REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de Technologie

Département Ingénierie des Systèmes Electriques

Mémoire de Master

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

DMVPN

« Dynamic Multipoint Virtual Private Network »

Réalisé par :

KENDJOUH Islam Abou Abderrahmane

Encadré par :

M. SEBTI Mohamed (Algérie Télécom)

MERAIHI	**Yassine :**	**Prof**	**UMBB**	**Président**
BENSAFI	**Noureddine :**	**MCB**	**UMBB**	**Examinateur**
MESSAOUDI	**Noureddine :**	**Prof**	**UMBB**	**Promoteur**

Année Universitaire : 2023/2024

Remerciements

Avant tout, je remercie Allah le tout puissant de m'avoir donné le courage et la patience nécessaires durant toutes ces années d'études, et de m'avoir donné la santé et la volonté pour entreprendre et achever ce modeste travail.

Je tiens à remercier monsieur ***Mohamed SEBTI*** *pour son aide immense, la qualité de son suivie ainsi que pour tous les conseils et les informations qu'il m'a prodigués avec un degré de patience et de professionnalisme sans égal.*

Je remercie mon promoteur, monsieur ***Noureddine MESSAOUDI*** *pour ses conseils éclairés, ses orientations précieuses et les enseignements enrichissants qu'il m'a prodigués tout au long de ce travail.*

Que les membres de jury trouvent, ici, l'expression de mes sincères remerciements pour l'honneur qu'ils me font en prenant le temps de lire et d'évaluer ce travail.

Je tiens énormément à remercier mes chers parents, pour leur support inconditionnel, leur patience et leur confiance depuis le début de mes études jusqu'au jour d'aujourd'hui.

Pour finir, je souhaite remercier toutes les personnes ayant apporté leur aide, leur soutien et contribué de près ou de loin à la réalisation de ce travail.

Dédicaces

Je dédie ce modeste travail à :

Mes chers parents, dont le soutien indéfectible, l'amour inconditionnel et les sacrifices ont été les fondations solides sur lesquelles j'ai pu bâtir mon chemin. Leur présence bienveillante et leur encouragement constant ont été une source infinie de motivation pour moi.

A mes chères sœurs Meriem et Amina que j'aime.

A ma famille de près ou de loin.

À tous mes amis et à toutes les personnes qui ont participé, de quelque manière que ce soit, dans la réalisation de ce modeste travail.

ISLAM

Résumé

Le DMVPN (Dynamic Multipoint Virtual Private Network) est une technologie de réseau basée sur les protocoles de tunneling VPN, il est principalement utilisé pour créer des connexions entre les sites distants à un réseau central de manière sécurisée et efficace. Il se distingue des VPN traditionnels par sa capacité à établir des tunnels de communication dynamiques sans nécessiter une configuration manuelle pour chaque site.

Les connexions sont initialement établies selon une architecture hub-and-spoke, puis les communications directes entre les spokes sont possibles une fois que les tunnels sont établis.

Ce projet vise à tester et à démontrer l'efficacité de la technologie DMVPN. En simulant les différentes phases, il évalue la facilité d'établissement des tunnels entre les sites distants et le hub central, ainsi que la capacité des sites distants à communiquer directement entre eux. Cela permet de vérifier la performance du réseau face à différents scénarios d'utilisation et de maintenance.

Mots clés : VPN, Routage, IPsec, Hub, Spoke, DMVPN, GRE, NHRP, Tunnel

---

Abstract

DMVPN (Dynamic Multipoint Virtual Private Network) is a networking technology based on VPN tunneling protocols, it is mainly used to create connections between remote sites to a central network in a secure and efficient manner. It differs from traditional VPNs in its ability to establish dynamic communication tunnels without requiring manual configuration for each site.

Connections are initially established using a hub-and-spoke architecture, then direct communications between spokes are possible once the tunnels are established.

This project aims to test and demonstrate the effectiveness of the DMVPN technology. By simulating the different phases, it evaluates the ease of establishing tunnels between remote sites and the central hub, as well as the ability of remote sites to communicate directly with each other. This makes it possible to check the performance of the network in the face of different usage and maintenance scenarios.

Keywords: VPN, Routing, IPsec, Hub, Spoke, DMVPN, GRE, NHRP, Tunnel

---

ملخص

DMVPN (الشبكة الافتراضية الخاصة الديناميكية متعددة النقاط) هي تقنية شبكات تعتمد على بروتوكولات نفقVPN ، وهي تستخدم بشكل أساسي لإنشاء اتصالات بين المواقع البعيدة والشبكة المركزية بطريقة آمنة وفعالة. وهو يختلف عن شبكات VPN التقليدية في قدرته على إنشاء أنفاق اتصال ديناميكية دون الحاجة إلى تكوين يدوي لكل موقع.

يتم إنشاء الاتصالات في البداية باستخدام بنية المحور والمتحدث، ثم تصبح الاتصالات المباشرة بين المتحدث ممكنة بمجرد إنشاء الأنفاق.

يهدف هذا المشروع إلى اختبار وإثبات فعالية تقنية DMVPN. ومن خلال محاكاة المراحل المختلفة، يتم تقييم مدى سهولة إنشاء الأنفاق بين المواقع البعيدة والمحور المركزي، فضلاً عن قدرة المواقع البعيدة على التواصل المباشر مع بعضها البعض. وهذا يجعل من الممكن التحقق من أداء الشبكة في مواجهة سيناريوهات الاستخدام والصيانة المختلفة.

الكلمات المفتاحية: VPN, Routage, IPsec, Hub, Spoke, DMVPN, GRE, NHRP, Tunnel

---

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

OSI : Open Systems Interconnection.

TCP/IP : Transmission Control Protocol/Internet Protocol.

DCN : Data Communication Network.

PAN : Personal Area Network.

LAN: Local Area Network.

MAN: Metropiltan Area Network.

WAN: Wide Area Network.

HTTP: HyperText Transfer Protocol.

FTP: File Transfer Protocol.

Wi-Fi: Wireless Fidelity.

P2P: Peer To Peer.

ISO: International Organization for Standardization.

DoS: Denial of Service.

DDoS: Distributed Denial of Service.

MitM: Man in the Middle.

DES: Data Encryption Standard.

AES: Advanced Encryption Standard.

RSA: Rivest-Shamir-Adleman.

ACL: Access Control List.

VLAN: Virtual Local Area Network.

NAT: Network Address Translation.

VPN: Virtual Private Network.

PPTP: Point-to-Point Tunneling Protocol.

L2TP: Layer 2 Tunneling Protocol.

IKEv2: Internet Key Exchange version 2.

SA: Security Association.

IPsec: Internet Protocole Security.

GRE: Generic Routing Encapsulation.

SSL: Secure Sockets Layer.

TLS: Transport Layer Security.

MPLS: Multi-Protocol Label Switching.

DMVPN: Dynamic Multipoint Virtual Private Network.

OEM: Original Equipment Manufacturer.

ISAKMP: Internet Security Association and Key Management Protocol.

AH: Authentification Header.

ESP: Encapsuling Security Payload.

NHRP: Next Hop Resolution Protocol.

NHC: Next Hop Client.

NHS: Next Hop server.

NBMA: Non-Broadcast-Multi-Access.

mGRE: multipoint Generic Routing Encapsulation.

EIGRP: Enhanced Interior Gateway Routing Protocol.

DUAL: Diffusing Update Algorithm.

OSPF: Open Shortest Path First.

EVE-NG: Emulated Virtual Environment Next Generation.

SSH: Secure Socket Shell.

IOS: Internetwork Operating System.

ISP : Internet Service Provider.

PPP : Point-to-Point Protocol.

Introduction générale

Dans le paysage actuel des télécommunications, les entreprises sont confrontées à une problématique majeure : comment assurer une connectivité réseau fiable et sécurisée entre des sites multiples et souvent éloignés, tout en maintenant des coûts et une complexité de gestion réduits ? Cette question est d'autant plus pertinente dans un contexte où la mobilité et le travail à distance sont devenus la norme, exigeant des solutions de réseau plus agiles et adaptables.

La solution à cette problématique réside dans l'innovation technologique du Dynamic Multipoint Virtual Private Network. Le DMVPN offre une alternative aux réseaux privés traditionnels en permettant la création de tunnels VPN dynamiques qui s'adaptent en temps réel aux changements de topologie du réseau. Grâce à l'utilisation de protocoles tels que GRE et NHRP, ainsi que le cryptage IPsec, le DMVPN simplifie la connectivité entre les sites distants, réduit les coûts opérationnels et améliore la sécurité des données.

En adoptant le DMVPN, les entreprises peuvent surmonter les défis de la connectivité réseau et se positionner avantageusement dans un environnement commercial de plus en plus compétitif et globalisé.

Organisation du mémoire

Ce mémoire comprend cinq chapitres principaux qui illustrent progressivement les différentes étapes que nous avons suivies pour parvenir à la réalisation de ce projet :

- ***Chapitre 1 " Généralités sur les réseaux Informatique" :*** Dans ce chapitre, nous nous concentrerons sur les bases théoriques des réseaux informatiques. Nous débuterons par une définition du concept de réseau, puis nous étudierons ses diverses classifications, architectures et topologies. Enfin, nous approfondirons notre compréhension des modèles de référence OSI et TCP/IP.
- ***Chapitre 2 "La sécurité Informatique" :*** Ce chapitre se concentre sur la sécurité informatique à travers l'exploration des types d'attaques courantes, des vulnérabilités et des méthodes de protection. Nous analyserons les approches pour sécuriser les réseaux, les systèmes d'exploitation, les applications et les données.

- ***Chapitre 3 "Initiation aux VPN" :*** Dans ce chapitre, nous allons explorer le monde des réseaux privés virtuels (VPN). Nous allons commencer par comprendre ce qu'est un VPN et comment il fonctionne. Nous allons également discuter des différents types de VPN, ainsi que les considérations à prendre en compte lors de la sélection d'un service VPN.
- ***Chapitre 4 "La technologie DMVPN" :*** Dans ce chapitre, nous abordons l'histoire, les principes et le fonctionnement de la technologie DMVPN. Nous détaillons également les divers modèles de déploiement et les phases clés associées à cette technologie.
- ***Chapitre 5 "Implémentation et configuration" :*** Ce chapitre commence par une présentation de l'organisme d'accueil ainsi que ses missions et ses objectifs fondamentaux. Ensuite, il détaille une démonstration pratique de l'implémentation de la technologie DMVPN à travers l'utilisation de l'émulateur EVE-NG.

Chapitre 1 : Généralités sur les réseaux Informatiques

1.1 Introduction

L'Internet d'aujourd'hui est sans doute le plus grand système d'ingénierie jamais créé par l'humanité, avec des centaines de millions d'ordinateurs connectés, de liaisons de communication et de commutateurs ; avec des milliards d'utilisateurs connectés…. Ce chapitre traite principalement de la théorie fondamentale des réseaux informatiques. Nous commencerons par définir ce qu'est un réseau et examinerons ses différentes classifications, architectures et topologies. Ensuite, nous explorerons les modèles de référence OSI et TCP/IP pour mieux comprendre leur fonctionnement et leur importance dans le domaine des réseaux.

1.2 Définition d'un réseau Informatique

Un réseau informatique, également appelé data communication network (DCN) en anglais, correspond à un ensemble de moyens matériels et logiciels reliés entre eux leur permettant d'échanger des informations et de partager des ressources. La liaison entre les différents éléments est faite avec ou sans fil.

Le modèle le plus simple comprend deux ordinateurs connectés par un câble. Dans cette situation, on évoque également la configuration peer-to-peer (P2P) ou en français pair à pair. Dans ce type de structure, il n'existe pas de hiérarchie : les deux participants sont au même niveau. Chaque ordinateur peut consulter les informations de l'autre et partager des ressources telles qu'un disque de stockage, des programmes ou des périphériques.

En général, les réseaux modernes sont beaucoup plus complexes et comprennent beaucoup plus d'outils informatiques que deux ordinateurs. La configuration de type client/serveur est généralement utilisée pour les systèmes à plus de dix participants. Dans cette approche, un ordinateur joue le rôle de point de commutation central (serveur) en mettant à disposition ses ressources. [1]

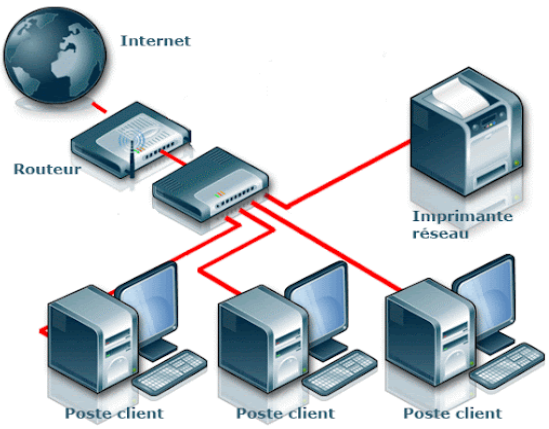

Figure 1.1: Réseau Informatique

1.3 Types de réseaux informatiques

Les critères permettant de distinguer un type de réseau d'un autre est difficiles et parfois déroutants. Nous utilisons quelques critères tels que la taille, la couverture géographique et la propriété pour faire cette distinction.[2] Un réseau informatique est principalement de quatre types :

1.3.1 Le réseau personnel ou PAN (Personal Area Network)

Un réseau personnel (PAN) est le plus petit réseau très personnel pour un utilisateur. Cela peut inclure des appareils compatibles Bluetooth ou des appareils compatibles infrarouge. PAN a une portée de connectivité jusqu'à 10 mètres. Le PAN peut inclure un clavier et une souris d'ordinateur sans fil, des écouteurs compatibles Bluetooth, des imprimantes sans fil et des télécommandes de téléviseur.

1.3.2 Le réseau local ou LAN (Local Area Network)

Un réseau local (LAN) est une infrastructure de communication qui relie des hôtes au sein d'une zone géographique restreinte, telle qu'un bureau, un bâtiment ou un campus. Chaque hôte possède une adresse unique qui permet d'acheminer les données vers le bon destinataire. Les LAN sont essentiels pour faciliter la communication et le partage de ressources au sein d'une organisation, offrant une connectivité locale efficace et sécurisée.

1.3.3 Le réseau métropolitain ou MAN (Metropiltan Area Network)

Un Réseau Métropolitain (MAN) est un type de réseau qui couvre une zone plus grande qu'un Réseau Local (LAN) mais plus petite qu'un Réseau Étendu (WAN), généralement au niveau d'une ville ou d'un grand campus. Utilisant des technologies à haute bande passante comme la fibre optique et les connexions sans fil, il permet une connectivité rapide et fiable entre plusieurs sites, facilitant la communication et le partage de ressources. Les MANs sont essentielles pour les entreprises, les gouvernements et les institutions éducatives qui nécessitent une communication efficace entre différents sites urbains. Bien que leur mise en œuvre soit coûteuse, ils offrent des vitesses de transfert élevées et améliorent considérablement la connectivité urbaine.

1.3.4 Le réseau étendu ou WAN (Wide Area Network)

Les WAN (Wide Area Network) appelés aussi réseaux longue distance se situent à l'échelle nationale et internationale. Ce sont généralement des réseaux de télécommunications gérés par des opérateurs, qui assurent la transmission des données entre les villes et les pays à l'échelle de la planète. Leurs supports de transmission sont variés (ligne téléphonique, ondes hertziennes, fibre optique, satellite, etc.). La plupart de ces types de réseaux sont publics.

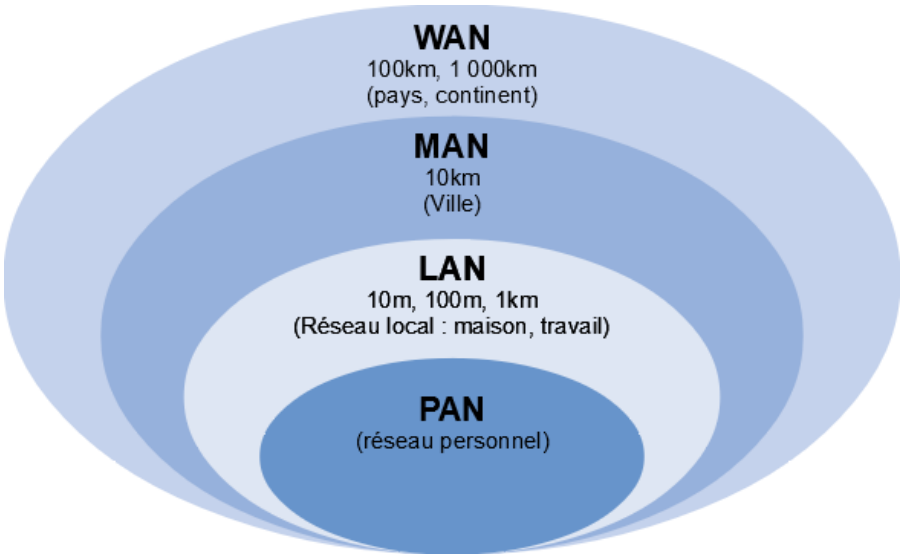

Figure 1.2: Classification des réseaux par portée géographique

1.4 Composants d'un réseau Informatique

Un réseau informatique est composé de plusieurs éléments essentiels. Voici les principaux composants:

- ***Postes informatiques (clients) :*** Ce sont les ordinateurs utilisés par les utilisateurs pour accéder au réseau. Ils peuvent être des ordinateurs de bureau, des ordinateurs portables, ou même des tablettes.
- ***Commutateurs (Switch) :*** Les commutateurs permettent de relier les postes clients, les serveurs et les imprimantes. Ils jouent un rôle crucial dans la communication entre les différents appareils du réseau.
- ***Modem (routeur) :*** Le modem (ou routeur) est utilisé pour se connecter au réseau Internet. Il agit comme une passerelle entre le réseau local et Internet, filtrant le trafic pour sécuriser le réseau local.
- ***Protocoles Internet :*** Les protocoles sont les langages de communication utilisés pour transférer des données sur Internet. Par exemple, HTTP est utilisé pour transférer des pages web, SMTP pour les e-mails, FTP pour le transport de fichiers, et POP3/IMAP pour la réception d'e-mails.
- ***Connexions :*** Les postes clients peuvent se connecter au réseau soit par câble (câble Ethernet) soit par ondes Wi-Fi. [3]

1.5 Architecture des réseaux

Les architectures réseau ont un rôle essentiel dans la communication et la partage des ressources entre les systèmes informatiques. Elles établissent les configurations et les techniques employées pour échanger des informations entre différents appareils et applications. Les architectures les plus fréquemment employées sont :

1.5.1 Poste à Poste ou P2P (Peer to Peer)

Réseau dans lequel tous les ordinateurs ont les mêmes possibilités de communication, et peuvent s'échanger des données ou partager les mêmes ressources, sans l'aide d'un serveur central ou de tout autre équipement d'interconnexion. [4]

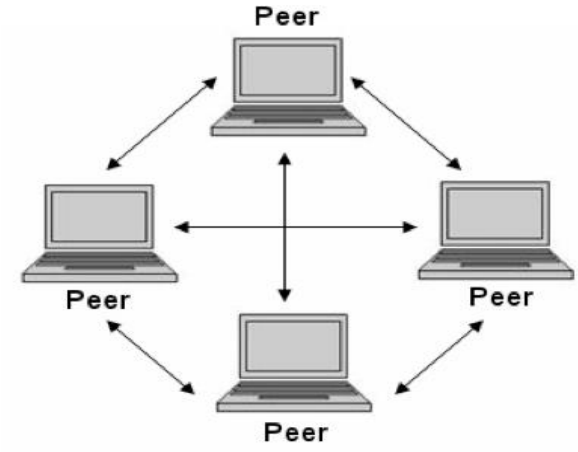

Figure 1.3: Architecture P2P

1.5.2 Client-serveur

Dans l'architecture client-serveur il y a un ordinateur centralisé qui est appelé un serveur et tous les autres ordinateurs sont appelés clients. Un serveur est dédié à répondre aux requetes des clients. Toutes les données sont stockées sur le serveur et peuvent être partagées avec les clients lorsqu'ils le demandent. Un serveur est responsable de la gestion des ressources, la gestion de la sécurité ainsi que la gestion du réseau. [4]

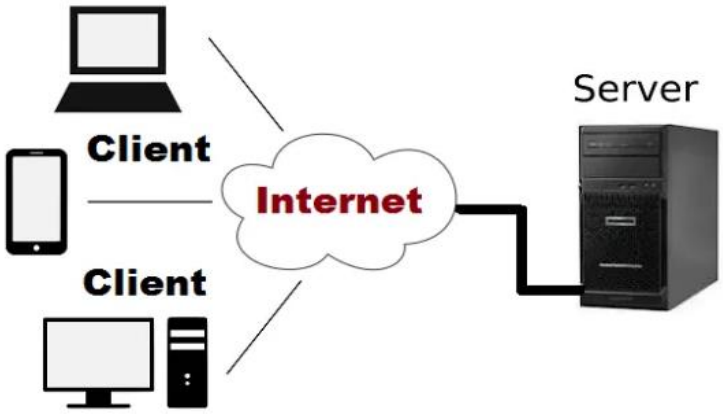

Figure 1.4: Architecture client-server

1.5.3 Trois tiers (Three-Tier)

L'architecture de réseau à trois niveaux est une configuration de réseau où chaque couche ou niveau est séparé logiquement et axé sur sa propre tâche. Cette configuration fournit trois environnements scalables indépendamment, qui séparent l'utilisateur final des serveurs d'application et de base de données.

Cela permet aux développeurs d'améliorer certaines parties de la pile réseau même si d'autres parties ne sont pas prêtes pour les mises à niveau. Par exemple, vous pouvez mettre à niveau vos serveurs de base de données, même si les serveurs d'application ne peuvent pas être mis à niveau en même temps en raison de problèmes tels que les dépendances logicielles ou les coûts de licence. [5]

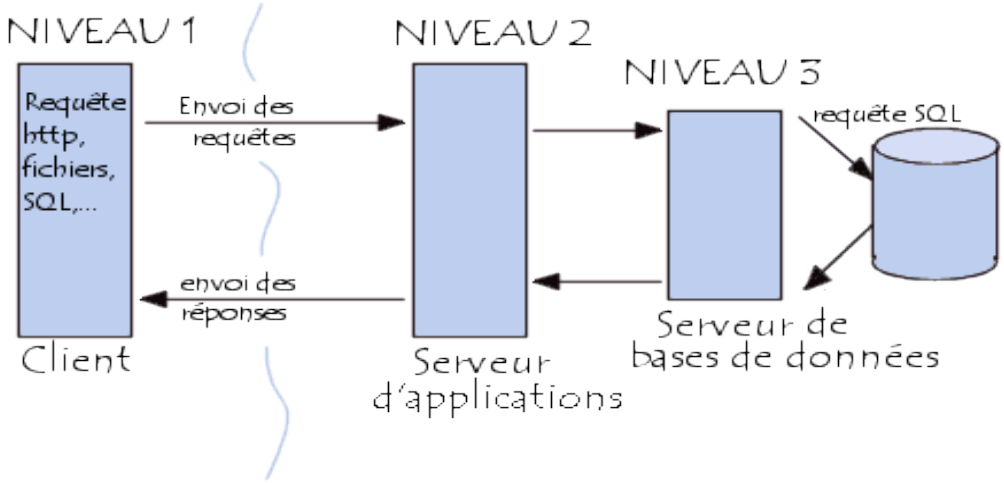

Figure 1.5: Three-Tier Architecture

1.6 Topologies des réseaux [4]

1.6.1 Topologie en bus

La topologie des bus, également appelée topologie de lignes, est un type de topologie réseau où tous les appareils d'un réseau sont connectés à un seul câble, appelé bus ou backbone. Ce câble sert de ligne de communication partagée, permettant à tous les appareils (ordinateurs, imprimantes, etc.) de recevoir le même signal simultanément.

La topologie du bus est bidirectionnelle, c'est-à-dire que les données sont transmises dans les deux directions sur le câble de la colonne vertébrale pour s'assurer qu'elle atteint le destinataire, indépendamment de sa position sur le bus. Selon le type de carte réseau, un câble de réseau twisted-pair (RJ-45 network cable) ou un câble coaxial est utilisé comme un bus (backbone cable) pour relier les périphériques de réseau, les ordinateurs ou les nœuds ensemble. [4]

1.6.2 Topologie en anneau (Ring)

La topologie en anneau est un réseau en boucle fermée dans lequel tous les appareils sont connectés dans une structure circulaire (en anneau).

Dans cette topologie, chaque appareil est connecté à deux autres appareils, un de chaque côté, formant un seul chemin continu pour la transmission des données. Les données sont envoyées d'un appareil à un autre en fonction du nœud voisin de leur nœud d'anneau.

Dans un réseau à topologie en anneau, les données se déplacent séquentiellement d'un nœud au suivant de manière unidirectionnelle. Cette topologie utilise généralement un mécanisme de contrôle de passage de Tokens pour garantir une transmission ordonnée des données et éviter les collisions. Dans ce mécanisme, seul le nœud détenteur du jeton a le droit de transmettre des données.

Lorsque vous souhaitez envoyer des données dans ce système, vous attendez que le token arrive sur votre appareil. Une fois que vous avez le token, vous pouvez joindre vos données et les envoyer au prochain appareil. L'appareil qui reçoit vos données devient le nouveau détenteur du token et le processus se répète. [4]

1.6.3 Topologie en étoile

Le système se repose sur un équipement central (le concentrateur ou hub) qui va diriger toutes les connexions. Si le concentrateur (hub) tombe en panne, le réseau est Indisponible. Par contre on peut retirer une station sans que le réseau entier ne tombe. L'inconvénient est que cela demande plus de câbles physiques [4].

1.6.4 Réseau maillé

Le réseau maillé est une topologie de réseau (filaire et sans fil) où tous les hôtes sont connectés pair à pair sans hiérarchie centrale, formant ainsi une structure en forme de filet. Chaque nœud doit recevoir, envoyer et relayer les données. Cette architecture évite les points névralgiques qui, s'ils tombent en panne, isolent une partie du réseau. Si un hôte est hors service, les données empruntent une route alternative. Les réseaux maillés sont utilisés pour leur tolérance aux pannes, leur capacité à optimiser le sans-fil, et leur réduction des coûts d'installation et d'exploitation. [4]

1.6.5 Topologie en arbre

Une topologie arborescente est une topologie de réseau hiérarchique ressemblant aux branches d'un arbre. Il combine les caractéristiques des topologies en étoile et en bus.

Dans cette topologie, les nœuds sont connectés à un nœud central, qui est ensuite connecté à un ou plusieurs nœuds à un niveau supérieur, et ce modèle continue de s'étendre vers l'extérieur comme un arbre. Le nœud le plus élevé est appelé « root (racine) » et sert de point d'origine au réseau. À partir de la racine, le réseau se ramifie vers des nœuds secondaires (nœuds intermédiaires), qui peuvent avoir leurs propres nœuds connectés (nœuds enfants), et ainsi de suite. [4]

1.7 Modèle OSI

Le modèle OSI (Open Systems Interconnection) est une norme de communication pour tous les systèmes informatiques en réseau. Proposé par l'ISO (International Organization for Standardization), il décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions. Le modèle OSI se compose de sept couches, allant de la couche physique, à la couche application. Chaque couche a des fonctions spécifiques, et l'ensemble du modèle permet d'assurer une communication efficace entre les ordinateurs.

Couches OSI	***Description***
1- Physique	Définit les caractéristiques physiques du réseau (câbles, signaux, etc.).
2- Liaison de données	Transmission de données fiable sur un seul lien physique.
3- Réseau	Routage des données sur le réseau (choix du meilleur chemin).
4- Transport	Assure un transport de données fiable entre applications.
5- Session	Gère les sessions de communication entre applications.
6- Présentation	Gère la représentation des données (formatage, chiffrement, etc.).
7- Application	Fournit des services aux applications (navigation web, email, etc.).

Tableau 1.1: Les couches du modèle OSI

1.8 Modèle TCP/IP (Transmission Control Protocol/Internet Protocol)

Le modèle TCP/IP est la méthode par défaut de communication des données sur Internet. Il a été développé par le Department of Defense des États-Unis pour permettre une transmission précise et correcte des données entre les appareils. Ce modèle se compose de quatre couches :

Couches TCP/IP	***Description***
1- Accès réseau	Cette couche gère la communication entre les périphériques locaux (par exemple, les cartes réseau) et les réseaux physiques (filaire ou sans fil). Elle inclut des protocoles tels que Ethernet.
2- Internet IP	Elle est responsable du routage des paquets de données à travers les réseaux. Le protocole IP permet d'adresser et d'acheminer les données entre les périphériques.
3- Transport	Cette couche gère la fiabilité de la communication. Le TCP assure la livraison fiable des données, tandis que l'UDP (User Datagram Protocol) est plus rapide mais moins fiable.
4- Application	Elle héberge les applications et services utilisés par les utilisateurs. Des protocoles tels que HTTP, SMTP, et FTP fonctionnent à cette couche

Tableau 1.2: Les couches du modèle TCP/IP

1.9 Conclusion

Les réseaux informatiques relient des machines et des dispositifs afin de partager des ressources et de transmettre des informations. Il existe différents types de réseaux, tels que les PAN, LAN, WAN et MAN, qui répondent à des exigences particulières. Les réseaux sont structurés selon diverses architectures, ce qui présente des bénéfices et des désavantages en ce qui concerne le coût, les performances et la fiabilité. Les modèles de communication réseau, comme OSI et TCP/IP, définissent la structure et la transmission des données. La compréhension de ces concepts fondamentaux est essentielle pour la conception, la configuration et la gestion efficaces des réseaux informatiques.

Chapitre 2 : La sécurité Informatique

2.1 Introduction

La sécurité informatique est l'ensemble des mesures et des pratiques visant à protéger les systèmes informatiques contre les menaces et les attaques. Elle est essentielle pour garantir la confidentialité, l'intégrité et la disponibilité des données et des services.

Ce chapitre explore les différents aspects de la sécurité informatique, notamment les types d'attaques courantes, les vulnérabilités et les techniques de protection. Nous examinerons les méthodes pour sécuriser les réseaux, les systèmes d'exploitation, les applications et les données.

2.2 Définition

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains requises afin de préserver, restaurer et assurer la sécurité des systèmes informatiques. Son objectif est de garantir la protection des biens informatiques tels que les systèmes, les réseaux, les appareils numériques et les données contre les accès non autorisées, les altérations de données et les cyberattaques. [6]

2.3 Les critères de sécurité

La sécurité de l'information dans une entreprise est une question essentielle qui préoccupe aujourd'hui tous les responsables. Afin de la mettre en œuvre, il est nécessaire de respecter quelques règles fondamentales, mais surtout, il est essentiel de respecter les critères majeurs en matière de sécurité. Il existe cinq criteres majeurs, comme illustré dans la Figure 2.1

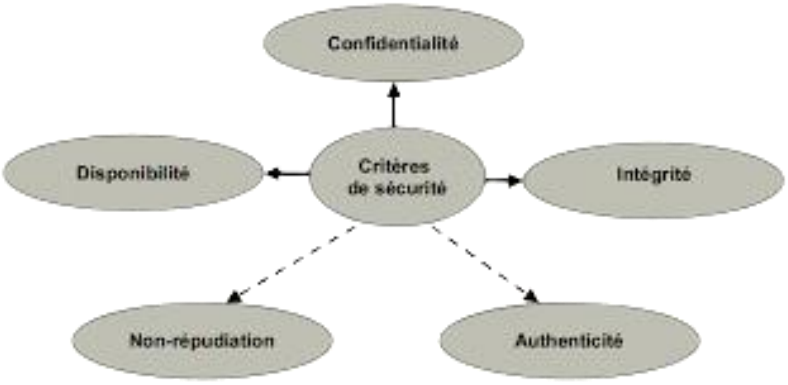

Figure 2.1: Critères de sécurité [7]

2.3.1 Intégrité

Le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions et services) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Une fonction de sécurité appliquée à une ressource pour contribuer à préserver son intégrité, permettra de la protéger plus ou moins efficacement contre une menace de corruption ou de destruction. [8]

2.3.2 Confidentialité

La confidentialité des données peut être définie comme la protection des données contre une divulgation non autorisée. Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données [9] :

- Limiter et contrôler leurs accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire.
- Rendre les données incompréhensibles en les chiffrant, seuls ceux qui disposent des moyens de déchiffrement appropriés peuvent y accéder.

2.3.3 Non répudiation

C'est le fait de ne pas pouvoir nier ou rejeter qu'un événement (actions, transactions) a eu lieu. A ce critère de sécurité peuvent être liées les notions suivantes [8] :

- L'imputabilité est l'attribution d'une action (un événement) à une entité déterminée ou personnes.
- La traçabilité permet de garder une trace numérique de tout événement (message électronique, transaction commerciale, transfert de données...).
- L'auditabilité définie la capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement (courant ou exceptionnel) effectué dans le cadre de procédure de contrôle spécifique et d'audit.

2.3.4 Authentification

C'est la propriété qui assure la vérification et la confirmation de l'identité des entités qui s'échangent des informations, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Parmi les moyens utilisés pour garantir l'authentification sont les login/mot de passe, certificats numériques, etc… [7]

2.3.5 Disponibilité

Assurer que l'information sur le système soit disponible aux personnes autorisées (garantir l'accès aux données). [9]

2.4 Terminologie de la sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini, il est nécessaire de définir certains termes [10] :

2.4.1 Vulnérabilité

Il s'agit d'une faille dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité de ce système.

2.4.2 Attaque

Une attaque est un programme, qui exploite une vulnérabilité dans un logiciel spécifique

2.4.3 Menace

Il s'agit d'un évènement, qui pourrait violer la sécurité d'un système d'information.

2.4.4 Contre-mesure

Il s'agit d'une procédure ou d'une technique, permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.

2.5 Les techniques d'attaques

Les hackers utilisent plusieurs techniques d'attaques qui peuvent être regroupées en trois familles différents [11] :

2.5.1 Attaques directs :

C'est la plus simple des attaques. L'hacker attaque directement sa victime à partir de son ordinateur à l'aide d'un logiciel ou d'un script lui permettant d'envoyer directement les paquets à la victime.

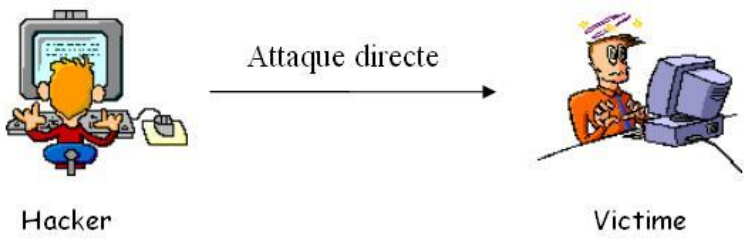

Figure 2.2: Attaque direct

2.5.2 Attaques indirect par rebond

Appelée « Attaque indirecte par rebond » car le principe est d'envoyer les paquets d'attaque à l'ordinateur intermédiaire, qui à son tour répercute l'attaque vers la victime.

Ce type d'attaque est appréciée des hackers, car elle permet de :

- Masquer l'identité de l'hacker.
- Utiliser les ressources de l'ordinateur intermédiaire pour attaquer car il est plus puissant.

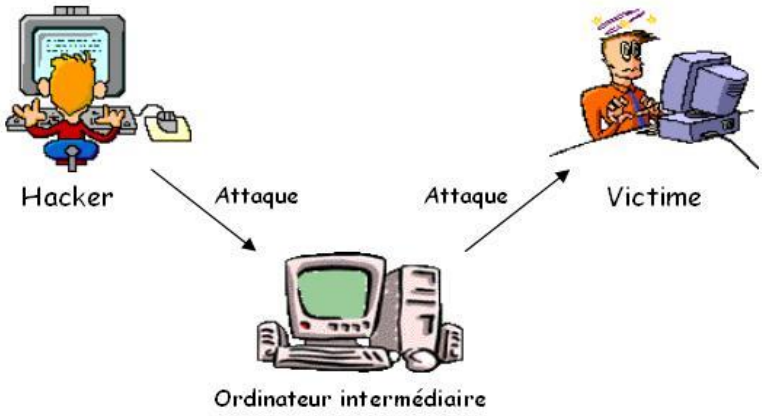

Figure 2.3: Attaque indirecte par rebond

2.5.3 Attaques indirectes par réponse

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue de l'hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.

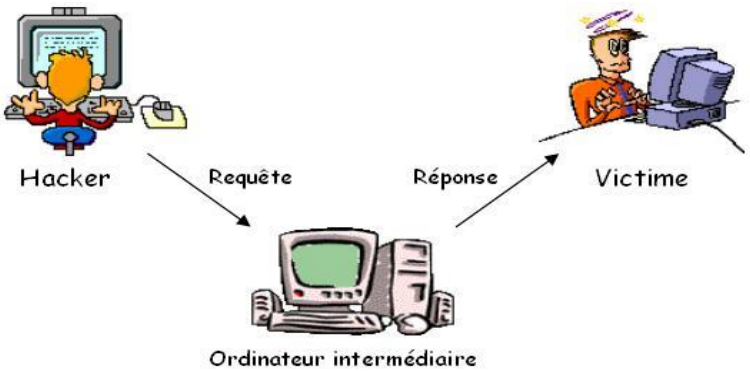

Figure 2.4: Attaque indirecte par réponse

2.6 Les types d'attaques :

2.6.1 Attaques par déni de service (DoS) et par déni de service distribué (DDoS)

Une attaque par déni de service **DoS** est une attaque malveillante visant à compromettre un système d'exploitation informatique en saturant un serveur, rendant ainsi un site Web ou une ressource indisponible. Elle se produit généralement via les failles d'un réseau qui héberge un site internet. L'objectif de l'hacker est de mettre en défaut le site en lui-même et de le bloquer. En revanche, une attaque par déni de service distribué **DDoS** provient de nombreuses sources distribuées. Elle est plus puissante et difficile à contrer, car elle utilise plusieurs ordinateurs ou machines pour saturer une ressource ciblée. Les conséquences d'une attaque par déni de service sont immédiates pour une entreprise, provoquant des pertes financières et nécessitant des investissements pour remettre à niveau le site infecté. [8]

2.6.2 Attaque de l'homme au milieu (MITM)

Une attaque de type homme du milieu, ou Man In The Middle, est une cyberattaque lors de laquelle un cybercriminel intercepte des données envoyées entre deux entreprises ou individus. L'objectif de cette interception est de voler, d'écouter ou de modifier les données à des fins malveillantes, comme l'extorsion de fonds.

Les attaques de l'homme du milieu reposent sur la manipulation de réseaux existants ou la création de réseaux malveillants, contrôlés par le cybercriminel. Le pirate intercepte le trafic et le laisse transiter, recueillant des informations au passage, ou le redirige vers un autre endroit. [9]

2.6.3 IP spoofing

L'usurpation d'adresse IP est la création de paquets IP contenant une adresse source modifiée afin de cacher l'identité de l'expéditeur ou pour se faire passer pour un autre système informatique, ou les deux.

2.6.4 Attaques par mot de passe

Les attaques de mot de passe sont l'une des formes les plus courantes de violation des données d'entreprise et personnelles. Voici quelques types d'attaques de mot de passe :

- ***Hameçonnage :*** Un hacker envoie un e-mail frauduleux se faisant passer pour un organisme de confiance, vous incitant à révéler vos informations personnelles.
- ***Pulvérisation de mots de passe :*** Le cybercriminel utilise un même mot de passe courant pour tenter d'accéder à plusieurs comptes d'une application donnée.

- ***Attaque par force brute :*** L'attaquant essaie de deviner les mots de passe en utilisant la méthode des essais et des erreurs. C'est l'une des plus anciennes attaques, mais elle est toujours utilisée. [8]

2.6.5 Logiciel malveillant (malware)

Un logiciel malveillant, également appelé malware, est un programme ou un code créé dans le but de causer des dommages à un ordinateur, un réseau ou un serveur. Presque toutes les cyberattaques modernes impliquent un type de logiciel malveillant.

La plupart des logiciels malveillants peuvent être classés dans l'une des catégories suivantes :

- **Virus :** Les Virus informatiques sont des codes qui ont la particularité de reproduire, d'infecter, d'activer et d'altérer ou même détruire le fonctionnement du système ou de l'information stockée.
- **Ver :** Se réplique automatiquement pour propager l'infection à un réseau.
- **Rootkit :** Permet aux pirates de contrôler à distance le terminal de la victime.
- **Cheval de Troie (Trojen) :** Prend l'apparence d'un code légitime.
- **Spyware :** Collecte des informations sur l'activité de l'utilisateur à son insu.
- **Adware :** Affiche des publicités indésirables.
- **Ransomware :** Bloque l'accès de la victime à ses données jusqu'au paiement d'une rançon.

Comme présenté dans la Figure 2.5, une attaque peut être classée par son comportement ou par la position de l'attaquant.

Une attaque peut être active ou passive.

- Une attaque active tente de modifier les ressources du système ou d'affecter leur fonctionnement.
- Une attaque passive tente d'apprendre ou d'utiliser des informations du système mais n'affecte pas les ressources du système.

Une attaque peut être perpétrée de l'intérieur ou de l'extérieur de l'organisation.

- Une attaque interne est une attaque initiée par une entité dans le périmètre de sécurité, c'est-à dire une entité autorisée à accéder aux ressources du système mais qui les utilise d'une manière non approuvée par ceux qui ont accordé l'autorisation.
- Une attaque extérieure est initiée depuis l'extérieur du périmètre, par un utilisateur non autorisé ou illégitime du système.

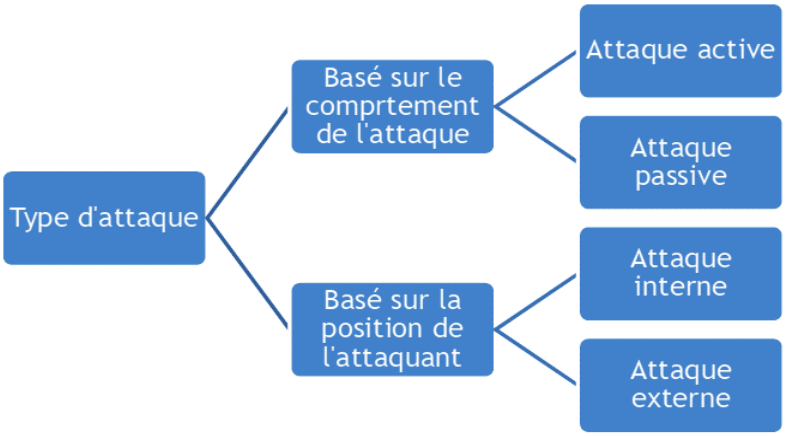

Figure 2.5: Les types d'attaques

2.7 Les mesures de sécurité

2.7.1 Antivirus

Un antivirus est conçu pour détecter, prévenir et éliminer les menaces telles que les spywares, les ransomwares, les chevaux de Troie et autres malwares. Son rôle principal est de protéger vos appareils et les réseaux contre les attaques malveillantes. Il identifie et supprime les fichiers et codes dangereux qui pourraient endommager vos données, corrompre le système d'exploitation ou compromettre la confidentialité des utilisateurs. [12]

2.7.2 Cryptage

Un ensemble de technique permettant de transformer les données dans le but de cacher leur contenu, empêcher leur modification ou leur utilisation illégale. Ceci donne la possibilité d'obtenir un texte en réalisant des algorithmes de déchiffrement. [12]

Elle est désormais utilisée pour assurer la confidentialité des données tout en assurant leur intégrité et leur authenticité.

2.7.2.1 Techniques de chiffrement

La sécurisation des échanges entre l'utilisateur et les différents services du réseau passe par un chiffrement des transactions. Deux systèmes de chiffrement s'offrent à nous, le chiffrement à clé symétrique et celui à clé asymétrique. [13]

- ***Chiffrement symétrique :*** également dite à clé secrète est la plus ancienne forme de chiffrement. Il s'agit de chiffrer le message envoyé grâce à une clé qui sera réutilisée par le destinataire pour déchiffrer le message crypté. Le problème de cette méthode est que tous les utilisateurs possèdent alors la même clé partagée, la sécurité n'existe plus puisque pour déchiffrer les transactions d'un autre utilisateur il suffit d'utiliser la clé unique que tous

les utilisateurs possèdent. Les algorithmes les plus connus dans le chiffrement symétrique : DES, AES, 3DES.

- ***Chiffrement asymétrique :*** La cryptographie asymétrique, ou cryptographie à clé publique repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de chiffrer le message et l'autre de le déchiffrer. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour chiffrer un message que seul le destinataire (en possession de la clé privée) peut le déchiffrer, garantissant la confidentialité du contenu. RSA est l'algorithme le plus utilisé dans le chiffrement asymétrique.

2.7.2.2 Hachage

Le hachage est une technique cryptographique qui transforme les données d'entrée en une chaîne de caractères alphanumériques de longueur fixe, appelée (empreinte) ou (digest). Cette empreinte est unique à chaque ensemble de données, et la moindre modification des données d'origine engendre une empreinte complètement différente. Le hachage est utilisé dans divers contextes pour assurer l'intégrité et la sécurité des informations. [14]

2.7.2.3 La différence entre un hachage et un chiffrement

Le chiffrement protège la confidentialité des données, les rendant lisibles uniquement par des parties autorisées, tandis que le hachage vérifie l'intégrité des données, garantissant qu'elles restent inchangées et non corrompues.

2.7.3 Firewall

Un firewall, aussi appelé pare-feu, est un logiciel ou un matériel qui permet de définir une politique de sécurité pour un réseau informatique.

Rôle du firewall :

- Bloquer l'accès non autorisé à un réseau et contrôle les communications entrantes et sortantes à l'aide d'un ensemble de règles de sécurité.
- Etablir une barrière de protection entre les réseaux fiables et les réseaux externes moins sécurisés.
- Utilisé par les entreprises et les particuliers, il protège contre les menaces pour les ordinateurs personnels et autres systèmes informatiques. [10]

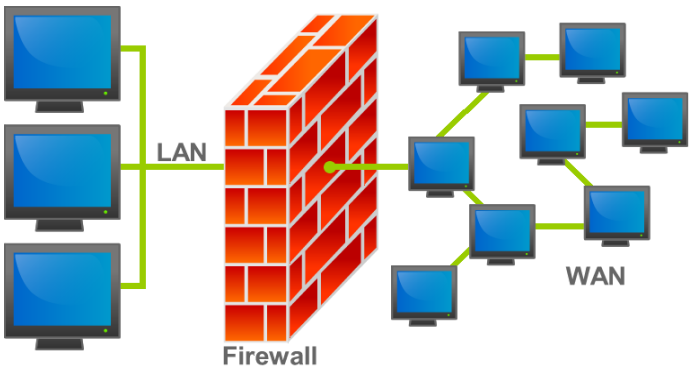

Figure 2.6: Firewall [15]

2.7.4 Les listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès ont pour objectif de disposer d'une fonction de filtrage prenant en compte l'historique des connexions en cours, afin de ne pas accepter du trafic qui n'aurait pas été demandé à partir d'une zone précise du réseau. [12]

2.7.5 VLAN (Virtual LAN)

Un VLAN, ou Réseau Local Virtuel, est une solution astucieuse qui permet de diviser un réseau Ethernet physique en plusieurs sous-réseaux logiquement distincts. Malgré leur partage d'une infrastructure physique unique, ces sous-réseaux agissent comme s'ils étaient séparés, offrant une isolation entre eux. [12]

2.7.6 NAT

La traduction d'adresses réseau (NAT) est un processus essentiel dans les réseaux informatiques. Le NAT modifie les adresses IP et les ports source et destination. Il réduit le besoin d'adresses publiques en masquant les plages d'adresses privées. Généralement, les routeurs et les pares-feux sont responsables de cette fonctionnalité.

Types de NAT :

- ***NAT statique :*** Traduit une adresse IP privée en une adresse publique fixe.
- ***NAT dynamique :*** Mappe les adresses IP privées à un pool d'adresses publiques.
- ***PAT (Port Address Translation) :*** Utilise une seule adresse IP publique avec des ports différents pour chaque adresse IP privée.

2.7.7 VPN

Un VPN applique un protocole de chiffrement pour faire transiter l'ensemble de votre trafic Internet par un tunnel chiffré entre votre ordinateur et un serveur VPN distant. Cette opération masque votre adresse IP et protège vos données, évitant ainsi que d'autres utilisateurs puissent les intercepter. (Nous le détaillerons dans le prochain chapitre).

2.8 Conclusion

Ce chapitre aborde les principaux défis de la sécurité informatique à l'ère numérique. Nous avons examiné les différentes techniques d'attaques et les types d'attaquants, ainsi que les mesures de base de protection individuelle et organisationnelle pour faire face aux attaques. Le prochain chapitre sera consacré aux VPN.

Chapitre 3 : Initiation aux VPN

3.1 Introduction

Le monde numérique d'aujourd'hui est de plus en plus interconnecté, mais aussi de plus en plus vulnérable. Alors que nous partageons et accédons à des informations en ligne, la sécurité et la confidentialité de ces informations deviennent une préoccupation majeure. C'est là qu'interviennent les Réseaux Privés Virtuels (VPN).

Dans ce chapitre, nous allons comprendre ce qu'est un VPN et explorer leur fonctionnement et leur caractéristiques. Nous aborderons les différents protocoles utilisés par les VPN, ainsi leur avantages et Inconvénients.

3.2 Définition et fonctionnement

Un VPN (Virtual Private Network) est un service qui crée un tunnel sécurisé sur internet. En chiffrant les données échangées entre votre ordinateur et les serveurs du VPN, il assure que vos informations restent privées et à l'abri des regards indiscrets. [16]

Un réseau VPN est basé sur le protocole de tunneling. Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

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. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les VPN d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation. [17]

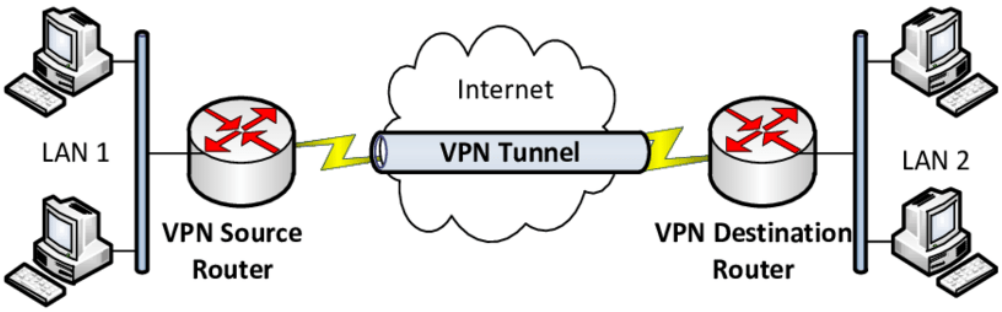

Figure 3.1: Structure de tunneling VPN [18]

3.3 Les différents types de VPN

Les entreprises font de plus en plus appel à des réseaux privés virtuels pour relier à leurs réseaux, leurs filiales, leurs télétravailleurs, leurs partenaires et d'autres utilisateurs. Alternative aux solutions d'appels à distance... Les VPN permettent de transférer en sécurité des données, pour un coût plus faible par l'utilisation d'Internet, à priori, déjà disponible. [19]

Suivant les besoins, on référence trois types de VPN :

- **Le VPN d'accès :** Il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion Internet afin d'établir une liaison sécurisée.

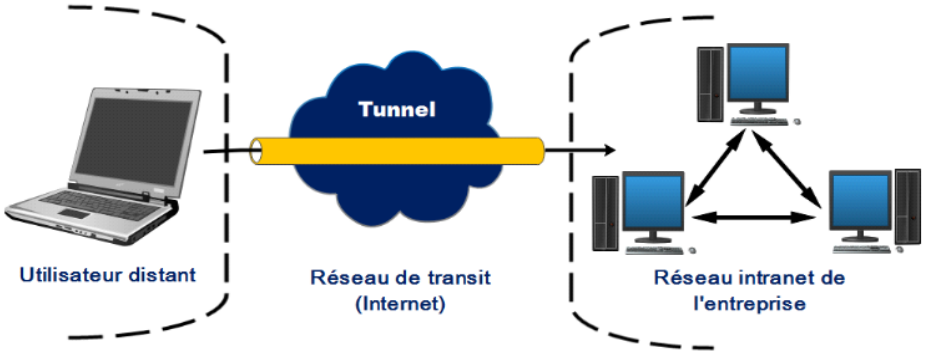

Figure 3.2: Architecture d'un VPN d'accès. [19]

- **L'intranet VPN :** Est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité de données. Une entreprise peut utiliser ce type de VPN pour communiquer avec ses clients et ses partenaires.

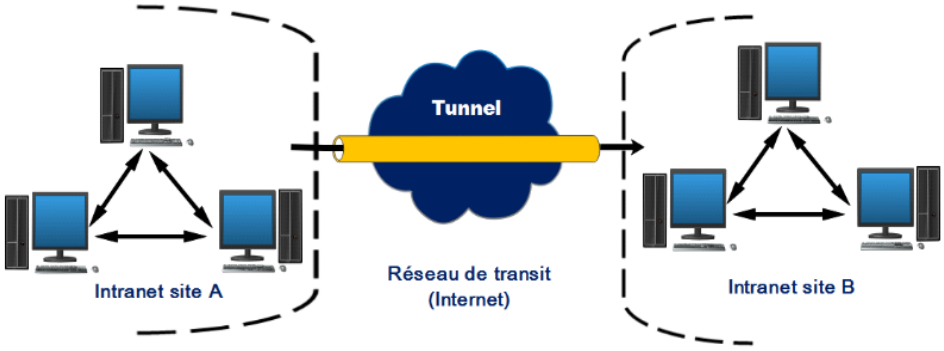

Figure 3.3: Architecture d'un VPN Intranet. [19]

- **L'extranet VPN:**

Une entreprise peut utiliser le VPN extranet pour communiquer avec ses clients, les fournisseurs et les partenaires au moyen d'un intranet d'entreprise reposant sur une infrastructure partagée à l'aide de connexions dédiées. Dans ce cas, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

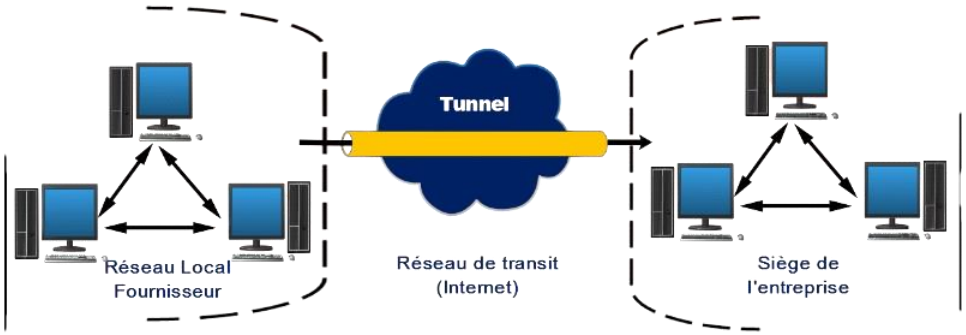

Figure 3.4: Architecture d'un VPN extranet. [19]

3.4 Les caractéristiques d'un VPN

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

- ***Authentification d'utilisateur :*** Seuls les utilisateurs autorisés doivent avoir accès au canal VPN.
- ***Cryptage des données :*** Lors de leur transport sur le réseau public les données doivent être protégées par un cryptage efficace.
- ***Gestion de clé :*** les clés de cryptage pour le client et pour le serveur doivent pouvoir être générées et régénérées.
- ***Prise en charge multi protocole :*** La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

3.5 Les principaux avantages des VPN

Comme nous venons de le voire les VPN disposent de nombreux avantages, Il existe plusieurs raisons pour lesquelles il est judicieux utiliser un VPN. Parmi ces avantages on trouve:

- Gratuité ou coût assez faible.
- Une couverture géographique mondiale.
- Sécurité assez efficace.
- Assure la continuité de transmission de données. [20]

3.6 Les Inconvénients des VPN

- Quelques failles de sécurité.
- Les performances ne sont pas toujours au rendez-vous.
- Utiliser un VPN Peut s'Avérer Compliqué. [20]

3.7 Les protocoles de tunneling

Les protocoles VPN se distinguent par leur mode opératoire et leur implication dans les couches du modèle OSI, les plus fréquents sont :

- PPTP, L2TP, Open source, GRE, SSL, IKEv2, WireGuard, IPsec, DMPVN.

3.7.1 PPTP (Point-to-Point Tunneling Protocol)

Le protocole PPTP (Point-to-Point Tunneling Protocol) est l'un des plus anciens protocoles VPN. Développé à l'origine par Microsoft dans les années 1990, PPTP a été conçu pour créer une connexion sécurisée et privée entre des utilisateurs distants et un réseau d'entreprise.

PPTP fonctionne en encapsulant les données transmises entre l'appareil d'un utilisateur et un serveur VPN dans un tunnel sécurisé et crypté. Ce tunnel est créé en établissant une connexion PPP (Point-to-Point Protocol) entre l'appareil de l'utilisateur et le serveur VPN. Une fois la connexion PPP établie, le protocole PPTP est utilisé pour crypter les données transmises.

Cependant, malgré son utilisation répandue, PPTP présente des failles de sécurité significatives qui le rendent vulnérable au piratage et à la surveillance. [21]

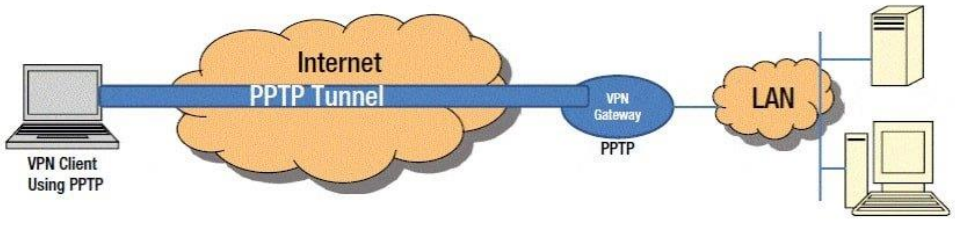

Figure 3.5: PPTP Architecture [22]

3.7.2 L2TP (Layer 2 Tunneling Protocol)

L2TP signifie protocole de tunnelisation de couche 2. L2TP a été proposé pour la première fois en 1999 comme amélioration de PPTP. Sachant que L2TP ne permet pas un chiffrement ou un système d'identification robuste, un autre protocole, appelé IPsec, est souvent utilisé conjointement avec L2TP.

IPsec utilise des algorithmes de chiffrement et des clés cryptographiques pour fournir à L2TP le chiffrement nécessaire. IPsec contrôle également les données qui circulent entre endpoints du tunnel de connexion créé entre l'utilisateur final et un serveur VPN en ligne.

Utilisés ensemble, L2TP et IPsec sont bien plus sécurisés que PPTP (Protocole de tunnellisation de point en point), mais ils restent plus adaptés à l'anonymisation qu'à la sécurité. [23]

3.7.3 OpenVPN

OpenVPN est un protocole open source de VPN qui permet de créer des connexions sécurisées et privées entre un appareil et un réseau distant, généralement via Internet, Il utilise es protocole SSL (Secure Sockets Layer) qui est un protocole de sécurité qui crée un lien chiffré entre un serveur Web et un navigateur Web pour assurer la sécurité des communications.

OpenVPN peut créer un tunnel en utilisant soit le protocole TCP pour une sécurité maximale, soit le protocole UDP pour une vitesse brute.

Pour le chiffrement, il se repose sur la bibliothèque OpenSSL qui fournit les algorithmes de cryptographie fondamentales à utiliser pour construire un réseau VPN sécurisé.

Figure 3.6: OpenVPN Logo

3.7.4 IKEv2

Le protocole IKEv2 (Internet Key Exchange version 2), également appelé IKEv2/IPsec, est un protocole VPN avancé développé conjointement par Cisco et Microsoft, qui offre un équilibre entre sécurité et vitesse. Il s'appuie fortement sur IPsec pour sécuriser la communication entre un client VPN et un serveur VPN.

IKEV2 met en place une association de sécurité (SA) qui négocie les clés de sécurité utilisées à la fois par le client VPN et par le serveur VPN.

Une fois que IKEv2 valide l'association de sécurité, un tunnel sécurisé est défini, qui incite à une communication cryptée entre les deux homologues. [24]

3.7.5 IPsec

IPsec est un protocole de sécurité pour les réseaux IP qui protège les données en transit en utilisant des mécanismes de chiffrement, d'authentification et de vérification de l'intégrité, Nous détaillerons ce protocole dans le prochain chapitre.

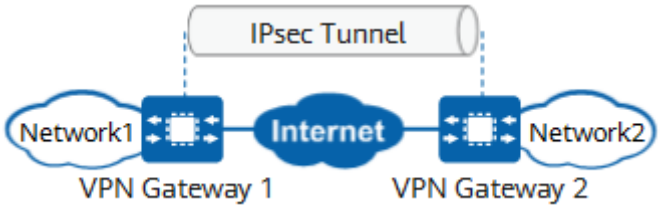

Figure 3.7: IPsec [25]

3.7.6 GRE (Generic Routing Encapsulation)

Le protocole GRE est un protocole de tunneling qui permet d'encapsuler des paquets de différents protocoles dans des paquets IP. Il est conçu pour encapsuler n'importe quel paquet de la couche réseau dans sa conception d'origine. Le paquet d'origine est le payload (information utile) du paquet final.

GRE a été développé par Cisco et peut encapsuler une large gamme de types de paquets de différents protocoles dans des paquets IP. Les tunnels GRE sont conçus pour ne pas avoir besoin de maintenir un état, ce qui signifie que chaque terminaison de tunnel ne conserve aucune information d'état ou de disponibilité de la terminaison distante. Ceci donne aux utilisateurs la flexibilité de configurer ou reconfigurer leur architecture IP sans être concernés par les problèmes de connectivité, en créant tunnel point à point virtuel vers des routeurs distants à travers des réseaux IP. [26]

3.7.7 SSL/TLS (Secure Sockets Layer) / (Transport Layer Security)

Ce sont des protocoles permettant de sécuriser les échanges sur internet. Développé à l'origine sous le nom SSL par Netspace. Ce sont des protocoles très largement utilisé car les protocoles de la couche application, comme http, n'ont pas besoin d'être profondément modifiés pour utiliser une connexion sécurisée. Ils sont seulement implémentés au-dessus de ces protocoles, ce qui donne pour le http : Https. Il permet l'utilisation d'un navigateur Web comme client VPN.

3.7.8 MPLS (Multi-Protocol Label Switching)

Est un protocole de niveau 3 (Réseau) qui permet d'établir un tunnel privé au sein d'un réseau public, il est utilisé par les fournisseurs d'accès à l'Internet pour proposer à leurs clients un moyen de créer un réseau privé entre plusieurs sites d'une même entreprise.

Protocole	***Avantages***	***Inconvénients***
PPTP	✚ Facile à configurer et à utiliser. ✚ Établissement de connexions rapides. ✚ Compatible avec tous les systèmes d'exploitation, les smartphones, les tablettes et les routeurs.	✚ Sécurité faible. ✚ Vulnérable aux attaques. ✚ Peut être facilement bloqué par les FAI.
L2TP/IPsec	✚ Facile à installer et à configurer. ✚ Connexions stables et fiables ✚ Sécurité renforcée par IPsec.	✚ Vitesse de connection réduite. ✚ Non compatible avec tous les systèmes d'exploitation.
OpenVPN	✚ Sécurité élevée. ✚ Configurabilité avancé. ✚ Permet de passer la plupart des firewalls et des restrictions réseaux/FAI. ✚ Open source.	✚ Difficile à configurer. ✚ Nécessite une installation supplémentaire. ✚ Compatibilité limitée.
IKEv2	✚ Extrêmement sécurisé. ✚ Connexion stable et fiable. ✚ Plus rapide que la plupart des autres protocoles.	✚ Prend en charge un nombre limité de plates-formes. ✚ Pas de solution opensource. ✚ Installation supplémentaire requise.
GRE	✚ Multi-protocole. ✚ Simplicité. ✚ Compatible avec un grand nombre d'équipements réseau.	✚ Sécurité faible. ✚ Non recommandé pour les utilisateurs professionnels.
SSL/TLS	✚ Offre un cryptage puissant des données. ✚ Protège les données saisies par les utilisateurs de votre site Web. ✚ Les données sont chiffrées de bout en bout.	✚ Coût du certificate. ✚ Problèmes de configuration.
MPLS	✚ Optimisation du trafic. ✚ Assure des connexions fiables pour les applications en temps réel.	✚ Coûteux. ✚ Déploiements gourmands en ressources.

Tableau 3.1: Comparatif des Protocoles VPN

3.8 Conclusion

Les VPN sont des outils essentiels pour garantir la confidentialité et la sécurité en ligne, offrant une solution efficace pour protéger les données et préserver l'anonymat en ligne.

Dans ce chapitre, nous avons exploré le concept des VPN, leur fonctionnement et leurs caractéristiques. Nous avons également abordé les différents protocoles utilisés par les VPN et évalué leurs avantages et inconvénients.

Chapitre 4 : La technologie DMVPN

4.1 Historique

Afin de sécuriser les connexions via internet, les fournisseurs de services arrivent en premier avec la solution d'IPsec, où deux sites sont connectés sur internet via un processus de tunnel crypté sécurisé. Cette dernière, malgré son excellent fonctionnement, ne peut malheureusement pas être évolutif entre plusieurs sites, car elle sécurise que les connexion point à point. En effet, l'ajout d'un site nécessite une configuration complexe, en interne de pour les équipement mis en production, mais surtout, pour la mise à l'échelle car plus les sites augmentes plus la configuration du site central devient rapidement difficile à gérer. Aussi, ce type de VPN ne supporte pas le routage dynamique et le Multicast.

Ces principales limites ont poussé les fournisseurs de services et les OEM (Original Equipment Manufacturer) à conclure une manière de connectivité évolutive et sécurisée entre sites via Internet et cette technologie est appelée DMVPN (Dynamique Multipoint Virtual Private Network).

Avec DMVPN, Cisco introduit une approche plus dynamique et automatisée des VPN multipoints. Il permet de créer des connexions sécurisées entre plusieurs sites distants tout en simplifiant la gestion et le déploiement des tunnels VPN. DMVPN utilise des protocoles de routage dynamique pour découvrir et mettre à jour plus facilement les routes entre les sites, offrant une connectivité transparente.

DMVPN est devenu populaire grâce à sa flexibilité, sa capacité et la simplification de la configuration. Il permet aux entreprises de connecter efficacement et en toute sécurité de nombreux sites distants, y compris des bureaux, des succursales et des utilisateurs mobiles.

Bien que DMVPN soit une technologie développée par Cisco, d'autres fournisseurs de matériel réseau ont également mis en œuvre des fonctionnalités similaires dans leurs solutions, sous d'autres noms ou standards (ADVPN de Fortinet). Cependant, le terme "DMVPN" est généralement associé à la solution développée par Cisco. [27]

4.2 Définition

DMVPN (Dynamic Multipoint VPN) est une technique de routage que nous pouvons utiliser pour créer un réseau VPN avec plusieurs sites sans avoir à configurer statiquement toutes les unités. Il s'agit d'un réseau « hub and spoke » où les spokes pourront communiquer directement entre eux sans avoir à passer par le hub. Le cryptage est pris en charge via IPsec, ce qui fait du DMVPN un choix populaire pour connecter différents sites à l'aide de connexions Internet classiques. [28]

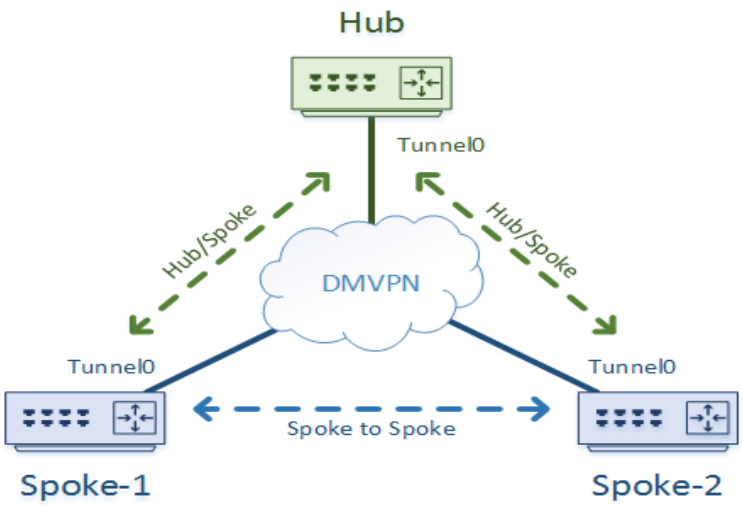

Figure 4.1: DMVPN Topology [29]

4.3 Principes du DMVPN

Le DMVPN est un mécanisme qui établie des tunnels IPsec/GRE (Generic Routing Encapsulation) directement entre les routeurs qui veulent interagir de manière simple et dynamique. GRE est un protocole d'encapsulation permettant l'encapsulation des paquets multidiffusion et diffusion dans un paquet de monodiffusion. Par conséquent, il sera chiffré en utilisant IPsec. Fondamentalement, la solution consiste à implémenter des paquets multidiffusion à l'aide de tunnels GRE, sécurisés par l'IPsec. [30] Les composants du DMVPN sont :

4.3.1 IPsec

IPsec est un ensemble de règles ou de protocoles de communication permettant d'établir des connexions sécurisées sur un réseau. Le protocole Internet (IP) est la norme commune qui détermine comment les données circulent sur Internet. IPsec ajoute le chiffrement et l'authentification pour rendre le protocole plus sûr. Par exemple, il chiffre les données à la source et les déchiffre à la destination. Il authentifie également la source des données.

4.3.1.1 Gestion des clés dans IPsec

- ***IKE (Internet Key Exchange) :*** Internet Key Exchange (IKE) est un protocole standard utilisé pour établir un canal de communication sécurisé et authentifié entre deux parties via un réseau privé virtuel (VPN). Le protocole garantit la sécurité de la négociation VPN, de l'hôte distant et de l'accès au réseau. Un rôle essentiel d'IKE consiste à négocier des associations de sécurité (SA) pour la sécurité IP (IPsec). Les SA sont des politiques de sécurité définies pour la communication entre deux ou plusieurs entités. Un ensemble

d'algorithmes et de clés mutuellement convenues sont utilisés et représentés par les deux parties lors de la tentative d'établissement d'un tunnel ou d'une connexion VPN. [30]

- ***ISAKMP (Internet Security Association and Key Management Protocol):*** est un canal sécurisé sur lequel IKE négocie les numéros de clé des datagrammes IP. Contrairement aux SA IPsec, les SA ISAKMP sont bidirectionnelles. Il n'est donc pas nécessaire de disposer de plus d'une association de sécurité. [31]
- ***Echange de clés Diffie-Helman :*** Cette méthode est utilisée dans les échanges du protocole IKE pour générer une clef secrète partagée entre les deux extrémités de façon sécurisée. Avec cette méthode, un observateur ayant capturé les échanges IKE ne peut pas remonter à la clef secrète partagée. La clef secrète partagée est utilisée pour calculer une valeur qui sert ensuite aux calculs des clefs utilisées dans les phases 1 et 2 du protocole IKE. Des groupes auxquels ont été associé une longueur de clef et une fonction de chiffrement doivent être choisis pour mettre en œuvre. L'échange de clefs. Plus, la clef comprend un nombre de bits important, plus le secret est solide. En contrepartie, le temps de calcul est lui aussi plus important. Cette méthode est appelée à chaque établissement ou renouvellement d'association de sécurité Pour des raisons d'amélioration, il faut ajouter à ce mécanisme d'échange de clefs la technique PFS (Perfect Forward Secrecy). Avec cette technique, les calculs de clefs sont plus sûrs dans la mesure où les nouveaux calculs de renouvellement de SA (Security association) ne se font pas à partir des anciennes clefs. [32]

4.3.1.2 Les protocoles de transformation

- ***Les en-têtes d'authentification AH (Authentification header) :*** Le protocole AH est conçu pour assurer l'intégrité en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données (pas de confidentialité). Son principe est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. La protection contre le rejeu se fait grâce à un numéro de séquence. Il est à noter que l'utilisation du protocole AH interdit l'utilisation des mécanismes de translation d'adresses. En effet, le contenu de la trame n'étant pas chiffré, le protocole AH ajoute une signature numérique au paquet IP sortant : un mécanisme de translation d'adresses réécrivant l'adresse source fausse systématiquement le calcul de vérification de la signature numérique effectuée à l'autre bout du tunnel VPN. [33]

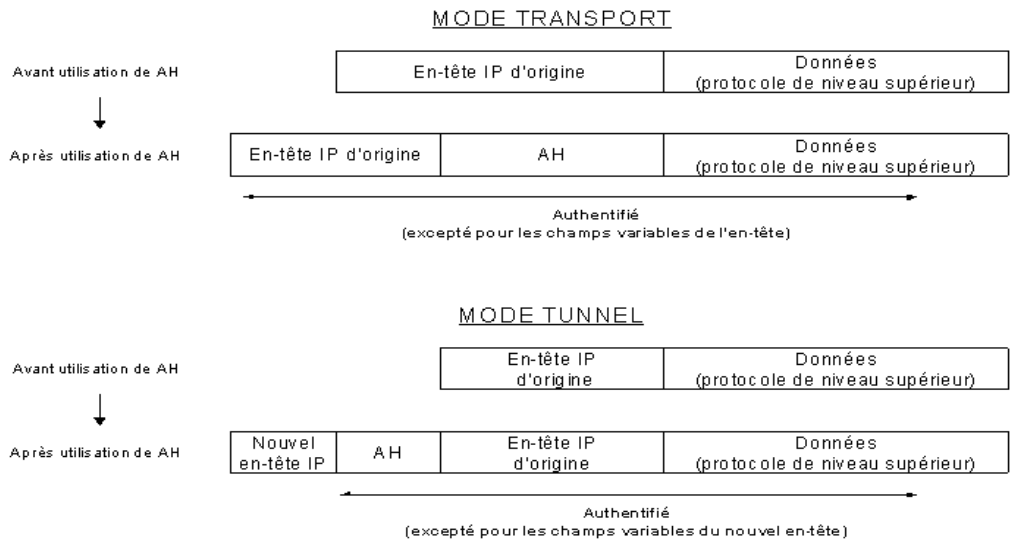

Figure 4.2: Encapsulation AH sur mode tunnel et transport [34]

- ***La technologie ESP (Encapsuling Security Payload) :*** ESP est un protocole de sécurité utilisé dans les réseaux informatiques. Il garantit la confidentialité des données en les chiffrant, ce qui protège contre l'analyse du trafic lorsque on utilise le mode tunnel. De plus, ESP vérifie l'intégrité des données en mode non connecté et permet l'authentification de l'origine des données, offrant ainsi une protection partielle contre les attaques de rejeu. Contrairement à AH, où l'on se contentait d'ajouter un en-tête supplémentaire au paquet IP, ESP fonctionne suivant le principe de l'encapsulation (les données originales sont chiffrées puis encapsulées). [33]

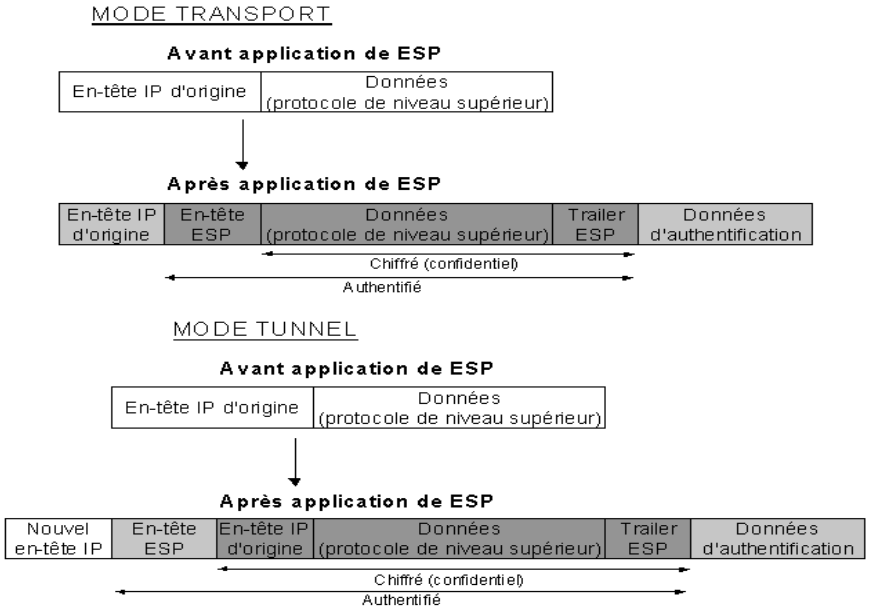

Figure 4.3: Encapsulation ESP sur mode tunnel et transport [34]

4.3.1.3 Modes d'IPsec

On distingue deux modes d'utilisation d'IPsec : le mode transport et le mode tunnel, la différence significative entre eux est la façon dont les datagrammes sont générés.

- ***Le mode Transport :*** Le mode transport IPsec protège uniquement la charge utile IP, c'est-à-dire le contenu des paquets IP, mais pas l'en-tête IP lui-même. Cela signifie que l'ordre des en-têtes IP et IPsec est le suivant : en-tête IP, en-tête IPsec (AH et ESP), charge utile IP (y compris l'en-tête de transport). Le mode transport est souvent utilisé pour la communication de bout en bout, comme entre un client et un serveur ou entre une station de travail et une passerelle, par exemple dans une session de bureau à distance. [35]

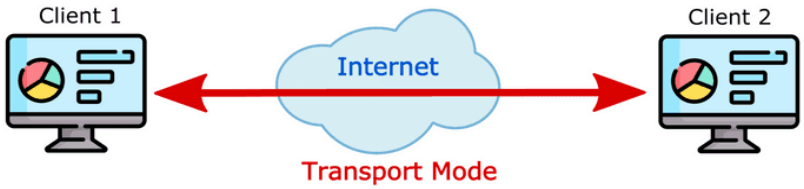

Figure 4.4: Mode Transport

- ***Le mode Tunnel :*** Le mode tunnel IPsec, quant à lui, protège l'ensemble du paquet IP, y compris l'en-tête IP. Cela signifie que le paquet IP original est encapsulé dans un nouveau paquet IP, avec un nouvel en-tête IP ajouté. L'ordre des en-têtes IP et IPsec est le suivant : nouvel en-tête IP, en-tête IPsec (AH et ESP), ancien en-tête IP, charge utile IP. Le mode tunnel est souvent utilisé entre des passerelles ou entre une station terminale et une passerelle, car il permet de protéger les données en encapsulant des paquets entiers qui sont décapsulés par une passerelle de sécurité. [35]

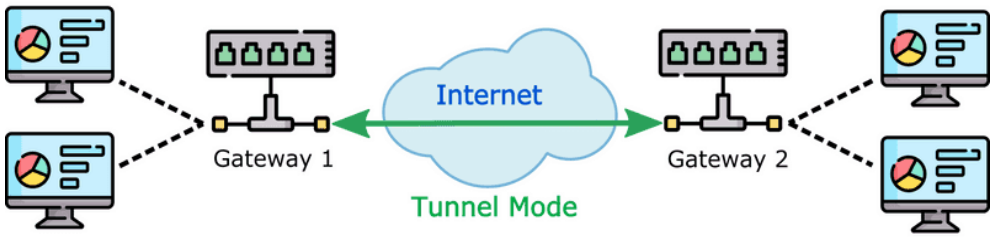

Figure 4.5: Mode Tunnel

4.3.2 Protocole NHRP (Next Hop Resolution Protocol) [36]

Le Next Hop Resolution Protocol (NHRP) est un protocole de résolution qui permet à un client next hop (NHC) de s'enregistrer dynamiquement au près des serveurs next hop (NHS). Avec la conception du DMVPN, le NHC est le routeur (spoke) et le NHS est le routeur (Hub). Une fois que tous les clients sont enregistrés, un spoke peut découvrir d'autres spokes au sein du même réseau NBMA (Non-Broadcast Multiple Access). Sans le protocole NHRP, les spokes doivent passer par le hub pour accéder à un autre spoke, cette limitation pourrait entraîner une certaine saturation au niveau du concentrateur (hub).

Dans la conception d'un réseau DMVPN, deux nouveaux termes s'imposent par rapport à la technologie NHRP :

- ***Le client NHC (Spoke) :*** c'est l'entité qui initie des demandes NHRP de divers types afin d'obtenir l'accès au service NHRP.
- ***Le serveur NHS (Hub) :*** C'est l'entité qui effectue le service de résolution du prochain bond au sein d'un réseau NBMA. Elle est aussi dite "serveur" car elle achemine le prochain bond aux clients (NHC).

4.3.2.1 Fonctionnement

Le rôle principal du protocole NHRP est de fournir le spoke par l'adresse IP de son spoke destinataire afin d'éviter le passage par le hub à chaque transmission de paquets. Pour cela il existe trois requêtes à exécuter:

- Tout d'abord, les clients (NHC) s'enregistrent auprès du serveur (NHS) et signalent leurs adresses publiques via la requête « NHRP Registration Request ». Le NHS garde une trace de toutes les adresses IP (adresse tunnel et adresse de l'interface physique) dans son cache.
- Lorsqu'un spoke veut écouler un trafic vers un autre spoke, il demandera au serveur (NHS) l'adresse IP publique de ce dernier via la requête « NHRP Resolution Request », qui est une requête de résolution du saut suivant.
- Le hub (NHS) vérifie son cache, trouve une entrée pour le spoke destinataire donc envoie l'adresse IP NBMA au spoke émetteur via la requête « NHRP Resolution Reply ». Maintenant le spoke peut envoyer des données à sa destination sans passer par le hub.

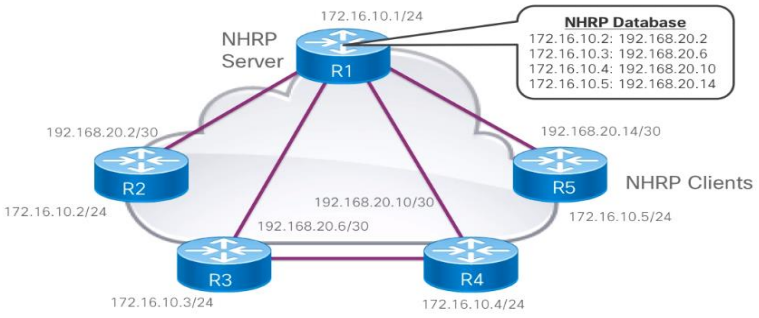

Figure 4.6: Protocole de résolution du prochain saut (NHRP) [37]

4.3.3 mGRE Tunnel (multipoint GRE)

Le MGRE permet de créer des tunnels multipoints, c'est-à-dire plusieurs tunnels à partir d'une seule pseudo-interface tunnel, il permet de supporter les multiples tunnels IPsec et contribue grandement à simplifier la configuration en diminuant la taille de cette dernière.

Dans un réseau DMVPN, le prochain type de configuration GRE utilise mGRE au niveau du site central (hub), et une configuration GRE normale point à point aux spokes. Les tunnels sont multipoints et sont configurées uniquement sur le routeur concentrateur.

Un seul mGRE peut ainsi s'occuper des nombreux tunnels GRE. Les tunnels mGRE n'ont pas de destinataire de tunnel défini, et ne peuvent seuls. NHRP comble cette lacune de mGRE car c'est lui qui a les destinations, où vont être dirigés les paquets. [38]

4.3.4 Protocoles de Routage

Le routage est une technique de réseau qui assure en permanence l'acheminement des données entre les différents sites d'un réseau. Dans le cas d'un DMVPN, le routage dynamique fait appel à plusieurs protocoles et algorithmes permettant aux routeurs de mettre en place des routes qui correspondent au mieux à l'état du réseau en temps réel.

4.3.4.1 Le protocole EIGRP

EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage développé par Cisco, il ne fonctionne que sur les produits Cisco. EIGRP utilise l'algorithme DUAL (Diffusing Update Algorithm) afin de gérer les chemins de routage. Cet algorithme offre la possibilité au routeur de stocker en mémoire toutes les tables de routage des voisins. Si un chemin tombe en panne, le routeur peut trouver rapidement un autre chemin.

Lorsque aucun chemin n'existe pour atteindre une destination donnée, le routeur EIGRP demande à ses voisins de lui fournir un chemin valide pour acheminer les paquets. Cette approche permet d'optimiser la recherche de chemins. Il a une distance administrative de 90.

Dans un réseau DMVPN (Dynamic Multipoint Virtual Private Network), il est nécessaire de désactiver la fonctionnalité de Split-Horizon. Normalement, cette règle empêche un routeur de publier un itinéraire via une interface qu'il utilise lui-même pour atteindre la destination. Cependant, avec DMVPN, cette restriction doit être levée pour permettre un routage efficace. [39]

4.3.4.2 Le protocole OSPF

OSPF (Open Shortest Path First) est un protocole de routage interne IP de type "à état de liens" développé par l'Internet Engineering Task Force (IETF). Il est conçu pour être un protocole de routage dynamique, ouvert et hautement fonctionnel, permettant de trouver la route la plus courte entre deux points du réseau. Il a une distance administrative de 110. OSPF fonctionnera sur la plupart des routeurs qui ne sont pas nécessairement des routeurs Cisco, contrairement au protocole EIGRP.

Les routeurs exécutant OSPF doivent établir des relations de voisinage (neighbor adjacency) avant d'échanger des routes. Comme OSPF est un protocole de routage d'état de liaison (Link State), les voisins n'échangent pas de tables de routage. Au lieu de cela, ils échangent des informations sur la topologie du réseau. Chaque routeur OSPF exécute ensuite l'algorithme SPF (Shortest Path First – Chemin le plus court) pour calculer les meilleures routes et les ajoute à la table de routage. Étant donné que chaque routeur connaît la topologie complète d'un réseau, la probabilité d'une boucle de routage est minime.

Chaque routeur OSPF stocke les informations de routage et de topologie dans trois tables :

- ***Table de voisins (Neighbor table) :*** stocke des informations sur les voisins OSPF.
- ***Table de topologie (Topology table) :*** stocke la structure de topologie d'un réseau.
- ***Table de routage (Routing table) :*** stocke les meilleurs itinéraires. [40]

4.4 Modèles de déploiement du DMVPN

Deux modèles de déploiement principaux permettent d'adapter l'architecture DMVPN aux besoins spécifiques de chaque organisation :

4.4.1 Modèle Hub-and-Spoke

Chaque spoke possède une interface GRE permettant de monter le tunnel vers le hub. Tout trafic entre les spokes passe par le hub. Ce modèle ne prend pas en compte les liaisons entre les spokes. [41]

4.4.2 Modèle Spoke-to-Spoke

Chaque spoke doit disposer d'une interface mGRE permettant aux tunnels dynamiques de transiter vers les autres spokes. Ce modèle prend en compte les liaisons entre différents spokes et offre une grande évolutivité de la configuration pour les périphériques. [41]

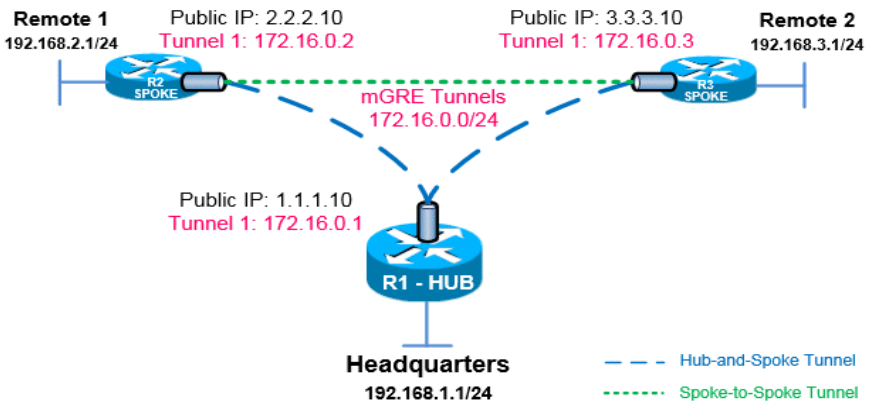

Figure 4.7: Modèles de déploiement du DMVPN [42]

4.5 Les phases du DMVPN

Le guide de conception DMVPN de Cisco présente trois phases distinctes. Chaque phase s'appuyant sur la précédente avec des fonctions supplémentaires.

4.5.1 Phase 1

La phase 1 de DMVPN consiste en des tunnels mGRE sur le hub et des tunnels point-to-point GRE sur les spokes. Le hub peut atteindre tous les spokes par l'intermédiaire de l'interface de tunnel, mais les spokes ne peuvent atteindre que le hub. Aucun trafic direct entre les spokes n'est autorisé. Les routes multicast sont échangées entre le hub et les sites distants, mais pas entre les spokes eux-mêmes. Cette configuration permet une gestion centralisée de la sécurité et du routage, mais limite le trafic direct entre les spokes. [43]

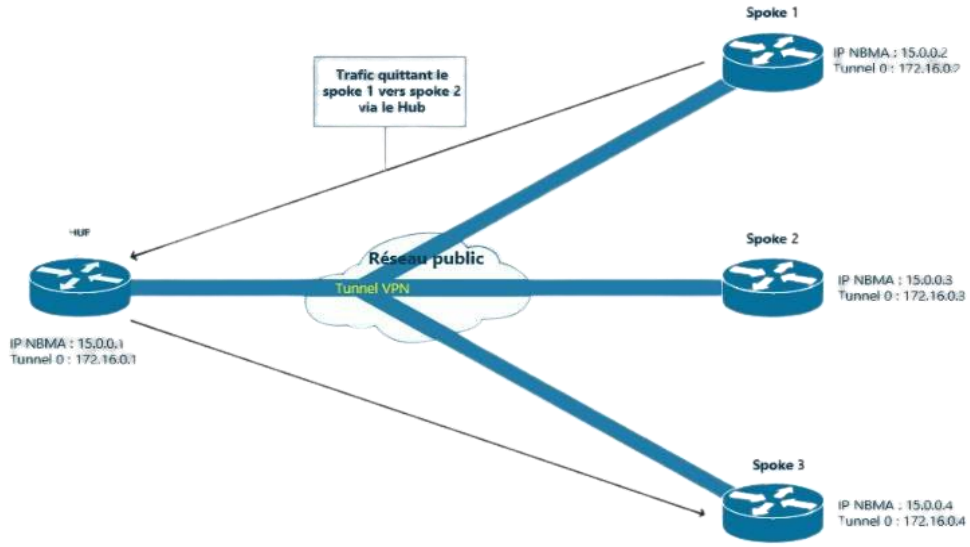

Figure 4.8: DMVPN Phase 1 scenario

4.5.2 Phase 2

La phase 2 de DMVPN permet l'établissement de tunnels mGRE sur les hubs et les sites distants, autorisant ainsi le trafic direct entre les sites distants. Les sites distants envoient des requêtes NHRP au hub pour obtenir l'adresse IP des autres sites distants.

Quand un spoke (NHC) a besoin d'envoyer un paquet via un next hop sur le cloud mGRE, il envoie un paquet NHRP Resolution Request au Hub (NHS). Le Hub lui répond par 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 pour les prochaines transmissions. Cette phase est plus scalable que la phase 1. [43]

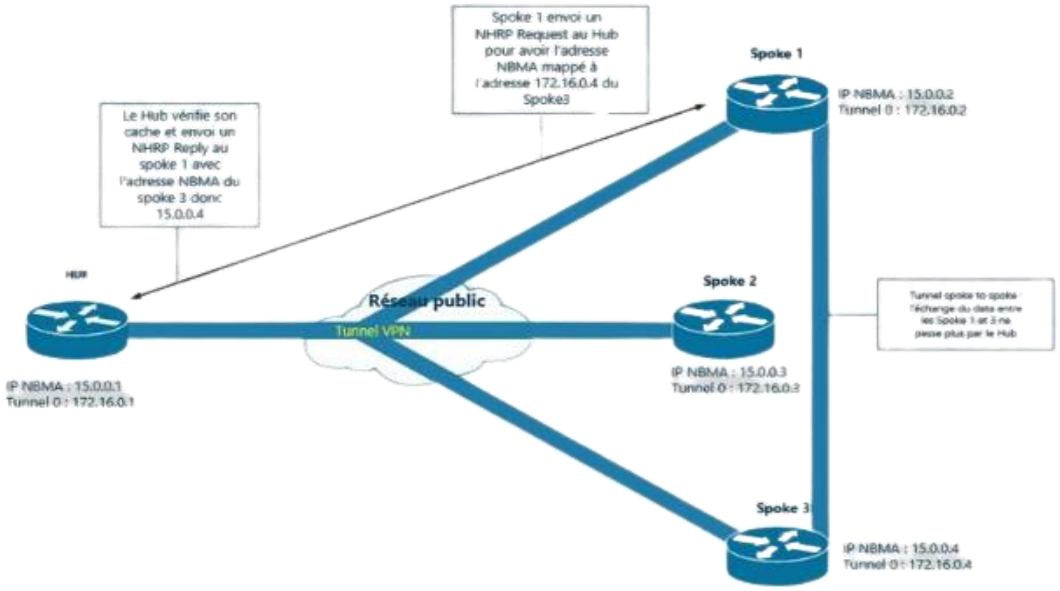

Figure 4.9: DMVPN Phase 2 scenario

4.5.3 Phase 3

La phase 3 de DMVPN améliore l'évolutivité de la phase 2 en permettant l'utilisation de n'importe quel protocole de routage et en utilisant les mécanismes de "NHRP redirects" et "shortcuts" pour gérer les flux de trafic.

Cette phase permet la communication spoke to spoke même avec le routage par défaut. Ainsi même si la table de routage pointe vers le hub, le trafic circule entre les spokes. Aucune limite sur le routage, nous obtenons toujours un flux de trafic spoke to spoke même lorsqu'on utilise des itinéraires par défauts.

Voici comment fonctionne la phase 3 de DMVPN :

1. Les spokes enregistrent leurs mapping (tunnel et NBMA) avec le Hub. Cela permet au Hub de découvrir dynamiquement les spokes et d'établir les relations de voisinages.
2. Les informations de routage sont échangées entre le hub et les spokes. Le hub peut summarizer les routes avant de les envoyer aux spokes, ce qui améliore l'évolutivité.
3. Quand un spoke reçoit un paquet destiné à un autre spoke, il envoie une requête NHRP au hub. Le hub répond avec un message NHRP Redirect contenant l'adresse NBMA du spoke destination.
4. Le spoke initial met à jour sa table de routage et envoie le paquet directement au spoke destination via un tunnel IPsec.
5. Les paquets suivants sont envoyés directement entre les spokes sans passer par le hub. [43]

La figure 4.10 représente les étapes du fonctionnement de la phase 3.

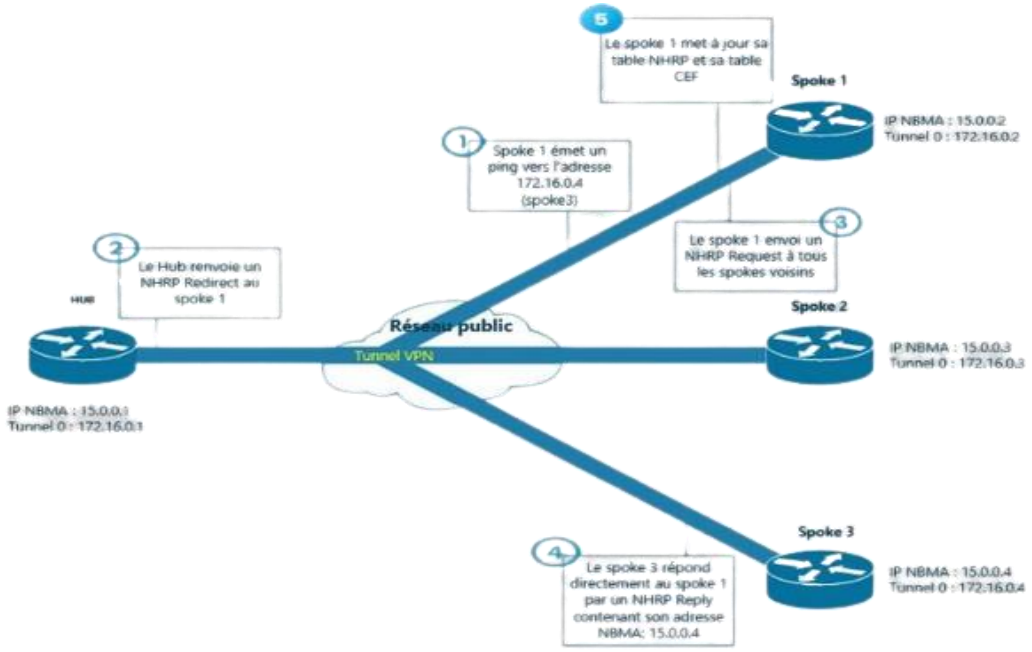

Figure 4.10: DMVPN Phase 3 scenario

4.6 Conclusion

Dans ce chapitre, nous commençons par explorer l'historique De la technologie DMVPN, son principe et son fonctionnement. Ensuite, nous avons présenté les différents modèles de déploiement ainsi que les différentes phases de cette technologie. Il est évident que DMVPN n'est pas simplement une autre technologie VPN mais une révolution dans la conception de l'architecture de ce dernier. La flexibilité, la stabilité et la qualité de service qu'il offre sont très efficaces contrairement au tunnel VPN traditionnel. On va illustrer la mise en œuvre pratique des concepts vus dans ce chapitre dans le chapitre qui suit.

Chapitre 5 : Implémentation et configuration de DMVPN

5.1 Introduction

Après avoir fait l'étude conceptuelle des VPN et la technologie DMVPN, nous consacrons ce chapitre à la phase de réalisation de notre projet.

Nous présentons en premier lieu l'organisme d'accueil ainsi que ses missions et objectifs. Ensuite, nous allons présenter une démonstration pratique de la mise en œuvre de la technologie DMVPN en utilisant l'émulateur EVE-NG, nous avons créé une topologie du réseau approprié pour faciliter la compréhension de l'implémentation de cette technologie.

5.2 Présentation de l'organisme d'accueil

5.2.1 Présentation du groupe ALGERIE TELECOM

Algérie Télécom est leader sur le marché algérien des télécommunications qui connait une forte croissance, offrant une gamme complète de services de téléphonie fixe et d'internet aux clients résidentiels et professionnels. Cette position s'est construite par une politique d'innovation forte adaptée aux attentes des clients et orientée vers les nouveaux usages.

Algérie Télécom est l'opérateur national des télécommunications en Algérie. Créé en 2003 suite à la restructuration de l'ancien Ministère des Postes et Télécommunications, son ambition est d'avoir un niveau élevé de performance technique, économique, et sociale pour se maintenir durablement leader dans son domaine, dans un environnement devenu concurrentiel. Son souci consiste, aussi, à préserver et développer sa dimension internationale et participer à la promotion de la société de l'information en Algérie.

5.2.2 Missions et objectifs

L'activité majeure d'Algérie Télécom est de :

- Fournir des services de télécommunication permettant le transport et l'échange de la voix, de messages écrits, de données numériques, d'informations audiovisuelles…
- Développer, exploiter et gérer les réseaux publics et privés de télécommunications.
- Etablir, exploiter et gérer les interconnexions avec tous les opérateurs des réseaux.

ALGERIE TELECOM est engagée dans le monde des technologies de l'information et de la communication avec les objectifs suivants :

- Accroître l'offre de services téléphoniques et faciliter l'accès aux services de télécommunications au plus grand nombre d'usagers, en particulier en zones rurales.
- Accroître la qualité de services offerts et la gamme de prestations rendues et rendre plus compétitifs les services de télécommunications.
- Développer un réseau national de télécommunication fiable et connecté aux autoroutes de l'information.

5.2.3 Organisation d'Algérie Télécom

ALGERIE TELECOM est organisée en Divisions, Directions Centrales, et Régionales, à cette structure s'ajoutent trois filiales :

- Algérie Télécom Mobile (ATM).
- Algérie Télécom Internet (ATI).
- Algérie Télécom Satellite (ATS).

5.2.4 Description de la direction opérationnelle

La direction opérationnelle est une entité opérationnelle dotée de l'autonomie budgétaire et financière. Elle est structurée en cinq départements et dotée de cinq cellules rattachées directement au directeur opérationnel des Télécoms.

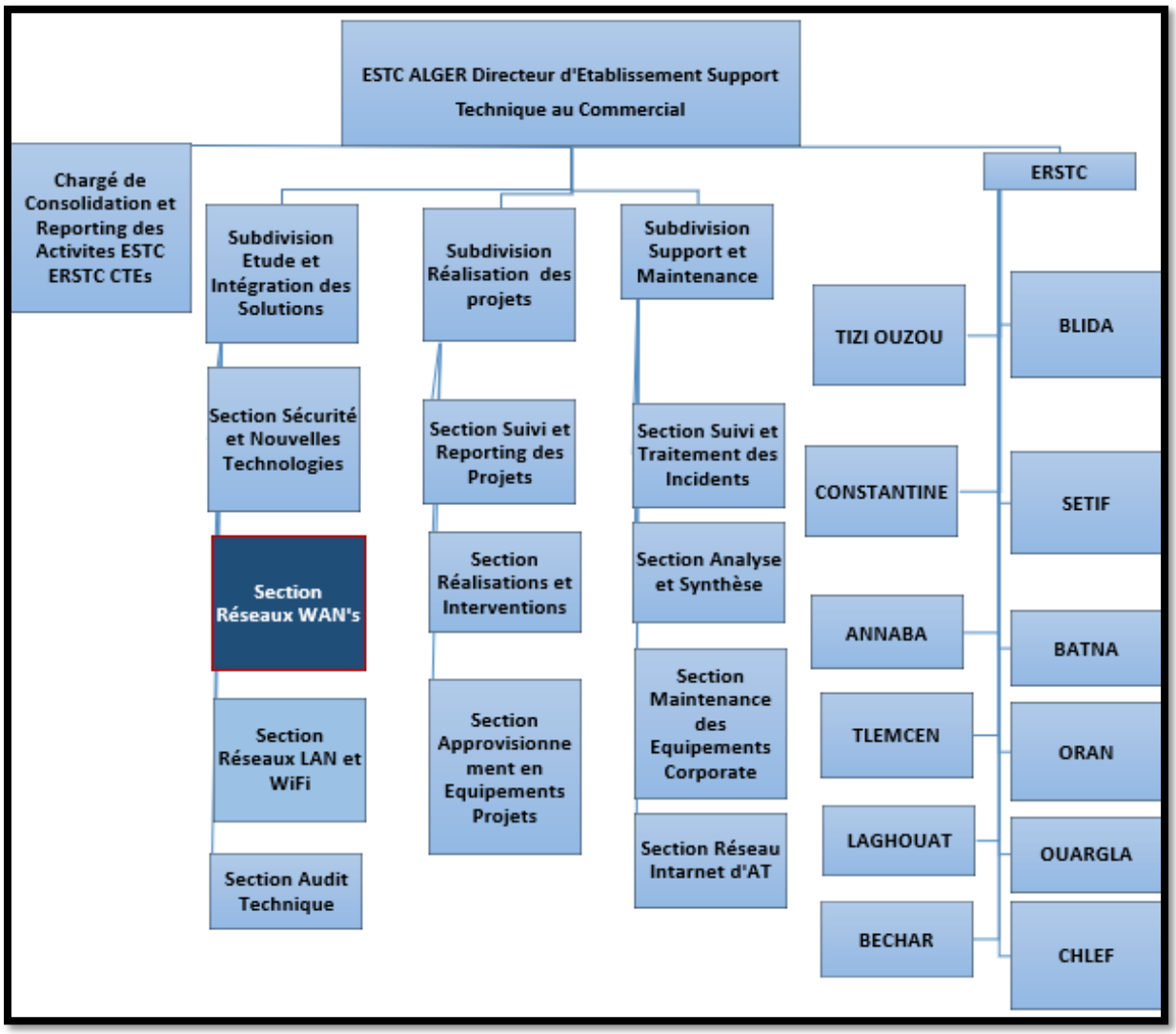

Figure 5.1: Organigramme de la direction opérationnelle de Télécommunications d'Alger Centre (Algérie Telecom)

5.3 Présentation des outils utilisées

5.3.1 VMware Workstation Pro

Est un logiciel de virtualisation très puissant qui permet d'exécuter plusieurs systèmes d'exploitation en tant que machines virtuelles sur une seule machine physique.

VMware Workstation est un outil puissant qui offre de nombreuses fonctionnalités avancées comme la création et la gestion de machines virtuelles, La virtualisation de réseaux le développement et le test de logiciels, la formation et l'éducation, les environnements de bureau virtuels…

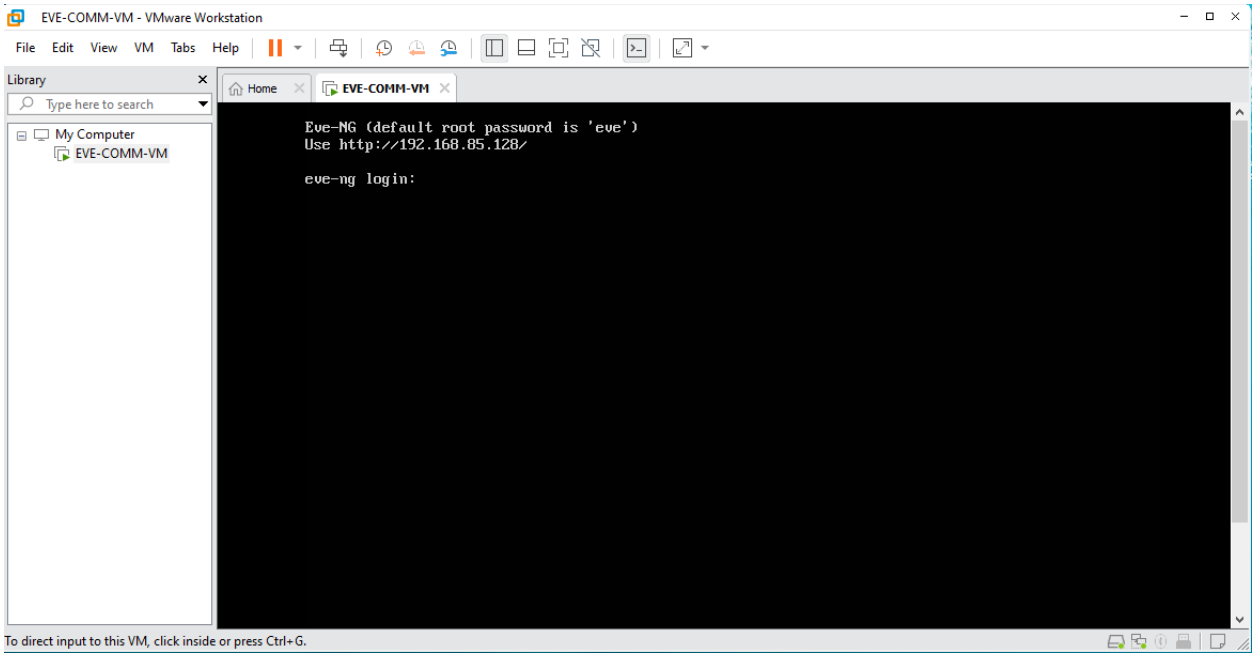

Figure 5.2: VMware Workstation interface

5.3.2 EVE-NG

EVE-NG (Emulated Virtual Environment Next Generation) est un logiciel de simulation de réseau puissant qui permet aux professionnels des réseaux et de la sécurité de créer et de gérer des laboratoires virtuels réalistes. Il s'agit d'une plateforme multiplateforme basée sur le Web qui offre un large éventail de fonctionnalités pour la conception, le test et le dépannage de réseaux complexes. EVE-NG est un outil précieux pour les professionnels des réseaux et de la sécurité qui ont besoin de créer et de gérer des laboratoires virtuels réalistes, sa capacité à simuler des environnements réalistes et à offrir une expérience utilisateur conviviale en fait un choix privilégié pour une large gamme de cas d'utilisation.

Figure 5.3: EVE-NG Logo

5.3.3 PuTTY

PuTTY est un émulateur de terminal gratuit et open source, une application de transfert de fichiers réseau et une console série pour les plates-formes Windows. Il vous permet de vous connecter à des ordinateurs ou des appareils distants à l'aide de divers protocoles tels que Secure Socket Shell (SSH), Telnet, connexion, etc. PuTTY est largement utilisé par les administrateurs système, les ingénieurs réseau et les développeurs pour gérer et contrôler les systèmes distants.

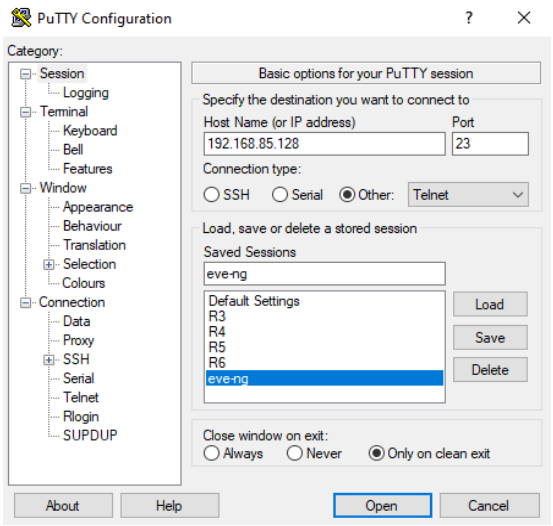

Figure 5.4: PuTTY interface

5.3.4 Cisco IOS images

Cisco IOS (Internetwork Operating System) est un logiciel d'exploitation développé par Cisco Systems pour ses équipements réseau, notamment les routeurs et les commutateurs. Les images IOS sont les fichiers binaires contenant le système d'exploitation qui peuvent être installés sur ces appareils pour leur permettre de fonctionner et de fournir divers services réseau.

5.3.5 Wireshark

Wireshark est un logiciel libre et open-source d'analyse de protocole réseau, ou analyseur de paquets. Il permet de capturer et d'examiner les données en transit sur un réseau informatique en temps réel, ce qui le rend précieux pour le dépannage réseau, l'analyse, le développement de logiciels et l'éducation. Wireshark est fréquemment utilisé par les administrateurs réseau, les ingénieurs de sécurité et les développeurs pour diagnostiquer et résoudre les problèmes réseau.

Figure 5.5: Wireshark Logo

5.4 Topologie du réseau

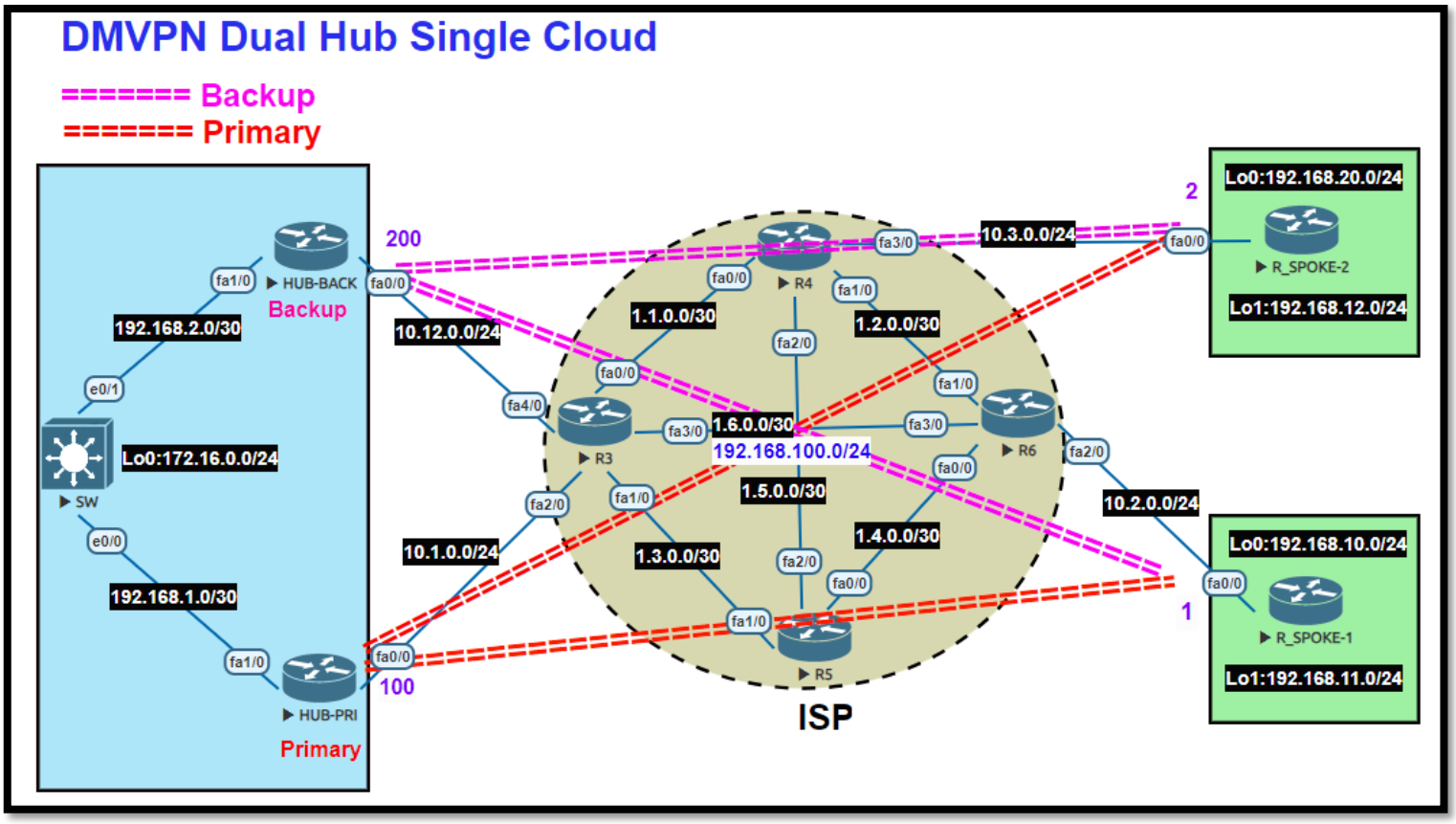

Figure 5.6: Topologie DMVPN dual Hub single Cloud sur EVE-NG

5.4.1 Les équipements utilisés

DMVPN est une solution propre à Cisco donc elle est déployée seulement sur les routeurs Cisco de série 7000 Dynamips (7206VXR).

Cette topologie réseau se compose de huit routeurs. Deux d'entre eux, nommés (Hub1 et Hub2), servent de routeurs centraux. Deux autres routeurs représentent les sites distants (spoke1 et spoke2). Quatre routeurs supplémentaires, désignés par ISP, représentent le Cloud. Enfin, un commutateur de niveau 3 (Layer 3 Switch) relie les deux routeurs centraux Hub1 et Hub2.

5.4.2 Explication de la topologie

La topologie DMVPN Dual Hub Single Cloud comprend deux hubs et un seul cloud, offrant redondance et résilience. Hub1 est le hub principal, tandis que Hub2 sert de secours. Deux routeurs spokes (Spoke1 et Spoke2) se connectent aux hubs via des tunnels GRE, permettant la communication directe entre eux grâce au NHRP. Un Switch de niveau 3 connecte Hub1 et Hub2, assurant la redondance interne. Cette configuration utilise un routage dynamique pour gérer les routes et peut être sécurisée avec IPsec pour garantir la confidentialité des données. L'avantage de cette configuration est qu'elle garantit la redondance. La configuration de Hub2 est similaire à Hub1. Sur les spokes, il suffit d'ajouter le deuxième routeur comme hub.

5.5 Configuration

5.5.1 Plan d'addressage :

Router	Interface	IP Address	Masque
HUB-PRI	Fa0/0 Fa1/0 Tunnel0	10.1.0.2 192.168.1.1 192.168.100.100	255.255.255.0 255.255.255.252 255.255.255.0
HUB-BACK	Fa0/0 Fa1/0 Tunnel0	10.12.0.2 192.168.2.1 192.168.100.200	255.255.255.0 255.255.255.252 255.255.255.0
Spoke 1	Fa0/0 Loopback0 Loopback1 Tunnel0	10.2.0.1 192.168.10.10 192.168.11.10 192.168.100.1	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0
Spoke 2	Fa0/0 Loopback0 Loopback1 Tunnel0	10.3.0.2 192.168.20.10 192.168.12.10 192.168.100.2	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0
ISP-R3	Fa0/0 Fa1/0 Fa2/0 Fa3/0 Fa4/0	1.1.0.1 1.3.0.1 10.1.0.1 1.6.0.1 10.12.0.1	255.255.255.252 255.255.255.252 255.255.255.0 255.255.255.252 255.255.255.0

ISP-R4	Fa0/0 Fa1/0 Fa2/0 Fa3/0	1.1.0.2 1.2.0.1 1.6.0.2 10.3.0.1	255.255.255.252 255.255.255.252 255.255.255.252 255.255.255.0
ISP-R5	Fa0/0 Fa1/0 Fa2/0	1.4.0.1 1.3.0.2 1.5.0.2	255.255.255.252 255.255.255.252 255.255.255.252
ISP-R6	Fa0/0 Fa1/0 Fa2/0 Fa3/0	1.4.0.2 1.2.0.2 10.2.0.2 1.6.0.2	255.255.255.252 255.255.255.252 255.255.255.0 255.255.255.252
Switch	e0/0 e0/1 Loopback0	192.168.1.2 192.168.2.2 172.16.0.10	255.255.255.252 255.255.255.252 255.255.255.0

Tableau 5.1: Plan d'addressage des routers

5.5.2 Configuration des interfaces

- **HUB-PRI**

```
R_HUB-PRI#sh ip int b
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            10.1.0.2        YES NVRAM  up                    up

FastEthernet1/0            192.168.1.1     YES NVRAM  up                    up

Tunnel0                    192.168.100.100 YES NVRAM  up                    up

R_HUB-PRI#
```

Figure 5.7: HUB-PRI interfaces configuration

- **HUB-BACK**

```
R_HUB-BACK#sh ip int b
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            10.12.0.2       YES NVRAM  up                    up

FastEthernet1/0            192.168.2.1     YES NVRAM  up                    up

Tunnel0                    192.168.100.200 YES NVRAM  up                    up

R_HUB-BACK#
```

Figure 5.8: HUB-BACK interfaces configuration

- **R_SPOKE-1**

```
R_SPOOKE-1#sh ip int b
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            10.2.0.1        YES NVRAM  up                    up

Loopback0                  192.168.10.10   YES NVRAM  up                    up

Loopback1                  192.168.11.10   YES NVRAM  up                    up

Tunnel0                    192.168.100.1   YES NVRAM  up                    up

R_SPOOKE-1#
```

Figure 5.9: Spoke1 interfaces configuration

- **R_SPOKE-2**

```
R_SPOOKE-2#sh ip int b
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            10.3.0.2        YES NVRAM  up                    up

Loopback0                  192.168.20.10   YES NVRAM  up                    up

Loopback1                  192.168.12.10   YES NVRAM  up                    up

Tunnel0                    192.168.100.2   YES NVRAM  up                    up

R_SPOOKE-2#
```

Figure 5.10: Spoke2 interfaces configuration

- **ISP-R3**

```
ISP-R3#sh ip int b
Interface                  IP-Address      OK? Method Status                Prot
ocol
FastEthernet0/0            1.1.0.1         YES NVRAM  up                    up

FastEthernet1/0            1.3.0.1         YES NVRAM  up                    up

FastEthernet2/0            10.1.0.1        YES NVRAM  up                    up

FastEthernet3/0            1.6.0.1         YES NVRAM  up                    up

FastEthernet4/0            10.12.0.1       YES NVRAM  up                    up

ISP-R3#
```

Figure 5.11: ISP-R3 interfaces configuration

➢ De la même manière les autres routers ISP sont configurés à l'aide de plan d'addressage. Voir (Tableau 5.1).

- **Layer 3 Switch**

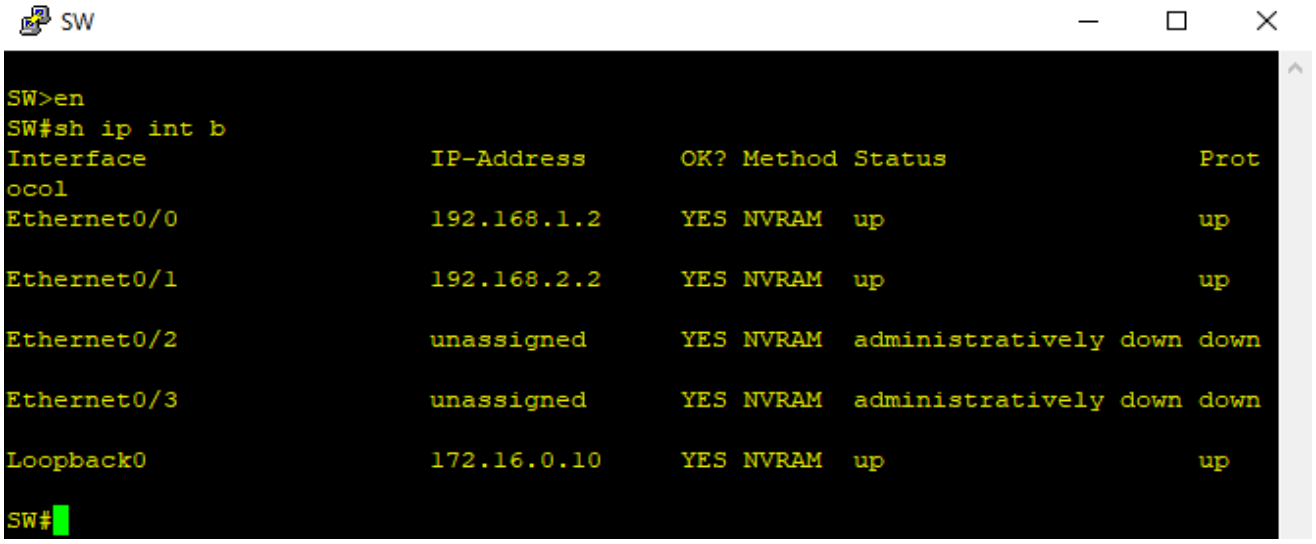

Figure 5.12: Switch interfaces configuration

5.5.3 Routage OSPF

- **Configuration OSPF**

Maintenant, nous allons nous concentrer sur la configuration du routage OSPF pour notre réseau. Cela implique la définition des zones de routage, l'établissement des adjacences entre les routeurs, et l'optimisation des chemins pour une communication efficace.

La table représentée dans la Figure 5.13 illustre les différentes routes sélectionnées par le protocole OSPF pour acheminer des paquets IP. Cette table précise l'adresse IP de destination et le masque, ainsi que l'interface via laquelle les paquets sont acheminés. En analysant cette table, nous constatons que tous les réseaux distants sont atteignables, ce qui démontre l'efficacité du routage OSPF dans la gestion des chemins et la connectivité du réseau.

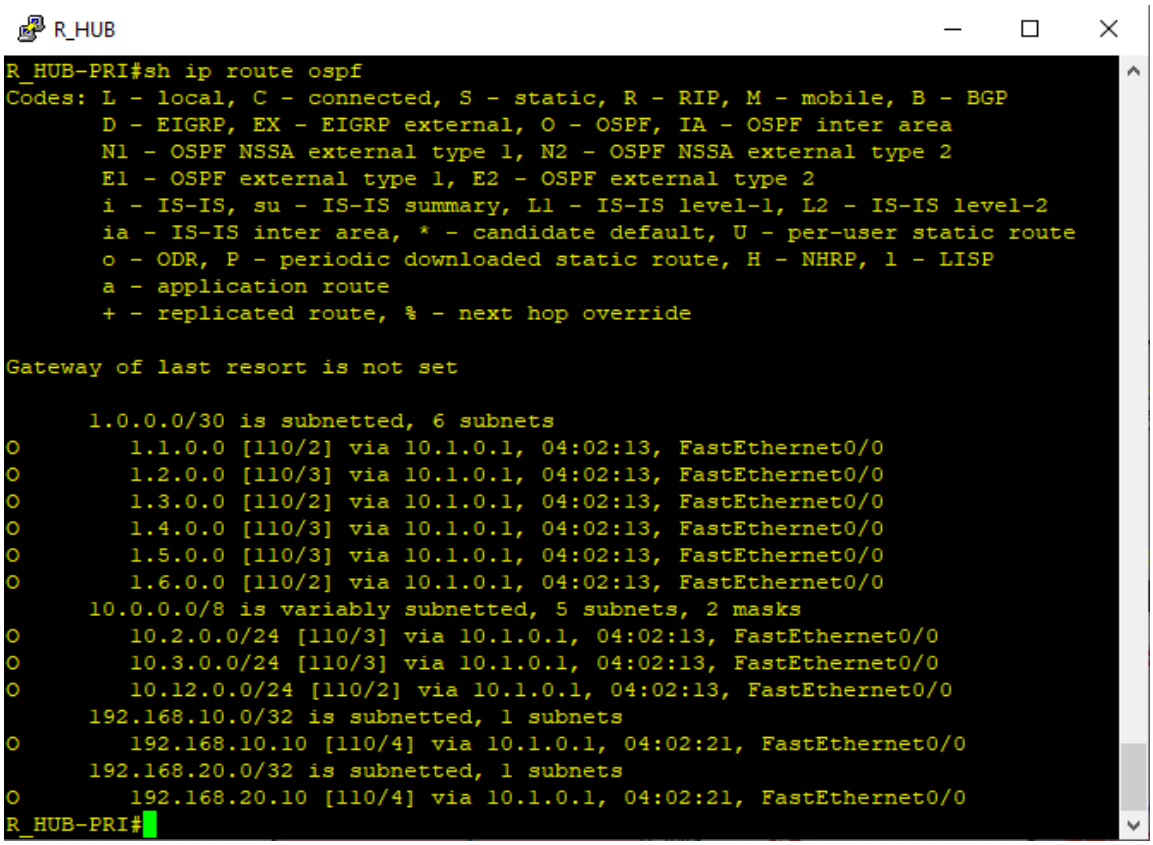

Figure 5.13: Table de routage OSPF du HUB-PRI

- **Test de connectivité**

Nous effectuons un test de connectivité entre le hub et les spokes.

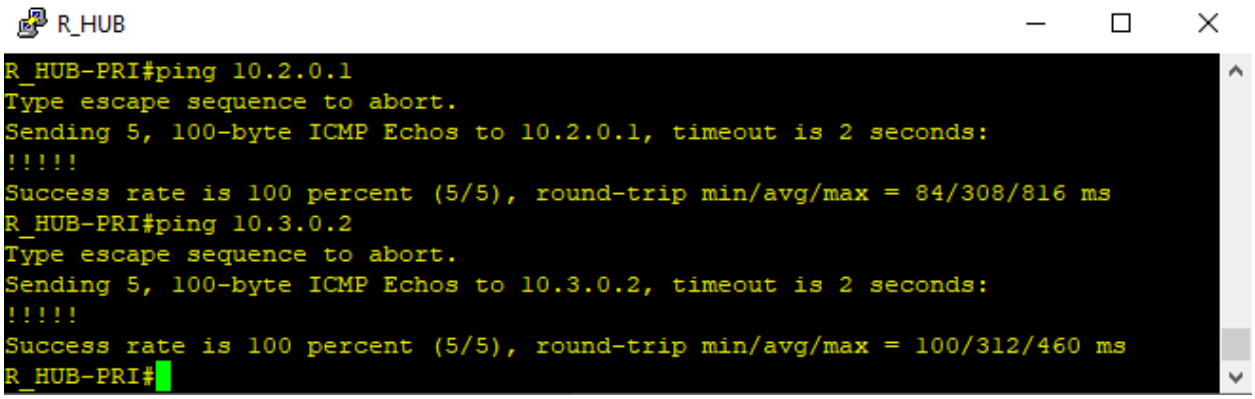

Figure 5.14: Test de connectivité (OSPF)

Dans la figure ci-dessus (Figure 5.14), il est clair que le ping entre le hub et les NBMA des spokes est réalisé sans aucun problème, ce qui démontre l'efficacité du routage OSPF dans l'établissement de la connectivité.

5.5.4 Implémentation des tunnels mGRE avec intégration de NHRP

- **Les commandes utilisés**

Interface tunnel0 : Créer une interface de tunnel.

Ip address : Définit une adresse IP pour l'interface du tunnel, ip address 192.168.100.100 255.255.255.0 (HUB-PRI), ip address 192.168.100.1 255.255.255.0 (R_SPOKE-1).

Ip NHRP map multicast dynamic : Permet à NHRP d'ajouter automatiquement des routeurs en étoile aux mappages NHRP multidiffusion.

Ip NHRP network-id 1 : Lors de l'utilisation de plusieurs réseaux DMVPN, il est nécessaire d'utiliser des ID de réseau pour différencier ces réseaux. Bien que cette valeur ne soit significative que localement sur chaque routeur, il est recommandé, pour des raisons de dépannage, d'utiliser la même valeur sur tous les routeurs. Cela simplifie l'administration et la gestion du réseau, facilitant ainsi l'identification et la résolution des problèmes éventuels (on a choisi 1 comme valeur d'ID).

Tunnel source FastEthernet 0/0 : cette commande définit la source de l'interface Tunnel.

Tunnel mode gre multipoint : Définit le mode d'encapsulation sur GRE pour l'interface du tunnel, la destination de tunnel est configurée à mGRE (multipoint) pour nous permettre de réaliser la phase 1 et ça nous permet aussi de passer à la phase 2.

Ip NHRP nhs 192.168.100.100: cette commande configure le HUB-PRI en tant que serveur de saut suivant NHRP.

Ip tcp adjust-mss 1360 : cette commande permet d'ajuste la valeur MSS des paquets TCP passant par un router. L'argument Max-Segment-Size spécifie la taille maxiumale du segment, en octets. La gamme va de 500 à 1460. La valeur numérique recommandé est de 1360 lorsque le nombre d'octets MTU IP est défini sur 1400. Avec ces paramètres recommandés, les sessions TCP redescendent rapidement à des paquets IP de 1400 octets afin que les paquets tiennent dans le tunnel.

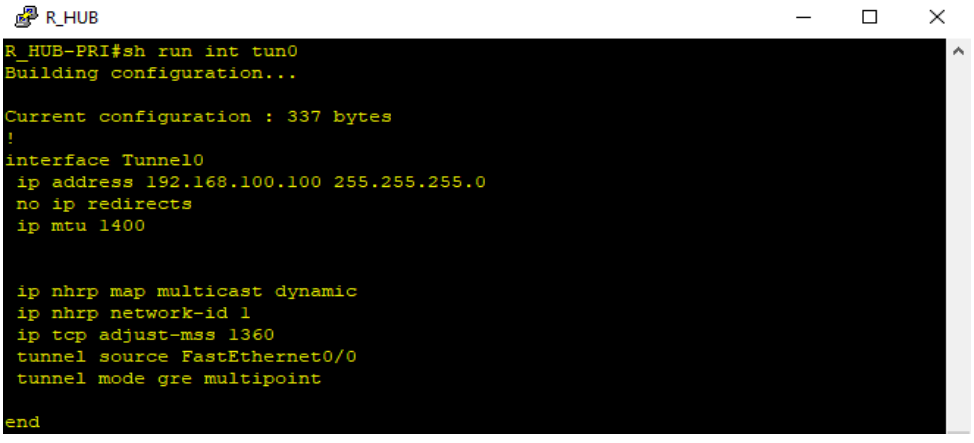

Figure 5.15: Établissement du Tunnel GRE pour le HUB-PRI

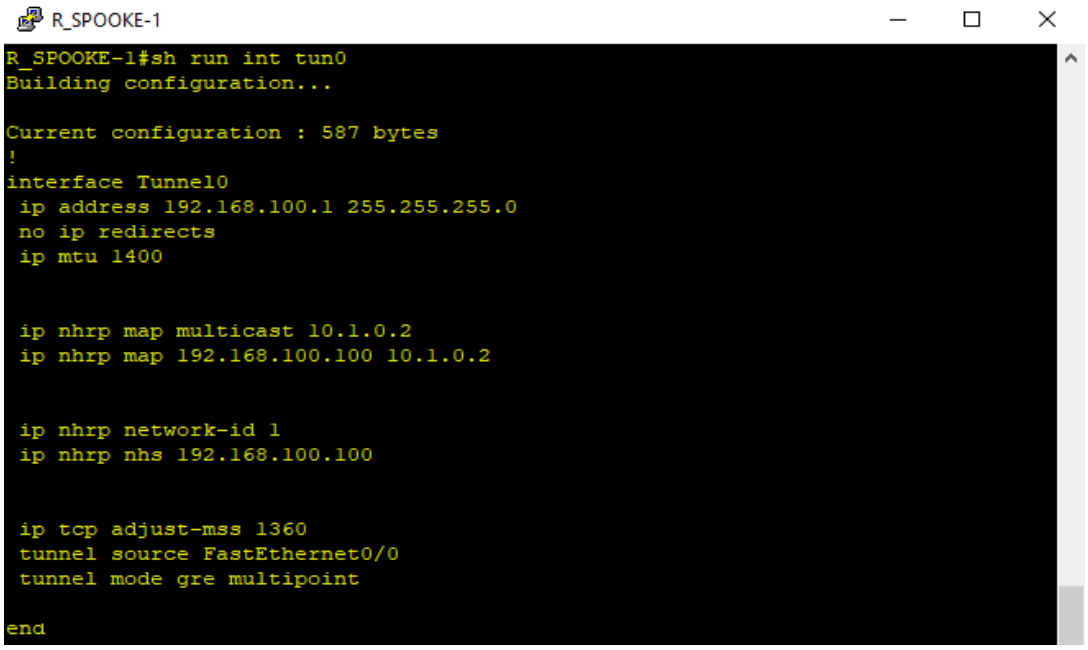

Figure 5.16: Établissement du Tunnel GRE pour le Spoke 1

5.5.5 Routage EIGRP

Avant de pouvoir tester notre solution, il nous manque encore un élément essentiel : le protocole de routage dynamique. Pour cette configuration, nous avons choisi d'utiliser le protocole EIGRP (Enhanced Interior Gateway Routing Protocol).

- **Les commandes utilisées**

Router eigrp 10 : Activer le protocole de routage EIGRP, et définir le numéro AS (on a choisi 1).

Network (Adresse tunnel) : Activer EIGRP dans l'interface tunnel.

Figure 5.17: La configuration EIGRP sur le HUB-PRI

Figure 5.18: La configuration EIGRP sur le Spoke 1

- **Test de connectivité**

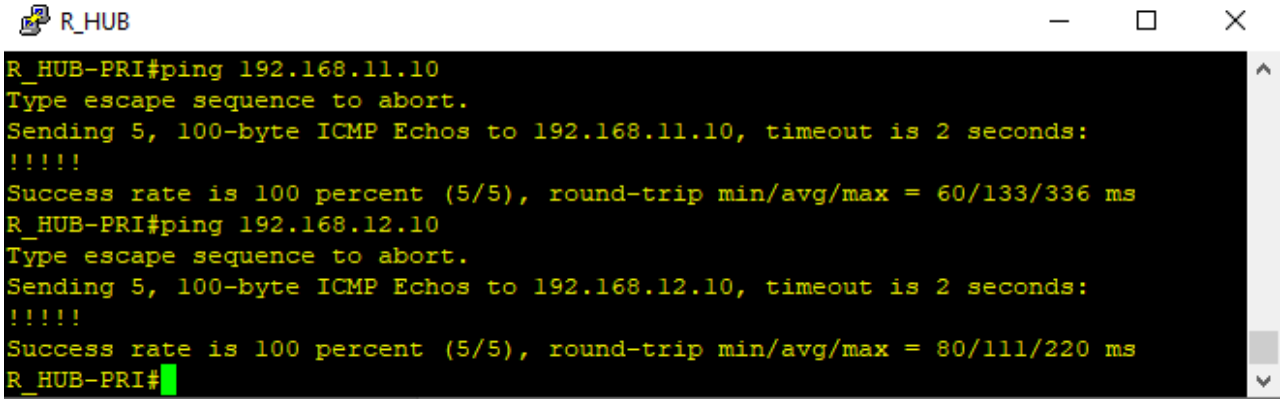

Figure 5.19: Test de connectivité (EIGRP)

La figure (Figure 5.19) montre que la connectivité entre les spokes et le hub est fonctionelle, avec des tests de ping réussis sans aucun problème. Cela indique que les tunnels GRE multipoint sont correctement configurés et que le routage dynamique via EIGRP fonctionne comme prévu.

5.5.6 Vérification de la fonctionnalité DMVPN

Après avoir terminé la configuration, la vérification de bon fonctionnement est obligatoire. Pour cette étape on va utiliser la commande **show dmvpn**.

- **Vérification sue le HUB-PRI**

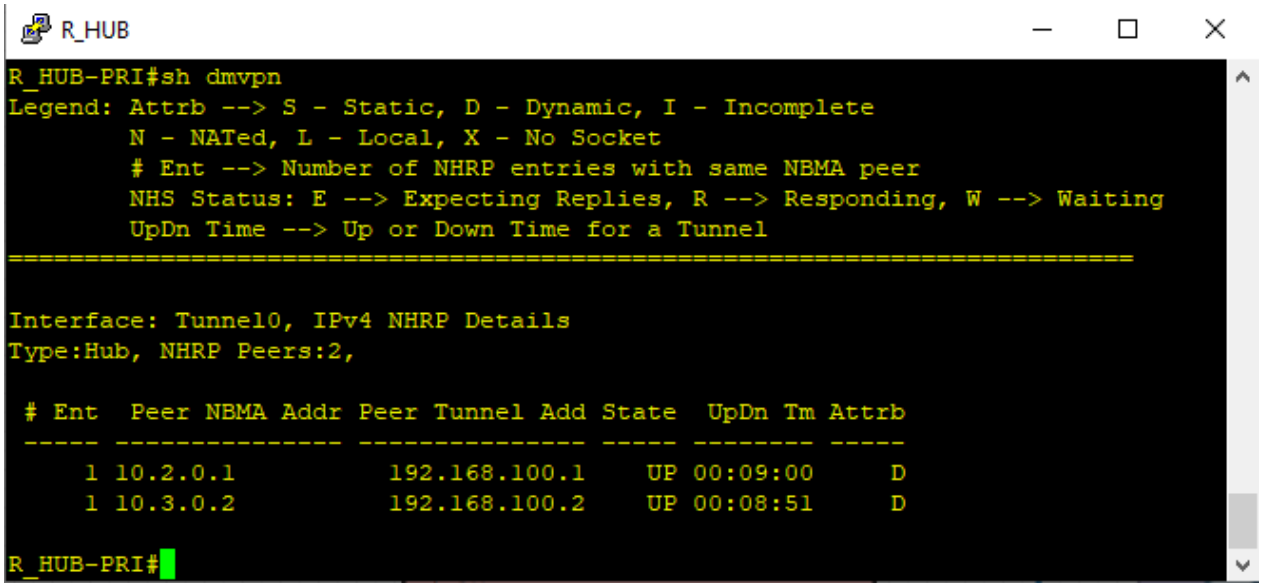

Figure 5.20: Output de la commande show dmvpn sur le HUB-PRI

La sortie de notre commande nous fournit les informations suivantes :

- Dans la première colonne, **#Ent** indique le nombre d'entrées dans la base de données NHRP pour le même spoke. Généralement, il n'y en a qu'une seule par spoke.
- La deuxième colonne **Peer NBMA Addr** affiche l'adresse IP publique du spoke. Tandis que la troisième colonne, **Peer Tunnel Add**, affiche l'adresse IP du tunnel local de chaque spoke.
- La colonne **State** indique l'état actuel du tunnel, qui est "UP" dans notre cas. Juste à côté de l'état se trouve **UpDN Tm**, qui affiche le temps écoulé depuis que le tunnel est dans son état actuel (UP).
- Enfin, la colonne **Attrib** montre le type de tunnels établis par les spokes. D signifie dynamique, S pour statique et I pour incomplet. Habituellement, les spokes dynamiques créeront des tunnels de type D. Les tunnels établis entre les rayons et le router concentrateur devraient être de type S, car le concentrateur reste statique.

- **Vérification sur le Spoke 1**

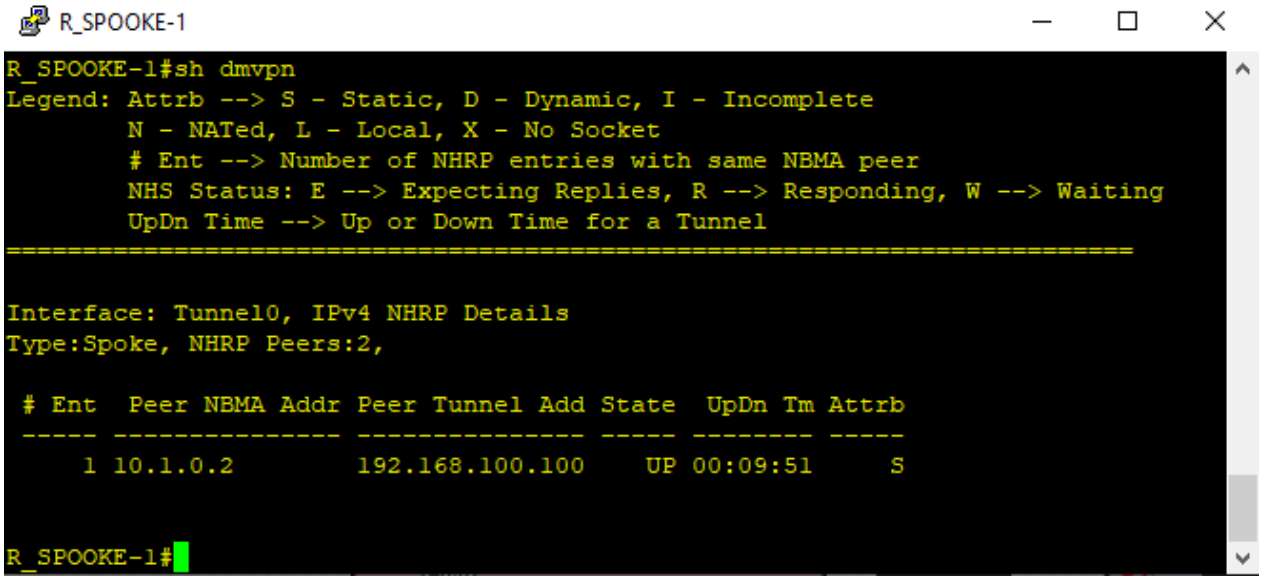

Figure 5.21: Output de la commande show dmvpn sur le Spoke 1

Comme nous l'avons mentionné précédemment, le Spoke1 établit un tunnel statique (S) avec le HUB.

PS : Bien que le DMVPN Phase 1 permette l'établissement de connexions entre les spokes et le hub, il présente l'inconvénient de ne pas permettre les connexions directes entre spokes (Spoke-to-Spoke) comme illusté dans la Figure 5.22. La Phase 2 du DMVPN apporte une solution à ce problème en autorisant la communication directe entre les spokes.

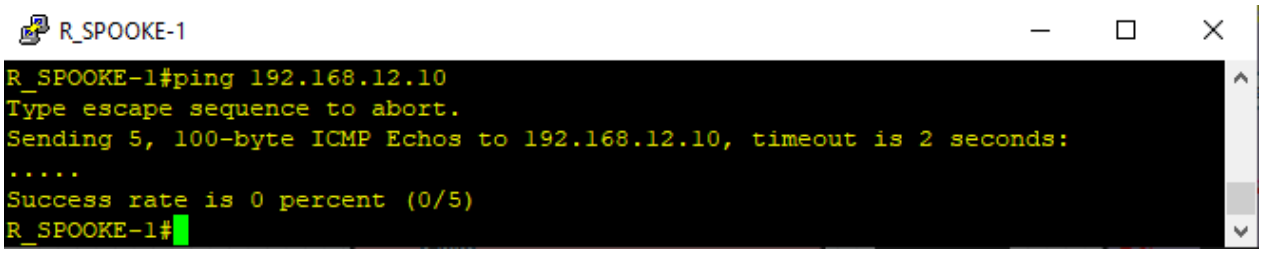

Figure 5.22: Test de connectivité Spoke-to-Spoke

5.5.7 DMVPN Phase 2

L'un des éléments fondamentaux de la solution DMVPN est la communication directe entre les spokes. Pour permettre cette communication spoke-to-spoke, il est crucial de passer de la phase 1 à la phase 2 de DMVPN. La phase 1 ne permet que les connexions spoke-to-hub, tandis que la phase 2 introduit la capacité pour les spokes de se connecter directement entre eux, améliorant ainsi l'efficacité et la performance du réseau.

- **Les commandes utilisées**

no ip split-horizon eigrp 10 : Désactive la fonctionnalité de "split horizon" sur l'interface de tunnel pour le processus EIGRP spécifié. Cela permet aux routes d'être annoncées correctement entre les spokes et le hub dans un réseau DMVPN.

no ip next-hop-self eigrp 10 : Empêche le routeur de se considérer lui-même comme le prochain saut lors de la redistribution des routes EIGRP via une interface de tunnel, aidant ainsi à éviter les boucles de routage.

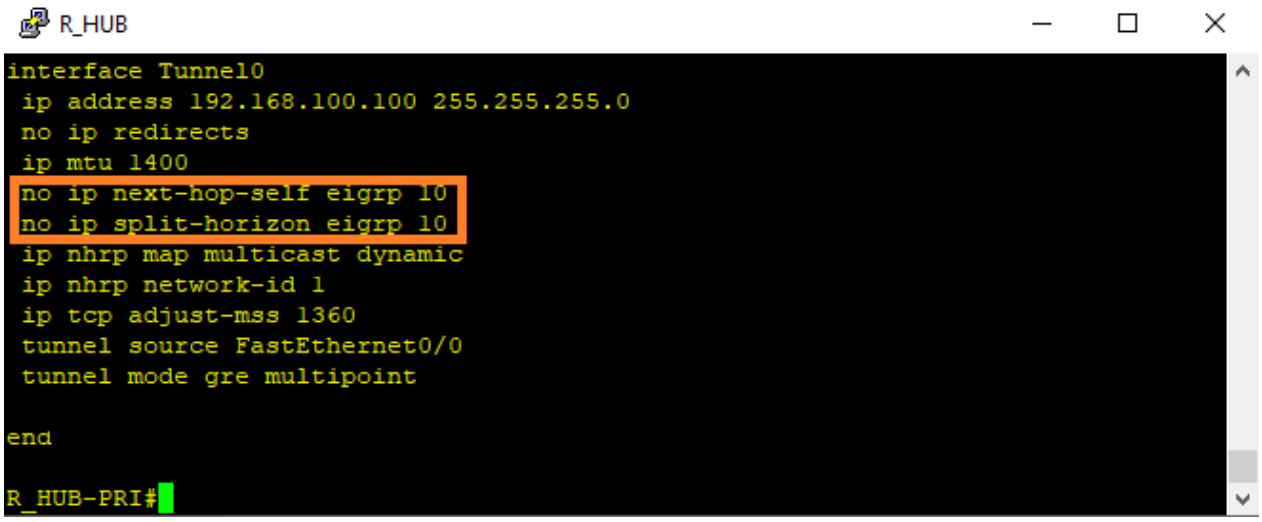

Figure 5.23: Phase 2 configuration (HUB-PRI)

- **Test de connectivité (Spoke-to-Spoke)**

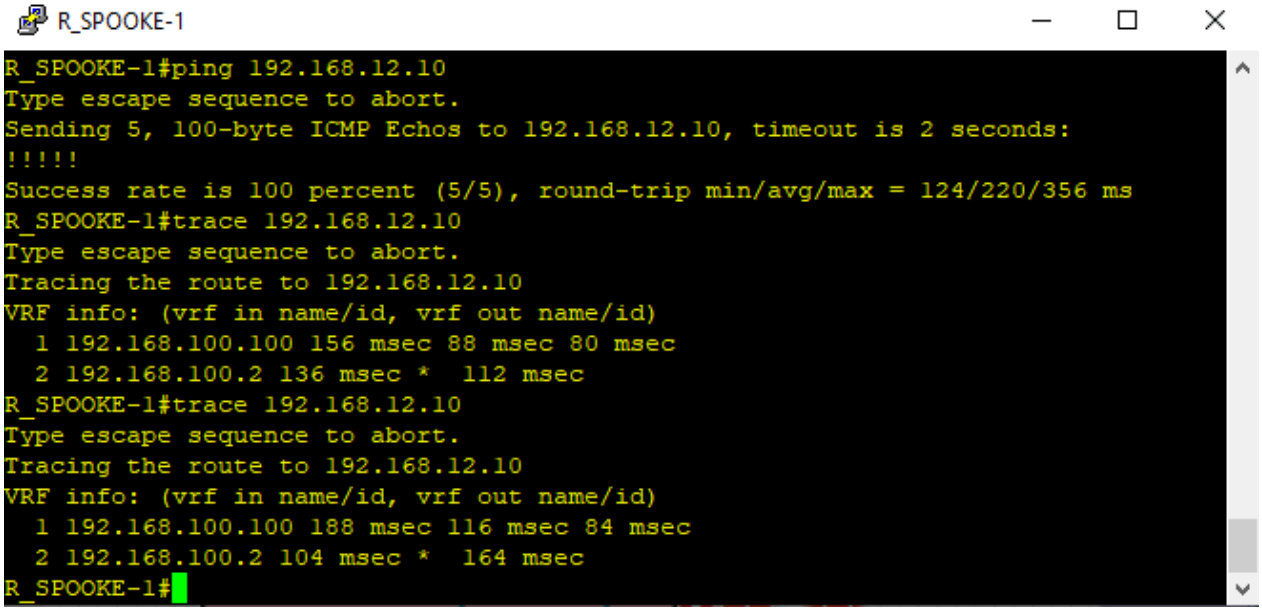

Figure 5.24: Test de connectivité phase 2

La Figure 5.24 montre que la connectivité entre les spokes fonctionne sans problème, grâce à la capacité du hub à permettre une connexion entre eux via sa résolution NHRP. Le traceroute montre clairement que le trafic passe toujours par le hub.

En DMVPN Phase 2, l'inconvénient majeur réside dans l'incapacité à établir des tunnels spoke-to-spoke, ce qui signifie que la communication entre les spokes doit nécessairement transiter par le hub. En revanche, la Phase 3 résout cette limitation en autorisant directement les tunnels spoke-to-spoke, éliminant ainsi la nécessité de passer par le hub pour les communications entre les spokes.

5.5.8 DMVPN Phase 3

La phase 3 représente une évolution de la phase 2 du DMVPN, introduisant la capacité essentielle d'établir des tunnels spoke-to-spoke, éliminant ainsi la dépendance obligatoire à passer par le hub pour les communications entre les spokes. En permettant une communication directe entre les spokes.

- **Les commandes utilisés**

ip nhrp redirect (HUB) : Permet aux hubs d'envoyer des messages ICMP Redirect aux spokes pour les informer d'une route plus optimale vers une destination (un autre spoke).

ip nhrp shortcut (Spoke) : permet aux spokes d'accepter et de traiter les messages ICMP Redirect, installant des routes de raccourci pour une communication directe plus efficace.

ip nhrp nhs 192.168.100.100 priority 1 cluster 1: Définit Hub1 comme NHS avec priorité 1 pour le cluster 1 (Primaire)

ip nhrp nhs 192.168.100.200 priority 2 cluster 1: Définit Hub2 comme NHS avec priorité 2 pour le cluster 1 (Backup).

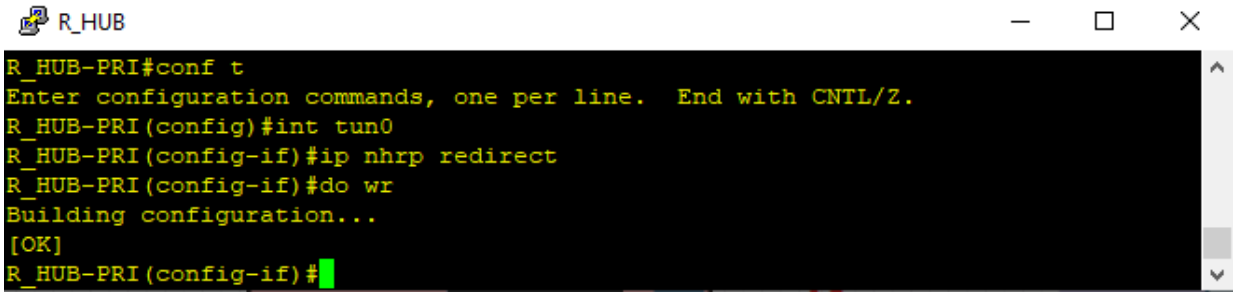

Figure 5.25: Phase 3 configuration pour les HUB

Figure 5.26: Phase 3 configuration pour les Spokes

- **Test de connectivité**

  Nous effectuons un test de connectivité entre le hub et les spokes.

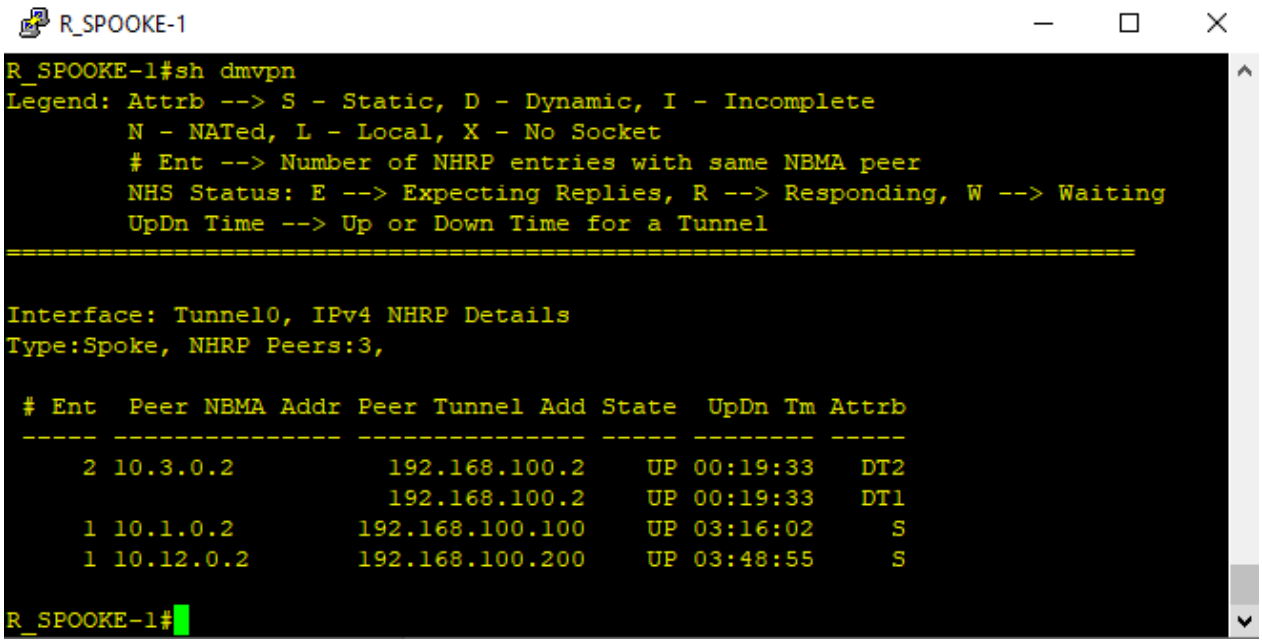

Figure 5.27: Output de la commande show dmvpn sur le Spoke 1

Dans la Figure 5.27, nous observons clairement qu'un tunnel direct a été établi entre les deux spokes

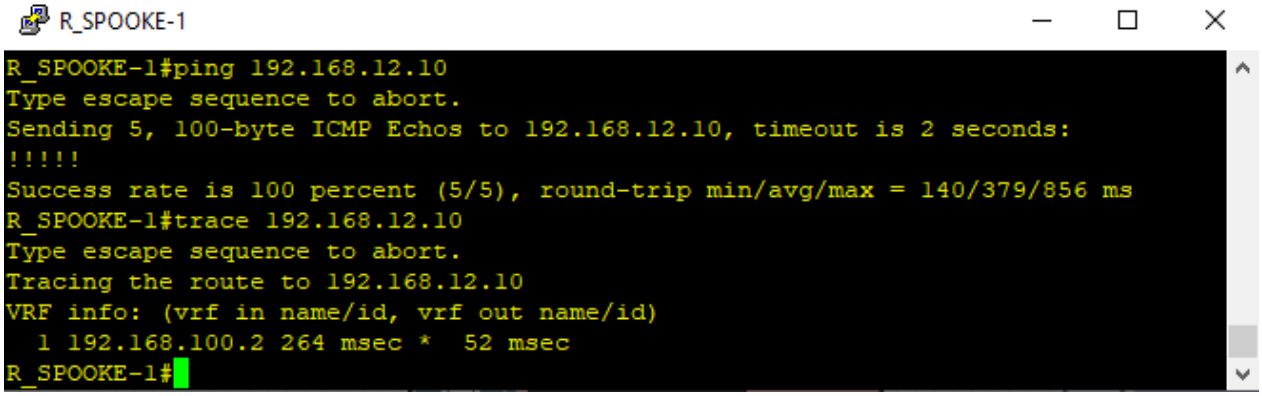

Figure 5.28: Test de connectivité Phase 3

Dans la Figure 5.27, on voit clairement que le traceroute passe directement de Spoke1 à Spoke2, illustrant ainsi la connexion directe entre les deux spokes sans passer par le hub central. Cela démontre l'efficacité de la configuration de la phase 3 du DMVPN.

5.5.9 Protection des Tunnels avec IPsec

En réalisant une capture Wireshark sur un des chemins de notre réseau on a distingué que plusieurs données sont transmises en clair comme les addresses IP privé, les masques, les protocoles utilisé ….

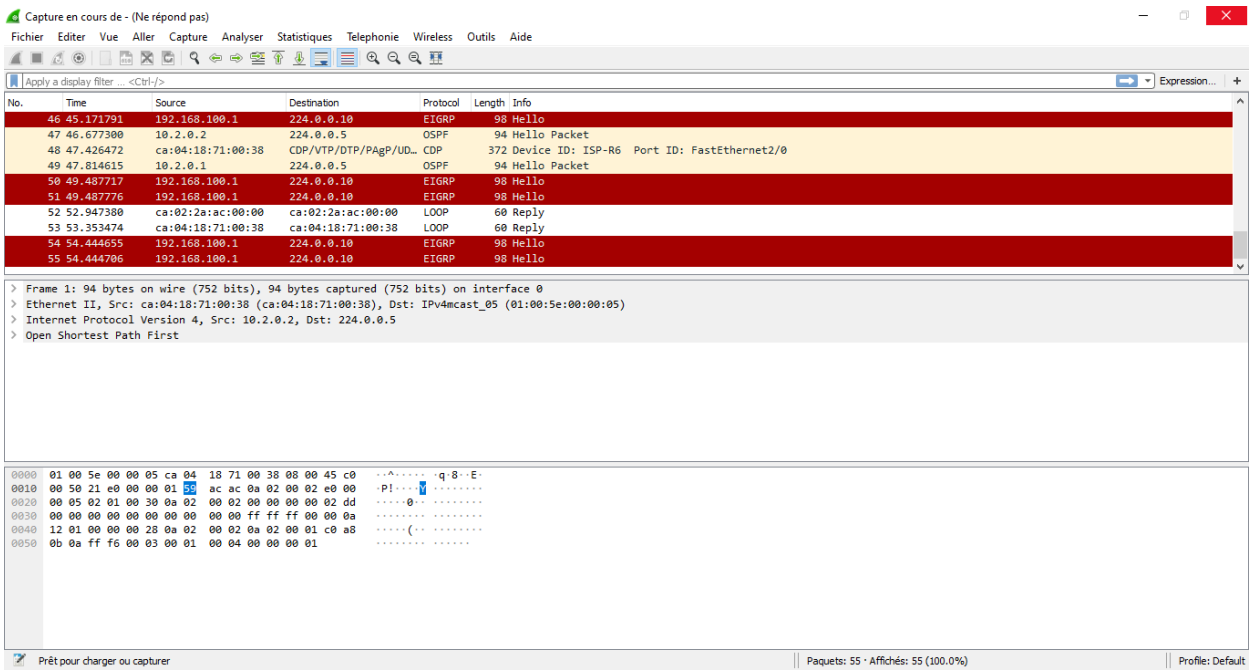

Figure 5.29: Capture Wireshark avant la création de IPsec

- **Les commandes utilisés**

crypto isakmp policy 10 : Cette commande lance le mode de configuration des politiques ISAKMP.

encr 3des : Cette commande permet de spécifier l'algorithme de chiffrement utilisé.

hash md5 : Cette commande permet de spécifier l'algorithme de hachage utilisé.

authentification pre-share : Utilise une clé pré-partagée pour l'authentification entre les routers VPN.

group 2 : Utilise le groupe Diffie-Hellman 2 pour l'échange de clés.

lifetime 86400 : Définit la durée de vie de l'association de sécurité en secondes. Après cette période, une nouvelle association doit être négociée.

crypto isakmp key memoire address 0.0.0.0: Cette commande permet de créer une clé d'authentification.

crypto ipsec-transform-set DMVPN Esp-3des esp-md5-hmac : Cette commande est utilisée pour créer une politique de sécurité IPsec qui sera appliquée aux tunnels IPsec.

mode transport : Indique que l'IPsec utilisera le mode transport.

crypto ipsec profile memo-DMVPN : cette commande permet de créer un profil IPsec à appliquer aux interfaces Tunnels.

set transform-set DMVPN : Associer les paramètres de sécurité IPsec (algorithmes de chiffrement et d'authentification) au profil IPsec.

tunnel protection ipsec profile memo-DMVPN (au niveau d'interface tunnel0) : Cette commande permet d'associer une interface tunnel à un profil IPsec.

Figure 5.30: IPsec profile creation

Pour tester l'efficacité de notre configuration IPsec, nous allons effectuer une autre capture Wireshark.

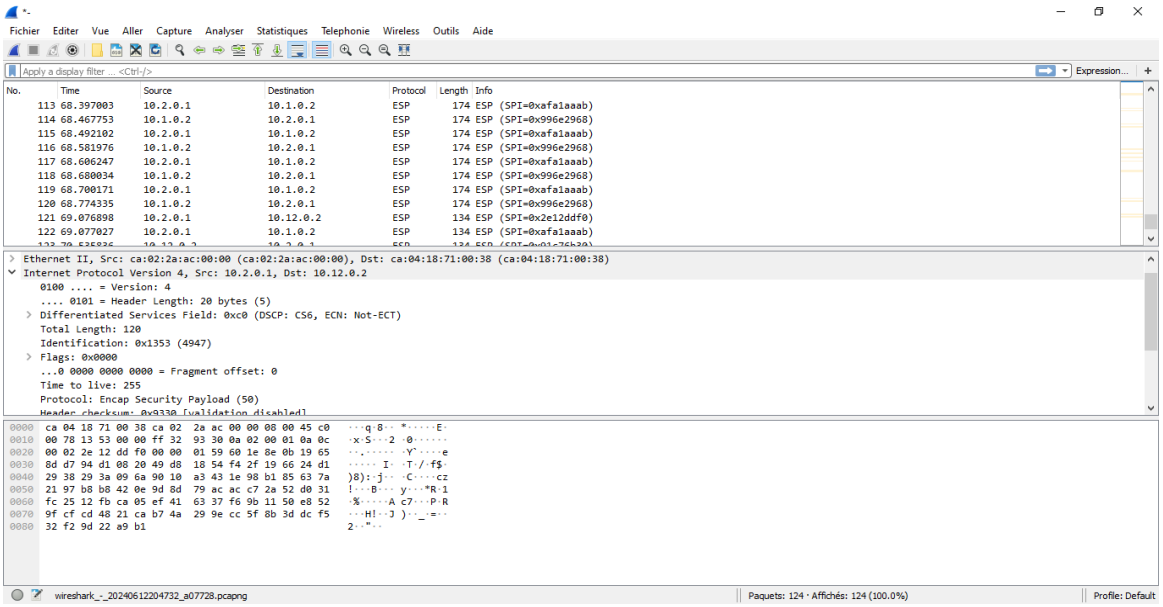

Figure 5.31: Capture Wireshark après la création de IPsec

On constate que toutes les données sont chiffrées avec succès, ce qui indique que la configuration IPsec fonctionne comme prévu.

5.5.10 Cas de défaillance

En cas de défaillance au niveau du HUB-PRI, l'importance du HUB-BACK devient évidente car il prend le relais dans le processus d'acheminement des données (comme illustré dans la Figure 5.34).

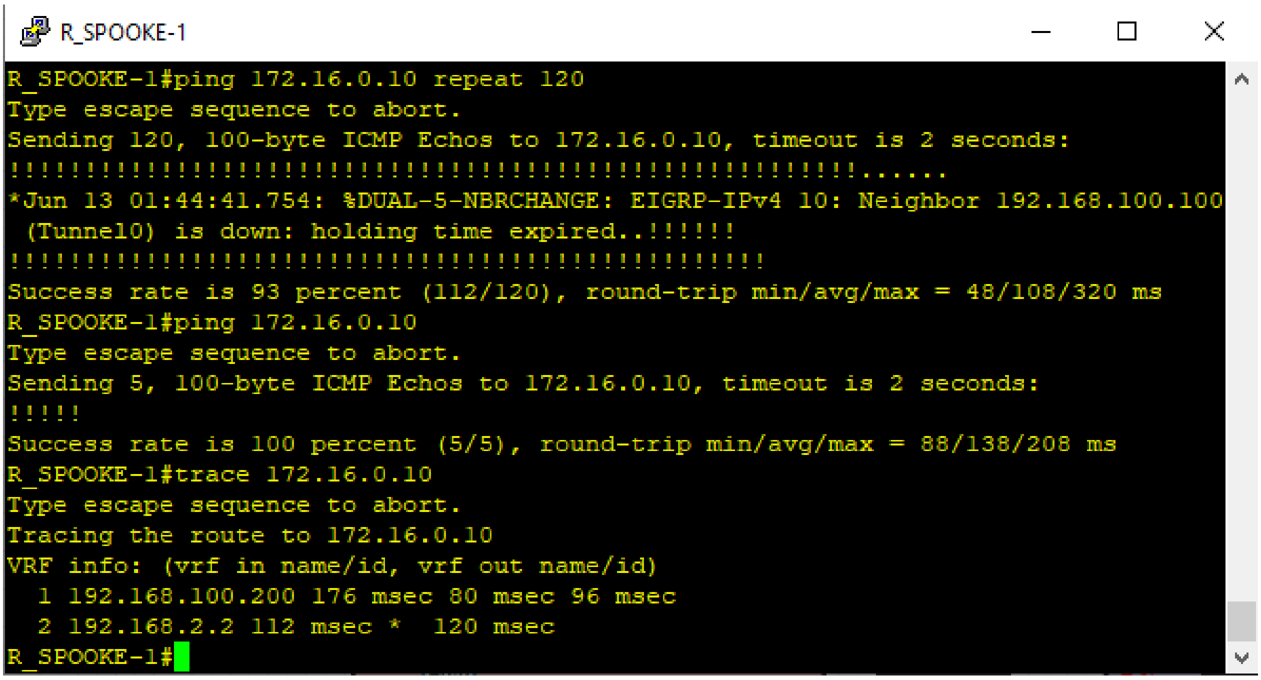

Figure 5.32: Défaillance au niveau du HUB-PRI

5.6 Conclusion

Dans ce chapitre, on a réalisé une implémentation réelle d'un réseau DMVPN et mettre en place tous les prérequis théoriques des chapitres précédents, l'implémentation de réseau a été réalisé en trois étapes, la première partie est consacrée à la configuration de la DMVPN phase 1, la deuxième partie présente l'évolution de la phase 1 vers la phase 2 et enfin dans la dernière partie, on procède à la configuration de la phase 3. Ce processus de déploiement pratique a permis de confirmer les performances et l'adaptabilité de solution DMVPN dans des scenarios réels.

Conclusion Générale

La technologie DMVPN s'est révélée être une solution cruciale pour les réseaux modernes, offrant une méthode innovante pour établir une connectivité sécurisée et flexible entre différents sites distants. Cette technologie permet de simplifier la gestion des réseaux, de réduire les coûts opérationnels et d'améliorer la performance globale en fournissant des communications directes entre les sites sans nécessiter un point de contrôle centralisé pour chaque communication. Grâce à ses capacités dynamiques, DMVPN répond efficacement aux besoins des entreprises qui cherchent à étendre leur réseau tout en maintenant un haut niveau de sécurité et de fiabilité.

Ce mémoire a été dédié à une exploration approfondie de cette technologie, en suivant un cheminement méthodique à travers cinq chapitres qui ont progressivement préparé le terrain pour une compréhension et une mise en œuvre réussie de DMVPN.

Nous avons commencé notre rapport en posant les bases en introduisant les concepts de base des réseaux informatiques. Nous avons exploré les définitions, les classifications, les architectures et les topologies des réseaux, ainsi que les modèles de référence OSI et TCP/IP, ce qui nous a fourni une fondation théorique indispensable.

Ensuite, nous avons approfondi la sécurité informatique, un aspect essentiel pour tout réseau moderne. Nous avons analysé diverses attaques et vulnérabilités, ainsi que les stratégies et méthodes de protection, mettant en évidence l'importance de sécuriser les réseaux, les systèmes d'exploitation, les applications et les données.

Dans le troisième chapitre, nous avons exploré les réseaux privés virtuels (VPN). Nous avons examiné leur fonctionnement et détaillé les différents types de VPN. Cette exploration nous a permis de mieux comprendre les critères de sélection d'un service VPN adapté, notamment dans un contexte de sécurité renforcée.

Enfin, le cœur de notre mémoire a été la technologie DMVPN. Nous avons exploré son histoire, ses principes et son fonctionnement. Nous avons examiné les modèles de déploiement et les phases clés associées à cette technologie soulignant son rôle crucial dans la création de réseaux sécurisés et flexibles., et nous avons conclu par une démonstration pratique d'implémentation à l'aide de l'émulateur EVE-NG, ce qui nous a permis de concrétiser les concepts théoriques en actions pratiques et de démontrer l'efficacité de DMVPN dans un environnement réel.

A la fin, ce stage m'a permis de développer mes compétences aussi bien sur le plan technique qu'organisationnel. J'ai également bénéficié d'une assistance exceptionnelle de la part de mes encadreurs et de mon promoteur afin de me préparer au monde professionnel.

Bibliographie

[2] *J. Dordoigne, « Réseaux Informatiques. » ENI, Paris, France, 2014.*

[3] *Riahla, « Généralités sur les réseaux informatiques. » UMBB, Boumerdes.*

[7] *C. A. Boussouf, « La sécurité informatique. » [Performance]. Université Mila.*

[8] *M. Mehoubi et N. Medjani, « Mémoire Master 2 "Sécurisation d'une infrastructure LAN /WAN à base d'équipements Cisco". » Université Tizi Ouzou, 2015.*

[9] *S. Ghernaouti-Hélie, sécurité informatique et réseaux, EYROLLES 3eme Edition, 2012.*

[12] *T. BahoniThisiri et S. Sahi, « Mémoire Master 2 "Solution VPN d'accès distant a l'intranet de l'université de Béjaïa : Application au réseau VLAN de scolarité". » Université de Béjaïa, Béjaïa, 2018.*

[10] *B. Laurent Bloch et W. Christophe, Sécurité informatique : principe et méthode, EYROLLES 2eme Edition, 2005.*

[13] *D. Mathieu, G. Olivier et M. Thomas, « Rapport du projet Portail Captif ».*

[20] *S. Boucherit et W. Khaled, « Mémoire Master 2 "Simulation d'un tunnel VPN-SSL pour la sécurisation d'une interconnexion de deux réseaux LANs". » Université de Béjaïa, Béjaïa, 2021.*

[27] *L. Merbah et N. Kaous, « Mémoire Master 2 "Etude et réalisation d'une architecture MPLS/VPN basée sur le principe de « hub & spoke »" » FT UMBB, Boumerdes, 2022/2023.*

[30] *N. Ghoualmi-Zine et R. Khelf, «A Survey on Dynamic Multipoint Virtual Private Networks» LRS CS Annaba University, Badji Mokhtar, 2019.*

[33] *B. Miganda, « Implémentation et interconnexion des réseaux privés virtuels. Cas des hôpitaux généraux de référence et clinique médicale privé. » BIOSADEC, Congo, 2015.*

[36] *R. Kabtane et A. M. Mancer, « Mémoire Master 2 "Etude et la mise en place d'une solution DMVPN via la technologie satellitaire VSAT iDirect". » USTHB, Alger, 2022.*

[41] *D. Diatou, G. Yakete et D. Sada, « Dynamic Multipoint Virtual Private Network (DMVPN) » INSTITUT SUPERIEUR D'INFORMATIQUE (ISI), 2013.*

Webographie

[1] https://www.ionos.fr/digitalguide/serveur/know-how/reseau-informatique-definition/. (Accès le 03/2024).

[4] https://alf.asso-web.com/uploaded/r-seau-informatique.pdf. (Accès le 03/2024).

[5] https://www.ibm.com/topics/three-tier-architecture. (Accès le 04/2024).

[6] https://www.ibm.com/fr-fr/topics/it-security. (Accès le 04/2024).

[11] http://wapiti.enic.fr/Commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2002ttnfa03/Vasseur-Marcq/Attaques/Types_attaques.htm#2. (Accès le 05/2024).

[14] https://blog.jesuisinformaticien.fr/cest-quoi-le-hachage-eninformatique/. (Accès le 05/2024).

[15] https://fr.m.wikiversity.org/wiki/Fichier:Firewall.png. (Accès le 05/2024).

[16] https://www.belcenter.be/blog/pourquoi-vpn-entreprise-pme-guide/#jsaccept-cookies. (Accès le 05/2024).

[18] https://www.researchgate.net/figure/VPN-Tunnelingstructure_fig1_320536838. (Accès le 05/2024).

[19] https://www.memoireonline.com/01/20/11531/m_Deploiement-d-uncoeur-de-reseau-IPMPLS35.html. (Accès le 05/2024).

[21] https://websitehosting.com/faq/pptp-protocol/. (Accès le 05/2024).

[22] https://www.hideipvpn.com/learning-center/what-is-pptp/. (Accès le 05/2024).

[23] https://www.expressvpn.com/what-is-vpn/protocols/l2tp. (Accès le 05/2024).

[24] https://www.privacyaffairs.com/ikev2-vpn-protocol/. (Accès le 05/2024).

[25] https://info.support.huawei.com/infofinder/encyclopedia/en/IPsec.html. (Accès le 05/2024).

[26] https://cisco.goffinet.org/ccna/wan/tunnels-gre/. (Accès le 05/2024).

[28] https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn. (Accès le 05/2024).

[29] https://networkdirection.net/articles/routingandswitching/dmvpn/dmvpn-and-dynamic-routing/. (Accès le 05/2024).

[31] https://www.techtarget.com/searchsecurity/definition/Internet-Key-Exchange. (Accès le 05/2024).

[32] https://md.inetdoc.net/s/8JtS3966t#L%E2%80%99%C3%A9change-de-cl%C3%A9s-Diffie-Hellman. (Accès le 05/2024).

[34] *ESEO, 2000. URL :* https://www.guill.net/view.php?cat=4&sec=2&cqr=5. (Accès le 2024).

[35] https://developpement-informatique.com/article/452/mode-tunnel-et-mode-de-transport-ipsec. (Accès le 05/2024).

[37] https://stucknactive.com/2019/03/04/1-20-next-hop-resolution-protocol/. (Accès le 05/2024).

[38] https://www.pluralsight.com/blog/it-ops/multipoint-gre-tunnel-introduction. (Accès le 05/2024).

[39] https://www.cisco.com/c/fr_ca/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html#related. (Accès le 05/2024).

[40] *Cyril, « Introduction à OSPF. » URL :* https://reussirsonccna.fr/introduction-a-ospf/. (Accès le 05/2024).

[42] https://www.plixer.com/blog/cisco-dmvpn-configuration/. (Accès le 06/2024).

[43] https://networklessons.com/cisco/ccie-routing-switching/introduction-to-dmvpn. (Accès le 06/2024).