directory et elle est utilisée pour stocker des informations sur les utilisateurs, les ordinateurs et les groupes dans un domaine. Il permet également la gestion des stratégies de groupe et l'authentification des utilisateurs et des ordinateurs.
2. **Active Directory Federation Services (AD FS) :** Il s'agit d'un service qui permet à des utilisateurs d'accéder à des applications et à des services situés en dehors de l'infrastructure de l'entreprise. AD FS permet l'authentification des utilisateurs à travers différents systèmes d'authentification.

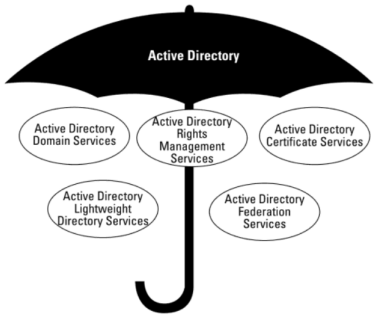


FIGURE 3.7 – Types d'Active Directory

3. **Active Directory Rights Management Services (AD RMS) :** Il s'agit d'un service qui permet de protéger les informations sensibles en limitant l'accès à ces informations à certaines personnes. AD RMS utilise des stratégies pour protéger les documents et les emails.
4. **Active Directory Certificate Services (AD CS) :** Il s'agit d'un service qui permet de gérer les certificats numériques utilisés pour l'authentification et le chiffrement. AD CS peut être utilisé pour déployer des certificats pour les utilisateurs, les ordinateurs et les services.

— **les rôles de serveur ADCS :**

Voici quelques rôles importants du serveur ADCS :

• Autorité de certification racine : une CA racine est la première autorité de certification dans une hiérarchie de certificats. Elle émet des certificats pour les autorités de certification intermédiaires et peut également émettre des certificats pour les clients [32].

• Autorité de certification intermédiaire (CA intermédiaire) : une CA intermédiaire est une autorité de certification qui émet des certificats pour les clients et les serveurs. Elle est signée par une CA racine et peut signer des certificats pour d'autres autorités de certification intermédiaires ou pour des clients [32].

•Autorité de certification autonome (CA autonome) :est une autorité de certification qui fonctionne indépendamment d'une hiérarchie de certificats. Elle peut être utilisée pour émettre des certificats pour des clients ou des serveurs qui ne font pas partie d'un domaine Active Directory [34].

3.3.2 Protocole RADUIS et la norme 802.1X

1. **Le protocole RADUIS :**

a) Définition : Le protocole RADIUS (Remote Authentication Dial-In User Service) est un protocole de sécurité informatique qui permet de centraliser l'authentification, l'autorisation et la comptabilité des connexions d'utilisateurs à un réseau. Il est largement utilisé dans les réseaux d'entreprise, les fournisseurs d'accès à Internet et les réseaux Wi-Fi pour contrôler l'accès des utilisateurs et des appareils. Le protocole RADIUS utilise des messages de requête et de réponse pour échanger des informations d'authentification et de contrôle d'accès entre le serveur RADIUS et les clients d'accès au réseau [10].

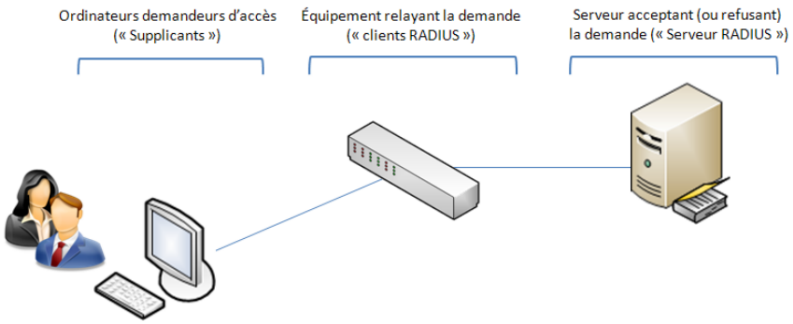


FIGURE 3.8 – Protocole Raduis

b) Le fonctionnement :

Le fonctionnement du protocole RADIUS implique plusieurs éléments [10] :

• Le serveur RADIUS : C'est le serveur qui gère les demandes d'authentification et d'autorisation. Il vérifie l'identité de l'utilisateur et autorise l'accès au réseau si l'utilisateur est authentifié.

• Le client RADIUS : C'est le client qui envoie les demandes d'authentification et d'autorisation au serveur RADIUS. Le client RADIUS peut être un point d'accès sans fil, un serveur VPN ou un commutateur réseau.

• L'utilisateur : C'est la personne qui tente de se connecter au réseau.

c) Le processus d'authentification RADIUS :

Le processus d'authentification RADIUS implique plusieurs étapes [16] :

1. L'utilisateur se connecte au réseau et fournit son nom d'utilisateur et son mot de passe.

2. Le client RADIUS envoie les informations d'identification de l'utilisateur au serveur RADIUS.

3. Le serveur RADIUS vérifie les informations d'identification de l'utilisateur en interrogeant une base de données d'utilisateurs. Cette base de données peut être stockée localement sur le serveur RADIUS ou sur un serveur d'annuaire distant.

4. Si l'utilisateur est authentifié, le serveur RADIUS envoie une réponse d'autorisation au client RADIUS, permettant ainsi à l'utilisateur d'accéder au réseau.

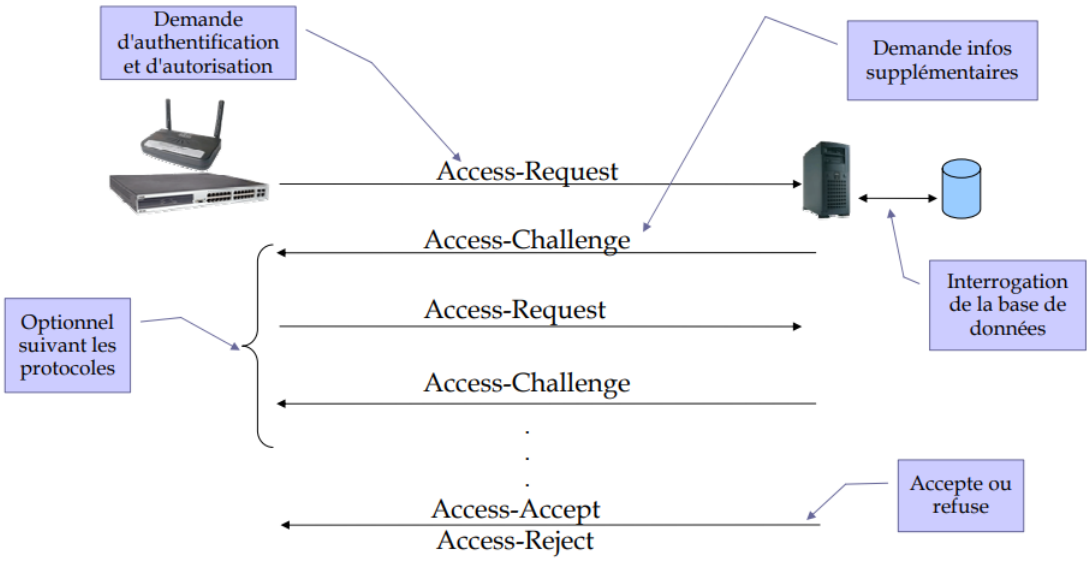


FIGURE 3.9 – Principe du protocole Radius

2. **La norme 802.1X :**

   a) Définition : La norme 802.1X est un protocole d'authentification réseau qui permet de contrôler l'accès aux réseaux filaires et sans fil. Elle fournit une méthode pour authentifier les utilisateurs ou les appareils avant de leur permettre de se connecter au réseau et permet de garantir la confidentialité des données transitant sur le réseau [35].

   b) La relation entre le protocole RADUIS et la norme 802.1X :

   Le protocole RADIUS est souvent utilisé en conjonction avec la norme 802.1X pour assurer l'authentification et l'autorisation des utilisateurs accédant à un réseau.

   La norme 802.1X définit le processus d'authentification des utilisateurs et des périphériques avant d'accorder l'accès au réseau, tandis que le protocole RADIUS est utilisé pour transmettre les informations d'identification de l'utilisateur et les autorisations d'accès au réseau à un serveur d'authentification centralisé. Ainsi, la norme 802.1X et le protocole RADIUS travaillent ensemble pour assurer un accès sécurisé et contrôlé aux réseaux [10].

3.3.3 Protocoles d'authentification

a) Le protocole EAP : Le protocole EAP (Extensible Authentication Protocol) est un protocole d'authentification des utilisateurs sur un réseau. Il permet de transporter des mécanismes d'authentification différents tels que les certificats, les mots de passe, les jetons de sécurité, etc [27].

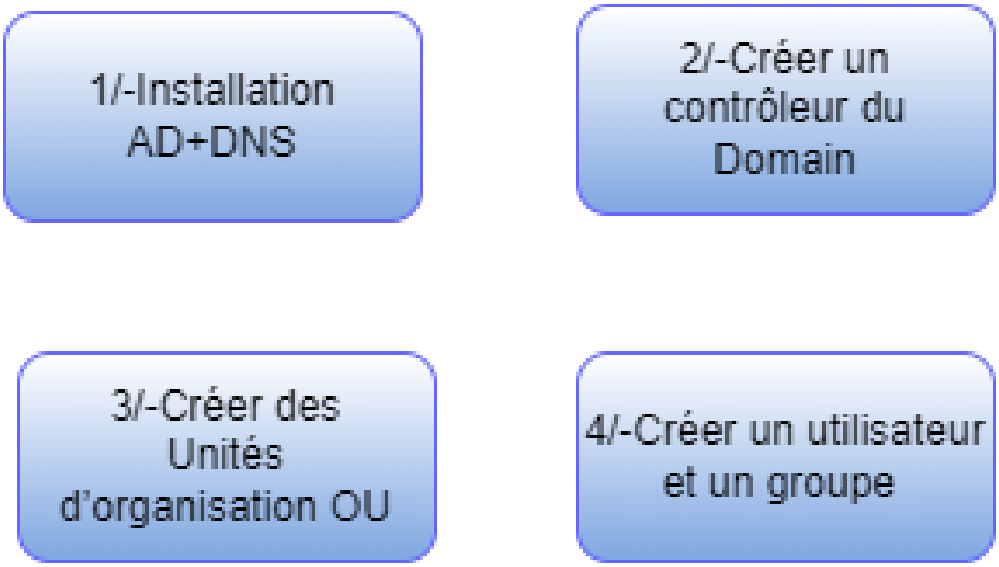
b) Le protocole PEAP : PEAP (Protected Extensible Authentication Protocol) est un protocole d'authentification de réseau sans fil qui permet une authentification sécurisée des utilisateurs et des appareils à travers des tunnels chiffrés. Il est basé sur le protocole EAP et utilise des certificats pour établir une connexion sécurisée entre le client et le serveur[35].

c) **Le protocole EAP/TLS :** Est un mécanisme d'authentification utilisé pour sécuriser les connexions dans les réseaux informatiques. Il combine l'EAP, qui offre une flexibilité dans le choix des méthodes d'authentification, avec TLS, qui fournit une sécurité et une confidentialité des données échangées.

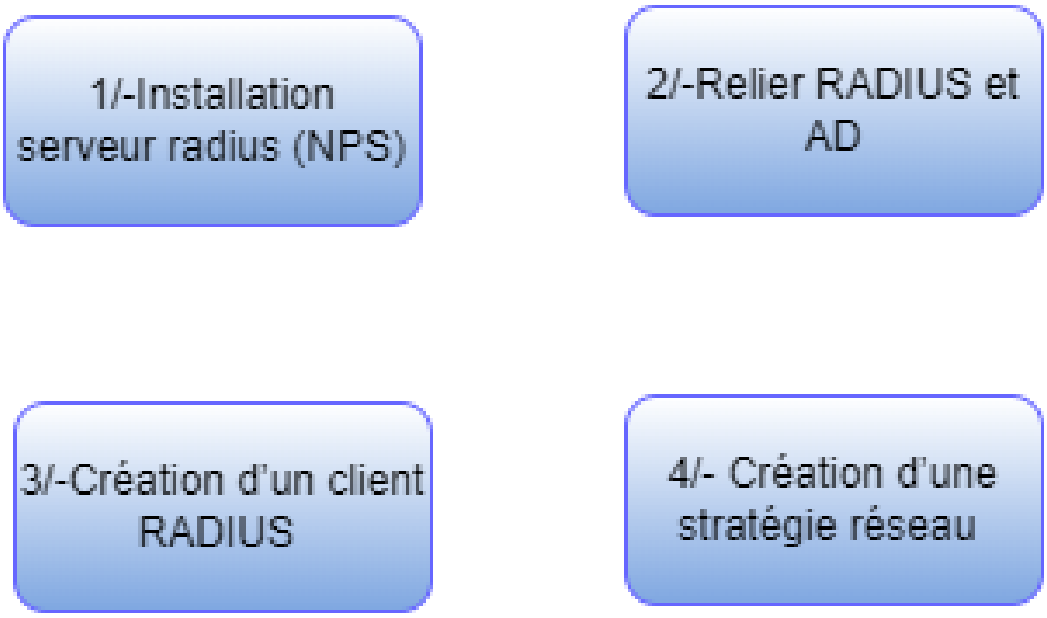
3.3.4 Ingénierie d'implimentation, choix de la solution

J'ai configuré deux serveurs pour répondre à différents besoins. Le premier serveur est équipé d'un rôle de serveur Active Directory, un serveur RADIUS (Service d'authentification d'utilisateur par composition d'un numéro d'appel distant) et un service de certificat Active Directory. Le deuxième serveur, quant à lui, a été installé avec un rôle de serveur VPN.
De plus, j'utilise un client Windows (ClientVPN) pour une connexion sécurisée au réseau interne de l'entreprise via le VPN SSTP.

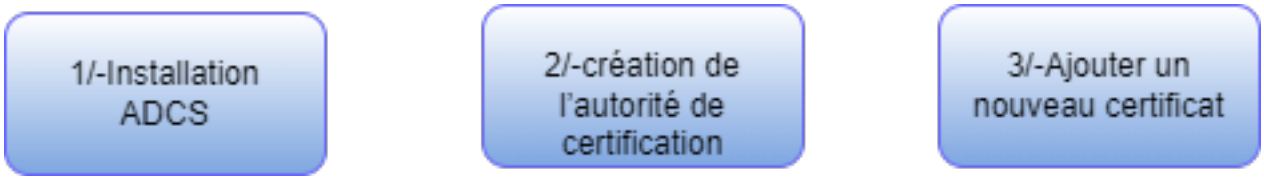
— Etapes à suivre, dans l'ordre, pour réaliser la configuration AD (Active Directory) et DNS (Domain Name System).



— Etapes à suivre, dans l'ordre, pour réaliser la configuration NPS RADIUS.



— Etapes à suivre, dans l'ordre, pour réaliser la configuration du service de certificats Active Directory (ADCS).



— Etapes à suivre, dans l'ordre, pour réaliser la configuration VPN (Virtual Private Network).

3.4 Conclusion

Ce chapitre a couvert les notions de base sur les VPNs, y compris leur définition, leur topologie, leur fonctionnement et leurs avantages. Nous avons également exploré les différents protocoles utilisés dans les VPNs, notamment le protocole SSTP pour une sécurité renforcée. En ce qui concerne l'administration et la sécurité avancée, nous avons abordé l'utilisation d'Active Directory, du protocole RADIUS et de la norme 802.1X. De plus, le protocole EAP et PEAP/TLS ont été présentés pour assurer une authentification sécurisée des utilisateurs. L'ensemble de ces connaissances permet de mettre en place un VPN robuste, sécurisé et fiable pour l'accès distant aux ressources de l'entreprise.

Chapitre 4

Réalisation et test

4.1 Introduction

Ce chapitre aborde la mise en œuvre du projet, en détaillant les conditions préalables et les étapes de configuration nécessaires à l'installation de différents logiciels et systèmes.
Cette section constitue le corps principal de ce mémoire, agrémenté de captures d'écran pour une meilleure compréhension.

4.2 Environnement de travail

4.2.1 Outils utilisés pour la réalisation du projet

VMware Workstation version 17 pro :

VMware Workstation version 17 Pro est un logiciel de virtualisation de bureau qui permet d'exécuter plusieurs systèmes d'exploitation sur un même ordinateur. Il est utilisé par les professionnels de l'informatique pour le développement, le test et la démonstration de logiciels et de configurations de réseau.

FIGURE 4.1 – VMware Workstation

Wireshark :

Wireshark est un logiciel open-source d'analyse de paquets réseau. Il est utilisé pour la détection et le dépannage de problèmes de réseau.

FIGURE 4.2 – Wireshark.

Windows Server 2022 :

Windows Server 2022 est la dernière version du système d'exploitation de Microsoft pour les serveurs. Il offre des fonctionnalités avancées pour la gestion des serveurs, la virtualisation, la sécurité, le stockage et les applications cloud. Windows Server 2022 est conçu pour répondre aux besoins des entreprises modernes et facilite la migration vers le cloud hybride.

FIGURE 4.3 – Windows Server 2022.

Windows 10 :

Windows 10 est un système d'exploitation développé par Microsoft pour les ordinateurs personnels. Il est la version la plus récente de la famille de systèmes d'exploitation Windows. Windows 10 propose de nombreuses fonctionnalités, y compris un menu de démarrage amélioré, une interface utilisateur moderne et une sécurité renforcée.

FIGURE 4.4 – Windows 10.

4.2.2 L'architecture proposée

La figure suivante illustre l'architecture du réseau que j'ai réalisée pour l'entreprise NTS

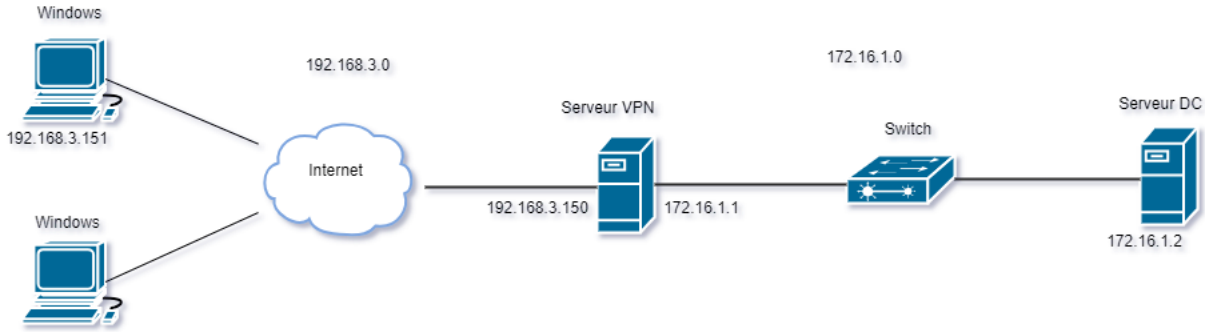


FIGURE 4.5 – L'architecture proposée.

4.2.3 Plan d'adressage

1. **Table d'adressage réseaux :**

	Adresse réseaux
LAN	172.16.1.0/24
WAN	192.168.3.0/24
Tunnel VPN	10.2.2.0/24

TABLE 4.1 – Tableau d'adresses réseau

2. **Table d'équipement :** Le tableau ci-dessous, montre l'attribution des adresses IP.

Nom d'équipement	@IP LAN	@IP WAN	Gateway	@DNS
DC	172.16.1.2		172.16.1.1	172.16.1.2
Serveur VPN	172.16.1.1	192.168.3.150		172.16.1.2
Client VPN		192.168.3.151	192.168.3.150	

TABLE 4.2 – Tableau d'adressage et équipements.

4.3 Installation des systèmes

4.3.1 Installation de la machine virtuelle Windows Server 2022 sous nom (DC)

J'effectue l'installation de la machine virtuelle Windows Server 2022 sous le nom "DC" en suivant les étapes après avoir ajouté son image sur VMWare Workstation.

Ci-dessous la figure qui montre la page d'accueil de serveur :

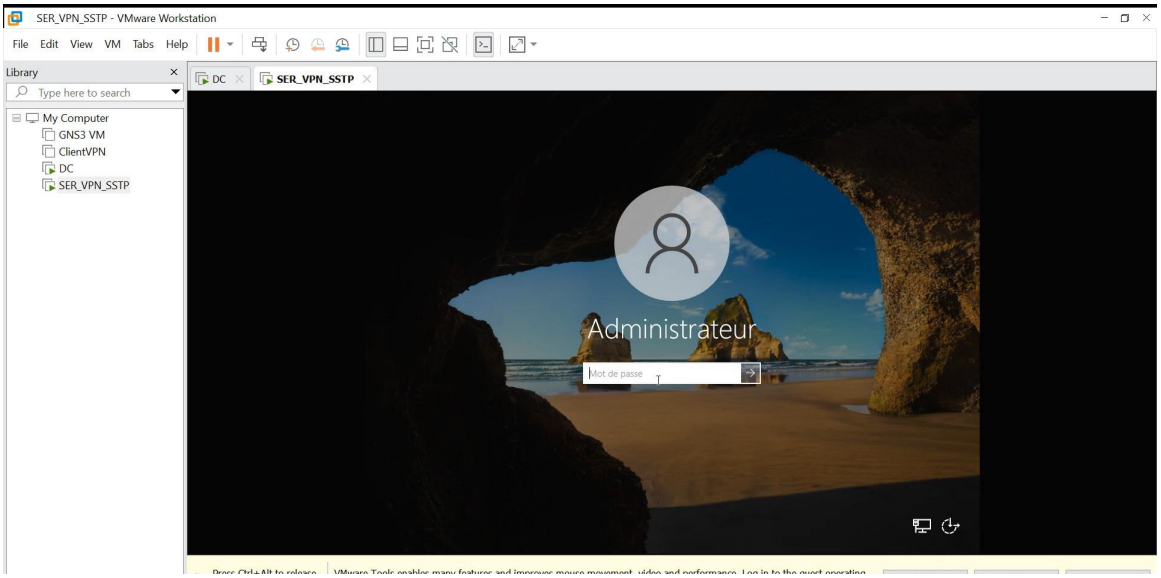


FIGURE 4.6 – La page d'accueil de Windows server 2022.

4.3.2 Installation et configuration de l'Active Directory (AD)+DNS :

1. **Installation AD+DNS :** Sur le serveur Windows, un contrôleur de domaine a été installé avec le nom de domaine "campusnts.com". Pour commencer l'installation, il est nécessaire d'ajouter le Service de rôle Active Directory. Lancez l'installation et ajoutez les fonctionnalités manquantes. La figure suivante montre les étapes d'installation :

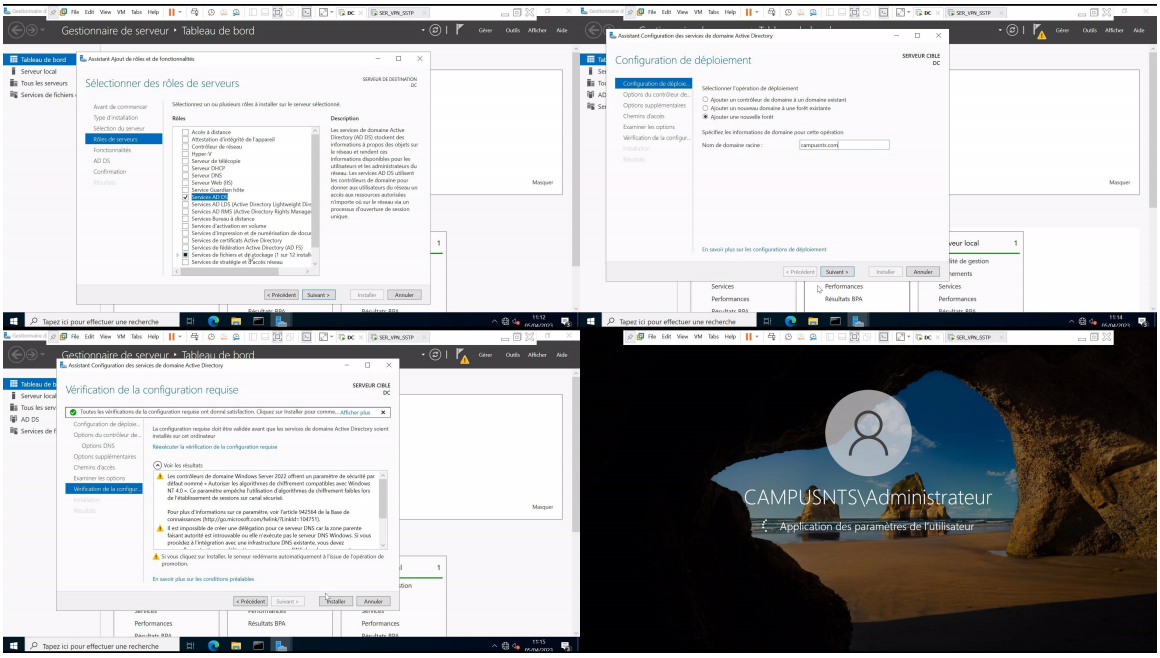


FIGURE 4.7 – Installation de l'active directory.

2. **Créer un contrôleur du Domain :** Une fois installé, je commence la configuration de l'Active Directory. La première étape consiste à ajouter une nouvelle forêt nommée campusnts.com. Ensuite, Windows me demande de sélectionner le niveau fonctionnel de la nouvelle forêt Active Directory. Dans mon cas, je vais placer un niveau de fonctionnalité de 2016. Windows me donne alors des options supplémentaires à installer, telles qu'un serveur DNS compatible avec mon Active Directory. Après avoir configuré et installé le service, le système nécessitera un redémarrage.

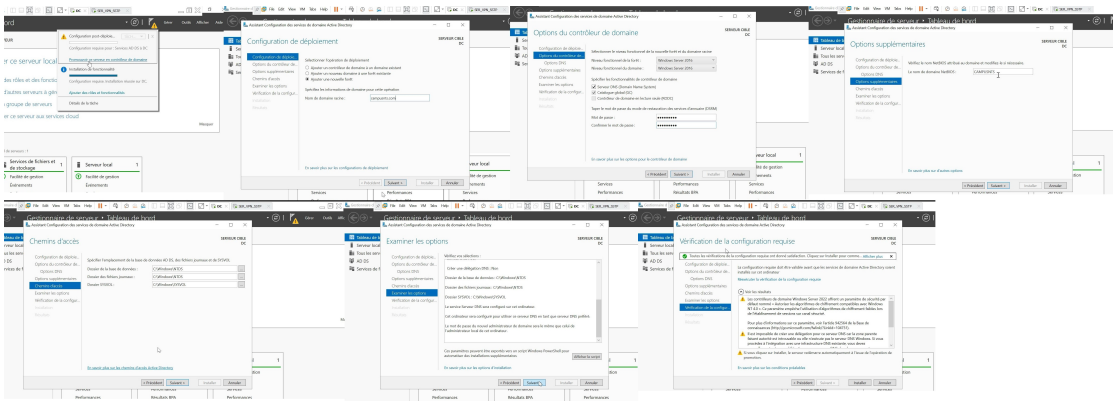


FIGURE 4.8 – Configuration des services de domaine active directory.

3. **Créer une Unité d'organisation OU :** Avec les deux rôles AD et DNS installés, je peux créer une nouvelle unité d'organisation en quelques clics. Tout d'abord, je me rends dans "outils" -> "utilisateurs et ordinateurs AD", puis je sélectionne le nom de mon domaine "campusnts.com". Ensuite, je clique sur le bouton droit de la souris et je choisis "nouveau" -> "Unité d'organisation". Je donne ensuite un nom à mon unité d'organisation, comme "site-béjaia". Avec cette nouvelle unité d'organisation, je peux organiser et gérer efficacement mes utilisateurs et ordinateurs AD.

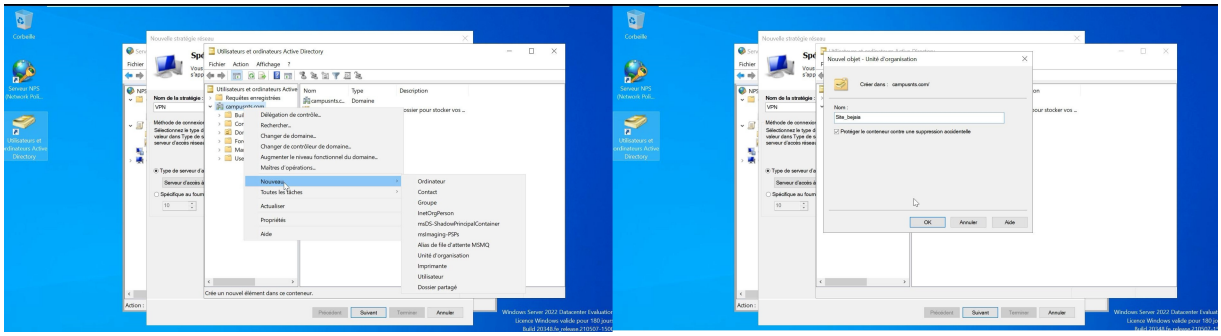


FIGURE 4.9 – Création une Unité d'organisation OU.

4. **Créer un utilisateur et un groupe :** Pour créer un compte utilisateur, je dois accéder à la section "Utilisateur" et cliquer sur le bouton "Nouveau". Ensuite, je remplis les informations correspondantes à l'utilisateur et définis un mot de passe pour sa session. Après validation, je peux créer des groupes et des ordinateurs pour l'utilisateur nouvellement créé. Enfin, j'ajoute l'utilisateur au groupe et lui donne l'accès à l'ordinateur. Je suis ces étapes pour une gestion efficace des comptes utilisateur.

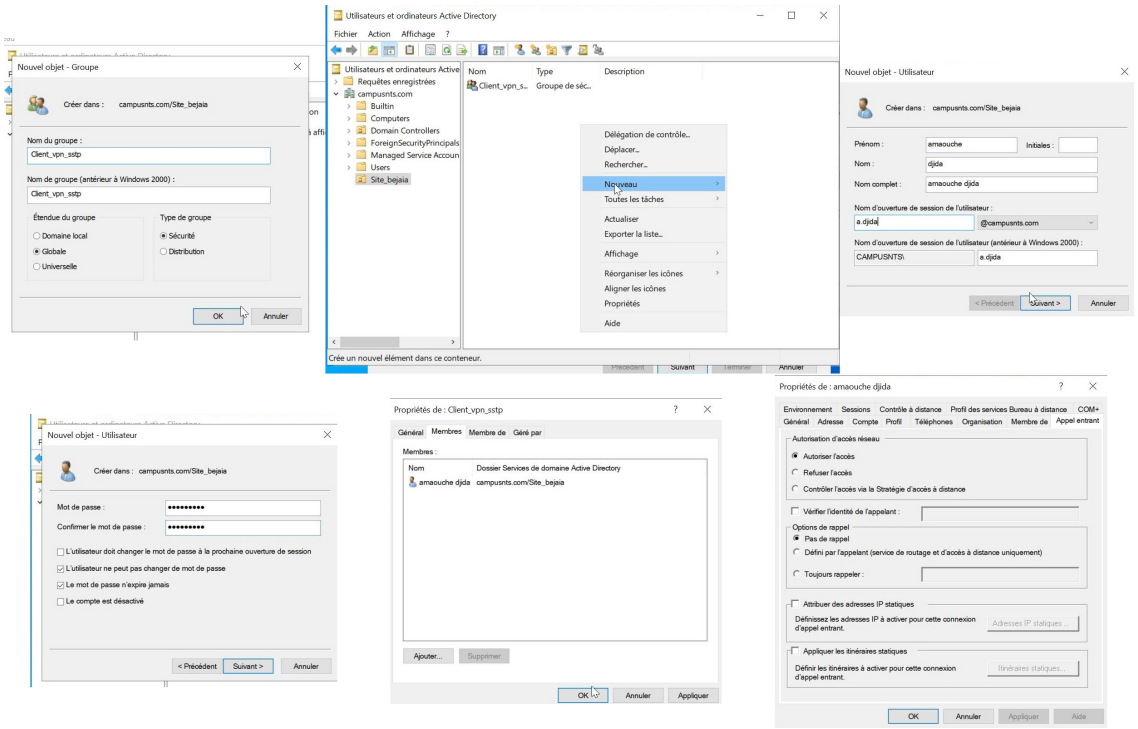


FIGURE 4.10 – Création un utilisateur et un groupe.

4.3.3 Installation et configuration de RADIUS

1. **Installation NPS :**

   J'ouvre le Gestionnaire de serveur et je clique sur "Ajouter des rôles et des fonctionnalités". Ensuite, je clique sur "Suivant" jusqu'à arriver à la page "Sélectionner des rôles de serveur". Je choisis "Services de stratégie et d'accès réseau" et je clique sur "Suivant" jusqu'à arriver à la page "Sélectionner des fonctionnalités". Je sélectionne "Serveur de stratégie réseau" et je clique sur "Suivant" jusqu'à arriver à la page "Installer"..

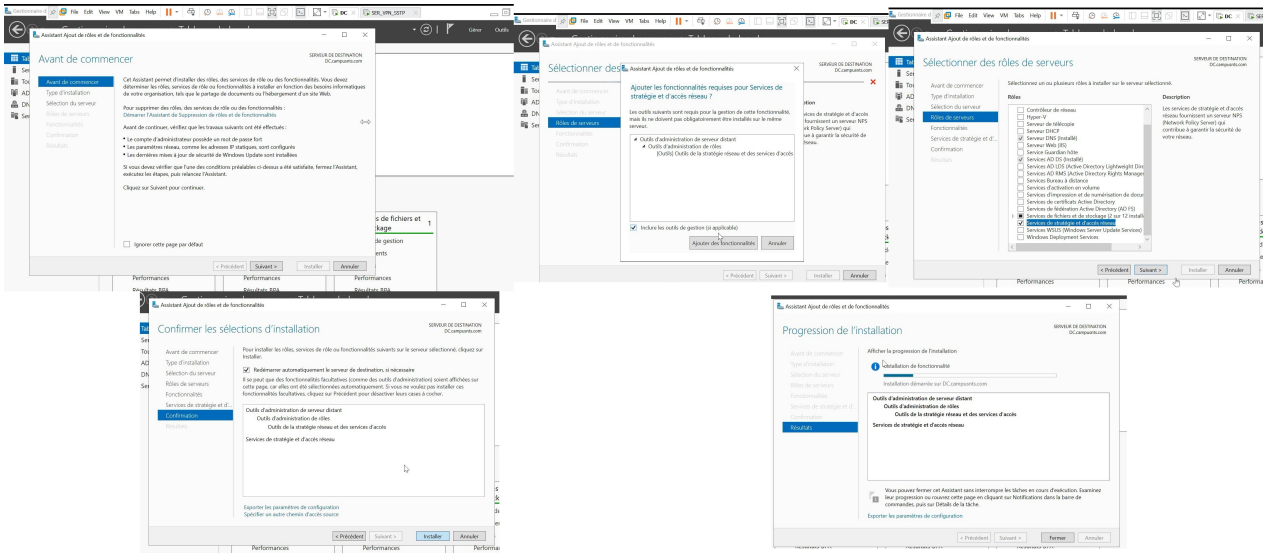


FIGURE 4.11 – Installation NPS.

Enfin, je relie le serveur NPS avec AD, comme la figure ci-dessus le montre.

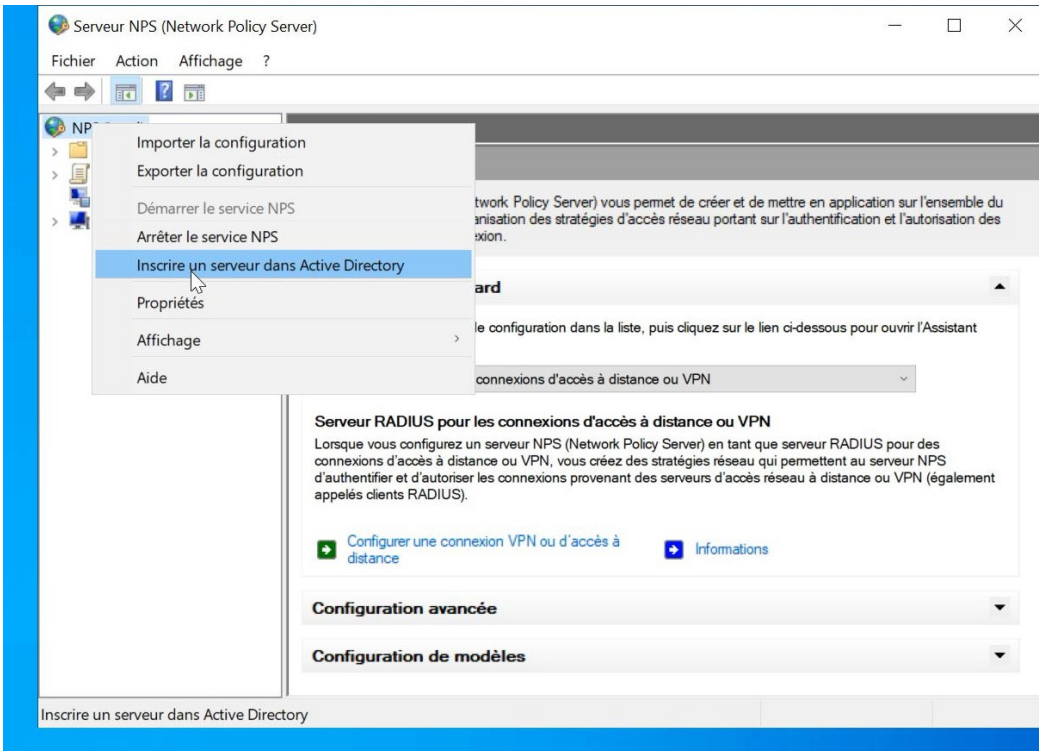


FIGURE 4.12 – Inscription de NPS avec AD.

2. **Création d'un client RADIUS :**

   Dans la console NPS, je clique sur l'onglet "Clients RADIUS". Ensuite, je fais un clic droit sur l'espace vide dans la fenêtre "Clients RADIUS" et je sélectionne "Nouveau client". Dans la boîte de dialogue "Nouveau client RADIUS", je saisis les informations du client.

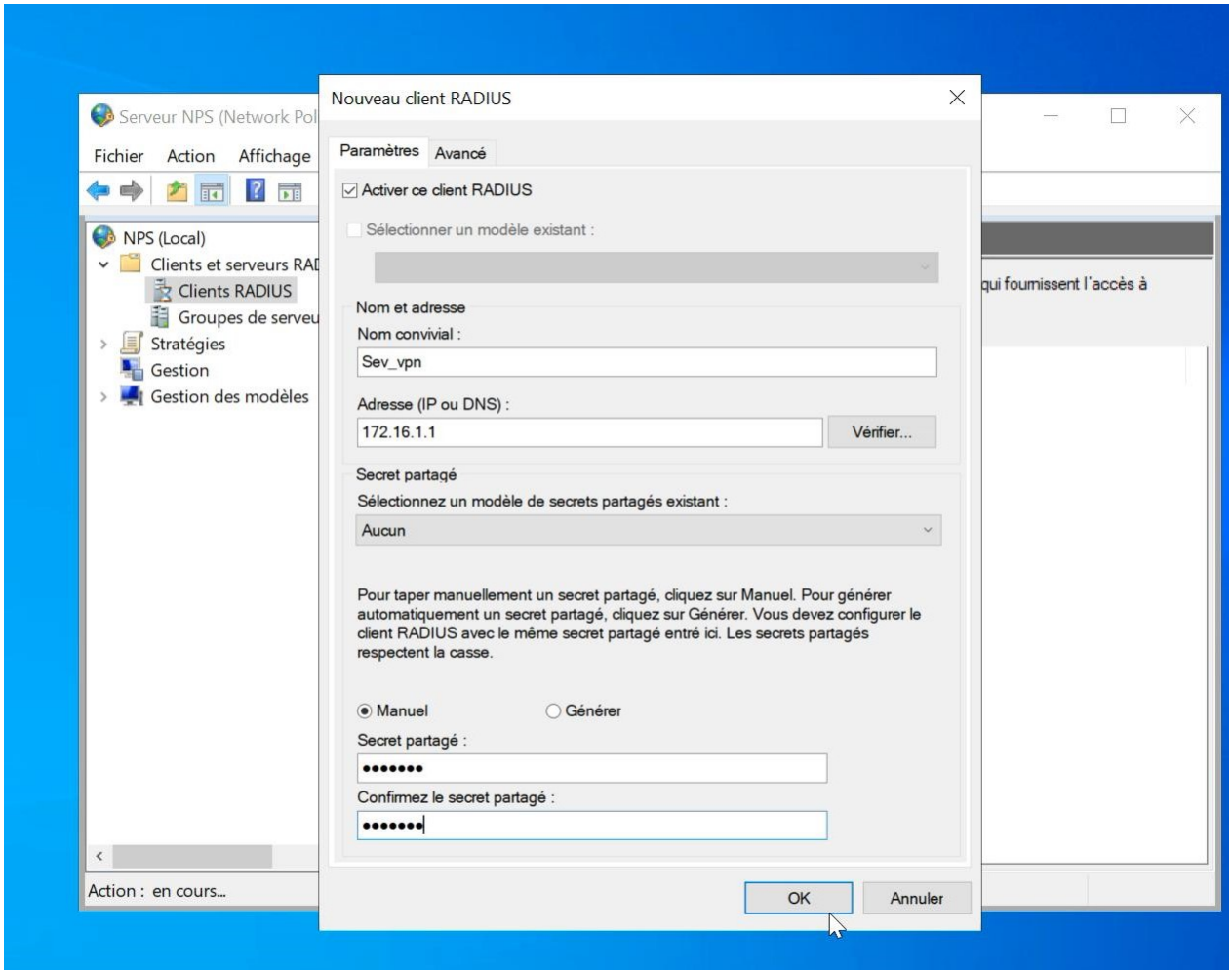


FIGURE 4.13 – Création d'un client RADIUS.

3. **Création d'une stratégie réseau :**

   Je clique avec le bouton droit de la souris sur l'espace vide dans la fenêtre "Stratégies réseau", puis je sélectionne "Nouvelle stratégie". Dans la boîte de dialogue "Assistant Nouvelle stratégie réseau", je suis les instructions pour configurer les paramètres de la stratégie réseau :

   — Nom de la stratégie : vpn.

   — Type d'accès réseau : serveur d'accès à distance.

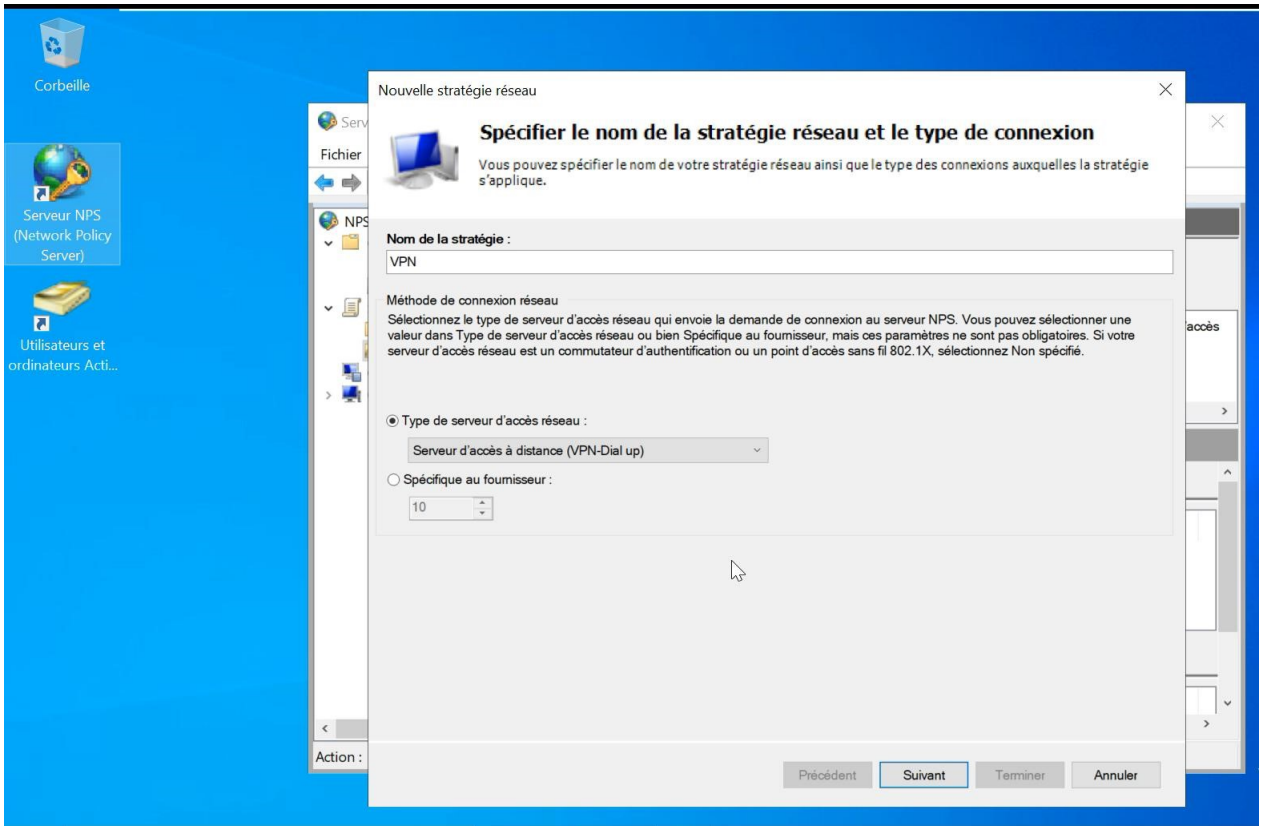
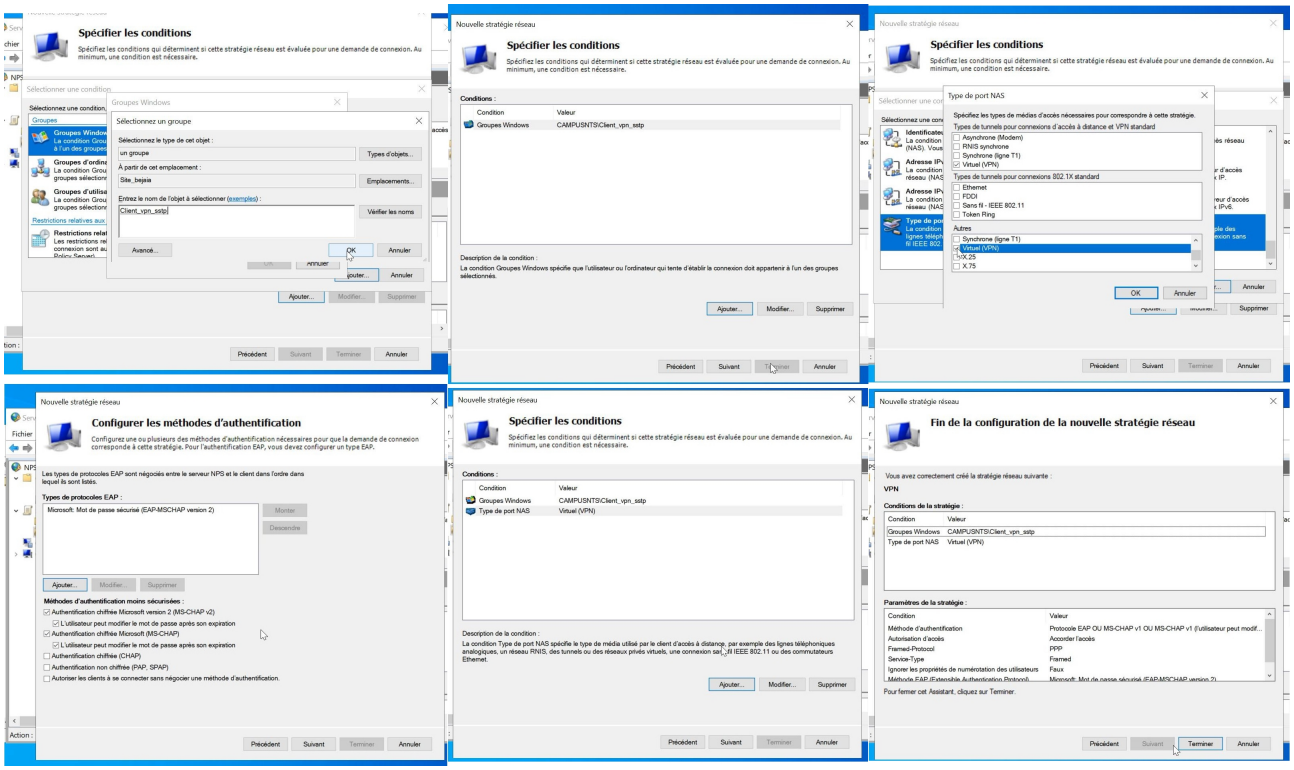


FIGURE 4.14 – Création d'une nouvelle stratégie.

— Autorisations : Je définis le groupe d'utilisateurs (Client-vpn-sstp), spécifie le type de média d'accès nécessaire et fais correspondre cette stratégie.

— Conditions d'authentification : Je configure les conditions d'authentification requises pour accéder au réseau, telles que le nom d'utilisateur, le groupe d'utilisateurs ou les informations de certificat.

— Je clique sur "Terminer" pour enregistrer la nouvelle stratégie réseau.



4.3.4 Installation et configuration du service de certificats Active Directory (ADCS) :

1. **Installation du service de certificats Active Directory (ADCS) :**

   Je vais installer le serveur de certificat sur la machine Windows Server. Pour commencer l'installation, je vais ajouter les services de certificats Active Directory. Ensuite, je vais lancer l'installation et ajouter les fonctionnalités nécessaires.

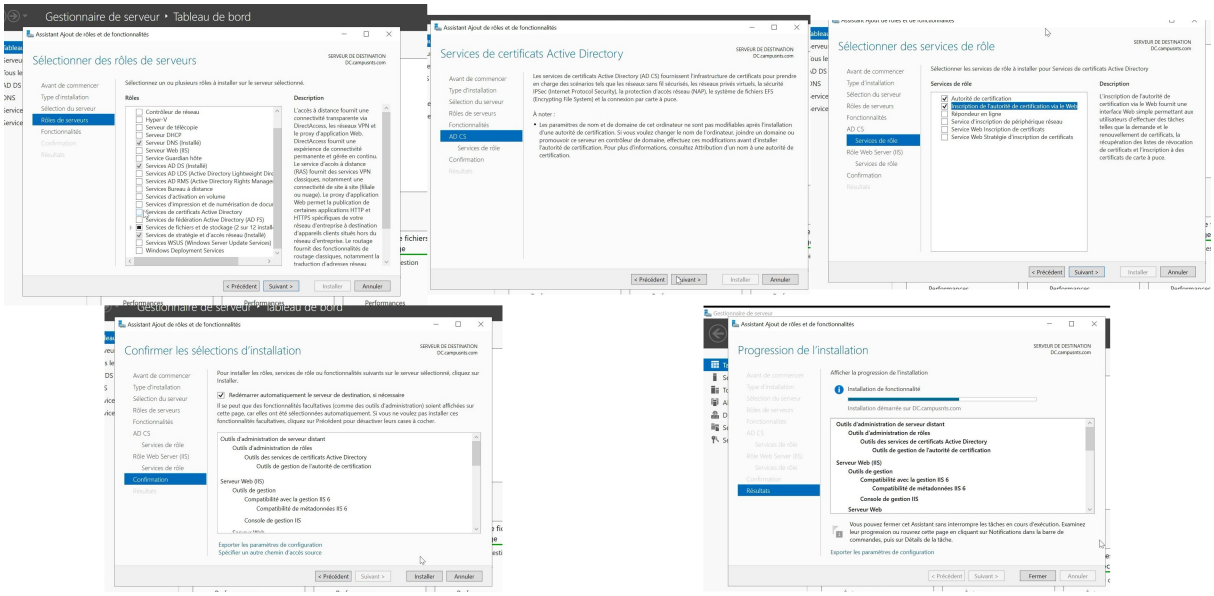


FIGURE 4.15 – Installation de l'ADCS.

2. **Configuration de ADCS et création de l'autorité de certification :**

   Depuis le gestionnaire de serveur, je clique sur l'icône de notification, puis je configure les services de certificats Active Directory pour ouvrir l'assistant de configuration. Ensuite, j'indique mon compte utilisateur, je coche l'autorité de certificat et je choisis le type "Autorité de certification d'entreprise". Je sélectionne une clé privée, je configure le chiffrement de la clé et je valide les informations.

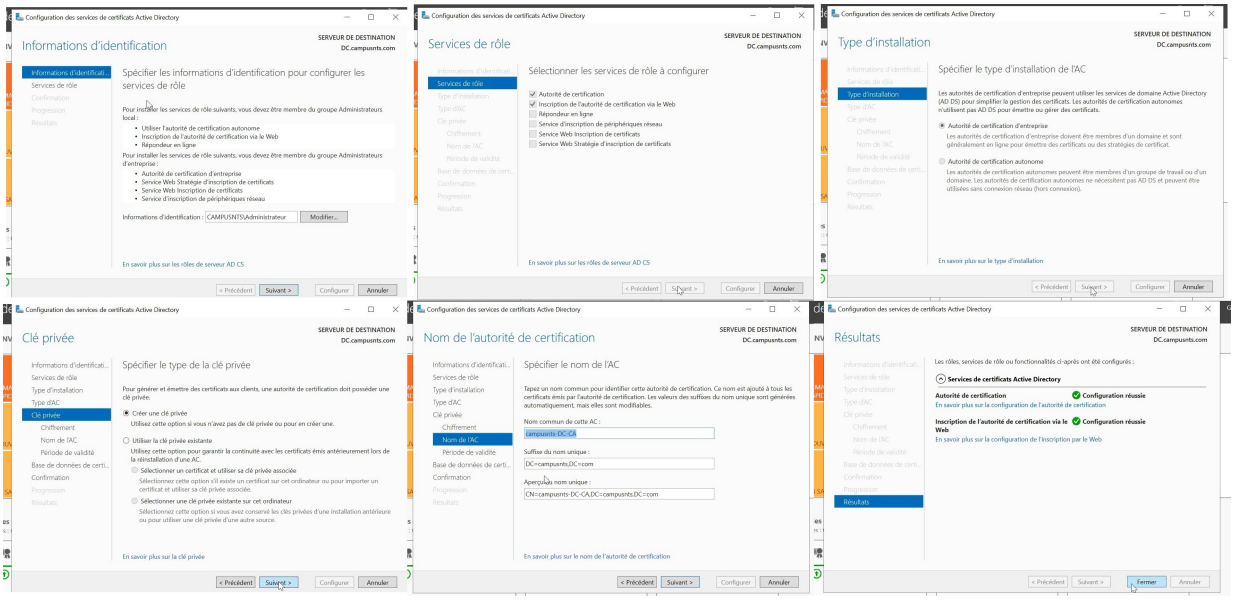


FIGURE 4.16 – Configuration de l'ADCS.

3. **Ajouter un nouveau certificat :**

   J'ouvre la console de gestion ADCS sur le serveur où le service ADCS est installé. Ensuite, je clique avec le bouton droit de la souris sur le dossier Certificats, je sélectionne "Toutes les tâches" et "Demander un nouveau certificat".

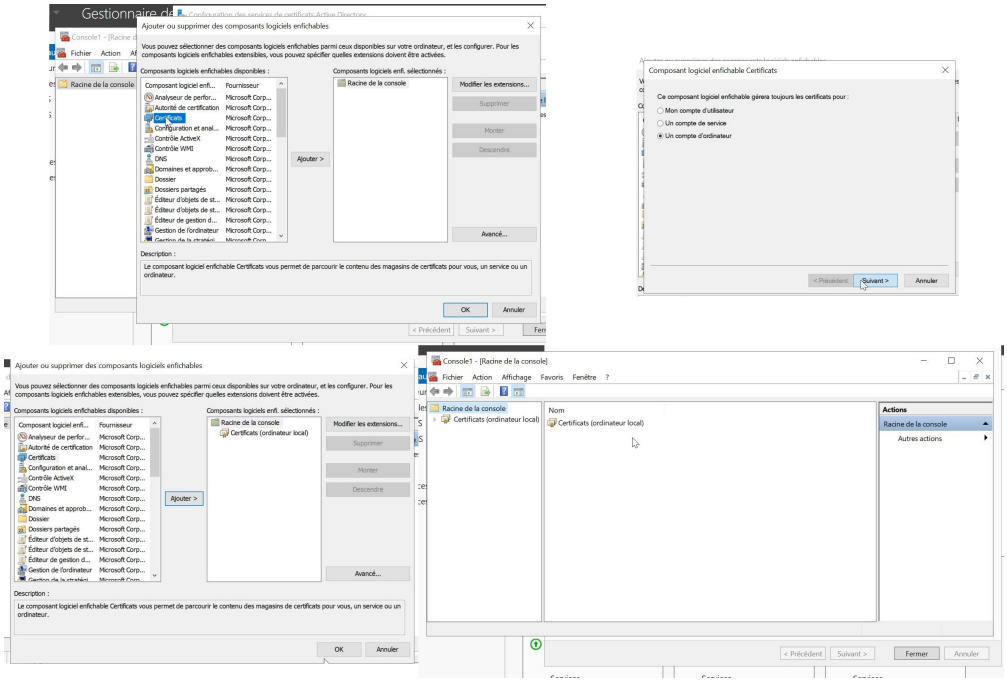


FIGURE 4.17 – Création d'un nouveau certificat.

4.3.5 Installation de la machine virtuelle Windows Server 2022 sous le nom (SER-VPN-SSTP)

J'installe la machine virtuelle Windows Server 2022 sous le nom "SER-VPN-SSTP", après avoir ajouté son image sur VMWare Workstation et en suivant les étapes.

Ci-dessous la figure qui montre la page d'accueil de serveur :

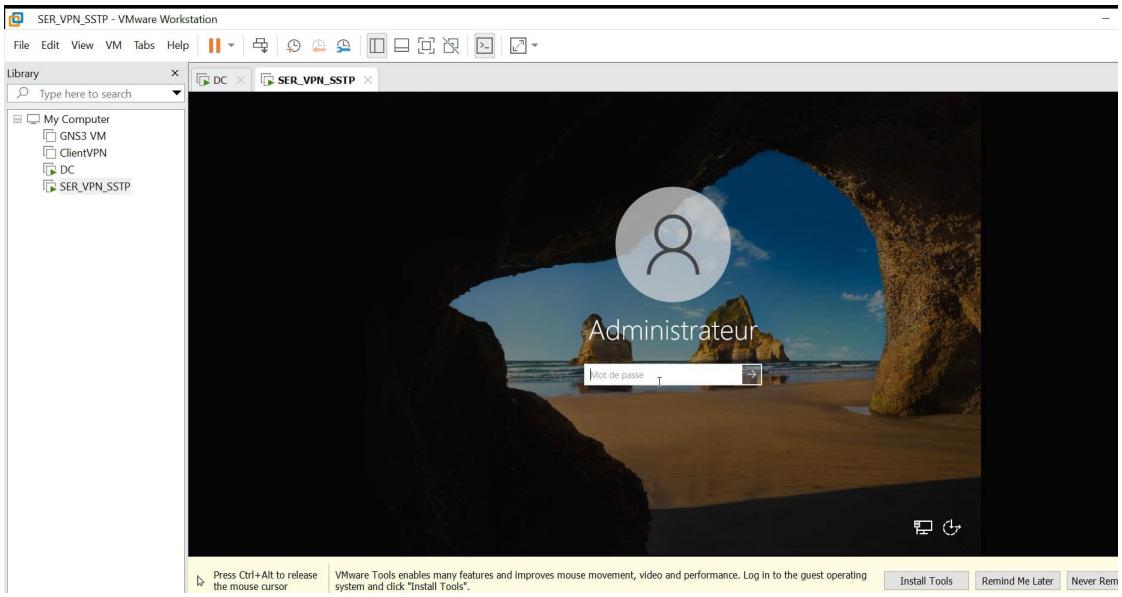


FIGURE 4.18 – Installation de la machine virtuelle Windows Server 2022.

1. **Connecter le serveur au domaine :**

Je vais connecter le serveur SER-VPN-SSTP au domaine campusnts.com.

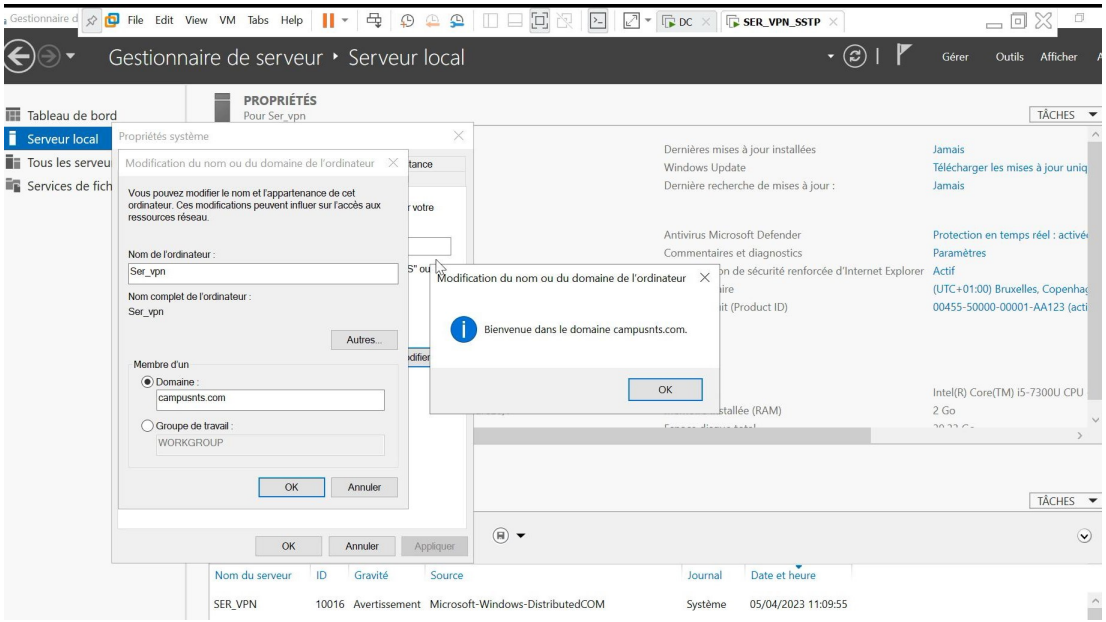


FIGURE 4.19 – connection de serveur vers le domaine.

2. **Installer le rôle VPN :**

   J'accède au Gestionnaire de serveur et je clique sur "Ajouter des rôles et des fonctionnalités". Je parcours les options et je sélectionne le rôle de serveur VPN. Ensuite, je suis les étapes d'installation pour configurer le serveur VPN.

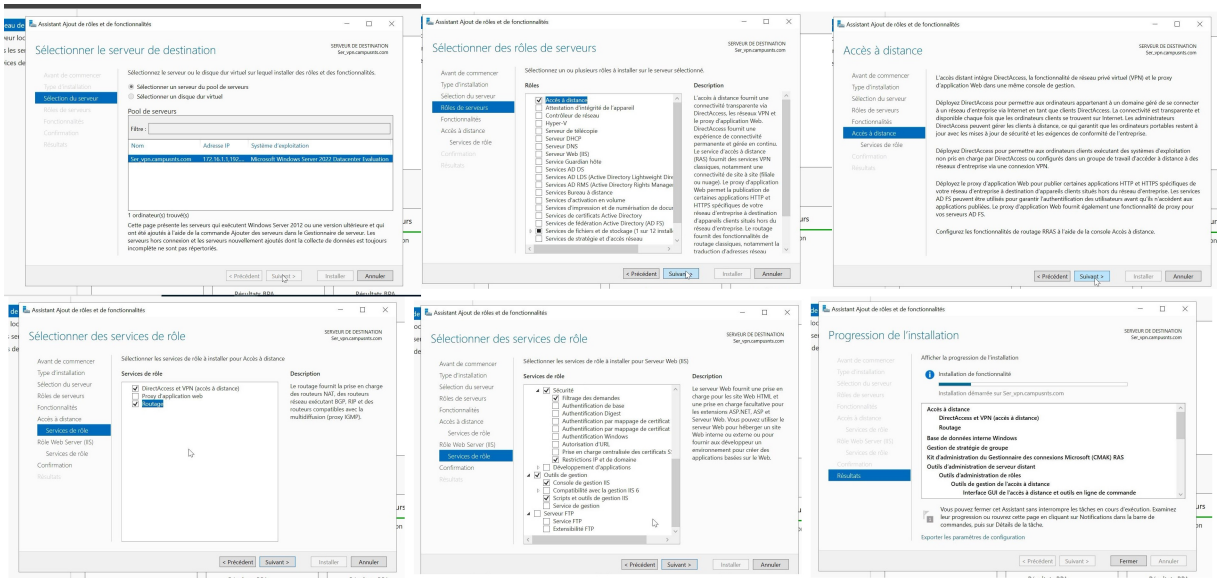


FIGURE 4.20 – Installation du VPN.

3. **Configurer et activer le serveur VPN :**

   J'accède au gestionnaire de serveur VPN pour configurer les paramètres de connexion. Je vais notamment configurer les certificats d'authentification, définir les limites d'utilisation et effectuer d'autres réglages nécessaires

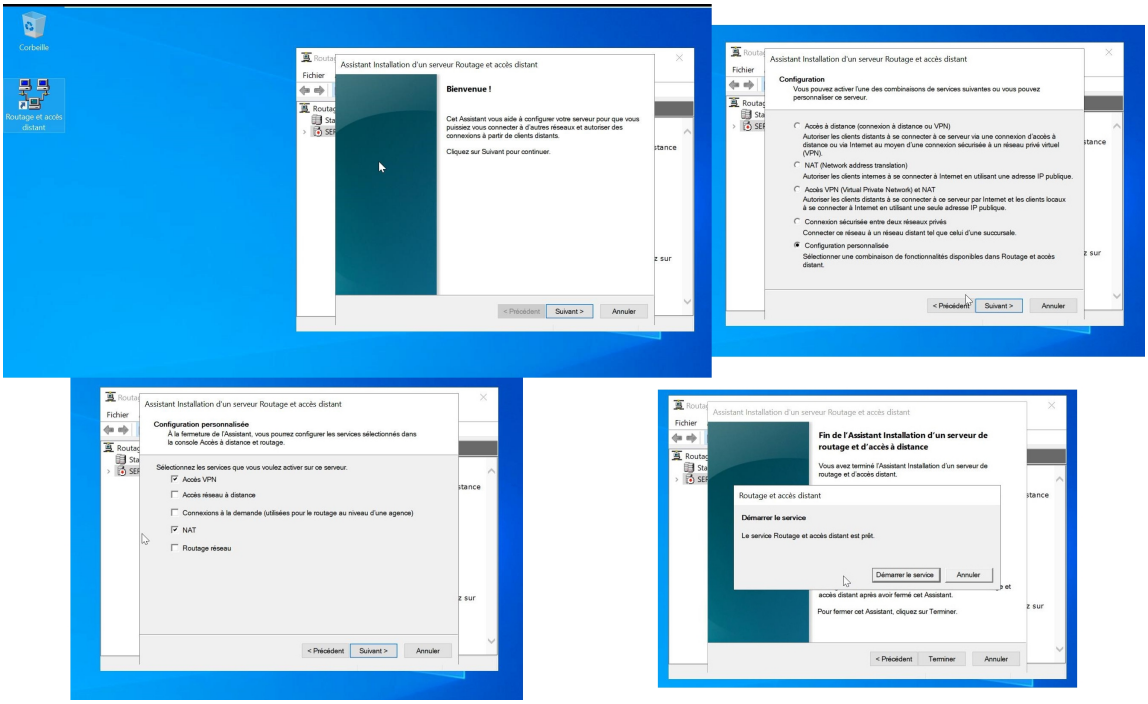
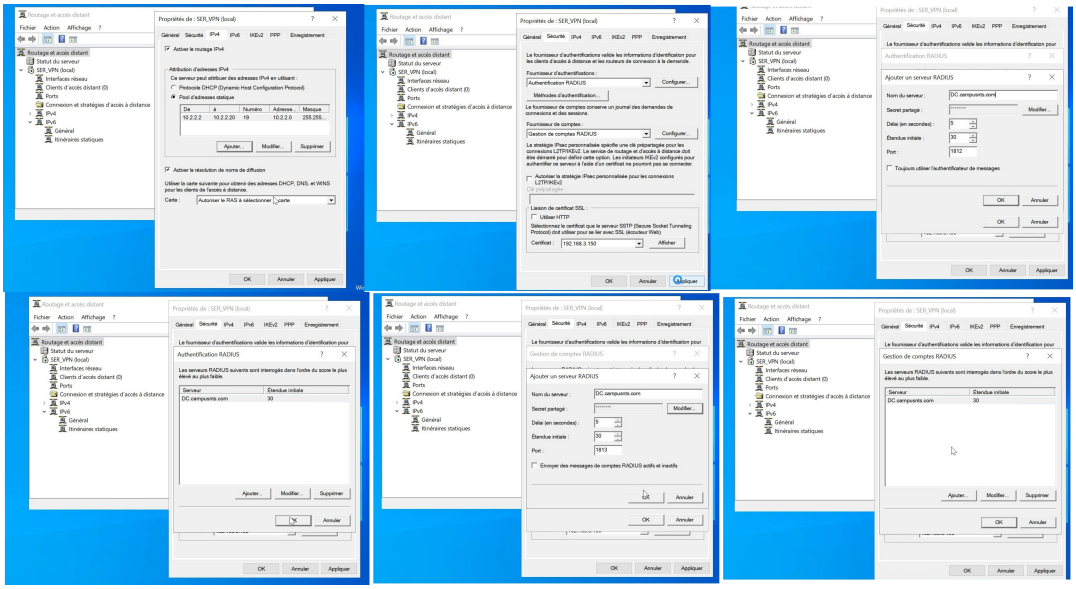
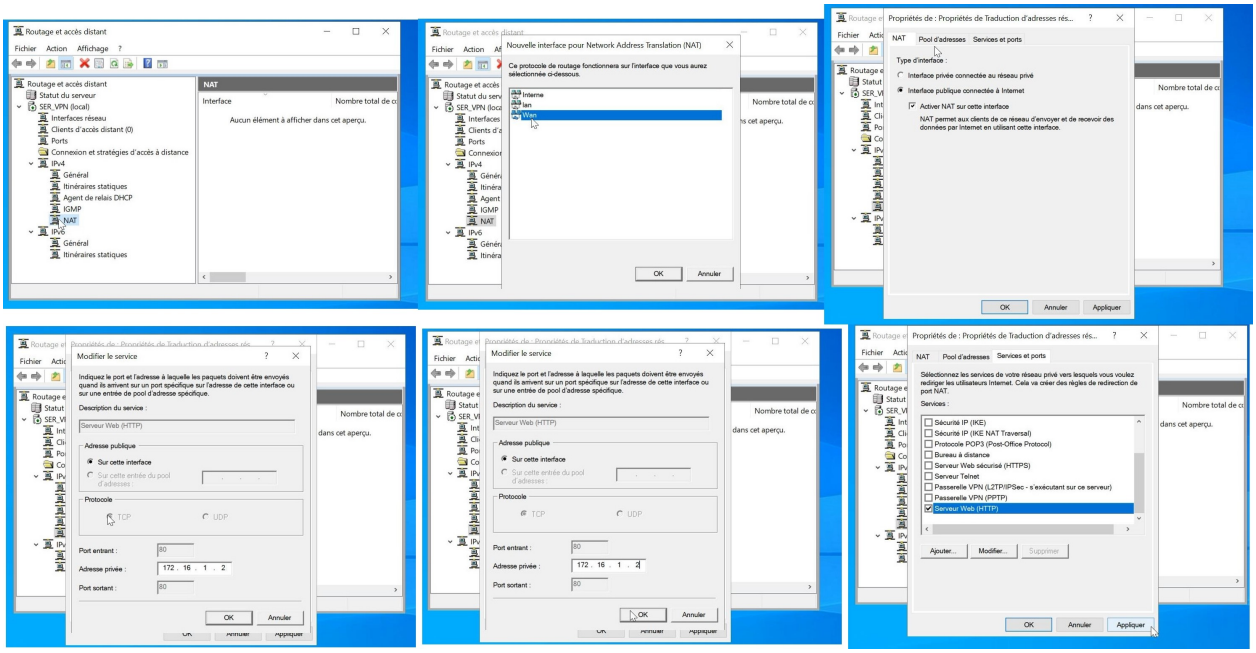


FIGURE 4.21 – Configuration du VPN.

Ci-dessous la figure qui montre les etape a suivre pour Paramétrez le serveur VPN et activez le NAT (Network Address Translation).





4.3.6 Installation de la machine virtuelle Windows 10

J'installe la machine virtuelle Windows 10 avec le nom "ClientVPN" après avoir ajouté son image sur VMWare Workstation et en suivant les étapes nécessaires. Ci-dessous la figure qui montre la page d'accueil de Windows :

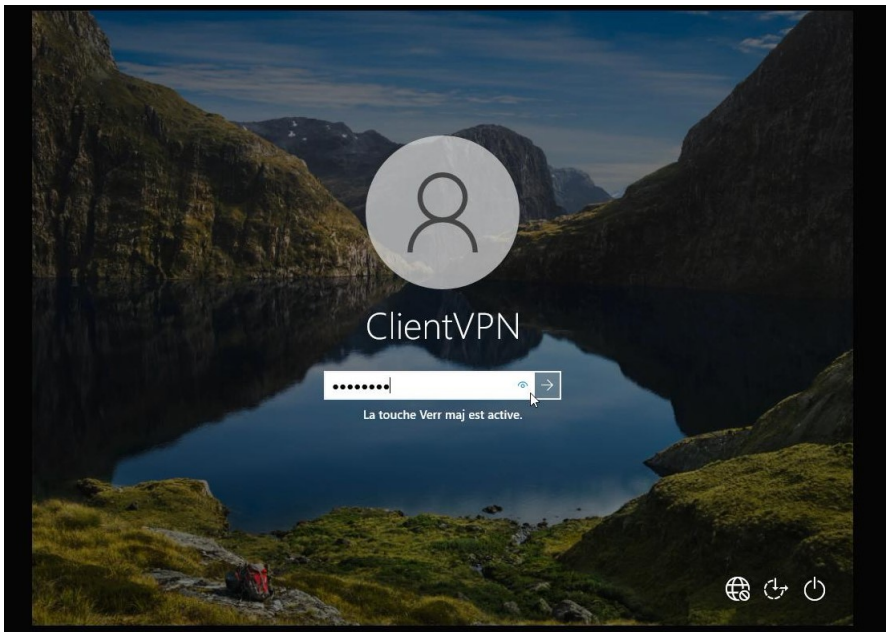


FIGURE 4.22 – La machine virtuelle Windows 10.

1. **Téléchargez le certificat d'autorité de certification :**

   Depuis mon poste client, je me rends sur http ://adresse-de-serveur-VPN/certsrv/ pour accéder au service de certification. Ensuite, je télécharge un certificat d'autorité de certification en cliquant sur l'option appropriée. Je sélectionne l'endroit où je souhaite enregistrer le certificat sur mon poste client.

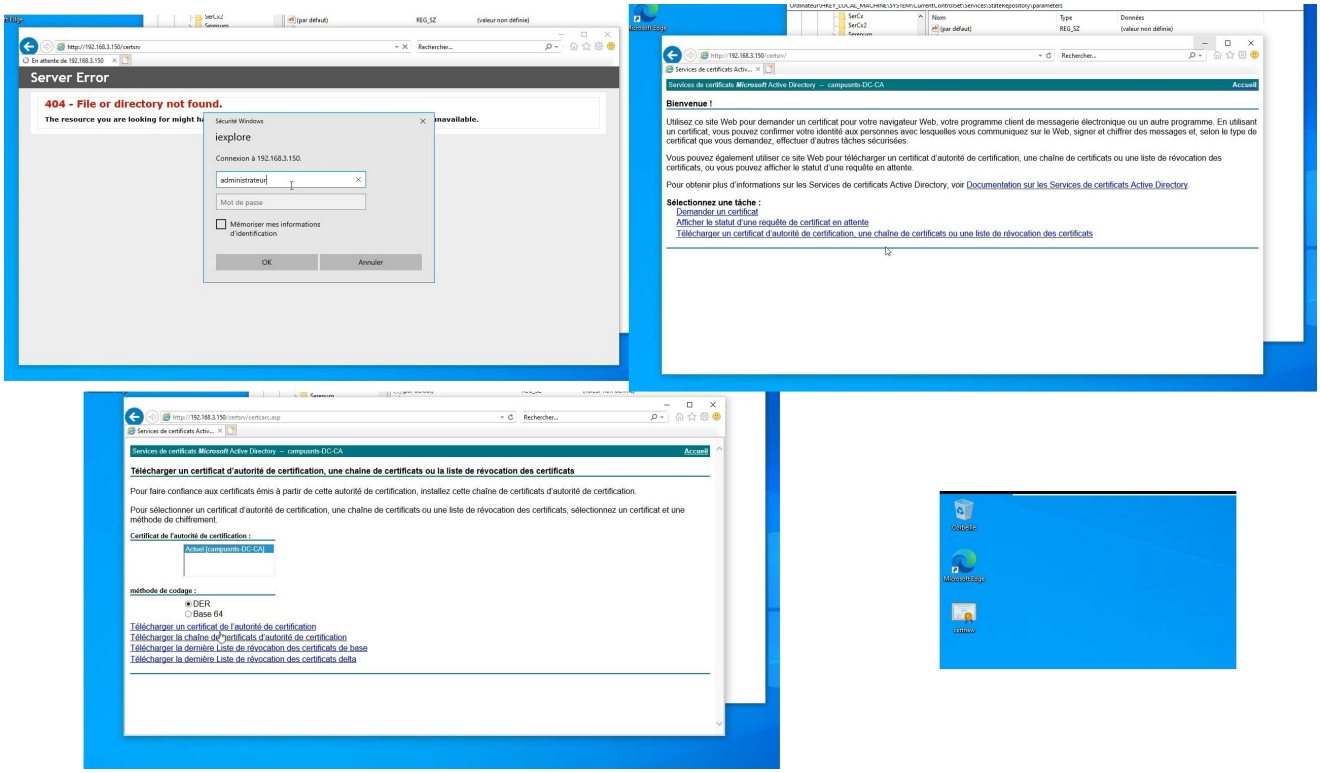


FIGURE 4.23 – Téléchargement du certificat.

2. **Installation et importation du certificat :**

   Après le téléchargement du certificat, je dois l'installer. L'image ci-dessus nous montre comment installer et importer le certificat.

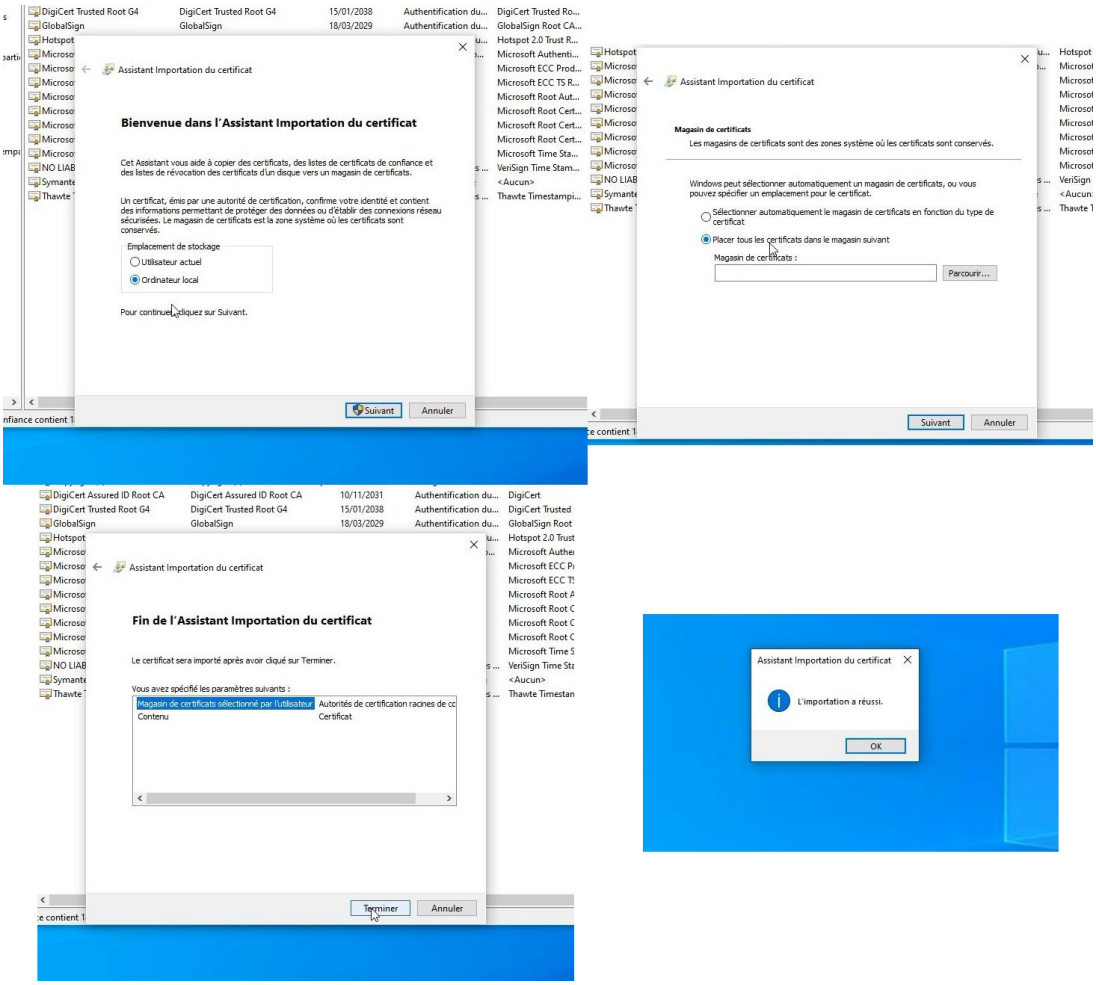


FIGURE 4.24 – Importationdu du certificat.

3. **Ajouter un certificat pour les clients :**

   J'ouvre la MMC (Microsoft Management Console), je clique sur "Ajouter/Supprimer un composant logiciel", puis sur "Certificats". Ensuite, je sélectionne "Ajouter", choisis "Un compte d'ordinateur" et je confirme en cliquant sur "OK"

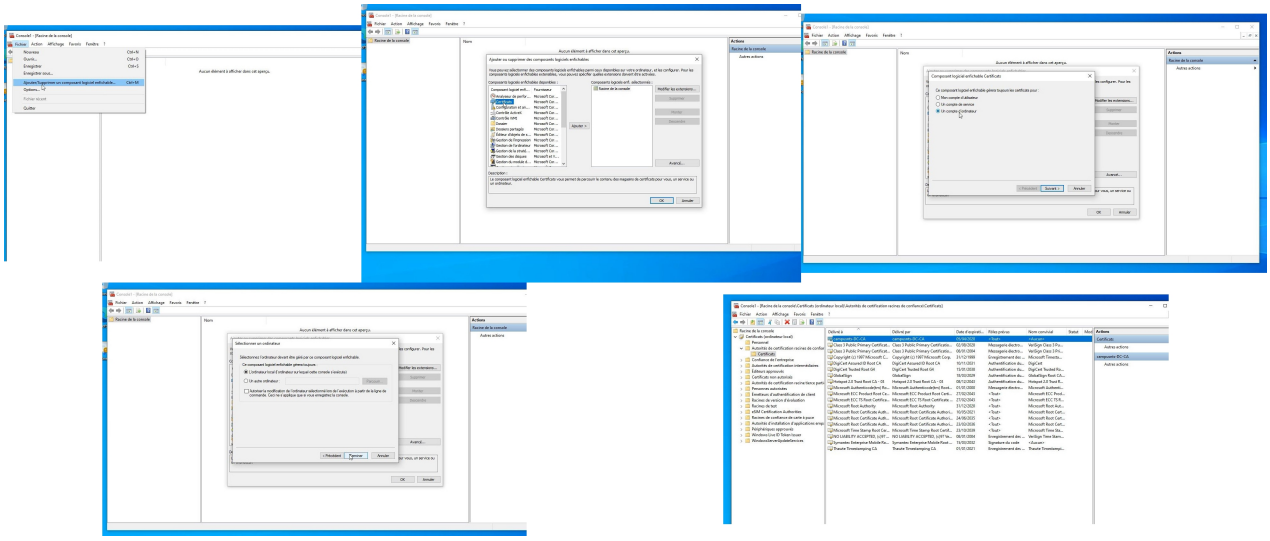


FIGURE 4.25 – Importation de la clé.

4. **Enlever la vérification de révocation :**

   Pour établir une connexion VPN plus rapide et éviter les problèmes de connectivité, je vais supprimer la révocation des certificats. Les images ci-dessus montrent les étapes pour effectuer cette opération.

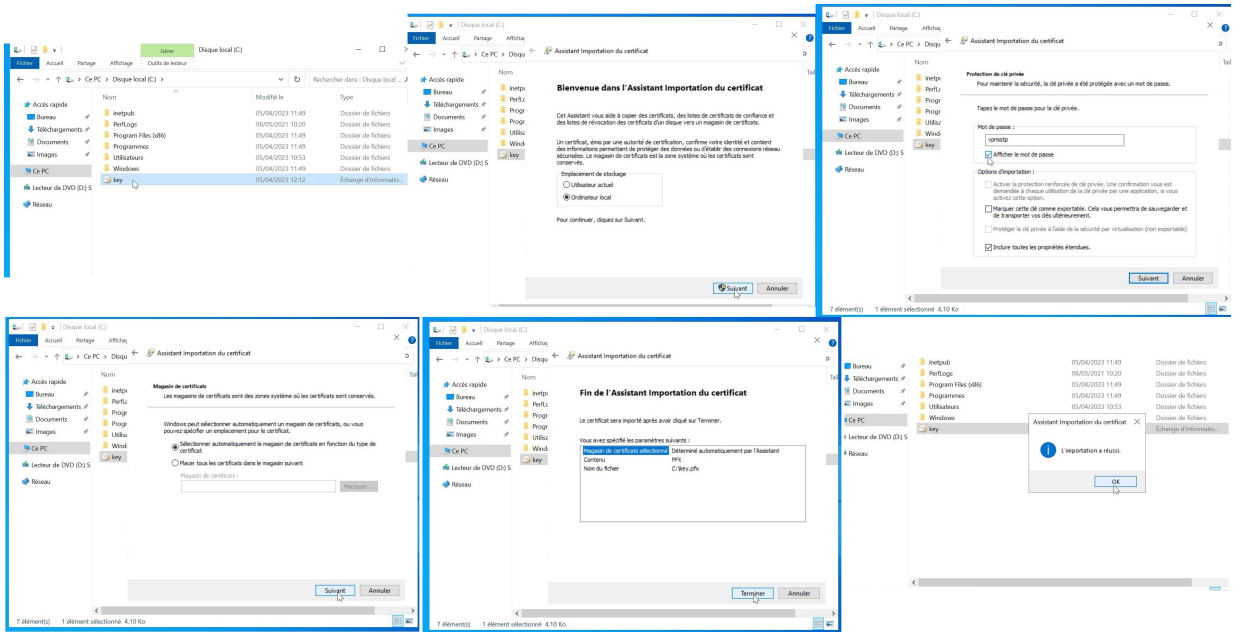


FIGURE 4.26 – Enlever la révocation.

5. **Ajouter une connexion VPN :**

   a. Je clique sur "Paramètres réseau et Internet", puis je sélectionne "VPN" dans le menu de gauche.

   b. Je clique sur "Ajouter une connexion VPN".

   c. Dans la fenêtre "Ajouter une connexion VPN", je configure les paramètres suivants :

   — Dans "Fournisseur de VPN", je sélectionne "Windows (intégré)".

   — Dans "Nom de la connexion", je saisis le nom de la connexion "VPN-SSTP".

   — Dans "Adresse du serveur", je saisis l'adresse IP (192.168.3.150) ou le nom de domaine de mon serveur VPN.

   — Dans "Type de VPN", je sélectionne "SSTP (Secure Socket Tunneling Protocol)".

   — Dans "Type d'information de connexion", je sélectionne "Nom d'utilisateur et mot de passe".

   — Ensuite, je saisis le nom d'utilisateur et le mot de passe appropriés.

   d. Je clique sur "Enregistrer".

   e. Une fois que la connexion VPN SSTP est ajoutée, je peux m'y connecter en cliquant sur l'icône VPN dans la barre des tâches et en sélectionnant la connexion que je viens de créer. J'entre ensuite mes identifiants et je me connecte.

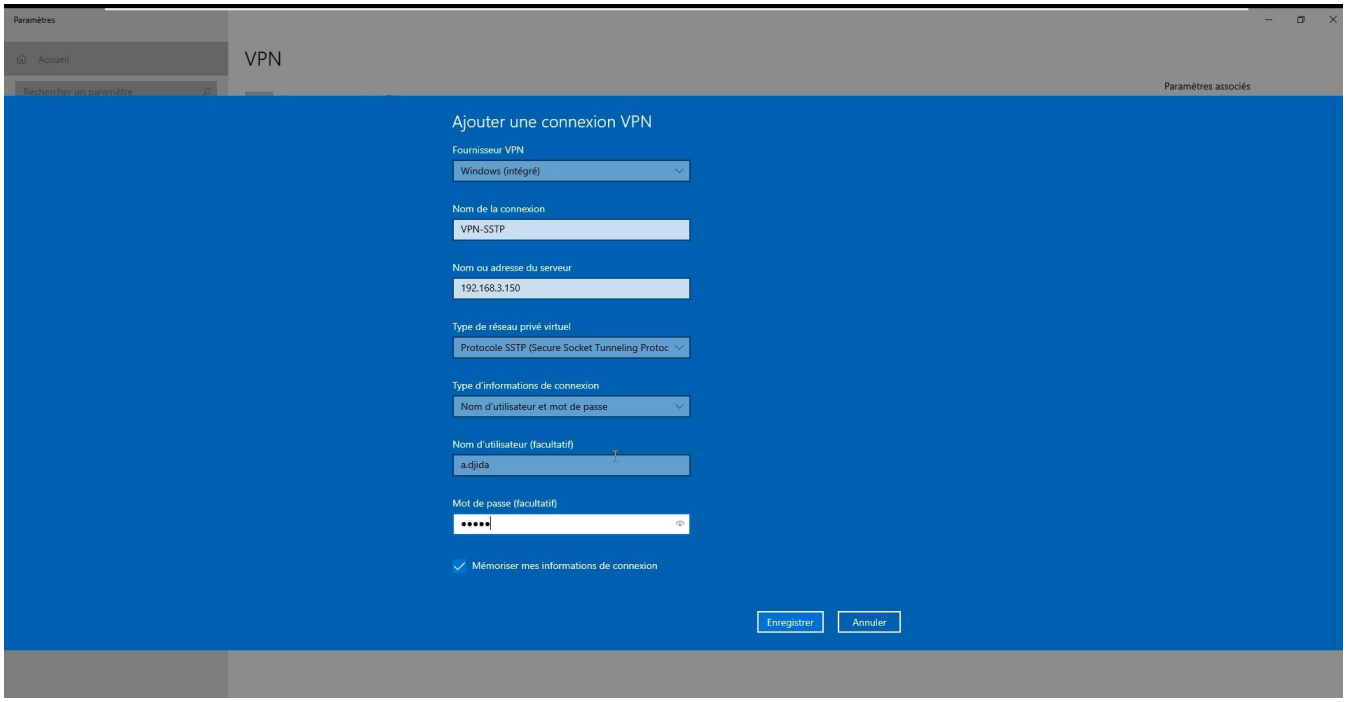


FIGURE 4.27 – Création d'une connexion VPN.

4.3.7 Tests

A) Résultat d'un Ping

Pour afficher les résultats de la commande Ping, j'ouvre une fenêtre d'invite de commande et j'exécute une commande similaire à celle reproduite ci-dessus en spécifiant une adresse IP valide sur mon réseau, comme indiqué sur l'image dans la page suivante :

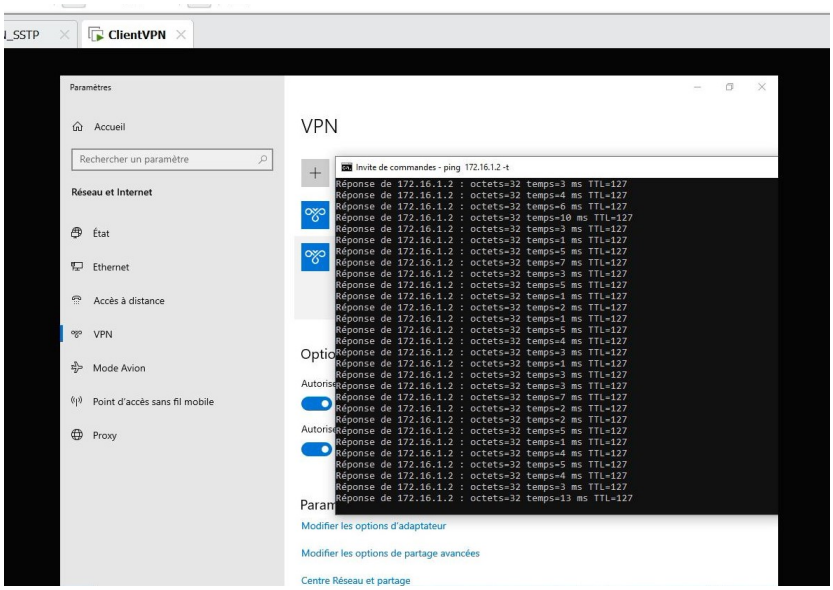


FIGURE 4.28 – Résultat d'un ping.

B) Analyse du trafic à l'aide de Wireshark

La capture présentée dans la page suivante montre les résultats de votre analyse de paquets à l'aide de Wireshark. Elle fournit des informations importantes telles que les adresses source et destination, le type de protocole et la longueur des données sélectionnées.

Lors de l'analyse du protocole SSTP avec Wireshark, j'ai pu observer des références à TLS (Transport Layer Security). En effet, le protocole SSTP utilise SSL/TLS pour établir une connexion sécurisée entre le client et le serveur.

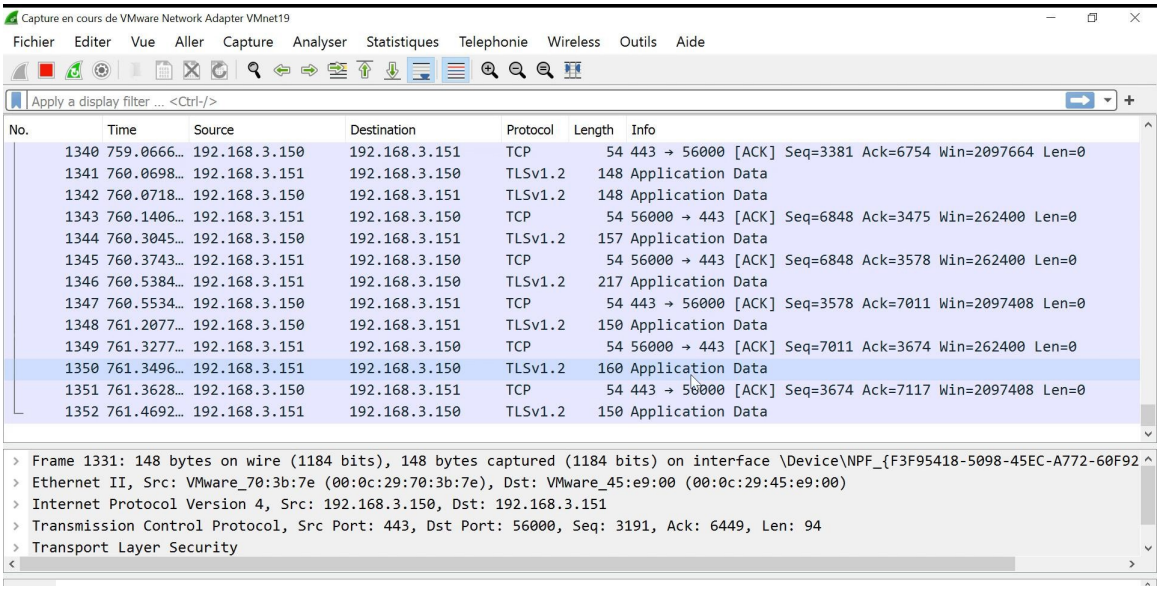


FIGURE 4.29 – Résultat de l'analyse avec Wireshark.

4.4 Conclusion

Dans ce chapitre, j'ai développé une solution sécurisée basée sur les VPN de type poste-à-site, utilisant le protocole SSTP. Cela m'a permis de comprendre le principe de fonctionnement, l'utilité et l'importance de cette solution pour la sécurité de tout réseau informatique.

CONCLUSION GÉNÉRALE

En conclusion générale, la mise en place d'un VPN SSTP avec ADCS sous Windows Server 2022 pour les clients mobiles via l'authentification RADIUS représente une solution de sécurité essentielle dans un monde de plus en plus connecté. Ce mémoire a exploré en détail les étapes clés de cette configuration, en mettant l'accent sur la protection des données sensibles lors de leur transmission.

L'utilisation du protocole SSTP offre un niveau élevé de cryptage et d'intégrité des données, garantissant ainsi des communications sécurisées entre les clients mobiles et le réseau privé. L'intégration d'ADCS facilite la gestion des certificats nécessaires à l'authentification des utilisateurs, renforçant ainsi la sécurité de l'accès au réseau.

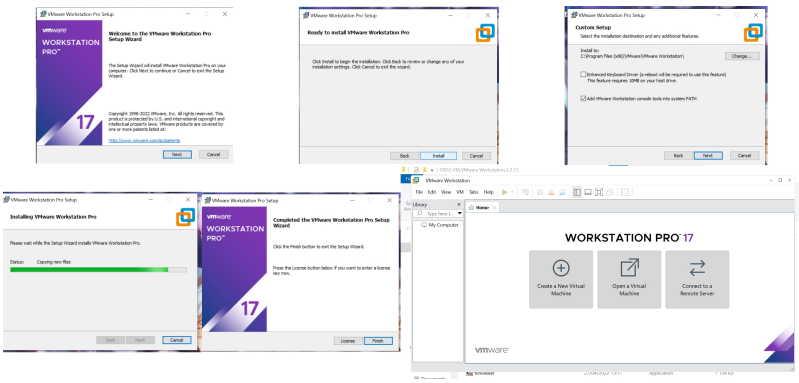
L'authentification RADIUS joue un rôle crucial en vérifiant l'identité des utilisateurs et en contrôlant leur accès, prévenant ainsi les accès non autorisés et assurant une gestion efficace des droits d'accès.

Dans un contexte où les appareils mobiles sont omniprésents et où les menaces de sécurité sont de plus en plus sophistiquées, la mise en place d'un VPN SSTP avec ADCS et l'authentification RADIUS est une réponse solide aux enjeux de confidentialité et de protection des données.

Annexes

Étapes d’installation du VMWare Workstation PRO 17

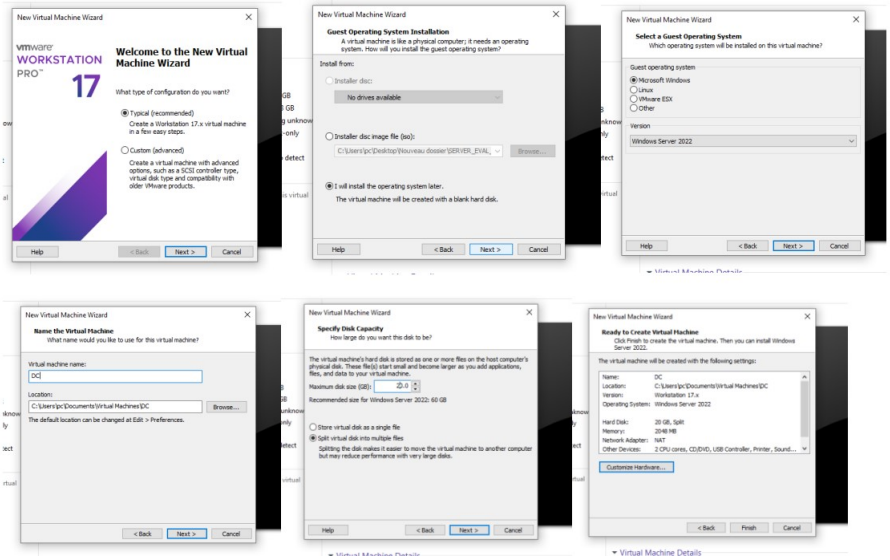
Pour installer le logiciel VMWare Workstation, il faut d’abord télécharger le fichier exécutable, puis lancer le programme. Ensuite, il suffit de suivre les étapes d’installation jusqu’à la fin, puis de cliquer sur "Finish". La figure suivante représente les différentes étapes.



Étapes d’installation du contrôleur de domaine (DC)

Lancez le logiciel de virtualisation et créez une nouvelle machine virtuelle. Sélectionnez les options appropriées telles que la quantité de mémoire RAM, l’espace de stockage, etc. Lorsqu’il vous est demandé de choisir le type de système d’exploitation, sélectionnez "windows Server 2022".

La figure ci-dessous représente les différentes étapes d’instalation.



Bibliographie

[1] PHILLOU, Jean-François and LEMAINQUE, Fabrice 2020. *Tout pour les Réseaux et Internet*. 5 éd. 11 rue Paul Bert, 92240 Malakoff : Dunod.

[2] RAHOUAL, Malek and SIARRY, Patrick, 2006. *Réseaux informatiques : Conception et optimisation*. 13 éd. 27 rue Ginoux, 75737 Paris Cedex 15, FRANCE : Technip.

[3] DROMARD, Danièle and SERT, Dominique, 2009. *Architecture des réseaux [synthèse de cours exercices corriges]*. France : IDT

[4] Green, Joel, 2022. *Je me perfectionne avec les réseaux*. 8 éd. 129 bis rue du Maréchal Foch 14750 Saint Aubin sur Mer : Broché.

[5] DOUSSY, Madeleine and All, 2005. *Information communication : première STG, sciences et technologies de la gestion spécialité communication, spécialité gestion*. Rosny-sous-bois : Bréal.

[6] Electric, Schneider, 2007. *Guide des solutions d'automatisme schématique*. 89, boulevard Franklin Roosevelt F92500 Rueil-Malmaison Cedex Electric Schneider.

[7] BORDERIES, François, CHATEL, Olivier and All, Juillet 1993. *Administration Réseau*. Rapport de fin d'année. Informatique. Grenoble : ENSIMAG.

[8] ACISSI, 2009. *Sécurité Informatique Ethical Hacking Apprendre l'attaque pour mieux se défendre*. Rue Benjamin Franklin 44800 st HERBLAIN : ENI.

[9] Hello Rank, décembre 2018. deessi.si [en ligne] Disponible sur `https://www.deessi.si/mettre-en-place-une-politique-de-securite-\informatique-les-bonnes-pratiques/` (consulté le 4 mars 2023)

[10] BORDERES, Serge, 20 mars 2007. *Méthodes d'authentification avec un serveur Radius* [cours]. Bordeaux : Institut d'Astrophysique de Paris.

[11] GHERNAOUTI, Solange, 2019. *Cyber sécurité Analyser les risques Mettre en œuvre les solutions*. 6 éd. 11 rue Paul Bert 92 240 Malakoff : Dunod

[12] `https://www.sfrbusiness.fr/room/securite/differents-types-menaces-informatiques-entreprises.html` (consulté le 14 mars 2023)

[13] SALVAIL, Louis, 2014. *Mécanisme de Sécurité des systèmes*. [10e cour]. Montréal : Université de Montréal.

[14] OECD, 18 février 1998. *La politique de cryptographie : les lignes directrices et les questions actuelles*. OECD.

[15] PhiLLOU, JEAN-FRANÇOIS and BAY, Jean-philippe, 2016. *Tout sur la Sécurite informatione*. 4 éd. 5 rue laromiguière, 75005 Paris : Dunod.

[16] BERTRAND Denis, 4 Décembre 2013, *étude et mise en œuvre du protocole 802.1x dans le cadre de la politique de sécurité de sphéria val de France*. Mémoire d'ingénieur CNAM. Informatique. Orléans : conservatoire national Des ARTS et Métiers centre Régional Associé d'ORLEANS.

[17] BEN AHMED, Naoufel, 2012. *La Signature en Droit Privé*. 1 éd. 95 rue de Londres- Tunis 1000 : Latrache. ISBN : 9796500349176.

[18] Cloudflare, 2023. cloudflare.com [en ligne] Disponible sur `https://www.cloudflare.com/fr-fr/learning/ssl/transport-layer-security-tls/` (consulté le 22 mai 2023)

[19] HUET, Franck. 2008. *Debian GNU/Linux : sécurité du système, sécurité des données, pare-feu, chiffrement, authentification*. Rue Benjamin Franklin 44800 st HERBLAIN : ENI.

[20] ARCHIER, Jean Paul, 2013, *les VPN fonctionnement, mise en œuvre et maintenance des Réseau Privés Virtuels*. 2 éd : ENI.

[21] HENMI, Anne, LUCAS, Mark and all, 2006, *firewall policies and VPN configuration*. 4 éd, 800 Hingham Street : Syngress.

[22] Techwiser, Avrile 2021. Techwiser.com [en ligne] Disponible sur `https://techwiser.com/vpn-protocol-explained/`. (consulté le 2 mars 2023)

[23] SSH, 2023. ssh.com [en ligne]. Disponible sur :`https://www.ssh.com/academy/ssh/protocol`.(consulté le 2 mai 2023)

[24] privacysavvy, 2023. https ://privacysavvy.com [en ligne]. Disponible sur : `https://privacysavvy.com/security/safe-browsing/what-is-layer-2-forwarding-l2f/`. (consulté le 22 mai 2023)

[25] IONOS, 10/08/2018. ionos.fr [en ligne]. Disponible sur :`https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-que-le-multiprotocol-label-switching-mpls/`.(consulté le 4 mai 2023)

[26] techtarget, 2000. techtarget.com [en ligne]. Disponible sur :`https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security`. (consulté le 12 mai 2023)

[27] FERRAG, Mohamed Amine, 2018. *Securite Informatione [cour et TD]*. Guelma : université 8 mai 1945

[28] TechShielder, 2022. TechShielder.com [en ligne]. Disponible sur :`https://techshielder.com/fr/vpn-sstp`. (consulté le 3 mars 2023)

[29] COTTIN, Véronique, 2001. *Active Directory Les services d'annuaire Windows 2000*. 44021 Nantes cedex 01 : ENI ; ISBN 9782746012721.

[30] JARNO, Bernard, 9 mars 2023. opportunites-digitales.com [en ligne] Disponible sur :`https://www.opportunites-digitales.com/protocole-sstp/`. (consulté le 23 mars 2023)

[31] CLINES, Steve and LOUGHRY, Marcia, 2009. *Active Directory For Dummies*. 2 éd. 111 River Street : Wiley.

[32] Forsenergy, 2016. Forsenergy.com [en ligne]. Disponible sur :https://forsenergy.com/fr-fr/certsvr/html/bac506b2-57be-45c2-bdf6-1f976eeeb475.htm. (consulté le 13 mai 2023)

[33] SERVIN, Claude, 2006. *RÉSEAUX & TÉLÉCOMS*. 2 éd. Paris : Dunod.

[34] RDR-IT, 2022, rdr-it.com [en ligne]. Disponible sur :https://rdr-it.com/mise-en-place-autorite-certification-windows-2012r2-2016/. (consulté le 23 mai 2023)

[35] CHUGHTAI, Farrukh, UlAMIN, Riaz, MALIK, Abdul Sattar , and SAEED, Nausheen, September 2019. Performance Analysis of Microsoft Network Policy Server and FreeRADIUS Authentication Systems in 802.1x based Secured Wired Ethernet using PEAP. The International Arab Journal of Information Technology, Vol. 16, N° 5, pp. 862-870.

Résumé

L'utilisation d'un VPN (réseau privé virtuel) est devenue essentielle dans le contexte actuel où les employés sont de plus en plus mobiles et ont besoin d'accéder aux ressources de l'entreprise à partir de n'importe quel endroit, tout en garantissant la confidentialité et la sécurité des données échangées. La mise en place d'un VPN SSTP avec ADSC pour les clients mobiles via une authentification RADIUS crée un réseau sécurisé. Un serveur RADIUS vérifie les informations d'authentification par rapport à l'Active Directory. Le serveur VPN utilise les certificats émis par ADSC pour établir des connexions sécurisées. Les clients mobiles installent un certificat sur leurs appareils pour s'authentifier auprès du serveur VPN. Cela permet un accès sécurisé aux ressources du réseau privé.

Mots clés : VPN, SSTP, AD, ADCS, RADUIS, VMWARE.

Abstract

The use of a Virtual Private Network (VPN) has become essential in the current context where employees are increasingly mobile and need to access company resources from anywhere, while ensuring the confidentiality and security of exchanged data. Implementing an SSTP VPN with ADSC for mobile clients through RADIUS authentication creates a secure network. A RADIUS server verifies authentication information against the Active Directory. The VPN server uses certificates issued by ADSC to establish secure connections. Mobile clients install a certificate on their devices to authenticate with the VPN server. This allows secure access to private network resources.

Keywords : VPN, SSTP, AD, ADCS, RADUIS, VMWARE.