0. INTRODUCTION GENERALE

L'interconnexion de deux sites d'une entreprise par liaison spécialisée à présenter un certain nombre de limites liées au cout qui est très élevé, mais le débit est garanti. Ainsi, la liaison entre deux sites d'une entreprise passant par internet est trop vulnérable aux attaques des pirates. C'est-à-dire les données transitant par l'internet sont trop exposées aux attaques de n'importe quel genre et cela, constitue un risque pour les entreprises.

Pour pallier à cela, il faut mettre en place un tunnel VPN permettant à ces deux sites d'échanger des données sans courir trop de risque ; d'où le VPN SITE TO SITE.

1. PROBLEMATIQUE

C'est une étape qui représente la nature des problèmes qui se posent au sein d'une entreprise en rapport au sujet qui fait l'objet de recherche. Elle est aussi définie comme un ensemble des questions que l'on se pose à propos d'un sujet. Elle reste le fondement, un guide dans l'analyse d'une étude scientifique[1].

Partant de notre sujet du travail, nous disons bien que la Cour des comptes étant une grande Institution Supérieure de Contrôle des biens public qui possède toutes les capacités du point de vue ébergement et autres services selon ses responsabilités, elle possède des sites distants dont, 1 site à Kinshasa Gombe sur l'avenue comite urbain, 1 à Kinshasa sur boulevard du 30 juin/Royal et bientôt d'autre site aux autres provinces.

Il éprouve des difficultés dans la communication entre les agents des sites distants de façon sécurisé que ça soit pour les sites de Kinshasa ou bien d'autres.

Avant de décrire l'implémentation d'un système d'interconnexion de sites distants de la Cour des comptes via la technologie VPN, certaines

[1] *Prof. Lepère MAKUMOLE, Cours Méthodes de recherche scientifique, G2 Gestion informatique/WUB,2022 inédit*

questions nous viennent à l'esprit dont la nécessité serait de les exprimer dans l'idéal d'avoir une vision sur le présent travail.

- Comment assurer les accès sécuritaires au sein de sites réparties sur de grandes distances géographiquement éloigné de la Cour des comptes ?

- Concrètement, comment une succursale de la Cour des comptes peut-elle accéder aux données situées sur un serveur distant de plusieurs milliers de Kilomètres ?
- Quels protocoles et quelle configuration assurent-ils l'accès sécurisé aux informations de la Cour des comptes ?

2. **HYPOTHESE**

Nous essayons dans la mesure possible d'envisager une politique optimale de partage des informations afin que l'échange des ressources ne pose plus de problème au sein de la Cour des comptes.

Dans le cadre de notre travail, nous avons jugé bon de joindre au système d'information existant au sein de l'institution, les applicatifs de l'Internet afin de lui permettre :

- Une bonne conservation et recherche aisée des informations en interne et externe ;
- L'échange des données entre les différentes chambres de l'ISC ;
- Une rapidité dans le traitement de l'information avec toutes les mesures de sécurité garantie ;
- La récupération de l'information en temps réel.

En vue de remédier toujours aux inquiétudes soulevées au travers des questions posées ci-haut, nous pensons que :

- Il existerait un moyen d'échange de l'information qui serait adapté à la gestion efficace et efficiente de la Cour des comptes ;

- Une configuration appropriée existerait et des systèmes d'exploitation tels que Windows Server, Unix, Linux…seraient mieux adaptés pour assurer l'accès sécurisé à l'information.

3. CHOIX ET INTERET DU SUJET

Vu l'objectif que l'institution estime qu'on lui accorde, nous avons jugé bon de porter notre choix sur ce sujet qui s'intitule : « **Implémentation d'un système d'interconnexion des sites distants via le réseau privé virtuel** » afin de faire profiter à l'institution cette étude et au monde scientifique nos connaissances acquises durant notre parcours universitaire.

4. DELIMITATION DU SUJET

Dans le cadre de ce travail, nous ne prétendons pas aborder tous les aspects liés à sa réalisation parce qu'il faut le limiter sur le plan spatio-temporel.

- Dans le temps, notre étude couvre la période allant de 2023-2024
- Dans l'espace, notre étude concerne uniquement l'interconnexion des sites de la Cour des comptes à l'aide d'un VPN.

5. METHODES ET TECHNIQUES UTILISEES

a. Méthodes

Tout chercheur se focalise sur une méthode susceptible de l'orienter à atteindre son objectif du problème qu'il étudie dans son travail. En d'autres termes la méthode est l'ensemble des moyens par lesquels, une discipline cherche à atteindre. Les vérités qu'elle poursuit, les démontrent et les vérifient[2].

Pour l'élaboration de notre travail, nous avons fait recours aux trois méthodes :

[2] *Prof. Lepère MAKUMOLE, Op.cit.*

- **Méthode historique** : Elle consiste à étudier le passé d'une entreprise pour mieux cerner sa situation actuelle afin de mieux préparer son évolution future ;
- **Méthode analytique** : Elle nous a permis d'analyser en détail le composant du système existant. Elle consiste à décomposer les éléments du système existant enfin de le définir, les analyser et d'en dégager les spécificités auxquelles le nouveau système fera face ;
- **Méthode descriptive** : Par cette méthode, certains principes et concepts ont été décrits tout simplement sans commentaire.

b. **Techniques**

La technique est l'ensemble organisé des procédés d'un travail, et comme tout travail nécessite des techniques, pour celui-ci nous avons opté pour :

- **Technique documentaire** : Elle met en présence de chercheur des documents concernant les informations recherchées.
- **Technique d'interview** : Elle consiste à interroger en vue d'avoir des points de vue avec les différents employés du service qui nous a intéressé pour acquérir les informations dont on a besoin. Cette technique nous a permis d'obtenir les renseignements sur l'étude de l'existant, par un jeu des questions réponses ;
- **Les contacts** : Nous ont permis de recueillir des informations concernant notre étude auprès des spécialistes dans le domaine des réseaux informatiques.

6. CANEVAS DU TRAVAIL

Hormis l'introduction générale et la conclusion générale, notre travail est subdivisé en deux parties principales comprenant chacune d'elle quelques chapitres à savoir :

PREMIÈRE PARTIE : APPROCHE THÉORIQUE

CHAPITRE 1 : Généralité sur le VPN

CHAPITRE 2 : Présentation de l'institution

DEUXIÈME PARTIE : APPROCHE PRATIQUE

CHAPITRE 3 : Planning prévisionnel de réalisation du projet

CHAPITRE 4 : Mise en œuvre de l'interconnexion des sites distants via le VPN

PREMIERE PARTIE : APPROCHE THEORIQUE

CHAPITRE I : **GÉNÉRALITÉ SUR LE VPN**

Le VPN (Virtuel Private Network) est un réseau privé virtuel qui est relié à l'internet par l'intermédiaire des équipements d'interconnexion, le VPN a la capacité de relier 2 sites différents et il est en mesure de sécuriser une liaison à moindre coût[3].

I.1. **Définitions**

Nous explicitons quelques définitions liées au VPN :

1. Le réseau VPN :

Il est réseau parce qu'il permet l'interconnexion de plusieurs sites distants ;

Il est privé parce qu'il est réservé à un groupe d'usagers qui sont déterminés par authentification, les données sont échangés de manière masquée aux yeux des autres par cryptage des données ;

Il est virtuel parce qu'il se base essentiellement sur les lignes partagés et non dédié.

2. Le réseau VPN est un réseau privé virtuel qui fait appel à un réseau public (Internet) pour connecter des sites ou les utilisateurs distants ;

3. Le VPN est un système qui permet de créer un lien direct entre les ordinateurs distants ;

4. Le VPN en informatique est une connexion inter-réseau permettant de relier 2 réseaux locaux différents par un protocole de tunnel.

VPN signifie Virtual Private Network, ce que nous traduisons par RPV (Réseau Privé Virtuel). C'est une technologie qui permet d'envoyer des données entre des ordinateurs appartenant à des sites distants, par

[3] *Prof Denis BOTA Cours Réseaux mobile télécom L2 télécom /UWB,2024 inédit*

l'intermédiaire d'un inter-réseau public de la même manière que s'il s'agissait d'une liaison privée point à point.

Il faut bien comprendre ce modèle : on construit par des moyens logiciels un réseau privé au-dessus d'une infrastructure publique (Internet ou un réseau d'opérateur).

I.2. **Objectifs d'un VPN**

Le VPN présente des objectifs tels que :

Il est un réseau qui permet d'établir un lien dans différents réseaux ;

Il permet l'interconnexion entre 2 ou plusieurs sites de façon sécurisée à très faible coût par une connexion Internet[4] ;

Il fournit aux utilisateurs et administrateurs du système d'information des conditions d'exploitation, d'utilisation et de sécurité à travers un réseau public identique à celle disponible sur le réseau privé.

I.3. **Principe de fonctionnement d'un VPN**

I.3.1. **Fonctionnalités d'un VPN**

Dans le VPN, la connexion entre les ordinateurs sont gérés de façon transparente par un logiciel qui crée un « tunnel » entre les ordinateurs connectés.

Par son but principal qui est : le VPN fournit aux utilisateurs et aux administrateurs du système d'information des conditions d'exploitation, d'utilisation et de sécurité à travers un réseau public (Internet) qui est disponible sur le réseau privé. Nous pouvons aussi dire autrement qu'on regroupe des réseaux privés qui sont séparés par un réseau public (Internet) tout en donnant une illusion aux utilisateurs qui ne sont pas séparés et qui gardent l'aspect sécurité mais le découpage se fait logiquement.

---

[4] *Stéphane LOHIER, préface de Guy PUJOLLE : Transmission et Réseaux, 4éEd DUNOD, paris, 2020, p.235-253*

Le VPN repose sur un protocole de « Tunnelisation » qui est un protocole de chiffrement des données entre deux ou plusieurs réseaux.

Les ordinateurs connectés au VPN qui sont dans un même réseau local (virtuel), ce qui permet de passer aux éventuelles restrictions sur le réseau tel que le « proxy » ou « FAI (fournisseur d'accès internet) » pour avoir la connexion Internet.

Le terme « tunnel » est utilisé pour évoquer entre l'entrée et la sortie de VPN les données sont déjà cryptées et il est incompréhensif pour tout utilisateur qui va se retrouver entre les deux extrémités du VPN comme les données passent par un tunnel.

Lorsqu'on établit une liaison VPN entre deux ou plusieurs ordinateurs connectés, on va appeler client l'élément qui permet de chiffrer et de déchiffrer les données du côté utilisateur (client) et le serveur VPN ou (serveur d'accès distants) l'élément qui assure le chiffrement et le déchiffrement des données du côté organisation. De cette manière ,lorsqu'un utilisateur exige d'accéder au réseau privé virtuel, sa requête sera transmise en clair vers le système passerelle qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure du réseau public (Internet) puis cette requête sera reçu de façon chiffré afin les ordinateurs distants vont alors fournir des données au serveur VPN de son réseau local qui va recevoir la requête chiffrée et à la réception du client VPN de l'utilisateur les données seront déchiffrées puis transmises à l'utilisateur.

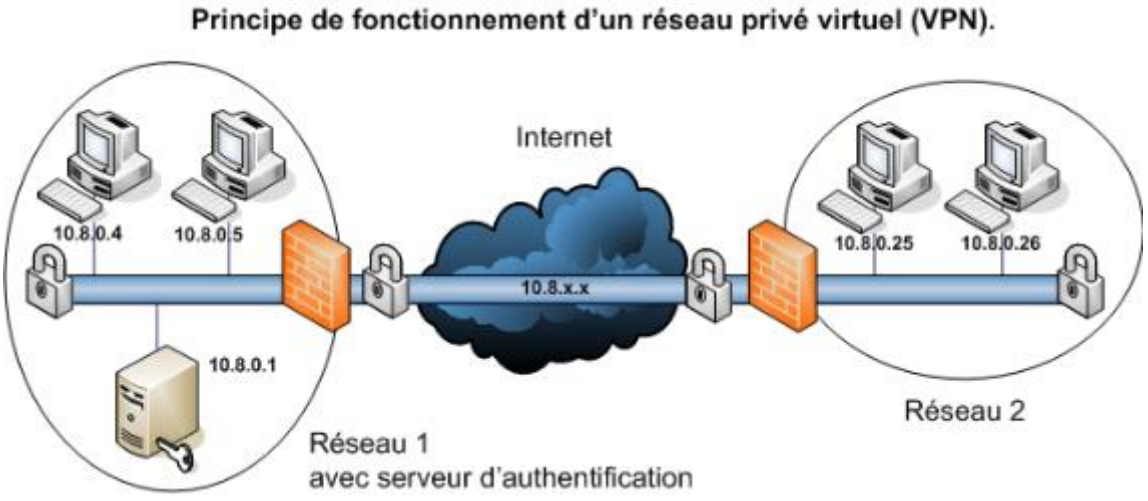


Figure I.1. Principe de fonctionnement de VPN.

I.3.2. **Avantages et inconvénients du VPN**

Comme toute autre technologie, le VPN présente les avantages ainsi que les inconvénients :

I.3.2.1. **Avantages**

La technologie VPN présente des avantages comme suit :

- Elle assure la sécurité des informations lors de la communication et chiffre les données ;
- Elle est simple et facile à utiliser : utilise les circuits de télécoms classiques ;
- Elle a une grande couverture géographique ;
- Elle est économique : utilise Internet en tant que média principale de transport, ce qui évite les coûts liés à une ligne dédiée.

l.3.2.2. **Inconvénients**

La technologie VPN présente des inconvénients comme :

- A l'absence de l'Internet on ne peut pas réaliser une connexion VPN si la connexion n'est pas bonne ;
- La qualité des services, c'est-à-dire le délai d'acheminement n'est pas garantie ;
- Les performances ne sont pas toujours au rendez-vous.

I.3.3. **Tunnelisation**

La Tunnelisation est un protocole qui permet aux données de passer par extrémité du VPN à une autre pour être sécurisée par des algorithmes de cryptographie.

I.3.3.1. **Les tunnels**

Par le tunnel, il est possible de passer directement d'une extrémité à une autre sans passer par le tracas de la circulation à la surface.

Les tunnels informatiques se rapprochent très fortement tout en proposant des moyens d'établir directement une liaison soit une relation entre deux réseaux privés distants à travers un inter-réseau qui est aussi complexe que l'Internet.

Il existe une grande possibilité de créer des tunnels informatiques tels que le PPP (Point to Point Protocol) peut être considéré comme un tunnel dans les configurations de PPPoE ou PPPoA. Ce sont des tunnels qui se situent au niveau de la couche 2 du modèle OSI qui est de même titre que celui du L2TP (Layer 2 Tunneling Protocol).

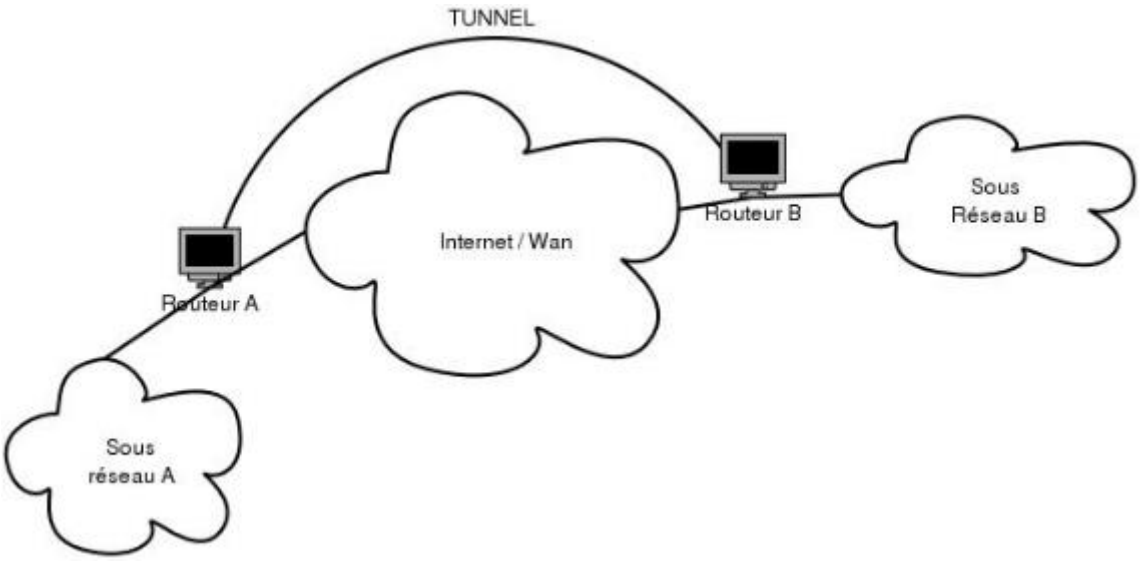


Figure I.2. Le tunnel VPN.

I.4. Types de VPN

Le VPN est classifié en 3 types qui sont :

1. Le VPN d'accès ;

2. Le VPN Intranet ;

3. Le VPN Extranet.

I.4.1. **Le VPN d'accès**

Le VPN d'accès permet à l'utilisateur isolé de se connecter dans un réseau local interne.

Dans ce cas, il peut avoir son propre client VPN afin de le connecter directement au réseau c'est-à-dire entre l'employé distant et l'entreprise au cas contraire il doit faire recoure au FAI (Fournisseur d'Accès Internet) qui va lui fournir un serveur d'accès qui se chargera de la connexion cryptée.

Mais la connexion entre l'utilisateur isolé et le serveur d'accès n'est pas cryptée (problème).

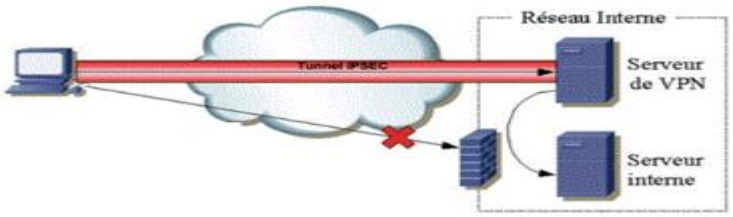


Figure I.3. VPN d'accès.

I.4.2. **L'Intranet VPN**

L'Intranet VPN est utilisé pour relier au moins deux intranets[5] entre eux, ce type de réseau est spécialement utile au sein d'une entreprise possédant plusieurs sites distants. Il est plus important parce qu'il garantit la sécurité, la totalité et l'intégralité des données. Des techniques de cryptographie sont mise en œuvre pour la vérification des données qui n'ont pas été abimé. Il s'agit donc d'une authentification au niveau du paquet pour assurer la validité des données, l'identification de leur source ainsi que la non répudiation. En générale les algorithmes utilisés font appel à des signatures numériques qui sont ajoutés aux

[5] http://www.intranet/vpn/.com.

paquets, la confidentialité des données est basée sur des algorithmes de cryptographie.

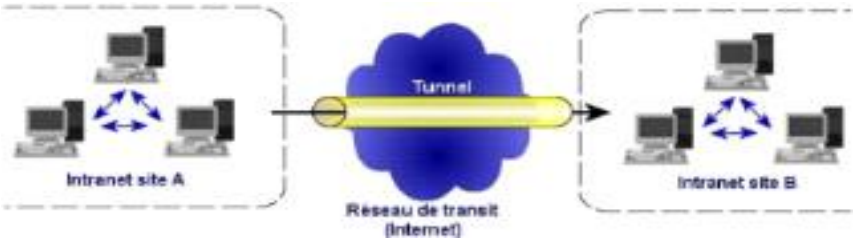


Figure I.4. L'Intranet VPN.

I.4.3. **L'Extranet VPN**

L'extranet VPN est utilisé dans une entreprise pour établir la communication entre les clients et ses partenaires.

Elle ouvre alors son réseau local à ces derniers. Dans ce cas, il est primordial que l'administrateur du VPN puisse tracer un tunnel entre les clients sur le réseau et gérer les droits de tout chacun.

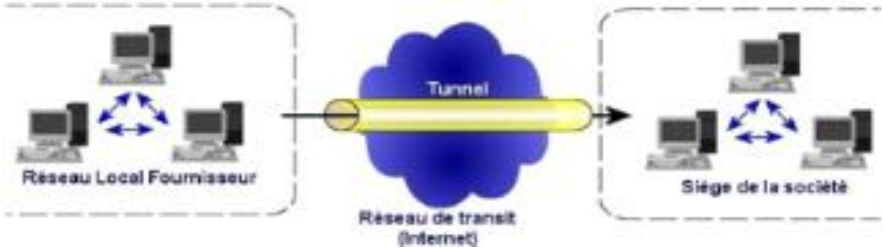


Figure I.5. L'Extranet VPN.

I.5. **Caractéristique d'un VPN**

Le VPN n'est qu'un concept et non une implémentation.

Il se caractérise par :

a. L'authentification des entités communicantes c'est-à-dire le serveur VPN doit s'assurer qu'il se communique avec le vrai client VPN et vice versa ;

b. L'authentification des utilisateurs c'est-à-dire seuls les agents ou utilisateurs autorisés ont droit de pouvoir se connecter au réseau privé et toute action effectuée sur le réseau droit être conservé ;

c. Gestion d'adresse : tous les utilisateurs doivent avoir une adresse privée et cette adresse doit rester confidentiel et le nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse privée à lui ;

d. Cryptage de tunnel : lors des échanges des données sur Internet, ces données doivent être efficacement cryptées entre le client et le serveur VPN et vice versa ;

e. Gestion de clés : les clés de cryptage entre le client et le serveur VPN doivent être générées et régénérées automatiquement ;

f. Le VPN doit prendre en charge tous les protocoles afin de réaliser un vrai tunnel comme s'il y avait réellement présence d'un câble entre les deux réseaux.

I.6. **Protocoles utilisés dans le VPN (protocole de tunnelisation)**

Il existe deux catégories de protocoles VPN :

I.6.1. **1ere catégorie : les protocoles qui nécessitent le matériel particulier**

A. Les protocoles de la couche deux du modèle OSI (liaison de donnée) dans la pile de protocole TCP/IP

1) PPTP (Point to Point Tunneling Protocol), est un protocole qui permet de créer des trames avec le protocole PPP (Point to Point Protocol) et de les cryptées puis les encapsulés dans un paquet IP. Ce qui permet de relier deux réseaux par un point to point virtuel qui est acheminé par une connexion IP sur Internet. Nous pourrons alors dire que deux réseaux sont reliés par une ligne directe.

La connexion s'effectue de la sorte :

Le client se connecte à l'Internet par son modem par le protocole PPP (classement) ;

Le client se connecte alors au serveur VPN par une connexion IP encapsulant les paquets GRE/PPP cryptés puis va former deux connexions l'une sur l'autre ;

La connexion normale sur Internet c'est-à-dire qu'elle achemine le trafic vers ou depuis Internet ;

La connexion virtuelle au-dessus de la connexion Internet : elle achemine le trafic vers le réseau VPN ;

A la fin de la connexion, le serveur Internet va fermer le tunnel.

Figure I.6. Le protocole PPTP.

2) L2TP (Layer 2 Tunneling Protocol), est un protocole qui est très proche du protocole PPTP. Cette fois si les trames PPP sont encapsulées dans le protocole L2TP lui-même.

Il existe deux types serveurs pour utiliser le L2TP[6] :

a. Le 1er type de serveur pour l'utilisation du L2TP : LAC

LAC (L2TP Access Concentrateur), c'est un concentrateur d'accès L2TP. Il a une responsabilité d'identification et construit le tunnel vers le LNS.

[6] *Prof Denis BOTA Cours Administration réseaux L2 télécom /UWB,2024, inédit*

Il se trouve obligatoirement dans une infrastructure du FAI (Fournisseur d'Accès Internet) de chaque usager du VPN, cela est donc très lourd et cher à mettre en place une mesure ou il faudra louer une place dans un serveur de connexion du FAI.

b. Le 2eme type de serveur pour l'utilisation du L2TP : LNS

LNS (L2TP Network Serveur), c'est un serveur réseau qui assure la communication du réseau auquel il est connecté et les LACS vers lesquels il y a présence d'un tunnel.

Il se retrouve généralement dans l'entreprise ou service auquel appartient l'utilisateur distant.[7]

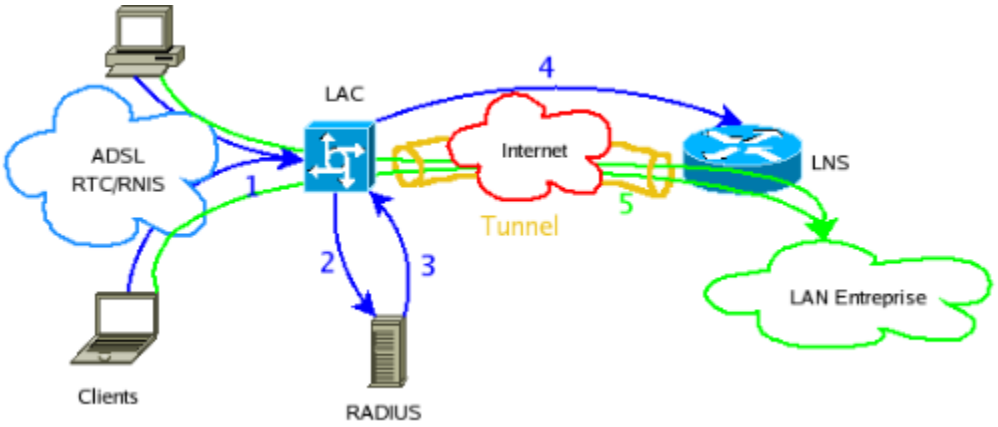


Figure I.7. Le protocole L2TP.

B. Les protocoles de la couche trois du modèle OSI (réseau) dans la pile de protocole TCP/IP.

1. IPsec

C'est un protocole définit par IETF (Internet Engineering Task Force) qui permet d'assurer la sécurité des échanges des données au niveau de la couche réseau du modèle OSI.

[7] Clade SERVIN, *Réseau et télécom, 4éme ed DUNOD,* Paris, 2021, p. 581

En effet, c'est un protocole qui apporte des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégralité et l'authentification des échanges.

Les services de sécurité fournie par l'IPsec

IPsec vise à prévenir diverses attaques qui sont rendues possible par le protocole IP notamment :

Il empêche à un adversaire d'espionner les données qui circulent sur le réseau ;

Il lui empêche d'accéder à des ressources ou données protégées.

Elle présente des services suivants :

a. Confidentialité de données et de protection partielle contre l'analyse du trafic : Les données transportées ne peuvent être lues par un utilisateur espionnant les communications aucun mot de passe, aucune information confidentielle ne circule en clair sur le réseau.

b. L'authenticité : il effectue l'authenticité des données et le contrôle d'accès continu. L'authenticité est composée de deux services qui sont généralement fournis simultanément par un même mécanisme : l'authentification de l'origine de données et l'intégralité.

L'authentification de l'origine de données garantissent que les données reçues proviennent de l'émetteur déclaré ;

L'intégralité garantit que les données n'ont pas été modifiées pendant son transfert.

Bref, ces services permettent en particulier de protéger ou d'assurer la sécurité à l'accès des ressources ou des données privées.

c. Protection contre le rejeu : La protection contre le rejeu permet la détection d'une tentative attaque qui consiste à envoyer de nouveau un paquet valide à prendre précédemment sur le réseau. Ces services sont basés sur des mécanismes cryptographiques modernes qui leur donnent un nouveau de sécurité élevé lorsqu'ils utilisent les algorithmes fort. Les

services de sécurité sont fournis au moyen de deux extensions du protocole IP appelées AH (Authentification Header) et ESP (Encapsulating Security Payload).

On distingue deux types de mode pour l'IPsec qui sont :

1. Le mode transport

Le mode transport, est un mode qui permet la protection des protocoles de niveau supérieur ;

IPsec récupère les données provenant de la couche quatre du modèle OSI (transport), il les signe et les cryptes puis ils les envoient au niveau de la couche trois du modèle OSI. Cela permet la transparence entre la couche quatre du modèle OSI et la couche trois du modèle OSI et du coup il est relativement facile de la mettre en place.

Il présente des inconvénients suivants :

A l'en tête, il est produite par la couche réseau et donc IPsec ne peut pas contrôler dans ce cas ;

Il ne peut pas masquer les adresses pour faire croire qu'entre un réseau LAN est entre deux LAN reliés ;

Il n'assure pas la garantie d'utiliser IPS non voulue.

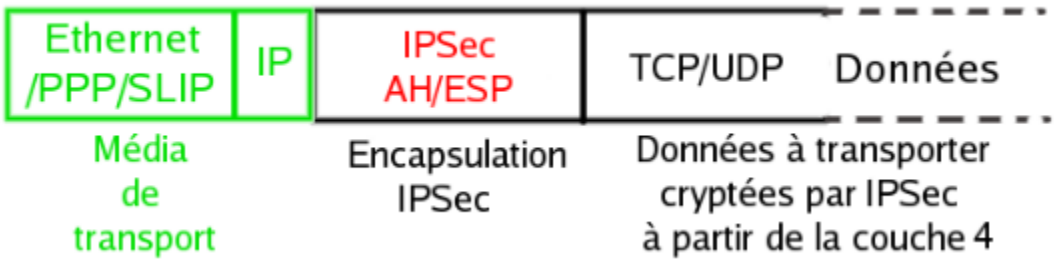


Figure I.8. Le protocole IP.

2. mode tunnel

Le mode tunnel, est un mode qui permet l'encapsulation des données IP. Les paquets circulent dans la pile de protocole (TCP/IP) jusqu'à la

couche trois du modèle OSI (réseau) et cette couche IP qui transmet ses données dans la couche IPsec[8].

Il y a donc un en-tête IP encapsulé dans les données IP et cette en-tête IP qui est réelle pour le transport sur net.

Il présente des avantages tels que :

L'en-tête IP réelle est produite dans la couche IPsec c'est-à-dire qu'elle permet l'encapsulation d'un en-tête IP avec les adresses relatives au réseau virtuel et en plus de les crypter de façon qu'ils ne soient pas modifiable ;

On a des adresses IP virtuelles donc qui tirent parti au mieux du concept VPN ;

Assure le contrôle total sur l'en-tête IP produite par IPsec pour l'encapsulation des données et de son en-tête IPsec.

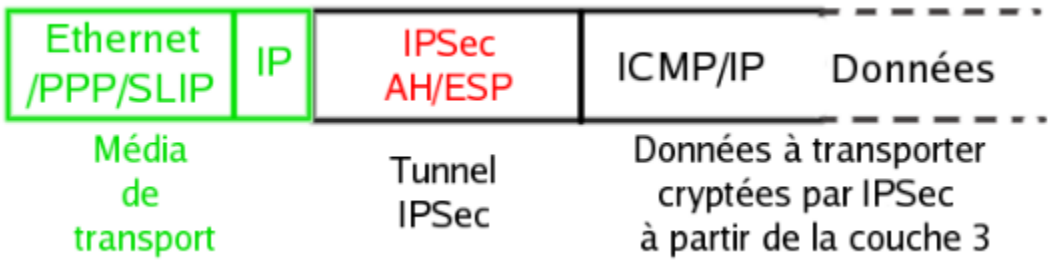


Figure I.9. Le protocole IPsec.

I.6.2. **2eme Catégorie : Les protocoles ne nécessitant qu'une couche logicielle[9]**

A. Les protocoles de niveau 4 (couche transport) du modèle OSI : Open VPN en SSL

SSL VPN (Secure Socket Layer Virtuel Private Network) est un type de VPN qui fonctionne au-dessus de transport layé et qui est accessible au navigateur web via le protocole http.

---

[8] https://www.google/developpement-informatique.com/article/452/mode-tunnel-et-mode-de-transport-ipsec
[9] *C.T Bope BONHOMI Cours system d'exploitation L2 télécom /UWB,2024, inédit.*

Open VPN est une solution qui se base sur le SSL.

Elle permet d'assurer deux choses à la fois sans passé par beaucoup de logicielle du point de vue client :

- L'authentification du client et du serveur ;
- La sécurisation du canal de transmission.

I.7. **Topologie de VPN**

La technologie VPN utilise deux topologies en étoile et en maillée.

I.7.1. **La topologie en étoile**

Dans cette topologie, toutes les ressources sont centralisées dans un même endroit, et c'est à ce nouveau qu'on retrouve le serveur d'accès distant (ou serveur VPN).

Dans ce cas, tout employés du réseau doit s'identifier, s'authentifier au serveur et peuvent alors accéder aux ressources qui se situent sur le réseau intranet.

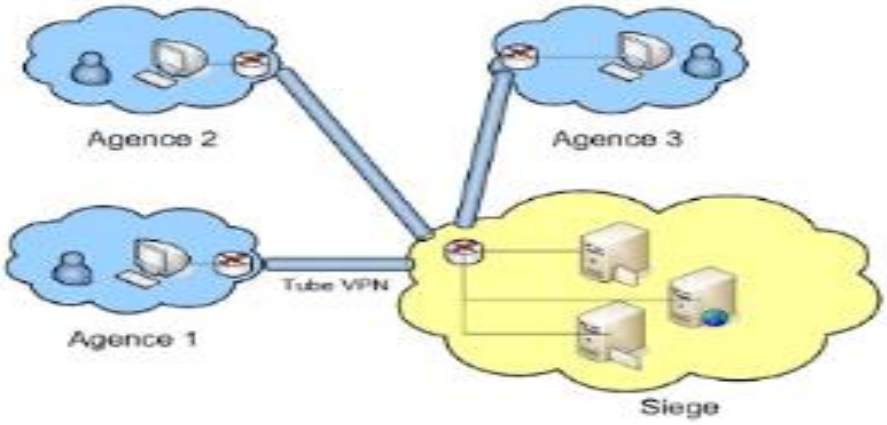


Figure I.10. Topologie en étoile.

I.7.2. **La topologie maillée**

Dans cette topologie, les routeurs ou passerelles présents aux extrémités de chaque site relié sont considérés comme étant des serveurs d'accès distant. Ces ressources à ce niveau sont

décentralisées sur chacun des sites soit les employés ne pourrons qu'accéder aux informations présentes sur l'ensemble du réseau.

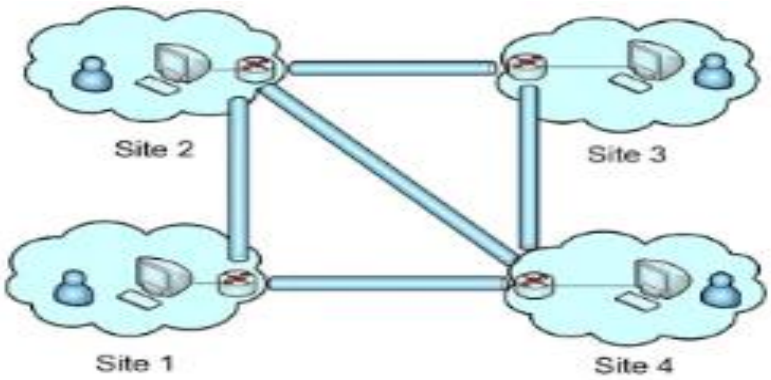


Figure I.11. Topologie maillée

I.8. **Éléments constitutifs**

Dans le cas d'une connexion VPN d'accès distant, plusieurs éléments sont nécessaires :

- Le serveur VPN : situé dans l'entreprise, qui accepte les connexions VPN des clients ;
- Le client VPN : distant, qui se connecte au serveur VPN ;
- Le tunnel : portion de connexion dans laquelle les données sont encapsulées ;
- La connexion VPN : portion de connexion dans laquelle les données sont chiffrées.

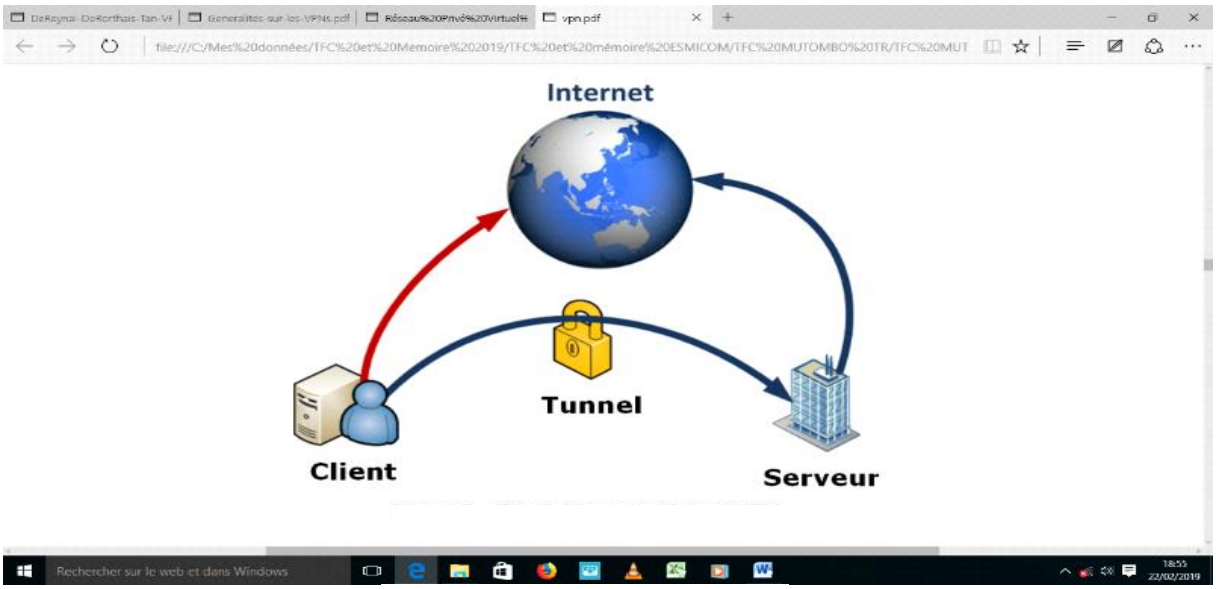


Figure I.12. Client/Serveur/Tunnel VPN.

En fait, dans une connexion VPN sécurisée, les données sont chiffrées et encapsulées dans la même portion de la connexion. Tout cela se réalise avec des protocoles de "Tunneling".

Un système de VPN sécurisé doit pouvoir mettre en œuvre les fonctionnalités suivantes :

- Authentification d'utilisateur : Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. Un historique des connexions et des actions effectuées sur le réseau peut être défini et conservé. Inversement, le client peut également être amené à authentifier le serveur afin de se protéger des faux serveurs VPN ;
- Gestion d'adresses : Chaque client sur le réseau dispose d'une adresse privée et confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse ;
- Cryptage des données : Lors de leur transport sur le réseau public les données doivent être protégées par un cryptage efficace ;
- Gestion de clés : Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées ;

- Prise en charge multi-protocole : La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.
- La mise en œuvre d'un VPN aboutit à l'encapsulation des données, avec ajout d'un en-tête aux données privées afin de leur permettre de traverser Internet.

I.9. **Les scénarios de la mise en œuvre d'un serveur VPN**

Deux scénarios sont envisageables quant au positionnement du serveur VPN de l'entreprise :

1. Serveur VPN en périphérie de réseau : Ici, le serveur VPN est aussi le serveur Proxy qui donne accès à Internet pour le LAN ; il est également le pare-feu du réseau local et assure le mécanisme NAT. Il dispose forcément de 2 interfaces réseau[10].

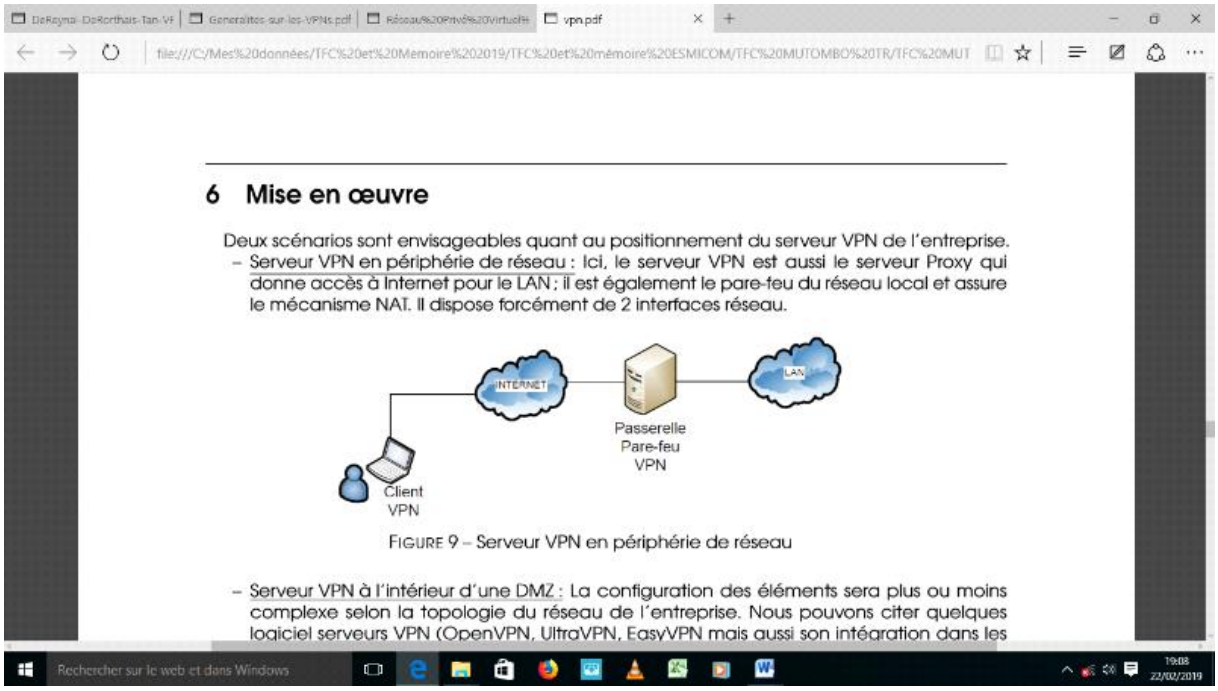
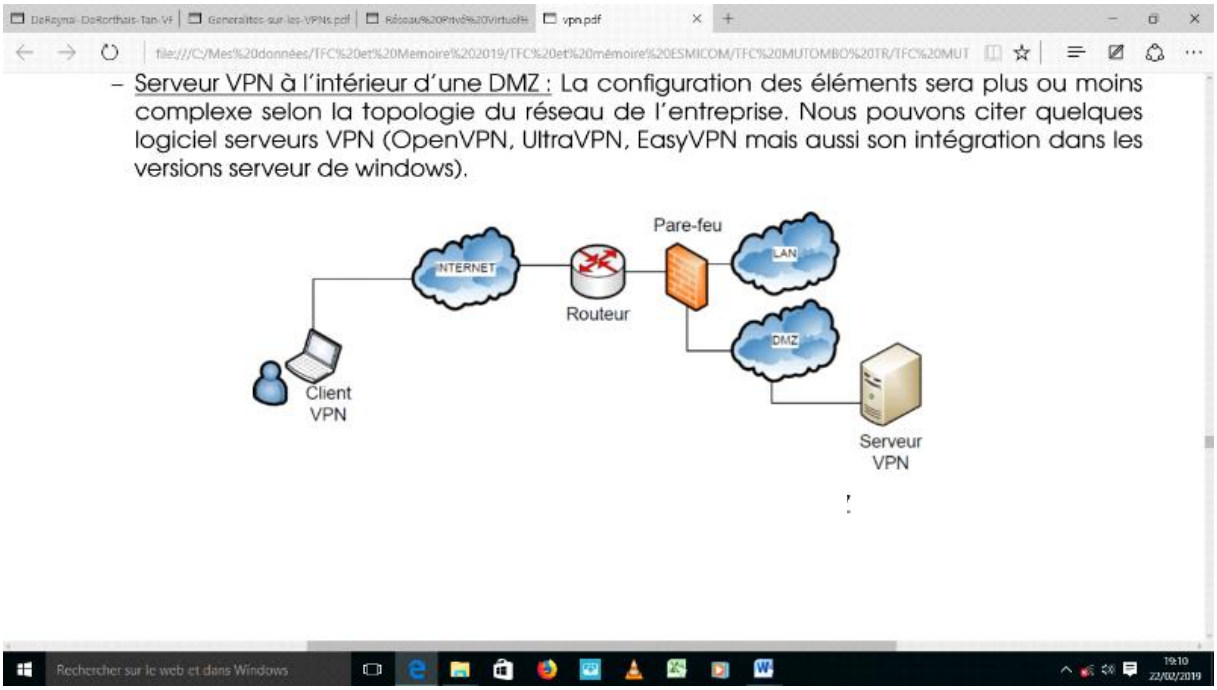


Figure I.13. Serveur VPN en périphérie de réseau.

2. Serveur VPN à l'intérieur d'une DMZ : La configuration des éléments sera plus ou moins complexe selon la topologie du

[10] *Prof Denis BOTA, Op.cit.*

réseau de l'entreprise. Nous pouvons citer quelques logiciels serveurs VPN (OpenVPN, UltraVPN, EasyVPN mais



aussi son intégration dans les versions serveur de Windows).

Figure I.14. Serveur VPN à l'intérieur de la DMZ.

I.10. **Solutions matérielles et logicielles**

I.10.1. **Solutions matérielles**

L'offre actuelle de solutions VPN est répartie en deux catégories : VPN autonomes et VPN intégrées, comprenant par exemple les pare-feu (firewall) ou les routeurs VPN. Ce sont les solutions VPN intégrées qui offrent potentiellement les plus importantes économies de coûts. Actuellement, des pare-feu déjà déployés, comme le "Cisco PIX", le "Nokia Checkpoint Firewall" et le "WatchguardFirebox", intègrent déjà des capacités VPN en option.

I.10.1.1. **Solution "VPN Intégrés"**

Pratiquement tous les routeurs, y compris les routeurs d'accès modulaires Cisco, intègrent également une solution VPN[11]. Le coût associé

[11] *https://www.cisco.com/c/fr_ca/solutions/small-business/resource-center/networking/how-to-set-up-router.html,Consulté le 22 août 2024 à 12h : 22*

à ces solutions est généralement déjà compris dans le coût du routeur ou du pare-feu. Dans ce type de scénario, activer des services VPN ne nécessite que quelques paramétrages du pare-feu ou du routeur.

Comme l'utilisation de réseaux VPN se fait généralement dans le cadre d'une politique de sécurité réseau complète, disposer d'une solution VPN intégrée peut permettre de réaliser des économies considérables en termes d'administration, notamment dans des environnements qui comprennent plusieurs pare-feu, routeurs et passerelles VPN.

Le Routeur Cisco 8921 est un bon exemple d'une solution intégrée.

Figure I.15. Cisco 892 - Routeur 10/100/1000 jusqu'à 50 tunnels VPN.

I.10.1.2. **Solution "VPN Autonomes"**

Les solutions VPN autonomes, que l'on appelle généralement des concentrateurs VPN, trouvent principalement leur place dans les entreprises ayant besoin de gérer plusieurs milliers de connexions VPN simultanées. Aucune solution VPN intégrée et aucun serveur VPN n'offre autant de fiabilité, de performances et une

telle capacité de montée en puissance. Le coût, en revanche, s'en ressent et vous risquez de payer très cher un concentrateur VPN d'entreprise qui offre ce type de fonctionnalités.

Nous pouvons citer en exemple, le DIGI Transport VC74002 gérant jusqu'à 3000 tunnels VPN.

Figure I.16. VC7400 - Jusqu'à 3000 tunnels VPN.

I.10.2. **Solutions logicielles**

Il faut aussi considérer les options offertes par la mise en place d'un serveur VPN pour des connexions sécurisées via internet.

Microsoft, Novell, UNIX, AS400 et Linux permettent d'utiliser des services VPN (certains mieux que d'autres). Il est probable que vous utilisiez déjà ces systèmes d'exploitation et que vous les maîtrisiez.

Mettre en place un serveur VPN peut vous faire réaliser des économies importantes si vous ne disposez pas d'un pare-feu ou d'un routeur VPN.

Figure I.17. Les différents logiciels du serveur VPN.

- OpenVPN (Linux/Windows) ;
- OpenSWAN (Linux) ;
- Tinc (Linux) ;

plus simplement dans l'OS du serveur.

I.11. **Conclusion partielle**

Dans ce premier chapitre, nous venons d'effectuer une étude présentative, descriptive, analytique et fonctionnelle sur le concept VPN, qui est un acronyme de Virtual Private Network.

Au cours de ce chapitre, nous avons parcouru les notions générales du réseau VPN en présentant les différents composants, topologies et modèles de ce réseau.

Par la suite nous avons plus loin aussi touché à la sécurité et au principe de la sécurité, ses objectifs ainsi que les attaques courantes de ce réseau.

CHAPITRE II : **PRESENTATION DE LA COUR DES COMPTES**

Section 1 : **SITUATION GEOGRAPHIQUE ET APERÇU HISTORIQUE**

II.1.1. **Situation géographique**

La Cour des comptes de la République Démocratique du Congo est Sise sur le n°13, avenue comité urbain, dans la commune de Gombe, Ville Province de Kinshasa, ayant comme référence la Cour de Cassation et la station-service SONAHYDROC. Il est entouré des avenues de la justice, de l'OMS, du colonel VANGU, des étoiles.

II.1.2. **Aperçu historique de la Cour des comptes**

On retrace les premiers rudiments de l'existence de la Cour des comptes de la République Démocratique du Congo vers les temps de la colonisation. La charte Coloniale du 18 octobre 1908 dans son article 13 confiait la gestion des finances publiques de la Colonie Congo-Belge au contrôle de la Cour des comptes de la Belgique.

Lors de l'accession du pays à l'indépendance, la loi fondamentale du 19 mai 1960 relative aux structures du Congo dans son article 243 institua pour la première fois une Cour des comptes propre au modèle congolais, tout en précisant les modalités de son organisation, laissant les finances du jeune Etat au contrôle de la Cour des comptes de Belgique, du moins pour l'exercice budgétaire en cours conformément au prescrits de l'article 254 de la même loi.

Trois ans après, le 16 avril 1963 intervint pour la première fois la promulgation de la loi portant organisation d'une Cour des comptes à essence parlementaire. Elle constitue la première apparition légale nationale en la matière. Le mobutisme fut emmené à dissoudre la Cour des comptes pour la faire revenir au bout de deux ans avec la venue de la Constitution du 24 juin 1967.

Vingt ans après, en février 1987, la Loi n°83-001 du 12 février 1983 instituant la commission parlementaire de contrôle des finances et des biens publics fut abrogé et il y eu l'entrée en vigueur de l'Ordonnance-loi

n°87-005 fixant composition et le fonctionnement de la Cour des comptes.

Au milieu de tous les changements intérieurs intervenus toutes dans la structuration et l'attribution des compétences des diverses institutions de la République, le texte encadrant l'organisation et le fonctionnement de la Cour des comptes ne connut pas de changement.

Le constituant dans la constitution du 18 février 2006telle que modifiés par la loi n°11/002 du 20 février 2011en son article 179, précise que la composition, l'organisation et le fonctionnement de la Cour des comptes sont fixées par une loi organique.

C'est au bout de douze ans que fut promulguée la loi organique portant composition, organisation et fonctionnement de la Cour des comptes le 13 novembre 2018. Dans un Etat qui répond depuis plus de vingt-cinq ans a la soumission au processus d'assistance par les institutions de BrettonWood , la Cour des comptes prit en 1992 la place d'une institution nécessaire et même indispensable chargée de répondre à la lutte contre la corruption, le gaspillages et les détournements de fonds publics. Conduire une étude sur la Cour des comptes et de discipline budgétaire ne saurait être faite sans passer au peigne fin ses origines et de son positionnement institutionnel dans le cadre des institutions publiques congolaises.

C'est à la suite d'un coup de pouce de la CEMAC que la Cour des comptes et de discipline budgétaire a eu un nouveau rôle et de nouvelles attributions au Congo. La CEMAC incita tous les Etats membres à mettre en place des Cours des comptes. Il y a existence au niveau de la CEMAC, d'une Cour des comptes communautaires des Etats membres dont le siège est installé au TCHAD. Les Etats membres ont la possibilité de faire recours à celle-ci ou leurs Cours des comptes propres. D'une façon précise, cette nouvelle façon de contrôler de la Cour des comptes les finances publiques prend sa source dans les Directives communautaires et recommandations relatives aux respects des lois de finances et au règlement général de la comptabilité publique. La consécration de la Cour

des comptes résulte donc du fait de l'existence d'un cadre juridique national appuyé par des recommandations de la CEMAC.

En effet, ce sont les directives de la CEMAC qui obligent les Etats à confier le contrôle juridictionnel des finances publiques aux Cours des comptes des Etats-parties.

Ainsi, l'article 3 de la section VI de la Directive relative au Code de transparence des finances publiques relatif au contrôle prévoit : « les finances publiques et les politiques qu'elles soutiennent sont soumises au contrôle externe de la Cour des comptes dont la création est obligatoire dans chaque Etats membres ».

Partant, la Cour des comptes par son adhésion aux organisations internationales supérieures de contrôle des finances publiques, à l'instar de l'INTOSAI, est l'institution supérieure de contrôle des finances publiques[12].

En République Démocratique du Congo, la mission de la Cour des comptes, qui est une institution supérieure de contrôle des finances publiques, est comme dans une confusion, comparé à la pratique de l'Inspection Générale des Finances (IGF). Ce service dépendant de la Présidence de la République opère tous azimuts le contrôle sur les entreprises publiques. Un peu plus bas nous allons démontrer les éléments de différence entre les deux organes afin d'élucider ce flou créant confusion.

[12] *Loi organique n°18/024 du 13 novembre 2018 portant composition, organisation et fonctionnement de la Cour des comptes*

SECTION 2 : **CADRE JURIDIQUE ET MISSION DE LA COUR DES COMPTES**

II.2.1. **Cadre juridique**

Le fonctionnement de la Cour des comptes est régi par un collectif des textes.

Les premiers textes législatifs organisant la Cour des comptes sont ceux de 1987. Ces textes sont les suivants :

L'ordonnance-loi n°87/005 du 06 février 1987, fixant la composition, organisation et fonctionnement de la Cour des comptes ;

L'ordonnance-loi n°87/032 portant statuts des magistrats de la Cour des comptes ;

L'ordonnance-loi n°87/031 relative à la procédure devant la Cour des comptes ;

L'ordonnance-loi n°87275 portant l'organigramme de la Cour des comptes.

Aujourd'hui, l'existence de la Cour des comptes est centrée sur des règles juridiques basées sur les textes suivants :

La constitution du 18 février 2006 telle que modifiée par la Loi n°11/002 du 20 janvier 2011 portant révision de la Constitution, en ses articles 178 à 180 ;

La loi n°11/011 du 13 juillet 2001 relative aux finances publiques, en ses articles 123 à 126 ;

Loi organique n°18/024 du 13 novembre 2018 portant composition, organisation et fonctionnement de la Cour des comptes.

II.2.2. **Mission de la Cour des comptes**

La Cour des comptes de la République Démocratique du Congo est l'Institution Supérieure de Contrôle des finances publiques, selon que dispose l'article 180 de la Constitution. Elle a pour mission d'effectuer de manière indépendante un contrôle externe à posteriori des finances de

l'Etat et de ses démembrements ainsi que des organismes, entreprises publiques et autres entités bénéficiant du concours financier de l'Etat. Elle porte un jugement sur la régularité des états financiers et des comptes des comptables publics selon une approche contradictoires et conformément à des normes généralement reconnues.

La Cour des comptes contribue par ses missions de vérification et de contrôle de conformité à l'amélioration de la gouvernance financière et au respect des principes de reddition des comptes. Elle soumet au président de la République, au Parlement et au Gouvernement un rapport assorti de recommandations sur les résultats de ses travaux.

Elle entend servir la Nation en veillant à une utilisation transparente et efficace des finances et des biens publics.

SECTION 3 : **VISION INSTITUTIONNELLE ET VALEURS**

II.3.1. **Vision institutionnelle**

Être une Institution de contrôle indépendante, écoutée et dont le travail est suivi d'effets ;

Être un centre d'excellence dont la crédibilité se fonde sur le profession1nalisme et la qualité de son travail ;

Être une institution de référence de par le comportement et l'éthique de son personnel.

II.3.2. **Valeurs**

- **Indépendance** : la Cour des comptes de la République Démocratique du Congo veille à son indépendance en portant des avis et des jugements de manière impartiale et souveraine ;
- **Professionnalisme** : la Cour des comptes effectue ses contrôles de façon objective et équitable en appliquant les normes professionnelles les plus élevées ;

- **Intégrité** : la Cour des comptes applique un code de déontologie stricte et utilise les normes les plus élevées en matière d'éthique professionnelle ;
- **Servir l'intérêt public** : la Cour des comptes promeut la bonne gouvernance et la transparence dans la gestion des finances publiques afin de participer à l'amélioration des conditions de vie de la population Congolaise.

SECTION 4 : **COMPOSITION DE LA COUR DES COMPTES**

Un siège, un parquet et un personnel administratif et technique. Tel est la composition de la Cour des comptes. Cependant, ne sont pris en considération en qualité de membres de la Cour des comptes que les magistrats du siège et le Procureur général près cette Cour.

Le siège est composé du Premier président, des Présidents des Chambres, des Conseillers maîtres, des conseillers référendaires et des conseillers. Le Procureur général exerce le Ministère Public près la Cour des comptes, il est assisté d'un ou de plusieurs premiers avocats généraux et d'un ou de plusieurs avocats généraux choisis, selon le cas, parmi les présidents des Chambres, les Conseillers maîtres et les conseillers référendaires.

Les membres de la Cour des comptes sont nommés, relevés de leurs fonctions et le cas échéant, révoqués par le Président de la République, après avis de l'Assemblée Nationale[13].

Les membres de la Cour des comptes ont la même préséance que les membres de la Cour suprême de justice[14].

1. Président de la Cour des comptes

Le Premier Président de la Cour des comptes est nommé, relevé, le cas échéant, révoqué de ses fonctions par le Président de la République, conformément à l'article 178 de la Constitution. Son mandat est d'une

[13] *Constitution RDC, art.178.*

[14] *Lo. n°87-005 du 6 février 1987, art 5.*

durée de 5 ans renouvelable une seule fois[15]. L'actuel Premier Président répond au nom de MUNGANGA NGWAKA Jimmy

Le Premier Président de la Cour des comptes assure la direction générale de la Cour des comptes. A ce titre, il définit l'organisation générale des travaux et arrête un programme annuel. Il préside les audiences solennelles et les sections réunies. Il peut présider les séances de Sections, des Chambres et des Commissions.

Le Premier président de la Cour des comptes signale au Président de la République, au Président de l'Assemblée nationale, au Président du Sénat, au Premier ministre, au Président de l'Assemblée provinciale, au Gouverneur de province, au Président de l'organe délibérant et au chef de l'exécutif de l'entité territoriale décentralisée, selon le cas, des propositions de la Cour des comptes qui n'ont pas eu de suite.

Le Premier président de la Cour des comptes représente le Conseil supérieur de la Cour des comptes. Il convoque et préside les réunions de l'Assemblée générale et du Bureau.

En cas d'absence ou d'empêchement, il est remplacé par le plus ancien des vice-présidents d'après l'ordre des nominations.

2. Procureur général près la Cour des comptes

Le procureur général près la cour des comptes est nommé, relevé de ses fonctions et, le cas échéant, révoqué par le Président de la République, conformément à l'article 178 de la Constitution.

Le Procureur Général près cette cour exerce son ministère par voie de conclusions, d'avis, de réquisition et de note. Il tient l'état des ordonnateurs, comptable publics assignataires des recettes et des dépenses tant du pouvoir central, de la province, de l'ETD que des entreprises du portefeuille, établissement et services publics et autres personnes morales assujetties au contrôle de la cour des comptes. Il veille à la production des comptes dans le délai prescrit et, en cas de

[15] *Lo. n°18/024 du 13 novembre 2018, art 17.*

retard, requiert l'application des amendes prévues par la loi. Il défère à la Cour des comptes les opérations présumées constitutives de gestion de fait, à son initiative ou à la demande du ministre ayant les finances ou le budget dans ses attributions, d'autres ministres intéressés, des responsables des ETD et des entreprises du portefeuille, de établissements et services publics, sur dénonciation des tiers sans préjudice du droit de la Cour de se saisir d'office de ces opérations.

Il présente des conclusions écrites sur les rapports qui lui sont communiqués, avec pièces à l'appui. Tous les rapports lui sont communiqués particulièrement les rapports concernant les quitus, les débets, les amendes, les décisions sur la compétence, les comptabilités de fait ainsi que les appels, les pourvois cassation, les recours en révision et les rétractations. Les autres rapports lui sont communiqués, soit sur sa demande, soit par décision des présidents des Chambres. Il peut, ainsi que les avocats généraux, assister aux séances des sections et des chambres et y présenter des observations orales. Il est présent ou représenté par un avocat général dans les commissions et comités institués au sein de la Cour. Il dispose d'un secrétariat.

3. Les présidents de Chambre

Les présidents de chambre sont choisis parmi les conseillers maitres[16].

Ils dirigent les activités de leurs Chambres. A ce titre, ils sont chargés entre autres de :

- Présider les audiences et réunions de leur Chambre et des sections ;
- Soumettre au Premier président de la Cour des comptes des propositions en vue de l'établissement du programme annuel d'activités et mettre en œuvre le programme approuvé ;

[16] *Loi organique n°18/024 du 13 novembre 2018 portant composition, organisation et fonctionnement de la Cour des comptes*

- Répartir, au vu du programme annuel de la Cour des comptes, les travaux entre les magistrats de la Chambre et, s'il échait, entre les sections, et veiller à leur traitement
- Informer régulièrement le Premier président de la Cour des comptes de l'état d'exécution du programme, et lui proposer toutes mesures propres à accroître les performances de l'institution ;
- S'assurer de la qualité des travaux effectués au sein de la Chambre, en veillant au perfectionnement constant de ses membres et à l'application des méthodologies, guides et normes de vérification édités par la Cour des comptes ;
- Formuler toutes suggestions pour l'amélioration de ces instruments de travail ;
- Transmettre au premier président de la cour des comptes les propositions d'insertion au rapport général émanant de leur chambre ;

En cas d'absence ou d'empêchement, il est remplacé par le plus ancien des conseillers d'après l'ordre des nominations.

4. Les premiers avocats généraux et les avocats généraux

Ils sont choisis, selon le cas, parmi les présidents des chambres, les conseillers maitres et les conseillers référendaires. Ils peuvent représenter le procureur général aux séances de différentes formations de la Cour des comptes et y présenter des observations orales. Ils exercent leurs fonctions sous l'autorité du procureur général. Ils sont affectés pour une durée de trois ans renouvelable une seule fois et, le cas échéant, changés d'affectation par le premier Président de la cour après avis du conseil supérieur de la Cour de comptes. En cas d'absence ou d'empêchement du procureur général, le premier avocat général, ou à défaut, l'avocat général le plus ancien dans l'ordre de nomination assure sa suppléance.

5. Le rapporteur général et les rapporteurs généraux adjoints

La Cour des comptes comprend un rapporteur général et deux Rapporteurs Généraux Adjoints choisis, selon le cas parmi les présidents des Chambres et les conseillers. Ils sont désignés et, les cas échéants, relevés de leurs fonctions par le Président de la République, sur proposition du conseil supérieur de la Cour des comptes et après avis de l'assemblée nationale.

Le rapporteur général assiste le premier président dans la gestion du personnel de la cour. Il assure la gestion des services administratifs et techniques ainsi que le greffe central, assiste aux séances des sections réunies, aux audiences solennelles et en dresse le procès-verbal, contresigne les arrêts et autres décisions des sections réunies, en délivre les expéditions et en conserve les minutes, assure la bonne garde et la tenue des archives de la cour.

Les rapporteurs généraux adjoints sont ceux qui assistent le rapporteur général.

6. Des magistrats (conseillers)

Les Conseillers sont repartis dans les sections. Il leur appartient d'instruire les dossiers et de rédiger les conclusions qui seront soumises aux délibérations de la Cour.

7. Du greffier en chef et des greffiers

Le greffier en chef et les greffiers sont désignés et relevés de leurs fonctions par le président de la Cour des comptes. Le greffier en chef est choisi parmi les greffiers de la Cour des comptes ayant le grade de directeur. Il est assisté de greffiers qui sont choisis parmi le personnel administratif de la Cour des comptes ayant au moins le grade de chef de bureau.

Le greffier en chef assure le fonctionnement du greffe de la Cour sous l'autorité du rapporteur général de la Cour des comptes.

Avant d'entrer en fonction, les greffiers de la cour de comptes prêtent le serment suivant devant la Cour des comptes : « je jure de

remplir loyalement et fidèlement les fonctions qui me sont confiées et de respecter le secret des délibérations de la Cour des comptes ».

Le greffier en chef assure la bonne tenue de et la gestion des registres, actes, documents, et autres archives de la Cour des comptes. En cas d'absence ou d'empêchement, le greffier en chef est suppléé par le greffier le plus gradé de suivant l'ordre de nomination.

8. Le personnel administratif et technique

Le personnel technique est constitué des fonctionnaires, auditeurs et vérificateurs qui assistent les magistrats dans les travaux de contrôle.

Le personnel administratif est constitué de tous les autres fonctionnaires qui ne participent pas aux travaux de contrôle.

Outre les dispositions générales du statut des agents de carrière des services publics de l'Etat, le personnel administratif et technique de la Cour des comptes est régi par un règlement d'administration particulier.[17]

II.4. **Analyse De L'existant**

Sur ce point nous allons faire notre étude sur nos deux sites ; à savoir : Site de la Gombe et le Site de Royal.

II.4.1. **Etudes Des Moyens**

1. **Moyens humains**

Cette étude est nécessaire pour mieux comprendre les qualifications du personnel prestant au sein de la Cour des comptes.

Grâce aux investigations menées, nous avons découvert que cette dernière possède un personnel qualifié et expérimenté :

[17] *Loi organique n°18/024 du 13 novembre 2018 portant composition, organisation et fonctionnement de la Cour des comptes, Art 23*

N°	NOMBRE	DESIGNATION	QUALIFICATION
1.	51	Magistrats	Conseillers
2.	11	Directeurs	
3.	59	Auditeurs	
4.	6	Chef de division	
5.	14	Greffiers	
6.	23	Vérificateurs	Personnelles Techniques et Administratifs
7.	16	Chef de bureaux	
8.	37	ATA1	
9.	14	ATA2	
10.	9	AGB1	
11.	2	AGB2	
12.	14	Huissiers	

Source : Direction de gestion des ressources humaines et intendances

2. **Moyens Matériels et Logiques**

a. **Site de Gombe**

Le matériel inventorié dans l'intendance est le suivant :

N°	NOMBRE	LIBELLE	MARQUE
1.	89	Tables	BOIS
2.	117	Chaises	MÉTALLIQUE
3.	4	Chaises	FAUTEUIL
4.	20	Armoires	MÉTALLIQUE
5.	50	Armoires	BOIS
6.	50	Ordinateurs fixe(i7, SDD : 1TB , RAM : 16G)	HP
7.	109	Lap Top (i7, SDD : 1TB , RAM : 16G)	HP
8.	50.	Imprimante LaserJet Canon MF453dw	Canon

Source : Division de l'intendance

II.4.2. **Liste descriptive des matériels utilisés pour le réseau intranet et la téléphonie**

Descriptions/Serveur	Qté
Routeur Cisco 2900 series modele CISCO 2911-SEC/K9 Cisco 2911 Security Bundle W/SEC license PAK	2
Serveur HP PROLIANT 380 MT de données, Capacité des disques durs 2 Téra B, RAM 6GB, processeur i5 : Windows Serveur 2012 STD 64 Bit Data backup racable + console	1
Serveur Dell processeur 2Xamd epyc9334 2.7GHz, 2x16GB DIMM, 1X480GB SSD SATA	1
Configuration serveur etusers, configuration de messagerie	1

Exchange et Outlook, restrictions d'accès sur les ressource et Installations.	
Mise à niveau d'administrateur réseau Cour des Comptes.	1
Internet Câblage LAN	
Rack 42 U Baie VDA-B 42U 66 pann. Lat+arrie 1200mm	1
Rack 15U Coffret KDBox 15U P600 vitré	5
Câblage UTP cat 6 (cartons)	22
Câblage SFTP6 (cartons)	8
Goulottes 100X 50	100
Goulottes 38X50	150
Goulottes 25X16	200
Prises doubles RJ45	250
Switch 24 ports Gigabyte POE Manageable	15
Patch panel 24 ports	20
Patch câbles originaux (3m) CORDON UUTP CAT64 550MHZ LSZH 3M	300
AP Wifi B, g et n, haute portée (wifi Power : 2.4GHZ Hi POWER 2X2 MIMO AirMax TDMA Station Atheros MIPS 24KC, 400MHZ 32MB SDRAM, 8MB Flash 2X10/100 BASE-TX (Cat. 6RJ-45) Ethernet Interface)	10
STABILISATEURS 5000 VA	5
STABILISATEURS 1500 VA	10
ONDULEURS 3000 VA	10
Installation LAN	1
Interphone-bureau Câblage VoIP sous réseau intranet	
Entrée de gamme : Voir VIP-IEE 802.3af PoE Ethernet IP phone (2*RJ45), Dot Matrix LCD,SMS	70

Haut de gamme: VIP-360PT. POE Business IP Phone, Graphic LCD W/Backlight, IAX2,2 Voice line, BLF/BLA ,QoS, VLAN, STUN, DND,Valler ID, Auto provision- SIP	20
FNSW-2400PS 24-Port 10/100 Web/Smart Ethernet POE Switch	5
PATCH PANEL 24 PORT CAT 6	5
Central téléphonique serveurs (OS+ applications)	
Serveur 1 : IPX- 1980 100/30 User SIP Base IP PBX, 8*FXO, Asterisk 1.8, IPV6, T.38, Voice Mail server, busy Lamp Field, skpe for SIP, PLANET DDNS, Auto provision for PLANET IP PHONE 500 User Asterisk base Advance IP PBX with 2-expandable PCL interface slots, proxy server-SIP2.0	1
IPX-21GS 4-Port GSM Module Gateway (1*FXS+1G*SM+1*PSTN)-SIP/H323 Dual protocol	1
VIP-480 4-port VolP Gateway (2*FXS+2*FXO)-SIP/H323 Dual protol	1
Casque Jabra pour interphone+logiciels de configuration.	50
Installation Téléphonique	1

b. **Site de Royal**

Le matériel inventorié dans l'enceinte du royal est le suivant :

N°	NOMBRE	LIBELLE	MARQUE
1.	89	Tables	BOIS
2.	117	Chaises	MÉTALLIQUE
3.	4	Chaises	FAUTEUIL
4.	20	Armoires	MÉTALLIQUE
5.	50	Armoires	BOIS
6.	50	Ordinateurs fixe(i7, SDD : 1TB , RAM : 16G)	HP
7.	109	Lap Top (i7, SDD : 1TB , RAM : 16G)	HP
8.	50.	Imprimante LaserJet Canon MF453dw	Canon

Source : Division de l'intendance

3. **Moyens Financiers**

La Cour des comptes jouit d'une autonomie administrative et financière et dispose d'une dotation propre. Cependant, pour la réalisation des certains projets, la source de financement peut être soit du gouvernement ou des partenaires.

II.5. **Critique De L'existant**

Il est d'une extrême importance que l'on applique un critique sérieux sur la gestion quotidienne; cette critique permettra d'une part, une sensibilisation aux principaux problèmes et d'autre part, fournira les besoins d'une réelle amélioration des conditions de travail.

Note critique portera sur :

- Les Objectifs
- Les Moyens

II.5.1. **Critique Des Moyens Utilises**

a) **Moyens Matériels**

En dépit de la situation Socio-économique de l'heure, il n'est pas surprenant qu'il y ait plus à déplorer sur ces moyens :

- On ne devrait pas limiter l'exploitation de l'ordinateur au traitement de texte et aux travaux sur Excel tel que nous avons constaté ;
- Pas de connexion internet dans tous les deux sites.

*b)***Moyens Financiers**

La Cour des comptes jouit d'une autonomie administrative et financière et dispose d'une dotation propre.

*a)***Synthèse des anomalies**

Les échanges des informations ce fait d'une manière archaïque ; il faut demander aux agents de se déplacer d'un Site à un autre, même pour une simple signature.

Dans le but de valoriser et de permettre la communicabilité et les échanges entre les sites dispersés, il est aujourd'hui d'une extrême importance d'intégrer les nouvelles techniques de l'information basés sur l'intranet et l'interconnexion des réseaux.

II.6. **Proposition Des Solutions**

1. **Solution centralisée**

L'informatique centralisée est caractérisée par l'implantation d'un ordinateur central ou d'un réseau local dont le serveur intègre l'essentiel des ressources et autour duquel gravite tous les utilisateurs (client serveur).

2. **Solution Intranet**

L'intranet est un réseau informatique utilisant les services du protocole TCP/IP pour assurer la communication. C'est-à-dire un réseau dont la configuration se fait sur base du protocole TCP/IP.

L'intranet est un réseau qui exprime la fusion d'un LAN et les atouts de l'internet, bâtit sur le TCP/IP.

3. **Solution Internet**

L'Internet est le réseau informatique mondial qui rend accessibles au public des services comme le courrier électronique et le World Wide web.

4. **Solution VPN**

C'est un réseau informatique constitué de plusieurs sites dont l'interconnexion se fait par le canal de l'Internet. On crée dans ce cas un chemin virtuel sur Internet.

II.6.1. **Choix De La Meilleure Solution**

Les avantages et les inconvénients dans différentes solution que nous venons d'énumérer, nous optons pour la solution d'intranet et le VPN, ce dernier pouvant nous permettre l'intégration de l'interconnexion des sites.

II.7. **Identification Des Flux**

Les utilisateurs sont répartis dans des sites différents et peuvent utiliser les mêmes applications et accéder aux mêmes données.

Ainsi, cette phase permet de caractériser les flux de chaque application (type, périodicité) et d'identifier les acteurs qui émettent et reçoivent les données.

II.7.1. **Présentation des flux**

Application	**De- vers**	**Objet**	**Type de flux**	**Périodicité**
Base de données	Tous les deux sites : Gombe & Royal	Gestion du personnel et logistique	Client-Serveur	Mise à jour : toutes les nuits Consultation : Tous les jours
Datawarehouse	Tous les deux sites : Gombe & Royal	administration	Transfert des gros fichiers	Mise à jour : toutes les nuits Consultation : Tous les jours
Messagerie	Intrasite et intersites		Transfert des fichiers (et de données)	Tous les jours
Visioconférence	Intersites	Formation, Forum de discussion, échange	Conversation (dialogue)	Suivant un calendrier ou par urgence

Serveur Web	Tous les sites	Information, accès aux bases de données	Transactionnel Client-serveur	Tous les jours
Connexion Internet	Tous les sites	Consultation Web Messagerie	Transactionnel Transfert des fichiers	Tous les jours

Les flux recensés peuvent être classés en trois catégories :

- Les flux conversationnels ;
- Les flux transactionnels
- Les flux de type transfert des fichiers

1. **Les flux de type conversationnel**

Les applications conversationnelles sont les plus courantes dans le monde TCP/IP. Le principe repose sur l'envoi d'un caractère avec écho distant.

Une session étant établie entre le poste de travail et une machine, tout caractère frappé sur le clavier est envoyé à la machine, traité par cette dernière, et enfin renvoyé tel quel pour affichage, éventuellement avec d'autres attributs.

Chaque caractère peut déclencher une action comme l'affichage d'une fenêtre. Le type de flux dépend de l'activité de l'utilisateur et est composé de trames courtes. Le temps de réponse est donc primordial pour ce type d'application.

Il se doit d'être plus régulier possible et tout utilisateur doit s'habituer au temps de réponse quelque soi sa qualité, à condition qu'il soit régulier.

2. **Les flux de type Transactionnel**

Le mode transactionnel est le fonctionnement le plus courant pour les applications critique sur les systèmes centraux. La technique consiste à envoyer un écran de saisie vers un terminal, à réaliser localement les modifications, puis à renvoyer les données modifiées vers le serveur.

Les flux générés entre serveurs web et navigateurs peuvent être assimilés au mode transactionnel, bien que le volume des pages web soit beaucoup plus important. Ces flux sont caractérisés par un trafic descendant (serveur web vers navigateur) plus important que le trafic montant (les données du formulaire ou clic sur une URL).

3. **Les flux de type Transfert de fichiers**

Ces flux sont caractérisés par des échanges soutenus et des trames longues. Leurs occurrences peuvent être prévisibles, dans la mesure où la majorité des transferts de fichiers est souvent associée à des traitements automatiques qui ont lieu en dehors des heures ouvrées, par exemple lors de la sauvegarde ou de la synchronisation de bases de données.

Pendant les heures ouvrées, ce type de flux peut dégrader les temps de réponse des flux transactionnels et surtout des flux conversationnels.

Cette interférence peut être contrôlée par des mécanismes de priorité positionnés sur les équipements d'interconnexion tels que les routeurs.

II.8. Contraintes Des Faisabilités De La Solution Choisie

La faisabilité de notre solution choisie peut être contrainte à 3 niveaux à savoir :

- **Contrainte fonctionnelle** : elle est justifiée par les besoins exprimés par les utilisateurs. Nous ne saurons apporter notre solution que si les besoins des utilisateurs se seraient sentis pertinent.

- **Contrainte technique** : elle est justifiée par les moyens techniques pouvant nous permettre d'apporter sans embuches notre solution que s'il existe les moyens techniques.

- **Contrainte économique** : elle est justifiée par les moyens financiers pouvant faire face du coût de réalisation et de mise sur pied de notre solution choisie.

II.9. Conclusion partielle

Ce deuxième chapitre se base sur les points phares du travail, nous avons présenté d'une manière claire et brève L'institution, son historique, ses objectifs, son système informatique existant et ensuite nous avons également porté nos suggestions pour une amélioration de ladite entreprise spécifique de son réseau informatique et c'est ainsi que nous mettons fin à ce chapitre.

DEUXİÈME PARTIE : APPROCHE PRATİQUE

CHAPITRE III : **PLANING PREVISIONNEL DE REALISATION DU PROJET**

III.1. **Introduction**

Dans ce chapitre, nous allons présenter les détails du projet, les étapes et les ressources financières.

Un projet est un ensemble d'activités ou d'actions à accomplir destiné à répondre à des objectifs précis dans un temps limité en rassemblant des ressources financières, matérielles et humaines nécessaire suivant un processus cohérent sous la responsabilité d'un individu appelé chef de projet.[18] En générale, la planification du projet informatique exige une préparation considérable, autrement ne pas s'y engagée. Tout projet quel qu'il soit informatique ou autre, doit être observé avec plus d'assiduité, cela nous ramène à repartir un projet quatre grandes étapes suivant :

Etude de faisabilité et examen des scenarios possible ;

- Conception ;
- Réalisation ;
- Mise en œuvre.

Un planning prévisionnel du projet est appelé à être planifier afin de pouvoir le maitriser dans certaines contraintes liées aux coûts et aux délais imposés avec une vérification constante sur le plan établi et respecté.

III.2. **Cadrage Du Projet**

Comme dit en amont dans ce chapitre, un projet est un système dans lequel sont définis les éléments et les variables, notamment, le temps le coût et les moyens matériels sous la responsabilité d'un individu. Il peut cependant être représenté par des outils graphiques permettant

[18] *Prof. KUTANGILA MAYOYA, Cours Projet informatique, L1 Telecom/WUB,2022 inédit*

de mieux visualiser l'ensemble des taches et des ressources disponibles pour cette démarche.

III.2.1. **Préparation D'un Problème D'ordonnancement**

La représentation d'un problème peut se faire par un graphe dans lequel le chemin d'une valeur optimale est l'objet d'une recherche. Il existe cependant plusieurs démarches ou méthodes à suivre pour atteindre ce but sur le plan d'ordonnancement, le plus utilisées sont notamment :

- Méthode de potentiel IMETRA ;
- Méthode PERT ;
- Méthode de GANT.

Afin d'élaborer avec compréhension notre projet et tracer notre chemin critique, sur base d'une méthode quelconque, nous avons opté en ce qui nous concerne la méthode PERT.

1) **Méthode PERT**

Pour Planning Evaluation and ReviewTechnic, PERT en sigle, c'est une technique de coordination des taches dont l'application nécessite une familiarité et une connaissance parfaite du projet. Elle permet de déclenchement de fin. Elle permet en outre d'identifier les dates limites de début et la fin ainsi que le chemin critique pour obtenir le délai global du projet.[19]

2) **Représentation et identification de tache**

Les différentes étapes de réalisation de réseau et de solution VPN sont reprises dans le tableau ci-dessus.

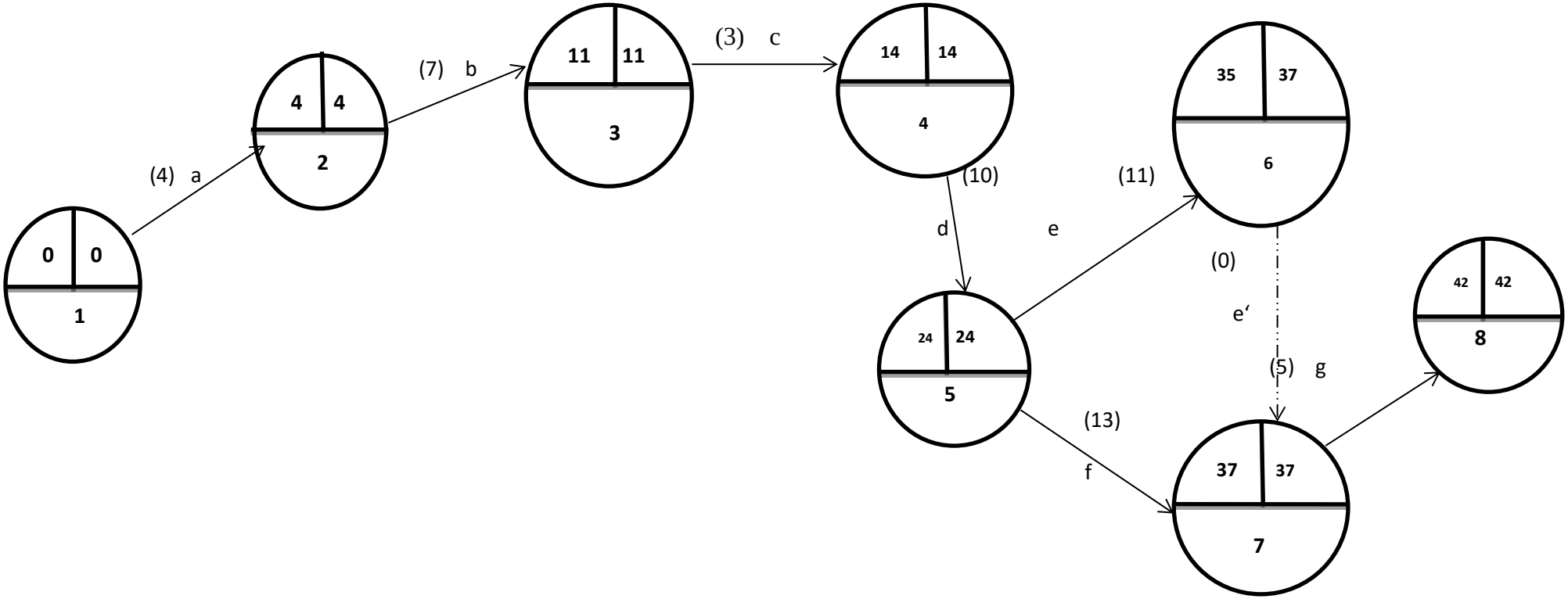
[19] *Prof. KUTANGILA MAYOYA, Op.cit.*

III.2.2. **Tableau D'identification Des Taches**

CODE TACHE	DESIGNATION	TACHE ANTERIEURE	DUREE EN JOUR	COÛT EN DOLLARDS
a	Analyse et description du schéma existant	-	4	500
b	Relever les défaillances et faiblesse du réseau existant	A	7	1.200
c	Proposition de la meilleure solution du réseau existant	B	3	2.300
d	Choix de fournisseur d'accès (VPN) et de matériels additionnels	C	10	54.431
e	Mise en œuvre des modifications proposées (Solution VPN)	D	11	2.000
f	Teste du Réseau et Formation des utilisateurs	d, e	13	1.000
g	Lancement du réseau	F	5	-

a) **Graphe brut**

Les taches toutes entières sont représentées sur un schéma typique



b) **Matrice booléenne**

C'est un outil de vérification du graphe, la présence d'un arc dans le graphe est symbolisée par le chiffre 1 tandis que l'absence d'un arc dans le graphe est symbolisée par le chiffre 0.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	0	1	0	0	0	0	0	0
2	0	0	1	0	0	0	0	0
3	0	0	0	1	0	0	0	0
4	0	0	0	0	1	1	0	0
5	0	0	0	0	0	1	0	0
6	0	0	0	0	0	0	1	0
7	0	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0

c) **Matrice value**

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	0	4	0	0	0	0	0	0
2	0	0	11	0	0	0	0	0
3	0	0	0	14	0	0	0	0
4	0	0	0	0	24	35	0	0
5	0	0	0	0	0	37	0	0
6	0	0	0	0	0	0	37	0
7	0	0	0	0	0	0	0	42
8	0	0	0	0	0	0	0	0

d) **Calcul de niveau**

Nous avons utilisé la méthode de sommet par numéro

N0= {1}

N1= {2}

N2= {3}

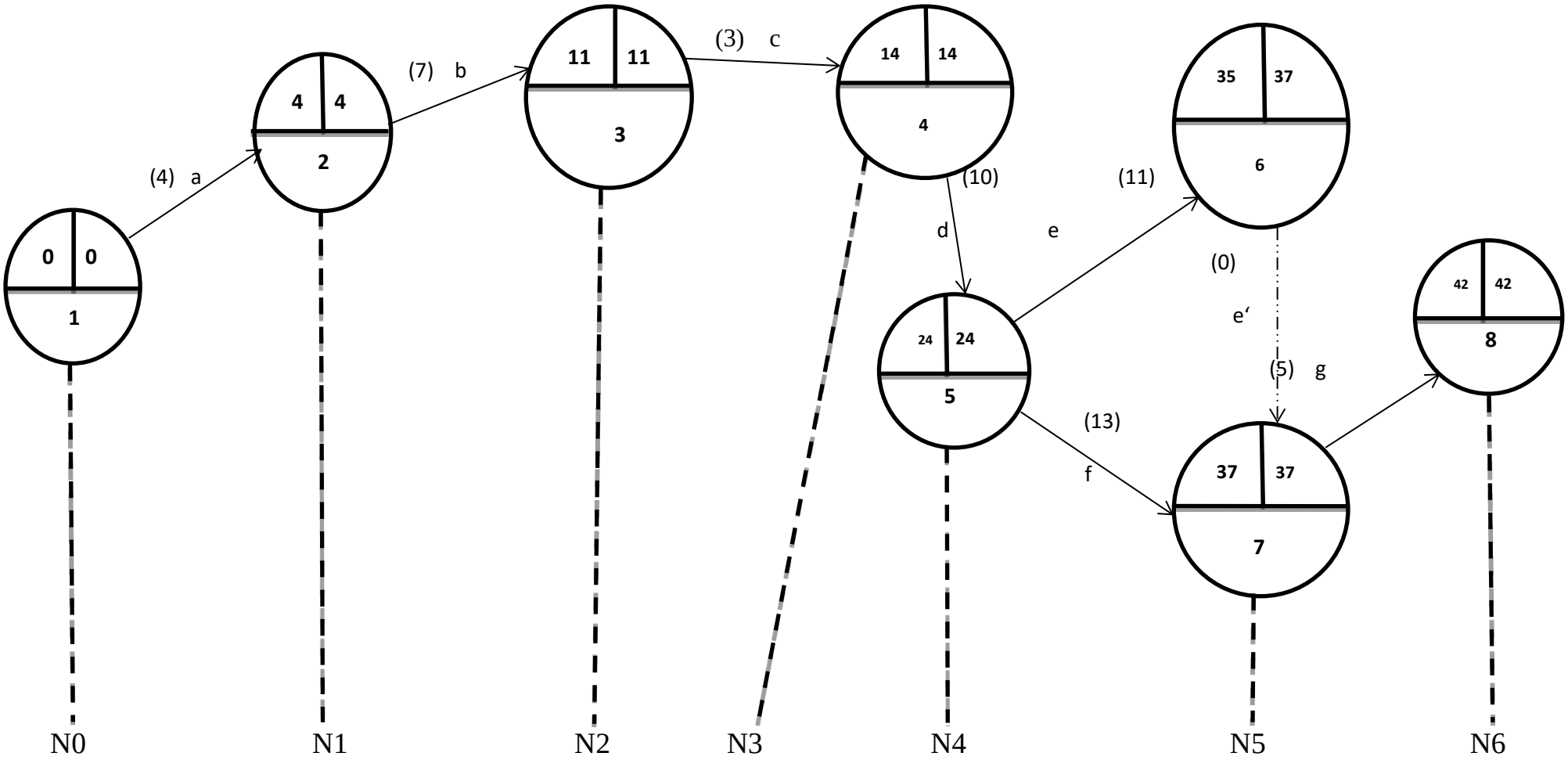
N3= {4}

N4= {5}

N5= {6,7}

N6= {8}

e) Graphe ordonné



f) La recherche des dates au plutôt (DTO) et des dates au plus tard (DTA)

- Date au plutôt : une date au plutôt est une date la plus rapprochée à laquelle une étape est censé être réalisée. Afin de la calculer, la formule ci-dessous est utilisée :

$$DTO(y) = Max + \{DTO(x) + d(i)\}$$

DTO (1) = 0
DTO (2) = DTO (1) + d (a) = 0 + 4 = 4
DTO (3) = DTO (2) + d (b) = 4 + 7 = 11
DTO (4) = DTO (3) +d (c) = 11 + 3 = 14
DTO (5) = DTO (4) + d (d) = 14 + 10 = 24
DTO (6) = DTO (5) + d (e) = 24 + 11 = 35
DTO (7) = DTO (6) + d (e') = 35 + 0 = 35
Max {DTO (5) + d (f) = 24 + 13 = 37}
DTO (8) = DTO (7) + d (g) = 37 + 5 = 42

- Date au plus tard, c'est une date dans laquelle une étape doit absolument commencée, afin de la calculer. La formule ci-dessous est utilisée :

$$DTA(x) = Min\{DTA(y) - d(i)\}$$

DTA (8) = 42
DTA (7) = DTA (8) – d (g) = 42 – 5 = 37
DTA (6) = DTA (7) – d (e') = 37 – 0 = 37
DTA (5) = DTA (6) – d (e) = 37 – 11 = 26
Min {DTA (7) – d (f) = 37 – 13 = 24}
DTA (4) = DTA (5) – d (d) = 24 – 10 = 14
DTA (3) = DTA (4) – d (c) = 14 -3 = 11
DTA (2) = DTA (3) – d (b) = 11 – 7 = 4

DTA (1) = DTA (2) – d (a) = 4 – 4 = 0

g) **Marge libre et mage totale**

Marge libre : est le délai dont on dispose pour la mise en route de la tâche (g), notamment lancement du réseau, sans pour autant compromettre la date au plutôt de l'étape (y).

Elle est calculée en utilisant la formule suivante :

ML (g) = DTO (y) – DTO (x) – d (i)

ML (a) = DTO (2) – DTO (1) - d (a) = 4 – 0 – 4 = 0
ML (b) = DTO (3) – DTO (2) – d (b) = 11 – 4 – 7 = 0
ML (c) = DTO (4) – DTO (3) – d (c) = 14 – 11 – 3 = 0
ML (d) = DTO (5) – DTO (4) – d (d) = 24 – 14 – 10 = 0
ML (e) = DTO (6) – DTO (5) – d (e) = 35 – 24 – 11 = 0
ML (e') = DTO (7) – DTO (6) – d (e') = 37 – 35 – 0 = 2
ML (f) = DTO (7) - DTO (6) – d (f) = 37 – 24 – 13 = 0
ML (g) = DTO (8) – DTO (7) – d (g) = 42 -37 -5 = 0

Marge totale : est le délai dont on dispose pour la mise en route de la tâche (g), lancement du réseau, sans pour autant modifier la date au plus tard de l'étape (y).

MT (g) = DTA (y) – DTO (x) – d (i)

MT (a) = DTA (2) – DTO (1) – d (a) = 4 – 0 – 4 = 0
MT (b) = DTA (3) – DTO (2) – d (b) = 11 – 4 – 7 = 0
MT (c) = DTA (4) – DTO (3) – d (c) = 14 – 11 – 3 = 0
MT (d) = DTA (5) – DTO (4) – d (d) = 24 – 14 – 10 = 0
MT (e) = DTA (6) – DTO (5) – d (e) = 37 – 24 – 11 = 2
MT (e') = DTA (7) – DTO (6) – d (e') = 37 – 35 – 0 = 2
MT (f) = DTA (7) – DTO (5) – d (f) = 37 – 24 – 13 = 0

MT (g) = DTA (8) – DTO (7) – d (g) = 42 – 37 – 5 = 0

h) **Chemin critique**

Le chemin critique est celui qui relie toutes les taches critique; les taches critiques sont celles dont la marge totale est nulle.

- Si DTO = DTA, alors l'étape est dite critique ; dans le cas contraire elle est dite non critique ;
- Si ML = MT alors la tâche est critique, dans le cas contraire, la tâche est dite non critique ;
- Le chemin critique correspond au chemin de valeur maximum du graphe P.E.R.T

Dans ce projet, le chemin critique se présente comme suit : a, b, c, d, f, g.

i) **Tableau des résultats de DTO et DTA**

SOMMET	DTO	DTA
1	0	0
2	4	4
3	11	11
4	14	14
5	24	24
6	35	37
7	37	37
8	42	42

j) **Tableau des résultats de marge libre et marge totale**

DUREES	MARGE LIBRE	MARGE TOTALE	OBSERVATION
a	0	0	Critique
b	0	0	Critique
c	0	0	Critique
d	0	0	Critique
e	0	2	Non critique
e'	2	2	Critique
f	0	0	Critique
g	0	0	Critique

K) **Présentation des résultats**

- La durée globale du projet est de 45 jours
- Le coût total du projet est calculé comme suit,
  Calcule : CT = 500 + 1.200 + 2.300 + 54.431 + 2.000 + 1.000 = 61.431$

III.3. **Conclusion partielle**

Tout projet est censé être fait avec soin dans le but de réaliser une bonne mise en œuvre. Dans ce chapitre, nous avons spécifié les différents procédés et démarches à suivre pour concrétiser le projet en se basant sur le réseau existant de l'entreprise.

CHAPITRE IV : **MISE EN ŒUVRE DE L'INTERCONNEXION DES SITES DISTANTS VIA LE VPN**

IV.1. **Introduction**

Dans cet ultime chapitre, nous allons expliquer le processus à suivre pour interconnecter les sites distants de l'Institut supérieure de contrôle par un réseau privé virtuel.

Pour y parvenir, il est nécessaire de faire intervenir certains matériels, logiciels, etc...

IV.2. **Intranet multi-site**

Un Intranet multi sites est un ensemble des réseaux dispersés ou éparpillés dans différents sites appartenant à une même entreprise.

IV.3. **Interconnexion des LANs**

Ce serveur aura la tâche de gérer et d'administrer les différents sites de l'Institution et de faire valoir l'ordre dans ce système.

IV.3.1. **Choix de la technologie**

Nous avons choisi la technologie VPN d'Intranet, car ce dernier permet de relier au moins deux intranets de l'Institution supérieure de contrôle entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données[20]. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...).

[20] *Claude SERVIN, Réseaux télécoms, 4éme Edition, Paris, 2013, p.338.*

IV.3.2. **Maquette**

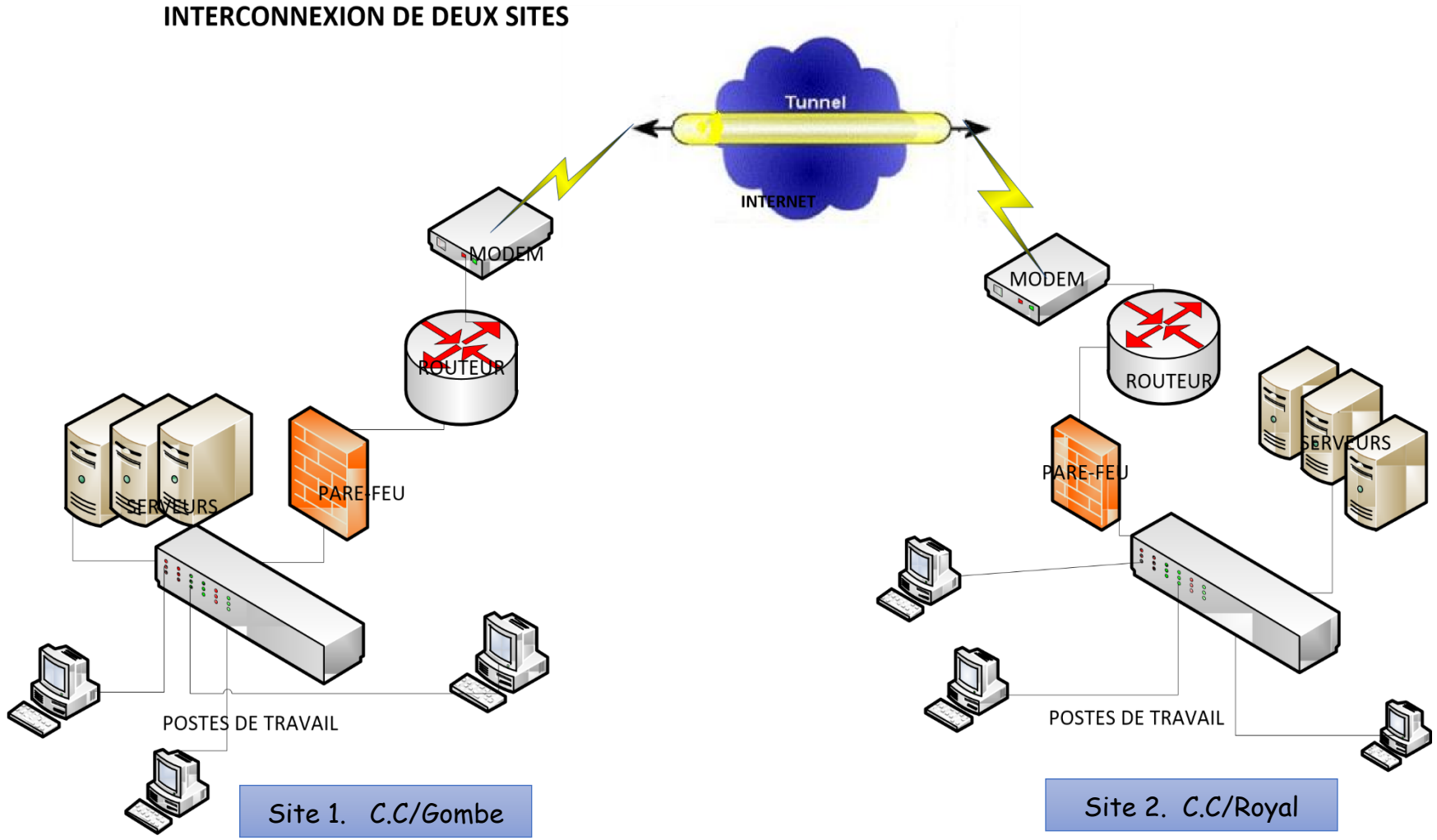


Fig INTERCONNEXION DE DEUX SITES

IV.3.3. **Choix de fournisseur d'accès internet**

Nous avons porté notre choix sur le fournisseur d'accès Internet Standard télécom.

A) Caractéristiques de la connexion Internet

Débit 512 Kbit/s : c'est le débit qui permet la connexion VPN du site/Gombe et du site/Royal de la Cour des comptes.

B) Matériels

Pour la connexion dédiée VPN, certains matériels sont fournis par Standard télécom tels que :

Routeur CISCO 892, avec ce type de routeur on n'a pas besoin du modem sur la ligne car il est incorporé dans le routeur en option.

Comme les sites de l'Institut supérieur de contrôle disposent maintenant d'un réseau informatique et la connexion Internet, passons à la configuration.

C) Présentation de résultats

Interface (Cisco Packet)

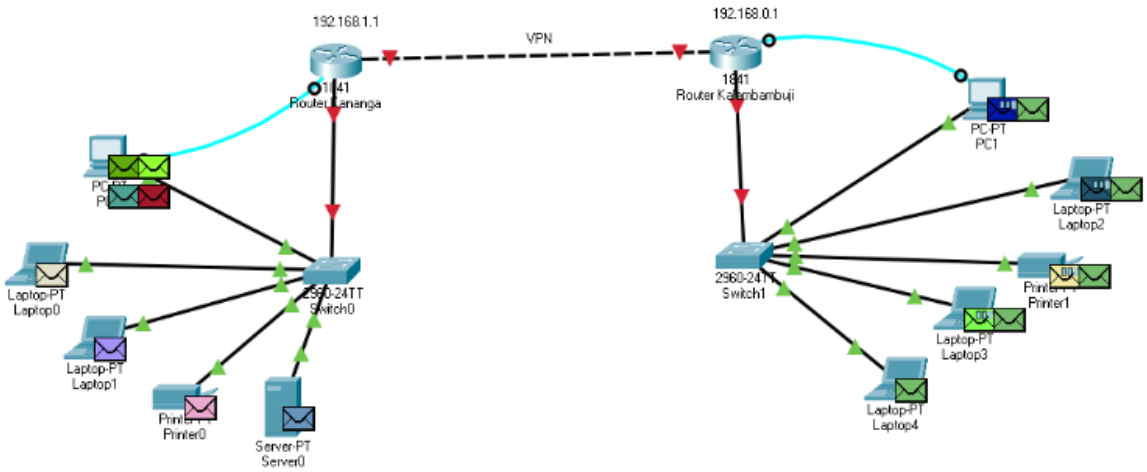


Fig. Interface Cisco Packet

D) Commande de configuration du routeur de deux sites

Principe de mise en place du tunnel VPN

La mise en place du tunnel VPN peut paraître complexe, mais il s'agit plutôt d'une tâche qui demande beaucoup de rigueur.

En effet, il va falloir s'assurer qu'aux deux bouts du tunnel la configuration des différents paramètres soit identique. Voici le détail de la configuration sur SITE1 :

Activation de ISAKMP (le protocole qui gère l'échange des clés,etc.)

SITE1 (config)# crypto isakmpenable

Création d'une stratégie de négociation des clés et d'établissement de la liaison VPN :

SITE1(config)# crypto isakmp policy 10

SITE1(config-isakmp)# encryption aes

SITE1(config-isakmp)# authentication pre-share SITE1(config-isakmp)# hash sha

SITE1(config-isakmp)# group 2

SITE1(config-isakmp)# lifetime 86400

On crée donc ici une stratégie avec un numéro de séquence 10. Ce numéro indique la priorité de l'utilisation de la stratégie. Plus petit est ce nombre plus la priorité est grande. On définit ensuite les paramètres :

- Encryptage AES
- Authentification par clé pré-partagées
- Algorithme de hachage SHA (valeur par défaut)

Méthode de distribution des clés partagées DH-2 (Algorithme de clé asymétriques Diffie-Hellman1024bits)

Durée de vie 86400 secondes (valeur par défaut)

On définit ensuite si on identifie le routeur par son adresse ou par son hostname (ici l'adresse), l'identification par hostname peut être utile si on fonctionne avec une adresse publique dynamique, ce qui permet d'éviter trop de modifications de configuration en cas de changement d'adresse.

SITE1 (config)# crypto isakmp identity address

On crée ensuite la clé pré-partagée, ici « CiscoLab » qu'on associe avec l'adresse de l'autre bout du tunnel donc 80.2.0.2

SITE1 (config) # crypto isakmp key 0 CiscoLab address 80.2.0.2

Le 0 indiquent qu'on définit la clé en texte clair, en opposition avec une clé déjà cryptée si on la copie d'un « show run » d'un routeur ou l'encryptage des mots de passe sont activé.

On a maintenant terminé la configuration de la partie qui gère la négociation des clés etc. La deuxième partie consiste à définir comment les données seront cryptées. Tout d'abord on crée la méthode de cryptage (transform-set) que l'on nomme VPNSET.

SITE1 (config)# crypto ipsectransform-set VPNSET esp-aes esp-sha-hmac.

Esp-aes est la méthode de cryptage, esp-sha-hmac est la méthode d'authentification. On définit ensuite la durée de vie de la clé de cryptage :

SITE1 (config) # crypto ipsec security-association lifetime kilobytes 4096

La durée de vie est ici limitée par un volume en kilobytes (4096), on peut également définir une durée de vie en secondes (ex:cryptoipsecsecurity-association lifetime seconds 3600).

Il faut maintenant créer une accès-list qui servira à identifier le traffic à traiter par le tunnel VPN. Pour SITE1, ce sera letraffic originaire de 192.168.1.1/24 à destination de 192.168.1.10/24. (Ce sera l'inverse pour SITE2). On crée donc une access-list étendue:

(SITE1(config)# ip access-list extended VPN

" SITE1 (config-ext-nacl)# permit ip 192.168.1.1 0.0.0.255 192.168.0.1 0.0.0.192

Reste maintenant à créer une Crypto-map dont le but est de rassembler les différents éléments configurés pour pouvoir les appliquer enfin à une interface.

" SITE1 (config)# crypto map VPNMAP 10 ipsec-isakmp

(SITE1(config-crypto-map)# match address VPN

(SITE1(config-crypto-map)# set peer 80.2.0.2

(SITE1(config-crypto-map)# set transform-set VPNSET

On a donc créé ici une Crypto-map nommée VPNMAP dans laquelle on intègre une séquence 10 (une seule crypto-map par interface, mais on peut ajouter plusieurs maps en leur indiquant des numéros de séquence différents), avec les paramètres suivants:

Activée pour le trafic correspondant à l'access-list VPN Destination du tunnel 80.2.0.2

Cryptage selon le transform-set VPNSET

La dernière étape consiste à appliquer cette cryptomap à l'interface WAN de SITE1.

(SITE1 (config)# interface serial 0/0

(SITE1(config-if)# crypto map VPNMAP

(SITE est prêt. Reste à faire l'équivalent sur SITE2. "

Parmi les points important, SITE2 soit avoir une stratégie isakmp identique à celle de SITE1 et l'access-list qui identifie le trafic à traiter par le tunnel VPN est inversée d'un point de vue de la source et de la destination.

(SITE2 (config)# crypto isakmp enable

(SITE2(config)# crypto isakmp policy 10

(SITE2 (config-isakmp)# encryption aes

(SITE2(config-isakmp)# authentication pre-share

(SITE2 (config-isakmp)# hash sha

(SITE2 (config-isakmp)# group 2

(SITE2 (config-isakmp)# lifetime 86400

(SITE2(config)# crypto isakmp identity address

(SITE2(config)# crypto isakmp key 0 CiscoLab address 80.1.0.2

(SITE2 (config)# crypto ipsec transform-set VPNSET esp-aesespsha-hmac

(SITE2(config)# crypto ipsec security-association lifetime kilobytes 4096

" SITE2(config)# ip access-list extended VPN

" SITE2(config-ext-nacl)# permit ip 192.168.0.1.255 192.168.1.1 0.0.0.255

" SITE2 (config)# crypto map VPNMAP 10 ipsec-isakmp

" SITE2(config-crypto-map)# match address VPN

" SITE2(config-crypto-map)# set peer 80.1.0.2

" SITE2(config-crypto-map)# set transform-set VPNSET

" SITE2 (config)# interface serial 0/0

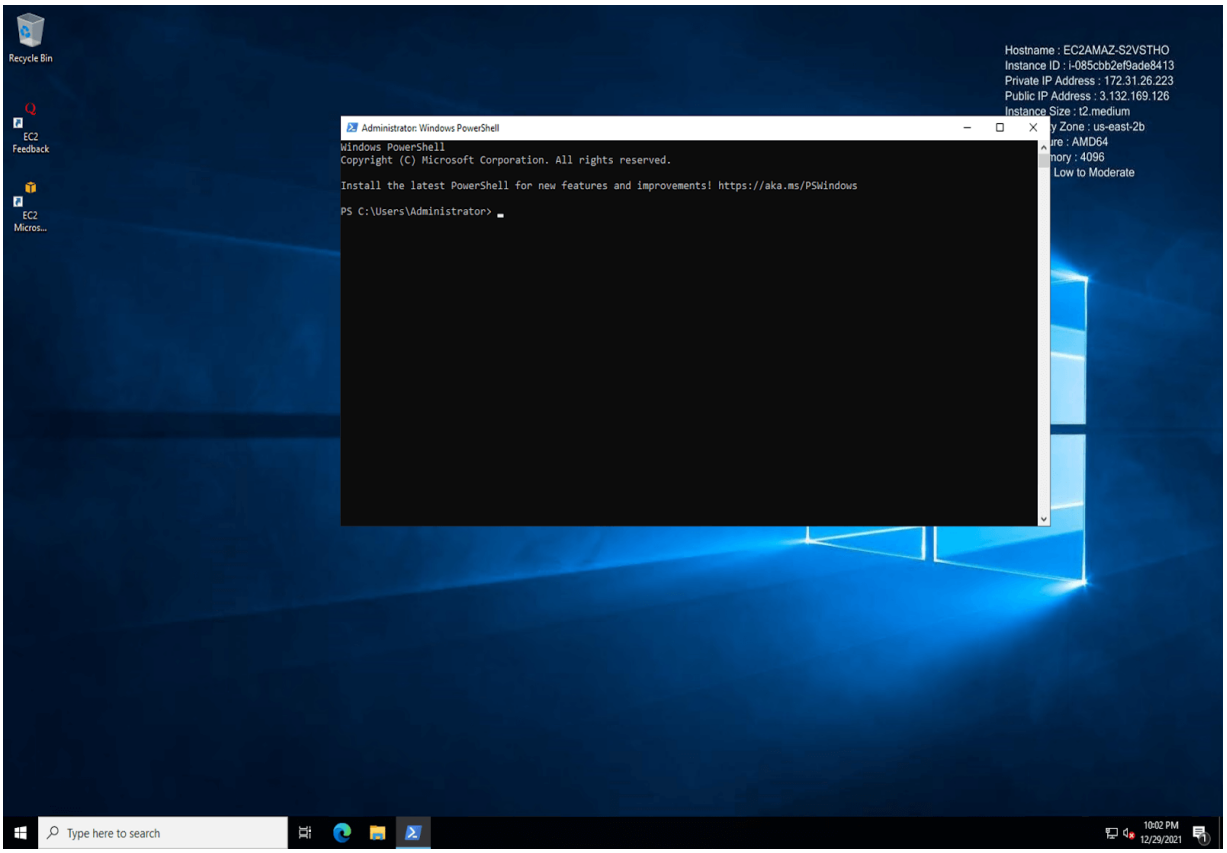
" SITE2(config-if)# crypto map VPNMAP

IV.4. **Installation et configuration du serveur VPN**

Dans notre cas, nous allons utiliser un serveur physique équipé du système d'exploitation « Windows server 2022 » et un client physique, équipé du système d'exploitation Windows 11 professionnel.

Étape 1 : Mettez à jour votre système Windows

Accédez au menu Démarrer et recherchez Windows Powershell. Cliquez avec le bouton droit de la souris sur le résultat de Windows Powershell et cliquez sur Ouvrir en tant qu'administrateur.



Nous allons maintenant installer le module de mise à jour Windows pour Powershell afin de mettre à jour le système. La mise à jour du système vous permet d'éviter tout problème ou vulnérabilité lors de la configuration d'un serveur VPN sur Windows Server 2022. Entrez la commande suivante pour installer le module de mise à jour Windows pour Powershell :

Module d'installation PSWindowsUpdate

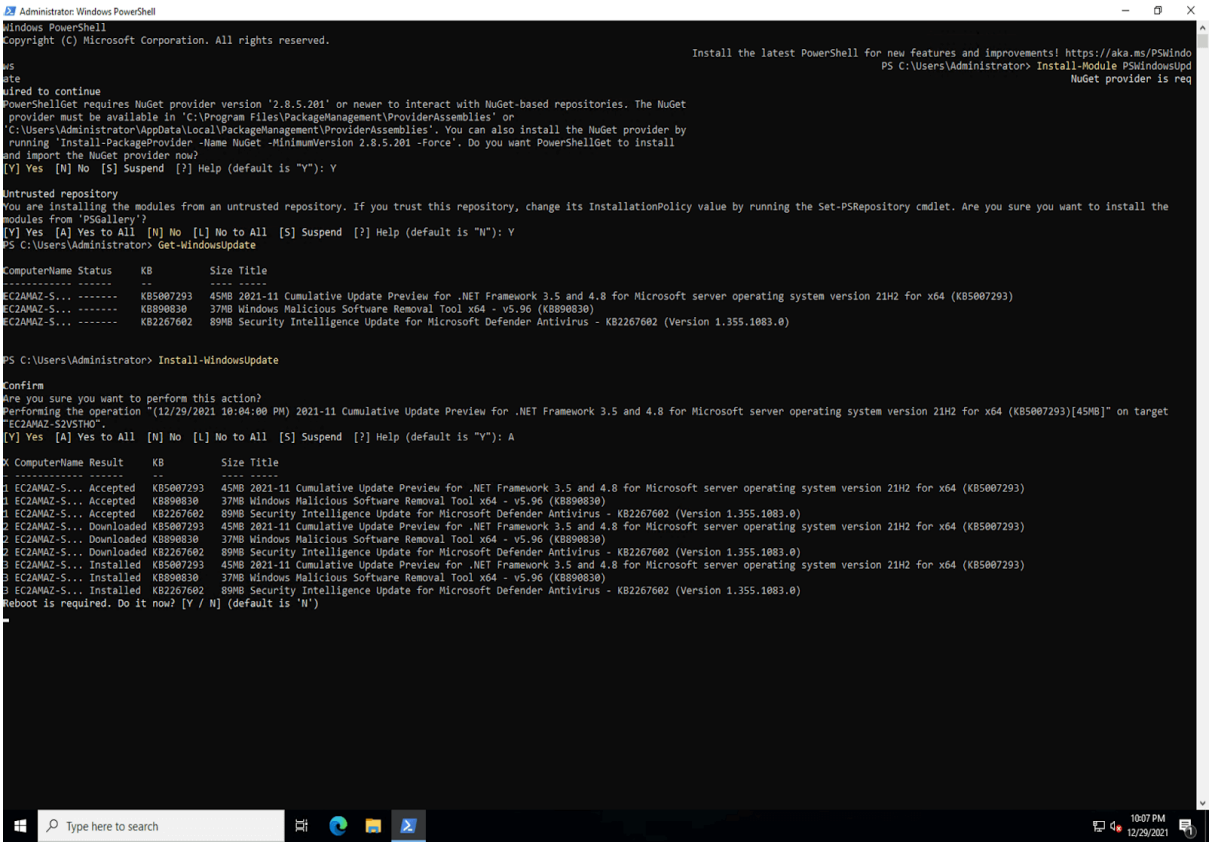
Powershell peut vous demander confirmation. Appuyez sur **Y** et sur Entrée pour confirmer.

Maintenant, entrez la commande suivante pour obtenir la liste des dernières mises à jour :

Obtenir WindowsUpdate

Enfin, installez toutes les dernières mises à jour en exécutant la commande suivante :

Installer-WindowsUpdate



Maintenant que votre serveur Windows 2022 est à jour, il vous sera demandé de redémarrer le système, **appuyez sur Y** ou redémarrez le système.

Étape 2 : installer le rôle d'accès à distance sur votre serveur Windows 2022

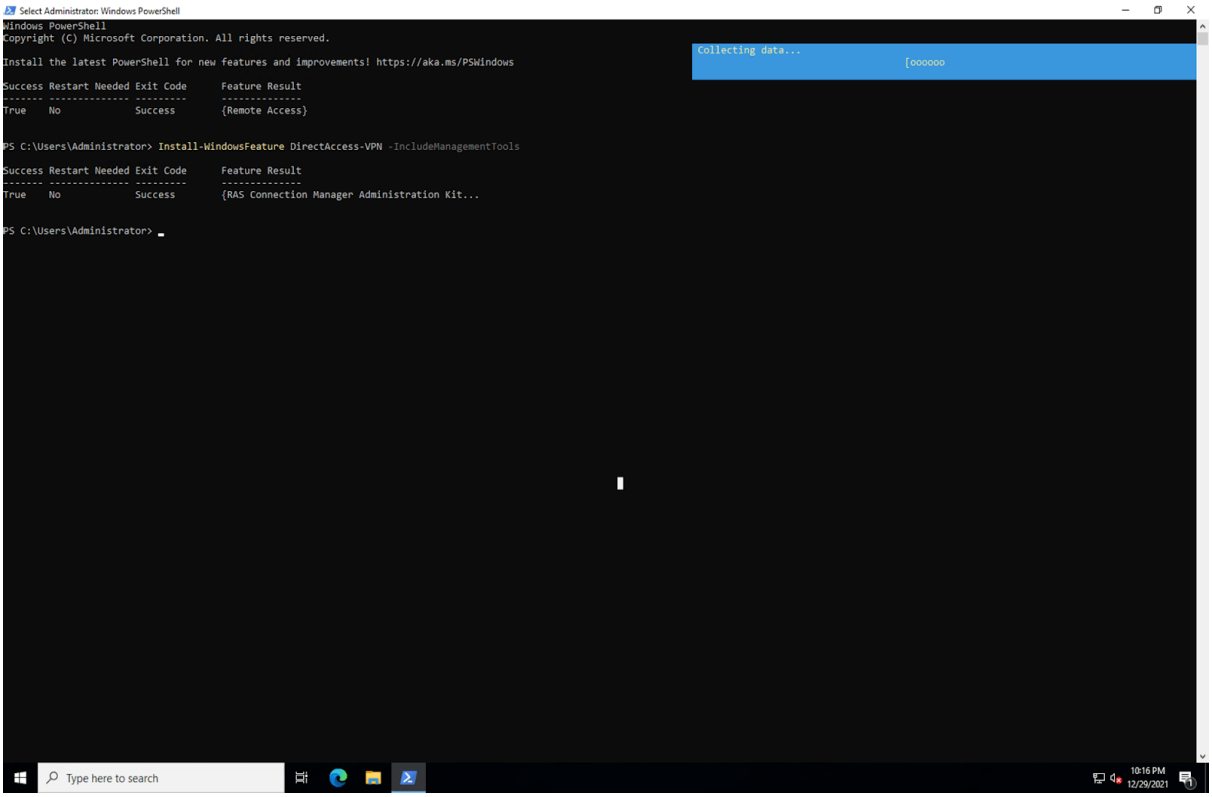
Lancez une nouvelle fenêtre Windows Powershell en mode administratif et entrez les commandes suivantes pour installer les éléments suivants :

- Fonctionnalité d'accès à distance
- Accès direct et VPN (RAS)
- Routage avec outils de gestion.

Installer-WindowsFeature RemoteAccess

Installer-WindowsFeature DirectAccess-VPN -IncludeManagementTools

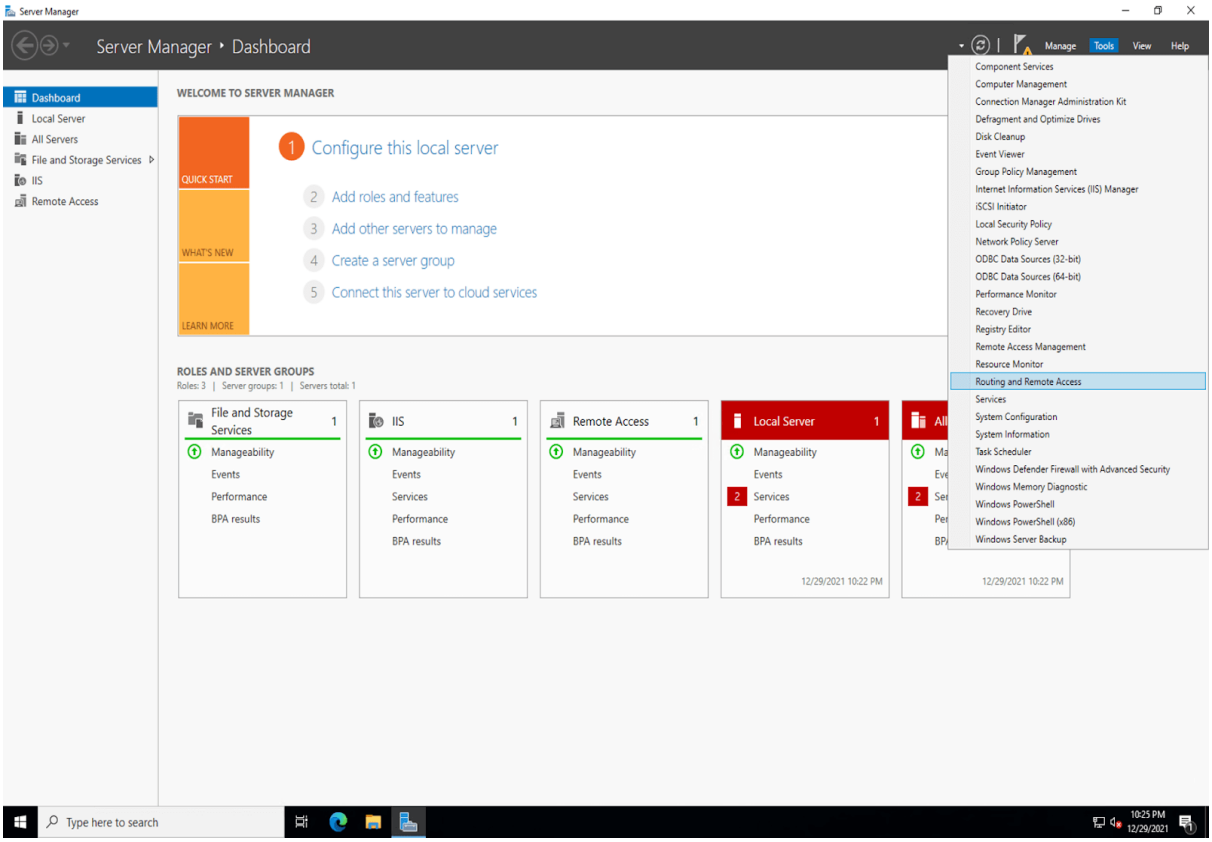
Installer-WindowsFeature Routing -IncludeManagementTools



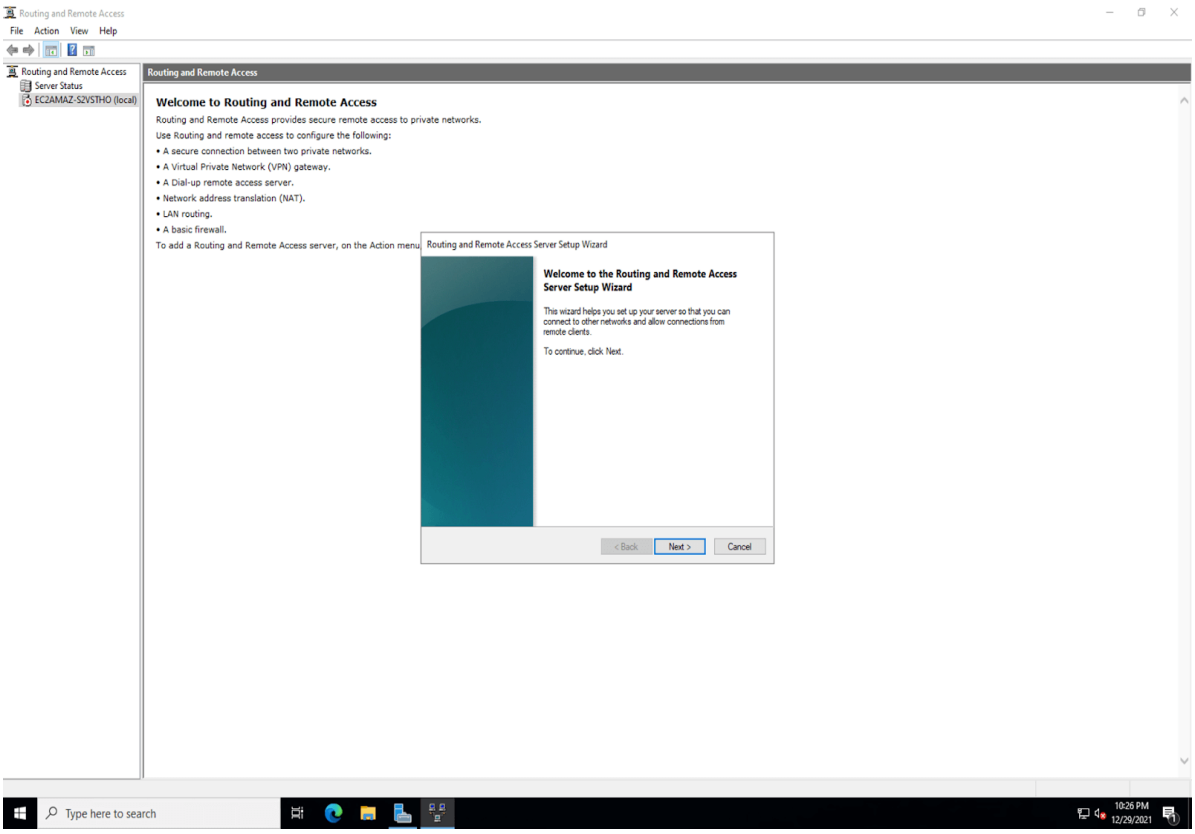
Étape 3 : Configurer le routage et l'accès à distance

Ouvrez le Gestionnaire de serveur Windows via le menu Démarrer.

Accédez à **Routage et accès à distance** à partir du menu déroulant **Outils** dans la navigation.

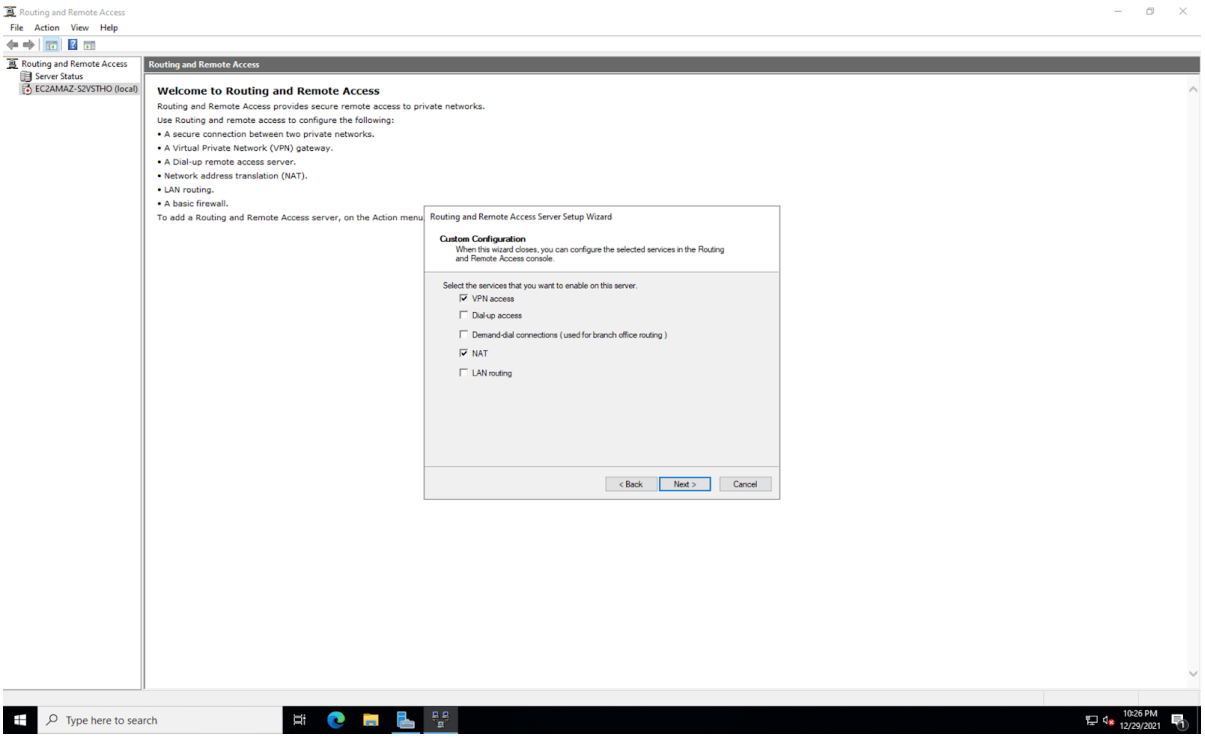


Cliquez avec le bouton droit de la souris sur votre serveur local dans le volet de gauche et cliquez sur l'option « *Configurer et activer le routage et l'accès à distance* ». L'assistant de configuration du serveur de routage et d'accès à distance s'ouvre.

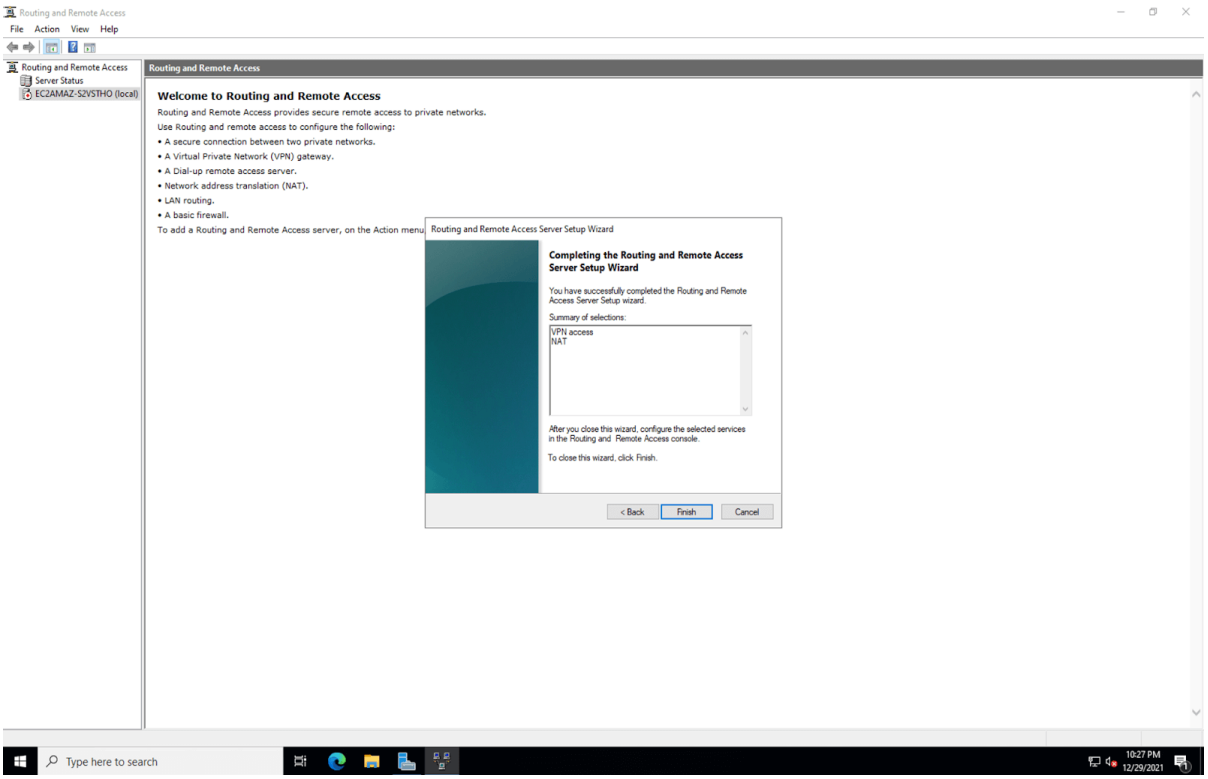


Dans l'assistant de configuration du serveur de routage et d'accès à distance, sélectionnez le bouton radio « **Configuration personnalisée** ». Nous procédons ainsi car nous allons configurer le routage et l'accès manuellement. Cliquez sur Suivant.

Cochez maintenant les cases « **Accès VPN** » et « **NAT** » lorsque l'assistant vous demande les services que vous souhaitez activer sur le serveur. Cliquez sur le bouton Suivant pour voir le résumé de votre sélection.



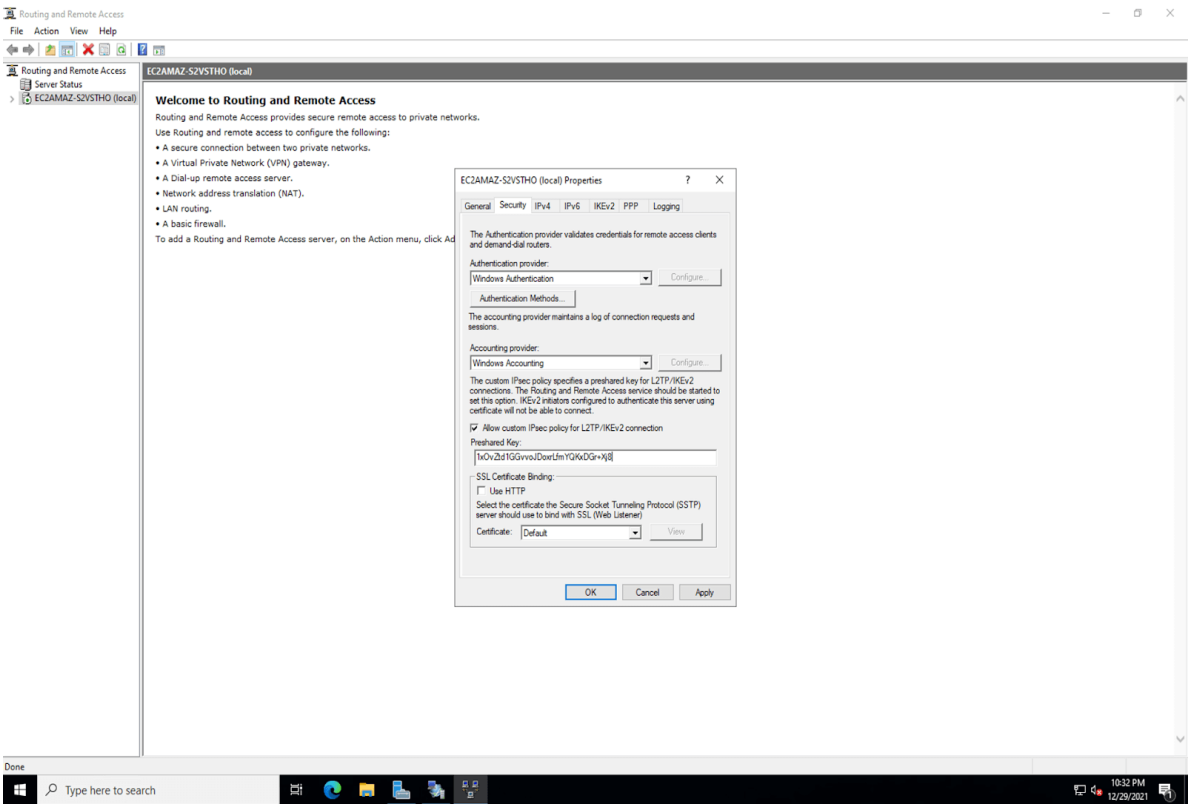
Enfin, après avoir cliqué sur le bouton Terminer, vous verrez une invite indiquant : « *Le service Routage et accès à distance est prêt à être utilisé.* » Exécutez le service en cliquant sur le bouton **Démarrer le service**.



Avant de configurer le routage et l'accès à distance, assurez-vous que votre environnement d'hébergement prend en charge ces configurations. Bien que Windows Server 2022 soit notre priorité, de nombreux fournisseurs d'hébergement Linux proposent également des options pour les configurations de serveur VPN.

Étape 4 : Configurer les propriétés du VPN

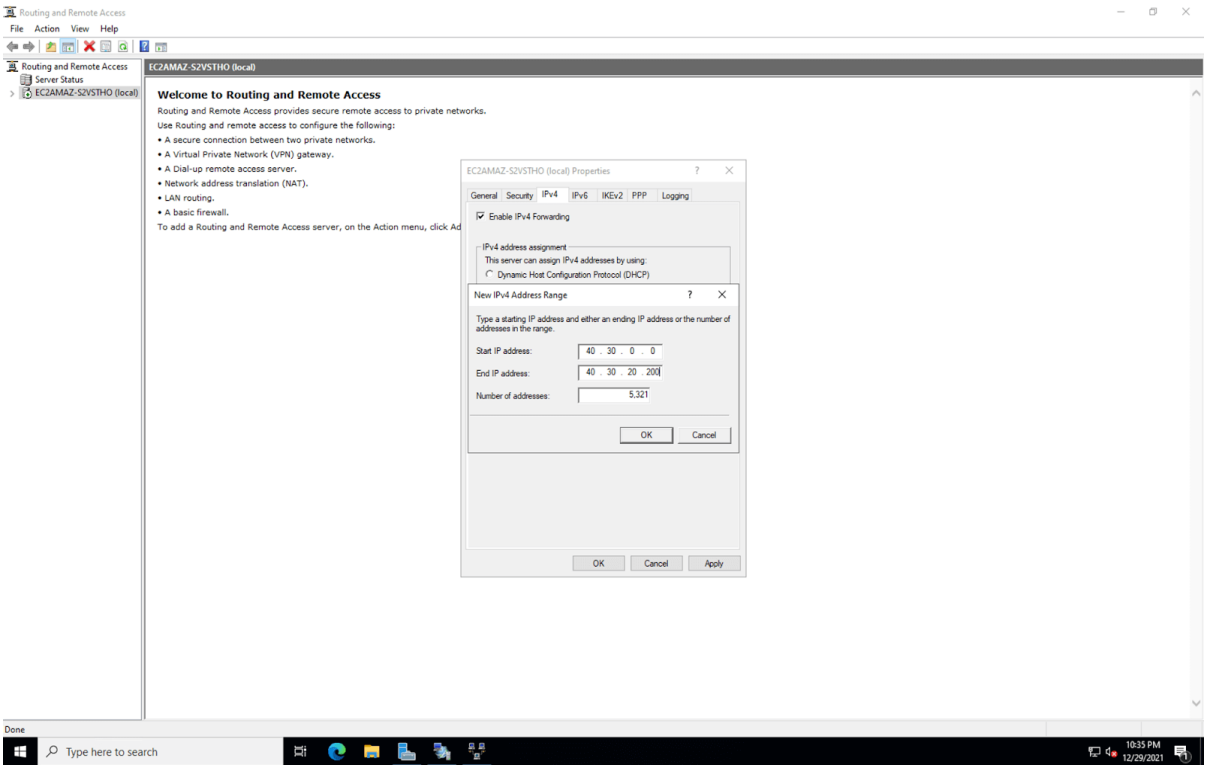
Votre serveur VPN sera exécuté sur votre système après l'étape 3. Il est maintenant temps de le configurer. Cliquez avec le bouton droit sur votre serveur local, sous le volet gauche de la fenêtre Routage et accès à distance, et accédez à « *Propriétés* ».



Accédez à l'onglet Sécurité et cochez la case « *Autoriser la stratégie IPSec personnalisée pour la connexion L2TP/IKEv2* ». Saisissez une clé PSK (clé pré-partagée) très longue en dessous. Vous pouvez générer une clé aléatoire à l'aide de n'importe quel outil. Vous pouvez également utiliser le générateur de clés aléatoires de Google Cloud .

Remarque : assurez-vous de stocker le PSK en toute sécurité avec vous, car il sera nécessaire lorsqu'un utilisateur souhaite se connecter à votre serveur VPN.

Ensuite, accédez à l'onglet IPv4 et sélectionnez le pool d'adresses statiques sous Attribution d'adresses IPv4. Cliquez ensuite sur le bouton « *Ajouter* » et une fenêtre contextuelle s'affichera pour vous permettre de saisir des plages d'adresses IP . Dans la fenêtre contextuelle, saisissez l'adresse de début et l'adresse de fin de la plage d'adresses IP à laquelle vous souhaitez que les utilisateurs attribuent.



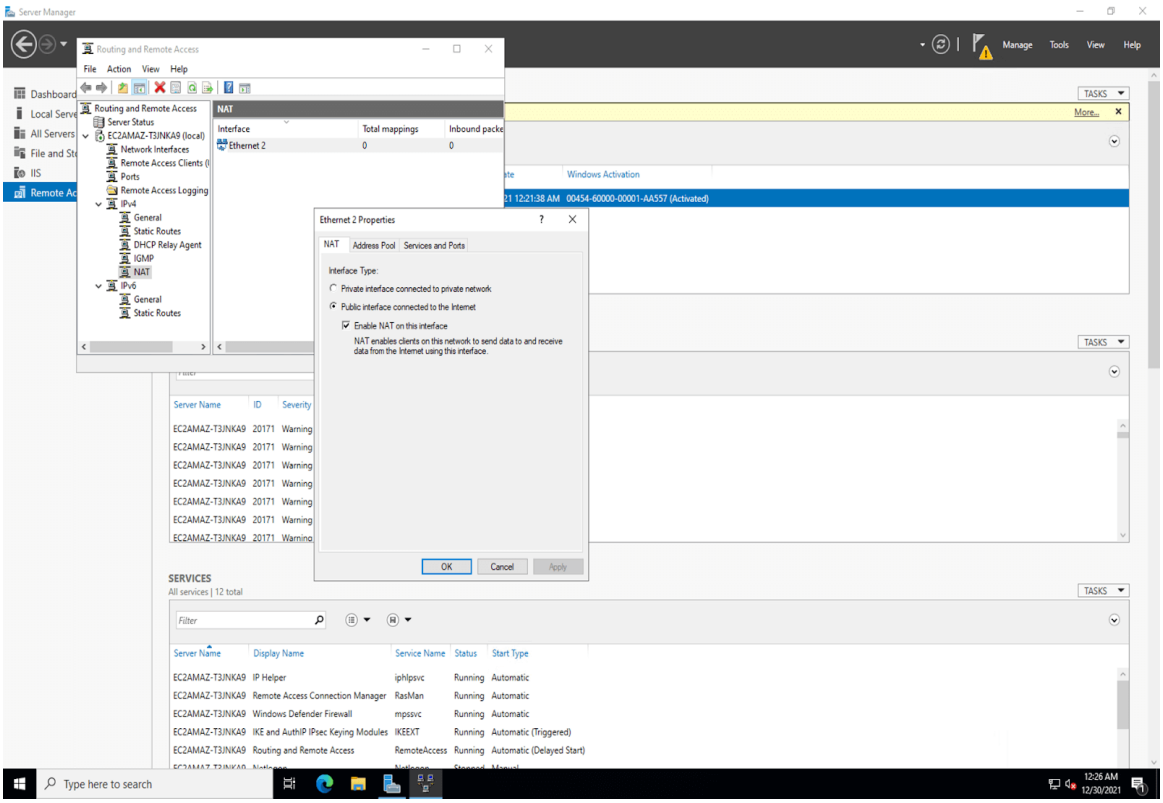
Cliquez sur le bouton **OK** pour enregistrer les plages d'adresses IP, puis cliquez sur le bouton **OK** dans la fenêtre Propriétés. Un message peut s'afficher indiquant que vous devez redémarrer le service Routage et accès à distance pour appliquer les modifications avec succès. Vous pouvez l'ignorer et cliquer sur **OK** , car nous allons de toute façon redémarrer le service après l'étape suivante.

Vous êtes toujours à la recherche d'un hébergeur fiable ? Consultez notre liste des [meilleurs fournisseurs d'hébergement VPS Windows]

Étape 5 : Configuration des propriétés NAT

Votre serveur local est répertorié dans le volet gauche de la fenêtre Routage et accès distant. Développez-le en cliquant sur la flèche à côté ou en double-cliquant dessus. De même, développez IPv4 répertorié sous votre serveur local. Vous y trouverez l'objet NAT. Cliquez avec le bouton droit sur NAT et sélectionnez l'option « *Nouvelle interface* ».

Choisissez « **Ethernet** » et appuyez sur OK pour continuer. Dans l'onglet NAT, cliquez sur le bouton radio « *Interface publique connectée à Internet* » et cochez la case « *Activer NAT sur cette interface* ».



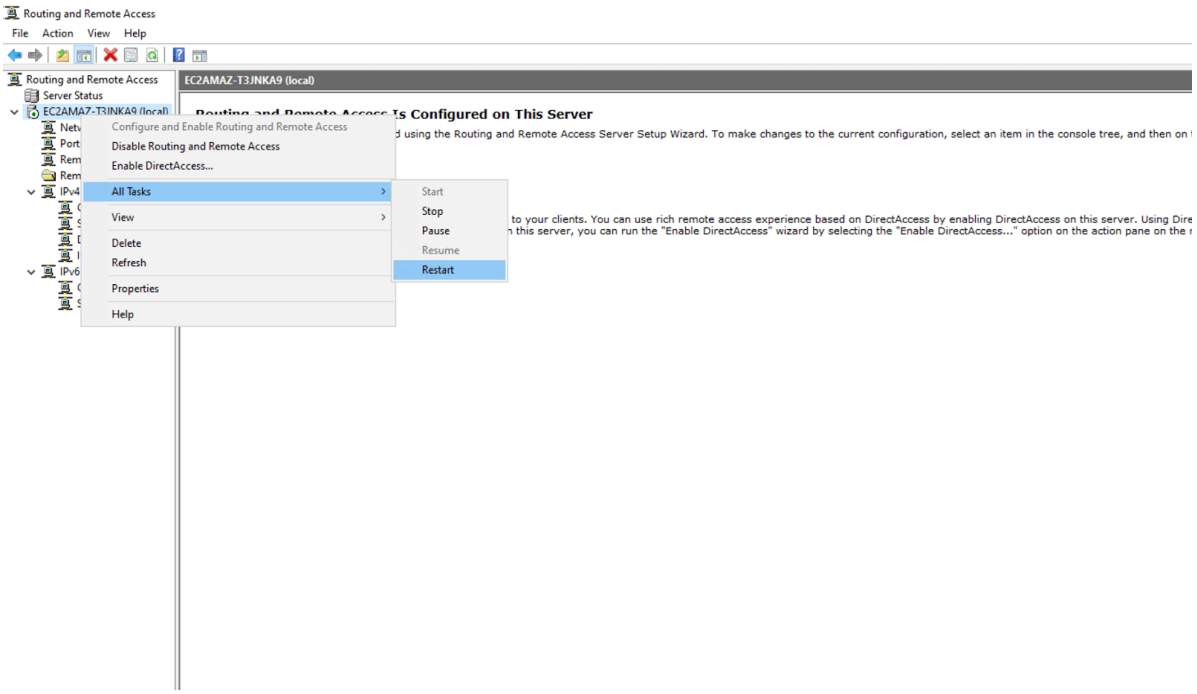
Ensuite, accédez à l'onglet « **Services et ports** » et cochez la case « **Passerelle VPN (L2TP/IPSec - exécutée sur ce serveur)** ». Vous verrez une nouvelle interface pour modifier les paramètres du service.

Maintenant, changez l'adresse privée de **0.0.0.0** à **127.0.0.1** et enregistrez en appuyant sur OK.

Enfin, enregistrez la configuration de l'interface NAT en cliquant sur OK.

Étape 6 : Redémarrer le routage et l'accès à distance

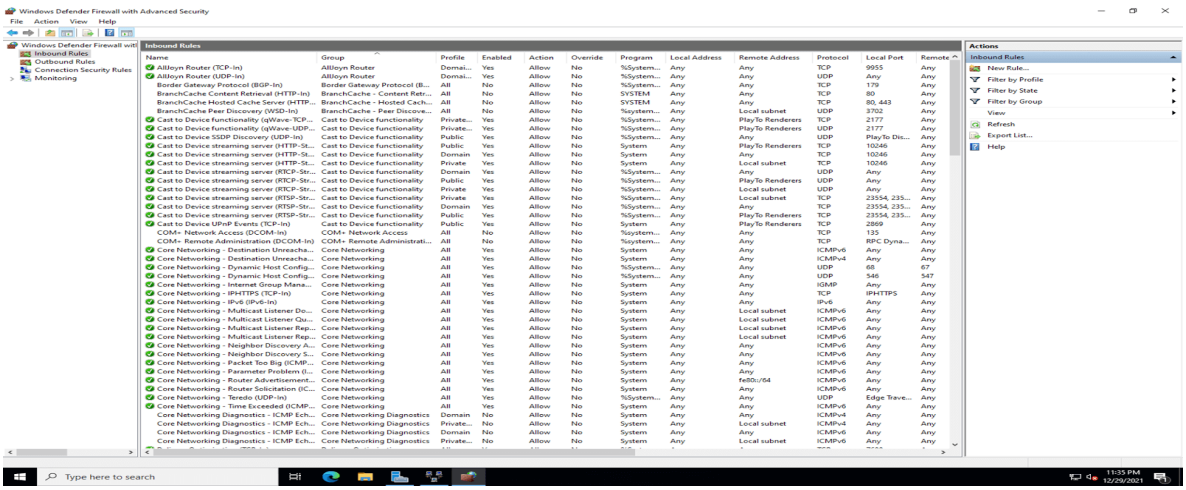
Cliquez avec le bouton droit de la souris sur votre serveur local dans le volet gauche de la fenêtre Routage et accès à distance. Cliquez sur « *Redémarrer* » sous « *Toutes les tâches* ».



Cela redémarrera tous les services et tâches du service Routage et accès à distance. Cela garantira également que nos modifications et configurations ont été appliquées.

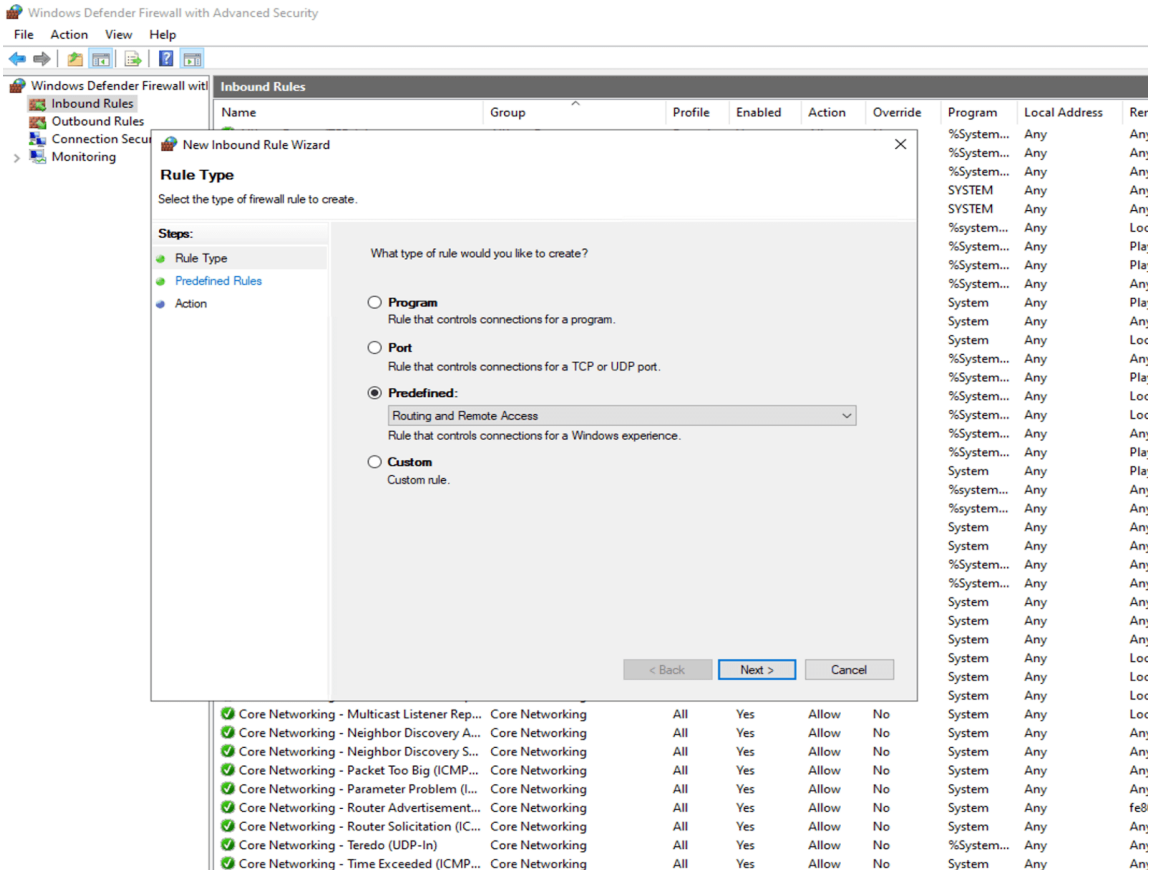
Étape 7 : Configurer le pare-feu Windows

Ouvrez le **pare-feu Windows Defender** via le menu Démarrer et accédez à « **Règles entrantes** ».

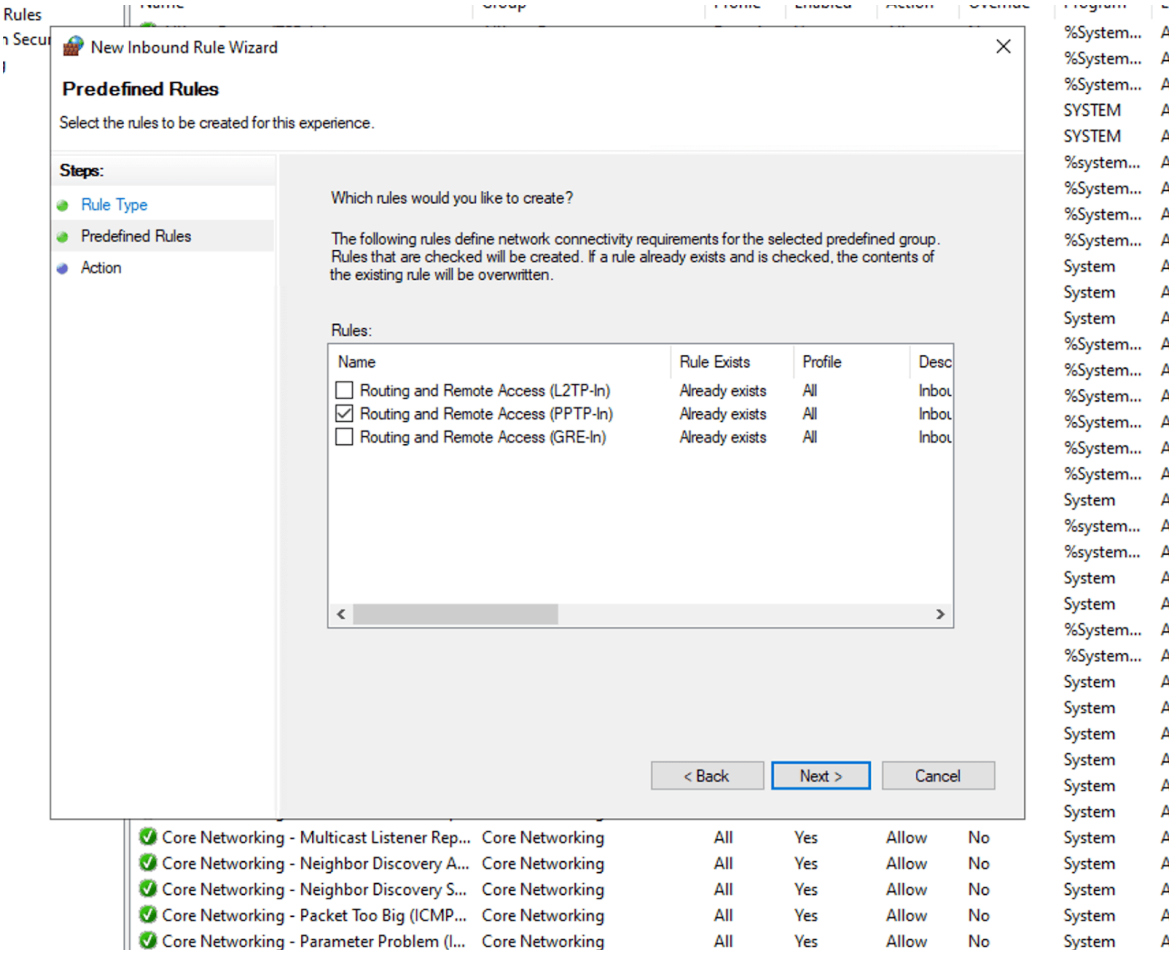


Dans le volet de gauche, sélectionnez « *Règles entrantes* » et dans le volet de droite, sélectionnez « **Nouvelle règle** ». L'assistant de création de nouvelle règle entrante s'ouvre.

Windows Server 2022 dispose déjà de règles prédéfinies pour l'exécution du serveur VPN. Il nous suffit de les activer. Dans l'assistant Nouvelle règle entrante, sélectionnez le bouton radio « *Prédéfini* » et sélectionnez l'option « *Routage et accès à distance* » dans le menu déroulant.



Dans la section « **Règles prédéfinies** », cochez la case « **Routage et accès à distance (L2TP-In)** » et cliquez sur Suivant.

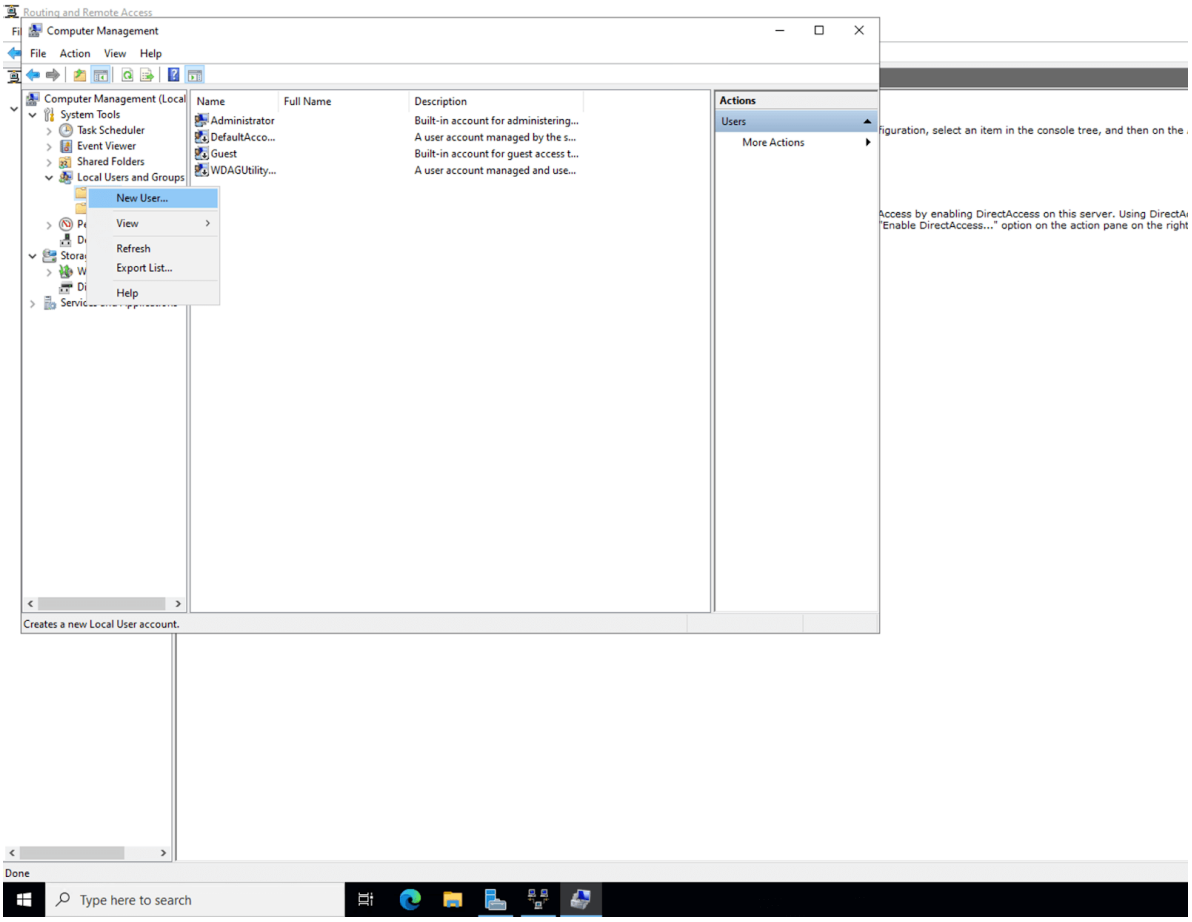


Dans la section « *Action* », sélectionnez l'option « *Autoriser la connexion* » et cliquez sur Terminer.

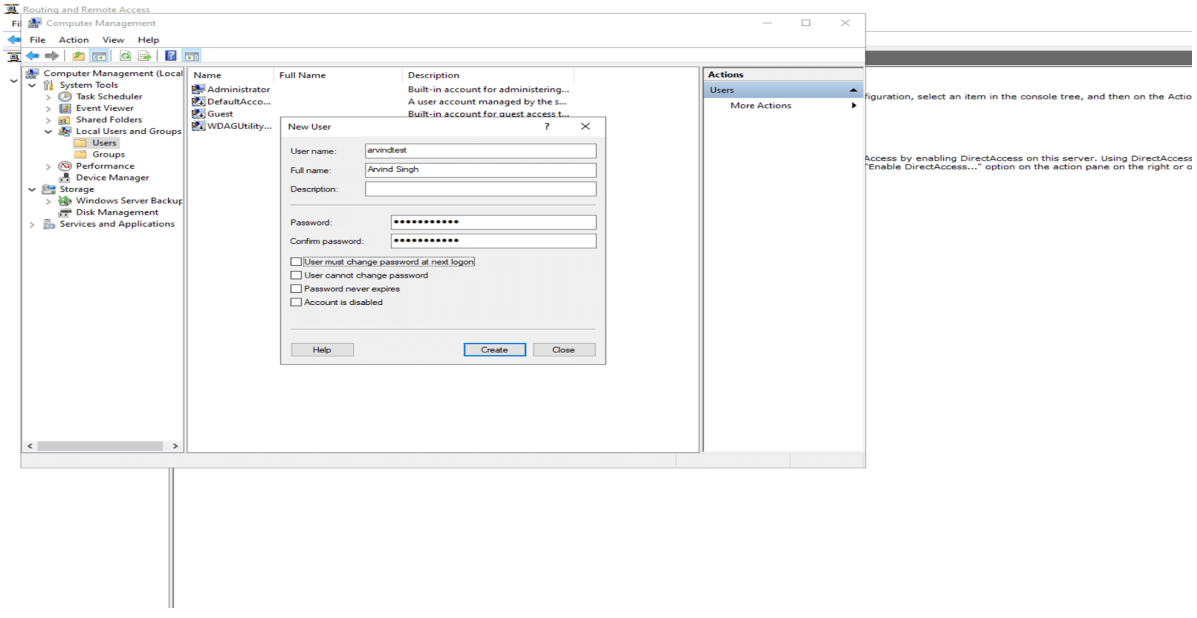
Nous avons configuré avec succès le pare-feu Windows pour autoriser le trafic entrant sur le port UDP 1701.

Étape 8 : Créer un utilisateur VPN

Ouvrez « **Gestion de l'ordinateur** » à partir du menu Démarrer. Vous verrez « **Utilisateurs et groupes locaux** » dans le volet gauche de la fenêtre Gestion de l'ordinateur. Développez-le et faites un clic droit sur « *Utilisateurs* ». Cliquez sur « *Nouveaux utilisateurs* » pour créer un nouvel utilisateur.

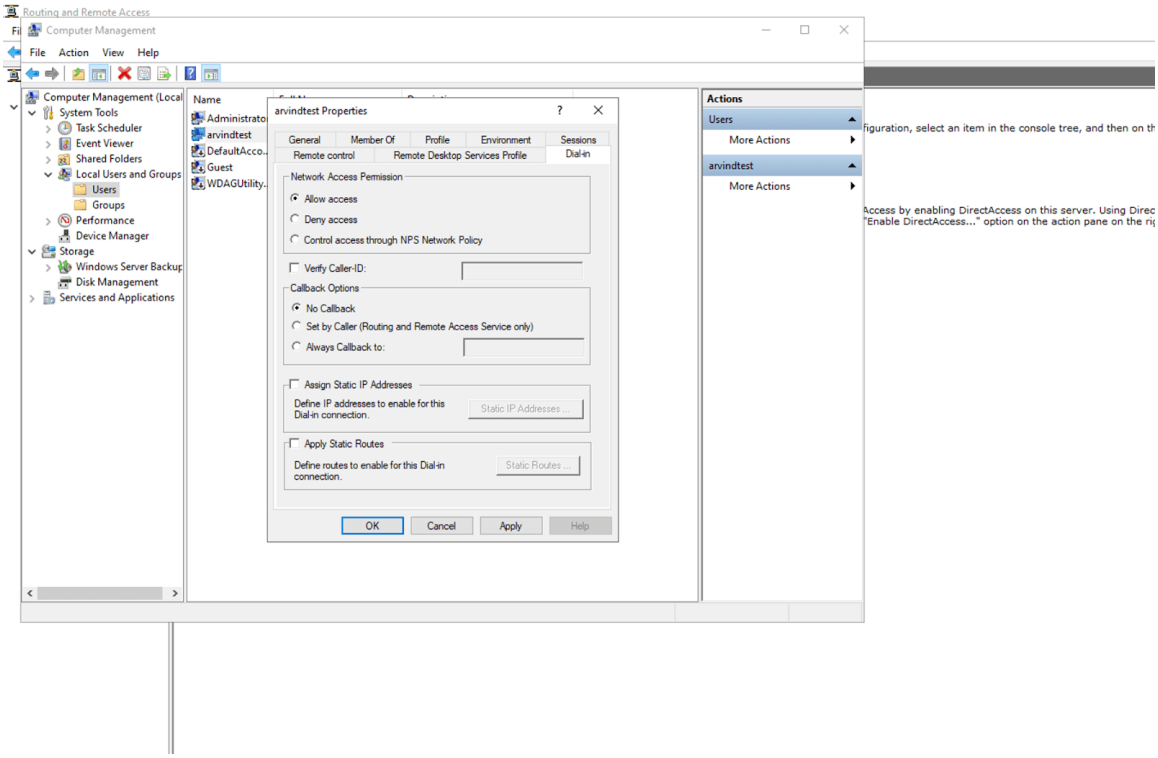


Une invite de dialogue Nouvel utilisateur s'ouvre. Saisissez un nom d'utilisateur, un nom complet et un mot de passe fort dans l'invite Nouvel utilisateur. Décochez la case « **L'utilisateur doit changer le mot de passe lors de la prochaine connexion** ». Cliquez sur Créer pour créer un nouvel utilisateur.



Vous trouverez l'utilisateur nouvellement créé répertorié dans la fenêtre Gestion de l'ordinateur. Cliquez avec le bouton droit de la souris sur l'utilisateur et cliquez sur l'option Propriétés.

Accédez à l'onglet Accès à distance des propriétés de l'utilisateur VPN. Sélectionnez le bouton radio **Autoriser l'accès pour le paramètre Autorisations d'accès au réseau**. Cliquez sur OK pour enregistrer les propriétés.



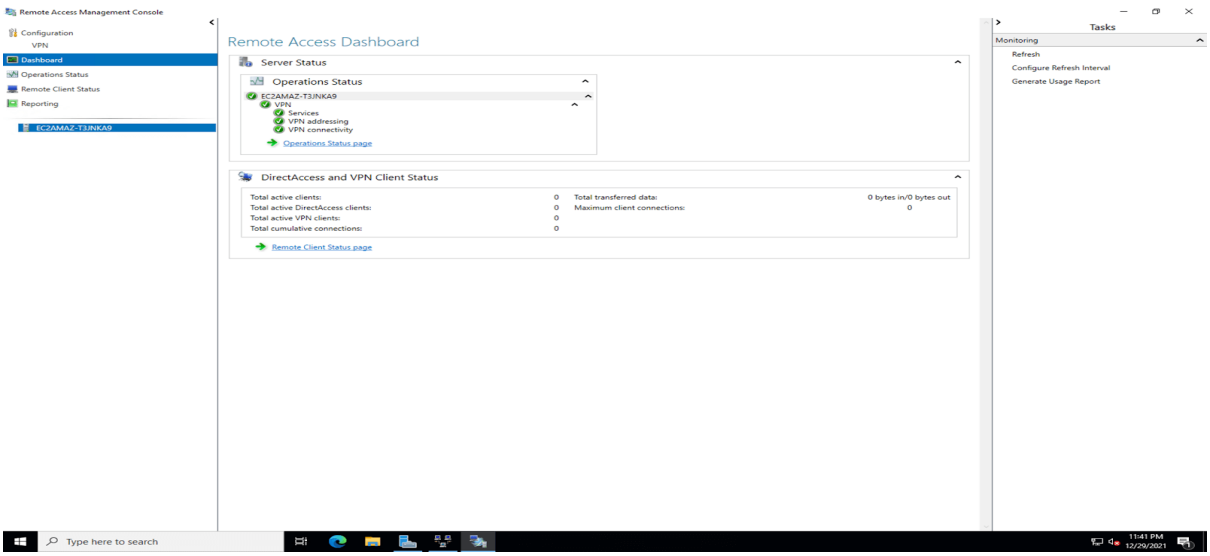
Vous avez configuré avec succès un serveur VPN L2TP/IPSec sur Windows Server 2022 et il est maintenant prêt à accepter les connexions.

Étape 9 : Connexion des clients VPN

Une fois votre serveur VPN correctement configuré, vous pouvez désormais vous connecter facilement au serveur VPN distant avec d'autres appareils. Il vous suffit de partager les informations d'identification PSK et Windows avec les utilisateurs qui souhaitent se connecter au serveur VPN.

Étape 10 : Surveillez votre serveur VPN

Ouvrez la console de gestion de l'accès à distance en la recherchant dans le menu Démarrer. Dans la console, vous devriez pouvoir voir l'état de votre serveur VPN dans le tableau de bord. Si vous avez installé le serveur VPN sur votre Windows Server 2022 avec succès en suivant le didacticiel, vous verrez une coche verte sur tous les services. La console de gestion de l'accès à distance peut également être utilisée pour voir les détails des clients connectés.



IV.5. **Conclusion partielle**

Dans ce chapitre, nous venons d'expliquer d'une manière claire et simple le processus de la mise en place d'une interconnexion des sites distants à travers la technologie VPN.

Nous avons montré comment la configuration de notre VPN se feras via la maquette et l'interface Cisco, et on a passé à la configuration du serveur physique équipé du système d'exploitation Windows Serveur 2022 et à un client physique, équipé du système d'exploitation Windows 11 professionnel.

CONCLUSION GENERALE

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats obtenus lors de l'implémentation d'un système d'interconnexion des sites distants de l'Institution Supérieur de Contrôle via le réseau privé virtuel. Nous avons en effet grâce à cette nouvelle technologie permis aux employés de partager de façon sécurisée leurs données via le protocole IPSec qui est le principal outil permettant d'implémenter les VPN, ce partage était possible en interne pour les utilisateurs du réseau local de l'institution, mais aussi en externe pour les utilisateurs dit « distants » situés en dehors du réseau local.

En effet, nous avons présenté un travail divisé en deux parties, à savoir l'approche théorique qui est subdivisé en deux chapitres dont le premier a porté sur les généralités sur le VPN, dans ce premier chapitre, nous avons brosser les notions et informations trouvées et jugées importantes et essentielles sur le VPN (Virtual Private Network) où nous avons effectué une étude présentative, descriptive, analytique et fonctionnelle sur le concept VPN, qui est un acronyme de Virtual Private Network.

Le second a porté sur l'étude de l'existant, dans lequel nous avons présenté l'institution et nous avons fait l'analyse de l'existant, critique de l'existant et proposé une solution VPN site-à-site qui consiste à mettre en place une liaison permanente, distante et sécurisée entre deux ou plusieurs sites de l'institution.

Et la deuxième partie intitulée approche pratique qui était aussi subdivisé en deux chapitres dont le premier a porté sur le Planning prévisionnel de réalisation du projet, le second et le dernier a porté sur l'interconnexion des sites distants via VPN, dans ce dernier chapitre, nous avons expliqué d'une manière claire et simple le processus de la mise en place d'une interconnexion des sites distants de l'institution supérieur de contrôle à travers la technologie VPN.

Nous avons montré comment la configuration de notre VPN se feras via la maquette et l'interface Cisco, et on a passé à la configuration du serveur physique équipé du système d'exploitation Windows Serveur 2022 et à un client physique, équipé du système d'exploitation Windows 11 professionnel.

En effet, la mise en place de VPN site-à-site permet aux réseaux privés de s'étendre et de se relier entre eux au travers l'internet. Cette solution mise en place est une politique de réduction des couts liés à l'infrastructure réseau des entreprises. Il en ressort que la technologie VPN basé sur le protocole IPSec est l'un des facteurs clés de succès qui évolue et ne doit pas aller en marge des infrastructures réseaux sécurisés et du système d'information qui progressent de façon exponentielle.

En tout état de cause, dans le cadre d'un accès restreint et plus sécurisé à l'internet, nous pourrons nous retourner sur le VPN ou le cryptage du réseau.

En définitive, comme tout travail scientifique, nous n'avons pas la prétention de réaliser un travail sans critique et suggestion de la part de tout lecteur afin de le rendre meilleur.

BIBLIOGRAPHIE

1. **Ouvrages**

1) Stéphane LOHIER, préface de Guy PUJOLLE : Transmission et Réseaux, 4éEd DUNOD, paris, 2020, p.235-253.

2) Clade SERVIN, Réseau et télécom, 4éme ed DUNOD, Paris, 2021, p. 581.

3) Dictionnaire Français version 2011.

4) Claude SERVIN, Réseaux télécoms, 4éme Edition, Paris, 2013, p.338.

2. **Sites Webs**

1) http://www.guill.net/reseaux/Vpn.html.

2) http://www.intranet/vpn/.com.

3) https://www.cisco.com/c/fr_ca/solutions/smallbusiness/resource-center/networking/how-to-set-up-router.html,Consulté le 22 août 2024 à 12h : 22.

3. **Statut**

1) Constitution RDC, art.178.

2) Loi organique n°18/024 du 13 novembre 2018 portant composition, organisation et fonctionnement de la Cour des comptes.

4. **Notes de cours**

1) Prof. Lepère MAKUMOLE, Cours Méthodes de recherche scientifique, G2 Gestion informatique/WUB,2022.

2) Prof Denis BOTA Cours Réseaux mobile télécom L2 télécom /UWB,2024.

3) Prof. KUTANGILA MAYOYA, Cours Projet informatique, L1 Telecom/WUB,2022 4) IVINZA LEPAPAA.C, Notes de cours de télématique II, L2 Info de gestion, ISC-Gombe, Kinshasa, 2011-2012.

TABLE DES MATIERES