Université SÂAD DAHLAB, Blida-1-

Faculté de Sciences

Département des Énergies Renouvelables

Par : ISMAIL Abdelhafid

Pour l'obtention du diplôme :

MASTER en INFORMATIQUE

Option : Sécurité des systèmes d'informations

Thème :

ÉTUDE ET MISE EN PLACE D'UNE SOLUTION VPN POUR LE E-LEARNING ET LE TELETRAVAIL

Soutenu devant le jury composé par :

Madame	BEY	FELLA	USDB	Président
Madame	BOUSTIA	NARHIMENE	USDB	Promoteur
Monsieur	BENYAHIA	MOHAMED	USDB	Examinateur

Année Universitaire : 2020/2021

Résumé

La période sensible de l'épidémie de Covid-19 a imposé la nécessité de poursuivre les études et de travailler à distance dans certains établissements et entreprises, via des plateformes de e-learning pour l'enseignement à distance, ou d'accès à distance pour les télétravailleurs, dont la connexion se fait via l'internet ouvert, ce qui rend divers systèmes d'information vulnérables aux différents risques. Il est donc nécessaire d'assurer une connexion sûre et une qualité acceptable, qui ne soit pas affectée par diverses perturbations externes.

Ce travail vise à étudier la technologie VPN comme une solution pour assurer une communication sécurisée pour les enseignants et les étudiants nomades dans l'enseignement à distance, ainsi pour les télétravailleurs et l'interconnexion entre les différentes branches des entreprises dans le télétravail. La mise en œuvre se base sur la solution VPN site à site qui permet l'interconnexion entre les différents sites d'une entreprise via le protocole IPSec en mode tunnel, qui est le plus à répondu, et devenu un standard pour VPN, fournissant les services de sécurité comme la confidentialité, l'intégrité, l'authentification mutuelle et le contrôle d'accès. D'autre part, la solution VPN d'accès distant pour la connexion des télétravailleurs vers ses entreprises, ainsi des enseignants et étudiants nomades vers les e-learning, en s'appuyant sur les avantages d'EzVPN qui fournit les services d'authentification et la garantie de tunnels sûrs.

Mots clés :

VPN, Site à site, IPSec, Tunnel, Services de sécurité, Accès à distance, EzVPN.

ملخص

فرضت الفترة الحساسة لوباء Covid-19 الحاجة إلى مواصلة الدراسات والعمل عن بعد في مؤسسات وشركات معينة عبر منصات التعلم الإلكتروني (e-learning) للتعليم عن بعد، أو تطبيقات وبرامج الوصول عن بُعد للعاملين المتنقلين، بحيث يتم الاتصال عبر الإنترنت، مما يجعل أنظمة المعلومات المختلفة عرضة للعديد من المخاطر، لذلك من الضروري ضمان اتصال آمن وجودة مقبولة لا تتأثر بالاضطرابات الخارجية المختلفة.

يهدف هذا العمل إلى دراسة تقنية VPN كحل لضمان الاتصال الآمن للمعلمين والطلاب بمنصات التعلم الإلكتروني، وكذلك الأمر بالنسبة للعاملين المتنقلين عند تواصلهم البعدي ببيئة العمل الخاصة بهم، ومن ثمة تنفيذ هذه التقنية استنادًا إلى حل VPN من موقع إلى موقع والذي يسمح بالترابط بين المواقع المختلفة للشركة عبر بروتوكول IPSec في وضع النفق، وهو الأكثر إجابة والذي أصبح معيارًا لـ VPN، مما يوفر خدمات الأمان مثل السرية والنزاهة والمصادقة المتبادلة والتحكم في الوصول. من ناحية أخرى، حل VPN للوصول عن بعد لربط العاملين عن بعد بشركاتهم، وكذلك المدرسين والطلاب بمنصات التعلم الإلكتروني، بناءً على مزايا EzVPN التي توفر خدمات المصادقة، وضمان الأنفاق الآمنة.

الكلمات المفتاحية :

تقنية VPN، موقع إلى موقع، بروتوكول IPSec، وضع النفق، خدمات الأمان، الوصول عن بعد، EzVPN.

Abstract

The sensitive period of the Covid-19 epidemic has imposed the need to continue studies and work remotely in some institutions and companies, with e-learning platforms for distance education, or remote access applications for teleworkers, which are connected via the open internet, making various information systems vulnerable to different risks. It is therefore necessary to ensure a secure connection and an acceptable quality, which is not affected by various external disturbances.

This work aims to study VPN technology as a solution to ensure secure communication for mobile teachers and students in remote education, for teleworkers and the interconnection between different branches of companies in telework. The implementation is based on the site-to-site VPN solution which allows the interconnection between the different sites of a company via the IPSec protocol in tunnel mode, which is the most answered, and has become a standard for VPN, providing the services security such as confidentiality, integrity, mutual authentication and access control. On the other hand, the remote access VPN solution for connecting teleworkers to its companies, as well as teachers and nomadic students to e-learning, based on the advantages of EzVPN which provides authentication services and the guarantee of safe tunnels.

Key words:

VPN, Site-to-site, IPSec, Tunnel, Services security, Remote access, EzVPN.

Remerciements

Je Tiens, en premier lieu, à remercier Allah, le tout puissant, de m'avoir donné autant de patience, courage et force pour réaliser ce travail.

Mes sincères remerciements vont en premier lieu à :

- ***Me BAY Fella***
- ***Mr BENYAHIA Mohamed***

Pour avoir accepté de faire partie du jury et d'examiner ce travail avec attention ;

À ma promotrice : ***Me BOUSTIA Narhimene***

Pour toutes leurs orientations pertinentes et pour leur disponibilité.

À mes ***parents*** *pour le soutient et les encouragements qu'ils me en fournis pendant cette période.*

À mes familles, mes amis et à tous ceux qui ont participé de près ou de loin à la réalisation de ce travail.

Sommaire

Liste des figures

Chapitre 1

Chapitre 2

Chapitre 3

Chapitre 4

Liste des tableaux

Chapitre 1

Chapitre 2

Chapitre 3

Liste des symboles et des abréviations

- **AES :** **A**dvanced **E**ncryption **S**tandard.
- **AH :** **A**uthentication **H**eader.
- **ASA :** **A**daptive **S**ecurity **A**ppliance.
- **AS :** **A**utonomous **S**ystem.
- **BGP :** **B**order **G**ateway **P**rotocol.
- **BSD :** **B**erkeley **S**oftware **D**istribution.
- **CA :** **C**ertificate **A**uthority.
- **CDMA:** **C**ode **D**ivision **M**ultiple **A**ccess.
- **CPU :** **C**entral **P**rocessing **U**nit.
- **DOI :** **D**omaine **O**f **I**nterpretation.
- **DOS :** **D**enial **O**f **S**ervice.
- **DTLS :** **D**atagram **T**ransport **L**ayer **S**ecurity.
- **EVDO :** **E**volution **D**ata **O**nly.
- **EIGRP :** **E**nhanced **I**nterior **G**ateway **R**outing **P**rotocol.
- **ESP :** **E**ncapsulating **S**ecurity **P**ayload.
- **FAI :** **F**ournisseur d'**A**ccès à l'**I**nternet.
- **GNS 3 :** **G**raphical **N**etwork **S**imulator 3.

- **GRE :** **G**eneric **R**outing **E**ncapsulation.
- **HMAC :** **H**ash-based **M**essage **A**uthentication **C**ode.
- **HSDPA :** **H**igh **S**peed **D**ownlink **P**acket **A**ccess.
- **HTTP :** **H**yper**T**ext **T**ransfer **P**rotocol.
- **HTTPS :** **H**yper**T**ext **T**ransfer **P**rotocol **S**ecure.
- **ICMP :** **I**nternet **C**ontrol **M**essage **P**rotocol.
- **IETF :** **I**nternet **E**ngineering **T**ask **F**orce.
- **IGMP :** **I**nternet **G**roup **M**anagement **P**rotocol.
- **IGP :** **I**nterior **G**ateway **P**rotocol.
- **IKE :** **I**nternet **K**ey **E**xchange.
- **IKEv2 :** **I**nternet **K**ey **E**xchange **v**ersion **2**.
- **IOS :** **I**nternet-work **O**perating **S**ystem.
- **IP :** **I**nternet **P**rotocole.
- **IPSec :** **I**nternet **P**rotocol **Sec**urity.
- **IPv4 :** **I**nternet **P**rotocole **v**ersion 4.
- **IPv6 :** **I**nternet **P**rotocole **v**ersion 6.
- **IPX :** **I**nternet **P**acket **X**change.
- **ISAKMP :** **I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol.
- **ISP :** **I**nternet **S**ervice **P**rovider.

- **KDC :** **K**ey **D**istribution **C**enter.
- **KINK :** **K**erberized **I**nternet **N**egotiation of **K**eys
- **LAN :** **L**ocal **A**rea **N**etwork.
- **L2TP :** **L**ayer **2** **T**unneling **P**rotocol.
- **MAC :** **M**essage **A**uthentication **C**ode.
- **MD5 :** **M**essage **D**igest **5.**
- **mGRE :** **m**ultipoint **G**eneric **R**outing **E**ncapsulation.
- **MPPE :** **M**icrosoft **P**oint to **P**oint **E**ncryption.
- **MSS :** **M**aximum **S**egment **S**ize.
- **MTU :** **M**aximum **T**ransmission **U**nit.
- **NAS :** **N**etwork **A**ccess **S**erver.
- **NAT :** **N**etwork **A**ddress **T**ranslation.
- **NBMA :** **N**on-Broadcast **M**ultiple **A**ccess.
- **NHS :** **N**ext **H**op **S**erver.
- **NHRP :** **N**ext **H**op **R**esolution **P**rotocol.
- **NSA :** **N**ational **S**ecurity **A**gency.
- **OS :** **O**perating **S**ystem**.**
- **OSPF :** **O**pen **S**hortest **P**ath **F**irst.
- **PC :** **P**ersonal **C**omputer.

- **PFS :** **P**erfect **F**orward **S**ecrecy.
- **PKI :** **P**ublic **K**ey **I**nfrastructure.
- **PPP :** **P**oint to **P**oint **P**rotocol.
- **PPTP :** **P**oint- to **P**oint **T**unneling **P**rotocol.
- **QoS :** **Q**uality **o**f **S**ervice.
- **RC4 :** **R**ivest **C**ipher version **4**.
- **RC5 :** **R**ivest **C**ipher version **5**.
- **RFC :** **R**equest **F**or **C**omments.
- **RIB :** **R**outing **I**nformation **B**ase.
- **RIP :** **R**outing **I**nformation **P**rotocol.
- **RSA :** **R**ivest - **S**hamir - **A**dleman.
- **SA :** **S**ecurity **A**ssociation.
- **SAD :** **S**ecurity **A**ssociation **D**atabase.
- **SHA-1 :** **S**ecure **H**ash **A**lgorithm **1**.
- **SKEME :** **S**ecure **K**ey **E**xchange **ME**chanism.
- **SP :** **S**ecurity **P**olicy.
- **SPD :** **S**ecurity **P**olicy **D**atabase.
- **SPF :** **S**hortest **P**ath **F**irst.

- **SPI :** **S**ecurity **P**arameters **I**ndex.
- **SSH :** **S**ecure **SH**ell.
- **SSL :** **S**ecure **S**ocket **L**ayer.
- **SSTP** **S**ecure **S**ocket **T**unneling **P**rotocol.
- **TCP :** **T**ransmission **C**ontrol **P**rotocol.
- **TLS :** **T**ransport **L**ayer **S**ecurity.
- **UDP :** **U**ser **D**atagram **P**rotocol.
- **UTM :** **U**nied **T**hreat **M**anagement.
- **VPN:** **V**irtual **P**rivate **N**etwork.
- **WAN :** **W**ide **A**rea **N**etwork.
- **Wi-Fi :** **W**ireless **F**idelity.
- **WSA :** **W**eb **S**ecurity **A**ppliance.
- **XAUTH :** e**X**tended **AUTH**entication.
- **3Com :** **Com**puter**, Com**munications and **Com**patibility.
- **3DES :** **3** (triple) **D**ata **E**ncryption **S**tandard.

INTRODUCTION GÉNÉRALE

À l'heure où la mobilité est un argument dans le domaine professionnel, ainsi que la période sensible qui a vu la propagation du virus Covid-19 surtout, et pour des raisons de santé, il est devenu nécessaire que les employés puissent travailler pour leurs entreprises partout dans le monde, et il est devenu nécessaire de continuer à étudier à distance pour les enseignants et les étudiants de la maison ou des lieux de quarantaine.

Pour des raisons évidentes de sécurité, toutes les informations essentielles à une entreprise ne peuvent pas être stockées sur un serveur accessible au public depuis internet, elles sont donc théoriquement inaccessibles depuis un réseau extérieur au réseau de l'entreprise, de sorte qu'un télétravailleur ne peut pas accéder à ses informations d'entreprise s'il n'est pas connecté au réseau de l'entreprise. D'ailleurs, lorsque l'étudiant ou l'enseignant accède à la plateforme e-learning via sa connexion à internet, il expose le trafic à des cyberattaques et à d'autres méthodes d'espionnage.

Pour remédier à ce problème, la technologie VPN (Virtual Private Network) a été mise en place pour contrer ce problème de sécurité et permettre à un utilisateur qui n'est pas connecté à un réseau interne de pouvoir quand même y accéder totalement ou partiellement à travers d'un réseau public.

Le principe du VPN est relativement simple, il a pour but de créer au travers d'un réseau public (et par conséquent non sécurisé) un tunnel crypté permettant de faire transiter des données jusqu'à un réseau privée disposant d'une connexion internet. Pour envoyer des données via ce tunnel, les deux parties (commerçant et entreprise par exemple) doivent se mettre d'accord sur l'algorithme de cryptage à utiliser. Le vendeur envoie ensuite ses données cryptées et signées (pour ajouter une sécurité supplémentaire) au tunnel. Ces données sont reçues par le serveur VPN de l'entreprise, qui les décrypte et vérifie leur intégrité et authencité.

Notre travail est organisé selon quatre chapitres :

Le premier chapitre est intitulé « Introduction aux réseaux privés virtuels », dans lequel nous présenterons quelques notions et concepts de base sur les VPN et leurs utilisations,

nous passerons par les différents protocoles qu'ils comprennent, et terminerons par une étude comparative entre les types de VPN.

Le deuxième chapitre intitulé « VPN de site à site », nous présenterons dans ce chapitre le concept associé au ce type, en plus, expliquerons les protocoles de ce type.

Le troisième chapitre intitulé « VPN d'accès à distance », sera consacré à la présentation de concept d'un autre type de VPN qui est l'accès à distance, et à parler des technologies les plus importantes fournies par Cisco dans ce type.

Le dernier chapitre intitulé « implémentation et simulation », sera consacré à la partie pratique de notre travail, dans lequel nous allons présenter l'environnement de travail GNS3, et d'autres outils, ainsi que la présentation des différentes étapes de la configuration pour la mise en place et la simulation de la solution.

Enfin, nous terminons par une conclusion.

CHAPITRE 1 : Introduction aux VPN

Un réseau privé virtuel désigne un réseau crypté dans le réseau internet, qui permet à une société dont les locaux seraient géographiquement dispersés de communiquer et partager des documents de manière complètement sécurisée, comme s'il n'y avait qu'un local avec un réseau interne.

Il peut être défini aussi comme un ensemble de ressources susceptibles d'être partagées par des flots de paquets ou de trames provenant de machines autorisées, ainsi qu'il peut utiliser des technologies et des protocoles quelconques. **[1]**

Nous verrons ici quelles sont les principales caractéristiques des VPN, et nous nous intéresserons ensuite aux protocoles permettant leur mise en place, tout en montrant pour chacun les points forts et les points de faiblesse selon différentes critères. Ensuite, nous discuterons les types de VPN à travers une étude comparative sous plusieurs aspects.

1.1 Besoins et avantages :

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

- **Authentification d'utilisateur :** Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel, ainsi qu'un historique des connexions et des actions effectuées sur le réseau peut être défini et conservé. Le client peut également être amené à authentifier le serveur afin de se protéger des faux serveurs VPN. **[2]**
- **Gestion d'adresses :** Chaque client sur le réseau dispose d'une adresse privé et confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse. **[2]**
- **Cryptage des données :** Lors de leur transport sur le réseau public, les données doivent être protégées par un cryptage efficace. **[2]**
- **Gestion de clés :** Les clés de cryptage pour le client et le serveur doivent être générées et régénérées. **[2]**
- **Prise en charge de multi protocole:** La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier le protocole IP. **[2]**

Le VPN offert les avantages suivants :

- Étendre la connectivité géographique et offre la possibilité d'un réseau mondial.
- Améliorer la sécurité.
- Plus flexible en cas d'évolution et de nouvelles implantations.
- Réduire le temps de transit.
- Notion de qualité de service :
  - ✓ Type best effort dans le cas de simples tunnels créés par l'utilisateur.
  - ✓ QOS bien meilleure dans le cadre d'une offre VPN d'opérateur.
- Minimiser les coûts :
  - ✓ Permet de réduire les coûts liés à l'infrastructure réseau des entreprises par la mise en place d'une liaison VPN.
  - ✓ La réduction des coûts par rapport à un WAN traditionnel. **[3]**

1.2 Principe de fonctionnement :

Un réseau VPN repose sur un protocole appelé "protocole de tunneling" qui est l'ensemble des processus d'encapsulation, de transmission et de décapsulation, il permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel, d'une façon où les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise. **[4]**

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire, par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. **[4]**

Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent une infrastructure partagée comme internet. **[4]**

1.3 Architecture des VPN :

Il existe principalement trois méthodes pour établir un réseau privé virtuel :

- Avec des routeurs (ou des concentrateurs VPN).
- Avec des dispositifs UTM (Unified Threat Management).
- Avec des contrôleurs sans fil et des points d'accès à distance.

Les diagrammes ci-dessous montrent un scénario où il y a quatre emplacements, l'un est le siège social (accès à internet au moyen de lignes), un autre est le bureau en succursale (accès à internet au moyen de lignes), et un autre est un bureau à domicile (accès à internet via une connexion haut débit fixe) et nous avons également du personnel de télétravail ou (accès à internet par les technologies mobiles à haut débit comme CDMA, EVDO, 3G, HSDPA …etc.).

1.3.1 VPN avec des routeurs ou concentrateurs :

Nous pouvons créer un réseau privé virtuel (VPN) entre le siège social et d'autres bureaux soit avec des routeurs ou via un concentrateur qui est un appareil VPN dédié à ces deux sites au cas où le volume VPN serait trop élevé et qu'il aurait besoin d'unités de traitement matériel dédiées.

Pour le bureau à domicile, un logiciel client VPN est chargé sur le PC qui établit un VPN avec le routeur concentrateur du siège social et nous pouvons faire la même chose pour les télétravailleurs également. **[5]**

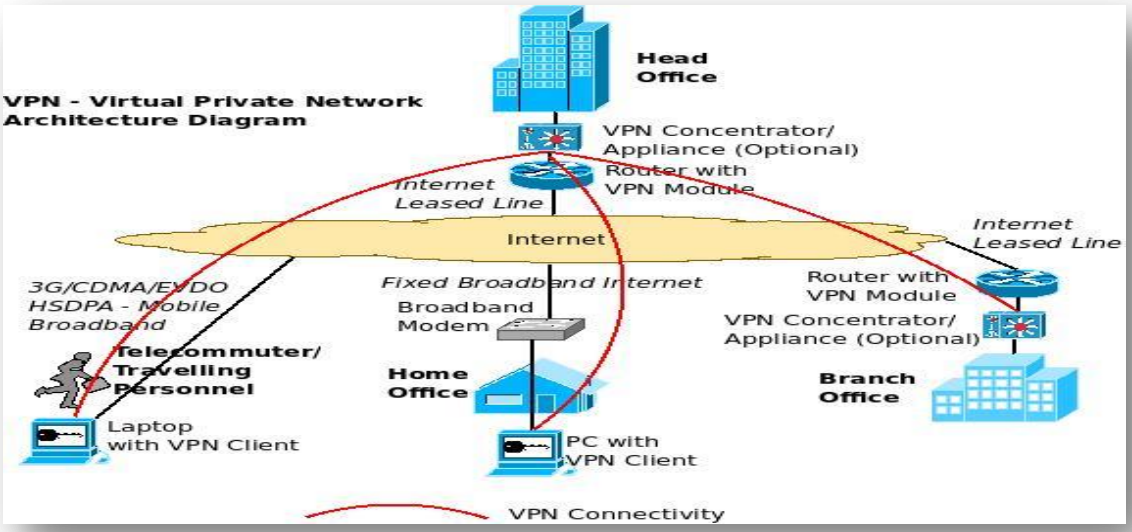

Figure 1-1 : Diagramme d'architecture VPN avec routeurs ou concentrateurs [5]

1.3.2 VPN avec UTM :

Comme la façon dont nous avons créé le VPN site à site entre le siège social et la succursale à l'aide de routeurs ou de concentrateurs VPN, nous pouvons également utiliser certains appareils UTM qui sont fournis avec des licences VPN intégrées pour établir le VPN site à site.

Le télétravailleur peut établir un VPN de la même manière en se connectant aux appareils UTM du siège social via le client VPN. **[5]**

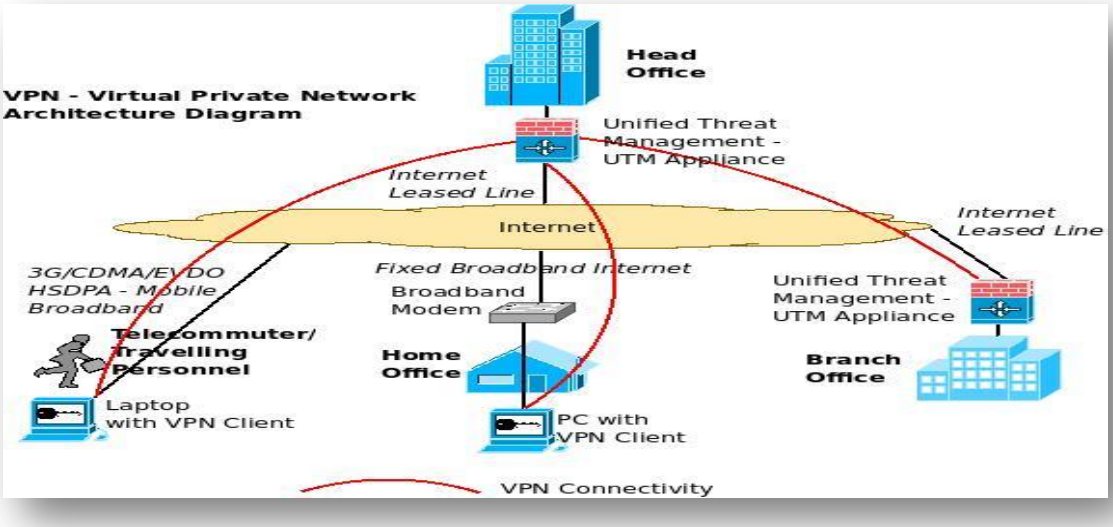

Figure 1-2 : Diagramme d'architecture VPN avec les appareils UTM [5]

1.3.3 VPN avec des contrôleurs sans fil :

C'est une alternative intéressante aux deux méthodes ci-dessus, ici, un contrôleur sans fil d'entreprise utilisé pour la gestion centralisée de plusieurs points d'accès sans fil dans l'entreprise peut lui-même agir comme un concentrateur VPN et établir des tunnels VPN avec d'autres contrôleurs, points d'accès à distance (bureau à domicile) et clients VPN (télétravailleurs).

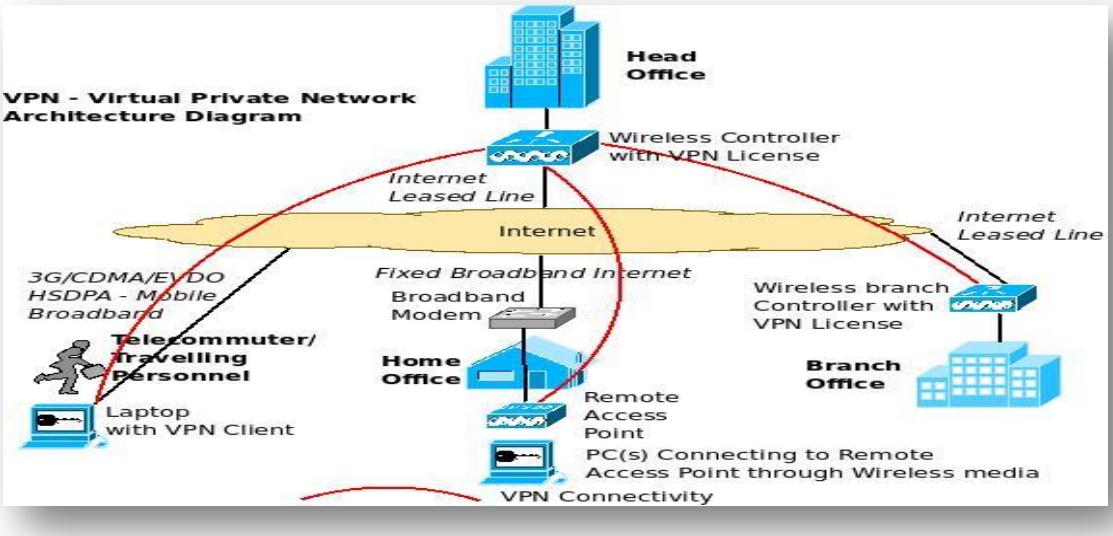

Figure 1-3 : Diagramme d'architecture VPN utilisant un contrôleur sans fil [5]

Les connexions VPN ne doivent pas toujours être du siège social aux succursales ou au télétravailleur comme indiqué dans les schémas ci-dessus, il peut être établi d'un site à un autre site, d'un site à plusieurs sites et de plusieurs sites à plusieurs sites en fonction de la configuration, des modèles et des types de connexion pris en charge par les différents appareils VPN. **[5]**

1.4 Protocoles utilisés dans les VPN :

Il existe différents protocoles VPN, chacun avec ses avantages et ses inconvénients. Ils sont fondamentaux pour construire un VPN et sécuriser les transmissions. Voyons maintenant les principaux protocoles VPN, tel que PPTP, L2TP/IPSec, et SSTP, et une comparaison entre eux.

1.4.1 PPTP :

Le protocole PPTP (Point-to-Point Tunneling Protocol) est l'un des protocoles VPN les plus anciens sur le marché, il était normalement destiné à permettre la connexion d'utilisateurs distants au site central d'une entreprise. L'idée originelle du protocole est de permettre l'encapsulation de datagrammes non TCP/IP, comme Apple Talk et IPX pour être téléportés à travers un réseau IP. Son usage s'est élargi à la connexion site à site car nous le trouvons également dans beaucoup de routeurs ou de pare-feu. **[6]**

Il a été créé à l'origine par Microsoft, Ascend et 3Com, et il n'a jamais été un standard reconnu par l'IETF mais son atout majeur a été sa présence sur tous les postes Windows depuis sa naissance. **[6]**

Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans les datagrammes IP :

- Le tunnel PPTP se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par clôture du tunnel par le serveur.**[6]**
- Lors de l'établissement de la connexion, le client effectue d'abord une connexion de type PPP et permet de faire circuler les données sur internet. **[6]**
- Par suite une deuxième connexion est établie, elle permet d'encapsuler les paquets PPP dans les datagrammes IP, et cette deuxième connexion qui forme le tunnel PPTP. **[6]**

La NSA a réussi à exploiter les failles de sécurité du protocole PPTP, cela ajouté à son manque de chiffrement de haut niveau explique pourquoi ce protocole n'est plus considéré comme sûr, cependant, l'absence de chiffrement fort fait de PPTP un protocole très rapide. **[6]**

1.4.2 L2TP / IPSec :

Le protocole L2TP (Layer 2 Tunneling Protocol) est un protocole de tunneling utilisé pour créer un « tunnel VPN » par lequel votre trafic de données est guidé, cependant, L2TP lui-même ne chiffre aucune donnée, c'est pourquoi, dans la quasi-totalité des cas, le protocole L2TP est associé au protocole IPSec, qui chiffre les données, c'est de là que vient le nom L2TP / IPSec.

IPSec (qui signifie Internet Protocol Security) est un protocole permettant de sécuriser les communications IP, il agit au niveau de la couche 3 (réseaux) du modèle OSI, il s'occupe du chiffrement de bout en bout des données dans le tunnel L2TP.

Le protocole L2TP / IPSec qui comprend le système de cryptage est intégré à tout OS modernes et à tous les appareils qui sont capables d'utiliser un VPN. L'utilisation de la combinaison L2TP / IPSec en tant que protocole VPN est beaucoup plus sûre et garantit plus de confidentialité et aussi plus simple que l'utilisation de protocole PPTP, puisqu'il utilise généralement le même client.

Comme tout protocole, L2TP / IPSec présente toutefois des défauts, l'un des inconvénients du protocole est le fait que certains pares feux bloquent les utilisateurs de ce protocole car L2TP utilise le port UDP 500 et que certains sites web le bloque. En ce qui concerne la vitesse, le protocole L2TP seul est très rapide en raison de son manque de chiffrement, cependant, l'ajout nécessaire d'IPSec peut ralentir un peu la connexion. **[7]**

1.4.3 SSTP :

Le SSTP (Secure Socket Tunneling Protocol) est un protocole VPN créé par Microsoft et disponible à partir de Windows Vista Service Pack, il s'agit d'un protocole Microsoft propriétaire, qui est mieux pris en charge par Windows et qui est intègre au système d'exploitation, donc il est plus stable sous Windows, il peut également être utilisé sous Linux mais pas sous MacOs.

Il n'est pas possible de faire du VPN « site-à-site » avec SSTP, seulement des connexions clients nomades. Présent nativement sur les clients, le serveur s'intègre avec les comptes Active Directory, pour cela, nos utilisateurs peuvent utiliser leurs mots de passes Windows ou des certificats générés automatiquement par notre contrôleur de domaine.

Il permet au trafic PPP ou L2TP de passer par un canal SSL/TLS sur le port TCP 443, ce qui le rend excellent pour passer à travers la plupart des pare-feu car le trafic semble normal. Lors de l'utilisation de SSTP, les utilisateurs doivent se connecter au TCP (Transmission Control Port), qui lance les procédures d'authentification du serveur principal, ensuite les clés de chiffrement sont envoyées au système de l'utilisateur, ce qui constitue la base du tunnel SSTP, et une fois cette base formée, les données peuvent être envoyées directement au serveur en toute sécurité. **[8]**

Tableau 1-1 : Comparaison entre les différents protocoles de VPN

	PPTP	L2TP / IPSec	SSTP
Généralité	Protocole VPN assez basique et le premier qui a été pris en charge par Windows.	Protocole de tunneling qui utilise le protocole IPSec pour la sécurité et le chiffrement.	Protocole VPN pour des connexions clients nomades, créé par Microsoft.
Chiffrement	Utilise le protocole MPPE pour chiffrer les données. Algorithmes utilisés : ***RSA, RC4*** avec une longueur de 128 bits.	Utilise le protocole IPSec pour chiffrer les données. Algorithmes utilisés : ***3DES, AES*** avec une longueur 256 bits.	Offre un chiffrement fort qui utilise les clés SSL. Algorithme utilisé : ***AES*** avec une longueur de 256 bits.

Exploitabilité	Peut être directement installé dans votre système d'exploitation, ainsi qu'il est intégré à de nombreux logiciels (nombreux fournisseurs VPN proposent ce protocole).		Disponible pour SEIL, Linux et RouterOS, mais il reste principalement une plateforme Windows, ainsi que plusieurs fournisseurs VPN proposent ce protocole.
Vitesse	De manière générale, PPTP est conçu pour être un protocole rapide, principalement en raison de son chiffrement relativement simple et de bas niveau.	Le protocole L2TP lui-même est très rapide car il ne propose qu'un tunnel de communication, mais pas de chiffrement, mais l'ajout nécessaire d'IPSec pour la sécurité rend L2TP / IPSec plus lent.	Le SSTP est un peu lent en raison du haut niveau de cryptage.
Stabilité et fiabilité	Avoir quelques problèmes de stabilité et de fiabilité, qu'ils peuvent être attribués à des problèmes de compatibilité.	Offre une stabilité et fiabilité considérable, mais dépend parfois de la stabilité du réseau.	Puisqu'il est totalement intégré à Windows, il est connu pour être à la fois stable, fiable et complètement compatible avec Windows.
Confidentialité et sécurité	PPTP est connu pour avoir plusieurs failles de sécurité.	L2TP, lorsqu'il est combiné avec IPSec, est connu pour être un protocole très sûr	SSTP est configuré avec le cryptage AES, cela le rend plus sécurisé que la plupart des autres protocoles. Il utilise également la technologie SSL v3, cela évite les problèmes de pare-feu et vous rend moins vulnérable au blocage.

Avantage	+ Facile à configurer. + Généralement rapide. + Compatible avec la plupart des plateformes.	+ Facile à configurer. + Capable de contourner les restrictions réseaux et les restrictions FAI. + Meilleur chiffrement que PPTP.	+ Facile à utiliser. + Capable de contourner la plupart des pare-feu. + Avoir un haut niveau de sécurité.
Inconvénient	- Le degré de stabilité et de fiabilité peut beaucoup varier. - Pas aussi sûr et privé que les protocoles modernes. - Détection et blocage des utilisateurs PPTP faciles pour les sites web, le gouvernement et les FAI.	- Il peut être bloqué par un pare-feu puisqu' utilise un port souvent bloqué « UDP 500 ».	- Fonctionne bien sur les plateformes Windows mais pas ailleurs. - Puisque propriété de Microsoft, il ne peut être audité par aucune tierce partie pour vérifier ses vulnérabilités.
Conclusion	Le protocole PPTP est généralement facile à configurer, mais moins stable et sécurisé que les protocoles modernes.	L2TP / IPSec est souvent plus lent que PPTP, mais peut contourner les blocages.	SSTP est plus destiné aux utilisateurs de Windows, en outre il est configuré pour utiliser l'algorithme de chiffrement AES, ce qu'il le rend plus fiable que L2TP/IPSec et encore plus que le PPTP bien évidemment.

1.5 Type des VPN :

Il existe trois types de VPN :

- VPN d'accès entre les employés distant et le réseau de l'entreprise.
- L'intranet VPN entre les succursales et le siège d'une entreprise.
- L'extranet VPN entre une entreprise et ses partenaires et clients privilégié.

1.5.1 Les VPN d'accès :

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé, comme le montre la figure suivante :

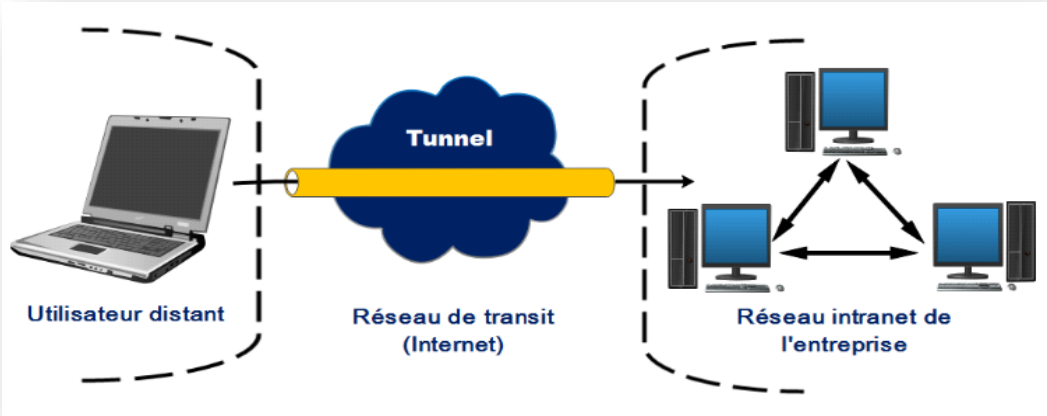

Figure 1-4 : Le fonctionnement d'un VPN d'accès [6]

Il est nécessaire pour ce type de VPN de définir une authentification forte afin de vérifier les utilisateurs distants. L'utilisateur utilise donc un ISP (Internet Service Provider) dans le but d'établir une communication sécurisée avec l'entreprise distante à l'aide de deux possibilités :

- Soit le client établit un tunnel crypté à travers l'ISP vers le réseau de l'entreprise avec un avantage de sécurité dont la communication est cryptée de bout en bout.

- Soit l'utilisateur communique avec le NAS (Network Access Server) de l'ISP, qui lui établit une communication cryptée avec le réseau de l'entreprise distante, ce qui permet entre autre à l'utilisateur de se connecter avec plusieurs réseaux en utilisant plusieurs tunnels, de plus, le client n'a pas besoin de transporter le logiciel lui permettant d'établir une communication cryptée. **[6]**

1.5.2 L'intranet VPN :

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux, ce type est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants afin de garantir la sécurité et l'intégrité des données, comme le montre la figure ci-dessous.

Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...) donc il est nécessaire de développer un fort cryptage pour protéger ces données circulantes. **[6]**

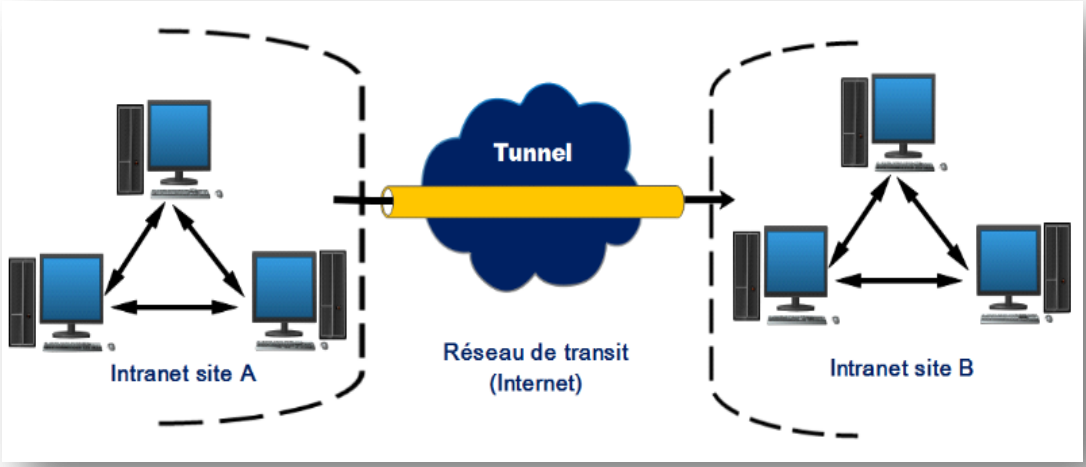

Figure 1-5 : Le fonctionnement d'intranet VPN [6]

1.5.3 L'extranet VPN :

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires stratégiques, ce qui nécessite une solution ouverte afin d'assurer l'interopérabilité avec les diverses solutions que les partenaires peuvent implémenter, comme il est mentionné dans la figure ci-dessous.

Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci. Souvent, seule une partie des ressources est partagée, ce qui nécessite une gestion rigoureuse des espaces d'échange. **[6]**

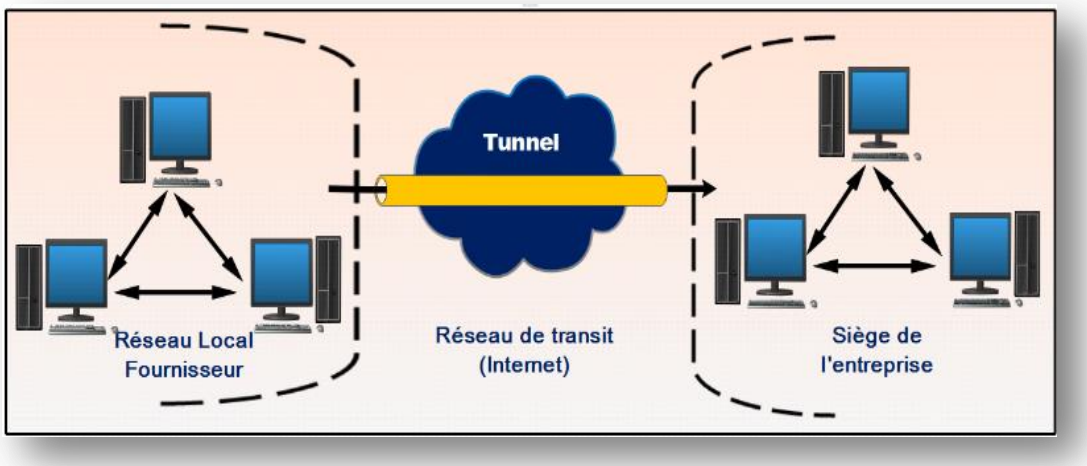

Figure 1-6 : Le fonctionnement d'extranet VPN [6]

1.6 Étude comparative :

Dans le VPN de site à site, la méthode de sécurité IPSec est utilisée pour créer un tunnel crypté d'un réseau client au site distant du client, et les utilisateurs multiples ne sont pas autorisés. Par contre dans le VPN d'accès à distance, les utilisateurs individuels sont connectés au réseau privé et permet à la technique d'accéder à distance aux services et aux ressources de ce réseau privé et les utilisateurs multiples sont autorisés. Il est le plus approprié pour les entreprises et les utilisateurs à domicile.

Voyons maintenant la différence entre le VPN de site à site et le VPN d'accès à distance, qui sont donnés ci-dessous :

Tableau 1-2 : Comparaison entre types VPN

Paramètres	VPN de site à site	VPN d'accès à distance
Philosophie	Utilise une méthode de sécurité appelée IPSec pour créer un tunnel crypté à partir d'un réseau client vers le site distant du client entre tout ou partie d'un réseau local des deux côtés.	Connecte les utilisateurs individuels à des réseaux privés.
Client VPN sur les périphériques finaux	Pas nécessaire d'être configuré sur chaque client.	Chaque utilisateur peut (Client VPN) ou non (Clientless) exiger d'avoir son propre client VPN.
Création du tunnel	Chaque utilisateur n'est pas obligé d'initier la configuration du tunnel VPN.	Chaque utilisateur d'accès à distance doit initier pour former un tunnel VPN.
Utilisateur cible	Les utilisateurs de la succursale doivent se connecter aux serveurs de l'administration centrale.	Utilisateurs itinérants qui veulent accéder aux ressources et aux serveurs du siège social en toute sécurité.

Cryptage / Décryptage	La passerelle VPN est responsable de l'encapsulation et du chiffrement du trafic sortant, en l'envoyant via un tunnel VPN sur internet vers une passerelle VPN homologue sur le site cible.	le logiciel client VPN encapsule et crypte ce trafic avant de l'envoyer via internet vers la passerelle VPN au bord du réseau cible.
Technologies appuyées	IPSec.	IPSec et SSL.
Flux de trafic multi-utilisateurs / VLAN	Permet à plusieurs utilisateurs / VLAN de circuler dans chaque tunnel VPN.	Ne permet pas au trafic d'utilisateurs multiples de passer par chaque tunnel VPN.

Conclusion :

Au cours de ce chapitre, nous avons brossé de façon claire les notions générales de VPN, son fonctionnement ainsi que les différents protocoles utilisés dans les VPN, puis nous avons fait une étude comparative entre les types VPN utilisés

CHAPITRE 2 : VPN de site à site

De nombreuses organisations ont plusieurs sites physiques, chacun avec son propre réseau local d'entreprise (LAN), bien qu'ils soient géographiquement séparés, ces sites multiples ont besoin d'un seul réseau étendu (WAN) d'entreprise pour assurer une communication sécurisée entre les sites.

Le réseau privé virtuel de site à site est un type de VPN qui garde les données cryptées entre deux emplacements sans avoir besoin d'identifiants ou d'applications client sur les appareils qui l'utilisent, il fournit cela en créant un lien crypté entre les passerelles VPN situées sur chacun de ces sites, ainsi qu'un tunnel VPN de site à site chiffre le trafic à une extrémité et l'envoie à l'autre sur l'internet public où il est décrypté et acheminé vers sa destination. Par exemple, une organisation qui a des bureaux à Oran, Alger et Constantine peut utiliser un VPN de site à site pour connecter tous les bureaux ensemble, en effet, cela crée un réseau entier (WAN), où les utilisateurs peuvent échanger des données et des informations entre eux à partir d'endroits complètement différents, tous cryptés et sécurisés par le VPN.

Étant donné que les VPN de site à site chiffrent les données à une passerelle, les utilisateurs n'ont pas besoin d'avoir le logiciel VPN installé sur leur ordinateur car tant qu'ils sont connectés au réseau de site, leurs données sont protégées.

Si nous utilisons un VPN à la maison, nous devons lancer l'application client, à nous connecter et à la maintenir en cours d'exécution aussi longtemps que nous souhaitons l'utiliser, mais avec un VPN de site à site, nous épargnons aux informaticiens la corvée d'avoir à installer individuellement un logiciel sur chaque appareil qui a besoin de protection.

Un extranet de site à site fonctionne à peu près de la même façon, c'est-à-dire que les employés ne verront pas le VPN ou n'auront à exécuter aucune application, juste à la différence que seules certaines informations sont partagées entre les sites. **[9]**

Dans ce qui suit, nous parlerons des protocoles utilisés dans le VPN de site à site, précisément, un protocole de tunneling, ainsi un protocole de sécurisation, tout en expliquant pour chacun, la notion générale et le principe de fonctionnement, ensuite nous discuterons d'une amélioration dans les VPN de site à site qui assure une flexibilité et stabilité considérable.

2.1 Encapsulation de routage générique (GRE) :

2.1.1 Concept général :

GRE est un protocole de mise en tunnel qui permet d'encapsuler n'importe quel paquet de la couche réseau qui utilise un protocole de routage à l'intérieur des paquets d'un autre protocole. Quand nous disons « encapsuler » signifie envelopper un paquet de données à l'intérieur d'un autre paquet de données, comme si nous mettions une boîte dans une autre boîte. Est un moyen qui a été développé par Cisco afin d'établir une connexion directe point à point dans un réseau, dans le but de simplifier les connexions entre des réseaux séparés, et qu'il fonctionne avec une variété de protocoles de la couche réseau.

Il permet d'utiliser des protocoles qui ne sont normalement pas pris en charge par un réseau, parce que les paquets sont enveloppés dans d'autres paquets qui utilisent des protocoles pris en charge, donc le GRE est un moyen de charger un type de paquet dans un autre type de paquet afin que le premier paquet puisse circuler sur un réseau sur lequel il ne pourrait normalement pas circuler. Par exemple, supposons qu'une entreprise ait besoin d'établir une connexion entre les réseaux locaux (LAN) de ses deux bureaux qui utilisent la dernière version du protocole internet « IPv6 », mais pour passer d'un réseau de bureau à un autre, le trafic doit transiter via un réseau géré par un tiers, or, ce réseau est quelque peu dépassé et ne prend en charge que l'ancien protocole « IPv4 ». Avec le GRE, la société pourrait envoyer du trafic par ce réseau en encapsulant des paquets « IPv6 » dans des paquets « IPv4 ». **[10]**

2.1.2 Mise en tunnel GRE :

L'encapsulation de paquets dans d'autres paquets est appelée « mise en tunnel », ces tunnels GRE sont généralement configurés entre deux routeurs, chaque routeur agissant comme une extrémité du tunnel, ainsi qu'ils sont configurés pour envoyer et recevoir des paquets GRE directement entre eux, d'ailleurs, les routeurs situés entre ces deux routeurs n'ouvriront pas les paquets encapsulés, ils ne se réfèreront qu'aux en-têtes entourant les paquets encapsulés pour pouvoir les transmettre. **[10]**

Pour comprendre pourquoi nous parlons de « mise en tunnel », nous pouvons mettre l'analogie suivante, imaginons un point A comme un appareil en réseau, et un autre point B comme un autre appareil en réseau, mentionnons que nous avons ainsi un réseau entre les deux appareils, et des paquets de données qui doivent aller du point A au point B.

Imaginons que ce réseau ne prenne pas en charge le type de paquets de données que les appareils des points A et B doivent échanger, donc par conséquent, les paquets de données ne peuvent pas passer et auront à parcourir un trajet beaucoup plus long via des réseaux supplémentaires. Mais le GRE crée un « tunnel » virtuel à travers le réseau afin de permettre le passage des paquets de données par le réseau qui ne les prend pas en charge.

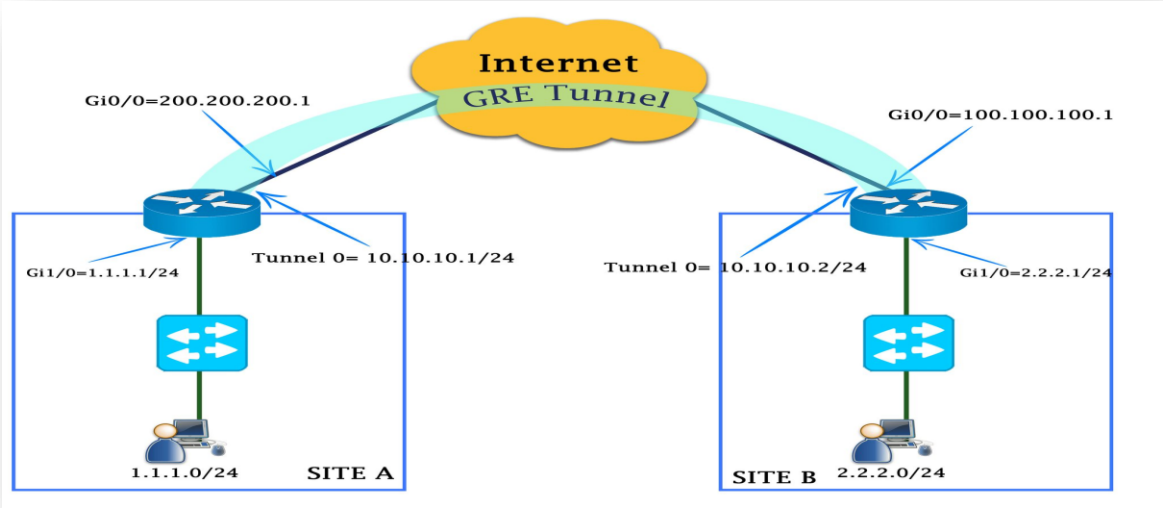

Figure 2-1 : Mise en tunnel GRE

2.1.3 Principe de fonctionnement :

Toutes les données envoyées sur un réseau sont divisées en petits morceaux appelés paquets, et tous les paquets ont deux parties :

- La charge utile (Payload).
- L'en-tête (Header).

La charge utile est le contenu réel du paquet, c'est les données qui sont envoyées, tandis que, l'en-tête contient des informations sur la provenance du paquet et le groupe de paquets auquel il appartient, en outre, chaque protocole de réseau attache un en-tête à chaque paquet.

Le GRE ajoute deux en-têtes à chaque paquet :

- L'en-tête GRE (longueur de 4 octets).
- L'en-tête IP (longueur de 20 octets).

L'en-tête GRE indique le type de protocole utilisé par le paquet encapsulé, d'autre part, l'en-tête IP encapsule l'en-tête (header) et la charge utile (payload) du paquet original, cela signifie qu'un paquet GRE a généralement deux en-têtes IP, l'un pour le paquet original, et l'autre ajouté par le protocole GRE, notons que seuls les routeurs à chaque extrémité du tunnel GRE se réfèreront à l'en-tête IP original. **[10]**

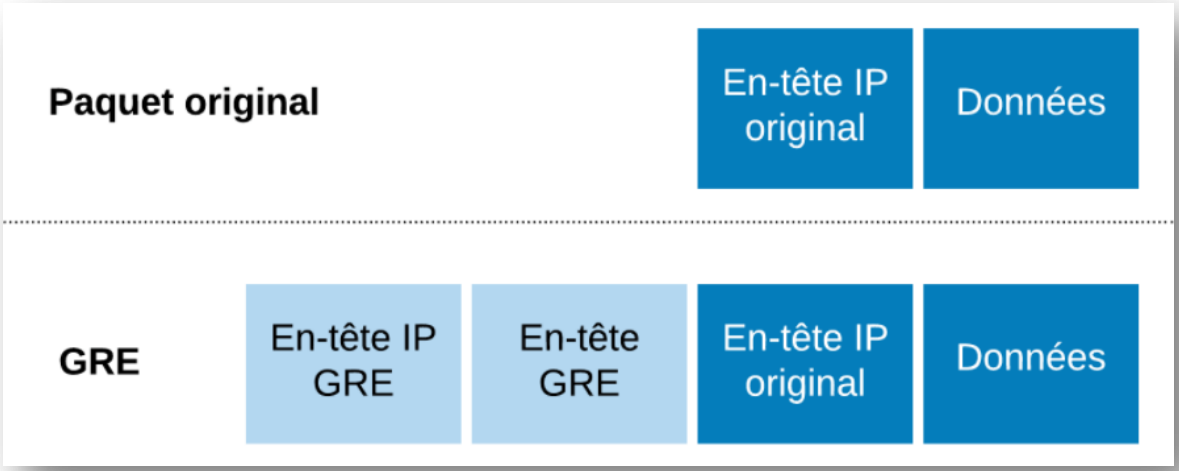

Figure 2-2 : Encapsulation GRE [10]

2.1.4 Impact de l'utilisation du GRE :

MTU et MSS sont des mesures qui limitent la taille des paquets de données circulant sur un réseau, tout comme la limite de poids des automobiles traversant un pont. Le MTU mesure la taille totale d'un paquet, y compris les en-têtes, tandis que MSS mesure uniquement le payload. Soulignons que les paquets qui dépassent le MTU sont fragmentés, ou découpés en plus petits morceaux, afin qu'ils puissent s'adapter au réseau.

Comme tout protocole, l'utilisation de GRE ajoute quelques octets à la taille des paquets de données, cela doit être pris en compte dans les paramètres MSS et MTU pour les paquets. Si le MTU est de 1 500 octets et le MSS de 1 460 octets (pour tenir compte de la taille des en-têtes IP et TCP nécessaires), l'ajout d'en-têtes GRE de 24 octets fera que les paquets dépasseront le MTU :

1 460 octets [payload] + 20 octets [en-tête TCP] + 20 octets [en-tête IP] + 24 octets [en-tête GRE + en-tête IP] = 1 524 octets

Par conséquent, les paquets seront fragmentés, cela ralentit les délais de livraison des paquets et augmente la puissance de calcul utilisée, car les paquets qui dépassent le MTU doivent être décomposés puis réassemblés.

Cela peut être évité en réduisant le MSS pour l'adapter aux en-têtes GRE, si le MSS est fixé à 1 436 octets au lieu de 1 460, les en-têtes GRE seront pris en compte et les paquets ne dépasseront pas le MTU de 1 500 octets :

1 436 octets [payload] + 20 octets [en-tête TCP] + 20 octets [en-tête IP] + 24 octets [en-tête GRE + en-tête IP] = 1 500 octets

Bien que la fragmentation soit évitée, le résultat est que les payloads sont légèrement plus petits, ce qui signifie qu'il faudra des paquets supplémentaires pour livrer les données, par exemple, si l'objectif est de fournir 150 000 octets de contenu (environ 150 ko), et si le MTU est fixée à 1 500 et qu'aucun autre protocole de couche 3 n'est utilisé, comparons le nombre de paquets nécessaires lorsque le GRE est utilisé et quand il ne l'est pas :

- Sans le GRE, MSS = 1 460 : *103 paquets.*
- Avec le GRE, MSS = 1436 : *105 paquets.*

Les deux paquets supplémentaires ajoutent quelques millisecondes de retard au transfert de données, cependant, l'utilisation du GRE peut permettre à ces paquets de prendre des chemins de réseau plus rapides qu'ils ne le pourraient autrement, ce qui peut compenser ce retard. **[10]**

2.2 Sécurité du protocole internet (IPSec) :

2.2.1 Concept général :

IPSec (Internet Protocol Security) est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau, il s'agit en fait, d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.

Il décrit des protocoles permettant de mettre en œuvre des tunnels sécurisés, au niveau 3 (IP), ces tunnels sont utilisés pour la sécurisation des protocoles des couches supérieures tels que TCP et UDP, d'ailleurs sa position dans les couches basses du modèle OSI lui permet donc de sécuriser tous type d'applications et protocoles réseaux basés sur IP sans distinction. IPSec est très largement utilisé pour le déploiement de réseau VPN à travers internet à petite et grande échelle. **[11]**

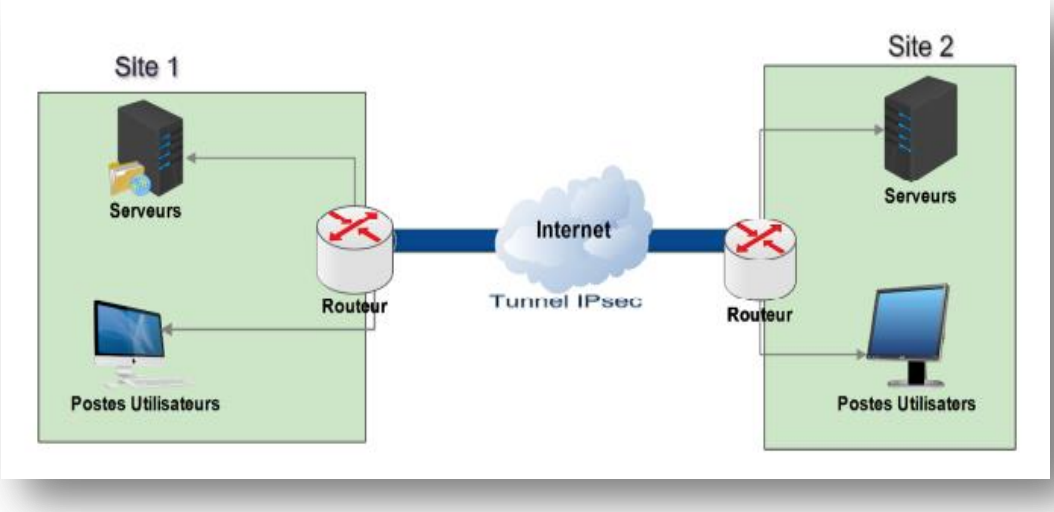

Figure 2-3 : Mise en oeuvre d'un tunnel IPSec [11]

2.2.2 Avantages d'IPSec :

L'apport majeur de cette techniques par rapport à d'autres solutions est qu'il s'agit d'une méthode standard conçue dans cet objectif précis, décrite par différentes RFC, et donc interopérable.

Cette méthode présente les avantages suivants :

- L'économie de bande passante, car la compression des en-têtes des données transmises est prévue par ce standard, de plus, ce dernier ne fait pas appel à de trop lourdes techniques d'encapsulation, comme les tunnels PPP sur lien SSH.
- La protection des protocoles de bas niveau comme ICMP et IGMP, RIP, etc.
- L'évolution continue d'IPSec, vu que les algorithmes de chiffrement et d'authentification sont spécifiés séparément du protocole lui-même. **[2]**

2.2.3 Fonctionnalités d'IPSec :

IPSEC est en fait un ensemble de protocoles qui fournissent des fonctionnalités uniques de sécurisation de la couche réseau entre deux équipements qui permettent :

- **La confidentialité des données :**
  Se fait par chiffrement pour protéger les données contre les tentatives d'écoute. Les algorithmes de chiffrement supportés sont : *DES, 3DES et AES.* **[3]**

- **L'intégrité des données et l'authentification :**
  Se fait grâce à la fonction HMAC (Hash-based Message Authentication Code) qui vérifie que les paquets n'ont pas été altérés et sont en cours de réception par un équipement autorisé, en d'autres termes, empêcher une attaque par détournement « man-in-the-middle » ou le vol de session. Les fonctions HMAC supporté par l'IPSEC sont le MD5 et le SHA-1. **[3]**

- **La détection d'anti-rejeu:**
  Se fait en incluant les numéros de séquence des paquets cryptées pour s'assurer à ce qu'un rejeu attaque ne se produise pas par un dispositif « man-in-the-middle ».**[3]**

- **L'authentification entre les équipements :**
  Veille qu'avant que les données soient transmises entre les équipements, qu'ils soient identifiés et validés, le dispositif d'authentification prend en charge les clés pré-partagées symétriques et asymétriques, ainsi que les certificats numériques.

Les connexions d'accès à distance prennent en charge l'authentification des utilisateurs en utilisant le XAUTH court pour l'authentification étendue. **[3]**

2.2.4 Gestion des flux IPSec :

Les flux IPSec sont gérés uni-directionnellement, ainsi, une communication bidirectionnelle entre deux machines utilisant IPSec sera définie par divers processus pour chacun des sens de communication. Les procédés détaillés ci-dessous respectent tout deux cette loi.

2.2.4.1 Politique de sécurité (SP) :

Une politique de sécurité SP défini ce qui doit être traité sur un flux, et comment nous voulons transformer un paquet. Il y sera indiqué pour un flux donné :

- Les adresses IP de l'émetteur et du récepteur (unicast, multicast ou broadcast).
- Par quel protocole il devra être traité (AH ou ESP).
- Le mode IPSec à utiliser (tunnel ou transport).
- Le sens de la liaison (entrante ou sortante).

Notons qu'une SP ne définit qu'un protocole de traitement à la fois, pour utiliser AH et ESP sur une communication, deux SP devront être créée. **[12]**

2.2.4.2 Association de sécurité (SA) :

Une association de sécurité SA défini comment sera traité le paquet en fonction de sa SP associée, elles ne sont que la "réalisation" des SP, et elle possède l'ensemble des propriétés de la liaison, ainsi, elle sera représentée par une structure de donnée contenant les informations suivantes :

- Un compteur permettant de générer les numéros de séquence des AH et ESP.
- Un flag (drapeau) permettant d'avertir qu'en cas de dépassement du compteur précédemment décrit, on doit interrompre la communication.
- Une fenêtre d'anti répétition dans laquelle doit tomber le prochain numéro de séquence.
- Information sur l'AH (algorithme d'authentification, clefs, durée de vie, etc.).
- Information sur l'ESP (algorithme d'authentification et de chiffrement, clefs, etc.).
- Mode IPSec utilisé (tunnel ou transport).
- Durée de vie de la SA.

- Unité de transmission maximale (MTU), qui est la taille maximale d'un paquet pouvant être transmis en une seule fois sur une interface.

Une SA est identifiée à un seul et unique flux unidirectionnel grâce à trois champs :

- L'adresse IP de destination (unicast, multicast ou broadcast).
- Le protocole utilisé (AH ou ESP).
- Le SPI (Security Parameter Index).

Notons qu'une SA ne sera associée qu'à un seul des protocoles AH ou ESP, si nous voulons protéger un flux avec ces deux protocoles, deux SA devront être créé. **[12]**

2.2.4.3 Bases de données SPD et SAD :

Tout système implémentant IPSec possède donc deux bases de données distinctes dans laquelle ils stockent leurs SP (SPDatabase) et leurs SA (SADatabase). La SPD défini donc le traitement de chaque type de trafic entrant ou sortant. **[13]**

2.2.5 Modes IPSec :

Il existe deux modes d'utilisation d'IPSec : le mode transport et le mode tunnel, notons que la génération des datagrammes sera différente selon le mode utilisé.

- **Mode Transport :** Ce mode est utilisé pour créer une communication entre deux hôtes qui supportent IPSec. Une SA est établie entre les deux hôtes, les entêtes IP ne sont pas modifiées et les protocoles AH et ESP sont intégrés entre cette entête et l'entête du protocole transporté. Ce mode est souvent utilisé pour sécuriser une connexion Point-To-Point.
- **Mode Tunnel :** Ce mode est utilisé pour encapsuler les datagrammes IP dans IPSec. La SA est appliquée sur un tunnel IP, ainsi, les entêtes IP originales ne sont pas modifiés et un entête propre à IPSec est créé. Ce mode est souvent utilisé pour créer des tunnels entre réseaux LAN distant, effectivement, il permet de relier deux passerelles étant capable d'utiliser IPSec sans perturber le trafic IP des machines du réseau qui ne sont donc pas forcément prête à utiliser le protocole IPSec. **[14]**

2.2.6 Protocoles utilisés par IPSec :

IPSec repose principalement sur deux protocoles destinés à sécuriser le trafic :

- **AH:** Authentication Header.
- **ESP:** Encapsulating Security Protocol.

2.2.6.1 Le protocole AH :

AH (Authentication Header) est conçu pour assurer l'intégrité et l'authentification des datagrammes IP, bien qu'il ne crypte pas les données de paquet IP, ainsi qu'il n'empêche pas les utilisateurs non autorisés de lire le contenu des paquets capturés, mais il garantit que les paquets n'ont pas été modifiés en route et qu'ils proviennent bien des systèmes identifié par l'adresse IP source contenu dans le paquet.

Le principe d'AH est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. **[12]**

La forme de la trame AH est présentée ci-dessous.

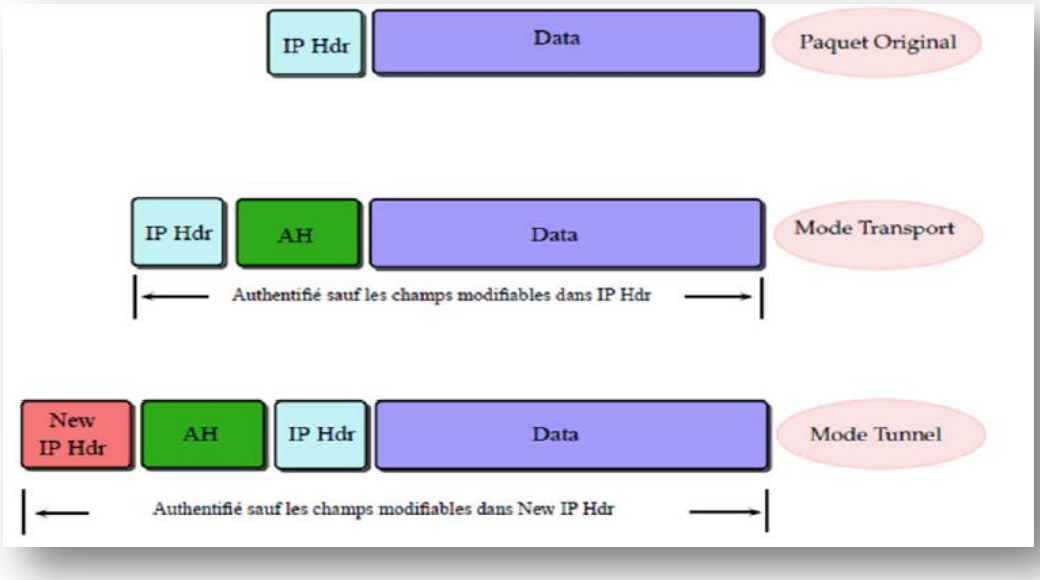

Figure 2-4 : Trame AH en mode tunnel et transport [12]

Les différentes méthodes d'intégrité utilisées dans ce mode sont :

- **MD5 (Message Digest 5) :** Algorithme de hachage conçu par Rivest (un des concepteurs de RSA), il opère sur des blocs de 512 bits, et le résultat est un digest de 128 bits (4 * 32 bits).

- **SHA-1 (Secure Hash Algorithme 1) :** Méthode basée sur MD4, et fonctionne avec des blocs de 512 bits et une clé de 160 bits.

L'application de ces méthodes sur un message produit un digest (haché) permettant de certifier l'intégrité et l'authenticité du message. Notons qu'il est impossible de retrouver le message à partir du digest, ainsi, si un bit du message change, le digest résultant est très différent à cause de l'effet d'avalanche. **[15]**

2.2.6.2 Le protocole ESP :

ESP (Encapsulating Security Payload) offre également la confidentialité et la sécurité des données du datagramme IP, elles sont alors chiffrées avant d'être transmises, suivant différents mécanismes et protocoles.

Il chiffre, d'une part, le champ « data » des paquets suivant un ensemble de paramètres négociés au préalable avec l'hôte distant, et d'autre part, utilise des mécanismes d'authentification (comme HMAC) afin de fournir une protection anti-rejeu ou encore une intégrité des données. Notons qu'en mode transport, seules les données transportées par le datagramme seront protégée, et en mode tunnels, ce sera l'intégralité du datagramme qui sera protégé. **[14]**

La forme de la trame ESP est présentée ci-dessous.

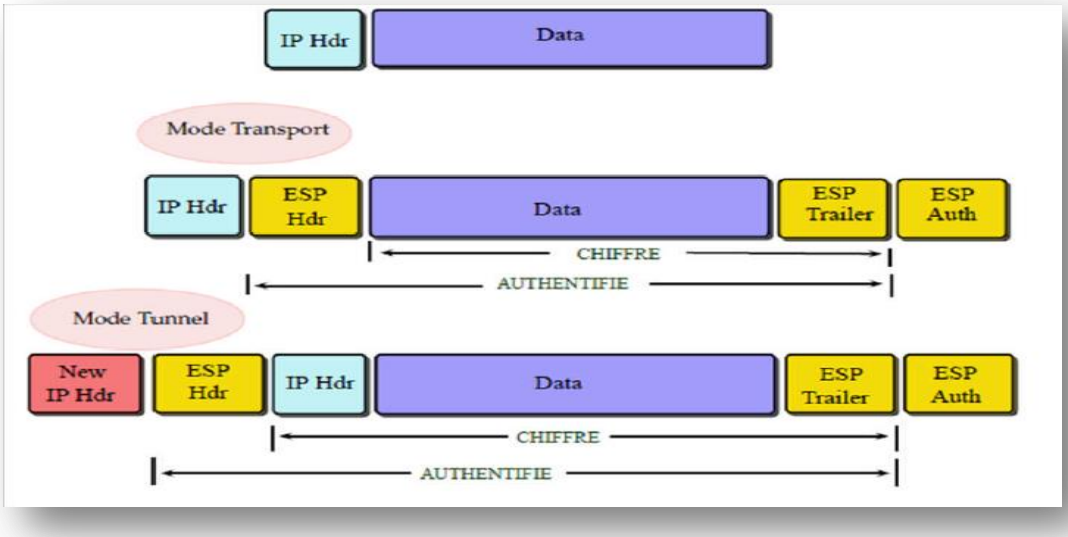

Figure 2-5 : Trame ESP en mode tunnel et transport [13]

Les méthodes de cryptage utilisées par ESP sont :

- **DES (Data Encryption Standard).**
- **3DES (Triple Data Encryption Standard).**

2.2.6.3 Le protocole AH et ESP :

Il est tout à fait possible d'utiliser les deux protocoles conjointement, même si cela reste très peu utilisé, mais lorsque l'on recherche à avoir une confidentialité des données et une authentification complète du paquet, il est possible d'utiliser dans un premier temps ESP afin de chiffrer les données et d'authentifier les champs concernés, puis d'apposer AH sur le paquet ESP obtenu. **[16]**

2.2.7 Gestion des clés pour IPSec :

La présence de mécanismes de chiffrement implique la prise en compte des problématiques de gestion de clés et de leur distribution à l'ensemble des systèmes destinés à être source et/ou destination d'une communication IPSec.

Pour la gestion et la distribution des clés, on peut, soit opter pour une gestion manuelle dans le cas de petites infrastructures, soit pour une gestion automatique, pour cela le protocole IKE (Internet Key Exchange), définie dans la RFC2409 a été défini comme protocole par défaut pour la gestion et la distribution des clés.

2.2.7.1 Différents types de clés :

- **Clés de chiffrement de clefs :** Ces clés sont utilisées afin de chiffrer d'autres clés et ont généralement une durée de vie longue, et comme les clés étant des valeurs aléatoires, l'utilisation d'autres clés pour les chiffrer rend les attaques par cryptanalyse plus difficiles à leur niveau.

- **Clés maîtresses :** Les clés maîtresses sont des clés qui ne servent pas à chiffrer mais uniquement à générer d'autres clés par dérivation, il peut ainsi être utilisée par exemple pour générer deux clés : une pour le chiffrement et l'autre pour la signature.

- **Clés de session :** Ces clefs, contrairement aux précédentes, servent à chiffrer des données. **[17]**

2.2.7.2 Infrastructure à clé publique (PKI) :

De nombreuses applications et protocoles utilisent le cryptage à clé publique sur d'importants réseaux, donc il est nécessaire de pouvoir gérer dans ce cas un nombre important de clés publiques, pour cela, on a recours à des infrastructures à clés publiques qui se basent généralement sur des autorités de certification CA (Certificate Authorities), qui garantissent l'authenticité des clés publiques et permettent une gestion hiérarchisée de celles-ci.

2.2.7.3 Échange des clefs et authentification:

La première étape lors de l'établissement d'une communication sécurisée, est l'authentification des interlocuteurs, ensuite, un échange de clé permet l'utilisation d'un mécanisme de sécurisation des échanges, notons que l'authentification est ainsi étendue à la suite de la communication. Les mécanismes de sécurisation des échanges sont :

- **Le secret de transmission parfait :** PFS (Perfect Forward Secrecy) est assurée par une renégociation régulière des clés, donc si un attaquant intercepterait et déchiffrerait une clé de session, celle-ci serait probablement déjà « périmée » avant qu'il puisse l'utiliser.

- **La protection de l'identité :** est respectée si un message intercepté ne permet pas de déterminer l'identité des tiers communiquant.

- **Protection de la circulation arrière :** « Back Traffic Protection » consiste en une génération de nouvelles clés de sessions sans utilisation de clés maîtresses, ces nouvelles clés étant indépendantes des clés précédentes, et la découverte d'une clé de session ne permet ni de retrouver les clés de session passées ni d'en déduire les clés à venir. **[18]**

2.2.7.4 Algorithme de Diffie-Hellman :

Inventé en 1976 par Diffie et Hellman, cet algorithme permet à deux tiers de générer un secret partagé sans avoir aucune information préalable l'un sur l'autre, il est basé sur un mécanisme de cryptage à clé publique, et fait donc intervenir les valeurs publiques et privées des tiers. Le secret généré à l'aide de ce protocole peut ensuite être utilisé pour dériver une ou plusieurs clés, que soit une clé secrète ou bien une clé de chiffrement de clés.

Le principe de Diffie-Hellman est comme suit : soient deux personnes A et B désirant communiquer sans utiliser une clé secrète, pour cela ils se mettent d'accord sur un canal qui n'est pas forcément sécurisé, et sur deux grands entiers premiers entre eux, « n » et « g », tels que n > g > 1, soulignons que pour que l'échange de clés soit sécurisé, il faut que « n » ait une taille de l'ordre de 512 ou 1024 bits. Ils prennent chacun chez eux un nombre aléatoire :

- A choisit un grand nombre entier aléatoire « x », puis calcule $X= g^x \bmod n$, et l'envoie à B.
- B choisit un grand nombre entier aléatoire « y », puis calcule $Y=g^y \bmod n$, et l'envoie à A.

Ensuite, chacun de leur côté :

- A calcule $k = Y^x \bmod n$.
- B calcule $k' = X^y \bmod n$.

On constate alors que $k = k' = g^{xy} \bmod n$, et donc que A et B sont parvenus à établir une clé secrète commune qui sera ensuite utilisée par un algorithme symétrique (DES par exemple). Notons que la clé publique correspond aux valeurs « X » et « Y » échangée par les deux protagonistes, et la clé privée correspond aux valeurs « x » et « y » conservée par les deux protagonistes, ainsi, le pirate peut intercepter X et Y mais il lui est très difficile d'en déduire x et y, et c'est sur ce principe que repose la sécurité de l'algorithme. **[19]**

2.2.7.5 Protocole IKE :

IKE (Internet Key Exchange) est un système développé spécifiquement pour IPSec, qui vise à fournir des mécanismes d'authentification et d'échange de clef adaptés à l'ensemble des situations qui peuvent se présenter sur l'internet. Il existe maintenant en deux versions, « IKEv1 » décrit dans le RFC 2409 de novembre 1998, et « IKEv2 » décrit dans le RFC 4306 de décembre 2005. Il faut savoir que les deux versions ne sont pas interopérables, dans lequel les deux extrémités du tunnel doivent utiliser la même version, par contre un même équipement peut parfaitement gérer certains tunnels dans la version 1 et d'autres dans la version 2.

Il est composé de plusieurs éléments, tel que le cadre générique ISAKMP et une partie des protocoles Oakley et SKEME. Lorsqu'il est utilisé pour IPSec, il est de plus complété par un « domaine d'interprétation » pour IPSec.

Le protocole IKE utilise l'infrastructure du protocole ISAKMP pour échanger des clés et définir des associations de sécurité (SA) entre deux machines, ainsi, il utilise également le protocole Oakley pour la création des clés, et le protocole SKEME pour les échanger. **[12]**

Les négociations IKE se font en deux phases, l'une permet de mettre en place un canal sécurisé afin de protéger la négociation qui se déroule lors de la deuxième phase, et l'autre permet de négocier les SA qui seront utilisées par IPSec pour protéger le trafic.

- **Phase I :**

Représente la négociation initiale afin d'établir l'association de sécurité (SA) ISAKMP entre les deux hôtes, elle peut se faire de manière robuste lorsque les conditions le permettent (notamment lorsque l'adresse IP du correspondant est connue à l'avance), il s'agit dans ce cas du « Main Mode » ou elle peut se faire par « Agressive Mode » qui ne présuppose pas la connaissance de l'IP de l'hôte.

Elle commence par envoyer la liste des propositions d'authentification, de chiffrement ainsi que les durées de vies à négocier, suivant la manière dont l'hôte distant est configuré, la négociation peut être ou ne pas être acceptée.

La deuxième étape consiste à calculer des clés de session par l'intermédiaire d'un échange Diffie-Hellman, puis une fois les clés de sessions établies, tout le trafic à partir de ce moment est chiffré. **[15]**

- **Phase II :**

Durant cette phase, les associations de sécurité (SA) IPSec sont négociées par IKE, pour sécuriser le flux de données en lui-même. Ces négociations sont déjà chiffrées et authentifiés puisqu'elles reposent sur l'association de sécurité (SA) ISAKMP fraîchement établie, on appelle également ce mode de négociation par « Quick Mode ».

Comme les associations de sécurité (SA) IPSec sont unidirectionnelles par nature, il va en suivre un double échange de clés de chiffrement, l'une pour le trafic entrant et l'autre

pour le trafic sortant. L'avantage que représente cette stratégie est de doubler le travail de l'attaquant à l'écoute du réseau, puisqu'il lui faudra déchiffrer le trafic dans les deux sens.

Durant cette phase sont négociés des paramètres comme les algorithmes de chiffrement, de calcul et de signature, les clés de chiffrement ou encore les durées de vies des différentes SA. **[15]**

2.2.7.6 Protocole ISAKMP :

Le protocole ISAKMP (Internet Security Association and Key Management Protocol), défini dans le RFC 2408, apporte une infrastructure permettant de définir et d'administrer des associations de sécurité (SA) entre deux ordinateurs devant communiquer de manière sécurisée.

Il fournit uniquement un cadre pour l'authentification et l'échange de clés, et est conçu pour être indépendant de l'échange de clés, notons que des protocoles tels que IKE (Internet Key Exchange) et KINK (Kerberized Internet Negotiation of Keys) fournissent un matériel de saisie authentifié à utiliser avec ISAKMP, par exemple: IKE décrit un protocole utilisant une partie d'Oakley et une partie de SKEME en conjonction avec ISAKMP pour obtenir du matériel de clé authentifié à utiliser avec ISAKMP.

Il définit les procédures d'authentification d'un pair communiquant, la création et la gestion d'associations de sécurité, les techniques de génération de clés et l'atténuation des menaces (comme par exemple le déni de service et les attaques par rejeu).

ISAKMP avoir un DOI (Domain Of Interpretation) défini pour être utilisé avec IPSec, ce dernier permet de spécifier les formats et les conditions requises lorsqu'ISAKMP est appliqué à IPSec. **[17]**

Il décrit actuellement cinq types d'échanges offrant des mécanismes de sécurité différents :

- Échange de base (Base exchange).
- Échange de protection d'identité (Identity protection exchange).
- Échange d'authentification unique (Authentication only exchange).
- Échange agressif (Aggressive exchange).

- Échange d'informations (Informational exchange).

2.2.7.7 Protocole Oakley :

Oakley est un protocole d'accord de clé qui permet aux parties authentifiées d'échanger des éléments de clé basé sur Diffie-Hellman avec des fonctionnalités additionnelles contre certaines attaques cryptographiques, il a été proposé par Hillarie Orman de l'université d'Arizona en 1998, et a servi de base au plus largement utilisé IKE. L'utilisation actuelle d'Oakley est avec le protocole ISAKMP pour la négociation des clés dans IPSec, il peut être utilisé avec ISAKMP (port 500) ou directement sur IP.

Les principales caractéristiques d'Oakley sont :

- Utilise les cookies contre les attaques de type DOS.
- Utilise un NONCE contre les attaques de rejeu des paquets.
- Assure une authentification contre les attaques de type « man-in-the-middle ».
- Permet au deux entités de négocier des groupes Diffie-Hellman. **[18]**

2.2.7.8 Le protocole SKEME :

SKEME (Secure Key Exchange Mechanism) est un protocole qui décrit une technique d'échange de clés permettant un renouvellement rapide des clés, il propose aussi des méthodes additionnelles comme la distribution manuelle des clés ou par un system KDC (Key Distribution Center). Développé en 1996 par Hugo Krawszyk de L'IBM spécifiquement pour IPSec. **[18]**

Il fournit quatre modes d'échange de clés:

- Un échange basé sur les clés publiques de Diffie-Hellman.
- Un échange basé sur l'utilisation des clés publiques mais sans Diffie-Hellman.
- Un échange basé sur l'utilisation d'un secret partagé et sur Diffie-Hellman.
- Un échange rapide basé uniquement sur des algorithmes symétriques.

2.3 VPN multipoints dynamique (DMVPN) :

2.3.1 Concept général et fonctionnement :

DMVPN (Dynamic Multipoint VPN) est une technique de routage que nous pouvons utiliser pour construire un réseau VPN avec plusieurs sites sans avoir à configurer statiquement tous les appareils, il s'agit d'un réseau en étoile « Hub et Spoke » où les Spokes pourront communiquer directement entre eux sans avoir à passer par le Hub.

Le chiffrement est pris en charge par IPSec, ce qui fait du DMVPN un choix populaire pour connecter différents sites en utilisant des connexions internet régulières. Il est en réalité un ensemble de technologies (IPSec, mGRE et NHRP) qui combinées pour facilite le déploiement des réseaux privés virtuels IPSec.

En général, il décrit un modèle de déploiement en étoile, dans lequel les ressources d'entreprise principales sont situées dans un site central de grande taille, avec un certain nombre de sites ou de succursales plus petits, connectés directement au site central via un VPN, comme illustré ci-dessous. **[20]**

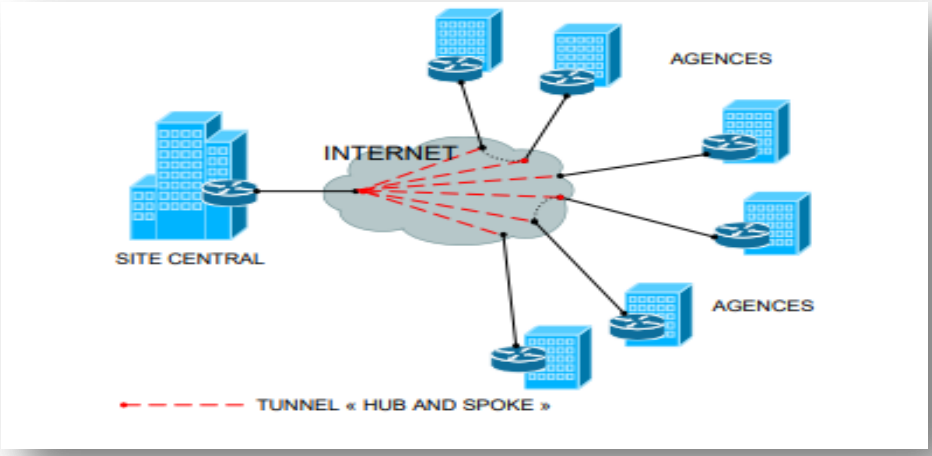

Figure 2-6 : Exemple de topologie DMVPN [20]

Son principe est de créer un tunnel GRE (Generic Routing Encapsulation) entre deux ou plusieurs réseaux différents, comme si une passerelle existait entre ces réseaux. Un routeur sera configuré en Hub et les autres routeurs seront configurés en Spoke, pour se faire, deux IGP sont utilisés : l'un pour la connectivité IP publique et monter les tunnels GRE, l'autre pour s'échanger des routes privées une fois le tunnel monté, ainsi que chaque routeur a une interface publique et une interface privée sur le même port. **[21]**

2.3.2 Avantages du DMVPN :

Les principaux avantages du DMVPN sont:

- Réduction des dépenses d'exploitation et d'immobilisation en intégrant la voix et la vidéo à la sécurité VPN.
- Simplification de la communication de la branche par une connectivité directe branche à branche pour les applications telles que la voix sur IP.
- Réduction de la complexité de déploiement par la mise en place d'une configuration simple.
- Amélioration de la résilience de l'activité en empêchant les perturbations et les services critiques.

2.3.3 Modèles de déploiement :

Le DMVPN propose deux modèles de déploiement possibles:

- **Hub-and-Spoke :**

  Dans ce modèle, chaque Spoke possède une interface GRE permettant de monter le tunnel vers le Hub, notons que chaque Hub et Spoke échangent ensuite les informations de routage IGP au travers de ce tunnel.

  Les Spokes (clients) s'enregistrent d'abord avec le Hub (serveur) en spécifiant manuellement l'adresse du Hub dans le tunnel GRE (tunnel destination), puis, ils envoient cela par l'intermédiaire du NHRP « *Registration Request* ».

  Enfin, les Hubs apprennent dynamiquement les adresses VPN (Privées) et adresses NBMA (publiques) de chaque Spoke, ainsi, tout trafic entre les Spokes passe par le Hub, donc ce modèle ne prend pas en compte les liaisons entre les Spokes. **[22]**

- **Spoke-to-Spoke :**

  Chaque Spoke doit disposer d'une interface mGRE permettant aux tunnels dynamiques de transiter vers les autres Spokes. Il lui faut apprendre l'entrée de routage sur le réseau de destination car le prochain saut doit être l'adresse IP du tunnel distant, et le Spoke doit aussi apprendre l'adresse NBMA de ce prochain saut.

Dans ces conditions le Hub peut préserver et informer les réseaux privés du prochain saut comme annoncé par les Spokes eux-mêmes, ce modèle prend en compte les liaisons entre différents Spokes et offre une grande évolutivité de la configuration pour les périphériques. **[22]**

2.3.4 Différentes phases du DMVPN :

Un DMVPN peut être déployé en trois différentes phases qui ont chacune leurs effets sur le fonctionnement de réseau existant. On peut citer que :

- Le comportement du trafic entre les Spokes est différent pour chacune des phases.
- Les designs de routage supportés par les différentes phases ne sont pas les mêmes.
- L'évolutivité du réseau est impactée par ces différentes phases.

Nous expliquons ces trois phases comme suit :

- **Phase 1 :**

  À cette phase, le Hub est utilisé pour le plan de contrôle du réseau et se trouve également dans le chemin du plan de données car il est le seul routeur qui utilise une interface GRE multipoint, et tous les Spokes utilisent des interfaces de tunnel GRE point à point régulières, cela signifie qu'il n'y aura pas de communication directe en étoile. **[23]**

  La configuration du Hub est ici simplifiée, car il n'a pas besoin de créer une table de registre NHRP pour chacun des nouveaux Spokes, d'autre part, les Spokes sont configurés pour du GRE point à point vers le Hub et enregistrent leurs IP logiques avec l'adresse NBMA sur le NHS (Next-Hop Server) qui est le Hub, afin qu'il sache les joindre dynamiquement. **[23]**

  Le protocole de routage envoie un minimum d'informations depuis le Hub vers les Spokes (route par défaut), et les Spokes annoncent leurs réseaux directement connectés au Hub qui a donc simplement besoin d'envoyer une route par défaut aux Spokes, étant donné que le trafic doit forcément remonter au Hub. **[23]**

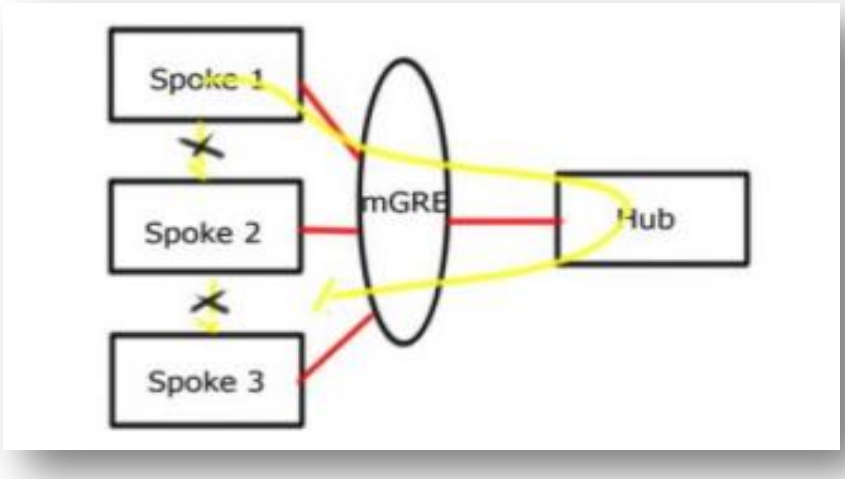

Figure 2-7 : DMVPN Phase 1 [23]

- **Phase 2 :**

Dans cette phase, le Hub est utilisé pour le plan de contrôle mais contrairement à la phase 1 pas nécessairement dans le plan de données car tous les Spokes utilisent des tunnels GRE multipoint, nous avons donc un tunnel direct « Spoke-to-Spoke ».

Lorsqu'un Spoke veut atteindre un autre Spoke, il envoie un paquet « *NHRP Resolution Request* » au Hub, et lui répond avec un paquet « *NHRP Resolution Reply* » depuis son cache et le Spoke peut alors connaitre l'adresse NBMA d'un autre Spoke et le contacter directement. **[23]**

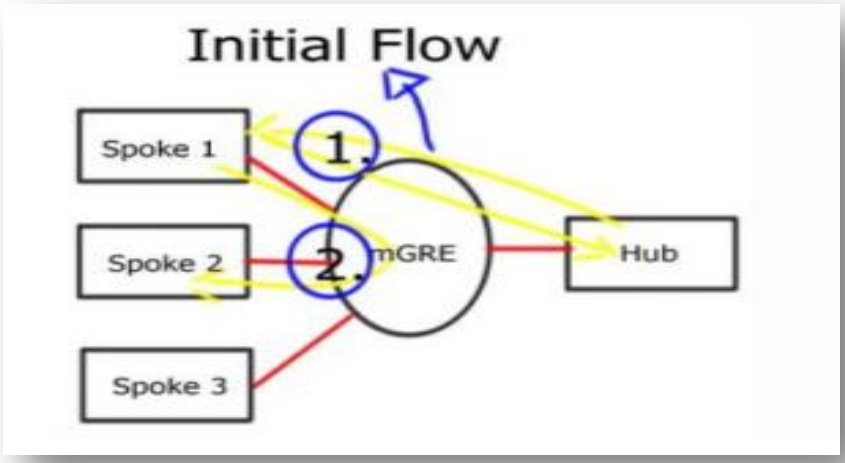

Figure 2-8 : DMVPN Phase 2 [23]

- **Phase 3 :**

Dans les phases précédentes, les Spokes ne reçoivent que la route par défaut des routeurs concentrateurs, et non les informations de routage détaillées nécessaires pour établir des tunnels en étoile.

À cette phase, nous pouvons utiliser n'importe quel protocole de routage avec n'importe quelle configuration, la redirection NHRP et les raccourcis prennent en charge les flux de trafic, cela améliore l'évolutivité de la phase 2.

En effet, on ajoute une redirection NHRP qui permet au plan de données des conversations « Spoke-to-Spoke » de joindre directement les Spokes sans passer par le Hub, ce qui fait que le Hub n'est plus le seul à détenir les informations NHRP. **[23]**

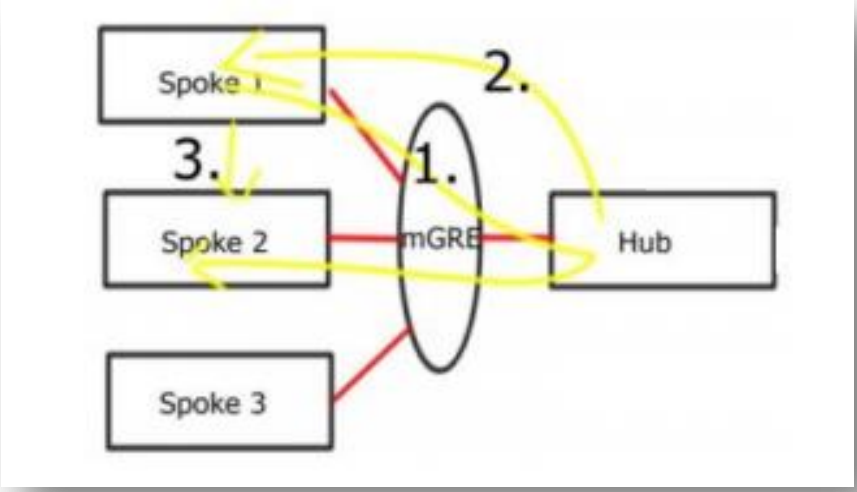

Figure 2-9 : DMVPN Phase 3 [23]

Voir ci-dessous un tableau récapitulatif des spécificités de chaque phase du DMVPN :

Tableau 2-1 : Comparaison des phases DMVPN

Phase 1	- Fonctionnalité « Hub and Spoke ». - GRE point-à-point sur les Spokes et mGRE sur le Hub. - configuration simplifié sur le Hub. - Adressage dynamique. - Supporte le protocole de routage et la multidiffusion. - Les Spokes n'ont pas besoin d'une table de routage complète.
Phase 2	- Fonctionnalité « Spoke to Spoke ». - Interface mGRE sur les Spokes. - Réduction de la charge sur les Hubs grâce au transfert de trafic direct « Spoke to Spoke ». - Les Hubs doivent s'interconnecter en chaîne. - Un Spoke doit avoir une table de routage complet. - Limitation des protocoles de routage. - Tunnel « Spoke to Spoke » déclenché par le Spoke lui-même.
Phase 3	- Possibilité de conception réseau à très grande échelle. - Rapport Spoke-Hub plus évolué. - Pas d'interconnections en chaîne. - Les Spokes n'ont pas besoin d'une table de routage complète. - Tunnel « Spoke to Spoke » déclenché par le Hub. - Pas de limitation du protocole de routage. - Route NHRP enregistrée dans le RIB.

2.3.5 Composants et terminologies :

DMVPN et en fait une combinaison des technologies suivantes :

2.3.5.1 GRE multipoint (mGRE) :

Est un protocole permettant de créer des tunnels multipoints entres différents sites, c'est-à-dire créer plusieurs tunnels à partir d'un seul pseudo interface tunnel. En ce moment, nous avons une topologie en étoile, la bonne chose à propos de DMVPN est que nous utilisons un GRE multipoint pour avoir plusieurs destinations, donc quand nous avons besoin de créer un tunnel entre une branche 1/2 ou 3/4, nous construisons automatiquement de nouveaux tunnels :

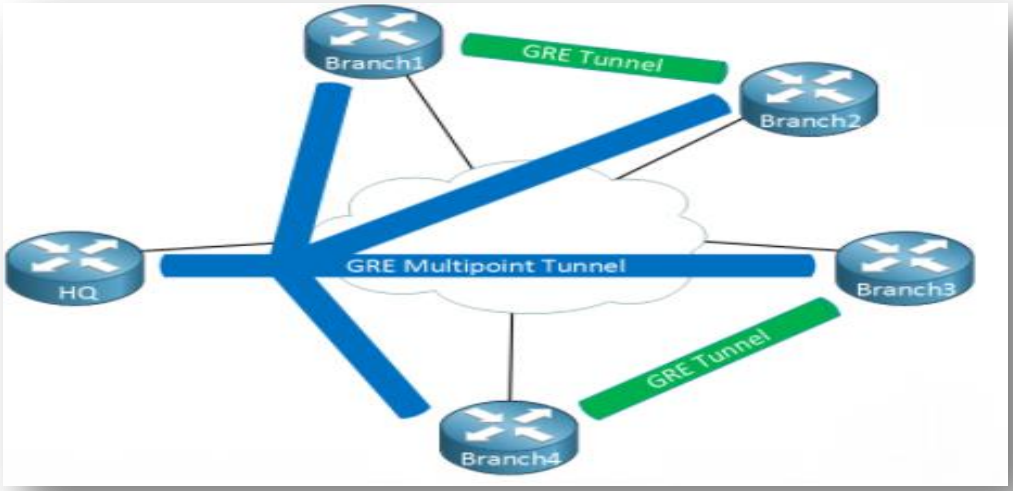

Figure 2-10 : Architecture mGRE [24]

Les adresses IP source et de destination «internes» sont connues pour être utilisées, il s'agit de l'adresse IP des interfaces de tunnel, nous encapsulons ce paquet IP, mettons un en-tête GRE devant lui, puis nous devons renseigner les adresses IP «externes» de source et de destination afin que ce paquet puisse être acheminé sur internet.

Le routeur « branch1 » connaît sa propre adresse IP publique, mais il n'a aucune idée de l'adresse IP publique de routeur « branch2 », pour résoudre ce problème, nous avons besoin de l'aide d'un autre protocole qui est NHRP. **[24]**

2.3.5.2 Protocole de résolution du prochain saut (NHRP) :

NHRP (Next Hope Resolution Protocol) est un protocole permettant aux routeurs distants de faire connaitre leur adresse IP servant à monter le tunnel GRE avec le serveur, ce dernier stocke de son côté les adresses IP pour permettre à chaque routeur de connaitre l'adresse de son voisin et ainsi établir un tunnel direct avec lui. Nous avons besoin d'aide notre routeur « branch1 » à comprendre quelle est l'adresse IP publique du routeur « branch2 », nous le faisons comme suit :

- Un routeur sera le serveur NHRP.
- Tous les autres routeurs seront des clients NHRP.
- Les clients NHRP s'enregistrent auprès du serveur NHRP et signalent leur adresse IP publique.
- Le serveur NHRP garde une trace de toutes les adresses IP publiques dans son cache.
- Lorsqu'un routeur souhaite acheminer quelque chose vers un autre routeur, il demande au serveur NHRP l'adresse IP publique de l'autre routeur. **[24]**

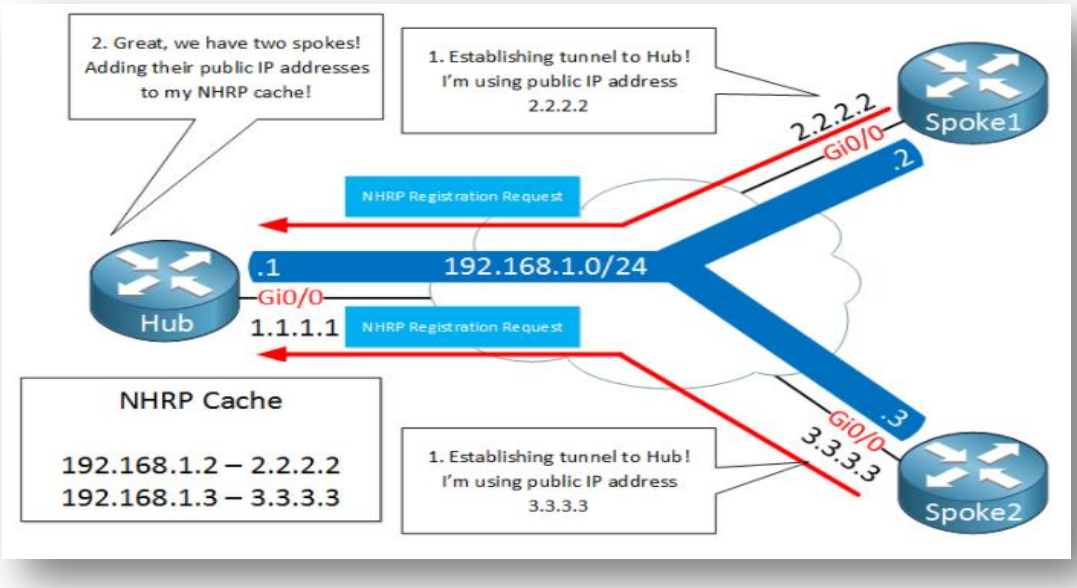

Figure 2-11 : Fonctionnement de NHRP [24]

2.3.5.3 Protocoles de routage :

La conception DMVPN recommande l'utilisation d'un protocole de routage dynamique pour propager les routes de la tête du réseau vers les succursales. Plusieurs protocoles de routage peuvent être utilisés :

- **Le protocole OSPF :**

OSPF (Open Shortest Path First) est un protocole de routage permettant au routeur du site central de propager les différentes routes aux sites distants, il permet aussi aux routeurs des sites distants d'annoncer leur réseau local au site central, il est utilisé par de nombreuses organisations comme un protocole de routage interne. **[25]**

- **Le protocole EIGRP :**

EIGRP (Enhanced Interior Gateway Routing Protocol) est le protocole de routage préféré lors de l'exécution d'un réseau DMVPN, c'est un protocole de vecteur de distance avancé, et cela le rend plus approprié pour DMVPN car il n'est pas limité par les limitations de topologie d'un protocole d'état de liaison, il peut résumer et manipuler les métriques à tout moment et n'a aucun concept de zones, cela rend beaucoup plus facile son déploiement et sa mise à l'échelle dans une topologie DMVPN. **[26]**

- **Le protocole BGP :**

BGP (Border Gateway Protocol) est un protocole de routage externe, adopté pour la connectivité entre systèmes autonomes, qui permet d'échanger des informations entre des réseaux ayant des politiques de routage différentes, et notamment d'assurer, par l'usage de vecteur de chemin, une protection contre les boucles de routage. **[27]**

2.3.5.4 Protocole de sécurité IPSec :

IPSec (Internet Protocol Security) est un protocole de chiffrement permettant de chiffrer le trafic entre deux sites, par l'utilisation des clés pré-partagées, dont nous avons discuté en détail précédemment. Il n'est pas requis mais recommandé puisque nous utilisons probablement DMVPN avec l'internet comme réseau de base, il pourrait être sage de crypter vos tunnels avec une mise en œuvre simple et rapide.

Conclusion :

Au cours de ce chapitre, nous avons discuté la notion générale d'un VPN de site à site, tout en montrant ses principaux protocoles. Nous avons commencé par le protocole de tunneling GRE qui est très utile lorsque nous possédons un réseau multi-sites et une agence qui possède une liaison sous engagement d'un opérateur tiers. Le manque de chiffrement dans ce protocole nous a fait passer au protocole de sécurité IPSec qui est une norme sûre, ouvert, et fiable pour une communication sécurisée. Ensuite, nous avons parlé de DMVPN qui permet d'établir des tunnels combinés entre IPSec et GRE directement entre les routeurs qui veulent dialoguer ensemble avec une simplicité et une scalabilité déconcertante et surtout de façon totalement dynamique.

CHAPITRE 3 : VPN d'accès à distance

Pour toute entreprise, rester en avance sur la concurrence signifie rester connecté à tout moment, chaque organisation vise donc à offrir une accessibilité complète aux ressources, même à ses travailleurs éloignés. C'est à ce moment qu'un VPN d'accès à distance entre en scène, il partage la responsabilité de votre organisation d'accorder un accès sécurisé aux ressources de l'entreprise.

Un VPN d'accès à distance permet aux utilisateurs qui travaillent à distance à se connecter au réseau privé prévu, d'accéder et d'utiliser en toute sécurité des applications et des données qui résident dans le centre de données et le siège social de l'entreprise à l'aide d'un client VPN, qui peut être basé sur le Web ou un logiciel en chiffrant tout le trafic que les utilisateurs envoient et reçoivent. De cette façon, il accorde un accès sécurisé pour les télétravailleurs qui les connecte en toute sécurité au réseau de leur organisation.

Pour ce faire, le VPN d'accès à distance crée un tunnel entre le réseau d'une organisation et un utilisateur distant qui est « virtuellement privé », même si l'utilisateur se trouve dans un lieu public, en effet, le trafic est chiffré, ce qui le rend inintelligible à toute écoute indiscrète, et donc les utilisateurs distants peuvent accéder et utiliser en toute sécurité le réseau de leur organisation de la même manière qu'ils le feraient s'ils étaient physiquement au bureau, il permet aux données d'être transmises sans qu'une organisation ait à se soucier de l'interception ou de la falsification de la communication.

Une fois la négociation du tunnel terminée, l'échanger d'une communication chiffrée avec la passerelle distante peut commencer, puis les données sont déchiffrées et partagées avec les serveurs internes. Maintenant, le serveur distant reconnaît l'utilisateur via la passerelle distante, et les données de cette passerelle transitent par le tunnel VPN sécurisé sur internet et atteignent l'utilisateur distant. **[28]**

Dans ce qui viendra, nous parlerons des technologies de Cisco dans le VPN d'accès à distance qui fournissent aux utilisateurs distants une communication sécurisée, fiable, et de bonne qualité. Ils sont divisées en deux catégories, l'une qui est « VPN basé client » comme Easy VPN et AnyConnect VPN, et l'autre qui est « VPN sans client », également appelée « Web VPN » afin que le navigateur soit celui qui joue le rôle d'un client VPN.

3.1 Easy VPN :

3.1.1 Concept général :

Easy VPN est une topologie VPN en réseau qui peut être utilisée avec une variété de routeurs, de PIX et de périphériques ASA, il simplifie considérablement la configuration et le déploiement du VPN pour les bureaux distants et les travailleurs mobiles, ainsi qu'il offre une flexibilité, évolutivité et facilité d'utilisation pour les VPN d'accès à distance, sachant que les politiques sont configurées entre les serveurs et les PC mobiles distants, exécutant le logiciel client VPN. Il implémente le protocole « Cisco Unity Client », permettant aux administrateurs de définir la plupart des paramètres VPN sur le serveur Easy VPN, simplifiant la configuration d'Easy VPN Remote.

« Security Manager » prend en charge la configuration des politiques Easy VPN sur les topologies VPN en étoile, dans une telle configuration, la plupart des paramètres VPN sont définis sur le serveur Easy VPN, qui agit comme le périphérique Hub, ainsi que les politiques gérées de manière centralisée sont poussées vers les périphériques clients Easy VPN par le serveur, ce qui minimise la configuration des périphériques distants (Spokes).

Le serveur Easy VPN peut être un routeur Cisco IOS, un pare-feu PIX ou un périphérique de la série ASA 5500, d'ailleurs, le client Easy VPN est pris en charge sur les pare-feu PIX 501, 506, 506E exécutant PIX 6.3. **[29]**

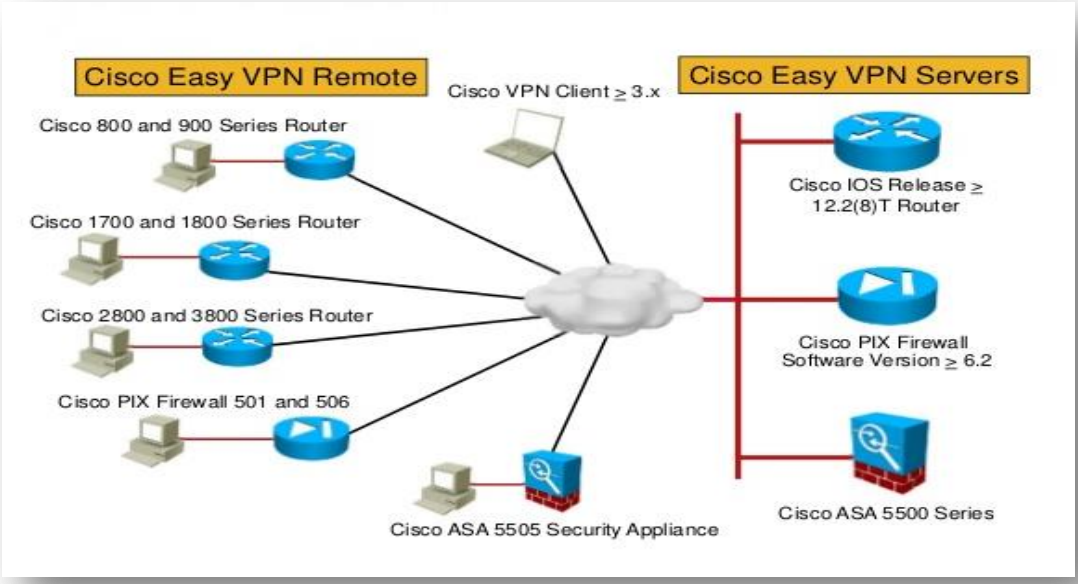

Figure 3-1 : Serveurs et clients pris en charge par Cisco EzVPN [29]

3.1.2 Interfaces d'EzVPN :

En règle générale, lors du démarrage de l'ASA, Easy VPN détermine l'interface de niveau de sécurité le plus élevé pour l'utiliser comme une interface sécurisée interne, et l'interface de niveau de sécurité le plus bas pour l'utiliser comme une interface externe sur laquelle le client VPN lance le tunnel vers la tête de réseau.

Au démarrage du système, les interfaces externes et internes d'Easy VPN sont déterminées par leur niveau de sécurité. L'interface physique avec le niveau de sécurité le plus bas est utilisée pour la connexion externe à un serveur Easy VPN, et 'interface physique avec le niveau de sécurité le plus élevé est utilisée pour la connexion intranet afin de sécuriser les ressources. Si Easy VPN détermine qu'il existe deux interfaces ou plus avec le même niveau de sécurité le plus élevé, il deviendra inactif. **[29]**

3.1.3 Processus de connexion :

Easy VPN utilise des tunnels IPSec IKEv1, la configuration du client matériel Easy VPN Remote doit être compatible avec la configuration VPN sur le serveur Easy VPN. Si nous utilisons des serveurs secondaires, leur configuration doit être identique à celle du serveur principal.

Easy VPN Remote configure l'adresse IP du serveur Easy VPN principal et, en option, jusqu'à 10 serveurs (de sauvegarde) secondaires. S'il est impossible de configurer le tunnel vers le serveur principal, le client tente de se connecter au premier serveur VPN secondaire, puis descend de manière séquentielle dans la liste des serveurs VPN à des intervalles de 8 secondes. Si le tunnel de configuration vers le premier serveur secondaire échoue et que le serveur principal se met en ligne pendant ce temps, le client procédera à la configuration du tunnel vers le deuxième serveur VPN secondaire.

Par défaut, le client matériel et le serveur Easy VPN encapsulent IPSec dans des paquets UDP (User Datagram Protocol), mais certains environnements, tels que ceux avec certaines règles de pare-feu ou les périphériques NAT et PAT, interdisent UDP, donc pour utiliser le protocole de sécurité d'encapsulation standard (ESP, protocole 50) ou l'échange de clés internet (IKE, UDP 500) dans de tels environnements, nous devons configurer le client et le serveur pour encapsuler IPSec dans les paquets TCP afin d'activer le tunneling sécurisé. Cependant, si notre environnement autorise UDP, la configuration d'IPSec sur TCP ajoute une surcharge inutile. **[29]**

3.1.4 Modes de fonctionnement :

Le mode détermine si les hôtes derrière Easy VPN Remote sont accessibles ou non depuis le réseau de l'entreprise via le tunnel. Nous avons deux modes de fonctionnement :

- **Le mode client :**

  Également appelé mode de traduction d'adresse de port (PAT), isole tous les appareils du réseau privé Easy VPN Remote de ceux du réseau d'entreprise, il permet aux appareils du site client d'accéder aux ressources du site central, mais interdit l'accès au site central pour les ressources du site client, ainsi que le réseau et les adresses du côté privé d'Easy VPN Remote sont masqués et ne sont pas accessibles directement. En ce mode, une seule adresse IP est transmise au client distant depuis le serveur lorsque la connexion VPN est établie, cette adresse est typiquement une adresse routable dans l'espace d'adressage privé du réseau client.

  Tout le trafic passant par le tunnel Easy VPN subit une traduction d'adresse de port (PAT) vers cette seule adresse IP poussée. La gestion des adresses IP n'est pas requise pour l'interface interne de client Easy VPN ou les hôtes internes. **[29]**

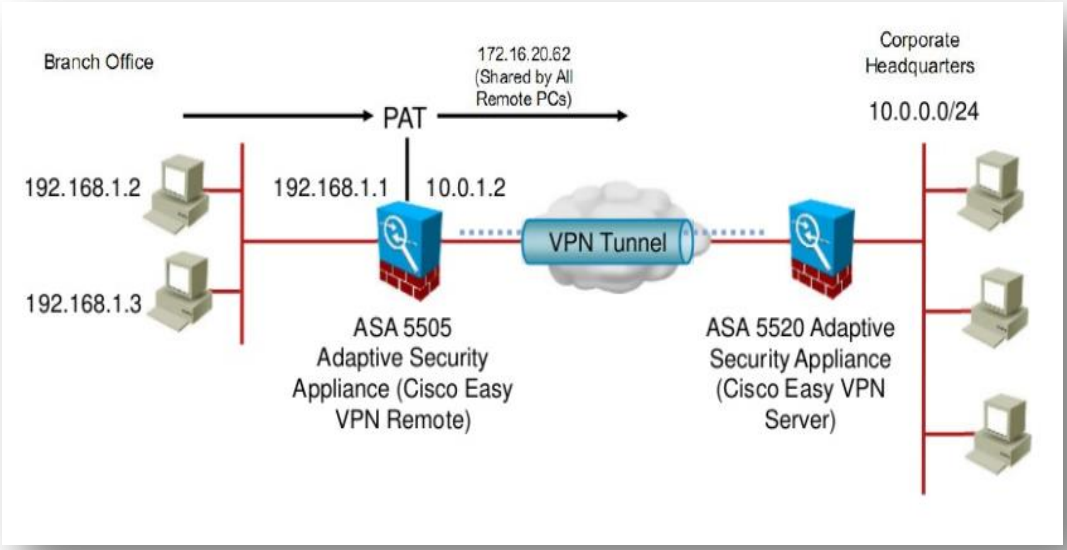

Figure 3-2 : Le mode client [29]

- **Le mode d'extension de réseau :**

NEM (Network-Extension Mode) rend l'interface interne et tous les hôtes internes routables sur le réseau de l'entreprise via le tunnel, vu qu'il spécifie que les hôtes à l'extrémité client du tunnel VPN doivent recevoir des adresses IP entièrement routables et accessibles par le réseau de destination. Il permet aux utilisateurs du site central d'accéder aux ressources réseau du site client et permet aux PC et aux hôtes clients d'accéder directement aux PC et aux hôtes du site central, notons que les hôtes du réseau interne obtiennent leurs adresses IP à partir d'un sous-réseau accessible (statiquement ou via DHCP) préconfiguré avec des adresses IP statiques.

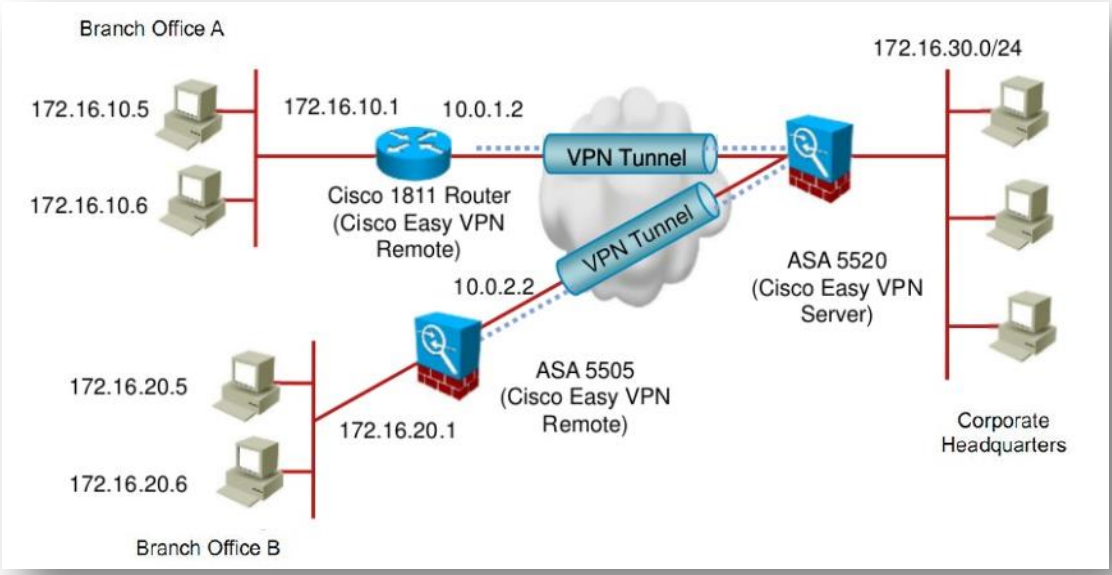

Figure 3-3 : Le mode d'extension réseau [29]

Il existe une amélioration du mode d'extension réseau, qui ne peut être configuré que sur les routeurs IOS, il permet d'attribuer automatiquement une adresse IP reçue via la configuration de mode à une interface de bouclage disponible, cette adresse IP peut être utilisée pour se connecter à votre routeur pour la gestion et le dépannage à distance (Ping, Telnet et Secure Shell), d'ailleurs, si nous sélectionnons cette option et que certains clients ne sont pas des routeurs IOS, ces clients sont configurés en mode d'extension réseau (NEM). **[29]**

3.2 Mobilité sécurisée AnyConnect VPN :

3.2.1 Concept général :

Les employeurs veulent créer des environnements de travail flexibles où les employés et les partenaires peuvent travailler n'importe où sur n'importe quel appareil, mais ils veulent également protéger les intérêts et les actifs de l'entreprise contre les menaces internet à tout moment et assure donc une sécurité permanente.

Cisco propose « AnyConnect Secure Mobility » pour étendre le périmètre du réseau aux points de terminaison distants, permettant l'intégration transparente des services de filtrage web offerts par l'Appliance de sécurité web. Il offre une nouvelle façon innovante de protéger les utilisateurs mobiles sur des plates-formes informatiques ou de téléphones intelligents, offrant une expérience plus transparente et toujours protégée pour les utilisateurs finaux et une application complète des politiques pour les administrateurs informatiques.

Cisco AnyConnect est un agent de point de terminaison de sécurité unifié qui fournit plusieurs services de sécurité pour protéger l'entreprise. Il offre également la visibilité et le contrôle dont vous avez besoin pour identifier qui et quels appareils accèdent à l'entreprise étendue. C'est une collection de fonctionnalités des produits Cisco suivants :

- Appliance de sécurité Web Cisco (WSA).
- Appliance de sécurité adaptative (ASA) de la gamme Cisco ASA 5500.
- Client Cisco AnyConnect.

Client Cisco AnyConnect est un client VPN propriétaire permettant de se connecter aux concentrateurs VPN Cisco. Il s'agit du client de nouvelle génération de l'éditeur, le premier à inaugurer le support des systèmes 64 bits grand public, il supporte les fonctionnalités IPSec et remplace le client d'ancienne génération « Cisco VPN Client ». Il fournit des connexions SSL et IPSec / IKEv2 sécurisées à l'ASA pour les utilisateurs distants.

Lorsque le client négocie une connexion SSL VPN avec l'ASA, il se connecte à l'aide de TLS (Transport Layer Security), et éventuellement, DTLS (Datagram Transport Layer Security). Ce dernier évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore les performances des applications en temps réel sensibles aux retards de paquets. **[30]**

3.2.2 Principe de fonctionnement :

Les utilisateurs distants et mobiles utilisent le client VPN sécurisé Cisco AnyConnect pour établir des sessions VPN avec l'Appliance de sécurité adaptative(ASA). Ce dernier envoie le trafic web à l'Appliance de sécurité web (WSA) avec des informations identifiant l'utilisateur par adresse IP et nom d'utilisateur, puis le WSA analyse le trafic, applique des politiques d'utilisation acceptables et protège l'utilisateur contre les menaces de sécurité. L'ASA renvoie tout le trafic jugé sûr et acceptable pour l'utilisateur.

Toute l'analyse du trafic internet est effectuée par l'Appliance de sécurité web, et non par le client sur l'appareil mobile, cela améliore les performances globales en ne surchargeant pas l'appareil mobile, dont certains ont une puissance de traitement limitée. De plus, en analysant le trafic internet sur le réseau, nous pouvons mettre à jour plus facilement et plus rapidement les mises à jour de sécurité et les politiques d'utilisation acceptable. **[30]**

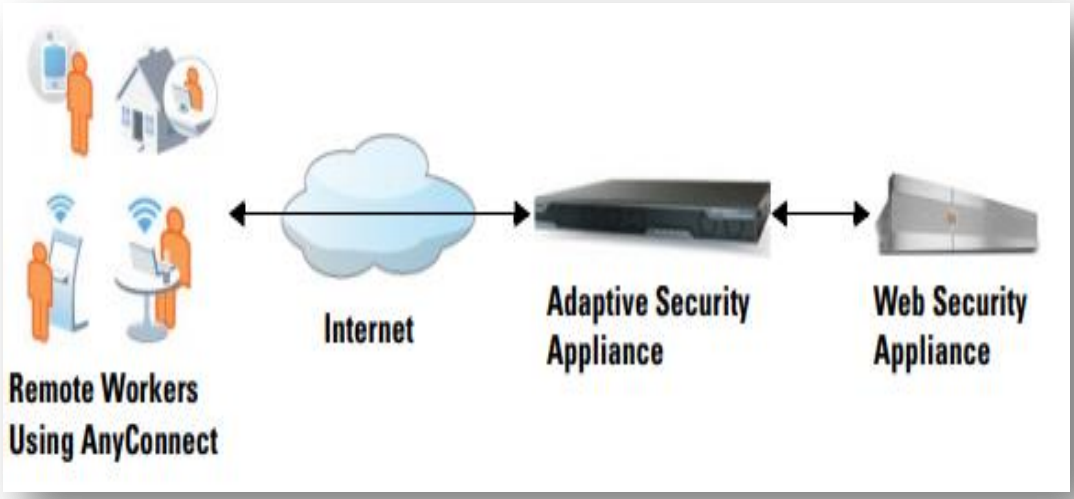

Figure 3-4 : Interaction produits Cisco pour AnyConnect [30]

3.2.3 Objectifs et fonctionnalités :

Grâce au client Cisco AnyConnect, les équipes informatiques seront en mesure d'identifier les vulnérabilités d'un réseau, les angles morts et les profils d'utilisateurs considérés comme à risque, cela permettra aux administrateurs de générer des rapports exploitables en vue de gérer l'exportation des données et de se prémunir

contre toutes sortes d'attaques issues de logiciels malveillants. Ainsi, avec Cisco Anyconnect, les entreprises seront en mesure de fournir un cryptage de grande qualité à tous leurs employés grâce à l'IPSec IKEv2 souhaitant accéder au réseau.

Cisco AnyConnect répond aux défis d'une main-d'œuvre mobile en offrant les fonctionnalités suivantes :

- **Connectivité sécurisée et persistante :**

  La connexion est sécurisée car l'utilisateur et l'appareil doivent être authentifiés et validés avant de pouvoir accéder au réseau, d'ailleurs, elle est persistante car AnyConnect est généralement configuré pour être toujours activé même lors de l'itinérance entre les réseaux. Bien qu'AnyConnect soit toujours activé, il est également suffisamment flexible pour appliquer différentes politiques en fonction de l'emplacement, permettant aux utilisateurs d'accéder à internet dans une situation de « portail captif », lorsque les utilisateurs doivent accepter les termes de l'accord avant d'accéder à internet. **[30]**

- **Sécurité persistante et application des politiques :**

  L'Appliance de sécurité web (WSA) applique des politiques contextuelles, notamment en appliquant des politiques d'utilisation acceptables et une protection contre les logiciels malveillants pour tous les utilisateurs, y compris les utilisateurs mobiles. Il accepte également les informations d'authentification des utilisateurs. **[30]**

3.2.4 Avantages et caractéristiques :

Mobilité sécurisée AnyConnect présentes les avantages suivantes :

- **Pour les utilisateurs finaux :**
  - Accès hautement sécurisé sur les PC et appareils mobiles courants.
  - Expérience utilisateur cohérente.
  - Connectivité intelligente, fiable et toujours active.
- **Pour les administrateurs de sécurité :**
  - Faible coût total de possession d'un seul client fournissant plusieurs services
  - Sécurité des points de terminaison contextuelle, complète et continue.
  - Étendre l'accès flexible et basé sur des politiques aux ressources de l'entreprise via les réseaux filaire, sans fil et VPN.

Elle présente ainsi les différentes caractéristiques, indiquées dans le tableau ci-dessous :

Tableau 3-1 : Différentes caractéristiques AnyConnect

Caractéristiques	Description
Conformité unifiée des terminaux	Le module de posture « Cisco AnyConnect ISE » fournit des contrôles de posture unifiés des points de terminaison et une correction automatisée. Il sert de source principale de vérification de la posture des terminaux pour les niveaux de système d'exploitation, les dernières mises à jour antivirus/spywares/malwares, l'inventaire des applications et du matériel et d'autres vérifications des terminaux pour déterminer l'état de conformité et renforcer la sécurité des terminaux. Pour les environnements VPN uniquement, l'Appliance de sécurité adaptative Cisco fournit une posture de point de terminaison à l'aide du module « Cisco AnyConnect Hostscan ».
Sécurité Web	En combinant la sécurité Web et l'accès VPN, les administrateurs peuvent fournir une mobilité complète et hautement sécurisée à tous les utilisateurs finaux. Les entreprises ont le choix entre plusieurs déploiements pour défendre le réseau contre les logiciels malveillants sur le web et pour contrôler et protéger l'utilisation du Web.
Protection hors réseau	Que les utilisateurs désactivent le VPN ou oublient de l'activer, « Cisco Umbrella Roaming » applique la sécurité au niveau de la couche DNS pour se protéger contre les logiciels malveillants, le phishing et les rappels de commande et de contrôle sur n'importe quel port ou protocole.
Prise en charge des appareils mobiles	Les services VPN peuvent être déployés sur les appareils les plus populaires utilisés par la main-d'œuvre diversifiée d'aujourd'hui.

3.3 VPN sans client :

3.3.1 Concept général :

Le VPN sans client (Clientless VPN) permet aux utilisateurs finaux d'accéder en toute sécurité aux ressources du réseau d'entreprise de n'importe où à l'aide d'un navigateur web compatible SSL. L'utilisateur s'authentifie d'abord avec une passerelle VPN sans client, qui permet ensuite à l'utilisateur d'accéder aux ressources réseau préconfigurées.

Il crée un tunnel VPN sécurisé d'accès à distance vers une ASA à l'aide d'un navigateur web sans nécessiter de client logiciel ou matériel. Il offre ainsi un accès sécurisé et facile à une large gamme de ressources web et à des applications web et héritées à partir de presque tous les appareils pouvant se connecter à internet via HTTP.

Il utilise le protocole Secure Sockets Layer et son successeur, Transport Layer Security (SSL/TLS) pour fournir une connexion sécurisée entre les utilisateurs distants et des ressources internes spécifiques et prises en charge que nous configurons en tant que serveur interne.

L'ASA reconnaît les connexions qui doivent être mandatées, et le serveur HTTP interagit avec le sous-système d'authentification pour authentifier les utilisateurs. L'administrateur réseau fournit l'accès aux ressources aux utilisateurs de sessions VPN sans client sur une base de groupe, et donc les utilisateurs n'ont pas d'accès direct aux ressources du réseau interne. **[31]**

3.3.2 Principe de fonctionnement :

Dans une connexion VPN SSL sans client, l'Appliance de sécurité adaptative (ASA) agit comme un proxy entre le navigateur web de l'utilisateur final et les serveurs web cible.

Lorsqu'un utilisateur se connecte à un serveur web compatible SSL, l'ASA établit une connexion sécurisée et valide le certificat SSL du serveur. Le navigateur ne reçoit jamais le certificat présenté, il ne peut donc pas examiner et valider le certificat.

L'implémentation actuelle du VPN sans client sur l'Appliance de sécurité adaptative ne permet pas la communication avec les sites qui présentent des certificats expirés. Il n'effectue pas non plus de validation de certificat d'autorité de certification de confiance sur ces sites SSL. Par conséquent, les utilisateurs ne bénéficient pas de la validation par

certificat des pages fournies à partir d'un serveur web compatible SSL avant d'utiliser un service compatible web. **[31]**

3.3.3 Avantages et caractéristiques :

- L'intégration parfaite avec la majorité des pare-feu permet de compléter l'infrastructure réseau sans avoir à acheter de matériel supplémentaire.
- Grâce au fonctionnement sans client de ces solutions, il n'est plus nécessaire d'installer ni de mettre à jour des clients VPN sur les différents ordinateurs, d'où un gain à la fois de temps et d'argent.
- Contrairement aux licences par tunnel, la licence illimitée en nombre d'utilisateurs réduit de manière significative les coûts liés au déploiement d'une solution d'accès distant sécurisée et évolutive.
- Offre des options évoluées, telles que l'accès à des ressources, services et applications supplémentaires sur le réseau de l'entreprise.
- Le contrôle granulaire de la configuration des règles permet aux administrateurs de limiter l'accès des utilisateurs à certaines ressources et d'en empêcher la visualisation ou l'utilisation sans autorisation.
- La personnalisation du portail par interface web permet d'afficher uniquement les ressources accessibles à l'utilisateur conformément aux règles de l'entreprise.
- La technologie de filtrage applicatif, analyse le trafic à la recherche de virus, vers, chevaux de Troie, logiciels espions ou autres menaces.

Conclusion :

Au cours de ce chapitre, nous avons discuté la notion générale d'un VPN d'accès à distance, puis nous avons parlé sur les technologies de Cisco dans ce type VPN, tout en montrant le concept général, le fonctionnement, et les avantages pour chacune.

CHAPITRE 4 : Implémentation et simulation

Dans ce chapitre nous allons en premier lieu, définir l'environnement du travail à utiliser qui est l'émulateur GNS3 (version 2.2.21), ce dernier pourra nous servir à reproduire une architecture physique ou logique complète du réseau avant la mise en production, ainsi tous les autres outils utilisés. Et en second lieu, nous décrirons la procédure de configuration et illustrons les différents tests d'évaluations garantissant le succès de l'implémentation réalisée pour le e-learning et le télétravail.

4.1 Description de l'environnement du travail :

4.1.1 Simulateur de réseau graphique GNS 3 :

GNS3 (Graphical Network Simulator), est un simulateur graphique de réseau qui permet de créer des topologies de réseaux complexes et d'établir des simulations. Il est un excellent outil pour l'administration des réseaux Cisco, qui est utilisé pour reproduire des différents systèmes d'exploitation dans un environnement virtuel, il permet aussi l'émulation en exécutant un IOS Cisco (Internet-work Operating Systems).

Pour fournir des simulations complètes et précises, GNS3 est fortement lié à :

- **Dynamips :** est un émulateur de routeurs Cisco capable de faire fonctionner des images Cisco IOS non modifiées, comme si elles s'exécutaient sur de véritables équipements. Son rôle n'est pas de remplacer de véritables routeurs, mais de permettre la réalisation de maquettes complexes avec de vraies versions d'IOS.

- **Dynagen :** est un produit complémentaire écrit en Python, s'interfaçant avec « Dynamips » grâce au mode hyperviseur, pour facilite la création et la gestion de maquettes grâce à un fichier de configuration simple décrivant la topologie du réseau à simuler et une interface texte interactive.

- **Qemu :** est une machine source de l'émulateur et de virtualisation générique et ouverte. Il est utilisé par GNS 3 pour exécuter Cisco ASA, PIX et IDS ainsi que tout système d'exploitation classique.

4.1.2 Images IOS :

Un IOS est un Système d'exploitation pour l'interconnexion des réseaux, il est administrable en lignes de commandes, propres aux équipements de systèmes Cisco. GNS3 est un logiciel de simulation qui utilise les IOS des routeurs Cisco, alors avant tout implémentation il faut intégrer les IOS Cisco dans le logiciel.

4.1.3 Objectif et avantages de GNS 3 :

L'utilisation d'un simulateur tel que GNS3 est très pratique pour la mise en point et l'évolution des configurations sur une maquette avant de les déployer en environnement de production. Son objectif est d'apporter aux étudiants et aux professionnels travaillant dans le domaine de l'administration systèmes et réseaux des nouvelles technologies de communication.

GNS 3 fournit les avantages suivants :

- Possibilité de capture des trames traversant un lien.
- Sauvegarde complète de toutes les configurations dans le répertoire projet.
- Permet de simuler des réseaux complexes composés d'équipements variés (routeurs, commutateurs, firewalls, IDS).
- tous les protocoles sont disponibles et exploitable en fonction de l'IOS ajouté, et il a même la possibilité d'ajouter une machine hôte ou une machine virtuelle à l'architecture. **[32]**

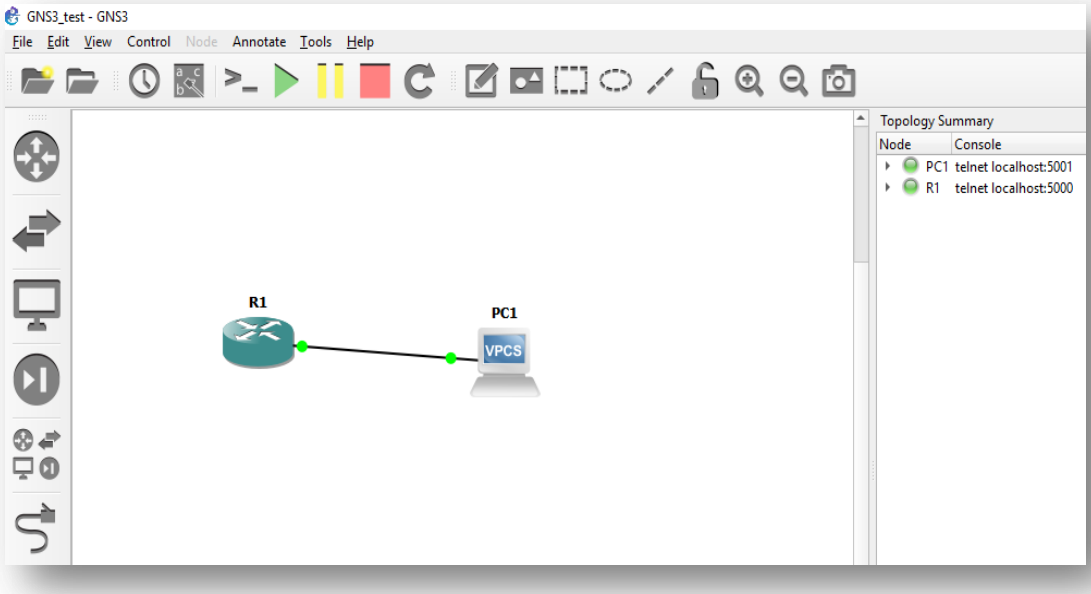

Figure 4-1 : L'environnement GNS 3

4.1.4 Autres outils utilisés :

4.1.4.1 L'analyseur Wireshark :

Wireshark est un analyseur de protocole gratuit pour Windows, Unix et ses dérivés, il permet d'examiner des trames à partir d'un fichier ou directement en les capturant sur le réseau. Il est possible d'obtenir un résumé ainsi qu'un décodage détaillé pour chaque paquet. En outre, ce logiciel possède des fonctionnalités très utiles comme les filtres de capture et d'affichage, et la reconstitution du flux d'une session TCP, de plus, le nombre de protocoles reconnus par l'analyseur est très élevé.

Son utilité est indéniable pour contrôler le bon fonctionnement de réseau, vérifier les trames transitant sur une interface d'un commutateur, et analyser les trafics inutiles ou ceux impactant les performances du réseau.

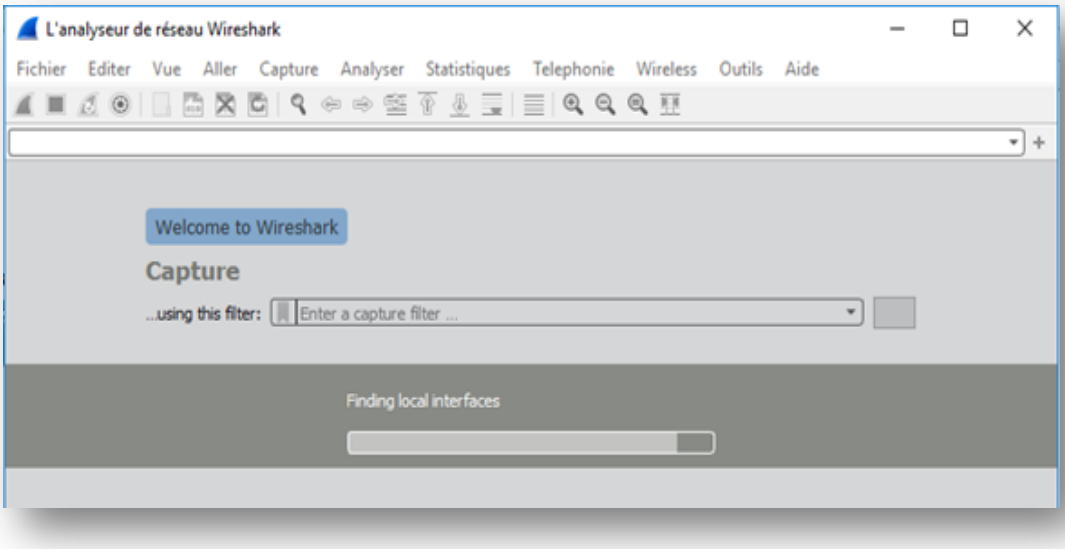

Figure 4-2 : L'analyseur de réseau Wireshark

4.1.4.2 VMware Workstation 16 Pro :

VMware (Virtual Machine) est un logiciel qui permet la création d'une ou plusieurs machines virtuelles, quand nous n'avons pas beaucoup de partitions et que nous voulons exécuter plusieurs systèmes d'exploitation et applications sur le même serveur physique, ou hôte. Les machines virtuelles sont reliées au réseau local avec une adresse IP différentes peuvent fonctionner en même temps, la limite dépond des performances de la machine hôte.

Les caractéristiques des VM offrent plusieurs avantages :

- **Partitionnement :**
  - Exécuter plusieurs systèmes d'exploitation sur une machine physique.
  - Répartir les ressources système entre les machines virtuelles.
- **Isolation :**
  - Assurer l'isolation des pannes et la protection de la sécurité au niveau matériel.
  - Maintenir les performances en déployant des contrôles avancés des ressources.
- **Encapsulation :**
  - Enregistrer dans des fichiers l'état complet des différentes machines virtuelles.
  - Déplacer et copiez des machines virtuelles aussi facilement que des fichiers.
- **Interopérabilité du matériel :**
  - Provisionner ou migrer n'importe quelle machine virtuelle vers n'importe quel serveur physique.

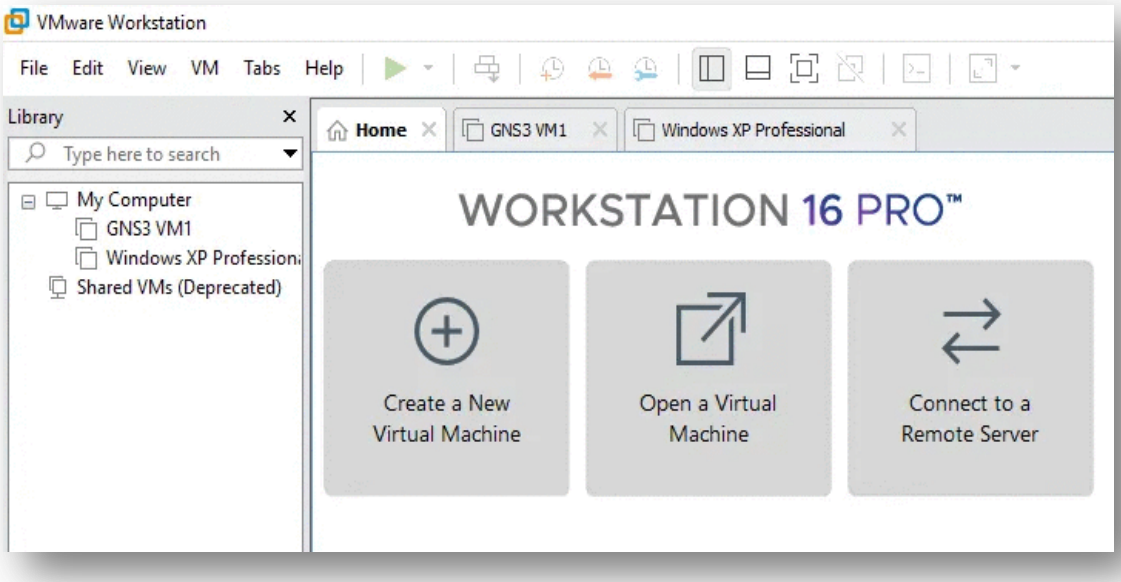

Figure 4-3 : Logiciel de virtualisation VMware Workstation 16 Pro

4.1.4.3 VPN client Cisco :

Cisco VPN Client est un client VPN utilisé dans le cadre d'infrastructures gérant des milliers de connexions, on le retrouve donc le plus souvent dans les grandes entreprises et de nombreuses universités. Il permet d'établir des connexions VPN auprès des concentrateurs VPN, des pare-feu PIX / ASA, et des routeurs IOS.

C'est un logiciel multiplateforme, compatible avec diverses versions de Windows, Mac OS X, Linux et Solaris. La version 5.0 que nous avons utilisés, est une version exclusivement réservée à Windows.

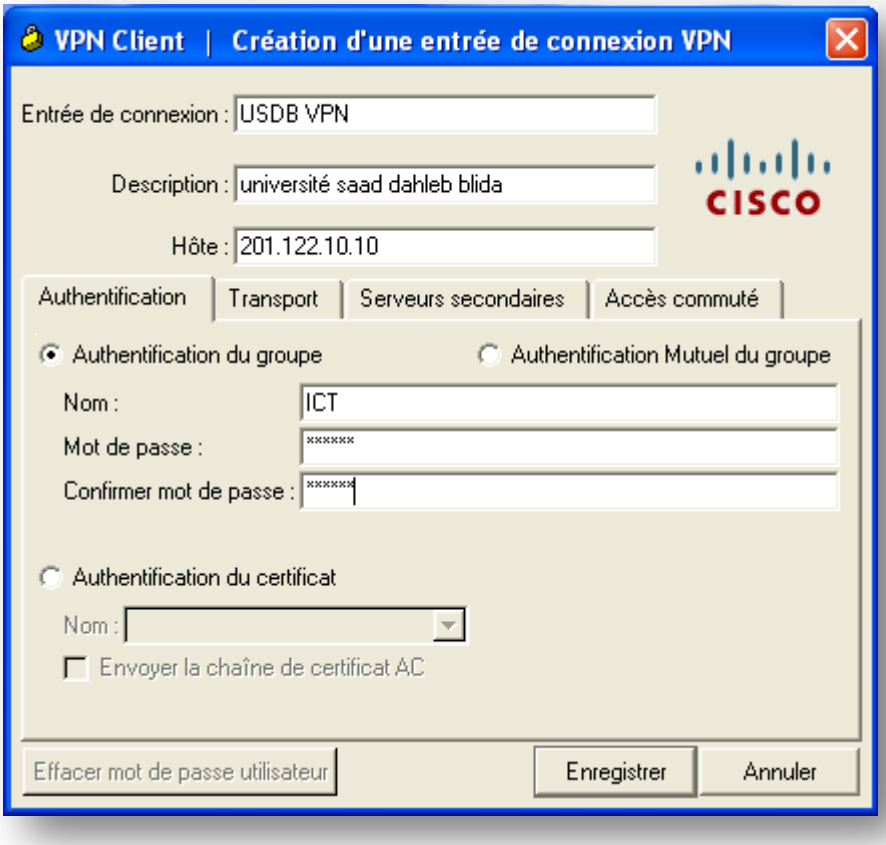

Figure 4-4 : Client VPN Cisco

4.2 VPN pour l'enseignement :

4.2.1 Problématique :

L'enseignement à distance ou « E-learning » est un moyen d'étudier sans avoir à aller à l'école pour suivre des cours. C'est une solution particulièrement intéressante pour les personnes qui ont une activité de jour (salariés, mères au foyer, etc.), sont à l'étranger ou ne peut pas voyager. Dans la période récente, coïncidant avec l'épidémie de Covid 19, qui a imposé une fermeture complète, le besoin d'éducation à distance est devenu essentiel.

Le réseau scolaire est probablement le principal moyen d'accéder à internet pour les enseignants, ce qui peut rendre ce réseau vulnérable aux fuites. Pour les étudiants, l'accès aux e-learning se fait via l'internet ouvert. Cela peut exposer leur trafic à des cyberattaques et à d'autres méthodes d'espionnage des données des enseignants, telles que les questions des examens et les devoirs, pour les transmettre aux étudiants. Et dans une plus large mesure, modifier les résultats et les notes des examens des étudiants, ainsi que leurs informations personnelles. Cela signifie que la nécessité de protéger les enseignants et les élèves de l'enseignement à distance contre les attaques en ligne est une nécessité urgente dans ce cas.

Notre cas d'étude vise sur un site e-learning de l'université SAAD Dahleb Blida pour l'enseignement à distance. Se pose alors la problématique d'accès par les étudiants nomades et les enseignants aux e-learning USDB, en toute sécurité et performance.

4.2.2 Solution proposée :

Le principal avantage d'Easy VPN est que les politiques IPSec sont gérées de manière centralisée sur le serveur (routeur principal fournissant la fonctionnalité IPSec) et sont transmises aux appareils clients, cela nécessite une configuration minimale du côté de l'utilisateur final, nous accordons donc une solution d'interconnexion fiable, moins couteuse et rapide à mettre en place.

C'est pourquoi nous avons choisi cette solution afin d'interconnecter les étudiants et les enseignants nomades au site E-learning USDB, afin d'assure la sécurité et la performance de cette connexion grâce à un simple accès internet et ce quel que soit le débit ou l'endroit où se trouve ses derniers.

La figure suivante illustre l'architecture de la solution proposée :

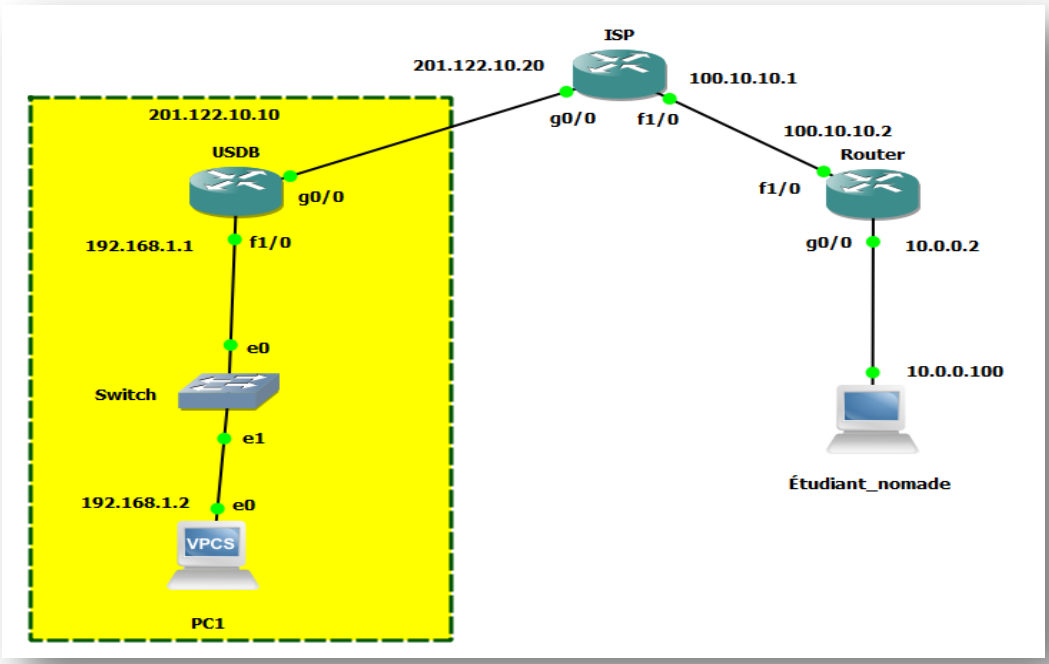

Figure 4-5 : Topologie d'un VPN accès à distance pour e-learning

4.2.3 Configuration du poste client :

Nous avons créé une machine virtuelle « Windows xp » à l'aide de VMware Workstation 16 pro pour un étudiant nomade, la figure suivante montre la configuration d'adresse IP de cette machine cliente :

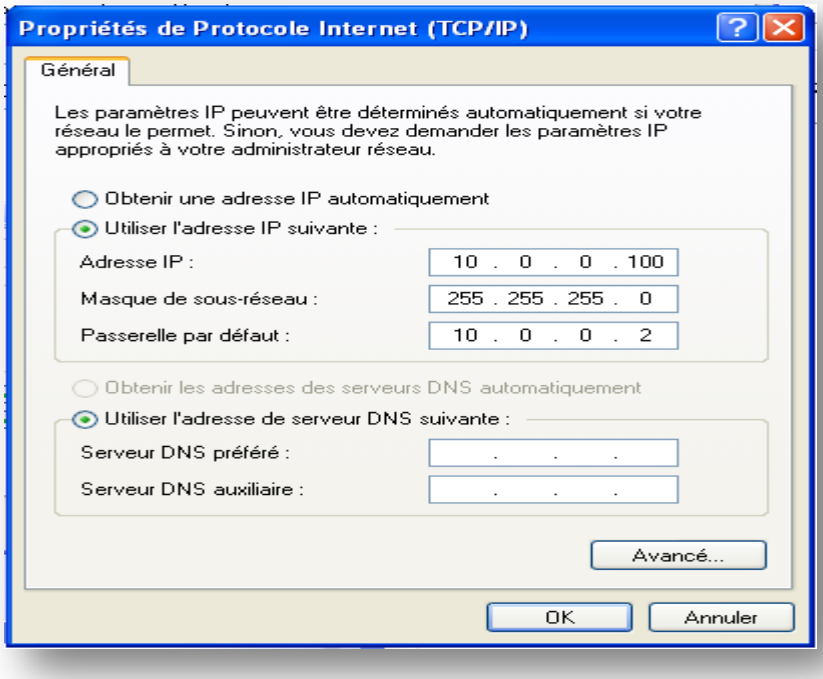

Figure 4-6 : Configuration de machine cliente "Étudiant nomade"

4.2.4 Configuration des routeurs :

4.2.4.1 Configuration des interfaces :

Nous allons changer les noms des routeurs, puis configurer et activer leurs différentes interfaces, et les mets directement connectés comme c'est présenté ci-dessous :

- **Routeur R1 *(ISP) :***

```
R1#conf t
R1 (config)#hostname ISP
ISP (config)#int g0/0
ISP (config-if)#ip address 201.122.10.20   255.255.255.0
ISP (config-if)#no shutdown
ISP (config-if)#exit
ISP (config)#int f1/0
ISP (config-if)#ip address 100.10.10.1   255.255.255.0
ISP (config-if)#no shutdown
ISP (config-if)#exit
ISP (config)#ip route 192.168.1.0   255.255.255.0   201.122.10.20
ISP (config)#ip route 10.0.0.0   255.255.255.0   100.10.10.1
```

- **Routeur R2 *(USDB) :***

```
R2#conf  t
R2 (config)#hostname USDB
USDB (config)#int g0/0
USDB (config-if)#ip address 201.122.10.10   255.255.255.0
USDB (config-if)#no shutdown
USDB (config-if)#exit
USDB (config)#int f1/0
USDB (config-if)#ip address 192.168.1.1   255.255.255.0
USDB (config-if)#no shutdown
USDB (config-if)#exit
USDB (config)#ip route 0.0.0.0   0.0.0.0   201.122.10.20
```

- **Routeur R3 *(Router) :***

```
R3#conf t
R3 (config)#hostname Router
Router (config)#int f1/0
Router (config-if)#ip address 100.10.10.2   255.255.255.0
Router (config-if)#no shutdown
Router (config-if)#exit
Router (config)#int g0/0
Router (config-if)#ip address 10.0.0.2   255.255.255.0
Router (config-if)#no shutdown
Router (config)#exit
Router (config)#ip route 0.0.0.0   0.0.0.0   100.10.10.1
```

4.2.4.2 Configuration du NAT :

La fonction NAT dans un routeur traduit les adresses IP sources (interne privée) en adresses IP global (externe publique). Nous appliquons cette fonction seulement sur le serveur VPN qui est le routeur R2 (USDB) dans notre cas.

- **Routeur R2 *(USDB) :***

```
USDB (config)# int g0/0
USDB (config -if)# ip nat outside
USDB (config -if)# int f1/0
USDB (config -if)# ip nat inside
```

4.2.4.3 Configuration de l'ACL:

Pour pouvoir autoriser le trafic entre un réseau de niveau de sécurité inferieur à un autre réseau de niveau de sécurité supérieur, nous faisons appel aux ACL. Ces derniers permettent de mettre en place la stratégie de filtrage à appliquer.

- **Routeur R2 *(USDB) :***

```
USDB (config)# access-list 100 permit any
USDB (config)# ip nat inside source list 100 interface g0/0
```

4.2.5 Configuration du VPN :

✓ **Étape 1 : Création du nouveau modèle d'authentification**

- **Routeur R2 *(USDB) :***

```
USDB (config)# AAA NEW
USDB (config)# aaa authentication login cisco local
USDB (config)# aaa authorization network cisco local
```

✓ **Étape 2 : Identification de domaine**

- **Routeur R2 *(USDB) :***

```
USDB (config)# ip domain name ICT.com
USDB (config)# multilink bundle-name authenticated
```

✓ **Étape 3 : Configuration de la politique ISAKMP (pour IKE phase 1)**

- **Routeur R2 *(USDB) :***

```
USDB (config)# crypto isakmp policy 1
USDB (config-isakmp)# encr 3des
USDB (config-isakmp)# authentication pre-share
USDB (config-isakmp)# group 2
USDB (config-isakmp)# crypto isakmp keepalive 10
```

✓ **Étape 4 : Création du groupe et configuration de profile**

- **Routeur R2 *(USDB) :***

```
USDB (config)# crypto isakmp client configuration group ICT
USDB (config-isakmp-group)# key  ICT123
USDB (config-isakmp-group)# pool  SDM_POOL_1
USDB (config-isakmp-group)# acl 199
USDB (config-isakmp-group)# crypto isakmp profile cisco
USDB (config-isa-prof)# match identity group ICT
USDB (config-isa-prof)# client authentication list cisco
USDB (config-isa-prof)# isakmp authorization list cisco
USDB (config-isa-prof)# client configuration address respond
USDB (config-isa-prof)# virtual-template 1
```

✓ **Étape 5 : Configurer l'ensemble de transformations IPSec (pour IKE phase 2)**

- **Routeur R2 *(USDB) :***

```
USDB (cfg-crypto-trans)# crypto ipsec transform-set TEST esp-3des esp-sha-hmac
USDB (ipsec-profile)# crypto ipsec profile Cisco
USDB (ipsec-profile)# set security-association idle-time 86400
USDB (ipsec-profile)# set transform-set TEST
USDB (ipsec-profile)# set isakmp-profile cisco
```

✓ **Étape 6 : Création d'un compte d'utilisateur avec tous les privilèges**

- **Routeur R2 *(USDB) :***

```
USDB (config)# username cisco123 privilege 15 password 0 cisco123
USDB (config)# interface Virtual-Template1 type tunnel
USDB (config-if)# ip unnumbered g0/0
USDB (config-if)# tunnel mode ipsec ipv4
USDB (config-if)# tunnel protection ipsec profile Cisco
```

✓ **Étape 7 : Autoriser le trafic des utilisateurs VPN**

- **Routeur R2 *(USDB) :***

```
USDB (config)# access-list 199 permit ip any any
```

✓ **Étape 8 : Attribuer l'adresse IP aux clients distants**

- **Routeur R2 *(USDB) :***

```
USDB (config)# ip local pool SDM_POOL_1 30.30.30.20   30.30.30.30
```

4.3 VPN pour le télétravail :

4.3.1 Problématique :

Des pandémies mondiales et des catastrophes naturelles aux pannes de courant et aux rues non déneigées, il y a tout simplement trop de situations qui pourraient empêcher les gens d'entrer au bureau, cette perte de travail peut être préjudiciable pour de nombreux particuliers et entreprises. Les entreprises du monde entier se rendent compte que le travail ne peut et ne doit pas dépendre d'un endroit en particulier, et que la flexibilité est cruciale pour que les organisations du monde entier puissent continuer à fonctionner en toutes circonstances.

Prenons l'exemple des employés à distance, lorsque les employés travaillent sur place, ils peuvent connecter leur ordinateur et leur appareil mobile directement au réseau interne de l'entreprise, mais si un employé travaille à distance, sa connexion à ce réseau interne doit se faire par l'internet public, ce qui peut exposer son trafic à des attaques de type « man-in-the-middle » et à d'autres méthodes d'espionnage de données sensibles, donc le télétravail augmente la vulnérabilité des employés aux pirates informatiques, car l'environnement est quelque peu différent d'un environnement de bureau.

Cela implique que la nécessité de protéger les travailleurs à distance et les informations de l'entreprise contre les attaques en ligne devient une considération vitale dans ce cas. Les entreprises utilisent généralement un réseau privé virtuel (VPN) pour donner un accès à distance pour ses employées aux applications et données internes, ou pour créer un réseau unique partagé entre plusieurs bureaux.

Notre cas d'étude vise sur une entreprise dispose d'un réseau local, pour atteindre ses objectifs et accomplir ses missions, elle doit relier ce dernier à ses filiales, ses télétravailleurs, ses partenaires et d'autres utilisateurs à travers internet. Se pose alors la problématique d'accès aux données du système d'informations entre les sites ou depuis l'extérieur, tout en garantissant la sécurité et la performance de ces échanges.

4.3.2 Solution proposée :

L'interconnexion IPSec accorde à l'entreprise une solution d'interconnexion fiable, moins couteuse et rapide à mettre en place grâce à des tunnels sécurisés entre les différents sites, voilà, pourquoi nous avons opté pour cette solution afin d'interconnecter le site de direction générale d'une entreprise situé à Alger avec un site distant situé à Oran. Notre

solution inclus aussi l'accès au système d'information locale pour les télétravailleurs de l'entreprise afin d'assure le contrôle et la sécurité de cette connexion grâce à un simple accès internet et ce quel que soit le débit ou l'endroit où se trouve ses derniers.

La figure suivante illustre la solution proposée :

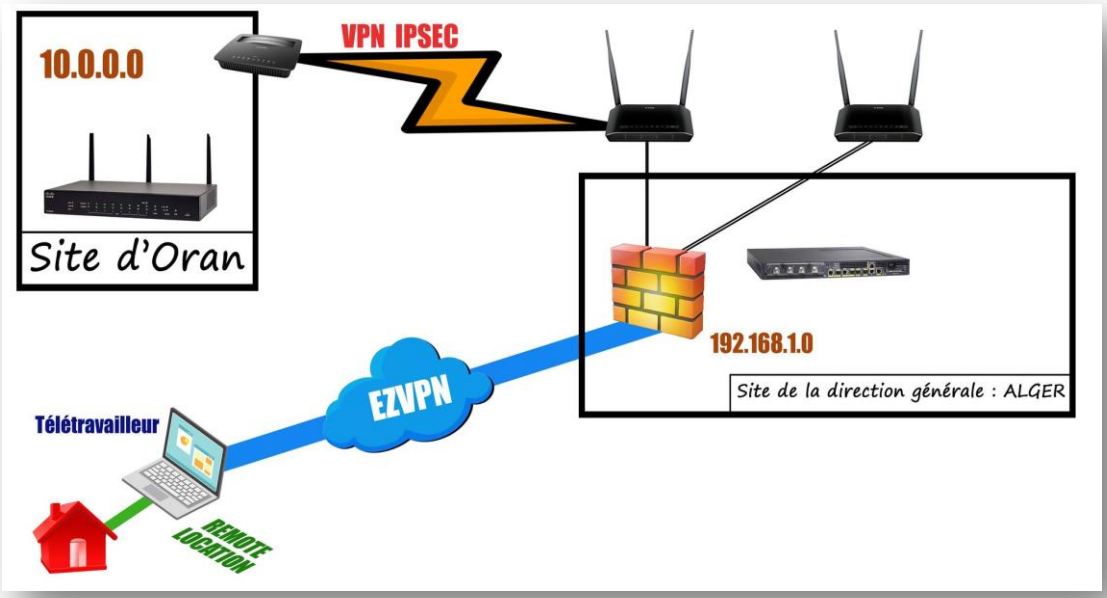

Figure 4-7 : Architecture proposée pour le télétravail

Pour mettre en œuvre cette solution au niveau de notre entreprise, nous allons procéder à deux types de VPN, site à site d'une part, en se basant sur le protocole IPSec, et d'autre part au VPN à distance qui permet aux télétravailleur d'accéder à distance au réseau d'entreprise et d'utiliser ses ressources (fichiers, courriers électroniques, applications, calendrier partagé, etc.) d'une façon contrôlé et totalement sécurisée grâce à un simple accès internet , via des tunnels VPN, quel que soit leur débit, fournisseur d'accès internet ou l'endroit où ils se trouvent.

L'architecture choisie pour VPN de site à site est représentée dans la figure suivante :

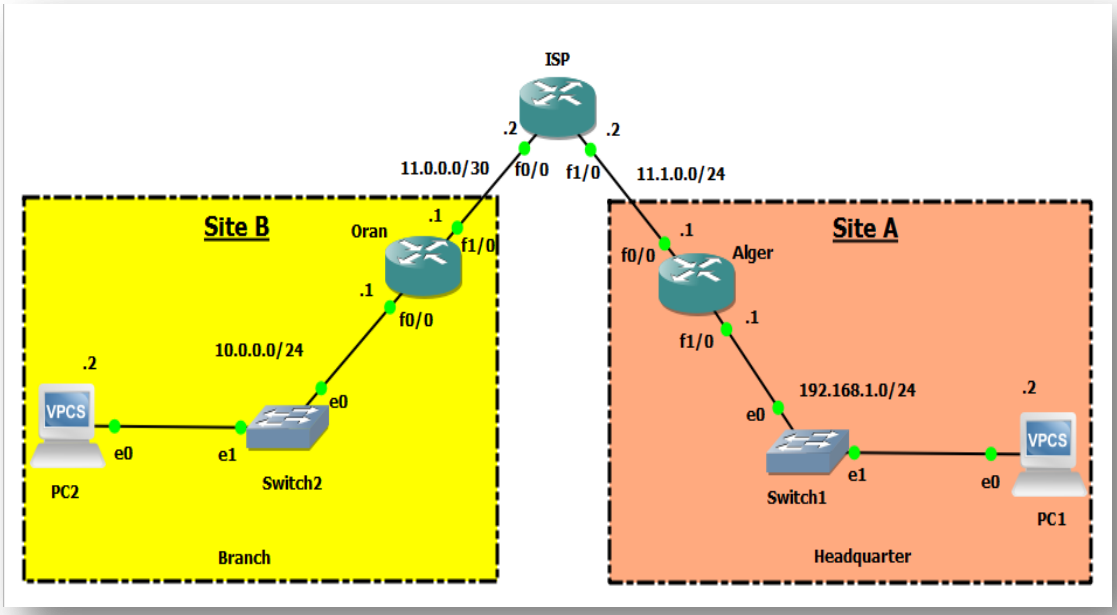

Figure 4-8 : Topologie de VPN site à site de branche

L'architecture choisie pour VPN d'accès à distance est représentée dans la figure suivante :

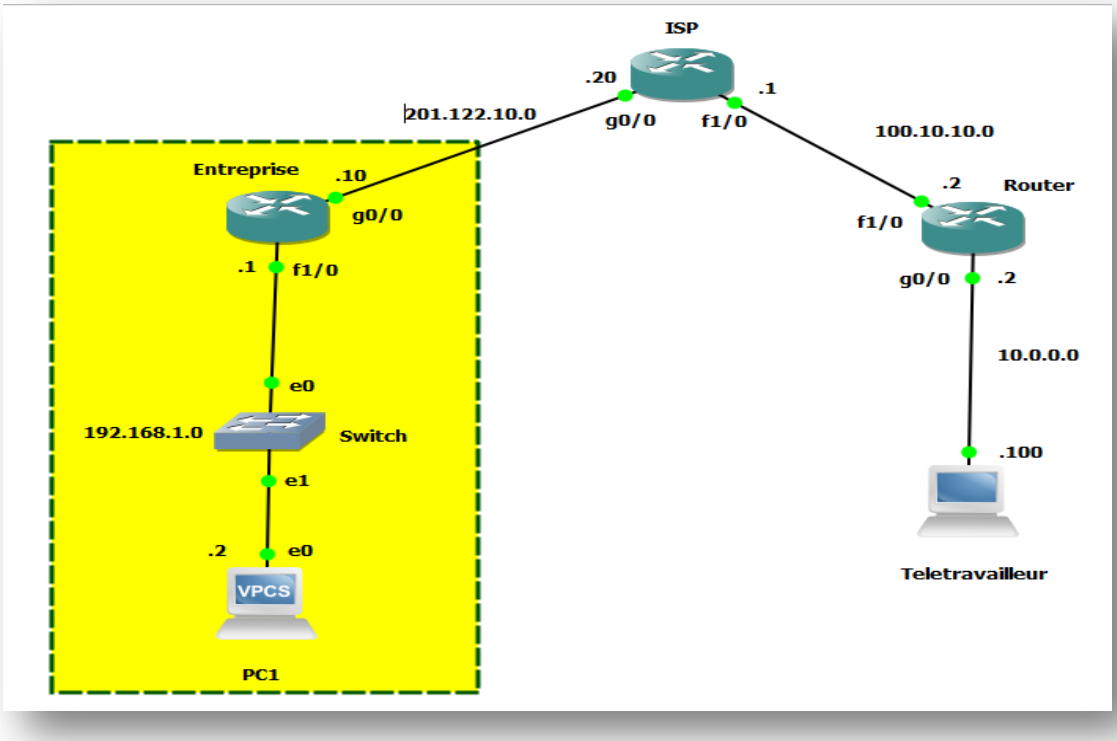

Figure 4-9 : Topologie de VPN d'accès à distance pour les télétravailleurs

4.3.3 Implémentation de VPN site à site :

4.3.3.1 Configuration de base :

Nous allons commencer par l'attribution des configurations de base réseau des différents routeurs.

✓ **Configuration des interfaces :**

D'abord, nous allons changer les noms des routeurs, puis configurer et activer leurs différentes interfaces, et les mets directement connectés comme c'est présenté ci-dessous :

- **Routeur R1 *(ISP) :***

```
R1#conf t
R1 (config)#hostname ISP
ISP (config)#int f0/0
ISP (config-if)#ip address 11.0.0.2   255.255.255.252
ISP (config-if)#no shutdown
ISP (config-if)#exit
ISP (config)#int f1/0
ISP (config-if)#ip address 11.1.0.2   255.255.255.0
ISP (config-if)#no shutdown
ISP (config-if)#exit
ISP (config)#ip route 10.0.0.0   255.255.255.0   11.0.0.2
ISP (config)#ip route 192.168.1.0   255.255.255.0   11.1.0.2
```

- **Routeur R2 *(Alger) :***

```
R2#conf t
R2 (config)#hostname Alger
Alger (config)#int f0/0
Alger (config-if)#ip address 11.1.0.1   255.255.255.0
Alger (config-if)#no shutdown
Alger (config-if)#exit
Alger (config)#int f1/0
Alger (config-if)#ip address 192.168.1.1   255.255.255.0
Alger (config-if)#no shutdown
Alger (config-if)#exit
Alger (config)#ip route 0.0.0.0   0.0.0.0   11.1.0.1
```

- **Routeur R3 *(Oran) :***

```
R3#conf t
R3 (config)#hostname Oran
Oran (config)#int f1/0
Oran (config-if)#ip address 11.0.0.1   255.255.255.252
Oran (config-if)#no shutdown
Oran (config-if)#exit
Oran (config)#int f0/0
Oran (config-if)#ip address 10.0.0.1   255.255.255.0
Oran (config-if)#no shutdown
Oran (config)#exit
Oran (config)#ip route 0.0.0.0   0.0.0.0   11.0.0.1
```

8.3.3.2 Configuration VPN:

Après avoir configuré les routeurs, nous allons entamer la configuration du VPN IPSec, en établissant un tunnel VPN qui sera configuré juste sur les routeurs d'extrémités, dans notre cas nous avons le routeur « Alger » et le routeur « Oran ». La mise en place du tunnel VPN entre les deux routeurs se fait selon plusieurs étapes illustrées ci-dessous :

✓ **Étape 1 : Configuration de la politique ISAKMP (pour IKE phase 1)**

Consiste à configurer les fonctions crypto d'ISAKMP qui gère l'échange des clés, en créant une stratégie de négociation des clés, toute en indiquant le schéma de connexion pour les associations de sécurités (SA), les types d'authentification et de chiffrement, ainsi la méthode de distribution des clés partagées (Diffie-Hellman group), et l'algorithme de hachage, ensuite, nous avons configuré la clé partagée.

- **Routeur R2 *(Alger) :***

```
Alger (config)# crypto isakmp policy 2
Alger (config-isakmp)# authentication pre-share
Alger (config-isakmp)# encryption aes
Alger (config-isakmp)# group 2
Alger (config-isakmp)# hash sha
Alger (config-isakmp)# exit
Alger (config)# crypto isakmp key CISCO address 11.0.0.1
```

- **Routeur R3 *(Oran) :***

```
Oran (config)# crypto isakmp policy 2
Oran (config-isakmp)# authentication pre-share
Oran (config-isakmp)# encryption aes
Oran (config-isakmp)# group 2
Oran (config-isakmp)# hash sha
Oran (config-isakmp)# exit
Oran (config)# crypto isakmp key CISCO address 11.1.0.1
```

✓ **Étape 2: Configurer l'ensemble de transformations IPSec (pour IKE phase 2)**

Dans cette étape, nous allons configurer les options de transformations des données, pour cela, nous allons créer la méthode de cryptage et la méthode d'authentification à utiliser, cette phase permettra durant l'association basée sur ISAKMP, de se mettre d'accord pendant les échanges afin de fixer la méthode de sécurisation des données. Les paramètres du « transform-set » devrons être les mêmes dans les deux côtés.

- **Routeur R2 *(Alger) :***

```
Alger (config)# crypto ipsec transform-set NAME esp-aes 256 ah-sha-hmac
Alger (config)# crypto ipsec security-association lifetime seconds 1800 (optionnel)
```

- **Routeur R3 *(Oran) :***

```
Oran (config)# crypto ipsec transform-set NAME esp-aes 256 ah-sha-hmac
Oran (config)# crypto ipsec security-association lifetime seconds 1800 (optionnel)
```

✓ **Étape 3: Définir le trafic intéressant (Must Mirror)**

Maintenant, nous allons créer une « access-list » qui servira à identifier le trafic à transiter et à traiter par le tunnel VPN, ce trafic sera originaire de l'adresse du site source destiné vers l'adresse du site destination.

- **Routeur R2 *(Alger) :***

```
Alger (config)# ip access-list extended LIST
Alger (config -ext-nacl)# permit ip 192.168.1.0   0.0.0.255   10.0.0.0   0.0.0.255
```

- **Routeur R3 *(Oran) :***

```
Oran (config)# ip access-list extended LIST
Oran (config -ext-nacl)# permit ip 10.0.0.0   0.0.0.255   192.168.1.0   0.0.0.255
```

✓ **Étape 4: Configurer la carte de chiffrement**

Dans cette étape, nous allons créer une « crypto-map » dont le but est de rassembler les différents éléments configurés pour pouvoir les appliquer enfin à une interface, c'est le module qui, une fois associée à une interface permettra de définir les conditions de connexion IPSec. Le numéro permet de définir le niveau de priorité, plus il est bas plus la « map » est prioritaire. Sa création se fait à l'aide des différentes étapes :

- ***match :*** liaison entre access-list et map.
- ***set peer :*** affecte la map au peer (adresse ip).
- ***set transform-set :*** transform set à utiliser (il est possible d'en mettre plusieurs).

- **Routeur R2 *(Alger) :***

```
Alger (config)# crypto map VPN_MAP 10 ipsec-isakmp
Alger (config-crypto-map)# match address LIST
Alger (config-crypto-map)# set peer 11.0.0.1
Alger (config-crypto-map)# set transform-set NAME
```

- **Routeur R3 *(Oran) :***

```
Oran (config)# crypto map VPN_MAP 10 ipsec-isakmp
Oran (config-crypto-map)# match address LIST
Oran (config-crypto-map)# set peer 11.1.0.1
Oran (config-crypto-map)# set transform-set NAME
```

✓ **Étape 5: Attribuer une carte de chiffrement à l'interface**

La dernière étape consiste à appliquer la « crypto-map » à l'interface de sortie du site, un message s'affichera indiquant que la « crypto map » fonctionne (active).

- **Routeur R2 *(Alger) :***

```
Alger (config)# int f0/0
Alger (config-if)# crypto map VPN_MAP

*Mar 1 00:45:16.843: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

- **Routeur R3 *(Oran) :***

```
Oran (config)# int f1/0
Oran (config-if)# crypto map VPN_MAP

*Mar 1 00:45:16.843: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

4.3.4 Implémentation de VPN accès à distance :

4.3.4.1 Configuration des interfaces :

- **Routeur R1 *(ISP) :***

```
R1#conf t
R1 (config)#hostname ISP
ISP (config)#int g0/0
ISP (config-if)#ip address 201.122.10.20   255.255.255.0
ISP (config-if)#no shutdown
ISP (config-if)#exit
ISP (config)#int f1/0
ISP (config-if)#ip address 100.10.10.1   255.255.255.0
ISP (config-if)#no shutdown
ISP (config-if)#exit
ISP (config)#ip route 192.168.1.0   255.255.255.0   201.122.10.20
ISP (config)#ip route 10.0.0.0   255.255.255.0   100.10.10.1
```

- **Routeur R2 *(Entreprise) :***

```
R2#conf  t
R2 (config)#hostname Entreprise
Entreprise (config)#int g0/0
Entreprise (config-if)#ip address 201.122.10.10   255.255.255.0
Entreprise (config-if)#no shutdown
Entreprise (config-if)#exit
Entreprise (config)#int f1/0
Entreprise (config-if)#ip address 192.168.1.1   255.255.255.0
Entreprise (config-if)#no shutdown
Entreprise (config-if)#exit
Entreprise (config)#ip route 0.0.0.0   0.0.0.0   201.122.10.20
```

- **Routeur R3 *(Router) :***

```
R3#conf t
R3 (config)#hostname Router
Router (config)#int f1/0
Router (config-if)#ip address 100.10.10.2   255.255.255.0
Router (config-if)#no shutdown
Router (config-if)#exit
Router (config)#int g0/0
Router (config-if)#ip address 10.0.0.2   255.255.255.0
Router (config-if)#no shutdown
Router (config)#exit
Router (config)#ip route 0.0.0.0   0.0.0.0   100.10.10.1
```

4.3.4.2 Configuration du NAT :

- **Routeur R2 *(Entreprise) :***

```
Entreprise (config)# int g0/0
Entreprise (config -if)# ip nat outside
Entreprise (config -if)# int f1/0
Entreprise (config -if)# ip nat inside
```

4.3.4.3 Configuration de l'ACL:

- **Routeur R2 *(Entreprise) :***

```
Entreprise (config)# access-list 100 permit any
Entreprise (config)# ip nat inside source list 100 interface g0/0
```

4.3.4.4 Configuration VPN:

✓ **Étape 1 : Création du nouveau modèle d'authentification**

- **Routeur R2 *(Entreprise) :***

```
Entreprise (config)# AAA NEW
Entreprise (config)# aaa authentication login cisco local
Entreprise (config)# aaa authorization network cisco local
```

✓ **Étape 2 : Identification de domaine**

- **Routeur R2 *(Entreprise) :***

```
Entreprise (config)# ip domain name Naftal.com
Entreprise (config)# multilink bundle-name authenticated
```

✓ **Étape 3 : Configuration de la politique ISAKMP (pour IKE phase 1)**

- **Routeur R2 *(Entreprise) :***

```
Entreprise (config)# crypto isakmp policy 1
Entreprise (config-isakmp)# encr 3des
Entreprise (config-isakmp)# authentication pre-share
Entreprise (config-isakmp)# group 2
Entreprise (config-isakmp)# crypto isakmp keepalive 10
```

✓ **Étape 4 : Création du groupe et configuration de profile**

- **Routeur R2 *(Entreprise) :***

```
Entreprise (config)# crypto isakmp client configuration group Naftal
Entreprise (config-isakmp-group)# key  Naftal123
Entreprise (config-isakmp-group)# pool  NAF_POOL_1
Entreprise (config-isakmp-group)# acl 200
Entreprise (config-isakmp-group)# crypto isakmp profile cisco
Entreprise (config-isa-prof)# match identity group Naftal
Entreprise (config-isa-prof)# client authentication list cisco
Entreprise (config-isa-prof)# isakmp authorization list cisco
Entreprise (config-isa-prof)# client configuration address respond
Entreprise (config-isa-prof)# virtual-template 1
```

✓ **Étape 5 : Configurer l'ensemble de transformations IPSec (pour IKE phase 2)**

- **Routeur R2 *(Entreprise) :***

```
Entreprise (cfg-crypto-trans)# crypto ipsec transform-set TEST esp-3des esp-sha-hmac
Entreprise (ipsec-profile)# crypto ipsec profile Cisco
Entreprise (ipsec-profile)# set security-association idle-time 86400
Entreprise (ipsec-profile)# set transform-set VPN_NAF
Entreprise (ipsec-profile)# set isakmp-profile cisco
```

✓ **Étape 6 : Création d'un compte d'utilisateur avec tous les privilèges**

- **Routeur R2 *(Entreprise) :***

```
Entreprise (config)# username emp123 privilege 15 password 0 emp123
Entreprise (config)# interface Virtual-Template1 type tunnel
Entreprise (config-if)# ip unnumbered g0/0
Entreprise (config-if)# tunnel mode ipsec ipv4
Entreprise (config-if)# tunnel protection ipsec profile Cisco
```

✓ **Étape 7 : Autoriser le trafic des utilisateurs VPN**

- **Routeur R2 *(Entreprise) :***

```
Entreprise (config)# access-list 200 permit ip any any
```

✓ **Étape 8 : Attribuer l'adresse IP aux clients distants**

- **Routeur R2 *(Entreprise) :***

```
Entreprise (config)# ip local pool NAF_POOL_1 40.40.40.10   40.40.40.40
```

4.4 Tests et optimisation :

4.4.1 Vérification de connectivité des interfaces :

4.4.1.1 VPN de site à site :

Nous allons tester la connectivité entre les retours une fois que nous terminons la configuration des interfaces. En vérifiant l'état des interfaces configurés, puis en envoyons une requête ICMP du routeur « Alger » vers le routeur « Oran » puis inversement comme le montre les figures suivantes :

```
Alger#sh  ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        11.1.0.1        YES manual up                    up
FastEthernet1/0        192.168.1.1     YES manual up                    up
FastEthernet2/0        unassigned      YES unset  administratively down down
FastEthernet2/1        unassigned      YES unset  administratively down down
Alger#
```

```
Oran#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.0.0.1        YES manual up                    up
FastEthernet1/0        11.0.0.1        YES manual up                    up
FastEthernet2/0        unassigned      YES unset  administratively down down
Oran#
```

```
ISP#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        11.0.0.2        YES manual up                    up
FastEthernet1/0        11.1.0.2        YES manual up                    up
FastEthernet2/0        unassigned      YES unset  administratively down down
FastEthernet2/1        unassigned      YES unset  administratively down down
ISP#
```

Figure 4-10 : Statut des interfaces 1

- **PC1 de routeur « Alger » vers PC2 de routeurs « Oran » :**

```
PC1> ping 10.0.0.2
84 bytes from 10.0.0.2 icmp_seq=1 ttl=61 time=152.768 ms
84 bytes from 10.0.0.2 icmp_seq=2 ttl=61 time=46.289 ms
84 bytes from 10.0.0.2 icmp_seq=3 ttl=61 time=38.225 ms
84 bytes from 10.0.0.2 icmp_seq=4 ttl=61 time=33.240 ms
84 bytes from 10.0.0.2 icmp_seq=5 ttl=61 time=56.335 ms

PC1>
```

solarwinds | Solar-PuTTY *free tool*

Figure 4-11 : Résultat d'une requête « Alger » vers « Oran »

- **PC2 de routeur « Oran » vers PC1 de routeurs « Alger » :**

Figure 4-12 : Résultat d'une requête « Oran» vers « Alger »

4.4.1.2 VPN d'accès à distance :

Nous allons vérifier l'état des interfaces configurés, puis nous testons la connectivité entre l'étudiant nomade et le serveur de site e-learning USDB avec le fournisseur d'accès à internet « ISP », en envoyons des requêtes ICMP comme les figures suivantes montrent :

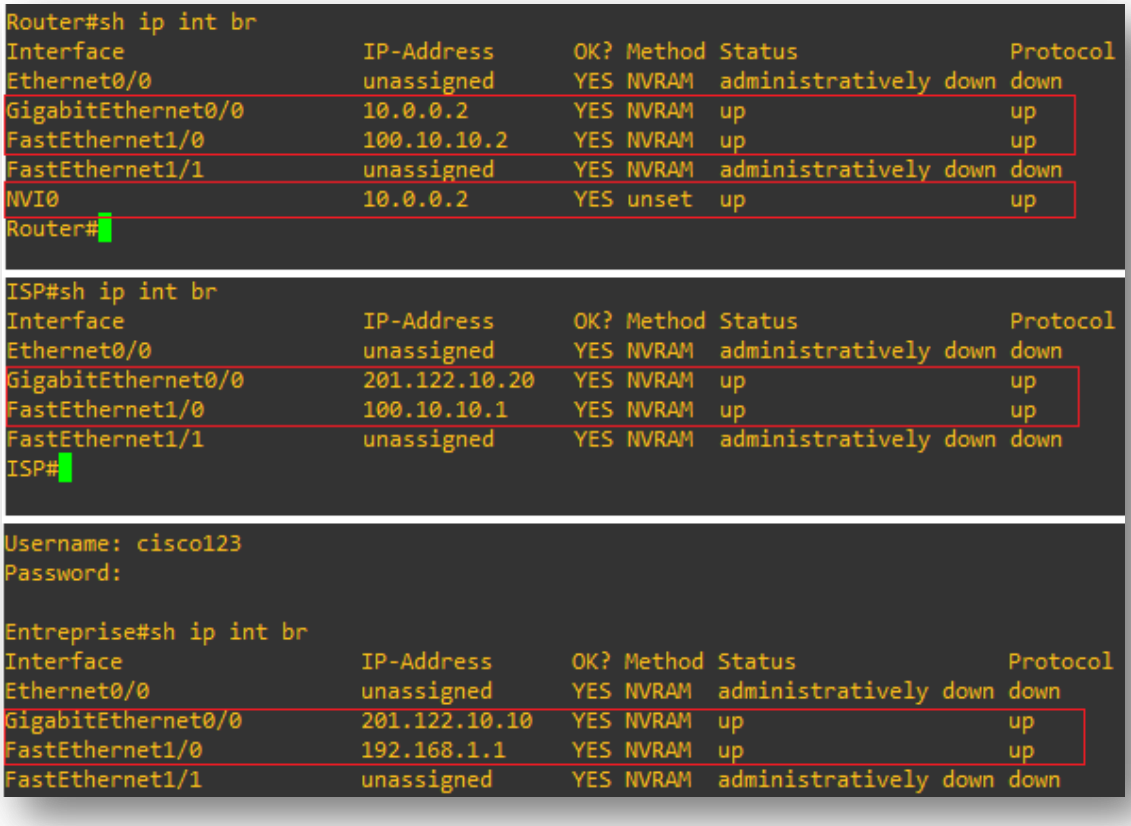

Figure 4-13 : Statut des interfaces 2

- **Requêtes ICMP pour tester la connectivité entre le routeur d'Étudiant nomade et le serveur de e-learning USDB *:***

```
USDB#ping 100.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.10.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/30/32 ms

Router#ping 201.122.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 201.122.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/43/60 ms
```

Figure 4-14 : Résultat des requêtes ICMP entre « USDB » et « Routeur »

4.4.2 Test de fonctionnement du VPN :

4.4.2.1 VPN de site à site :

Nous allons d'abord, tester le fonctionnement du VPN en vérifiant les informations retournées par ce VPN sur les deux routeurs.

- **Routeur « Alger » :**

```
Alger#sh crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set NAF_VPN: { ah-sha-hmac  }
   will negotiate = { Tunnel,  },
   { esp-256-aes  }
   will negotiate = { Tunnel,  },

Alger#
```

solarwinds | Solar-PuTTY free tool

Figure 4-15 : Vérification du fonctionnement de VPN sur « Alger »

- **Routeur « Oran » :**

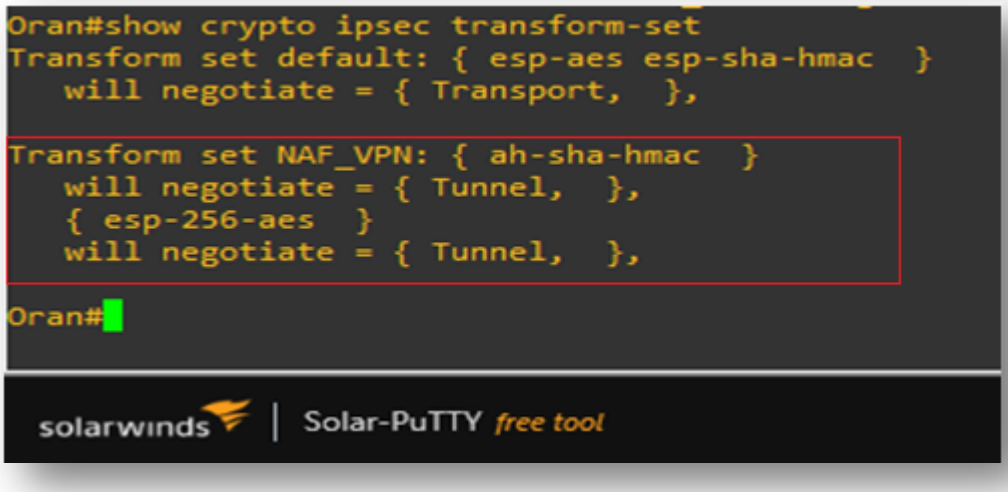

Figure 4-16 : Vérification du fonctionnement de VPN sur « Oran »

Ensuite, nous allons vérifier la « map vpn » sur les deux routeurs, et nous obtenons les résultats suivants :

- **Routeur « Alger » :**

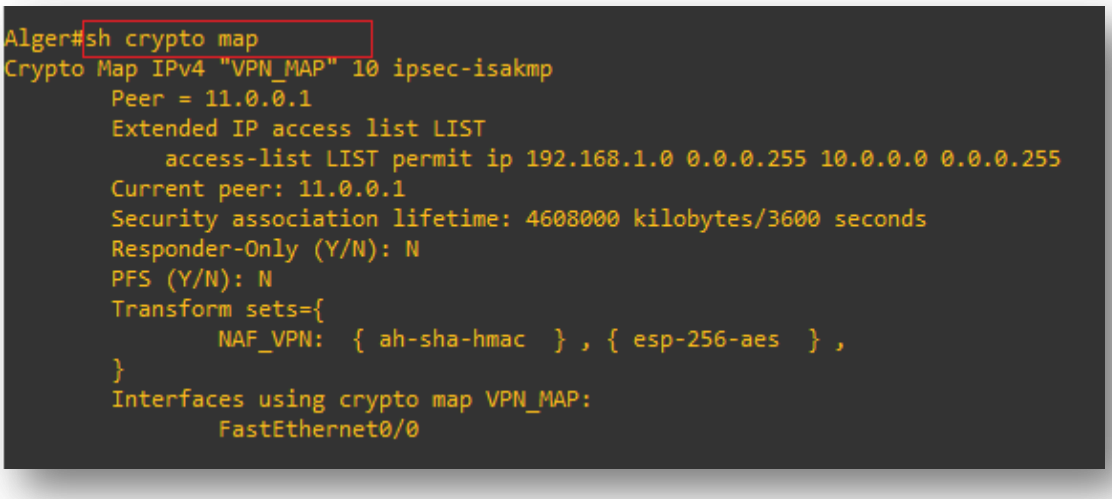

Figure 4-17 : Vérification de la map-vpn sur « Alger »

- **Routeur « Oran » :**

```
Oran#
Oran#sh crypto map
Crypto Map IPv4 "VPN_MAP" 10 ipsec-isakmp
        Peer = 11.1.0.1
        Extended IP access list LIST
            access-list LIST permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
        Current peer: 11.1.0.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                NAF_VPN:  { ah-sha-hmac  } , { esp-256-aes  } ,
        }
        Interfaces using crypto map VPN_MAP:
                FastEthernet1/0
```

Figure 4-18 : Vérification de la map-vpn sur « Oran »

Pour finir, il nous reste à vérifier les opérations d'ISAKMP sur les deux routeurs, nous obtiendrons les résultats suivants :

- **Routeur « Alger » :**

```
Alger#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
11.0.0.1        11.1.0.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

Alger#
```

solarwinds | Solar-PuTTY *free tool*

Figure 4-19 : Vérification des opérations ISAKMP pour « Alger »

- **Routeur « Oran » :**

```
Oran#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
11.0.0.1        11.1.0.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA

Oran#
```

solarwinds | Solar-PuTTY *free tool*

Figure 4-20 : Vérification des opérations ISAKMP pour « Oran »

4.4.2.2 *VPN d'accès à distance :*

Lorsque la configuration est terminée, nous lançons le VPN Client Cisco sur la machine cliente « Étudiant_nomade » afin d'activer la connexion VPN. Il nous demandera de s'authentifier, comme la figure suivante montre :

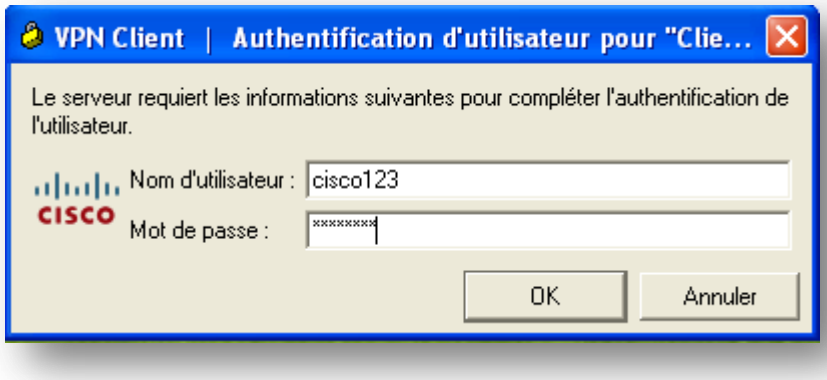

Figure 4-21 : Authentification de client VPN

Maintenant, nous entamons la vérification des informations de session client connecté au serveur « USDB », le résultat est représenté dans les figures suivantes :

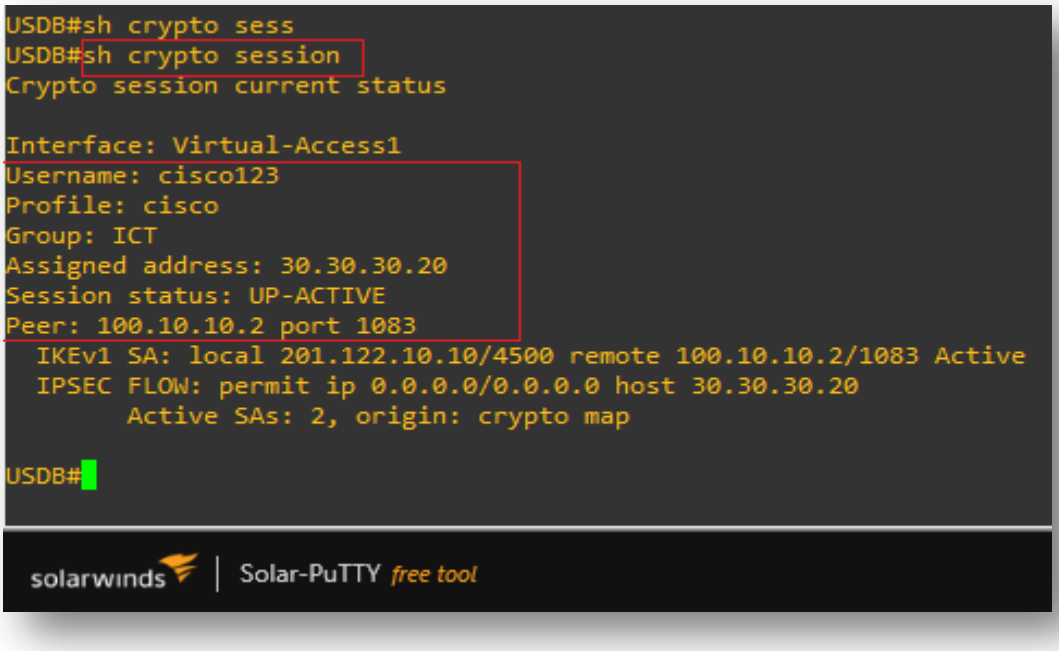

Figure 4-22 : Vérification de la session client

Pour finir, il nous reste à vérifier les opérations d'ISAKMP sur le routeur « USDB », nous obtiendrons le résultat suivant :

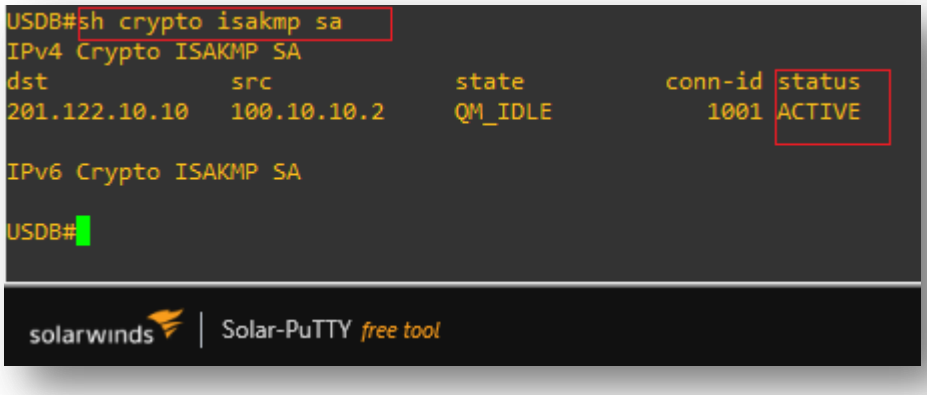

Figure 4-23 : Vérification des opérations ISAKMP

Maintenant, le client « Étudiant_nomade » peut accéder au e-learning en toute sécurité, en envoyons une requête ICMP comme le montre la figure suivante :

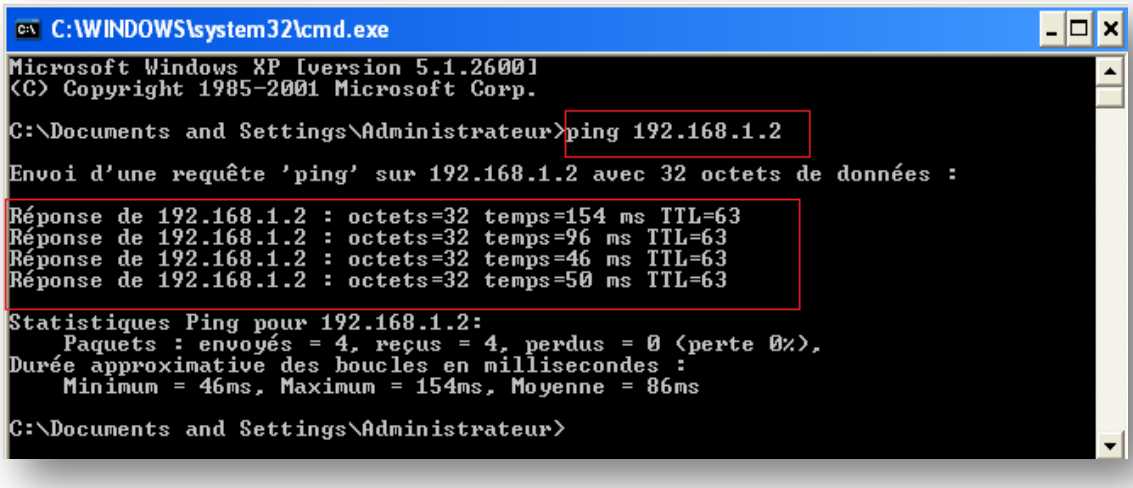

Figure 4-24 : Résultat d'une requête ICMP vers e-learning USDB

4.4.3 Capture de trafic du réseau :

Le résultat capté sous l'analyseur wireshark avant la mise en place d'une solution VPN, affiche la liste des paquets ICMP et leur contenu en claire, ainsi que la liste des adresses sources et destination des requêtes effectuées.

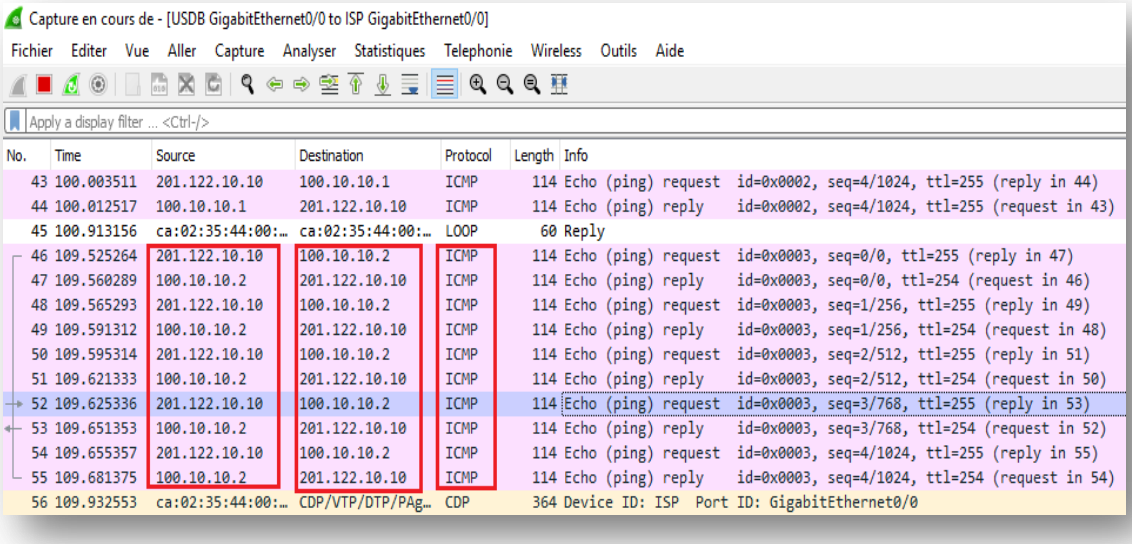

Figure 4-25 : Capture de résultat avant la mise en œuvre de VPN

Après la mise en œuvre de VPN, nous constatant qu'il est impossible de voir qu'il s'agit de paquets ICMP, la seule chose visible c'est qu'il y a un trafic crypté d'un bout à l'autre du tunnel.

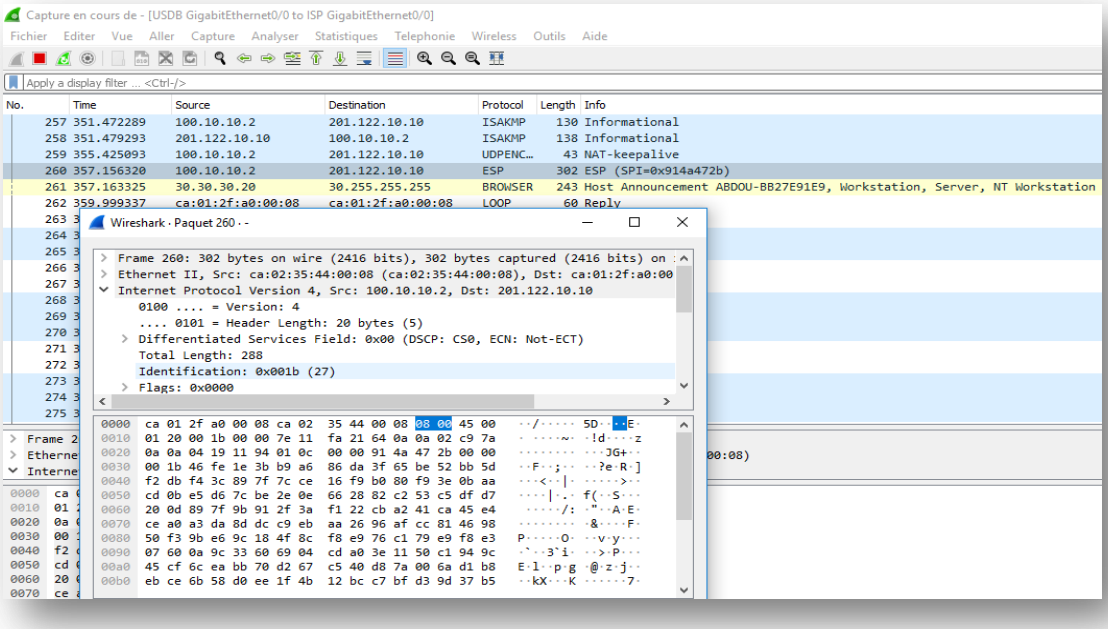

Figure 4-26 : Capture de résultat après la mise en œuvre de VPN

4.4.4 Optimisation de déploiement d'un VPN :

Après voir la mise en place d'une solution VPN pour le télétravail et l'enseignement à distance, Nous passerons vers l'automatisation de la configuration pour les VPN d'accès à distance à l'aide d'une application desktop.

4.4.4.1 Étude conceptuelle :

- **Diagramme des cas d'utilisation :**

La figure ci-dessous représente le diagramme des cas d'utilisations qui décrit les utilisations requises par notre application :

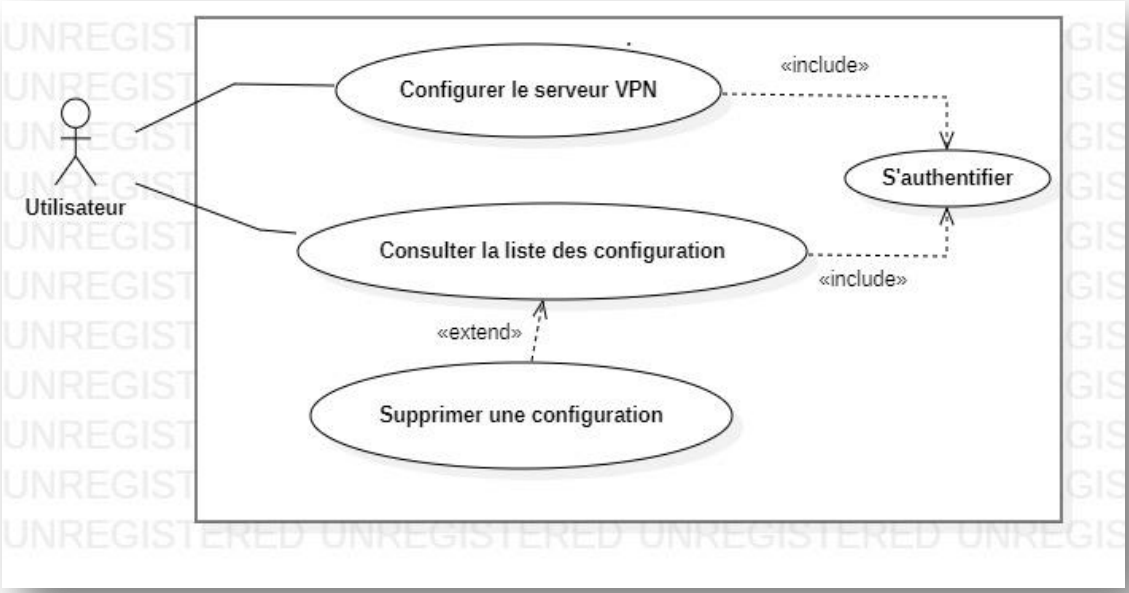

Figure 4-27 : Diagramme des cas d'utilisation

- **Diagrammes de séquence :**

Un diagramme de séquence est un diagramme d'interaction qui expose la façon dont les opérations sont effectuées.

❖ **Authentification :**

Lorsque l'utilisateur veux accéder à notre application, il sera obligé de s'authentifier avant d'y accéder en saisissant son nom d'utilisation et mot de passe, après la saisie le système envois une requête au serveur pour traiter les informations envoyées, si les informations sont correcte l'utilisateur accédera à sa session sinon un message d'erreur sera affiché et reconduira l'utilisateur à la page authentification.

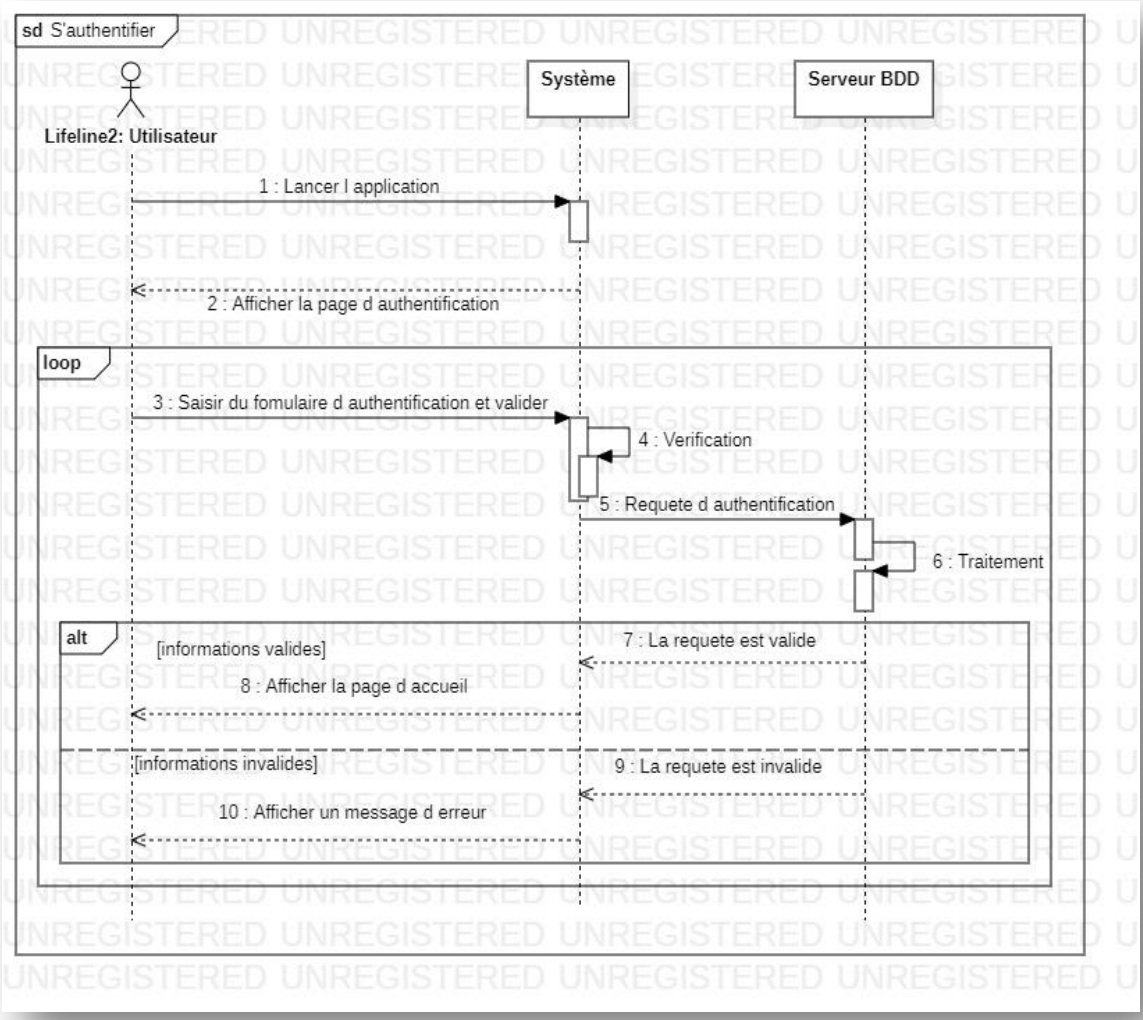

Figure 4-28 : Diagramme de séquence d'authentification

❖ Configuration du serveur VPN :

Pour faire une nouvelle configuration, l'utilisateur doit saisir le nom de domaine, le nom de groupe, la clé de groupe, le nom de pool, un nom d'utilisateur, et un mot de passe pour un membre de groupe, il doit préciser le nombre des privilèges pour un membre, et finalement l'adresse IP de pool.

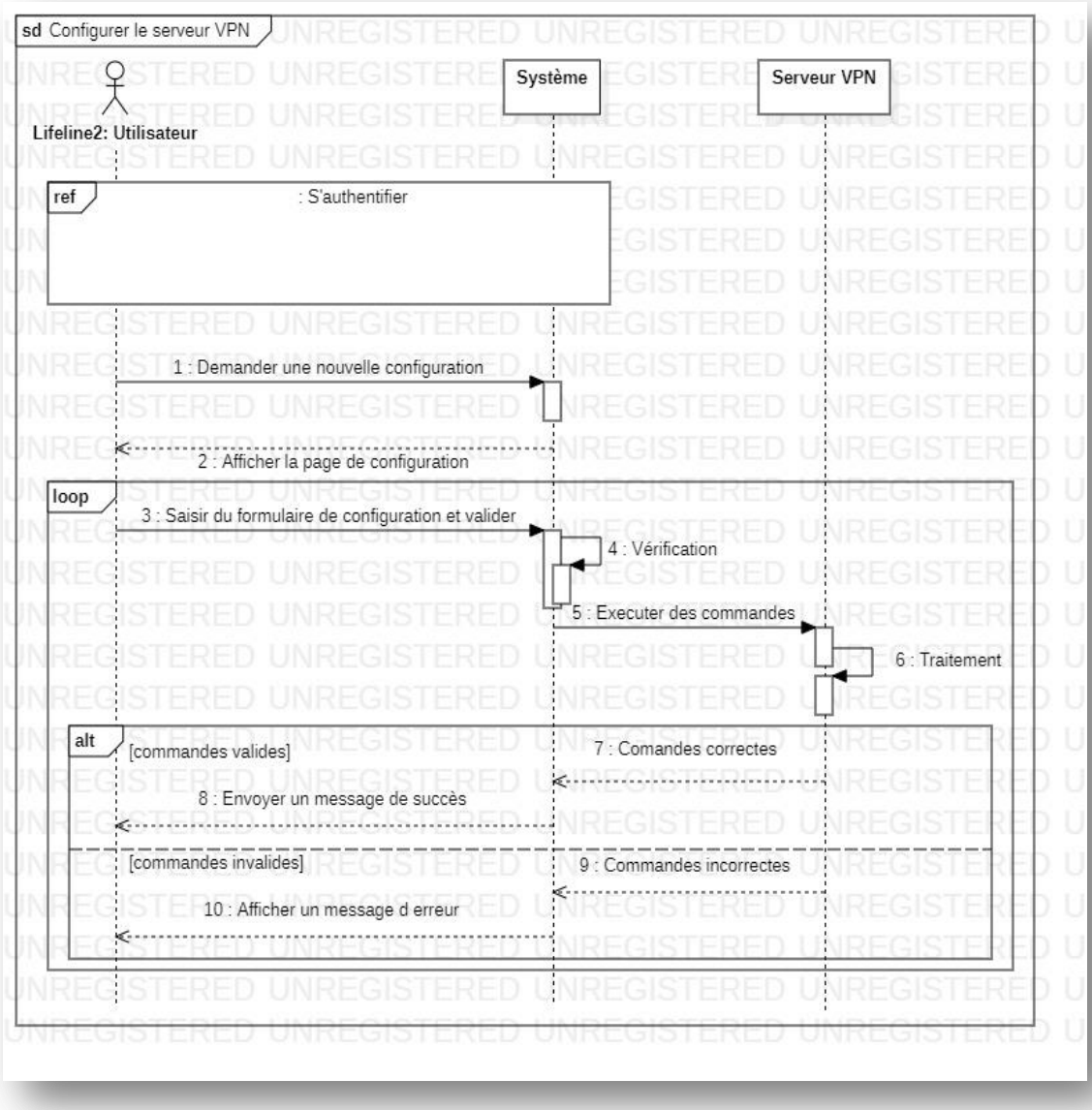

Figure 4-29 : Diagramme de séquence de configuration

❖ **Consultation la liste des configurations :**

L'utilisateur peut consulter la liste de ses configurations. Par option il peut supprimer une configuration.

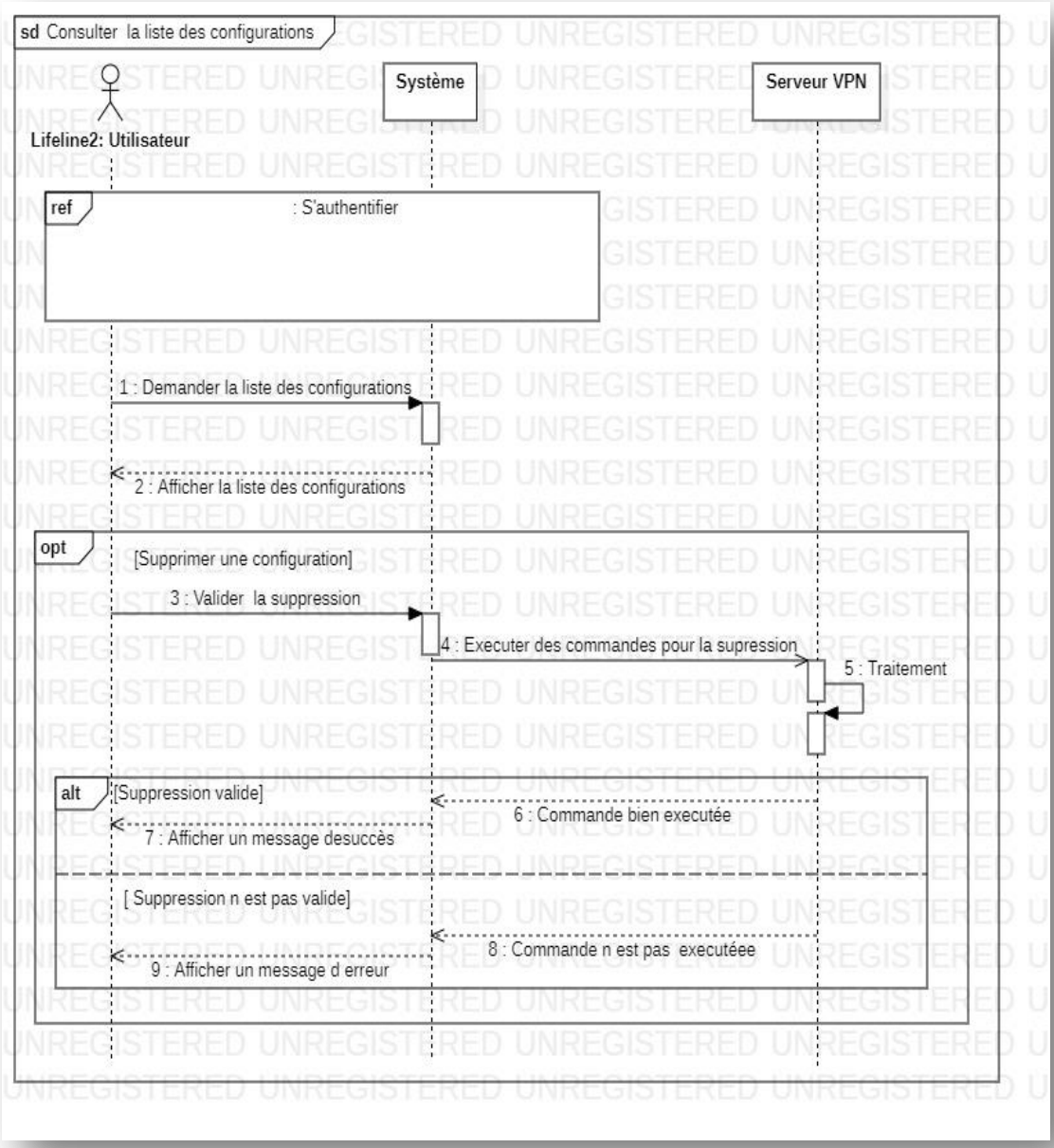

Figure 4-30 : Diagramme de séquence de consultation

4.4.4.2 Représentation des interfaces :

- **Authentification :**

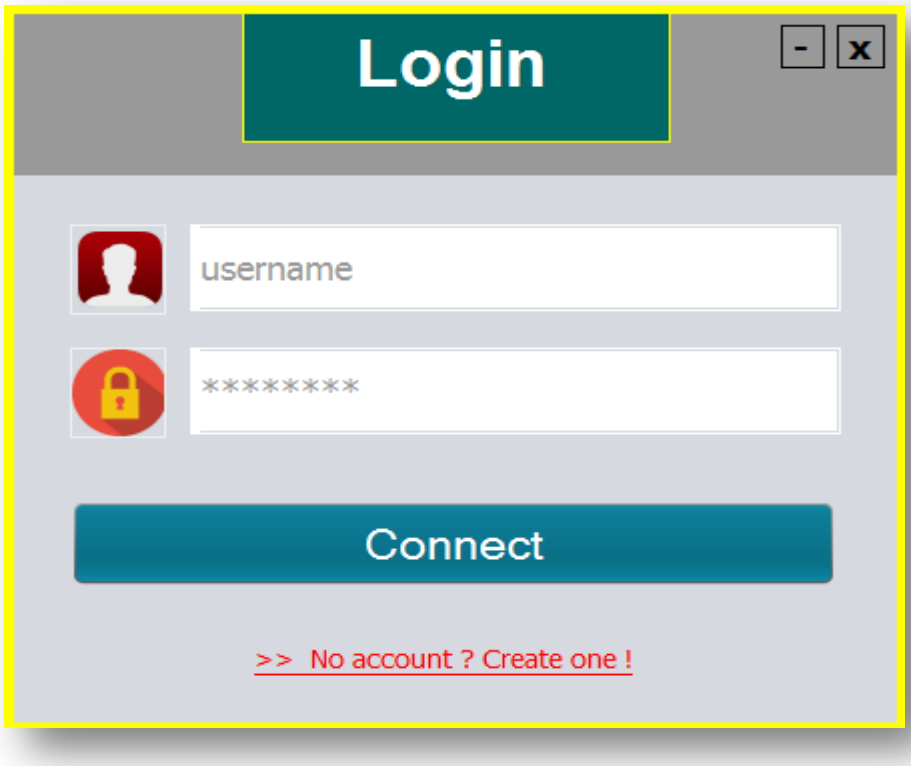

Figure 4-31 : Interface d'authentification

- **Nouvelle configuration :**

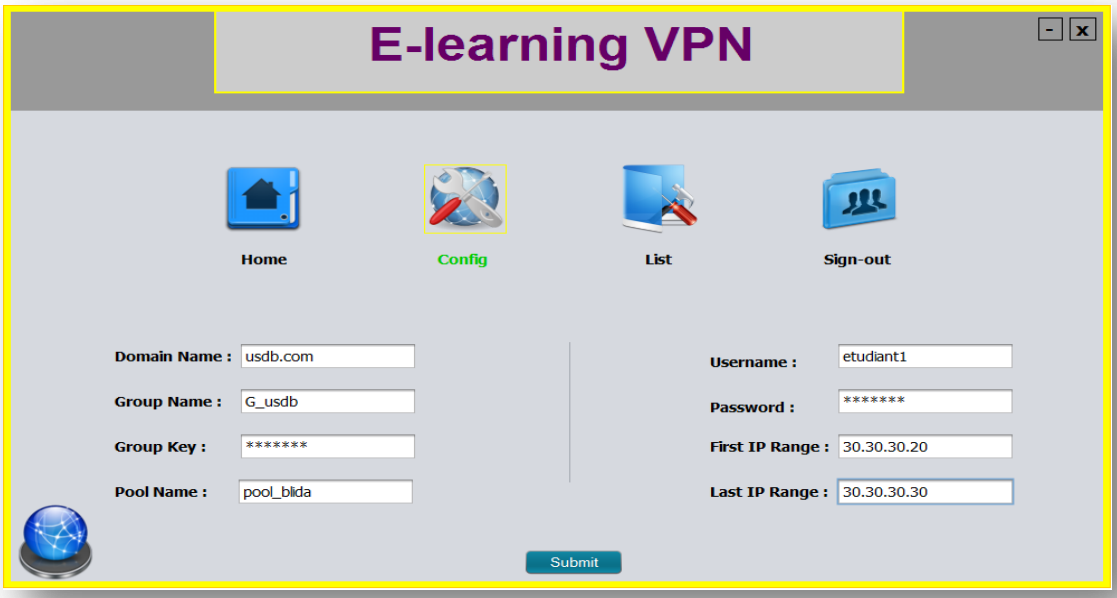

Figure 4-32 : Interface de configuration

- **La liste des configurations :**

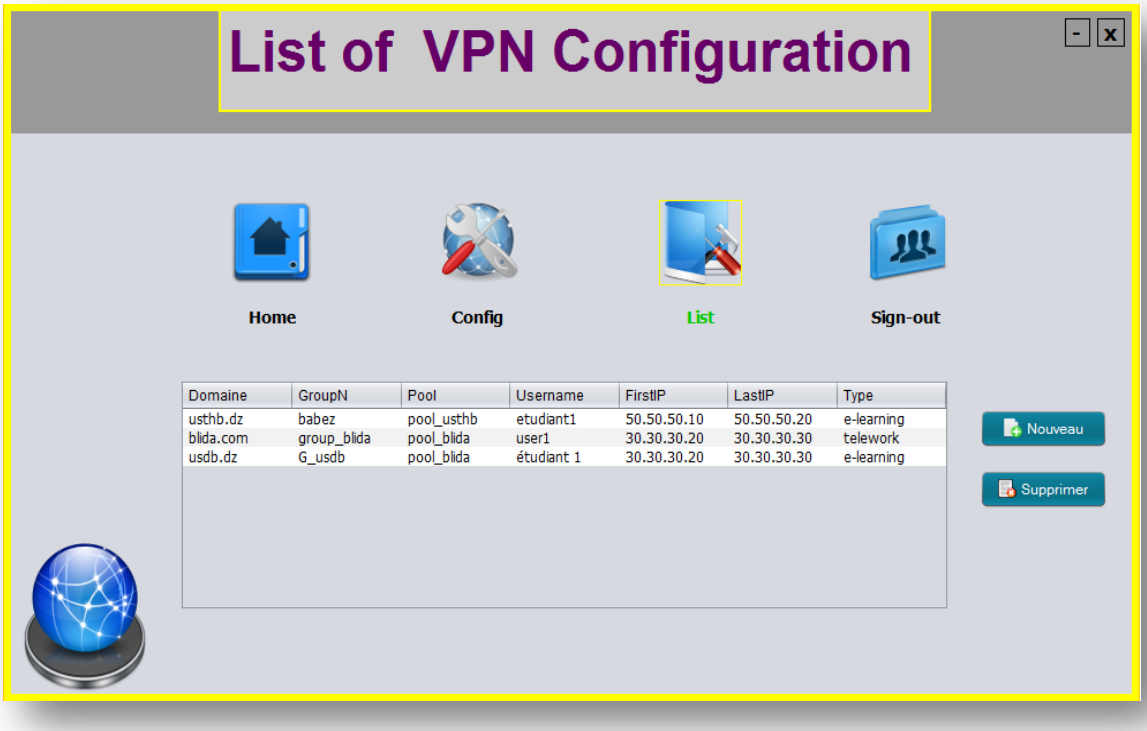

Figure 4-33 : Interface de liste des configurations

Conclusion :

Dans ce chapitre, nous avons décrit l'environnement du travail GNS3 et tous les autres outils utilisés, ensuite, nous avons présentés les différentes étapes de l'implémentation de notre solution VPN, ainsi que les résultats des différents tests effectués afin de vérifier le bon fonctionnement de cette solution, et à la fin nous avons présenté l'application pour l'automatisation de configuration de VPN d'accès à distance.

CONCLUSION GÉNÉRALE

Les épidémies et les catastrophes naturelles surviennent comme des causes hors de portée humaine, et peuvent perturber les études et le travail, et par conséquent retarder ou rater les objectifs et les tâches des entreprises. Ainsi qu'à un moment où les réseaux ont évolué au fil du temps à une vitesse vertigineuse, leur interconnexion à internet les a directement exposés à des attaques informatiques complexes. Il devient indispensable de mettre en place des solutions efficaces de protection du réseau contre ces attaques, en particulier lorsqu'il s'agit d'accès à distance pour les étudiants et les enseignants nomades en utilisant des plateformes e-learning, ou pour les télétravailleurs lorsqu'ils sont connectés à leur environnement de travail d'entreprise. Afin de garantir un niveau élevé de sécurité, une protection vigilante contribue à garantir la continuité des études, et de l'activité de l'entreprise et minimise les conséquences onéreuses des intrusions.

Dans notre cas, nous avons opté pour la mise en place d'une solution VPN permettant de réaliser un réseau privé sécurisé en utilisant l'infrastructure d'un réseau partagé, cette solution est scindée en deux parties garantissant une sécurité performante de haut niveau: les VPN site à site, permettant à l'entreprise de faire des transitions de données et de communiquer avec les autres sites, et à distance permettant aux télétravailleurs d'accéder au réseau d'entreprise. D'autre part une solution VPN d'accès à distance également pour les enseignants et les étudiants nomades pour qu'ils puissent d'accéder aux e-learning en toute sécurité. En effet, cette technologie permet aux employés de partager de façon sécurisée leurs données via le protocole IPSec en mode tunnel pour la solution VPN de site à site qui permet d'avoir une interconnexion sécurisée entre une direction générale situé à Alger, et une branche situé à Oran, ainsi que via le protocole IPSec en mode transport dans la solution d'accès à distance EzVPN qui assure un accès sûr pour les télétravailleurs et les utilisateurs de e-learning.

Ce travail a fait l'objet d'une expérience intéressante, et a eu énormément d'apport sur nos connaissances et nos compétences en termes de configuration dans un environnement GNS3. Il peut être enrichi en terme de perspectives, par un l'implémentation d'un modèle de déploiement en étoile, en utilisant le DMVPN pour avoir une dynamité de configuration considérable, et par l'utilisation de système RADIUS qui est un protocole client/serveur permettant de centraliser des données d'authentification et de définir les accès d'utilisateurs distants au réseau.

Références bibliographiques

[1] : G. PUJOLLE, « les réseaux », 5ème édition, EYROLLES, Août 2006.

[2] : D. SLIMANOU, « Mise en place d'une solution VPN sur pare-feu, Cas d'étude : Entreprise Tchin-Lait (Candia) », Master Professionnel en Informatique, spécialité Administration et Sécurité des Réseaux, 2017.

[3] : O. A. BENCHCHAOUI, « SSL VPN », projet technique, UNIVERSITÉ PARIS EST, Septembre 2011.

[4] : J.ARCHIER, « Les VPN - fonctionnement, mise en œuvre et maintenance des Réseaux Privés Virtuels », Édition ENI, Juin 2010.

[5] : https://excitingip.com/780/an-introduction-for-enterprise-vpn-virtual-private-network/

[6] : Xavier Lasserre et Thomas Klein, « Réseaux Privés Virtuels - VPN », Janvier 2007.

[7] : B. Patel, B. Aboba, W. Dixon, G. Zorn et S. Booth, « Securing L2TP using IPsec », Novembre 2001.

[8] : https://www.purevpn.fr/blog/openvpn-vs-sstp-vpn/

[9] : https://www.impactmybiz.com/blog/blog-site-to-site-vpn/

[10] : https://www.cloudflare.com/fr-fr/learning/network-layer/what-is-gre-tunneling/

[11] : http://www.hsc.fr/ressources/articles/ipsec-intro/ipsec-intro.pdf

[12] : J. MATTHIEU, « Les réseaux privés virtuels », Laboratoire supinfo des technologies unix, 2001-2002.

[13] : D. de REYNAL, J. G. de RORTHAIS et S. S. TAN, « Présentation sur les VPN », UFR Ingénieurs, France, 2004.

[14] : J. SOLANKI, « Etude IPSec et intégration de l'extension (mode config) dans le module IPSec des utms netasq », Rapport de stage, Université Bordeaux, Avril-Septembre 2008.

[15] : L. ARCHIM_EDE, Thomas CHEVALIER, Julien HERBIN, Sylvestre LEDRU et Nicolas PELLEGRIN, « Sécurité de l'information Tunnels et VPN », l'université paris 12, Mai 2004.

[16] : E. DENIZOT, J. PEREIRA, A. BERGER, « VPN (Virtual Private network), niveau 2 et niveau 3 », UPPA, 2007.

[17] : M. SUTER, « Sécurité informatique dans les entreprises suisses», Center for Security Studies (CSS), ETH, Zurich, Août 2006.

[18] : L. BLOCH, C. WOLFHUGEL, « Sécurité informatique Principes et méthodes », édition EYROLLES, Paris, 2007.

[19]: https://wakaziva.pagesperso-orange.fr/crypto/4.htm

[20] : S. Lynn, « DMVPN/GET VPN Design & Case Study », Consulting Systems Engineer CCIE 5507, 2008.

[21] : « Dynamic Multipoint VPN Design Guide », Version 1.1, Cisco Validated Design, Juillet 2008.

[22] : M. Sullenberger, « Advanced Concepts of DMVPN », BRKSEC-3052, Cisco Live, Février 2017.

[23] : Benoit, « DMVPN Phase », CCIE, Network Life, 2014.

[24]: https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn

[25] : « IP Routing: OSPF Configuration Guide », Cisco IOS Release 12.4T, Cisco Systems, Inc., CA 95134-1706 USA, 2011.

[26] : T. DANG NGOC, « Routage », Université de Cergy-Pontoise, 2012–2013.

[27] : Luc De Ghein, « Scaling BGP », BRKRST-3321, Cisco Live, Février 2016.

[28]: https://vpnstore.com/what-is-remote-access-vpn-and-how-does-it-work/

[29]:https://www.cisco.com/c/en/us/td/docs/iosxml/ios/sec_conn_esyvpn/configuration/15-mt/sec-easy-vpn-15-mt-book/sec-easy-vpn-srvr.html?dtid=osscdc000283

[30]:https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/wsa70/user_guide/AnyConnect_Secure_Mobility_SolutionGuide.pdf/

[31]:https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/vpn_clientless_ssl.pdf/vpn_groups.pdf?dtid=osscdc000283

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