RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88
https://www.ifri-uac.bj Courriel : contact@ifri-uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Sécurité Informatique

Présenté par :
Enagnon Mahougnon Jules **HOUNDEKANNOU**

Conception et mise en place d'un réseau multisite sécurisé utilisant Dynamic Multipoint VPN

Sous la supervision :
Ing. Victor **OYETOLA**

Membres du jury :

SAHO Nelson	Docteur	Ministère des Affaires Etrangères	Président
GOUDALO Jospy K.	Ingénieur	Caisse Autonome de Gestion de la Dette	Examinateur
OYETOLA Victor	Ingénieur	Université d'Abomey-Calavi	Rapporteur

Année Académique : **2024-2025**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Liste des figures vi

Liste des tableaux vii

Liste des acronymes viii

Introduction 1

1 Revue de littérature 4

2 Conception technique et implémentation 13

3 Résultats et Analyses 29

Conclusion 36

Bibliographie 37

Webographie 38

Table des matières 39

Dédicace

Le cœur de l'homme médite sa voie, mais c'est l'Éternel qui dirige ses pas. **[Proverbes 16 : 9]**

À

Tous ceux qui, par leurs encouragements, leur soutien et leur sagesse, ont permis de donner vie à ce projet. À ceux qui croient que chaque chemin, même incertain, est une occasion de grandir. Que cette œuvre soit un témoin de la volonté divine et de la persévérance humaine pour l'essor des sciences informatiques, particulièrement en Afrique et au Bénin.

Remerciements

La réalisation de ce projet de mémoire a été rendue possible grâce à la contribution et au soutien de nombreuses personnes à qui je souhaite exprimer ma reconnaissance. Je tiens à remercier sincèrement :

- Le Professeur Eugène C. EZIN, Directeur de l'Institut de Formation et de Recherche en Informatique (IFRI), pour la formation de qualité et les conseils avisés.
- L'Ingénieur Victor OYETOLA, mon maître de mémoire, pour sa confiance, ses précieux conseils et sa disponibilité constante tout au long de ce parcours.
- L'ensemble des professeurs de l'IFRI, pour leur dévouement et leur engagement à fournir les outils nécessaires à notre réussite académique.
- Madame Marthe PADONOU, Responsable Service Quality et Delivery, et Monsieur Nick Aurel HOUESSOU, Responsable de la Sécurité des Systèmes d'Information, à Moov Africa Bénin pour leurs orientations expertes et leur accompagnement personnalisé.
- Monsieur Narcisse TOSSA, Administrateur Réseau à MOOV Africa Bénin, pour son expertise technique et sa patience qui ont été déterminantes les pour ma formation.
- Monsieur Spéro ADONON, Administrateur Système Linux et Bases de données à Moov Africa Bénin et Monsieur Camara, Hardware Support dont le soutien technique et les conseils avisés ont été essentiels à mon apprentissage et à ma réussite
- L'ensemble du personnel de la Direction des Systèmes d'Information, pour l'environnement de travail stimulant et convivial qu'ils ont partagé avec moi.
- À ma famille, mon plus grand pilier, merci pour votre amour inconditionnel, votre soutien sans faille et votre foi en moi, qui m'ont donné la force de persévérer et d'atteindre chaque étape de ce chemin.

Que chacun de vous trouve ici l'expression de ma profonde gratitude. Votre soutien a été un pilier de cette aventure, et je vous en suis infiniment reconnaissant.

Résumé

L'expansion des entreprises à travers plusieurs sites géographiques exige des solutions de connectivité évolutives et sécurisées. Face à la nécessité d'échanger des données en temps réel avec une protection optimale, les VPN classiques, bien que largement adoptés, révèlent des limitations structurelles lorsqu'ils doivent s'adapter à des infrastructures en pleine croissance. Leur rigidité, la complexité de leur administration et leur faible scalabilité constituent des obstacles majeurs à une gestion efficace des interconnexions multisites. Dans cette étude, nous avons entrepris une approche expérimentale comparative en implémentant successivement un VPN IPsec et un DMVPN dans un environnement simulé sous GNS3. Cette méthodologie nous permet d'analyser de manière objective les performances de chaque technologie en termes de latence, de bande passante, d'optimisation des flux et de facilité d'administration. Les premières analyses confirment que le VPN IPsec, bien qu'offrant une sécurité robuste grâce à son chiffrement avancé, impose une gestion rigide et des configurations complexes, notamment en matière de gestion des tunnels et de redondance des liens. En revanche, le DMVPN, en exploitant le protocole NHRP (Next Hop Resolution Protocol) et en permettant l'établissement dynamique des tunnels entre sites, s'avère bien plus flexible et optimisé pour les infrastructures évolutives.

Mots clés : VPN, DMVPN, Sécurité, Réseau, Données.

Abstract

As companies expand across multiple geographies, they need secure, scalable connectivity solutions. Faced with the need to exchange data in real time with optimum protection, conventional VPNs, although widely adopted, reveal structural limitations when it comes to adapting to growing infrastructures. Their rigidity, administrative complexity and low scalability are major obstacles to the efficient management of multisite interconnections. In this study, we undertook a comparative experimental approach by successively implementing an IPsec VPN and a DMVPN in a simulated environment under GNS3. This methodology enables us to objectively analyze the performance of each technology in terms of latency, bandwidth, flow optimization and ease of administration. Initial analyses confirm that IPsec VPN, while offering robust security thanks to its advanced encryption, imposes rigid management and complex configurations, particularly in terms of tunnel management and link redundancy. DMVPN, on the other hand, exploits NHRP (Next Hop Resolution Protocol) and enables dynamic tunnelling between sites, proving far more flexible and optimized for scalable infrastructures.

Key words: VPN, DMVPN, Security, Network, Data.

Liste des figures

1.1 Architecture du DMVPN 10

2.1 Schéma de l'architecture réseau 14
2.2 Informations sur les interfaces du routeur ALLADA 16
2.3 Informations sur les interfaces du routeur COTONOU 16
2.4 Configuration de l'ISP 17
2.5 Détails de configuration IKE 17
2.6 Configuration de la politique ISAKMP : routeur COTONOU 18
2.7 Configuration de la politique ISAKMP : routeur CALAVI 19
2.8 Détails ACL : routeur ALLADA 19
2.9 Détails ACL : routeur COTONOU 19
2.10 Activation du DMVPN : routeur COTONOU 21
2.11 Activation du DMVPN : routeur CALAVI 22
2.12 Configuration EIGRP : routeur CALAVI 23
2.13 Configuration EIGRP : routeur CALAVI 23
2.14 Informations sur les tunnnels : routeur COTONOU 23
2.15 Informations sur les tunnnels : routeur ALLADA 24
2.16 Informations sur les tunnnels : routeur CALAVI 24
2.17 Etablissement du tunnel ISAKMP : routeur ALLADA 25
2.18 Etablissement du tunnel ISAKMP : routeurCOTONOU 25
2.19 Détails des associations IPSec : routeur COTONOU 26
2.20 Activation du routage dynamique : routeur COTONOU 27
2.21 Activation du routage dynamique : routeur ALLADA 27
2.22 Activation du routage dynamique : routeur CALAVI 27

3.1 Ping PC1 vers PC2 29
3.2 Ping PC1 vers PC2 30
3.3 Ping ALLADA vers COTONOU 30
3.4 Ping COTONOU vers ALLADA 30
3.5 Ping COTONOU vers CALAVI 30
3.6 Capture wireshark : VPN site-to-site 32
3.7 Capture wireshark : DMVPN 33

Liste des tableaux

1.1 Tableau de comparaison détaillée entre les VPN traditionnels et le DMVPN 11

2.1 Tableau de configuration de l'adressage. 15
2.2 Tableau de configuration de l'adressage. 20

Liste des acronymes

3DES :

Triple Data Encryption Standard

ACL :

Access Control List

AES :

Advanced Encryption Standard

AH :

Authentication Header

BGP :

Border Gateway Protocol

CDP :

Cisco Discovery Protocol

DH :

Diffie-Hellman

DMVPN :

Dynamic Multipoint Virtual Private Network

DTP :

Dynamic Trunking Protocol

eBGP :

External Border Gateway Protocol

EIGRP :

Enhanced Interior Gateway Routing Protocol

ESP :

Encapsulating Security Payload

GRE :

Generic Routing Encapsulation

HMAC :

Hashed Message Authentication Code

HSRP :

Hot Standby Router Protocol

iBGP :

Internal Border Gateway Protocol

ICMP :

Internet Control Message Protocol

IDS :

Intrusion Detection System

IKE :

Internet Key Exchange

IKEv1 :

Internet Key Exchange version 1

IKEv2 :

Internet Key Exchange version 2

IPS :

Intrusion Prevention System

IPsec :

Internet Protocol Security

IS-IS :

Intermediate System to Intermediate System

ISAKMP :

Internet Security Association and Key Management Protocol

ISP :

Internet Service Provider

L2TP :

Layer 2 Tunneling Protocol

LAN :

Local Area Network

MAN :

Metropolitan Area Network

MD5 :

Message Digest Algorithm 5

mGRE :

Multipoint Generic Routing Encapsulation

MPLS :

Multiprotocol Label Switching

MTU :

Maximum Transmission Unit

NAT :

Network Address Translation

NBMA :

Non-Broadcast Multi-Access

NetFlow :

Network Flow Monitoring

NHRP :

Next Hop Resolution Protocol

OSPF :

Open Shortest Path First

PAT :

Port Address Translation

PKI :

Public Key Infrastructure

PoP :

Point of Presence

PPTP :

Point-to-Point Tunneling Protocol

PSK :

Pre-Shared Key

QoS :

Quality of Service

RIP :

Routing Information Protocol

SHA :

Secure Hash Algorithm

SNMP :

Simple Network Management Protocol

Syslog :

System Logging Protocol

TCP :

Transmission Control Protocol

UDP :

User Datagram Protocol

VPN :

Virtual Private Network

VRF :

Virtual Routing and Forwarding

VRRP :

Virtual Router Redundancy Protocol

WAN :

Wide Area Network

ZBF :

Zone-Based Firewall

Introduction générale

Dans un monde où la connectivité est au cœur des échanges économiques et stratégiques, les entreprises et institutions font face à un défi de taille : assurer la sécurité et la fluidité des communications entre des sites toujours plus nombreux et dispersés géographiquement. Qu'il s'agisse de multinationales, de services gouvernementaux ou d'organisations en pleine expansion, la nécessité d'un accès distant fiable et sécurisé aux ressources informatiques est devenue primordiale. Historiquement, les réseaux privés virtuels (VPN) se sont imposés comme la solution de référence pour sécuriser les échanges de données sur des infrastructures publiques comme Internet. Toutefois, face à l'augmentation exponentielle du volume de données et à l'évolution des besoins en connectivité, cette technologie atteint ses limites, notamment en matière de gestion et de scalabilité.

1. Contexte

La modernisation des réseaux d'entreprise repose sur des solutions capables de concilier sécurité, flexibilité et efficacité opérationnelle. Les architectures VPN classiques, bien que largement adoptées, imposent une gestion rigide et une surcharge potentielle des infrastructures. Le DMVPN, en s'appuyant sur le routage dynamique et le protocole NHRP, promet une gestion plus agile des interconnexions multisites tout en garantissant un chiffrement robuste via IPsec.

2. Problématique

Face aux exigences croissantes des réseaux multisites, les VPN traditionnels, reposant sur des **configurations point-à-point fixes**, imposent des ajustements manuels lourds et des coûts significatifs en maintenance, surtout à mesure que le nombre de sites augmente. Le Dynamic Multipoint Virtual Private Network (DMVPN) émerge comme une solution innovante, permettant des connexions dynamiques et sécurisées entre sites sans configuration manuelle extensive. Comment le DMVPN peut-il garantir la sécurité, la flexibilité et la performance des réseaux d'entreprise multisite, tout en simplifiant la gestion et en réduisant les coûts de maintenance ?

3. Objectifs

L'objectif principal de ce mémoire est de démontrer comment l'intégration d'un DMVPN dans les réseaux d'entreprise multisite permet d'améliorer la flexibilité, la sécurité, et la performance des infrastructures réseau tout en simplifiant leur gestion.

Objectifs spécifiques

a) **Étude approfondie des protocoles** utilisés par le DMVPN, à savoir : **mGRE**, **NHRP**, **IPsec**

b) **Conception et simulation d'un VPN site to site et du DMVPN** à l'aide de **GNS3**, simulant un environnement multisite typique.

c) **Tests de performance** pour mesurer la **latence**, la **scalabilité**, et l' **évolutivité** du réseau.

d) Formulation des **recommandations** et des **meilleures pratiques** pour l'implémentation et la maintenance d'un réseau DMVPN dans un contexte d'entreprise.

4. Méthodologie

Pour atteindre ces objectifs, la méthodologie adoptée dans ce mémoire comprend les étapes suivantes :

a) Recherche documentaire :

- Une étude approfondie des publications scientifiques, des normes industrielles, et des études de cas sur les VPN traditionnels et le DMVPN.
- Analyse des protocoles clés (mGRE, NHRP, IPsec) utilisés dans la configuration du DMVPN.

b) Conception d'un prototype :

- Utilisation de l'outil de simulation GNS3 pour modéliser un réseau VPN site-to-site.
- Utilisation de l'outil de simulation GNS3 pour modéliser un réseau DMVPN multisite.
- Configuration des routeurs pour supporter le mGRE, le NHRP, et l'IPsec.

c) Simulation et tests :

- Exécution de scénarios simulant différents types de trafic pour évaluer les performances du DMVPN.
- Analyse des échanges entre les hôtes du réseau avec Wireshark

d) Analyse des résultats : Comparaison des performances entre un VPN traditionnel et un DMVPN pour en démontrer les avantages.

e) Formulation des recommandations et perspectives : Proposer des lignes directrices pour intégrer le DMVPN dans des environnements réseau existants et perspectives d'améliorations.

5. Structure du document

Ce mémoire est structuré en plusieurs chapitres, chacun abordant un aspect clé de l'étude. Le premier chapitre, qu'est la revue de littérature, explore les concepts théoriques liés aux VPN, en mettant l'accent sur le DMVPN et ses avantages par rapport aux VPN traditionnels. Ensuite, le chapitre Conception Technique et Implémentation détaille la mise en œuvre du prototype VPN site-to-site et du DMVPN, illustré par des captures d'écran des configurations et des scénarios de test. Le troisième chapitre, les résultats et analyses, présente les résultats des tests de performance et de sécurité effectués sur le réseau DMVPN, accompagnés d'une analyse comparative avec les VPN traditionnels. S'en suivent la conclusion et les perspectives qui résument les principales conclusions de l'étude et proposent des pistes pour des recherches futures.

Chapitre 1

Revue de littérature

Introduction

L'évolution des réseaux multisites a été fortement influencée par la globalisation des entreprises et le besoin croissant d'une connectivité sécurisée entre leurs bureaux situés dans des zones géographiques différentes. À mesure que les entreprises ont étendu leurs opérations à travers le monde, il est devenu fondamental d'interconnecter efficacement leurs sites pour **partager des ressources** et **optimiser les processus métiers.** Dans les années 1980 et 1990, les entreprises se reposaient sur des technologies comme les lignes louées (leased lines) pour établir des connexions point-à-point entre leurs différents bureaux. Cette approche, bien que fiable, était coûteuse et inflexible, car chaque site devait être connecté via des circuits dédiés, entraînant des frais d'infrastructure élevés. Avec l'émergence d'Internet comme un réseau global, les entreprises ont cherché des moyens d'utiliser cette infrastructure publique pour réduire les coûts tout en maintenant un haut niveau de sécurité. C'est dans ce contexte que les réseaux privés virtuels (VPN) sont apparus comme une solution efficace pour interconnecter des sites distants de manière sécurisée, sans recourir aux lignes dédiées onéreuses.

1.1 Les réseaux privés virtuels (VPN)

1.1.1 Introduction aux réseaux privés virtuels (VPNs)

Les réseaux privés virtuels (VPNs) sont des technologies de réseau qui permettent de sécuriser les communications sur des réseaux publics, comme l'Internet, en créant des "tunnels" chiffrés pour acheminer des données. Le principal objectif d'un VPN est de garantir la confidentialité, l'intégrité et l'authentification des communications entre des sites distants ou entre un client distant et un réseau privé.
Un VPN peut être utilisé pour plusieurs raisons, parmi lesquelles :

- **Sécuriser l'accès à distance** pour les utilisateurs qui se connectent depuis des emplacements externes.
- **Relier plusieurs sites géographiquement dispersés**, permettant une communication transparente comme si les sites étaient connectés localement.

- **Protéger la confidentialité des données** échangées sur des réseaux publics, en utilisant des techniques de chiffrement avancées.

1.2 Types de VPN

Il existe plusieurs types de VPNs en fonction de l'architecture du réseau et des besoins spécifiques. Les deux principaux types sont :

a. VPN Site-to-Site

Un VPN Site-to-Site permet de connecter deux ou plusieurs sites distants via un réseau public sécurisé. Ce type de VPN est couramment utilisé par les entreprises ayant des bureaux dans plusieurs régions. Il permet aux employés de différentes branches de l'entreprise d'accéder aux ressources du réseau interne de manière sécurisée, même si elles sont géographiquement éloignées.
Les VPN Site-to-Site sont souvent utilisés avec IPsec pour garantir la sécurité des données transmises. Ce type de VPN est configuré sur des routeurs ou des pare-feu, qui établissent une connexion sécurisée entre les réseaux locaux (LAN) de chaque site.

b. VPN Client-to-Site

Le VPN Client-to-Site permet à un utilisateur distant (un employé travaillant à domicile, par exemple) de se connecter à un réseau d'entreprise via un tunnel sécurisé. Contrairement au VPN Site-to-Site, où la connexion est établie entre les sites, le VPN Client-to-Site implique l'utilisation d'un logiciel client VPN (par exemple, Cisco AnyConnect, OpenVPN) installé sur l'ordinateur de l'utilisateur. Ce client établit une connexion sécurisée avec le serveur VPN de l'entreprise, permettant à l'utilisateur d'accéder aux ressources du réseau interne.
Les VPN Client-to-Site sont couramment utilisés pour le télétravail, en permettant aux employés de se connecter de manière sécurisée à l'entreprise, quelle que soit leur localisation.

c. VPN SSL (Secure Sockets Layer)

Les SSL VPNs sont une variante des VPNs qui utilisent le protocole SSL/TLS pour sécuriser les connexions entre un client (souvent un navigateur web) et un serveur. Ce type de VPN est couramment utilisé pour l'accès distant sécurisé, en particulier lorsque les utilisateurs n'ont pas besoin d'un logiciel client VPN dédié.
Les SSL VPNs sont populaires car ils ne nécessitent pas de configuration complexe de la part de l'utilisateur final. Ils peuvent être utilisés via un simple navigateur web, ce qui simplifie l'accès aux applications internes pour les employés en déplacement ou les partenaires externes.

1.3 Fonctionnement d'un VPN

Un réseau privé virtuel (VPN) permet de sécuriser les transferts de données sur Internet en créant un tunnel chiffré entre l'appareil de l'utilisateur et un serveur distant. Ce processus implique plusieurs étapes : la configuration du réseau, l'authentification des utilisateurs, l'établissement du tunnel sécurisé, la transmission des données et la gestion continue des connexions [2].

1.3.1 Configuration initiale

Avant d'établir une connexion VPN, une infrastructure sécurisée doit être mise en place.

1.3.1.1 Infrastructure et composants

L'architecture d'un VPN repose sur :

- Un **passerelle VPN** assurant la connexion entre le réseau interne et les appareils externes.
- Un **logiciel client** installé sur les terminaux des utilisateurs.
- Une **infrastructure réseau** comprenant routeurs, pare-feu et commutateurs pour garantir l'intégrité des communications.

1.3.1.2 Configuration et politiques de sécurité

Les administrateurs définissent des politiques d'accès et des règles de sécurité pour :

- Déterminer les utilisateurs et appareils autorisés.
- Sélectionner des standards de chiffrement robustes.
- Configurer les routes réseau permettant le passage du trafic chiffré.

1.3.2 Phase d'initiation

L'établissement d'une connexion VPN passe par une authentification et un protocole de négociation.

1.3.2.1 Authentification des utilisateurs

L'identité des utilisateurs est vérifiée à travers :

- **Certificats numériques** délivrés par une autorité de certification (CA).
- **Authentification multi-facteurs** (MFA) combinant mot de passe, biométrie ou jeton physique.
- **Services d'annuaire** tels qu'Active Directory pour centraliser la gestion des accès.

1.3.2.2 Établissement de la connexion sécurisée

Après l'authentification, un protocole de négociation est engagé :

- Sélection du **protocole VPN** (IKEv2, OpenVPN, WireGuard, etc.).
- Choix d'une **suite cryptographique** définissant l'algorithme de chiffrement et la méthode d'échange de clés.

1.3.3 Création du tunnel VPN

Une fois l'authentification réussie, un tunnel chiffré est établi.

1.3.3.1 Sélection du protocole de tunneling

Le choix du protocole conditionne la sécurité et la compatibilité du VPN :

- **IPsec** : Sécurise le trafic au niveau IP.
- **L2TP** : Combiné à IPsec pour une meilleure sécurité.
- **OpenVPN** : Basé sur SSL/TLS, flexible et sécurisé.

1.3.3.2 Échange de clés et chiffrement

Pour garantir la confidentialité, un échange de clés sécurisé est réalisé :

- **Diffie-Hellman (DH)** permet aux deux parties de générer une clé commune sans transmission directe.
- **AES (Advanced Encryption Standard)** assure un chiffrement robuste.
- Utilisation de **Perfect Forward Secrecy (PFS)** pour renouveler les clés et empêcher leur compromission.

1.3.4 Transmission des données

Une fois le tunnel sécurisé en place, les données peuvent être transmises en toute confidentialité.

1.3.4.1 Attribution d'adresses IP et intégration réseau

Chaque client VPN reçoit une **adresse IP privée** permettant de rejoindre le réseau cible. Les politiques d'accès définissent les ressources accessibles selon l'identité de l'utilisateur.

1.3.4.2 Optimisation des performances

Pour améliorer le débit et réduire la latence :

- Compression des données pour réduire l'empreinte réseau.
- Choix du protocole adapté (PPTP privilégie la vitesse, OpenVPN offre un bon équilibre sécurité/rapidité).

1.3.4.3 Routage et intégrité des paquets

Le VPN assure un acheminement optimal des paquets :

- Utilisation de **commutation de paquets** dynamique pour éviter la congestion.
- Chiffrement des paquets en transit pour garantir leur intégrité et confidentialité.

1.3.5 Routage et accès aux ressources

Deux stratégies de routage sont envisageables :

- **Tunneling complet** : Tout le trafic passe par le VPN, assurant une sécurité maximale mais consommant plus de bande passante.
- **Tunneling fractionné** : Seul le trafic destiné au réseau de l'entreprise passe par le VPN, réduisant la charge réseau mais exposant certaines connexions directes.

L'accès aux ressources est régulé par des **listes de contrôle d'accès (ACL)** et des politiques de sécurité strictes.

1.3.6 Gestion continue de la connexion

Le maintien de la connexion VPN repose sur :

- Vérifications d'intégrité (**checksums, numéros de séquence**) pour détecter toute altération.
- Envoi de **messages Keepalive** et **heartbeats** pour éviter la coupure des sessions inactives.

1.3.7 Fermeture de la connexion

Lorsque la session VPN se termine, des mesures sécuritaires sont appliquées :

- **Envoi d'un message de fermeture** pour s'assurer que les deux parties reconnaissent la fin de la session.
- **Suppression des clés de session** et nettoyage des ressources utilisées.
- **Enregistrement des logs** pour audit et détection d'anomalies.

1.3.8 Limites des VPN traditionnels pour les entreprises multisites [3].

a. Complexité de configuration :

Les VPNs traditionnels, en particulier les VPNs IPsec, nécessitent une configuration point-à-point entre chaque site. Cela signifie que pour chaque nouveau site ajouté, il faut configurer manuellement une connexion avec chaque site existant. Cette approche devient rapidement ingérable pour les entreprises ayant de nombreux sites. La **conséquence** directe est l'augmentation des coûts de gestion et risques d'erreur humaine lors des configurations.

b. Rigidité

Les VPNs traditionnels ont une topologie fixe. Chaque changement dans la structure du réseau (par exemple, ajout ou suppression de sites) nécessite des modifications importantes dans les configurations existantes.

c. Coûts élevés

Le coût d'implémentation et de maintenance des VPN traditionnels peut être prohibitif, en particulier avec MPLS, qui nécessite souvent du matériel spécialisé et des contrats avec les fournisseurs de services. De plus, chaque site nécessite un équipement dédié pour gérer le chiffrement IPsec, ce qui augmente les coûts initiaux.

Les VPN IPsec nécessitent des configurations manuelles et sont souvent difficiles à adapter aux infrastructures multisites dynamiques. Le MPLS offre une qualité de service supérieure, mais il est limité en termes de flexibilité et scalabilité, en plus d'être coûteux. Les limites des VPN traditionnels en termes de flexibilité, scalabilité, et coûts ont ouvert la voie à des solutions plus dynamiques comme le DMVPN. Ce dernier permet de résoudre ces problèmes avec des connexions sécurisées, évolutives et plus faciles à configurer.

1.4 Présentation du DMVPN (Dynamic Multipoint Virtual Private Network)

1.4.1 Contexte et émergence du DMVPN

a. Pourquoi le DMVPN a-t-il été développé ?

Le DMVPN (Dynamic Multipoint Virtual Private Network) a été développé par Cisco pour offrir une connectivité dynamique entre les sites en utilisant des protocoles avancés tels que mGRE (Multipoint Generic Routing Encapsulation) et NHRP (Next Hop Resolution Protocol) [4].

b. Les principaux avantages du DMVPN :

Le **Dynamic Multipoint Virtual Private Network (DMVPN)** offre plusieurs avantages, notamment en termes de réduction de la complexité et de scalabilité accrue. Voici un détail approfondi de ces deux avantages [5, 1] :

1. **Réduction de la complexité :** Le principal atout du DMVPN réside dans sa capacité à simplifier la gestion des connexions entre plusieurs sites.
    - **Connexion dynamique :** Le DMVPN repose sur une architecture où les sites se connectent de manière dynamique, c'est-à-dire que les routeurs n'ont pas besoin de configurations statiques pour chaque site distant. Lorsque de nouveaux sites sont ajoutés, le DMVPN permet à ces sites de rejoindre le réseau de manière autonome, sans nécessiter de modifications manuelles des configurations sur les autres sites
    - **Utilisation de mGRE (Multipoint Generic Routing Encapsulation) :** Le DMVPN repose sur le protocole mGRE, qui permet de créer un tunnel générique multipoint. En utilisant mGRE, un seul tunnel est configuré entre le routeur central et chaque site, ce qui réduit le besoin de configurer manuellement un tunnel pour chaque connexion entre tous les sites.
    - **NHRP (Next Hop Resolution Protocol) :** NHRP est utilisé pour résoudre dynamiquement l'adresse IP du prochain saut (next-hop) dans le réseau. Lorsque deux sites veulent com-

muniquer, NHRP facilite la découverte de l'adresse IP du site distant, sans nécessiter de configurations préalables ou de routes statiques.

2. **Scalabilité accrue :** Dans un réseau d'entreprise avec plusieurs sites, la croissance du nombre de sites peut rapidement entraîner une gestion complexe des connexions, des ressources et des coûts. Le DMVPN surmonte ce défi en permettant une topologie flexible et évolutive.

   - **Topologie Hub-and-Spoke par défaut :** Dans la configuration de base du DMVPN, les sites sont connectés au routeur central (hub), mais ne sont pas directement connectés entre eux. Dans cette architecture, le routeur central agit comme point de transit pour les communications entre les sites.
   - **Passage à une topologie Full Mesh :** L'un des avantages importants du DMVPN est qu'il permet une transition facile vers une topologie Full Mesh (maillage complet). Dans ce modèle, chaque site peut communiquer directement avec n'importe quel autre site, sans passer par le hub central. Ce type de communication entre sites permet de réduire la latence et la surcharge du routeur central, car les données circulent directement entre les sites.
   - **Scalabilité horizontale :** Avec le DMVPN, l'ajout de nouveaux sites ne nécessite pas de modifications importantes de la configuration des autres sites. La capacité du DMVPN à évoluer sans perturber l'infrastructure permet une croissance du réseau beaucoup plus fluide.
   - **Réduction de la charge sur le hub :** Dans un modèle Full Mesh, le DMVPN permet aux sites de communiquer directement, ce qui désengorge le hub et optimise l'utilisation de la bande passante.

1.4.2 Architecture du DMVPN

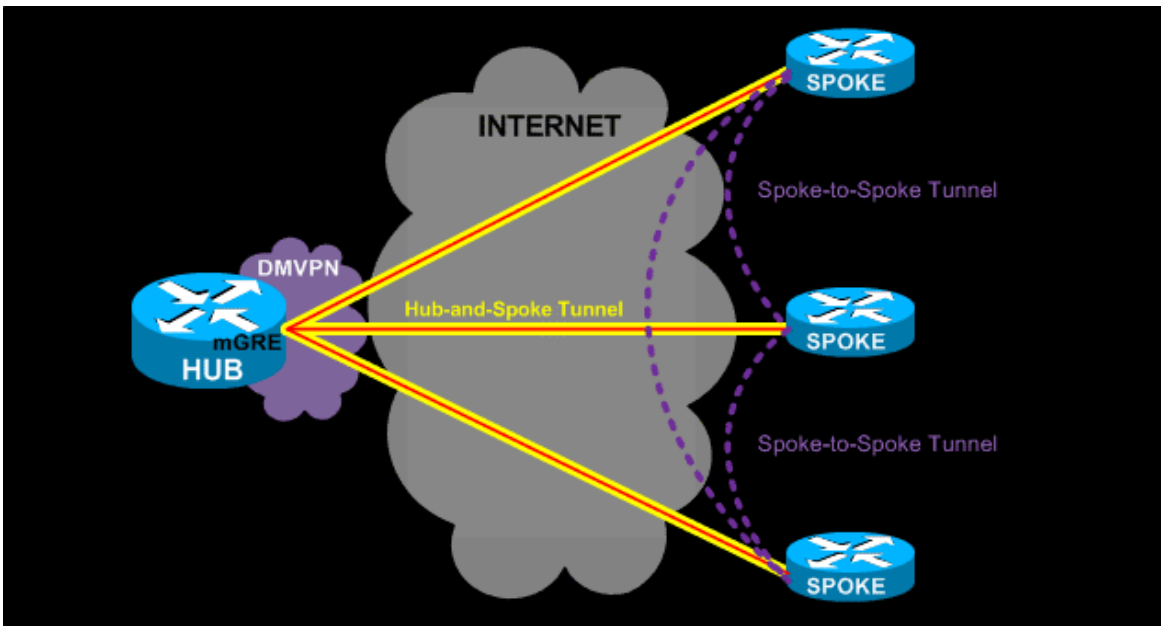


FIGURE 1.1 : Architecture du DMVPN

Caractéristiques principales du DMVPN :

- **Tunnels dynamiques :** Les connexions ne sont établies que lorsqu'elles sont nécessaires, ce qui réduit la consommation de bande passante.
- **Topologie flexible :** Il peut être configuré en mode hub-and-spoke (le hub central gère les connexions entre sites) ou évoluer vers une architecture full mesh où chaque site peut communiquer directement avec les autres.

Architecture du DMVPN :

- **Hub-and-Spoke :**
  → **Hub central** : Le hub est le point de convergence des connexions. Tous les sites (spokes) se connectent initialement au hub pour découvrir d'autres sites.
  → **Spokes :** Les sites (spokes) peuvent établir des connexions directes entre eux après avoir résolu l'adresse IP via le NHRP, réduisant ainsi la dépendance au hub.
- **Full Mesh (évolutif) :** Une fois que les spokes se sont authentifiés via le hub, ils peuvent établir des connexions directes entre eux, améliorant ainsi la latence et la performance pour les communications inter-sites.

1.5 VPNs traditionnels vs DMVPN

Le tableau suivant présente une comparaison détaillée entre les VPN traditionnels et le DMVPN. Ce tableau met en lumière les principales différences en termes de flexibilité, scalabilité, réduction des coûts, sécurité et gestion des connexions. [2, 6].

TABLE 1.1 : Tableau de comparaison détaillée entre les VPN traditionnels et le DMVPN

Critères	VPN Traditionnel	DMVPN
Flexibilité	Rigidité dans la configuration, chaque nouvelle connexion nécessite des ajustements manuels.	Dynamique, permet la création de tunnels automatiques sans reconfigurer les équipements existants.
Scalabilité	Difficulté à étendre le réseau, nécessitant des configurations manuelles pour chaque nouveau site.	Facilité d'ajouter de nouveaux sites sans perturber l'infrastructure existante, utilisant NHRP pour la découverte.
Coûts d'infrastructure	Requiert un matériel spécialisé pour chaque site distant, entraînant des coûts élevés.	Utilise l'infrastructure Internet existante, réduisant les besoins en matériel et les coûts de maintenance.
Maintenance	Nécessite une gestion manuelle de chaque connexion VPN point-à-point.	Réduction significative des interventions humaines grâce à l'automatisation des connexions et à la gestion dynamique via NHRP.

Critères	VPN Traditionnel	DMVPN
Sécurité	Basée sur IPsec, mais avec des connexions statiques qui peuvent exposer certains points d'attaque.	Sécurisé par IPsec avec tunnels dynamiques, réduisant la surface d'attaque et le risque d'intrusion.
Gestion des connexions	Trafic entre sites acheminé à travers un hub central, ce qui peut entraîner une latence accrue.	Permet des connexions directes entre sites, réduisant la latence et optimisant l'utilisation de la bande passante.
Adaptabilité à la croissance	Les modifications et l'ajout de sites exigent des configurations manuelles complexes.	Adaptable et scalable, de nouveaux sites peuvent se connecter automatiquement sans reconfiguration majeure.
Exemple d'application	Une entreprise avec de nombreux bureaux doit configurer manuellement chaque site distant.	Une entreprise en expansion peut ajouter facilement des sites à son réseau, garantissant la continuité des activités sans perturbation.

Conclusion

Ce chapitre a permis de retracer l'évolution des réseaux multisites, en comparant les solutions VPN traditionnelles avec le DMVPN. Nous avons mis en évidence les insuffisances des approches traditionnelles et démontré comment le DMVPN constitue une avancée significative pour améliorer la flexibilité, la sécurité et la performance des réseaux d'entreprise.

Chapitre 2

Conception technique et implémentation

Introduction

Ce chapitre présente la mise en œuvre d'un réseau sécurisé en environnement simulé, en débutant par l'implémentation d'un VPN Site-to-Site basé sur IPsec, puis en évoluant vers un DMVPN (Dynamic Multipoint Virtual Private Network) afin d'évaluer les avantages et limitations de chaque solution. L'étude couvre les prérequis techniques, la configuration des équipements, ainsi que les tests de connectivité et de performances. Une attention particulière sera accordée à la comparaison des deux architectures, en examinant leurs impacts sur la flexibilité, la scalabilité et la gestion du trafic réseau.

Notre démarche consistera à :

- **Implémentation et analyse du VPN Site-to-Site :** Configuration d'un tunnel sécurisé basé sur IPsec entre deux sites.
- **Mise en place et évaluation du DMVPN :** Phase 1, avec une communication centralisée via un hub ; Phase 2, expliquant les tunnels dynamiques sans implémentation ; et Phase 3, optimisant le réseau via NHRP pour des connexions directes et une meilleure performance

Enfin, une évaluation comparative sera menée pour déterminer la solution la plus adaptée à notre architecture et aux besoins d'un réseau scalable et performant.

2.1 Matériels et logiciels utilisés

Pour cette simulation, nous utilisons GNS3 avec les équipements suivants :

- **Routeurs Cisco C7200** (support DMVPN et GRE multipoint)
- **Switches virtuels** pour la connectivité locale
- **PCs** pour les tests
- **Wireshark** pour analyser les flux réseau

2.2 Conception du réseau multisite

L'architecture présentée dans le schéma montre un réseau interconnectant trois sites géographiques : Cotonou, Calavi et Allada, via un fournisseur de services internet (ISP). Chaque site possède un routeur connecté à l'ISP, avec des interfaces locales reliées à des ordinateurs personnels (PC1, PC2, et PC3) sur chaque site respectif. Le routeur Cotonou est le hub central avec une connexion à l'ISP, et les routeurs Calavi et Allada sont les spokes. Les adresses IP attribuées aux différentes interfaces de chaque site sont clairement définies pour assurer une connectivité et une sécurité optimales au sein du réseau.

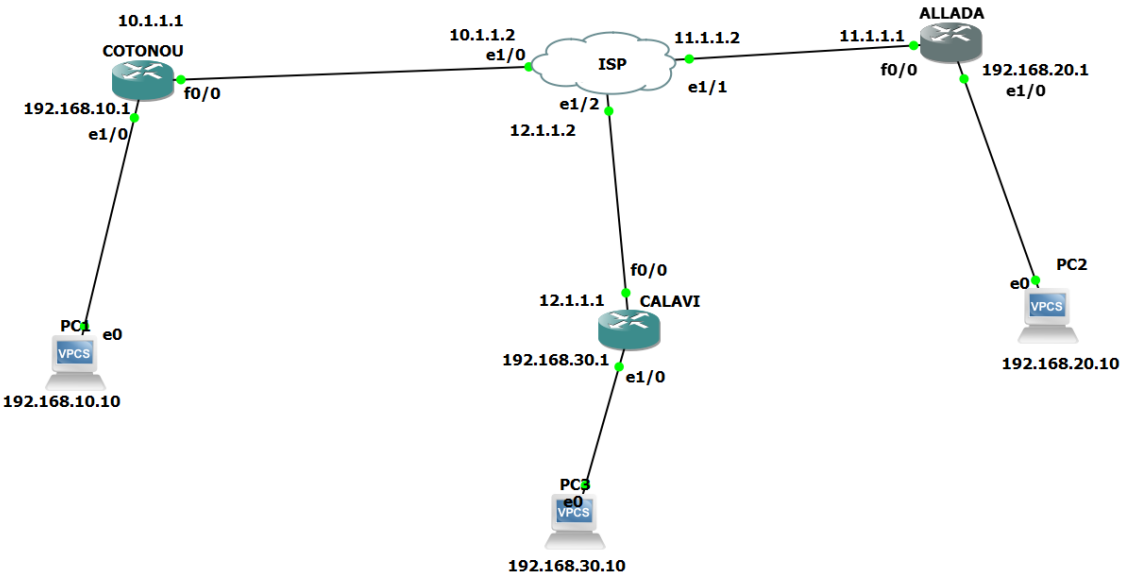


FIGURE 2.1 : Schéma de l'architecture réseau

2.3 Configuration du VPN site-to-site

Dans notre cas ici, nous devons configurer un VPN site-to-site qui pour créer une liaison entre un site situé à COTONOU, un autre à CALAVI et un troisième à ALLADA. Voici la méthodologie que nous avons suivi : **Conception du réseau et configuration IP :**

- Attribuer des adresses IP statiques aux interfaces de chaque routeur
- Utiliser la commande ip address sur les interfaces respectives pour configurer le réseau.

Phase 1 (IKE) :

- Configurer les politiques ISAKMP (Internet Security Association and Key Management Protocol) pour définir les méthodes de chiffrement, de hachage, d'authentification et de groupe Diffie-Hellman.
- Définir une clé pré-partagée pour l'authentification du pair et configurer l'adresse du pair.

Phase 2 (IPSec) :

- Définir le jeu de transformation IPSec avec les algorithmes de chiffrement et de hachage choisis.
- Configurer une liste de contrôle d'accès (ACL) pour définir le trafic qui sera chiffré.
- Appliquer le jeu de transformation IPSec et la carte de cryptage sur les interfaces, afin que le trafic soit chiffré lorsqu'il correspond à l'ACL.

Vérification et tests :

- Vérifier les configurations à l'aide des commandes comme show crypto isakmp sa et show crypto ipsec sa pour s'assurer que les tunnels VPN sont actifs.
- Tester la connectivité entre les sites en utilisant des commandes de ping et wireshark.

Voici le tableau d'adressage que nous utiliserons :

2.3.1 Plan d'adressage

Chaque équipement dispose d'adresses distinctes :

Équipement	Interface	Adresse IP	Masque	Description
COTONOU	FastEthernet0/0	10.1.1.1	255.255.255.252	Lien point-à-point vers ISP
COTONOU	Ethernet1/0	192.168.10.1	255.255.255.0	LAN local connecté à PC1 (Cotonou)
CALAVI	FastEthernet0/0	12.1.1.1	255.255.255.252	Lien point-à-point vers ISP
CALAVI	Ethernet1/0	192.168.30.1	255.255.255.0	LAN local connecté à PC3 (Calavi)
ALLADA	FastEthernet0/0	11.1.1.1	255.255.255.252	Lien point-à-point vers ISP
ALLADA	Ethernet1/0	192.168.20.1	255.255.255.0	LAN local connecté à PC2 (Allada)
ISP	e1/0	10.1.1.2	255.255.255.252	Lien point-à-point vers COTONOU
ISP	e1/1	11.1.1.2	255.255.255.252	Lien point-à-point vers ALLADA
ISP	e1/2	12.1.1.2	255.255.255.252	Lien point-à-point vers CALAVI
PC1 (Cotonou)	e0	192.168.10.10	255.255.255.252	Interface connectée à COTONOU
PC2 (Allada)	e0	192.168.20.10	255.255.255.0	Interface connectée à ALLADA
PC3 (Calavi)	e0	192.168.30.10	255.255.255.0	Interface connectée à CALAVI

TABLE 2.1 : Tableau de configuration de l'adressage.

Ce tableau détaille le plan d'adressage IP du réseau VPN standard, couvrant les interfaces des sites **COTONOU**, **CALAVI**, **ALLADA**, l'**ISP**, ainsi que les postes clients connectés.

Les liens physiques entre l'ISP et chaque site utilisent des sous-réseaux `/30` (masque `255.255.255.252`), optimisés pour les connexions point-à-point, ce qui permet d'économiser les adresses IP tout en assurant une communication directe entre équipements.

Les réseaux locaux (LAN) de chaque site sont segmentés en sous-réseaux `/24`, offrant une plage suffisante d'adresses pour les hôtes et une gestion simple des adresses.

Cette structure d'adressage garantit une segmentation claire du réseau, facilite le routage et optimise l'utilisation des ressources IP dans un contexte VPN classique.

2.3.2 Adressage IP des routeurs

Nous commençons par configurer les adresses IP au niveau de chaque équipement de notre réseau. Les captures montrent la configuration des interfaces réseau des routeurs COTONOU et ALLADA. Les interfaces principales FastEthernet0/0 et Ethernet1/0 sont configurées et actives avec les adresses IP 10.1.1.1 et 192.168.10.1 pour Cotonou, et 11.1.1.1 et 192.168.20.1 pour Allada. Ces configurations montrent que les routeurs sont prêts pour des connexions réseau de base.

```
ALLADA#sh ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            11.1.1.1        YES manual up                    up
Ethernet1/0                192.168.20.1    YES manual up                    up
Ethernet1/1                unassigned      YES unset  administratively down down
Ethernet1/2                unassigned      YES unset  administratively down down
Ethernet1/3                unassigned      YES unset  administratively down down
Ethernet1/4                unassigned      YES unset  administratively down down
Ethernet1/5                unassigned      YES unset  administratively down down
Ethernet1/6                unassigned      YES unset  administratively down down
Ethernet1/7                unassigned      YES unset  administratively down down
ALLADA#
```

FIGURE 2.2 : Informations sur les interfaces du routeur ALLADA

```
COTONOU#sh ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.1.1.1        YES manual up                    up
Ethernet1/0                192.168.10.1    YES manual up                    up
Ethernet1/1                unassigned      YES unset  administratively down down
Ethernet1/2                unassigned      YES unset  administratively down down
Ethernet1/3                unassigned      YES unset  administratively down down
Ethernet1/4                unassigned      YES unset  administratively down down
Ethernet1/5                unassigned      YES unset  administratively down down
Ethernet1/6                unassigned      YES unset  administratively down down
Ethernet1/7                unassigned      YES unset  administratively down down
COTONOU#
```

FIGURE 2.3 : Informations sur les interfaces du routeur COTONOU

2.3.3 Addressage IP de l'ISP

Les captures montrent la configuration des interfaces Ethernet1/0 et Ethernet1/1 sur le routeur ISP. L'interface Ethernet1/1 est configurée avec l'adresse IP 11.1.1.2, et l'interface Ethernet1/0 avec 10.1.1.2, toutes deux avec un masque de sous-réseau 255.255.255.252. Les commandes no shut assurent que les interfaces sont activées et prêtes à fonctionner. Ces interfaces permettront aux communications entre les routeurs et la connexion internet.

```
ISP#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#
ISP(config)#int e1/1
ISP(config-if)#ip add 11.1.1.2 255.255.255.252
ISP(config-if)#int e1/0
ISP(config-if)#ip add 10.1.1.2 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#
```

FIGURE 2.4 : Configuration de l'ISP

2.3.4 Configuration proprement dite du VPN site-to-site

Nous commençons notre configuration par le routeur du site d'ALLADA

```
ALLADA#show crypto isakmp policy

Global IKE policy
Protection suite of priority 2
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
ALLADA#
```

FIGURE 2.5 : Détails de configuration IKE

Cette capture montre la configuration de la politique ISAKMP pour la phase 1 de la connexion VPN. Le protocole de chiffrement utilisé est Triple DES (3DES) avec l'algorithme de hachage Message Digest 5 (MD5) et une clé prépartagée pour l'authentification. Le groupe Diffie-Hellman est configuré avec une clé de 1024 bits, et la durée de vie de la clé est définie sur 86400 secondes (24 heures). La même configuration ISAKMP est appliquée sur CALAVI et COTONOU, car ces deux routeurs partagent les mêmes paramètres de sécurité pour établir un tunnel VPN sécurisé. Ces réglages sont essentiels pour assurer

```
COTONOU#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: cmap, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   current_peer 11.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 201, #pkts encrypt: 201, #pkts digest: 201
    #pkts decaps: 183, #pkts decrypt: 183, #pkts verify: 183
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 11.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x39242559(958670169)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xE1BFD89B(3787446427)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5, flow_id: SW:5, sibling_flags 80000046, crypto map: cmap
        sa timing: remaining key lifetime (k/sec): (4513653/2861)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:
 --More--
```

FIGURE 2.6 : Configuration de la politique ISAKMP : routeur COTONOU

show crypto ipsec sa : Cette commande montre l'état du tunnel IPSec actif entre les sites. On peut observer les informations telles que le nombre de paquets cryptés et décryptés, ainsi que l'adresse IP locale et distante des tunnels. Cela confirme que la configuration IPSec est fonctionnelle et les sessions sont établies avec succès, indiquant que le VPN fonctionne correctement.

```
COTONOU#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
11.1.1.1        10.1.1.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

FIGURE 2.7 : Configuration de la politique ISAKMP : routeur CALAVI

show crypto isakmp sa : Cette sortie montre l'état des SA ISAKMP (Internet Security Association and Key Management Protocol) entre les périphériques. L'état QM_IDLE indique que le processus ISAKMP est dans une phase stable, prête à utiliser les clés pour établir la connexion sécurisée. Le tunnel ISAKMP est bien configuré et opérationnel.

2.3.5 Définition des ACL

```
ALLADA#sh access-lists
Extended IP access list VPN
    10 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 (384 matches)
ALLADA#
```

FIGURE 2.8 : Détails ACL : routeur ALLADA

```
COTONOU#sh access-lists
Extended IP access list VPN
    10 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 (386 matches)
COTONOU#
```

FIGURE 2.9 : Détails ACL : routeur COTONOU

Dans ces captures, nous voyons les résultats de la commande show access-lists sur les routeurs ALLADA et COTONOU. Les deux routeurs utilisent une ACL étendue nommée VPN qui permet le trafic IP entre les réseaux 192.168.10.0/24 et 192.168.20.0/24.

- Sur ALLADA, l'ACL permet le trafic depuis le réseau 192.168.20.0/24 vers 192.168.10.0/24 avec un total de 384 correspondances.
- Sur COTONOU, l'ACL permet le trafic dans l'autre sens, depuis 192.168.10.0/24 vers 192.168.20.0/24, avec 386 correspondances.

Ces ACLs sont utilisées pour définir quel trafic doit être chiffré dans le cadre de la configuration du tunnel VPN IPSec entre les deux sites.

2.4 Configuration du DMVPN

Nous allons configurer un VPN dynamique multipoint (DMVPN) permettant de créer des tunnels sécurisés entre plusieurs sites, où COTONOU est le hub et CALAVI et ALLADA sont les spokes. Nous utiisons le tableau d'addressage précédemment utilisé. Nous y ajoutons les addresses IP des tunnels. Voici le tableau qui récatipule ces informations :

Périphérique	Interface	Adresse IP	Masque
COTONOU	Tunnel0	172.16.0.1	255.255.255.255
CALAVI	Tunnel0	172.16.0.2	255.255.255.255
ALLADA	Tunnel0	172.16.0.3	255.255.255.255

TABLE 2.2 : Tableau de configuration de l'adressage.

Ce tableau présente l'adressage IP dédié aux interfaces tunnel dans le réseau DMVPN. Chaque routeur possède une adresse IP unique configurée avec un masque `/32` (255.255.255.255), correspondant à une adresse spécifique sans plage associée. Cette approche facilite la gestion des tunnels GRE dynamiques en permettant au protocole NHRP de résoudre précisément chaque endpoint, améliorant ainsi la scalabilité et la flexibilité du réseau.

L'utilisation de `/32` sur les interfaces tunnel évite les conflits d'adresses, simplifie le routage, et garantit une communication point-à-point sécurisée et efficace entre les sites distants. Chaque périphérique utilise une interface de tunnel appelée Tunnel0, avec un masque de sous-réseau de 255.255.255.252 pour un adressage point à point.

2.5 Configuration de DMVPN

La configuration d'un réseau DMVPN (Dynamic Multipoint Virtual Private Network) permet de créer des connexions VPN dynamiques et sécurisées entre plusieurs sites distants. Cette solution optimise la flexibilité du réseau en établissant automatiquement des tunnels point-à-point, tout en simplifiant la gestion et en réduisant les coûts liés à l'infrastructure.

2.5.1 Routeur COTONOU

Sur le routeur COTONOU, nous activons le service DMVPN. Cette capture montre la configuration de l'interface Tunnel0 sur le routeur COTONOU . L'adresse IP 172.16.0.1 a été attribuée à l'interface tunnel, avec un masque de sous-réseau 255.255.255.255. Les configurations de NHRP (Next Hop Resolution Protocol) et de l'authentification avec la clé pré-partagée cisco123sont en place. Le mode tunnel GRE multipoint est activé, permettant une communication entre plusieurs sites 10.1.1.1 et la clé 100 pour sécuriser les connexions.

```
COTONOU#sh run
COTONOU#sh running-config int tunnel0
Building configuration...

Current configuration : 300 bytes
!
interface Tunnel0
 ip address 172.16.0.1 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp shortcut
 ip nhrp redirect
 no ip split-horizon eigrp 100
 tunnel source 10.1.1.1
 tunnel mode gre multipoint
 tunnel key 100
end

COTONOU#
```

FIGURE 2.10 : Activation du DMVPN : routeur COTONOU

2.5.2 Routeur CALAVI

L'adresse IP 172.16.0.3 a été attribuée à l'interface tunnel, avec un masque de sous-réseau 255.255.255.5. La configuration NHRP est également présente, avec l'authentification utilisant la clé pré-partagée cisco123, et la résolution dynamique des chemins via les commandes ip nhrp mapet ip nhrp map multicast. La source du tunnel est définie 12.1.1.1, et le mode tunnel GRE multipoint est activé, tout comme la clé de sécurité 100 pour sécuriser les connexions. La configuration de l'interface Tunnel0 sur ALLADA diffère de celle de CALAVI par l'adresse IP utilisée sur l'interface tunnel, qui est 172.16.0.2, et le tunnel source, défini ici sur 11.1.1.1. Le reste des paramètres de configuration, comme l'authentification avec la clé pré-partagée cisco123 et le mode GRE multipoint, sont similaires.

```
CALAVI#sh run
CALAVI#sh running-config int tunnel 0
Building configuration...

Current configuration : 291 bytes
!
interface Tunnel0
 ip address 172.16.0.3 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco123
 ip nhrp map 172.16.0.1 10.1.1.1
 ip nhrp map multicast 10.1.1.1
 ip nhrp network-id 1
 ip nhrp nhs 172.16.0.1
 tunnel source 12.1.1.1
 tunnel mode gre multipoint
 tunnel key 100
end

CALAVI#
```

FIGURE 2.11 : Activation du DMVPN : routeur CALAVI

2.6 Configuration du routage EIGRP

Pour permettre la communication dynamique entre les sites via DMVPN, EIGRP est utilisé. Sur ces captures, nous voyons l'activation d'EIGRP sur les routeurs ALLADA et COTONOU .
ALLADA : La commande **router eigrp 100** est utilisée pour activer EIGRP, suivie de la définition des réseaux **192.168.20.0** et **172.16.0.0** pour la publicité des routes. Un message de mise à jour indique que le voisinage EIGRP avec l'adresse **172.16.0.1** (Cotonou) a été établi avec succès via l'interface Tunnel0.

COTONOU : De même, sur Cotonou , EIGRP est activé, et les réseaux **192.168.10.0** et **172.16.0.1** sont ajoutés à la configuration, ce qui permet de former la relation de voisinage EIGRP avec ALLADA via le tunnel.

```
COTONOU(config-if)#router eigrp 100
COTONOU(config-router)#net 192.168.10.0
COTONOU(config-router)#net 172.16.0.1
COTONOU(config-router)#
```

FIGURE 2.12 : Configuration EIGRP : routeur CALAVI

```
ALLADA(config-if)#router eigrp 100
ALLADA(config-router)#net 192.168.20.0
ALLADA(config-router)#net 172.16.0.0
ALLADA(config-router)#
*Mar 18 02:27:11.119: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 172.16.0.1 (Tunnel0) is up: new adjacency
```

FIGURE 2.13 : Configuration EIGRP : routeur CALAVI

Cette commande a également été saisie sur CALAVI avec le même résultat. Cela confirme que les trois routeurs ont établi une adjacence EIGRP via le tunnel DMVPN, permettant ainsi l'échange dynamique de routes.

2.7 Vérification de la configuration DMVPN

Après la configuration, nous utilisons la commande **show dmvpn** pour vérifier que le tunnel DMVPN est opérationnel.

```
COTONOU#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Hub, NHRP Peers:2,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1         11.1.1.1       172.16.0.2    UP 03:35:00     D
     1         12.1.1.1       172.16.0.3    UP 02:42:42     D

COTONOU#
```

FIGURE 2.14 : Informations sur les tunnnels : routeur COTONOU

```
ALLADA#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1        10.1.1.1      172.16.0.1    UP 03:23:10     S

ALLADA#
```

FIGURE 2.15 : Informations sur les tunnnels : routeur ALLADA

```
CALAVI#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
        NHS Status: E --> Expecting Replies, R --> Responding
        UpDn Time --> Up or Down Time for a Tunnel
==========================================================================

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1        10.1.1.1      172.16.0.1    UP 02:39:02     S

CALAVI#
```

FIGURE 2.16 : Informations sur les tunnnels : routeur CALAVI

Dans cette capture, on peut observer l'état de la session NHRP sur les trois routeurs impliqués dans le DMVPN. Sur CALAVI, l'interface **Tunnel0** est configurée en tant que **spoke**, avec un seul pair (COTONOU), et l'adjacence NHRP est établie avec succès. Sur COTONOU, l'interface Tunnel0 agit en tant que hub, ayant des adjacences NHRP avec CALAVI et ALLADA. Enfin, sur ALLADA, l'interface Tunnel0 est également configurée en tant que spoke, avec COTONOU comme peer. Ces détails confirment que le DMVPN est correctement configuré et opérationnel, avec une communication fluide entre le hub (COTONOU) et les spokes (CALAVI et ALLADA).

2.8 Vérifier les sessions IPSec

Les captures d'écran montrent l'état des sessions ISAKMP sur les routeurs ALLADA et COTONOU, vérifié avec la commande show crypto isakmp sa.

```
ALLADA#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.1.1.1        11.1.1.1        QM_IDLE           1001 ACTIVE
```

FIGURE 2.17 : Etablissement du tunnel ISAKMP : routeur ALLADA

```
COTONOU#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.1.1.1        11.1.1.1        QM_IDLE           1002 ACTIVE
10.1.1.1        12.1.1.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

FIGURE 2.18 : Etablissement du tunnel ISAKMP : routeurCOTONOU

Voici les points principaux observés :

- **ALLADA** : Le tunnel ISAKMP entre les adresses IP locales **10.1.1.1** et distantes **11.1.1.1** est en état **QM_IDLE**, ce qui signifie qu'il est dans une phase stable, prêt à utiliser les clés pour établir une communication sécurisée. Le **conn-id 1001** est actif, indiquant que la session est en fonctionnement.
- **COTONOU** : Deux sessions ISAKMP sont visibles, une entre **10.1.1.1** et **11.1.1.1**, et une autre entre **10.1.1.1** et **12.1.1.1**, toutes deux également en état **QM_IDLE**, ce qui montre qu'elles sont prêtes pour l'échange de clés. Les **conn-id** sont respectivement **1002** et **1001**, et toutes les deux sont actives.

Cela confirme que les tunnels ISAKMP sont correctement établis entre les routeurs, prêts pour l'échange de clés et l'initiation de tunnels sécurisés via DMVPN.

2.9 Vérifier les associations de sécurité IPSec

La capture présente l'état des associations de sécurité IPSec sur le routeur Cotonou, vérifié avec la commande **show crypto ipsec sa**.

```
COTONOU#sh crypto ipsec sa

interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (11.1.1.1/255.255.255.255/47/0)
   current_peer 11.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 205, #pkts encrypt: 205, #pkts digest: 205
    #pkts decaps: 207, #pkts decrypt: 207, #pkts verify: 207
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 11.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0xE1675174(3781644660)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x39699092(963219602)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 3, flow_id: SW:3, sibling_flags 80000046, crypto map: Tunnel0-head-0
        sa timing: remaining key lifetime (k/sec): (4543717/2748)
        IV size: 16 bytes
--More--
```

FIGURE 2.19 : Détails des associations IPSec : routeur COTONOU

Voici les points clés observés :

- Le tunnel est configuré avec l'adresse IP locale **10.1.1.1** et l'adresse distante **11.1.1.1**, correspondant à la configuration du DMVPN entre Cotonou et Allada.
- La sécurité du tunnel est établie avec une clé pré-partagée et utilise le chiffrement **ESP-AES** avec **HMAC-SHA** pour assurer la confidentialité et l'intégrité des paquets.
- Un total de 205 paquets ont été encryptés, avec 207 paquets vérifiés et 205 paquets de hachage traités, ce qui montre un échange constant et sécurisé de données entre les sites.
- Les statistiques de décompression et de compression des paquets montrent qu'aucune compression n'est utilisée, ce qui est courant dans les configurations **IPSec** modernes.
- La session de tunnel reste active avec un **MTU** de 1500 octets, et la durée de vie restante des clés est de 45 437 717 secondes (environ 525 jours).

Cela confirme que le tunnel **IPSec** est fonctionnel, stable et protège efficacement le trafic entre Cotonou et Allada via le DMVPN.

2.10 Activation du routage dynamique

Les captures montrent les tables de routage EIGRP des trois routeurs, Cotonou, Calavi et Allada, après l'établissement de la connectivité DMVPN.

```
COTONOU(config-if)#router eigrp 100
COTONOU(config-router)#net 192.168.10.0
COTONOU(config-router)#net 172.16.0.1
COTONOU(config-router)#
```

FIGURE 2.20 : Activation du routage dynamique : routeur COTONOU

```
ALLADA(config-if)#router eigrp 100
ALLADA(config-router)#net 192.168.20.0
ALLADA(config-router)#net 172.16.0.0
ALLADA(config-router)#
*Mar 18 02:27:11.119: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 172.16.0.1 (Tunnel0) is up: new adjacency
```

FIGURE 2.21 : Activation du routage dynamique : routeur ALLADA

```
CALAVI#show ip route eigrp
D    192.168.10.0/24 [90/26905600] via 172.16.0.1, 00:17:18, Tunnel0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:45:01, Null0
D    192.168.20.0/24 [90/28185600] via 172.16.0.1, 00:16:29, Tunnel0
CALAVI#
```

FIGURE 2.22 : Activation du routage dynamique : routeur CALAVI

Sur **Allada**, nous pouvons voir que :

- Le réseau **192.168.30.0/24** est accessible via le tunnel DMVPN avec Cotonou,
- Le réseau **192.168.10.0/24** est accessible via le même tunnel avec Calavi.
- Le réseau **172.16.0.0/16** est répertorié comme un résumé, ce qui indique une agrégation des réseaux pour une gestion plus efficace.

Sur **Calavi**, les entrées montrent également que :

- Les réseaux **192.168.10.0/24** et **172.16.0.0/16** sont accessibles via le tunnel DMVPN avec Allada et Cotonou,
- La route **172.16.0.0/16** est également indiquée comme un résumé.

Sur **Cotonou**, la table de routage montre que :

- Les réseaux **192.168.30.0/24** et **192.168.20.0/24** sont accessibles via le tunnel DMVPN avec Allada et Calavi,
- L'agrégation de **172.16.0.0/16** est également présente.

Ces informations confirment que les trois sites sont correctement interconnectés via DMVPN, avec des routes EIGRP établies et une propagation des réseaux entre les différents sites.

Avec la configuration de DMVPN en place, nous avons maintenant un réseau sécurisé qui permet la communication entre plusieurs sites via des tunnels dynamiques. L'utilisation d'EIGRP et de NHRP garantit la connectivité dynamique, tandis que l'activation de la phase 3 permet la communication directe entre les sites sans passer par le hub.

Conclusion

Ce chapitre a détaillé l'implémentation et la configuration des solutions VPN site-to-site et DMVPN pour établir des connexions sécurisées entre les sites de Cotonou, Calavi et Allada. Nous avons abordé la configuration des tunnels, la mise en place de l'IPSec pour sécuriser les échanges et l'application du routage dynamique avec EIGRP dans le cadre du DMVPN. Les résultats ont montré que le DMVPN offre une solution plus flexible et évolutive, permettant des connexions directes entre sites sans surcharger le hub. De son côté, le VPN site-to-site reste une solution plus simple, mais devient moins adaptée à mesure que le réseau s'agrandit. Ces configurations ont permis de tester et valider la connectivité, la sécurité et la performance, offrant des bases solides pour des déploiements futurs en entreprise.

Chapitre 3

Résultats et Analyses

Introduction

L'implémentation du VPN site-to-site et du DMVPN ont été réalisée afin de créer une connexion sécurisée et fiable entre les sites de Cotonou, Calavi et Allada. Ce chapitre présente une analyse détaillée des résultats obtenus pour les deux configurations, en mettant l'accent sur plusieurs critères essentiels tels que la connectivité, les performances, la sécurité et la scalabilité du réseau. L'objectif est de mesurer l'efficacité des solutions VPN mises en place, d'identifier les points forts et les éventuelles limitations de chaque approche, et de proposer des recommandations adaptées pour leur déploiement optimal en environnement d'entreprise.

3.1 Vérifications de la connectivité et de la topologie

Afin de valider le bon fonctionnement du VPN site-to-site et du DMVPN, une série de tests a été effectuée pour vérifier la connectivité entre les sites de Cotonou, Calavi et Allada. Ces tests ont permis de confirmer la stabilité et l'efficacité des configurations mises en place.

3.1.1 Site to site VPN

Les pings entre les PC montrent une latence stable entre les sites, avec des temps de réponse allant de 90,178 ms à 92,350 ms pour le trafic de Cotonou (PC1) vers Allada (PC2), et de 90,803 ms à 93,130 ms pour le trafic de Calavi (PC3) vers Cotonou (PC1)

```
PC1> ping  192.168.20.10
84 bytes from 192.168.20.10 icmp_seq=1 ttl=62 time=92.178 ms
84 bytes from 192.168.20.10 icmp_seq=2 ttl=62 time=90.713 ms
84 bytes from 192.168.20.10 icmp_seq=3 ttl=62 time=91.426 ms
84 bytes from 192.168.20.10 icmp_seq=4 ttl=62 time=91.751 ms
84 bytes from 192.168.20.10 icmp_seq=5 ttl=62 time=92.350 ms
```

FIGURE 3.1 : Ping PC1 vers PC2

```
PC2> ping 192.168.10.10
84 bytes from 192.168.10.10 icmp_seq=1 ttl=62 time=90.803 ms
84 bytes from 192.168.10.10 icmp_seq=2 ttl=62 time=92.499 ms
84 bytes from 192.168.10.10 icmp_seq=3 ttl=62 time=93.189 ms
84 bytes from 192.168.10.10 icmp_seq=4 ttl=62 time=92.137 ms
84 bytes from 192.168.10.10 icmp_seq=5 ttl=62 time=93.130 ms
```

FIGURE 3.2 : Ping PC1 vers PC2

3.1.2 DMVPN

Nous utilisons la commande ping pour tester la connectivité entre les différents sites. Ces captures montrent des tests de connectivité via des pings effectués entre les différents sites via le tunnel DMVPN. Le premier PC (Cotonou, 172.16.0.2) pingue le deuxième PC (Calavi, 172.16.0.3), et le troisième PC (Allada, 172.16.0.1) pingue le PC de Cotonou (172.16.0.2). Tous les pings montrent des temps de réponse compris entre 75 ms et 77 ms, ce qui indique une latence stable et faible entre les sites connectés via DMVPN, confirmant que les tunnels sont opérationnels et que la communication entre les sites est fluide. Ces résultats témoignent de l'efficacité et de la performance du tunnel DMVPN configuré entre les sites Cotonou, Calavi et Allada.

```
PC2> ping 172.16.0.1
84 bytes from 172.16.0.1 icmp_seq=1 ttl=254 time=76.897 ms
84 bytes from 172.16.0.1 icmp_seq=2 ttl=254 time=76.426 ms
84 bytes from 172.16.0.1 icmp_seq=3 ttl=254 time=75.889 ms
84 bytes from 172.16.0.1 icmp_seq=4 ttl=254 time=77.208 ms
84 bytes from 172.16.0.1 icmp_seq=5 ttl=254 time=75.343 ms

PC2>
```

FIGURE 3.3 : Ping ALLADA vers COTONOU

```
PC1> ping 172.16.0.3
84 bytes from 172.16.0.3 icmp_seq=1 ttl=254 time=76.717 ms
84 bytes from 172.16.0.3 icmp_seq=2 ttl=254 time=75.894 ms
84 bytes from 172.16.0.3 icmp_seq=3 ttl=254 time=75.914 ms
84 bytes from 172.16.0.3 icmp_seq=4 ttl=254 time=75.129 ms
84 bytes from 172.16.0.3 icmp_seq=5 ttl=254 time=76.528 ms

PC1>
```

FIGURE 3.4 : Ping COTONOU vers ALLADA

```
PC1> ping 172.16.0.2
84 bytes from 172.16.0.2 icmp_seq=1 ttl=254 time=75.437 ms
84 bytes from 172.16.0.2 icmp_seq=2 ttl=254 time=76.918 ms
84 bytes from 172.16.0.2 icmp_seq=3 ttl=254 time=76.612 ms
84 bytes from 172.16.0.2 icmp_seq=4 ttl=254 time=77.050 ms
84 bytes from 172.16.0.2 icmp_seq=5 ttl=254 time=76.534 ms

PC1>
```

FIGURE 3.5 : Ping COTONOU vers CALAVI

La latence mesurée pour le DMVPN est clairement plus avantageuse par rapport au VPN site-to-site. En effet, le DMVPN offre une meilleure performance, particulièrement lorsque les sites doivent

échanger fréquemment des données. Cela illustre bien l'un des avantages majeurs du DMVPN, à savoir la réduction de la dépendance au hub central, ce qui améliore la réactivité du réseau.

3.2 Scalabilité et évolutivité des topologies

L'évolutivité d'un réseau est un critère clé dans le choix de la topologie, surtout lorsqu'il s'agit d'ajouter de nouveaux sites. Les topologies VPN site-to-site et DMVPN offrent chacune des avantages, mais présentent aussi certaines contraintes en termes de scalabilité. En ajoutant un site supplémentaire à notre configuration existante, comme un site à Porto Novo, il faut bien comprendre ces limites pour déterminer la solution la plus appropriée.

3.2.1 Scalabilité du VPN Site-to-Site

La topologie VPN site-to-site repose sur un modèle centralisé, où chaque site distant doit établir un tunnel sécurisé avec le hub. Bien que ce modèle soit simple à configurer pour un petit nombre de sites, il devient rapidement complexe et peu évolutif à mesure que le nombre de sites augmente.

3.2.2 Scalabilité du DMVPN

Le DMVPN est conçu pour être beaucoup plus flexible et scalable par rapport au VPN site-to-site. Dans le DMVPN, les sites (spokes) ne dépendent pas uniquement du hub pour leur communication ; ils peuvent établir des connexions directes entre eux une fois la résolution d'adresse dynamique effectuée par NHRP. Cependant, il y a quelques contraintes à prendre en compte. En ajoutant un site à Porto Novo dans un environnement DMVPN, il n'est pas nécessaire de configurer un tunnel direct vers chaque autre site. Porto Novo peut rejoindre directement les autres sites via le tunnel dynamique multipoint une fois que la résolution d'adresse via NHRP a été effectuée. Cela évite d'ajouter un tunnel dédié à chaque nouvelle connexion.

Le VPN site-to-site est adapté pour de petits réseaux avec un nombre limité de sites, mais il présente des limitations de scalabilité à mesure que le nombre de sites augmente. Chaque nouveau site nécessite un tunnel dédié, ce qui rend la gestion plus complexe et augmente la charge sur le hub central. Le DMVPN offre une solution beaucoup plus scalable et flexible, idéale pour des réseaux en expansion. L'ajout de sites, comme celui de Porto Novo, est plus simple et n'implique pas de surcharge sur le hub. De plus, la capacité des sites à établir des connexions directes entre eux améliore la performance du réseau et réduit la latence. Ainsi, si la croissance du réseau est prévue, le DMVPN constitue une solution plus adaptée pour un déploiement extensible et efficace, en particulier lorsque de nouveaux sites doivent être ajoutés régulièrement.

3.3 Méthodes de chiffrement et de hachage

3.3.1 VPN site-to-site

Cette capture montre le trafic ESP entre l'interface FastEthernet0/0 de Cotonou (10.1.1.1) et l'interface Ethernet1/0 de l'ISP (11.1.1.1). Le protocole ESP est utilisé pour garantir la confidentialité des don-

nées transmises dans un tunnel VPN IPSec. Chaque paquet capturé mesure 166 octets et contient un SPI (Security Parameter Index) unique, qui permet de suivre et de sécuriser les communications au sein du tunnel. La capture montre des transmissions régulières et continues, avec une latence stable entre les deux points.

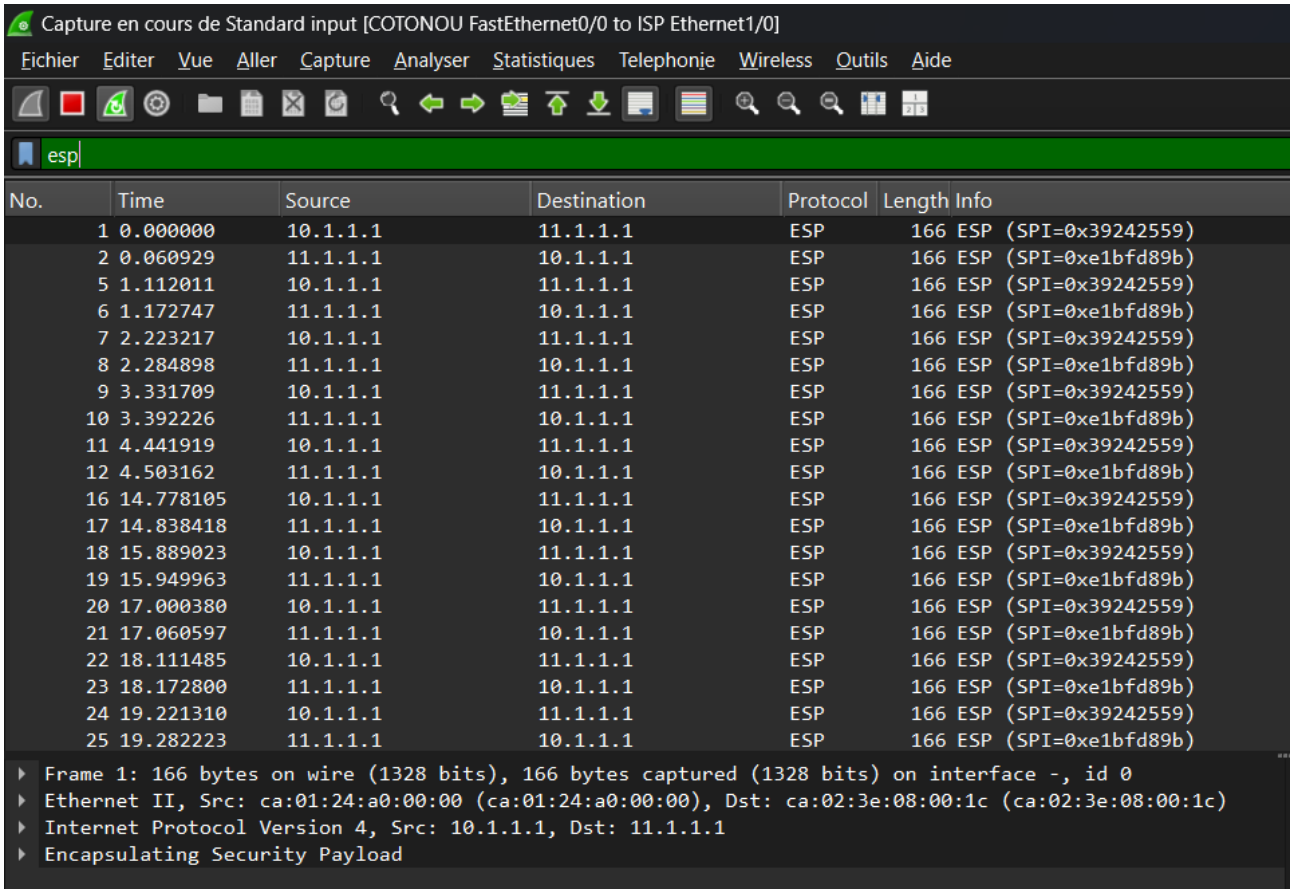


FIGURE 3.6 : Capture wireshark : VPN site-to-site

La configuration du VPN Site-to-Site entre Cotonou, Calavi et Allada a été effectuée avec succès en suivant une méthodologie claire. Nous avons configuré les interfaces réseau avec des adresses IP statiques et utilisé ISAKMP pour établir des politiques de sécurité robustes en phase 1. La phase 2 a vu la configuration du tunnel IPSec avec les algorithmes de chiffrement et de hachage appropriés pour sécuriser les échanges. Les ACLs ont été définies pour chiffrer le trafic pertinent, garantissant ainsi la confidentialité. Les tests de connectivité ont montré des latences stables et une communication efficace entre les sites. Enfin, la surveillance des connexions IPSec a confirmé l'établissement correct des tunnels sécurisés, assurant une solution VPN stable et fiable pour ces trois

3.3.2 DMVPN

La capture montre un trafic ESP (Encapsulating Security Payload) entre le routeur Cotonou et l'ISP via le tunnel DMVPN. Chaque paquet capture un total de 166 octets, transportant des données sécurisées. Le champ SPI (Security Parameter Index) est un identifiant unique pour chaque paquet, utilisé pour suivre les associations de sécurité. On observe différents SPIs associés aux paquets, garantissant une transmission sécurisée et cohérente au fil du temps. L'adresse source est le routeur CALAVI(12.1.1.1), et la destination est COTONOU(10.1.1.1), ce qui confirme la sécurisation des communications via le VPN

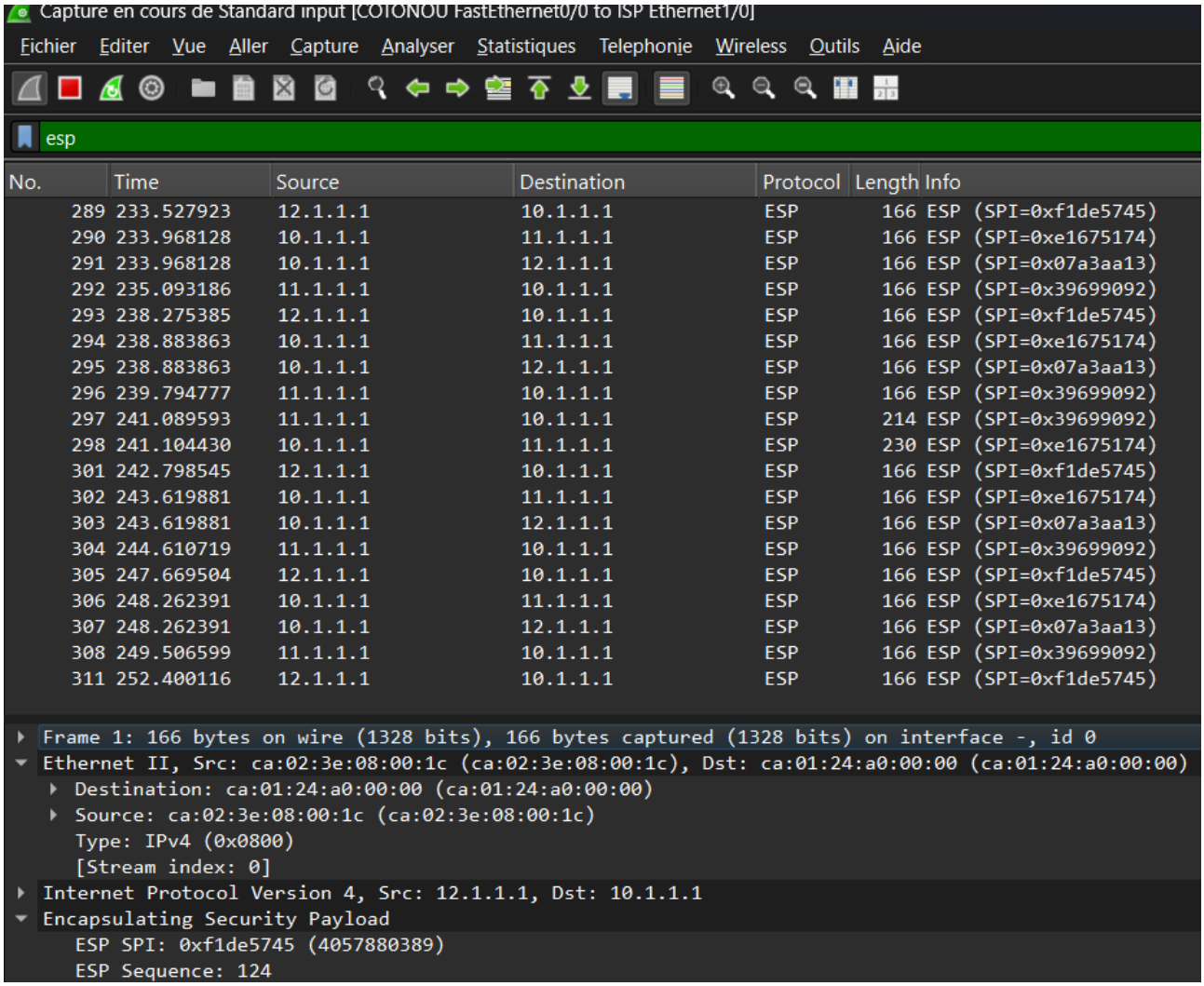


FIGURE 3.7 : Capture wireshark : DMVPN

3.4 Résilience et tolérance aux pannes

Dans notre cas, nous avons deux topologies principales à considérer : le VPN site-to-site et le DMVPN. Les sites impliqués sont Cotonou, Calavi, et Allada, avec Cotonou agissant comme le hub et Calavi et Allada comme les spokes dans les deux configurations. En cas de panne ou de défaillance, la capacité à maintenir la connectivité et la performance du réseau est déterminante.

3.4.1 Résilience et tolérance aux pannes pour le VPN site-to-site

Le VPN site-to-site fonctionne sur une architecture statique où les connexions entre les sites sont établies via des tunnels définis et fixes. Chaque tunnel VPN a un lien direct entre deux sites, avec Cotonou servant de hub central pour les communications entre Calavi et Allada. Toute panne sur le routeur de Cotonou entraînerait une perte de connectivité pour Calavi et Allada. Les sites Calavi et Allada ne peuvent communiquer entre eux que via Cotonou, ce qui en fait un point de défaillance unique. Par exemple, si la liaison entre Cotonou et Calavi ou Allada tombe en raison d'une panne du routeur Cotonou, la communication entre tous les sites sera interrompue.

3.4.2 Résilience et tolérance aux pannes pour le DMVPN

Le DMVPN, en revanche, utilise un modèle de routage dynamique qui permet de réagir automatiquement aux pannes et de reconfigurer les tunnels en cas de défaillance des équipements ou des liens. Avec Cotonou comme hub et Calavi et Allada comme spokes, le DMVPN offre une solution plus souple pour maintenir la connectivité après une panne. En cas de panne sur Cotonou ou une défaillance de lien, le DMVPN utilise EIGRP pour recalculer les routes dynamiques et établir des chemins alternatifs entre Calavi et Allada sans passer par Cotonou. Par exemple, si Cotonou tombe en panne, Calavi et Allada pourront se connecter directement sans que Cotonou soit impliqué. Cela permet de maintenir les échanges entre les sites, même en l'absence du hub.

3.5 Coût opérationnel

Le coût opérationnel évalue l'efficacité des coûts d'administration du réseau. Dans notre cas, nous avons comparé VPN Site-to-Site et DMVPN en termes de gestion, maintenance et évolutivité.

3.5.1 VPN Site-to-Site

Chaque site nécessite une configuration manuelle pour établir des tunnels. Par exemple, l'ajout de Porto Novo implique de configurer le tunnel entre Cotonou et Porto Novo, ainsi que des mises à jour sur tous les autres routeurs. Chaque modification (ajout de site, changement d'IP) nécessite de mettre à jour manuellement chaque tunnel, ce qui augmente les coûts d'administration au fur et à mesure que le réseau grandit.

3.5.2 DMVPN

L'ajout de Porto Novo se fait en configurant simplement le tunnel sur ce site. Le routage dynamique via EIGRP et NHRP gère automatiquement les connexions entre les sites sans intervention manuelle sur les autres équipements. Les pannes et les ajouts de sites sont gérés dynamiquement, réduisant le temps et les coûts d'administration. DMVPN offre un coût opérationnel inférieur à long terme. Il simplifie la gestion et les mises à jour grâce à son modèle dynamique. À l'inverse, VPN Site-to-Site devient de plus en plus coûteux à mesure que le réseau s'étend.

3.6 Perspectives d'évolution du DMVPN : Ajout d'un Hub secondaire

Bien que l'architecture **Dynamic Multipoint VPN (DMVPN)** actuelle offre une grande flexibilité et résilience, l'ajout d'un hub secondaire peut encore améliorer la résilience et la tolérance aux pannes, en apportant une solution de redondance pour assurer une disponibilité continue du réseau, même en cas de défaillance du hub primaire. Actuellement, si Cotonou, le hub primaire, tombe en panne, les sites Calavi et Allada doivent dépendre d'un mécanisme de reconfiguration dynamique pour se connecter directement. Toutefois, l'ajout d'un hub secondaire permettrait une réduction des risques associés à une panne du hub primaire, en assurant une continuité du service sans nécessiter de reconfiguration[1, 2].

Conclusion

L'implémentation des solutions VPN site-to-site et DMVPN pour les sites de Cotonou, Calavi et Allada a permis d'évaluer leur efficacité sur plusieurs critères. Le DMVPN s'est montré supérieur en termes de performances, scalabilité, résilience et coût opérationnel. Il offre une latence plus faible, une gestion simplifiée lors de l'ajout de nouveaux sites comme Porto Novo, et une résilience accrue grâce à son modèle de routage dynamique permettant de contourner les pannes du hub principal. En comparaison, le VPN site-to-site, bien que simple à configurer, devient rapidement limité et coûteux à mesure que le réseau se développe, notamment en raison de sa gestion manuelle des tunnels et de son point de défaillance unique. Le DMVPN représente donc une solution plus robuste et adaptée aux réseaux en croissance, offrant une connectivité flexible et une gestion optimisée sur le long terme.

Discussion

Le DMVPN améliore la flexibilité et la scalabilité des réseaux multisites grâce à des tunnels dynamiques et une résolution d'adresses automatisée. Il réduit la charge sur le hub en permettant des communications directes entre sites, diminuant ainsi la latence. Cependant, cette architecture demande une expertise technique renforcée, notamment pour la gestion du routage dynamique et la sécurisation des tunnels IPsec. La mise en place de hubs secondaires et l'intégration de SD-WAN peuvent renforcer la résilience et la gestion globale. Le DMVPN est une solution performante et évolutive, idéale pour des réseaux complexes, à condition d'être correctement planifiée et sécurisée.

Conclusion générale et perspectives

L'implémentation des solutions VPN site-to-site et DMVPN pour les sites de Cotonou, Calavi et Allada a permis d'évaluer leur efficacité sur plusieurs critères. Le DMVPN s'est montré supérieur en termes de performances, scalabilité, résilience et coût opérationnel. Il offre une latence plus faible, une gestion simplifiée lors de l'ajout de nouveaux sites comme Porto Novo, et une résilience accrue grâce à son modèle de routage dynamique permettant de contourner les pannes du hub principal. En comparaison, le VPN site-to-site, bien que simple à configurer, devient rapidement limité et coûteux à mesure que le réseau se développe, notamment en raison de sa gestion manuelle des tunnels et de son point de défaillance unique. Le DMVPN représente donc une solution plus robuste et adaptée aux réseaux en croissance, offrant une connectivité flexible et une gestion optimisée. Sur le long terme, nous explorerons :

- **l'élargissement géographique :** exploiter la flexibilité du DMVPN pour intégrer rapidement d'autres sites, comme Porto-Novo ou des régions plus éloignées, tout en minimisant les ajustements matériels et logiciels.
- **l'optimisation des performances réseau :** ajouter des outils de surveillance réseau (comme NetFlow ou Wireshark) pour analyser en continu la latence et les performances. Identifiez les goulots d'étranglement pour encore améliorer la fluidité.
- **le plan de résilience améliorée :** élaborer un plan de reprise après sinistre basé sur les capacités dynamiques du routage DMVPN. Simulez des scénarios de panne pour tester et renforcer la stabilité du réseau.
- **la sécurité renforcée :** intégrer des politiques de sécurité robustes comme le cryptage IPSec et l'authentification multi-facteurs (MFA) pour tous les points de connexion du DMVPN, afin de protéger le réseau contre les menaces grandissantes.
- **l'innovation et exploration technologique :** explorer des technologies complémentaires comme SD-WAN (Software-Defined Wide Area Network), qui pourrait encore améliorer l'agilité et la gestion des connexions pour un réseau encore plus sophistiqué.

Bibliographie

[4] "CISCO Firewall X". In : (2025). Consulté le 18 décembre 2024. URL : https://www.firewall.cx/cisco/cisco-routers/cisco-router-dmvpn-configuration.html.

[5] Chamandeep Kaur DR YOGESH KUMAR SHARMA. "The Vital Role of Virtual Private Network in Making Secure Connection Over Internet World". In : *International Journal of Recent Technology and Engineering* (2020). Consulté le 19 novembre 2024.

[6] Zeus KERRAVALA. "The Evolution of Virtual Private Network". In : *Enterprise Computing Networking* (2024). Consulté le 08 décembre 2024.

Webographie

[1] The Visual AGE. *Guide DMVPN phases*. Consulté le 20 janvier 2025. 2015. URL : https://network-insight.net/2015/02/03/design-guide-dmvpn-phases.

[2] PALO ALTO. *Fonctionnement de DMVPN*. Consulté le 06 janvier 2025. 2024. URL : https://www.paloaltonetworks.com/cyberpedia/how-does-a-vpn-work.

[3] PALO ALTO. *Histoire du DMVPN*. Consulté le 10 janvier 2025. URL : https://www.paloaltonetworks.com/cyberpedia/history-of-vpn.

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

. iv

Abstract v

. v

Liste des figures vi

Liste des tableaux vii

Liste des acronymes viii

Introduction 1

1 Revue de littérature 4

Introduction 4

1.1 Les réseaux privés virtuels (VPN) 4

1.1.1 Introduction aux réseaux privés virtuels (VPNs) 4

1.2 Types de VPN 5

1.3 Fonctionnement d'un VPN 5

1.3.1 Configuration initiale 6

1.3.1.1 Infrastructure et composants 6

1.3.1.2 Configuration et politiques de sécurité 6

1.3.2 Phase d'initiation 6

1.3.2.1 Authentification des utilisateurs 6

1.3.2.2 Établissement de la connexion sécurisée 6

1.3.3 Création du tunnel VPN 6

1.3.3.1 Sélection du protocole de tunneling 7

1.3.3.2 Échange de clés et chiffrement 7

1.3.4 Transmission des données 7

1.3.4.1 Attribution d'adresses IP et intégration réseau 7

1.3.4.2 Optimisation des performances 7

1.3.4.3 Routage et intégrité des paquets 7

1.3.5 Routage et accès aux ressources 8

1.3.6 Gestion continue de la connexion 8

1.3.7 Fermeture de la connexion . . . 8
1.3.8 Limites des VPN traditionnels pour les entreprises multisites [3]. . . . 8
1.4 Présentation du DMVPN (Dynamic Multipoint Virtual Private Network) . . . 9
1.4.1 Contexte et émergence du DMVPN . . . 9
1.4.2 Architecture du DMVPN . . . 10
1.5 VPNs traditionnels vs DMVPN . . . 11
Conclusion . . . 12

2 Conception technique et implémentation **13**
Introduction . . . 13
2.1 Matériels et logiciels utilisés . . . 13
2.2 Conception du réseau multisite . . . 14
2.3 Configuration du VPN site-to-site . . . 14
2.3.1 Plan d'adressage . . . 15
2.3.2 Adressage IP des routeurs . . . 16
2.3.3 Addressage IP de l'ISP . . . 16
2.3.4 Configuration proprement dite du VPN site-to-site . . . 17
2.3.5 Définition des ACL . . . 19
2.4 Configuration du DMVPN . . . 20
2.5 Configuration de DMVPN . . . 20
2.5.1 Routeur COTONOU . . . 20
2.5.2 Routeur CALAVI . . . 21
2.6 Configuration du routage EIGRP . . . 22
2.7 Vérification de la configuration DMVPN . . . 23
2.8 Vérifier les sessions IPSec . . . 25
2.9 Vérifier les associations de sécurité IPSec . . . 25
2.10 Activation du routage dynamique . . . 26

3 Résultats et Analyses **29**
Introduction . . . 29
3.1 Vérifications de la connectivité et de la topologie . . . 29
3.1.1 Site to site VPN . . . 29
3.1.2 DMVPN . . . 30
3.2 Scalabilité et évolutivité des topologies . . . 31
3.2.1 Scalabilité du VPN Site-to-Site . . . 31
3.2.2 Scalabilité du DMVPN . . . 31
3.3 Méthodes de chiffrement et de hachage . . . 31
3.3.1 VPN site-to-site . . . 31
3.3.2 DMVPN . . . 32
3.4 Résilience et tolérance aux pannes . . . 33
3.4.1 Résilience et tolérance aux pannes pour le VPN site-to-site . . . 33
3.4.2 Résilience et tolérance aux pannes pour le DMVPN . . . 34
3.5 Coût opérationnel . . . 34
3.5.1 VPN Site-to-Site . . . 34
3.5.2 DMVPN . . . 34

3.6 Perspectives d'évolution du DMVPN : Ajout d'un Hub secondaire 34
Conclusion 34

Conclusion **36**

Bibliographie **37**

Webographie **38**

Table des matières **39**