République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER PROFESSIONNEL

En

Informatique

Option

Administration et sécurité des réseaux

Thème

Mise en place d'une politique de sécurité approfondie d'un VPN à multi-sites. Cas d'étude : entreprise SONELGAZ.

Présenté par : M^{lle}.**KASMI Yousra**
M^{lle}.**MAY Tiziri**

Devant le jury composé de :

Président	**ATMANI Mouloud**	**Maître de Conf. A**	**U. A/Mira Béjaia.**
Examinateur	**MOKETEFI Mohand**	**Maître de Conf. B**	**U. A/Mira Béjaia.**
Examinatrice	**BOUKERRAM Samira**	**Maître Assist. A**	**U. A/Mira Béjaia.**
Encadreur	**Karima ADEL**	**Professeur**	**U. A/Mira Béjaia.**

Promotion 2022/2023.

⁂ Remerciements ⁂

Avant d'entamer ce projet de fin d'étude, nous tenons à rendre grâce à Dieu de nous avoir donné le courage et la volonté pour la réalisation de ce travail, nous tenons à exprimer notre sincère gratitude envers tous ceux qui nous aidés ou ont participé au bon déroulement de ce projet.

nous sommes particulièrement reconnaissants à : encadrice professeur ADEL, d'avoir accepté de diriger notre travail qui nous a beaucoup aider, nous la remercie pour sa qualité humaine et professionnelle, pour sa patience, sa directive, ses remarques constructives et son aide inestimables.

Les membres du jury, d'avoir accepté d'examiner ce travail malgré leurs occupations Nous tenons a remercier notre maitre de stage M. IDRI Bachir pour son sérieux et ses conseils,ainsi qu'à toute l'équipe du service Informatique de l'entreprise SONELGAZ.

Nos sincères remerciements pour nos parents pour leurs soutiens, leurs encouragements et leurs sacrifices.

Nous remercions également tout le corps professionnel du département d'Informatique de l'université Abderahmane MIRA de Bejaia.

Enfin, nous tenons a remercier tous ceux qui ont contribué de prés ou de loin pour l'élaboration de ce travail.

⁕ $\mathcal{D}$*édicaces* ⁕

C'est avec profonde gratitude et sincères mots, que je dédie ce modeste travail de fin d'étude avec grand amour

A mes chers parents Redouane et Nouara qui ont sacrifié leur vie pour notre réussite et nous ont éclairé le chemin par leur conseils judicieux.

j'éspere q'un jour ,je pourrais vous rendre un peu de ce que vous avez fait pour moi,que dieux vous prete du bonheur et longue vie.

Amon chère mari Kamel et mon précieux offre du dieu pour toute la patience et le soutient dont il a fait preuve pendant toute au long de ce travail. Merci à toi pour ta confiance ,ton aide et ta présence .

A mes chères beaux parents Ammar et Saida

A mes chèr frères Salah et Nabil et leurs femmes Bouchra et Laure pour touts les encouragements qui m'ont donné.

A ma chère grande soeur Naima et son mari Abid

A Fatima ma petite soeur .

A mes nieces Djana et Yousra

A toutes mes beaux frère (Rabah,Boubker ,Sadi) et mes belles soeurs (Nacira,Rbiha,koka,Samia et Ghozlan) et leurs enfants.

A Yousra chère amie avant d'etre binome

A mes coupines (Sara ,Yasmine ,Nesrine ,Ahlem ,Lamia)

$\mathcal{M}$.***Tiziri***

⁕ *Dédicaces* ⁕

C'est avec profonde gratitude et sincères mots, que je dédie ce modeste travail de fin d'étude avec grand amour

À mes chèrs parents Djamal et Karima, je tiens à vous exprimer ma reconnaissance infinie pour votre soutien inconditionnel tout au long de ma vie et pour votre présence constante à mes cotés, votre amour votre encouragement et vos précieux conseils ont été les piliers de ma réussite et de ma persévérance. votre confiance en moi, votre patience et votre motivation ont été des sources d'inspiration sans fin.

À mon chèr mari Sofiane je suis fier d'appeler un homme aussi exceptionnel que toi tes encouragements constant, ton soutien indéfectible et ta confiance en mes capacités ont été des sources d'inspirations inépuisables.Tu as été mon plus grand motivateur.

À mes chères beaux parents Abed nour et Akila.

À mon chèr frère Baderdinne et a tout mes beaux frères (Badredinne, Salim, Mohemmad,Abed Rehman).

A mes chères soeur Badra et Sonia et son mari Kousseilla.

A mes chères belles soeur (Manel, Chaima, Salsabil, Sydra, Ilham).

A Tiziri chère ami avant d'etre binome.

A mes copines (Sara, Amel, Chahinaz).

ℳ. ***Yousra***

TABLE DES MATIÈRES

Table des Matières **i**

Liste des tableaux **iv**

Liste des figures **v**

Liste des acronymes **viii**

Liste des acronymes **viii**

Introduction générale **1**

1 Présentation du cadre d'étude et de stage **3**

1.1 Présentation générale de SONELGAZ 3

1.1.1 Création et évolution 4

1.1.2 Situation géographique de SONELGAZ 4

1.1.3 Organigramme de l'entreprise 5

1.1.4 Activités et les objectifs de SONELGAZ 5

1.2 Présentation du service d'accueil (Département informatique) 6

1.2.1 Activités de DGSI 6

1.2.2 Présentation du réseau informatique de sonelgaz 7

1.2.3 L'architecture de l'entreprise 7

1.2.4 Présentation de l'environnement matériels et logiciels du réseau informatique . . . 8

1.2.5 Politique de sécurité du réseau en place 9

1.3 Problématique 9

1.4 Solution proposée 9

1.5 conclusion 10

2 Généralitées sur les réseaux et la sécurité informatique **11**

2.1 Réseau informatique 11

2.1.1 Définition 11

2.1.2 Classification des réseaux 11
2.1.3 Les équipements d'interconnexion 16
2.1.4 Les équipements matériels 16
2.1.5 Les connecteurs réseaux 16
2.1.6 Les normes de communications 17
2.1.7 Adressage IP 18
2.2 Sécurité informatique 19
2.2.1 Définition 19
2.2.2 Terminologies de la sécurité informatique 19
2.2.3 Objective de la sécurité informatique 19
2.2.4 Politique de sécurité informatique 19
2.2.5 Les attaques informatiques 20
2.2.6 Mécanismes de sécurité 21
2.3 Conclusion 21

3 Les réseaux privées virtuels 22
3.1 Les lignes spécialisées 22
3.2 Définition 22
3.3 L'intérêt du VPN 23
3.4 Protocoles des VPN 23
3.4.1 Niveau 2 23
3.4.2 Niveau 2.5 24
3.4.3 Niveau 3 et plus 24
3.5 Les modes d'IPsec 26
3.5.1 Mode transparent 26
3.5.2 Mode tunnel 26
3.6 Topologies des VPNs 26
3.6.1 VPN d'entreprise 27
3.6.2 VPN opérateur ou VPN extranet 27
3.7 Conclusion 28

4 L'implémentation des solutions 29
4.1 Architecture proposée 29
4.2 Présentation des outils de travail 29
4.2.1 Partie software 29
4.2.2 Partie hardware 31
4.3 Partie configuration 31
4.3.1 Présentation des quatres sites 31
4.3.2 Création des tunnels IPsec 43
4.3.3 Création de tunnel GRE 48
4.3.4 Création de tunnel SSL 49
4.3.5 Configuration de l'Active Directory(AD) 50
4.3.6 53

4.3.7 Tableau d'adressage des vlans et le routage inter-VLANs 53
4.3.8 Création d'un client VPN 53
4.4 Création d'un tunnel VPN IPsec "Client to site" 53
4.5 Configuration VPN à travers l'application FortiClient 54
4.6 Partie test 55
4.6.1 Les tests de site de bejaia 55
4.6.2 Les tests de site d'Alger 56
4.6.3 Les Tests de site de Sétif. 57
4.7 Conclusion 57

Conclusion générale et perspectives **58**

Bibliographie **59**

LISTE DES TABLEAUX

1.1 Les équipements de raccordement du réseau infonrmatique SONELGAZ. 8
1.2 Les équipements terminaux de SONELGAZ. 9

4.1 Tableau d'adressage HSRP du routeur R2. 38
4.2 Tableau d'adressage HSRP du routeur R1. 38
4.3 Tableau d'adressage des VLANs et le routage inter-VLANs. 53

TABLE DES FIGURES

1.1 Logo de SONELGAZ. 3
1.2 Situation géographique de SONELGAZ 5
1.3 L'organigramme de SONELGAZ 6
1.4 L'architecture de l'entreprise SONELGAZ de BEJAIA. 8

2.1 Réseau LAN 12
2.2 Réseau MAN 12
2.3 Réseau WAN 13
2.4 Topologie en bus 13
2.5 Topologie en étoile 14
2.6 Topologie en anneau 14
2.7 Topologie en arbre 15
2.8 Topologie maillée 15
2.9 Les différents types de capables. 17
2.10 Comparaison des modèles OSI et TCP/IP 18
2.11 Classifications des attaques 20

3.1 Exemple d'utilisation d'un VPN 23
3.2 Exemple d'emploi IPsec entre sites distants 24
3.3 Détails des champs de l'en-tête AH 24
3.4 Détails des champs de l'en-tête ESP 25
3.5 Entête GRE 25
3.6 Les modes d'IPsec 26

4.1 L'architecture proposée pour l'entreprise SONELGAZ. 30
4.2 Configuration du firewal de Bejaia 32
4.3 Interface d'authentification 32
4.4 Configuration du port 1 de firewal de Bejaia 32
4.5 Création de l'interface inter-VLAN. 33
4.6 Création du VLAN 10 (DGI) de Bejaia 33

4.7 Création d'une zone. 34
4.8 Création de la route statique de Bejaia vers l'Internet. 34
4.9 Autorisation du fortigate de bejaia de se connecter à l'internet. 35
4.10 Configuration du firewal du Alger 35
4.11 Configuration du port 1 du firewal d'Alger 36
4.12 Configuration du port 2 du firewal d'Alger 36
4.13 Configuration du port 3 du firewal d'Alger 36
4.14 Création de la route statique de Alger vers l'Internet. 37
4.16 Configuration du routeur R2 du Alger 38
4.17 Création du NAT et autorisation des VLANs à se connecter. 38
4.18 Les interface d'entrès et l'interface de sortie 39
4.19 Configuration du routeur1 39
4.20 Configuration du protocole DHCP 40
4.21 Configuration des VLANs du site d'Alger 40
4.22 Configuration de mode trunk. 40
4.23 Le protocole CDP entre les deux switchs. 41
4.25 Configuration du routeur de sétif. 41
4.26 Configuration du firewal de Constantine 42
4.27 Configuration du port 1 de firewal de Constantine. 42
4.28 Configuration du port 2 de firewal de Constantine 42
4.29 Création de la route statique de Constantine vers l'Internet. 43
4.30 Autorisation du fortigate de constantine de se connecter à l'internet. 43
4.33 Résultat de la création de tunnel entre Bejaia et Alger. 44
4.34 Le cryptage de la clé de tunnel Bejaia-Alger. 45
4.35 La modification de la phase 1 de tunnel Bejaia-Alger. 45
4.36 Création de tunnel ALGER-BEJAIA. 46
4.37 Première étape de la création de tunnel Constantine-Alger. 46
4.38 Configuration de tunnel Constantine-Alger. 46
4.39 Attribution de l'addresse à distance. 47
4.40 Création de la première route statique de tunnel Constantine-Alger. 47
4.41 Création de la deuxième route statique de tunnel Constantine-Alger. 47
4.42 Création d'une policie entrante de tunnel Constantine-Alger. 48
4.43 Création d'une policie sortante de tunnel Constantine-Alger. 48
4.44 Création de tunnel Alger-Constantine. 49
4.45 Configuration de tunnel Sétif-Bejaia. 49
4.46 Configuration de tunnel Bejaia-Sétif 50
4.47 Création de tunnel SSL 50
4.48 Configuration de tunnel Sétif-Bejaia. 50
4.49 Création d'une policy SSL. 50
4.50 Création d'une connexion VPN SSL. 51
4.51 Configuration du serveur local 51
4.52 L'ajout du role AD DS. 51

4.53 L'ajout d'une nouvelle foret 52
4.54 Option de controleur de domaine. 52
4.55 Ouverture de la session Administration. 52
4.57 Création et sécurisation de tunnel IPsec Client to site 54
4.59 Attribution des addreses au tunnel. 54
4.60 Configuration VPN. 54
4.61 Connexion des clients. 55
4.62 Connexion des clients. 55
4.63 La capture de protocole ESP sur Wireshark. 56
4.64 Ping entre CLIENT-VPN et Bejaia 56
4.65 Ping entre Alger et Bejaia. 56
4.66 Test DHCP. 56
4.67 Test entre le site Sétif et INTER-VLAN BEJAIA. 57

LISTE DES ACRONYMES

A	ADSL	Asymmetric Digital Subscriber Line.
	AD	Active Directory
	AH	Authentification Header.
C	CIDR	Classless Inter-Domain Routing.
	CISCO	Computer Information System Company
D	DGRH	Direction Gestion des Ressources Humaines.
	DGSI	Division Gestion Systèmes Informatiques.
	DMZ	Zemilitarized Zone.
	DT-G-E	Division Technique du GAZ et Eléctricité.
E	ESP	Encapsuling security Payload.
F	FTP	File Transfer Protocol.
G	GNS3	Graphical Network Simulator-3.
	GRTE	Société Algérienne de Gestion du Réseau de Transport de l'Electricité
	GRTG	Societé Algérienne de Gestion du Réseau de Transport de Gaz.
	GRE	Generic Routing Encapsulation.
H	HSRP	Hot Standby Router Protocol.
I	IP	Internet Protocol.
	IOS	Internetwork Operating System.
	IPSec	Internet Protocol Security
L	LAN	Local Area Network.
	L2F	Layer 2 Forwarding.
	L2TP	Layer 2 Tunnelin Protocol.
M	MAN	Métropolitain Area Network.
	MPLS	Multi Protocole Label Switching.
O	OS	opérateur Système électrique.
	OSI	Open Systems Interconnection.
P	PAN	Personal Area Network.
	PC	Personal Computer.
	PPTP	Point to Point Tunneling Protocol.
Q	QOS	Quality of service .

R	RJ45	Registered Jack 45 .
S	SDA	.Société Algérienne de Distribution de l'Electricité et du gaz d'Alger
	SDC	Société Algérienne de Distribution de l'Electricité et du gaz du centre.
	SDE	Société Algérienne de Distribution de l'Electricité et du gaz de l'Est.
	SDO	Société Algérienne de Distribution d'électricité et du gaz de l'Ouest.
	SFP	Small Form-Factor Pluggable.
	SONELGAZ	Societe Nationale de l'Electricité et du Gaz.
	SPE	Société Algérienne de Production de l'Electricité.
	SSH	Secure Shell.
	SSL	.Secure Sockets Laye
T	TCP/IP	Transmission Control Protocol/Internet Protocol.
	TLS	Transport Layer Security.
U	UDP	User Datagram Protocol.
	USB	Universal Serial Bus.
V	VPN	Virtual Private Network.
	VLAN	Virtual Local Area Network.
	VLSM	Variable Length Subnet Masking.
	VMWARE	Virtual Machine""Ware".
W	WAN	Wide Area Network.

INTRODUCTION GÉNÉRALE

Les systèmes d'informations ainsi que les réseaux informatiques sont devenus beaucoup plus importants dans le quotidien des établissementsents et entreprise. L'évolution thechnologique a amené ses bénéfices mais a également ses dangers. En effet, aujourd'hui que nous soyons une personne tierce ou une entreprise, nous disponsons tous d'informations confidentielles sur des appareils ou des réseaux. L'échange d'information, via ce grand réseau (Internet) peut créer un risque de modification ou de vol par des personnes malveillantes dans le but de s'enrichir illégalement. Dont il peut provoquer un mauvais impact sur plusieurs niveaux d'une entreprise.

Parfois les entreprises est située sur plusieurs sites géographiques. Par conséquence, l'interception ou l'altération des données sensibles qui transitent sur internet à destination de ses filiales représentent des risques non negligeables. Par ailleurs les nouvelles tendances de nomadisme et de l'informatique permettent non seulement, aux utilisateurs d'avoir accèes aux ressources. Mais, aussi de transporter une partie du système d'information en dehors de l'infrastructure sécurisée de l'entreprise. D'où la nécessité de mettre en place des démarches et des mesures pour évaluer les risques et définir les obejectifs de sécuritée à atteindre.

Par palliers à ce problème de sécurité et d'interconnexion, il est primodial d'implémenter des mécanismes et des solutions sûres assurant la confidentialité et la sécurité du transfert entre deux ou plusieurs entités d'un réseau public.

Pour faire face à ces problématiques de sécurité et d'interconnexion, il est primordial de mettre en œuvre des mécanismes et des solutions fiables garantissant la confidentialité et la sécurité des transferts entre deux ou plusieurs entités au sein d'un réseau public.

Notre objectif dans ce projet est de mettre en place une solution de sécurité qui assure l'interconnexion des sites distants de l'entreprise SONELGAZ. Nous souhaitons également offrir un accès distant aux ressources de l'entreprise de manière fiable et économique, en particulier pour certains travailleurs.

Ce mémoire est structuré en quatre principaux chapitres, avec le plan suivant :

Le premier chapitre de ce mémoire est intitulé "Présentation du cadre d'étude et de stage". Dans ce chapitre, nous commençons par présenter l'entreprise dans laquelle nous avons effectué notre stage, à savoir SONELGAZ. Nous décrivons brièvement l'activité et le secteur d'activité de l'entreprise.

Le deuxième chapitre de ce mémoire est consacré aux généralités des réseaux informatiques. Dans cette partie, nous commençons par présenter les notions de base sur les réseaux informatiques. Nous définissons ce qu'est un réseau informatique, ses principaux composants et son fonctionnement global.Dans

la deuxième partie de ce chapitre, nous nous concentrons sur la sécurité des réseaux. Nous mettons en évidence les enjeux et les défis liés à la sécurité des réseaux informatiques, en particulier dans un contexte où les cyberattaques sont de plus en plus fréquentes et sophistiquées.

Le troisième chapitre intitulé « l'état de l'art » est consacré aux généralités sur les VPN.

Le quatriéme chapitre. Pratique, n'a qu'un seul point qui concernera la configuration et la mise en œuvre des VPN.

Enfin, notre mémoire s'achéve avec une conclusion générale résumant les connaissances acquises durant la réalisation du projet .

CHAPITRE 1

PRÉSENTATION DU CADRE D'ÉTUDE ET DE STAGE

Introduction

Aujourd'hui la vie quotidienne serait inimaginable sans électricité etgaz. Il faut donc savoir les produire efficacement et en continu. Pour cela la société SONELGAZ qui s'en charge de la distribution de l'énergie électrique et gazière aux clients finaux, toute en assurant la qualité et la continuité de service. Ainsi, pour comprendre le déroulement et le fonctionnement de l'entreprise SONELGAZ nous commencerons par présenter l'organisme d'accueil et structure d'accueil après un bref stage au sein de SONELGAZ précisément la Concession de distribution de Bejaïa (CDB) à cité TOBAL.

1.1 Présentation générale de SONELGAZ

SONELGAZ (Societe Nationale de l'Electricité et du Gaz)(Voir la figure 1.1 est une entreprise public algérienne spécialisée dans la production, la transmission , la distribution et la commercialisation d'électricité et de gaz naturel[7].
La continuité dans la fourniture d'énergie représente l'un les plus importants critères de qualité de service, ce qui incite SONELGAZ a mettre en œuvre tous les moyens nécessaires pour satisfaire les demandes).

FIGURE 1.1 – Logo de SONELGAZ.

1.1.1 Création et évolution

En 1969, SONELGAZ a été créée en tant qu'entreprise publique pour gérer la production et la distribution d'électricité et de gaz dans tout le pays. Au cours des années suivantes, Sonelgaz a continué à se développer et à étendre son réseau de distribution, en construisant de nouvelles centrales électriques et en améliorant les infrastructures de transport et de distribution[7].
Au fil des années, Sonelgaz a également été confrontée à des défis, notamment la nécessité de moderniser ses installations et d'améliorer l'efficacité énergétique, ainsi que la nécessité de répondre à la demande croissante d'énergie en Algérie. Pour relever ces défis, Sonelgaz a entrepris des projets d'investissement importants pour moderniser ses centrales électriques et ses réseaux de distribution[7].
Aujourd'hui, Sonelgaz est une entreprise prospère et bien établie en Algérie, qui continue de jouer un rôle clé dans le secteur de l'énergie du pays. Elle a également élargi ses activités à d'autres pays africains, en fournissant des services de conseil et de formation dans le domaine de l'énergie[7].

Sonelgaz est érigé en groupe industriel composé de 39 filiales et 5 sociétés en participation , on compte : [7]
• La Société Algérienne de Production de l'Electricité (SPE) ;
• La Société Algérienne de Gestion du Réseau de Transport de l'Electricité(GRTE) ;
• La Société Algérienne de Gestion du Réseau de Transport de Gaz (GRTG) ;
• l'opérateur Système électrique (OS),chargé de la conduite du système production/transport de l'électricité ;
• La Société Algérienne de Distribution de l'Electricité et du gaz d'Alger (SDA) ;
• La Société Algérienne de Distribution de l'Electricité et du gaz du centre (SDC) ;
• La Société Algérienne de Distribution de l'Electricité et du gaz de l'Est(SDE) ;
• La Société Algérienne de Distribution d'électricité et du gaz de l'Ouest(SDO).

1.1.2 Situation géographique de SONELGAZ

La Dirtribution de Béjaïa alimente en énergie électrique et gazière les clients résidant sur le territoire de la wilaya de Béjaia. (Voir la figure 1.2)

— Siège social : cité Tobal - Béjaïa.

— Nombre de clients Electricité : 312143 clients.

— Nombre de clients Gaz : 106000 clients.

— La concession de distribution de Bejaia contient 10 agences commerciales chargées de la prise en charge de la clientèle qui sont :
• Bejaïa, Seddouk, Kherrata, Aokas, Amizour, El-kseur. Sidi-Aich, Tazmalt, Akbou et les Quatre chemins.
• Cinq districts électricité chargés de développement, maintenance du réseau électrique qui sont :

FIGURE 1.2 – Situation géographique de SONELGAZ

Béjaia, Kherrata, Amizour, Sidi-Aich, Akbou.

• Cinq districts gaz chargés de développement, maintenance du réseau gaz qui sont : Béjaia, Kherrata, Amizour, Sidi-Aich, Akbou.

1.1.3 Organigramme de l'entreprise

Cette figure1.3 représente l'organigramme de l'entreprise de SONELGAZ.

1.1.4 Activités et les objectifs de SONELGAZ

Activités de SONELGAZ sont centrées sur la production, la distribution et la commercialisation d'électricité et du gaz naturel, pour cela elle vise à assurer une production et une distribution d'énergie efficace, fiable et durable, parmi ses activités et ses objectifs on cite :

• Production d'électricité ;
• Production du gaz naturel ;
• Distribution d'électricité ;
• Transport de gaz naturel ;
• distribution de gaz naturel ;
• Commercialisation d'électricité et de gaz naturel ;
• Services d'ingénierie et de maintenance ;
• Réduire les coûts de production et de distribution d'énergie pour offrir des tarifs compétitifs à ses clients ;

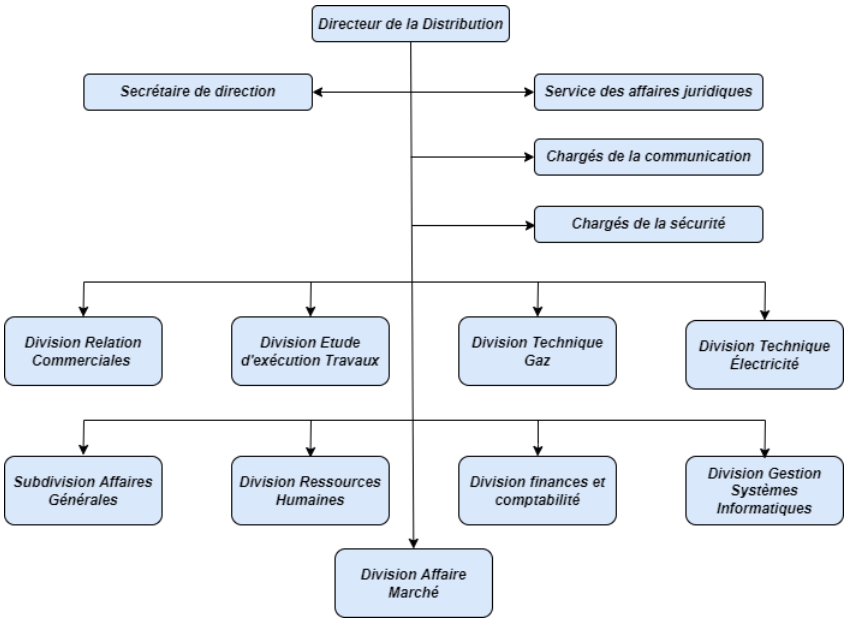


FIGURE 1.3 – L'organigramme de SONELGAZ

• Assurer un approvisionnement fiable en électricité et en gaz naturel à ses clients, en maintenant des normes élevées de qualité et de sécurité ;
• Améliorer l'efficacité énergétique de ses activités ;
• Respecter les normes environnementales et de santé publique en adoptant des pratiques durables dans ses activités.

1.2 Présentation du service d'accueil (Département informatique)

La Division de Gestion de Systèmes Informatique (DGSI) est chargée de la planification, de la mise en œuvre et de la maintenance des systèmes informatiques utilisée par sonelgaz.
les principes responsabilités de DGSI peuvent inclure :

— Configuration et maintenance des logiciels et des matériels informatiques ;
— Gestion d'un réseau informatique et de la connectivité ;
— Sécurisation de système informatique et des données de l'entreprise ;
— Gestion des bases de données.

1.2.1 Activités de DGSI

La gestion de système informatique est une discipline vaste et complexe qui implique de nombreuses activités de la division pour assurer le bon fonctionnement de système informatique. Voici quelques-unes :
• Gestion des systèmes d'exploitation ;
• Gestion de réseau ;

- Gestion de la sécurité ;
- Gestion des données ;
- Gestion des applications ;
- Gestion des projets.

1.2.2 Présentation du réseau informatique de sonelgaz

A fin de pouvoir récolté toutes les informations nécessaires pour proposer une solution adéquate qui réponds aux besoins des utilisateurs, nous avons besoin d'apporter une lumière sur l'étude de l'existant qui est une phase importante dans le développement d'un projet informatique.

Le réseau informatique local de la direction de la distribution de Béjaïa est composée de :

1. **Deux armoires informatiques**.
   - **Armoire rez-de-chaussée :** contenant 3 switchs stackés qu'on illustrera par suite par un seul switch. Elle couvre les division : informatique, commerciale et électricité.
   - **Armoire premier étage :** compronant 5 switch stackés, couvrant les bureaux du deuxième et troisième étage.
2. **Un routeur cisco 2600**.
3. **Téléphonie IP**.
4. **Des serveurs de base de données, de gestion des fichiers**.

Ce réseau est conçu en modèle hiérarchique, c'est-à-dire, il est divisé en 3 couches comme suit :

- **Couche d'accès**
  - Sert d'interface pour des périphériques finaux ;
  - Contrôle des périphériques qui sont autorisés à communiquer sur le réseau ;
  - Inclus routeurs, commutateurs, pont...
- **Couche distribution**
  - Regroupe les données reçues à partir des commutateurs de la couche d'accès en vue de leur routage vers la destination finale ;
  - Gère le flux du trafic réseau à l'aide de stratégies ;
  - Délimite les domaines de diffusion via les fonctions de routage via des VLAN définis au niveau de la couche d'accès.
- **Couche cœur**
  - Constitue le réseau fédérateur à haut débit de l'interéseau ;
  - Essentielle à l'inter-connectivité entre les périphériques de la couche distribution ;
  - Regroupe le trafic provenant de tous les périphéries de la couche distribution ;
  - Capable de réacheminer rapidement d'important de quantité de données.

1.2.3 L'architecture de l'entreprise

La figure ci-desous 1.4 nous montre l'infrastructure réseau de l'entreprise SONELGAZ à Bejaia.

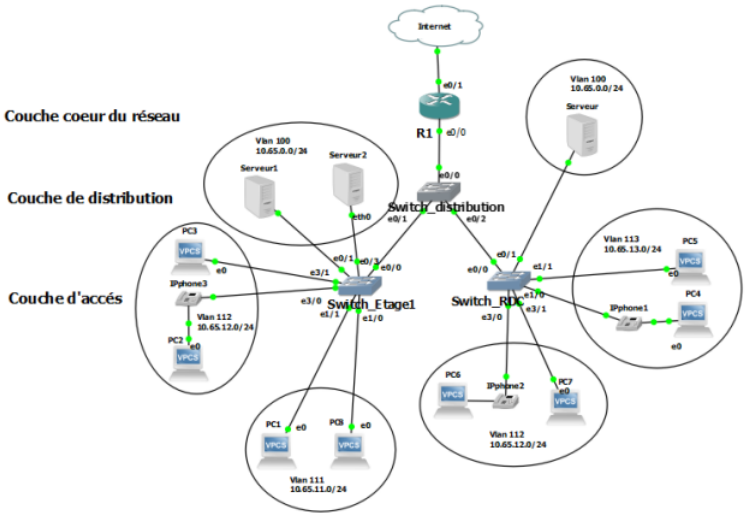


FIGURE 1.4 – L'architecture de l'entreprise SONELGAZ de BEJAIA.

1.2.4 Présentation de l'environnement matériels et logiciels du réseau informatique

SONELGAZ est une infrastructure complexe qui comprend une variété de matériels et de logiciels pour permettre la gestion de l'entreprise. Voici une brève présentation de hardwares et softwares utilisés sur le réseau :

1. Les différentes matériels du réseau informatique.

Équipement	Marque	Quantité	Caractéristique
Routeur	Fortinet Fortigate 60F, Cisco 2600	2	1 port USB , 1 port console , 2 ports DMZ , 2 ports WAN , 2 ports HA ,12 ports RJ45 ,2 ports SFP+ Forti-Link , 4 ports SFP Slots et 4 ports RJ45/ SFP shared Medias Pairs. Slots
Commutateur	DELL , Huawei	12	26 ports RJ45 et 2 ports SFP

TABLE 1.1 – Les équipements de raccordement du réseau infonrmatique SONELGAZ.

Équipement	Marque	Quantité	IOS
PC bureau	DELL , HP	12O	Windows 10
PC portable	HP ,Lenovo	30	Windows 10
Serveur	HP ,IBM	10	Linux/Windows
Enduleur	APC	130	/
Imprimante réseau	IPSON , CANON KYCERA	8	/
Imprimante laser	HP	30	/
Caméra de surveillance	@lhua	14	/
modem	ADSL	2	/

TABLE 1.2 – Les équipements terminaux de SONELGAZ.

2. Les logiciels

Les logiciels utilisés dans SONELGAZ :

— Antivirus Kespersky

— Microsoft Office Word

— Application de gestion commerciale

— Application de gestion comptabilité

1.2.5 Politique de sécurité du réseau en place

L'entreprise doit mettre en place des politiques et des pratiques de sécurité pour protéger leurs réseaux informatiques contre les menaces externes et internes.

1.3 Problématique

A l'issu d'une étude préalable du réseau SONELGAZ et leur communication avec les district à laquelle elle est reliée , nous avons recensé des insuffissances Du réseau existant en terme de sécurité qui se résume aux points suivants :

• manque des équipements de défense : Pare-feu...

• les connexions entre les différentes sites peuvent être exposées aux risques de sécurité tels que les attaques de pirate informatiques , l'espionnage et le vol de donnés.

• la difficulté relatives à la confidentialité des informations échangées entre les sites •

1.4 Solution proposée

Nous avons opté pour une solution VPN site à site qui consiste a mettre en place une liaison permanente, distante et sécurisée entre les différentes sites de groupe SONELGAZ ; afin de résoudre au mieux les différentes préoccupations manifestées par les responsables informatiques de SONELGAZ.
cette solution permet de garantir la sécurité, la confidentialité et l'intégrité des données, elle est conomique et efficace et à moindre coût.

1.5 conclusion

Dans ce chapitre, dans un premier lieu nous avons donné un bref aperçu sur l'historique de la Société Sonelgaz ensuite nous avons cité ses différents filiales. Suivi par les activités et les objectifs de sonelgaz. dans la deuxième partie, nous avons présenté la Division de Gestion de Système Informatique, accompagnée de ses activités, nous avons étudié son réseau informatique existant, rémunéré ces faiblesses et nous avons posé une problématique.

CHAPITRE 2

GÉNÉRALITÉES SUR LES RÉSEAUX ET LA SÉCURITÉ INFORMATIQUE

Introduction

Avant de s'approfondir dans l'essentiel de notre projet, il est recommandé de commencer par discuter les fondamentaux des réseaux informatiques ainsi que les concepts de la sécurité informatique, son objectif et les différentes attaques et les mécanismes de sécurité.

2.1 Réseau informatique

2.1.1 Définition

Un réseau informatique en général est le résultat de la connexion entre deux à plusieurs machines informatiques, afin que les utilisateurs et les applications qui fonctionnent sur ces machines puissent communiquer et échanger des informations[1]. Le terme réseau peut désigner l'ensemble des machines ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés, ce qui est le cas l'orsque on parle d'Internet.
Un réseau informatique peut servir a plusieurs buts et parmi eu le partage de ressources, la communication entre personnes et processus, la garantie de l'unicité de l'information et aussi il sert a standardiser les applications,bon parle généralement de groupware.

2.1.2 Classification des réseaux

1. **Selon la taille**
   On distingue différents types de réseaux selon leurs tailles, leurs vitesses de transfert de données ainsi que leurs étendues, on définit généralement quatre catégories de réseaux :

   - Réseaux personnels ou PAN (Personal Area Network) ;
   - Réseaux locaux ou LAN (Local Area Network) ;

- Réseaux métropolitains ou MAN (Metropolitain Area Network) ;
- Réseaux étendus ou WAN (Wide Area Network).

(a) **LAN :** Ce sont des réseaux de taille plus ou moins modeste sur une distance comprise environ entre 10m et 1km.
Il désigne un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux par un réseau à l'aide d'une même technologie (ethernet ou wifi)[8]. (voir Figure 2.1)

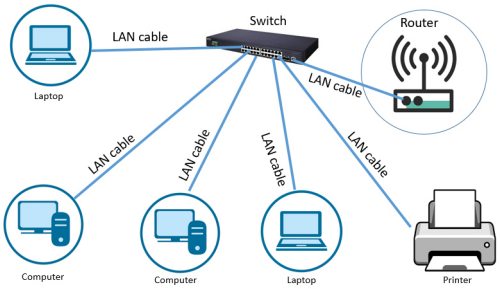


FIGURE 2.1 – Réseau LAN

(b) **MAN :** Les réseaux métropolitains interconnectent plusieurs réseaux locaux sur une distance compris environ entre 1km et 100km.
Ces réseaux peuvent être placés sous une autorité privée ou publique comme le réseau intranet d'une entreprise[8]. (Voir Figure 2.2)

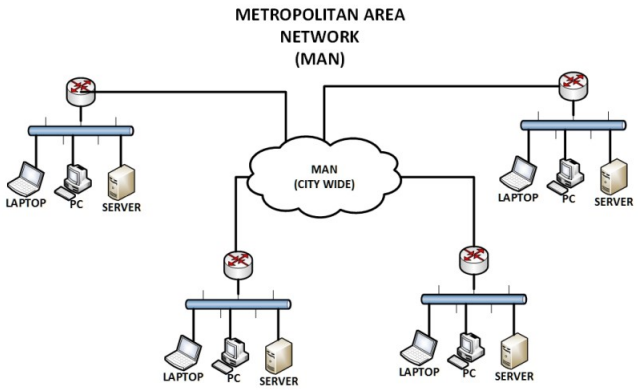


FIGURE 2.2 – Réseau MAN

(c) **WAN :** Les réseaux WAN ou étendus sont destinés à assurer la transmission des données sur une très grande distance géographique.

Ils interconnectent les réseaux LANs ou MANs à l'échelle d'un pays, d'un continent ou de la planète entière[8]. (Voir Figure 2.3)

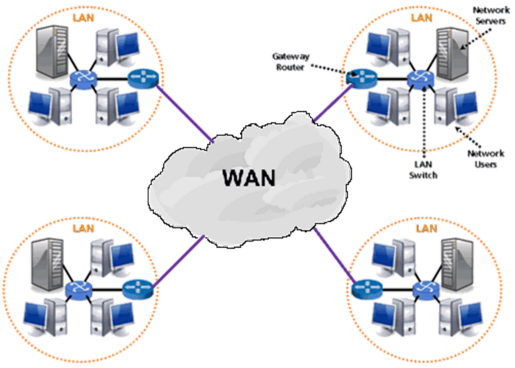


FIGURE 2.3 – Réseau WAN

2. **Selon la topologie**
3. **Topologies physiques :** Elle définit la manière dont les équipements sont reliés entre eux c'est-à-dire elle désigne la disposition ou l'organisation physique (l'architecture d'un réseau)des nœuds du réseau[2].
   On distingue généralement les topologies suivantes :

   • **Topologie en bus :** Dans la topologie en bus, tous les ordinateurs sont connectés à une même ligne de transmission par le biais d'un câble. Cette topologie est utilisée dans la plupart de temps par les réseaux Ethernet et dans les petites entreprises et les établissements scolaires. (Voir Figure 2.4)

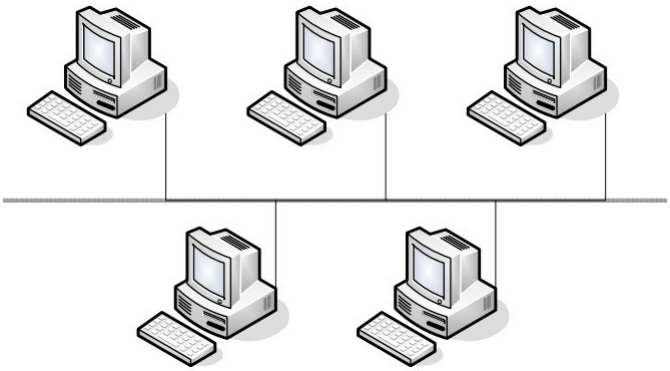


FIGURE 2.4 – Topologie en bus

• **Topologie en étoile :** Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur(en anglais Hub).
Contrairement aux réseaux construits sur une topologie en bus, les réseaux avec une topologie en

étoile sont beaucoup moins vulnérables car une des connexions peu être débranchée sans paralyser le reste du réseau. Cette configuration offre notamment une meilleure gestion du trafic, une facilité de dépannage et une évolutivité aisée. (Voir Figure 2.5)

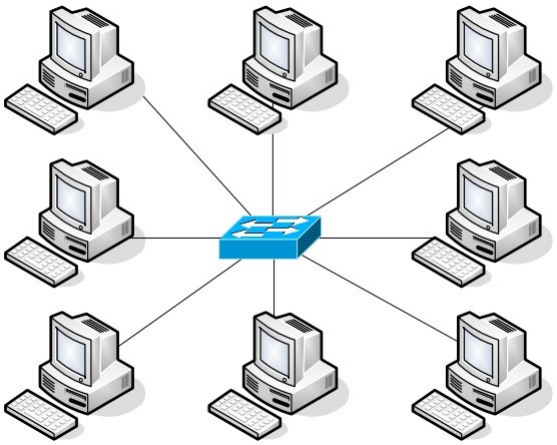


FIGURE 2.5 – Topologie en étoile

• **Topologie en anneau :** La topologie en anneau repose sur une boucle fermée ou toute les stations sont connectées en chaîne les unes aux autres par une liaison point à point. Les données circulent dans un sens unique autour de l'anneau, d'une station à une autre, jusqu'à ce qu'elles atteignent leur destination. (Voir Figure 2.6)

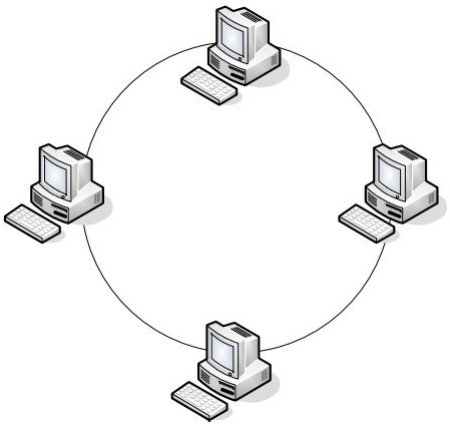


FIGURE 2.6 – Topologie en anneau

• **Topologie en arbre (ou hiérarchique) :** La topologie en arbre repose sur une hiérarchie des équipements réseaux. Dans cette structure, chaque nœud est connecté à un nœud parent, sauf pour le nœud racine qui n'a pas de parent. Chaque nœud peut également avoir plusieurs nœuds

enfants. Cette topologie est souvent utilisée pour les réseaux de télécommunications, les réseaux de distribution d'énergie et d'autre système distribuées.(Voir Figure 2.7)

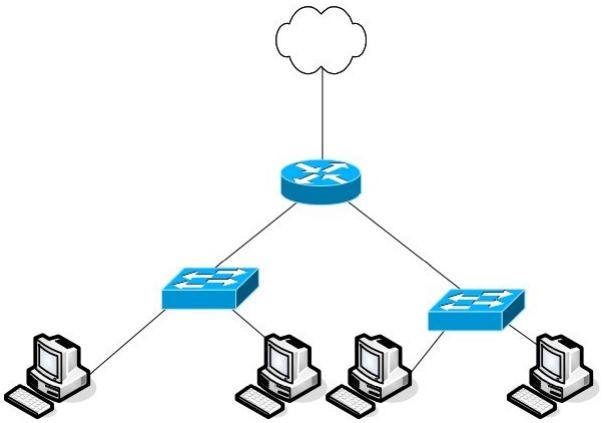


FIGURE 2.7 – Topologie en arbre

• **Topologie maillée :** La topologie maillée est la structure de réseaux qui Constitue une série de liaisons point à point reliant divers nœuds sans passer par un point central.
Dans la topologie complètement maillée il existe plusieurs chemins de transferts entre les différents nœuds, donc elle garantit le transfert des données en cas de panne d'un nœud. L'internet est un réseau fortement maillé.(Voir Figure 2.8)

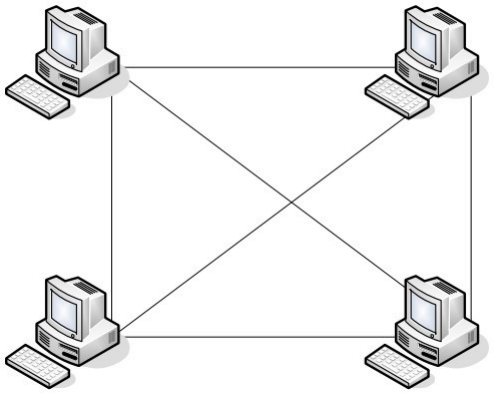


FIGURE 2.8 – Topologie maillée

4. **Topologies logiques :** Par opposition à la topologie physique, elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI[2].

2.1.3 Les équipements d'interconnexion

Deux réseaux quelconques doivent être reliés par l'intermédiaire d'un équipement connecté à chacun d'eux, cet intermédiaire permet la communication et l'échange de données entre ces réseaux distincts. Plusieurs dispositifs d'interconnexions se mettent en place et parmi eux on trouve :

— Le routeur : C'est un périphérique intermédiaire dans un réseau informatique qui garantit que les paquets sont acheminés entre deux réseaux indépendants. Ce routage est implémenté selon l'ensemble de règles formant la table de routage et son fonctionnement est simple. Étant connecté au boîtier via un câble Ethernet, il diffusera la connexion et la récupérera ainsi sur tous les appareils et ordinateurs connectés au réseau[5].

— Le commutateur(Switch) : commutateur réseau agit comme un point central où les appareils tels que les ordinateurs, les imprimantes, les serveurs et autres périphériques réseau peuvent se connecter entre eux afin de communiquer et d'échanger des données. L'information qui reçoit le Switch se dirige uniquement vers le bon destinataire contrairement au concentrateur hub qu'il envoie à tous les périphériques connectés. Donc un Switch a les mêmes fonctions qu'un hub mais le Switch est beaucoup plus performant[5].

— Point d'accès sans fil : Également connue sous le nom AP(Access point) est un équipement d'interconnexion utilisé pour connecter des dispositifs sans fil à un réseau câblé, permet ainsi l'accès à internet ou à un réseau local sans fil[5].

2.1.4 Les équipements matériels

1. **Carte réseau** : Est l'interface entre l'ordinateur et le réseau. Elle assure donc les échanges et les transferts des données avec les autres appareils présents sur le réseau tels que des serveurs, des imprimantes ou même des PCs. Elle est identifiée avec une adresse physique (l'adresse Mac)[14].
2. **La fibre optique** : Permet de transmettre des données sous forme d'impulsions lumineuses avec un débit nettement supérieur à celui des autres supports de transmissions filaires. Elle est constituée du cœur, d'une gaine optique et d'une enveloppe protectrice[11].(Voir Figure 2.9)
3. **La paire torsadée** : Sont des câbles constitués au moins de deux brins de cuivres entrelacés en torsade et recouverts des isolants[11]. (Voir Figure 2.9)
4. **Le câble coaxial** : Est composé d'un fil de cuivre entouré successivement d'une gaine d'isolation, d'un blindage métallique et d'une gaine extérieure[11]. (Voir Figure 2.9)

2.1.5 Les connecteurs réseaux

1. **Connecteur BNC** : Adapter pour les câbles coaxiaux.[3]
2. **Connecteur RJ45** : Adapter aux câbles à paires torsadées.[3]
3. **Connecteur fibre optique** : Utiliser pour les fibres optiques.[3]

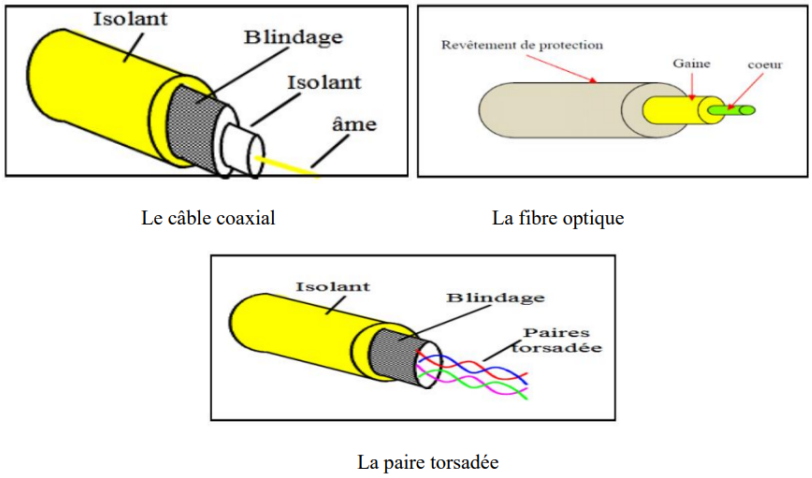


FIGURE 2.9 – Les différents types de capables.

2.1.6 Les normes de communications

a) **Le modèle OSI(open system interconnection) :**
Il s'agit d'un modèle de communication entre tous les systèmes informatiques au sein du réseau qui définit une architecture en couches. Ce modèle a été développé par l'ISO(International Organisation for Standardisation) pour faciliter l'interopérabilité et la communication entre différents systèmes informatiques et réseaux.
Le modèle OSI est composé de sept couches,dont les quatre premières sont dites basses et les trois supérieures dites hautes.

• **Couche physique :** Cette couche sert à transmettre les signaux entre les différents ordinateurs. C'est elle qui gère l'émission et la réception d'un ou plusieurs bits [10].

• **Couche liaison de donnés :** La couche liaison de donnée assure un service de transport des trames, eelle gère les adresses physiques, la détection d'erreurs et le cadrage [10].

• **Couche réseau :** Cette couche est responsable de l'acheminement et la transmission des données entre différents réseaux, elle gère les adresses IP, les tables de routages et la commutation de paquets [10].

• **Couche transport :** C'est la couche qui réalise le découpage des messages en paquets, elle fournit des fonctionnalités telles que la vérificatication des erreurs, le contrôle des flux et le contrôle de congestion [10].

• **Couche session :** La couche cinq gère la synchronisation des communications et la gestion des transactions. Elle assure l'ouverture et la fermeture des sessions(des communications)entre usagers, elle fait le lien entre les adresses logiques et les adresses physiques [10].

• **Couche présentation :**Cette couche est chargée du codage des données applicatives,elle convertit les données applicatives manipulées par les programmes en chaîne d'octets [10].

• **Couche application :** La septième couche du modèle OSI est responsable des services directement fournit aux utilisateurs finaux, tels que le transfert des fichiers, la messagerie électronique et la navigation web [10].

b) **La pile protocolaire TCP/IP (Transmission Control Protocol/Internet Protocol)**
La pile TCP/IP est une suite de protocoles, provient des noms des deux protocoles majeurs TCP et IP. A la différence du modèle OSI qui a d'abord été normalisé avant d'être appliqué, le modèle TCP/IP a tout d'abord été déployé avec succès avant d'être normalisé.(Voir Figure 2.10)
Il est composé de quatre couches :

• **Couche accès au réseau :** Cette couche est regroupée les couches physiques et liaison de données du modèle OSI. Elle assure une bonne gestion du médium (détection de colisions) et permet l'acheminement des informations entre l'émetteur et le récepteur au niveau des adresses MAC [13].
• **Couche réseau :** Cette couche est chargée de fournir le paquet de données (datagramme) et déterminer le meilleur chemin à travers le réseau[13].
• **Couche transport :** C'est la couche qui est responsable de l'établissement de connexion de communication fiable entre les applications sur différents appareils, elle permet la segmentation des données, les vérifications des erreurs, le contrôle de flux et le contrôle de congestion[13].
• **Couche application :** C'est la couche de haut niveau, elle englobe les couches OSI d'application, de présentation et de session, elle correspond directement avec l'utilisateur[13].

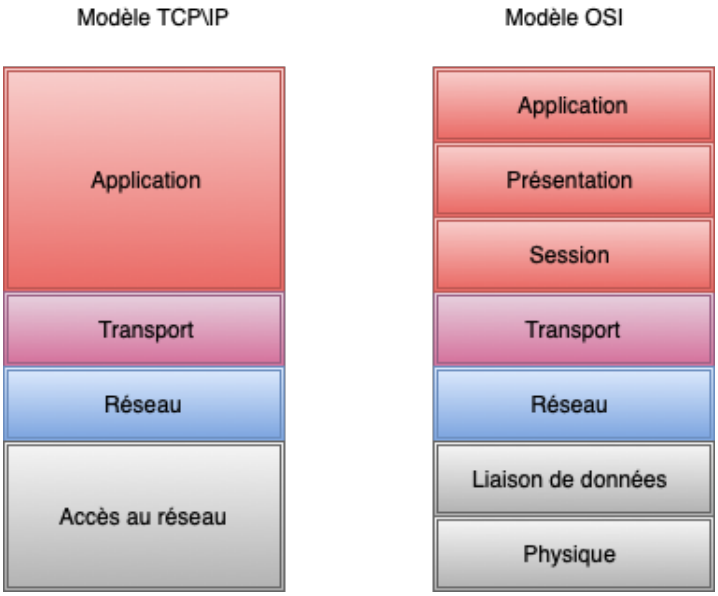


FIGURE 2.10 – Comparaison des modèles OSI et TCP/IP

2.1.7 Adressage IP

C'est le processus d'attribution d'adresses uniques aux dispositifs connectés à un réseau IP. Les adresses IP sont des identifiants numériques qui sont attribués aux dispositifs selon un schéma hiérarchique. Il existe deux techniques d'adressage IP :

1. **CIDR (Classless Inter-Domain Routing)**
C'est une méthode de notations des adresses IP, elle a été introduite pour remplacer le système de notation d'adresse IP basé sur les classes d'adresses qui était utilisé dans le protocole IPv4.

2. **VLSM (Variable Length Subnet Masking)**
   C'est une technique d'adressage IP avancée qui permet de subdiviser un réseau en sous réseaux de tailles variables. Cette méthode offre une meilleure utilisation des adresses IP disponibles, une plus grande flexibilité dans la conception du réseau et une gestion simplifiée des adresses IP.

2.2 Sécurité informatique

2.2.1 Définition

La sécurité informatique est défini par l'ensemble des mesures et des pratique mises en place pour protéger les systèmes informatique, les réseaux, les données et les utilisateurs contre les menaces, les attaques et les risques liés à la technologie de l'information.

2.2.2 Terminologies de la sécurité informatique

1. **Les attaques :** Est l'exploitation d'une faille d'un système informatique à des fins non connue par l'exploitant du système et généralement prejudiciables.
2. **Les vulnérabilités :** Toute lacune ou faille de nature matérielle ou logicielle qui pourrait être exploitée pour réaliser une attaque.
3. **Les menaces :** C'est la possibilité qu'une vulnérabilité soit exploitée accidentellement ou malicieusement par un agent.
4. **Les risques :** Est le degré d'exposition des actifs informationnels aux menaces, en fonction de la valeur de ces actifs des mesures en place pour en préserver la sécurité.
5. **Les contre-mesures :** Ce sont les procédures ou technique permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.

2.2.3 Objective de la sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs.
• Confidentialité : maintenir le bon fonctionnement du système d'information.
• Intégrité : assurer que les informations n'ont pas été altérées par des entités non autorisées ou inconnues.
• Disponibilité : assurer l'accès et la continuité d'un service afin de préserver le bon fonctionnement de système.
• Authentification : assurer que seuls les personnes autorisées aient accès aux ressources.
• Non-repudiation : garantir qu'une transaction ne peut être niée.

2.2.4 Politique de sécurité informatique

La politique de sécurité informatique est un ensemble de règles, de procedure et de pratique mises en place pour protéger les systèmes d'infomation, les données les ressources informatique d'une organisation contre les menaces et les attaques.

• Les principaux éléments à prendre en compte lors de la mise en place d'une politique de sécurité contre les intrusions informatiques sont [16]

— L'identification des enjeux, des risques et des techniques de piratage utilisées.

— Les mesures de sécurité dans un réseau : pour pouvoir se défendre contre les dangers omniprésents. L'authentification des utilisateurs, leurs droits d'accès, les ports et les services, les outils de sécurité, les audits et les sauvegardes seront abordés.

— Les principales opérations à effectuer avant et/ou après les attaques.

2.2.5 Les attaques informatiques

1. **Objectives des attaques**
   • **Interception :** Qui vise la confidentialité ;
   • **Interruption :** Qui vise la disponibilité ;
   • **Modification :** Qui vise la confidentialité et l'integrité ;
   • **Fabrication :** Qui vise l'authentification et l'integrité ;
   • **Rejeu :** Ré-envoyer d'anciens données.

2. **Les différentes étapes d'une attaque**
   • **Identification de la cible :** Cette étape permet de recolter un maximum de renseignement sur la cible en utilisant des informations publiques et sans engager d'actions hostiles.
   • **Le scanning :** L'objectif et de compléter les informations réunies sur une cibles visées, il est ainsi posible d'obtenir les adresses IP utilisées, les services accessibles de meme qu'un grand nombre d'informations de topologie détaillée.
   • **Exploitation des failles :** Permet d'exploiter les failles identifiées sur les éléments de la cible , que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitaton présebtes sur le réseau.
   • **La progression :** Cette étape l'attaquant a ses droit vers root(administrateur) sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations,...).
   • **Effacement des traces :** Dans cette dernière étape consiste à la suppression des preuves de l'attaque.

3. **La classification des attaques**
   Le schèma suivent représente la classification des attaques 2.11 :

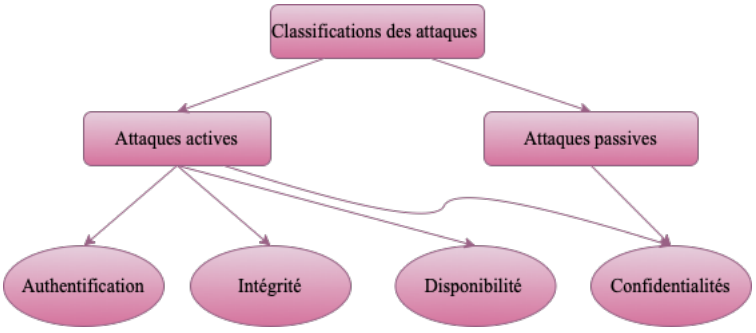


FIGURE 2.11 – Classifications des attaques

2.2.6 Mécanismes de sécurité

1. **Antivirus :** Est un logiciel conçu pour détecter, prévenir et éliminer les logiciels malveillants tel que les virus, les vers et les chevaux de Troie
2. **Chiffrement :** Consiste à transformer une donnée (texte, son, image,...) afin de la randre incompréhensible par unr personne autre qui la possède et celui qui en est le destinataire.
3. **Pare-feu :** Il permert d'assurer la sécurité du réseau en controlent le trafic entrant et sortant entre un réseau interne et d'un réseau externe.
4. **Les VLANs(Vertuel Local Area Networks) :** Permet de créer des domaines de diffusion gérer par les commutateurs indépendamment d'emplacement ou se situent les noeuds, se sont des domaines de diffusion gérer logiquement.
5. **Reseaux privés virtuels (VPN) :** Le VPN permet de créer une conneion sécurisé et chiffré entre un appareil et réseau distant via internet, il offre un moyen de sécurisé les communication et de protéger la confidentialité des données lorsqu'elles sont transmises sur des réseaux publics.

2.3 Conclusion

Dans ce chapitre nous avons présenté les réseaux informatiques de façon générale,nous avons cité les critères basiques qui montrent le rôle d'un réseau informatique et sa nécessité ainsi sur la sécurité informatique et ses objectifs, les terminologies liées à cette dernière et quelque notions sur les attaques pour l'objectif de bien définir le concept d'administration au sein d'une entreprise. Le chapitre suivant sera consacré pour les VPNs et la sécurité.

CHAPITRE 3

LES RÉSEAUX PRIVÉES VIRTUELS

Introduction

En raison des terribles développements qui se produisent dans le monde de la technologie, en particulier dans les réseaux informatiques, comme nous l'avons mentionné dans le deuxieme chapitre, les informaticiens ont créé les réseaux privées virtuels pour assurer la confidentialité pour chaque utilisateur. Nous allons aborder dans ce troisième chapitre, quelques notions sur les réseaux privés vertuels ainsi que les concepts sur leurs fonctionnements et leur intérêt.

3.1 Les lignes spécialisées

Les lignes spécialisées ou les lignes louées sont des connexions réseaux dédiées qui permet la transmission de données à moyens et hauts débit en liaison point à point ou multipoint entre des sites distants. On peut citer quelques lignes spécialisées couramment utilisées avant l'utilisation des réseaux virtueles privées (VPN) :

• **Ligne T1 \ E1** : Souvent utilisée pour reliée des sites distant dans les réseaux d'entreprise.

• **Ligne T3 \ E3** : Géneralement utilisée pour fournir une connectivité à haut débit pour des applications nécessitant une bande pasante importante.

• **Ligne ATM \ Frame Relay** : Ces types de liges étaient géneralement pour fournir une connectivité à commutation de cellules ou de trames.

3.2 Définition

Un réseau privé virtuel(VPN) décrit la possibilité d'établir une connexion réseau protégée lors de l'utilisation de réseaux publics.

Le VPN relie deux réseaux physiques LAN par une liaison qui n'est pas réellement sûre et surtout pas dédiée à cet usage pour cela est dit vertuel. Et privée car les données sont cryptées et seuls les deux réseaux se voient mais ne sont pas vus de l'extérieur.

Le principe du VPN est basé sur la technique du tunnelling, cela consiste à construire un chemin virtuel

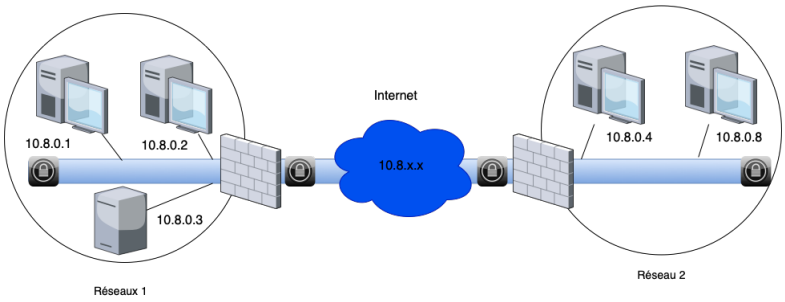


FIGURE 3.1 – Exemple d'utilisation d'un VPN

après avoir identifié l'émetteur et le destinataire. Ensuite la source chiffre les données et les achemine en empruntant ce chemin virtuel.(Voir Figure 3.1)

3.3 L'intérêt du VPN

Un VPN permet de créer une connexion sécurisée et cryptée entre une appareil et un serveur distant pour protéger les données contre les pirates informatique, En masquant l'adresse IP réelle, un VPN garantit également l'anonymat et la vie privée en ligne. De plus VPN permet de contourner les geo-blocages sur le web et peut également optimiser la bande passante et réduisant la congestion d'un reseau et en améliorant les temps de réponses[4].

3.4 Protocoles des VPN

Il existe plusieurs protocoles utilisés pour établir une connexion sécurisée entre l'appareil et le serveur VPN distant.
Voici une brève disciprtion des protocoles les plus communément utilisés dans le cadre de VPN.

3.4.1 Niveau 2

• **PPTP (Point to Point Tunneling Protocol) :** C'est un protocole développé par Microsoft, est l'un des plus anciens protocoles VPN toujours en utilisation, qui opère sur le port 1723 de TCP, il permet d'acheminer des protocoles non internet (NetBios,IPX,Appeltalk..)sur un reseau internet. PPTP ne spécifie pas le cryptage, il s'appuie plutôt sur le protocole point à point pour mettre en oeuvre les fonctions de sécurité.

• **L2F (layer 2 forwarding) :** Cisco a développé ce protocole autour des années 1996, il est désormais quasi-obsolète. L2F a été spécialement conçue pour le tunnel de trafic PPP. • **L2TP (layer 2 Tunneling Protocol) :** Ce protocole est une amélioration à la fois de PPTP et L2F, L2TP n'assure que le transport de données et leur l'intégrité mais pas de confidentialité,ainsi les données transitent. Pour cette raison, L2TP encapsule souvent des paquets IPsec pour assurer la confidentialité des données.

3.4.2 Niveau 2.5

• **MPLS (Multi Protocole Label Switching) :** Le protocole MPLS est effectué dans un niveau hybrides 2.5 qui n'existe pas dans les couches OSI, car il est souvent situé dans un niveau intermédiaire entre le niveau 2 et le niveau 3, permet d'améliorer la qualité de service et la performance de réseau en utilisant des étiquettes pour identifier les chemins de transmission des paquets de données à travers le réseau.

3.4.3 Niveau 3 et plus

• **IPSec (Internet Protocol Security) :** IPSec est un protocole qui désigne un ensemble de mécanisme destinés à sécurisé l'échange données a travers l'internet, il assure la confidentialité, l'authentification et l'intégrité des données, issu des travaux de l'IETF. Il a été conçu d'une manier à être supporter par IPV4 et a été intégrer dans IPV6.(Voir Figure 3.2)

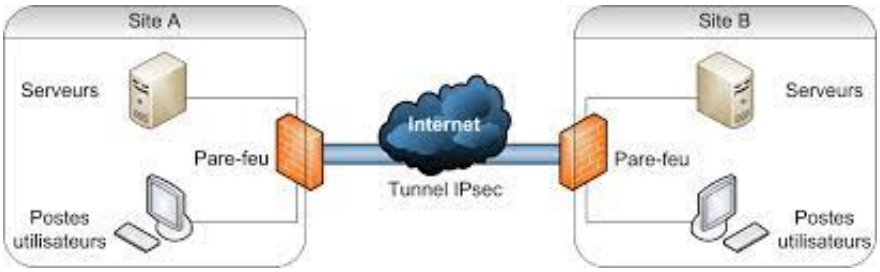


FIGURE 3.2 – Exemple d'emploi IPsec entre sites distants

IPsec est basé sur deux mecanismes différents assurant les rôles de sécurisation : AH (Authetification Header) et ESP (Encapsuling security Payload) :

1. **AH :** Protège autant de données que possible dans les datagrammes IP en grantissant l'intégrité et l'authentificatiion des données. Toutes les données ne peuvent pas être sauvegarder car certains champs de l'entêtes sont modifiable et donc de nature non prédictible.(Voir Figure 3.3)

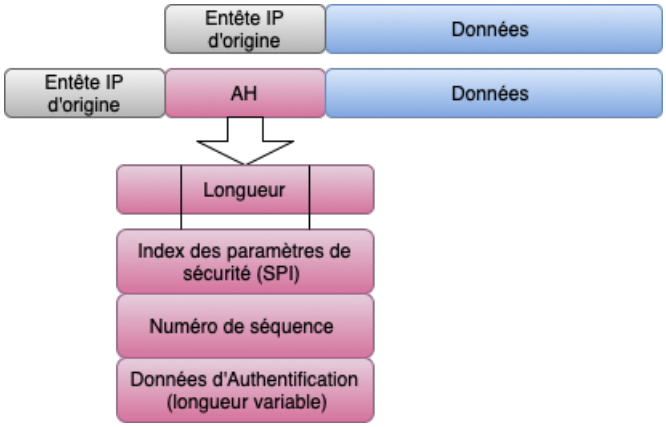


FIGURE 3.3 – Détails des champs de l'en-tête AH

2. **ESP :** le protocole ESP assure la confidentialité, l'intégrité et est utilisé avec IKE pour authentifier les données échangées. Il garantit également la protection contre le rejeu. Il est possible d'utiliser uniquement les fonctionnalités d'intégrité et d'authentification sans chiffrement (ce qui peut satisfaire la plupart des cas d'utilisation d'AH).(Voir Figure 3.4)

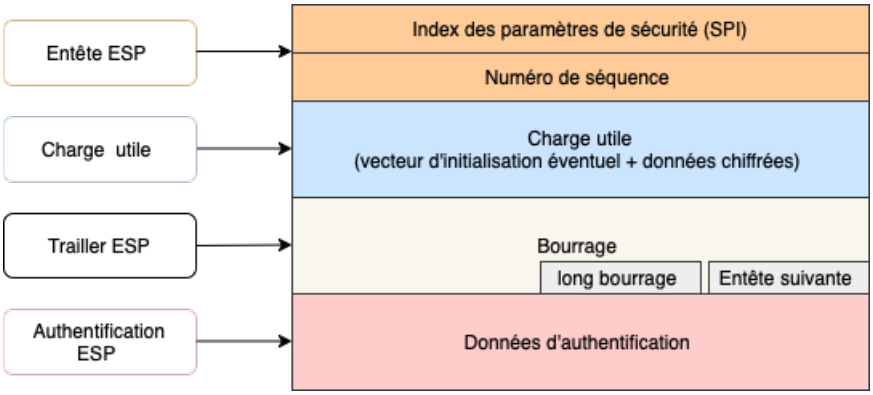


FIGURE 3.4 – Détails des champs de l'en-tête ESP

• **GRE (Generic Routing Encapsulation) :** GRE est un protocole de tunneling utilisé pour encapsuler et chiffrer des paquets de données sur le réseau IP, il est développé par Cisco aussi est une solution fiable de communication sécurisée, à condition d'utiliser IPsec comme solution de cryptage. (Voir Figure 3.5)

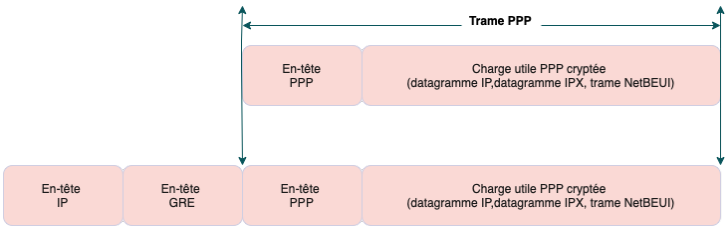


FIGURE 3.5 – Entête GRE

• **SSH (Secure Shell) :** SSH permet une connexion sécurisée de type console (équivalent à Telnet) ou transfert de fichier (notamment de type FTP), sa croissance est limitée par le succès grandissant de SSL \ TLS. Néanmoins il reste encore un protocole à concéder pour ceratins usages.

• **SSL \ TLS (Secure Secrets Layer Transport Layer Security) :** Ces protocoles sont prospèrent car ils sont très simple à mettre en oeuvre et aide à franchir les pare-feu en utilisant le port 443, de nombreux cas ils ne nécessitent qu'un simple navigateur pour être utilisable. Il sont maintenant implémentés nativement d'autres logiciels (clients messagerie, clients FTP).

3.5 Les modes d'IPsec

La communication entre deux hotes protègée par IPsec, est susceptible de fonctionner suivant deux modes différents (Voir Figure 3.6) :

3.5.1 Mode transparent

Il s'agit d'un mode par défaut pour IPsec, l'orsque ce mode est utilisé IPsec crypte uniquement la charge utile IP, les entêtes IP ne sont pas modifiée et les protocoles AH et ESP sont combinés entre cet entête et l'entête du protocole transporté.
Le mode transparent est utilisé pour la communication de bout en bout entre un client et un serveur. Il protége une charge IP dans les protocoles de la couche supérieure tels que les protocoles UDP et TCP.

3.5.2 Mode tunnel

Le mode tunnel est utilisés pour sécuriser les communicatios entre deux réseaux, tels q'un réseau privé d'entreprise et un réseau distant via une connexion VPN.
Dans ce mode l'intégralité du paquet IP, y compris l'entête IP, est crypté en mode tunnel l'IPsec enveloppe le paquet original, le crypte, ajoute un nouvel entête IP et l'envoie de l'autre coté du tunnel VPN. Enfin, l'utilisation du mode tunnel résulte en des paquets plus gros qu'en mode transparent pour une meme quantité de données utiles. La consommation en ressources réseaux est donc plus importante.

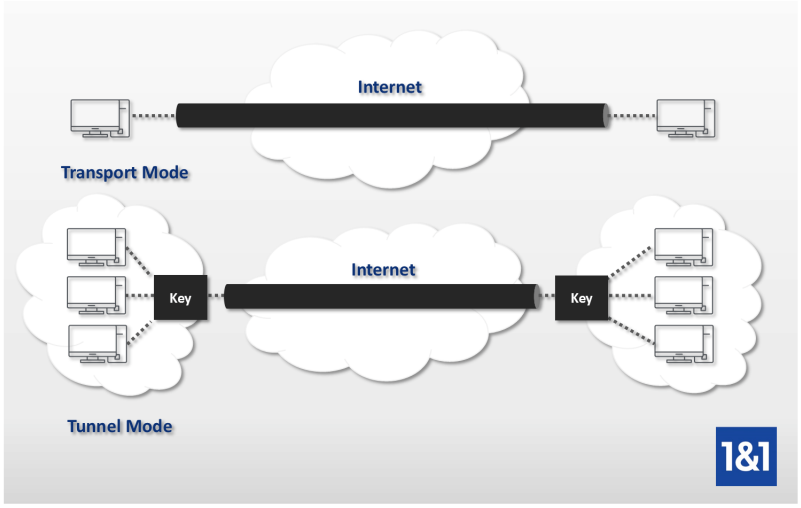


FIGURE 3.6 – Les modes d'IPsec

3.6 Topologies des VPNs

Il est important de choisir la topologie des VPN appropriée en fonction des besoins de sécurité, de suivre les meilleures pratiques de sécurité pour garantir la confidentialité et l'intégrité des données dans

un réseau.
On peut distinguer deux grandes catégories de VPNs : le VPN d'entreprise et le VPN opérateur.

3.6.1 VPN d'entreprise

Il est utilisé par les entreprises pour permettre à ses employés de travailler à distance et d'accéder aux ressources de maniére sécurisé.

1. **VPN site à site**
   C'est un des cas les plus fréquents, il s'agit de relier deux sites d'une même entreprise ou bien le site d'une entreprise et celui d'un fournisseur ou d'un client.
   Un VPN de site à site est un outil puissant qui peut aider les entreprises à connecter leurs ressources distribuées de manière sécurisée et efficace, tout en réduisant les coûts et en améliorant les performances.
2. **VPN poste à site**
   Il est souvent utilisé par les travailleurs distants pour accéder aux ressources de l'entreprise depuis un emplacent extérieure, comme travailler à domicile ou en déplacement. Cela permet aux utilisateurs distants d'accéder aux fichiers, aux applications et aux autres ressoures de l'entrprise de manière sécurisée, comme s'il étaient sur le même réseau local.

3.6.2 VPN opérateur ou VPN extranet

VPN opérateur c'est à dire un opérateur spécialisé dans les offre VPN. Il assure la sécurité du réseaux et sa performance. Il est assez courant de parler d'un VPN opérateur car il est comme meme difficile, sans la complicité du personnel de l'opérateur,d'intercepter les communications échangés entre les sites.

1. **Caractéristiques du VPN opérateur ou extranet**
   Les caractéristiques du VPN opérateur incluent :
   • Sécurité élevée grace à des protocoles de cryptage avancée pour protéger les données en transit contre les attaques malveillantes.
   • Fiabilité et disponibilité grace à la garantie de l'opérateur d'ue connexion stable et une disponibilité élevée.
   • Haute performances avec une bande passante élevée, une faible latence et une vitesse de connexion rapide.
   • Configuration personnalisée pour répondre aux besoins spécifiques des entreprises.
2. **Avantages et inconvenients**[6]
   Les principaux avantages de ce type de réseau sont :
   • transparence totale pour les postes du réseaux ;
   • Possibilité de mettre en place de la QOS(Quality of service) pour privilégier les traffics les plus prioritaires et garantir à ceux-ci un maximum de bande passante ;
   • Assurence sur les performances proposées par le réseau(débit et temps de transit des messages).

   Cependant ,il y a quelque inconvénients à prendre en compte tels que :
   • Les abonnements des sites au réseau opérateur peuvent etre couteux ;
   • Il est nécessaire d'avoir un opérateurunique pour tout le réseau VPN ;

• L'ajout d'un protocole de cryptage est nécessaire pour éviter la capture des messages dans le réseau privatif.

3.7 Conclusion

Ce chapitre nous a donné l'opportunité en premier lieu de découvrir et de mieux comprendre le concept des VPNs, ou nous avons présenté ses notions de base et ces topologies ainsi que les différents protocoles nécessaires pour le fonctionnements d'un VPN.
Ce bagage théorique nous permettra à faire une simulation d'une solution VPN qui va être aborder dans le chapitre suivant.

CHAPITRE 4

L'IMPLÉMENTATION DES SOLUTIONS

Introduction

Dans ce chapitre nous avons effectué une configuration VPN entre quatres sites distants. nous commençons avec une représentation de l'ogicies utilisé avant d'exposer l'architecture permettant de réaliser l'idée désirée.

4.1 Architecture proposée

Cette figure 4.1 représente l'architecture que nous avons proposé pour l'entreprise SONELGAZ.

4.2 Présentation des outils de travail

4.2.1 Partie software

1. **Les logiciels utilisés**

   • **GNS3**

   GNS3(Graphical Network Simulator-3) c'est un logiciel open-source largement utilisé pour simuler et émuler des réseaux informatiques. Il permet aux utilisateurs de créer des topologies réseaux virtuelles.
   GNS3 utilise la technologie de virtualisation pour émuler les fonctionnalités et les comportements des appareils.

   • **Vmware Workstation version 17.0.0**

   VMware Workstation est un logiciel de virtualisation qui permet de gérer des machines virtuelles sur un ordinateur. Il permet plusieurs copies du même système d'exploitation et prend en charge plusieurs systèmes d'exploitation exécutés sur un PC Windows ou Linux. Il fonctionne efficacement comme une solution pour réduire les coûts informatiques et augmenter l'efficacité de l'agilité.

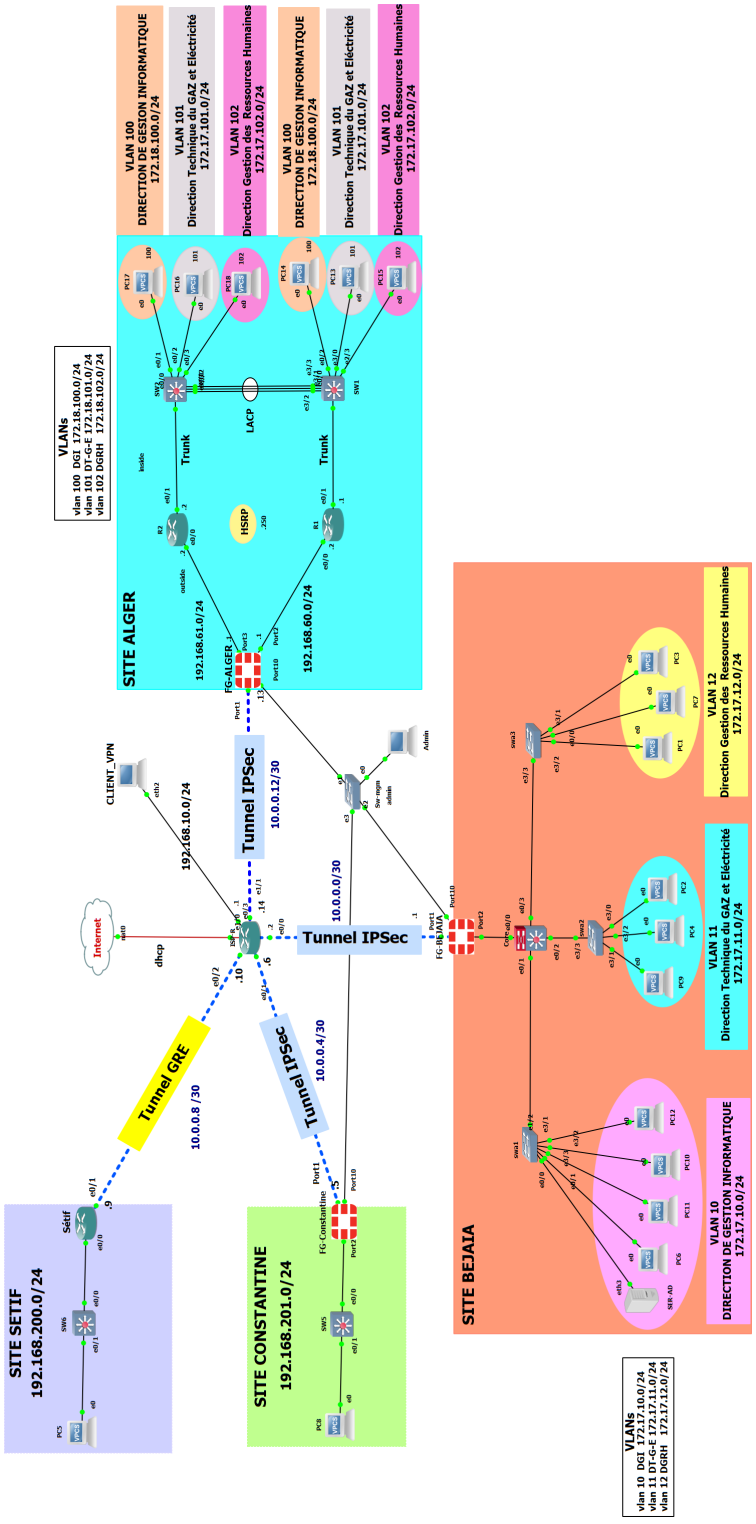


FIGURE 4.1 – L'architecture proposée pour l'entreprise SONELGAZ.

- **Wireshark**

Wireshark est un logiciel open-source de capture et d'analyse de paquets réseau. Il est largement

utilisé pour l'analyse du trafic réseau, le dépannage des problèmes de réseau et la sécurité des réseaux.

Wireshark permet aux utilisateurs de capturer et d'examiner le trafic qui circule sur un réseau, d'analyser les paquets de données et de visualiser les informations détaillées sur les protocoles utilisés.

• **FortiClient** FortiClient est un logiciel de sécurité tout-en-un développé par la société Fortinet. Il s'agit d'une solution de sécurité multiplateforme qui offre une gamme de fonctionnalités pour protéger les appareils et les réseaux contre les menaces en ligne.

2. **Les systèmes d'exploitations utilisés**

   • **Windows 10**

   Windows 10 est un système d'exploitation développé par Microsoft et constitue la version la plus récente de la famille des systèmes d'exploitation après Windows 7 et Windows 8.1. Cette nouvelle version est la première à fonctionner sur toutes les plateformes existantes : ordinateurs de bureau et portables, Smartphones et tablettes. L'interface de l'IOS s'adapte automatiquement au format et au mode de saisie.

   • **Windows Server 2022**

   Windows Server 2022 est la dernière version du système d'exploitation serveur de Microsoft, qui succède de Windows Server 2019. Ce système fournit une plateforme de serveur puissante, sécurisée et fiable pour répondre aux besoins des entreprises modernes.

4.2.2 Partie hardware

Les équipements utilisés dans l'architecture que nous avons proposé sont les mêmes équipements de l'entreprise.

4.3 Partie configuration

4.3.1 Présentation des quatres sites

L'architecture au dessus relie quatre sites dans quatres villes différentes disposant chaqu'un d'un réseau local que nous avons défini avec une adresse de classe.

1. **Site de Bejaia**

   Il est représenté par :

   (a) **Un firewal (Fortigate) :** pour lequel nous avons attribué deux interfaces, une relié au réseau LAN par un switch distribution et l'autre à un réseau WAN par un routeur.

   • **La configuration du fortigate :** La première étape consiste à renomer le fortigate par "FG-BEJAIA", puis lui attribuer l'adresse IP et autoriser l'accès à travert le ping, http, https et ssh. (Voir Figure 4.2)

   • **Le routage Inter-Vlan :** La deuxième étape consiste à configurer les interfaces du fortigate, pour celà nous allons tout d'abord connecter au pare-feu via le Web, une interface d'authentification s'affichera pour tous les trois pare-feu qui existent.

   Après nous allons introduire le login ainsi que le password. (Voir Figure 4.3)

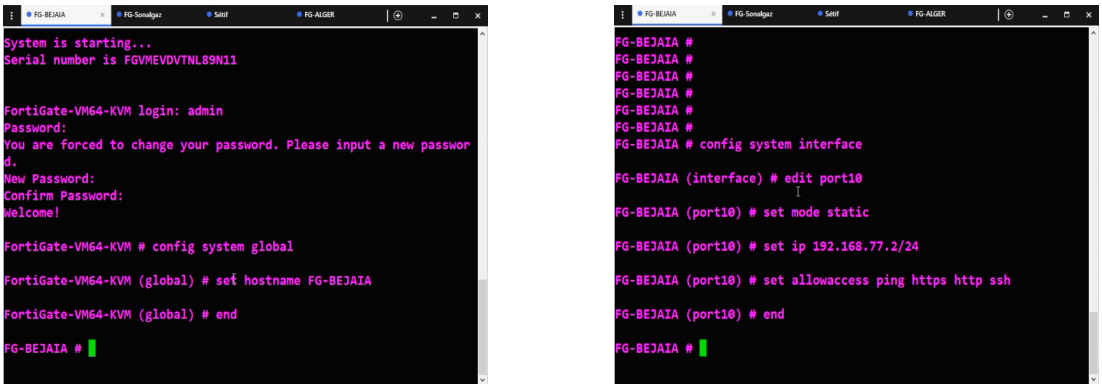


FIGURE 4.2 – Configuration du firewal de Bejaia

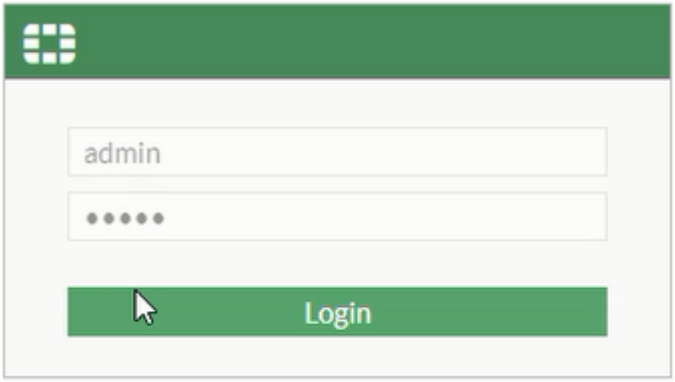


FIGURE 4.3 – Interface d'authentification

Une fois connecté, on sera placé dans le tableau de bord, pour configurer l'interface WAN sur le port 1 il faut passer par [Système Management]->[Network]->[Interface]. (Voir Figure 4.4)

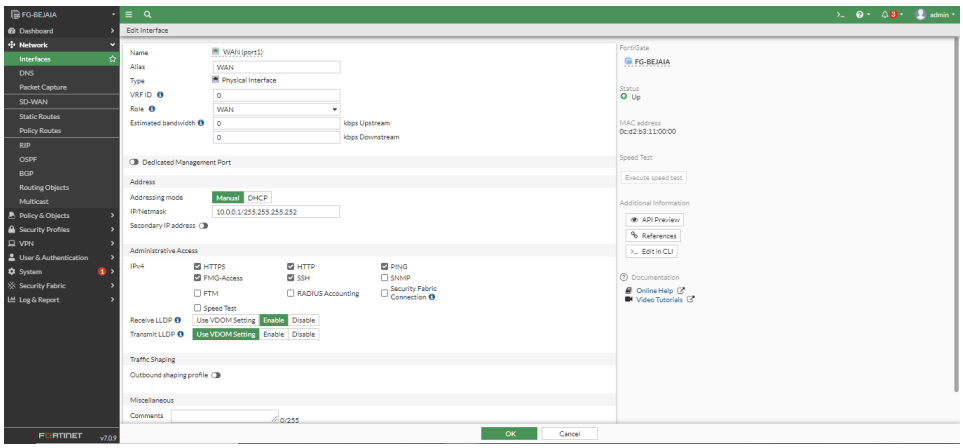


FIGURE 4.4 – Configuration du port 1 de firewal de Bejaia

Après la configuration du port 1 on passe au interfaces VLANs qui seront configurées sur le port 2, on clique sur le port 2 puis nous avons crée une interface nommée inter-VLAN. (Voir la figure 4.5)

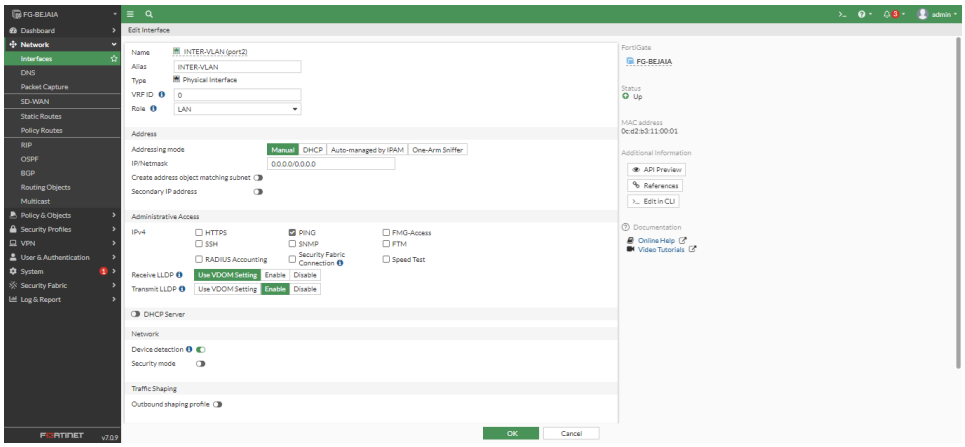


FIGURE 4.5 – Création de l'interface inter-VLAN.

Dans cette étape nous allons créer trois interfaces VLANs :
VLAN 10 DGI qui va avoir cette adresse IP 172.17.10.0/24.
VLAN 11 DT-G-E qui va avoir cette adresse IP 172.17.11.0/24.
VLAN 12 DGRH qui va avoir cette adresse 172.17.12.0/24.
Pour celà nous allons cliquer sur [Create new]-> [Interface], puis nous allons afficher la fenetre de création et nous remplissons les information comme illustre la figure 4.6.

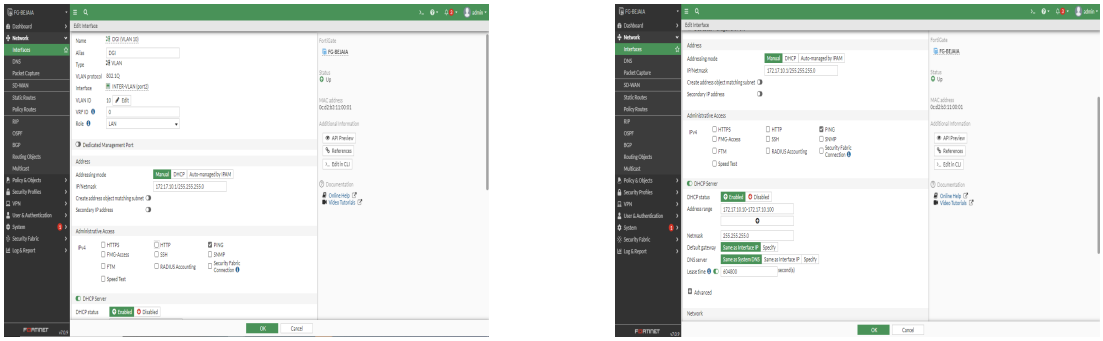


FIGURE 4.6 – Création du VLAN 10 (DGI) de Bejaia .

- **Création d'une zone**

La création d'une zone permet de faciliter la gestion et la maintenance des politiques à l'avenir.
Pour cela nous allons sur [Network]-, nous cliquons sur "Create New""Zone".
Une fois l'interface de création d'une zone apparait, nous allons introduire le nom puis nous ajoutons les membres de l'interface (vlan 10, 11, 12) comme le montre la figure 4.7.

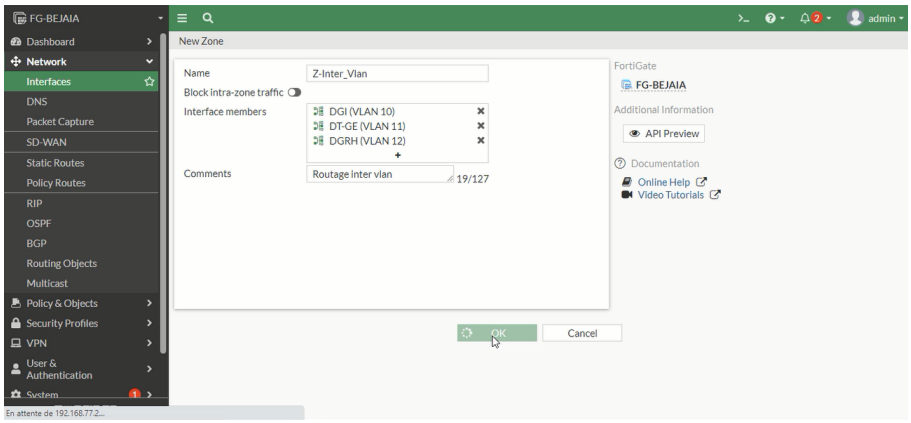


FIGURE 4.7 – Création d'une zone.

• **Création de la route statique vers l'Internet**

Il suffit juste d'aller sur [Network]->[Static Routes] puis en tape sur Create New, ensuite on remplie les informations suivantes :

Destination c'est 0.0.0.0 0.0.0.0 pour les trois fortigate.

Gateway Address : 10.0.0.2.

Interface : WAN (Port 1).

(Voir Figure 4.8)

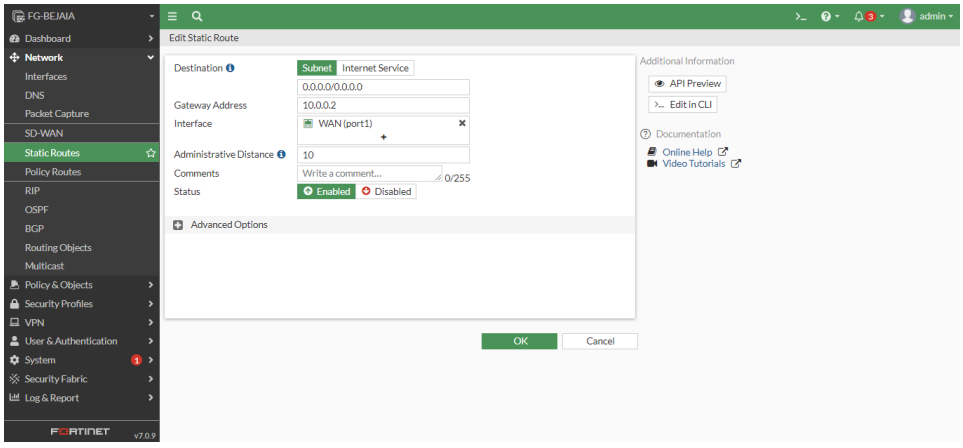


FIGURE 4.8 – Création de la route statique de Bejaia vers l'Internet.

• **Autorisation de la connexion du fortigate vers l'Internet**

Pour configurer l'autorisation de la connexion vers internet, nous allons accéder à [Policy and Object]->[Firewal Policy], puis nous allons cliquer sur "Create New" puis nous allons introduire le nom, l'interface d'entrée, l'interface de sortie, la source, la destination ainsi que les services. (Voir Figure 4.9)

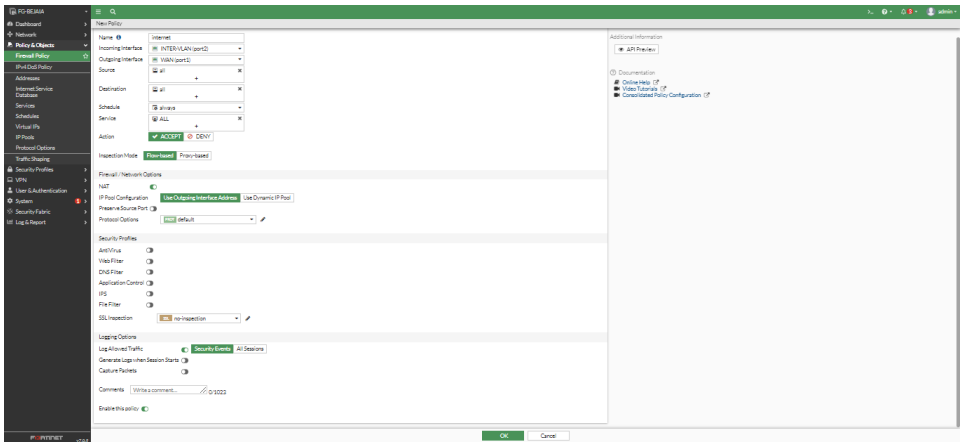


FIGURE 4.9 – Autorisation du fortigate de bejaia de se connecter à l'internet.

(b) **Switch distribution**

Il est relié à 3 interfaces VLANs (VLAN 10, VLAN 11 et VLAN 12) avec des switchs d'accès.

2. **Site d'Alger**

Il représenté par :

(a) **Un firewal (fortigate) :** Pour lequel nous avons attribué trois interfaces, deux reliées aux réseau LAN et une relié à un réseau WAN.

• **La configuration du fortigate :** La première étape consiste à renomer le fortigate par "FG-ALGER", puis lui attribuer l'adresse IP et autoriser l'acces à travert le ping, http, https et ssh. (Voir Figure 4.10)

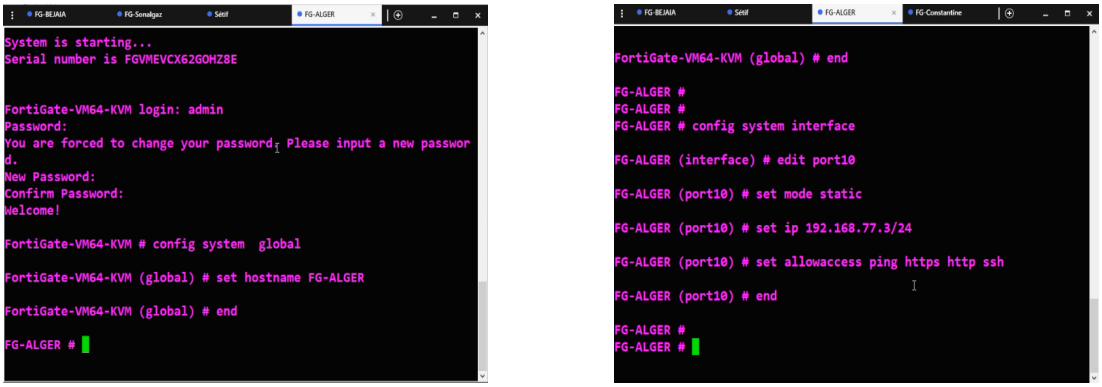


FIGURE 4.10 – Configuration du firewal du Alger

• **La configuration des interfaces :** On se place ici dans le tableau de bord, pour configurer l'interface WAN sur le port 1 il faut passer par [Système Management]->[Network]->[Interface]. (Voir Figure 4.11)

Maintenant nous configurons le port 2 ou se trouve un réseau LAN. (Voir Figure 4.12)

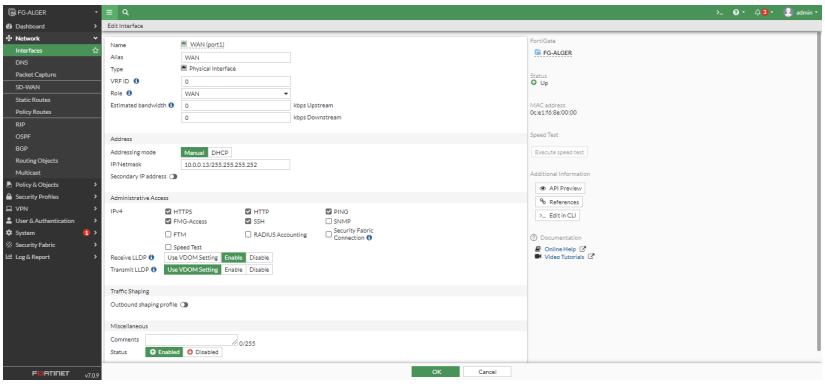


FIGURE 4.11 – Configuration du port 1 du firewal d'Alger

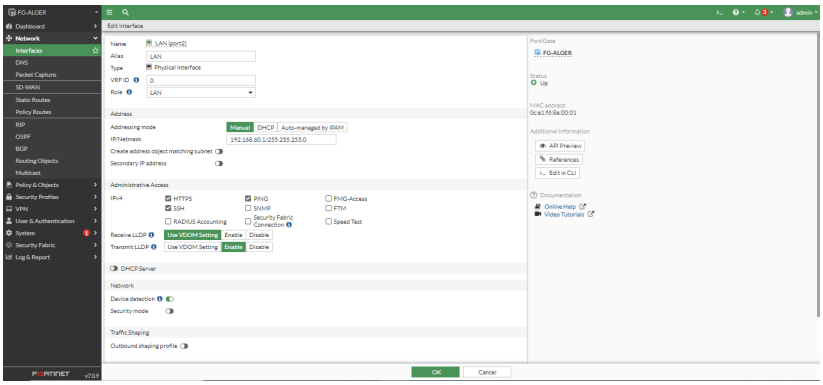


FIGURE 4.12 – Configuration du port 2 du firewal d'Alger

Enfin le port 3 qui est aussi un réseau LAN dont les 2 routeurs du port 1 et le port 2 sont configuré avec le protocol HSRP dans le but d'assurer la passerelle par défaut d'un sous réseau en dépit d'une panne d'un routeur. (Voir Figure 4.13)

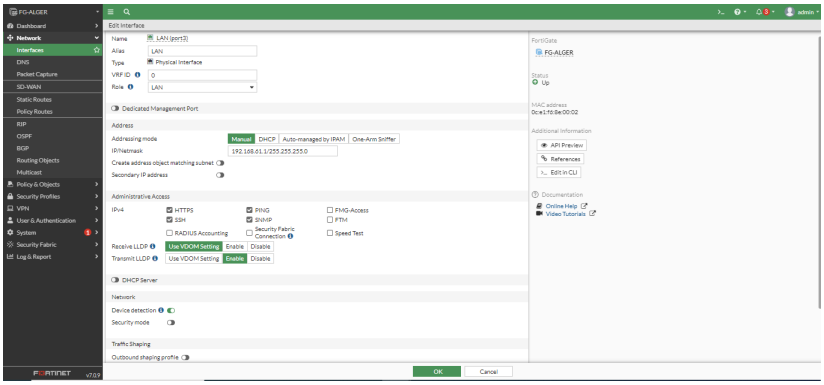


FIGURE 4.13 – Configuration du port 3 du firewal d'Alger

- **Création de la route statique vers l'Internet**

La création se fait avec la même méthode illustré avant et pour les informations sont les mêmes juste la Gateway qui va changer. (Voir Figure 4.14)

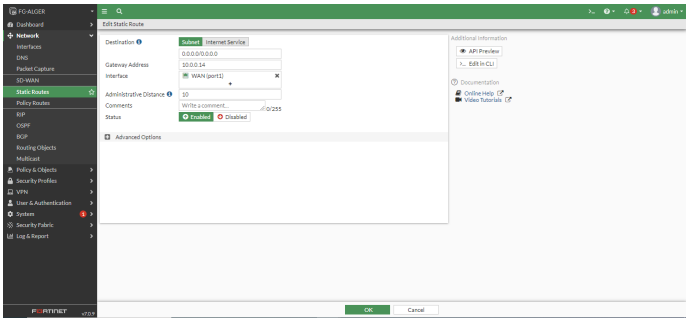


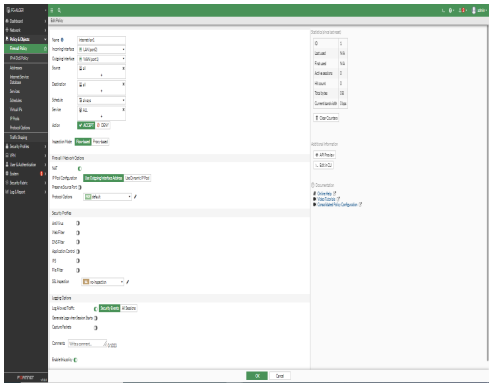
FIGURE 4.14 – Création de la route statique de Alger vers l'Internet.

• **Autorisation de la connexion du fortigate vers l'Internet**

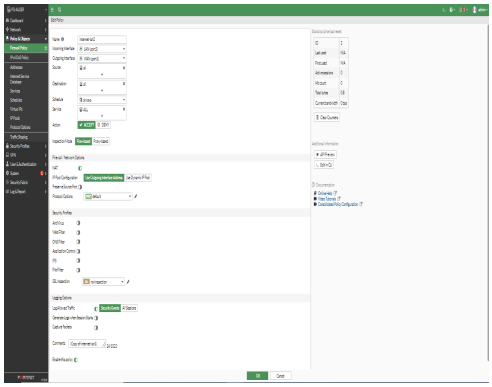
À Alger nous avons deux ports LAN, donc on doit autoriser la connection vers l'internet pour les deux.

Au début on autorise le port 1 à se connecter à l'internet. (Voir Figure 4.15a)

Puis le port 2 à se connecter à l'internet. (Voir Figure 4.15b)



(a) Policie du port 1



(b) Policie du port 2

(b) **Routeur R2 (Port3)** Pour configurer le routeur 2 on identifie une addresse à l'interface, après la configuration de HSRP dans l'aquelle on établie l'ID de VLAN, les groupes existant et leurs addresses, le statut et la priorité. (Voir Figure 4.16)

Pour faciliter la communication entre le réseau locale d'Alger et le réseau externe (internet), nous avons utilisé le NAT statique. Donc dans cette étape nous montrons la création du NAT et l'autorisation des trois VLANs (100, 101, 102) à se connecter au réseau WAN. (Voir Figure 4.17)

Enfin nous découpons les interface de routeur2 en "inside" et "outside" en but de renforcer la protection du réseau, de controler les flux de traffic et d'optimiser les performations du réseau en fonction des besoins spécifiques de chaques zone. (Voir Figure 4.18)

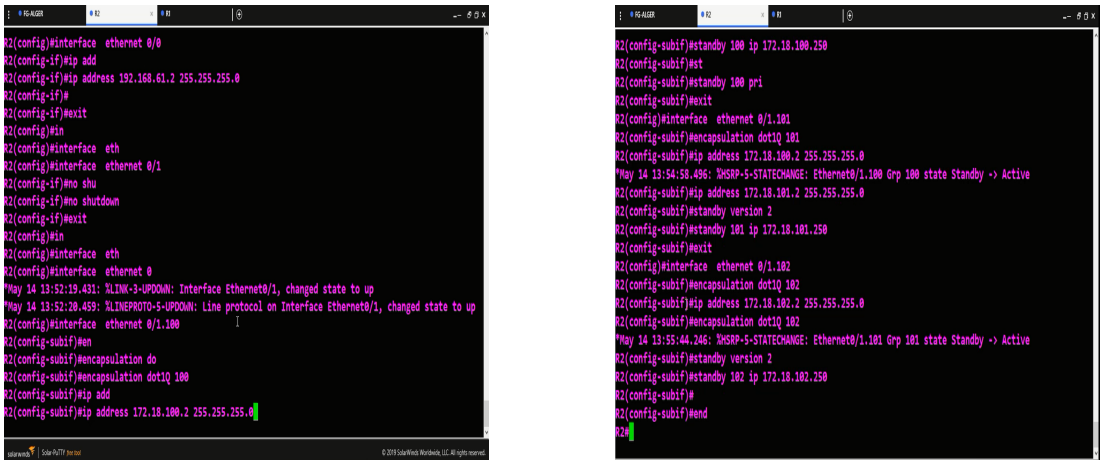


FIGURE 4.16 – Configuration du routeur R2 du Alger

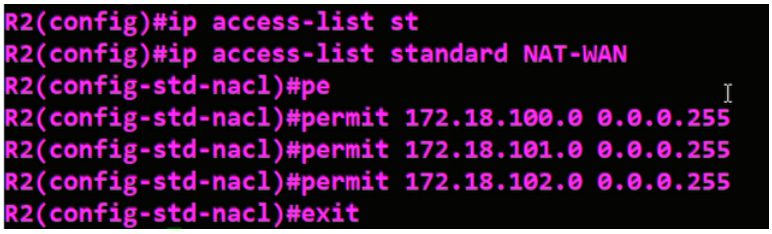


FIGURE 4.17 – Création du NAT et autorisation des VLANs à se connecter.

Nous avons utilisé le protocole HSRP entre les routeurs R1 et R2 pour la redondance.

Tableau d'adressage HSRP du routeur R2

Ce tableau résume l'adressage HSRP que nous avons fait dans le routeur R2.

Interface	Groupe	Priorité	Statut	Active	IP Virtuele
Ethernet0/1.100	100	100	Standby	172.18.100.1	172.18.100.250
Etherneth0/1.101	101	100	Standby	172.18.101.1	172.18.101.250
Ethernet0/1.102	102	100	Standby	172.18.102.1	172.18.102.250

TABLE 4.1 – Tableau d'adressage HSRP du routeur R2.

(c) **Routeur R1 (Port2) :** Le routeur R1 est le routeur prioritaire, donc nous avons lui donné une addresse IP, le router vers internet et créer le routage interVLAN et HSRP avec la priorité 150 pour que nous montrons que c'est le routeur actif, et sans oublier la configuration du NAT exactement comme le routeur2. (Voir Figure 4.19)

Tableau d'adressage HSRP du routeur R1 : Nous avons résumé le routage HSRP du routeur R1 dans un tableau d'adressage.

Interface	Groupe	Priorité	Statut	Standby	IP Virtuele
Ethernet0/1.100	100	150	Active	172.18.100.2	172.18.100.254
Etherneth0/1.101	101	150	Active	172.18.101.2	172.18.101.254
Ethernet0/1.102	102	150	Active	172.18.102.2	172.18.102.254

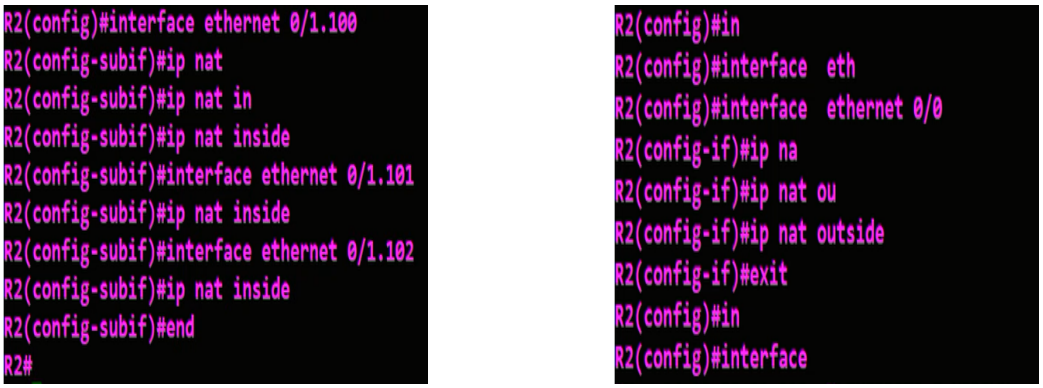


FIGURE 4.18 – Les interface d'entrès et l'interface de sortie

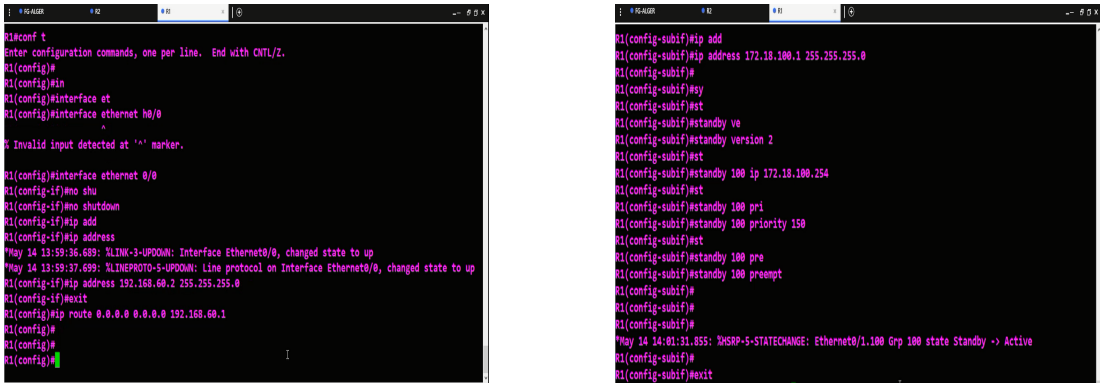


FIGURE 4.19 – Configuration du routeur1

TABLE 4.2 – Tableau d'adressage HSRP du routeur R1.

Configuration du protocole DHCP : Nous avons employé le protocole DHCP pour l'attribution dynamique des addresses IP aux VLANs (100, 101, 102) pour les deux routeurs. (Voir Rigure 4.20)

(d) **Switch1 et Switch2**

Configuration des VLANs : Nous avons configuré les trois VLANs et nous les avons affecté aux ports qui convients. (Voir Figure 4.21)

Configuration du mode trunk : Les liens trunks au niveau des deux switchs d'acées sont configurés comme le montre la figure4.22.

Le mode trunk est géneralement utilisé avec des protocoles de regroupement de liens tels que LACP (Link Aggregation Control Protocol).

Configuration du protocole LACP entre les deux switchs : Nous commençons par lancer le protocole CDP entre les deux switchs pour que nous verrons les intrfaces reliées directement à l'autre switch. (Voir Figure 4.23)

Puis nous avons fait un groupe de même numéro dans chaque switch qui porte le groupe actif de LACP. (Voir Figure 4.24a)

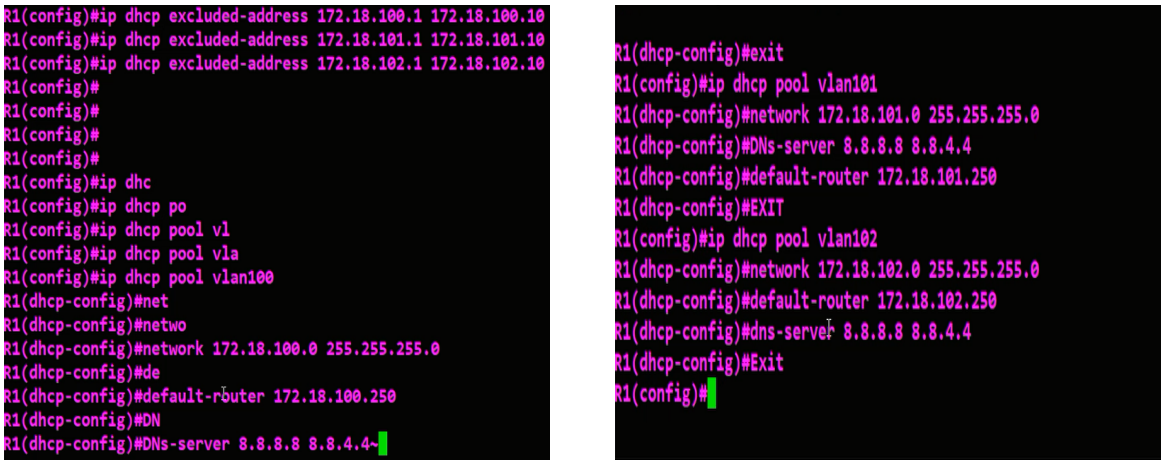


FIGURE 4.20 – Configuration du protocole DHCP

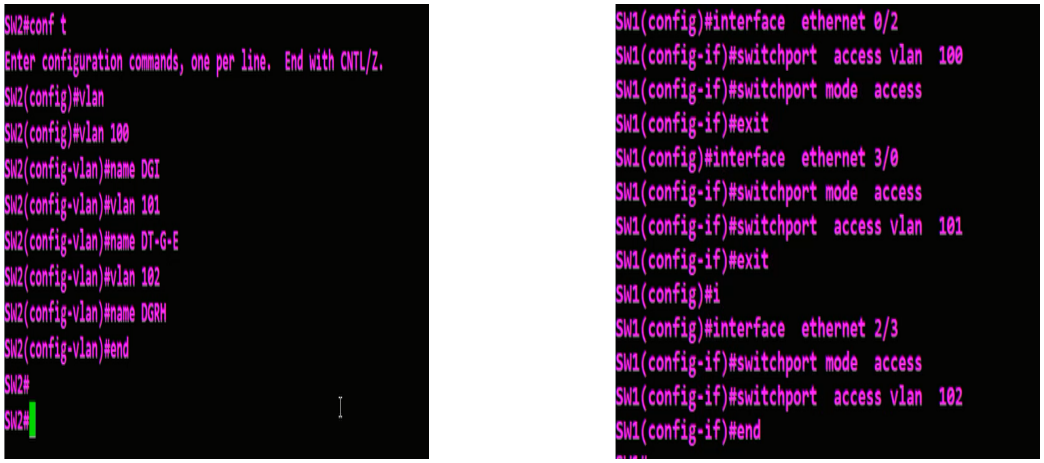


FIGURE 4.21 – Configuration des VLANs du site d'Alger

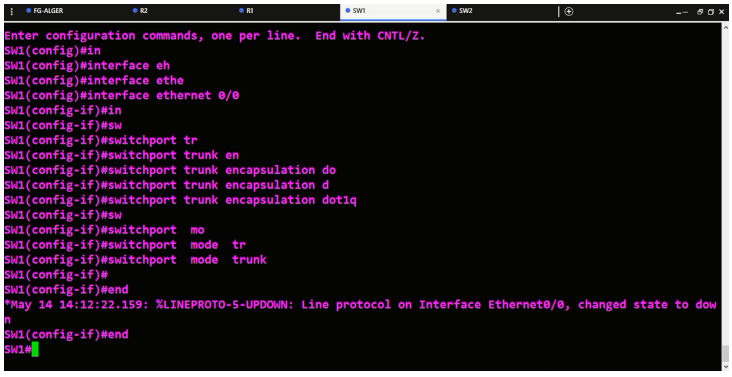


FIGURE 4.22 – Configuration de mode trunk.

Après nous avons effectué l'agrégation et l'équilibre de charge avec les addresses sources destinations MAC. (Voir Figure 4.24b)

3. **Site de sétif**

   Représenté par :

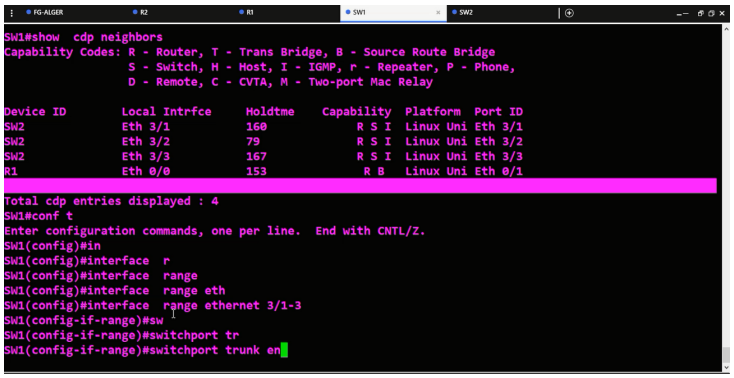
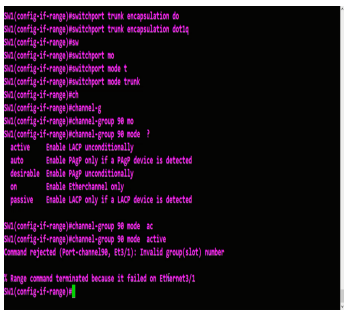
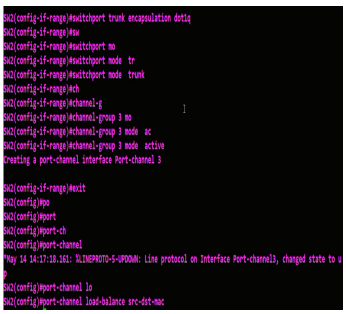


FIGURE 4.23 – Le protocole CDP entre les deux switchs.



(a) Configuration du protocole LACP



(b) L'agrégation et l'équilibre de charge

(a) **Un routeur** pour lequel nous avons attribué deux interfaces une relié au réseau LAN par un switch et l'autre à un réseau WAN. voici la configuration du routeur 4.25

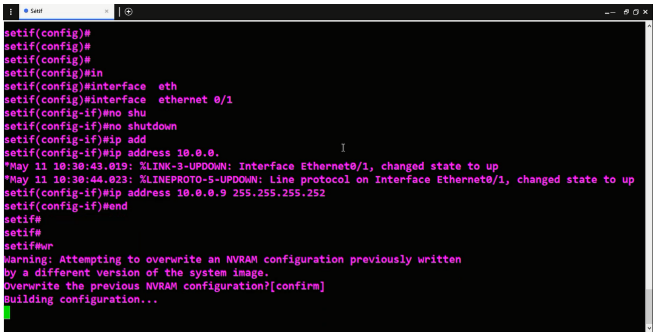


FIGURE 4.25 – Configuration du routeur de sétif.

(b) **Un switch :**Qui est relié au PC.

4. **Site de Constantine**

   Représenté par :

   (a) **Un firewal (Fortigate)** pour lequel nous avons attribué deux interfaces une relié au réseau LAN par un switch et l'autre à un réseau WAN.

La configuration du fortigate : La première étape consiste à renomer le fortigate par "FG-CONSTANTINE", puis lui attribuer une adresse IP et autoriser l'accès à travert le ping, http, https et ssh. (Voir Figure 4.26)

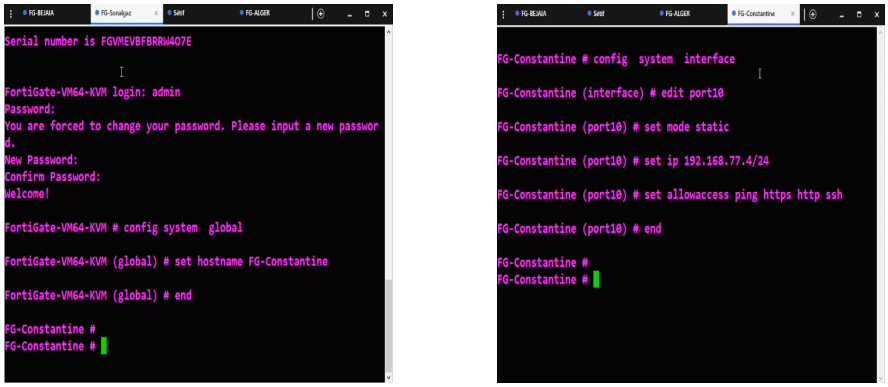


FIGURE 4.26 – Configuration du firewal de Constantine

On se place ici dans le tableau de bord, pour configurer l'interface WAN sur le port 1 il faut passer par [Système Management]->[Network]->[Interface]. (Voir Figure 4.27)

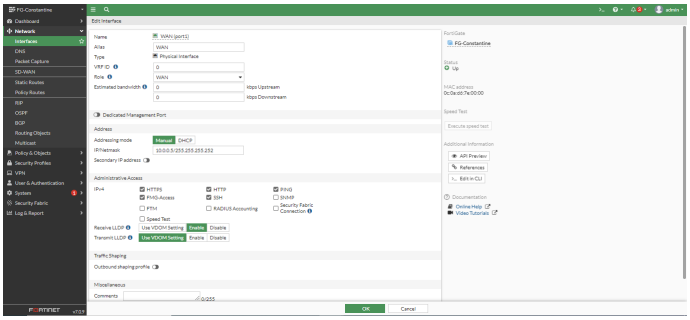


FIGURE 4.27 – Configuration du port 1 de firewal de Constantine.

Maintenant nous configurons le port 2 où se trouve le réseau LAN2. (Voir Figure 4.28)

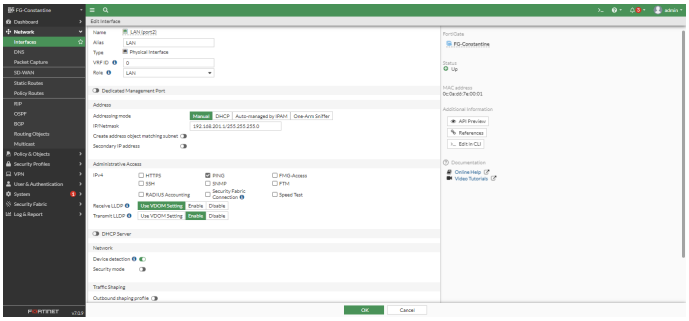


FIGURE 4.28 – Configuration du port 2 de firewal de Constantine

Création de la route statique vers le réseau Internet

La méthode est déja illustré dans les deux sites précidents.

La gateway :10.0.0.6 (Voir Figure 4.29)

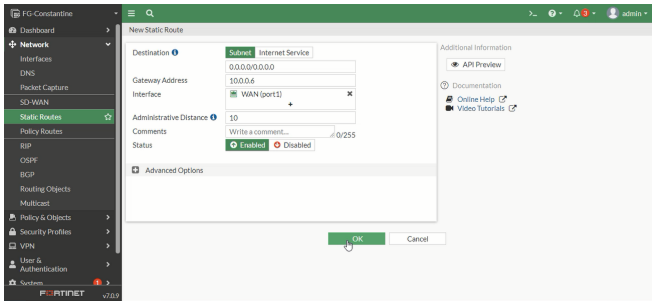


FIGURE 4.29 – Création de la route statique de Constantine vers l'Internet.

Autorisation de la connexion du fortigate vers l'Internet

Ici on autorise le site de constantine à se connecter à l'internet. (Voir Figure 4.30)

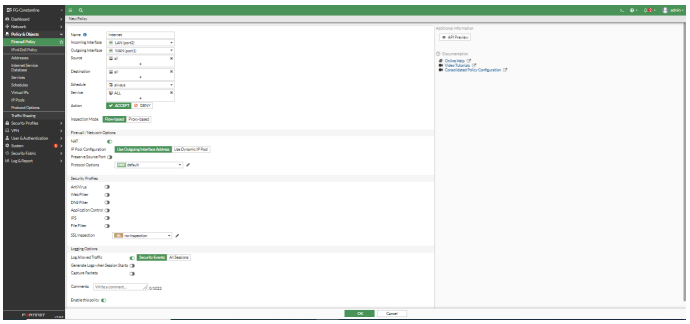


FIGURE 4.30 – Autorisation du fortigate de constantine de se connecter à l'internet.

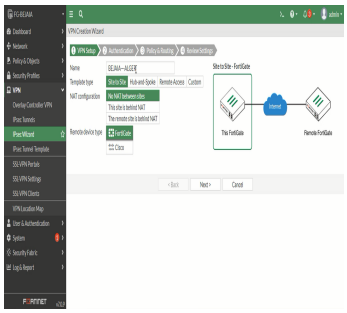
(b) **Un switch**

4.3.2 Création des tunnels IPsec

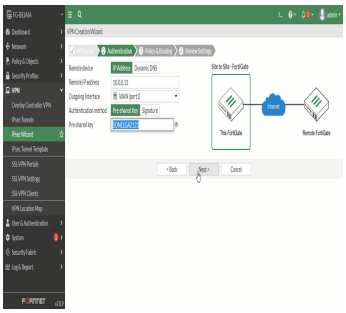
1. **Tunnel VPN entre Bejaia-Alger** Pour créer un tunnel IPsec entre Bejaia et Alger d'une façon automatique nous allons sur le fortigate de Bejaia à travers un serveur Web après on suit les étapes suivantes : [VPN]->[IPsec Tunnels] puis on clique sur "Create New" et on choisi "IPsec Tunnel". Maintenant on se retrouve dans une page qui s'appelle "VPN creation Wizard, nous passerons par quatre étapes :

   Etape 1 : "VPN Setup" dans laquelle nous introduissons le nom de tunnel, son type, l'utilisation du NAT et le type de l'équipement qui existe à Alger, puis on clique sur "next". (Voir Figure 4.31a)

   Etape 2 : "Authentification" dans laquelle nous choisissons le type d'addresse (static ou dynamique),pius on ajoutons l'adresse IP du port WAN et un mot de passe sécurisé (la clé privé) qui va décoder les données dans les deux cotés. (Voir Figure 4.31b)



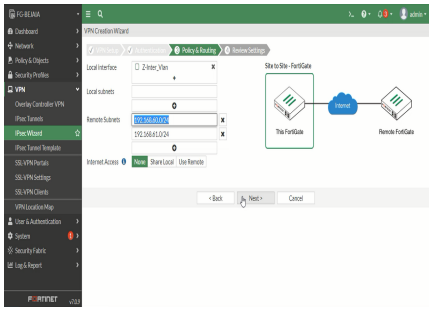
(a) Etape 1.



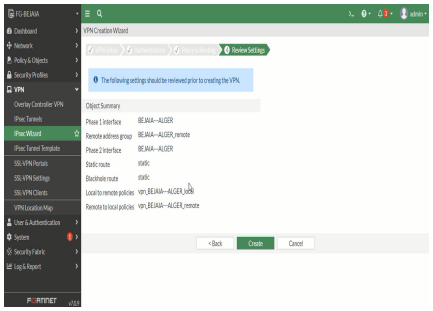
(b) Etape 2.

Etape 3 : "Policy and Routing" dans laquelle nous introduisons les interfaces locales qui vont sortir à l'extérieur, dans notre cas c'est l'interVLAN, puis on peut spécifier l'adresse des VLANs qu'ils sortiront sinon on laisse la case vide si on veut qu'il sortira tout l'interVLAN. Après on doit entrer les adresses des réseaux à distance de Alger qui vont se connecter à bejaia, puis next. (Voir Figure 4.32a

Etape 4 : c'est la dernière étape de la création, dans la dernière les deux phases qui vont être afficher : phase 1 pour l'échange de clés, phase 2 pour le cryptage des données à l'interieur de tunnel, puis "create". (Voir Figure 4.32b)



(a) Etape 3



(b) Etape 4

Enfin le tunnel IPsec est crée. Voici la création dans la figure 4.33.

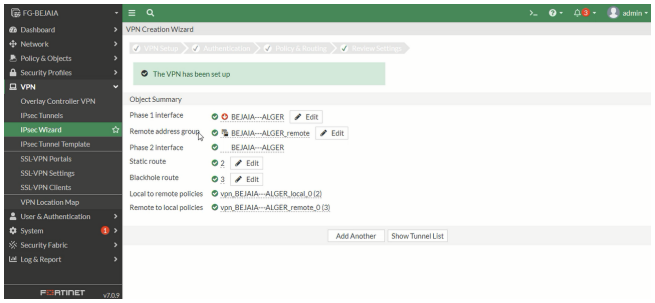


FIGURE 4.33 – Résultat de la création de tunnel entre Bejaia et Alger.

Ensuite On clique sur "Show Tunnel List" pour faire des modifications dans le tunnel. Dans l'authentification on peut rendre le mot de passe crypté en cliquons sur la version 2 de chiffrement. (Voir Figure 4.34

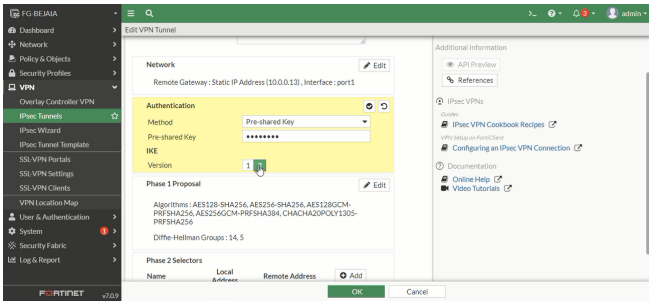


FIGURE 4.34 – Le cryptage de la clé de tunnel Bejaia-Alger.

Dans la phase 1 nous modifierons le chiffrement de cryptage, celui de l'authentification et le groupe de Diffie-Hellman . (Voir Figure 4.35)

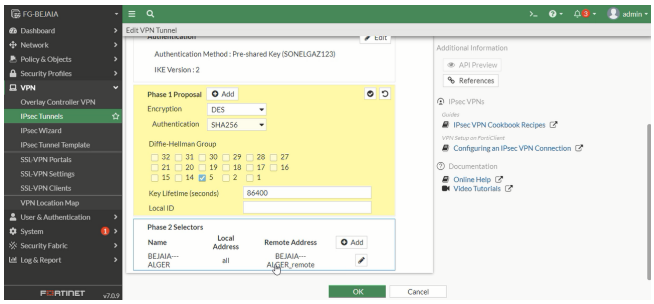


FIGURE 4.35 – La modification de la phase 1 de tunnel Bejaia-Alger.

Dans la phase 2 on fera les mêmes modification qu'on a fait dans la phase 1.

2. **Tunnel VPN entre Alger-Bejaia** Pour la création de tunnel Alger-Bejaia nous avons accédé au fortigate de Alger et nous avons fait les mêmes étape de création et les mêmes modification qu'on a fait dans le tunnel BEJAIA-ALGER. Voici une figure qui illustre la création 4.36.

3. **Tunnel VPN entre Constantine-Alger** Pour créer un tunnel IPSec de Constantine à Alger d'une façon manuelle, nous avons exécuté la premiere étape comme la création de tunnel Bejaia-Alger. (Voir Figure 4.37)

Puis nous pouvons personnalisé en cliquant sur "Custom" et de là on peut créer notre tunnel manuellement sans passer par les étapes ilustrés dans le tunnel Bejaia-Alger. (Voir Figure 4.38

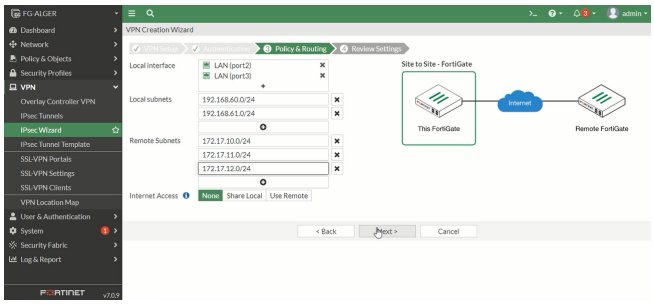


FIGURE 4.36 – Création de tunnel ALGER-BEJAIA.

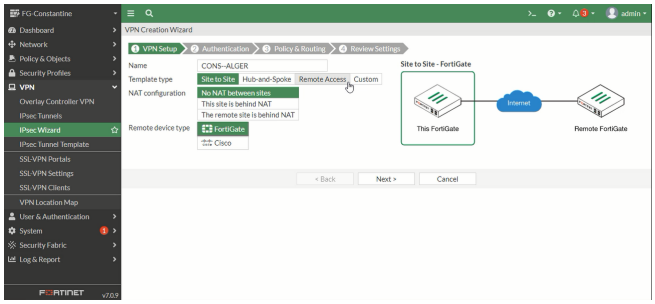


FIGURE 4.37 – Première étape de la création de tunnel Constantine-Alger.

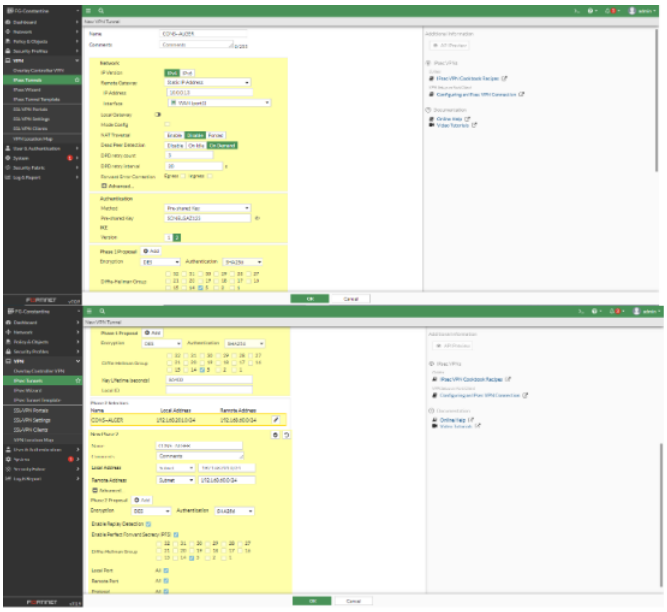


FIGURE 4.38 – Configuration de tunnel Constantine-Alger.

Dans l'étape précédante nous avons saisie l'addresse à distance "Remote address" d'un seule réseau LAN de Alger.

Donc on doit retourner à la phase 2 pour rajouter l'addresse du dexième réseau. (Voir Figure 4.39)

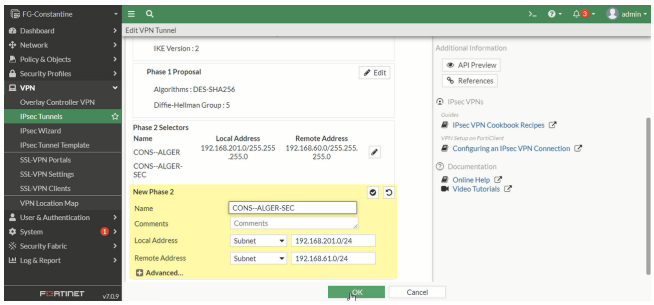


FIGURE 4.39 – Attribution de l'addresse à distance.

La seule différence dans cette méthode c'est qu'on doit créer le routage manuellemet . Pour celà nous allons sur [Network]->[Static Route]. Et nouis créerons deux routes statiques.
La première route de tunnel au premier réseau LAN distant de Alger. (Voir Figure 4.41)

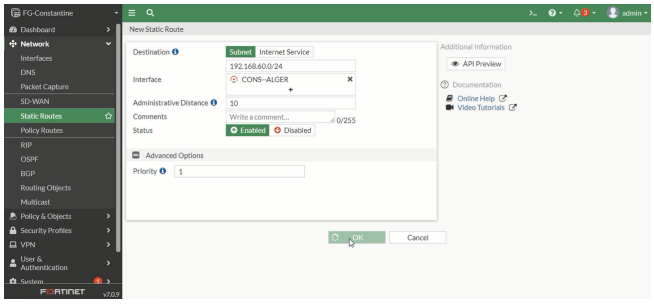


FIGURE 4.40 – Création de la première route statique de tunnel Constantine-Alger.

La dexième route statique de tunnel Constantine-Alger s'adresse à le deuxième réseau LAN de Alger. (Voir Figure 4.41)

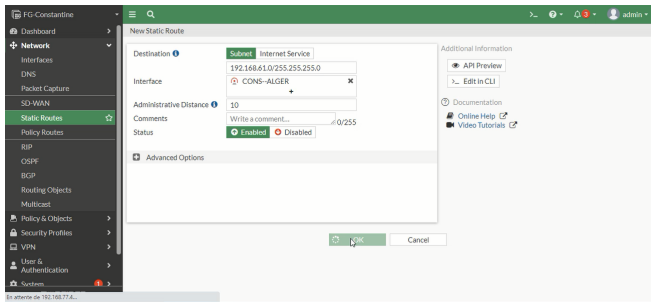


FIGURE 4.41 – Création de la deuxième route statique de tunnel Constantine-Alger.

Concernant les politiques de sécurité nous avons créé deux policies .
Une policie entrantes"IN" de réseau LAN au tunnel Constantine-Alger.(Voir Figure 4.42)

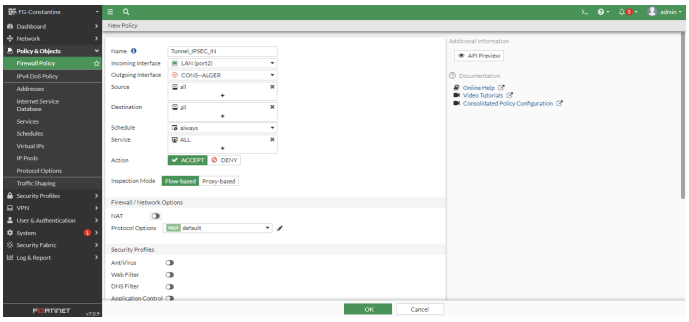


FIGURE 4.42 – Création d'une policie entrante de tunnel Constantine-Alger.

Et une policie sortante "OUT" de tunnel Constantine-Alger au réseau LAN. (Voir Figure 4.43)

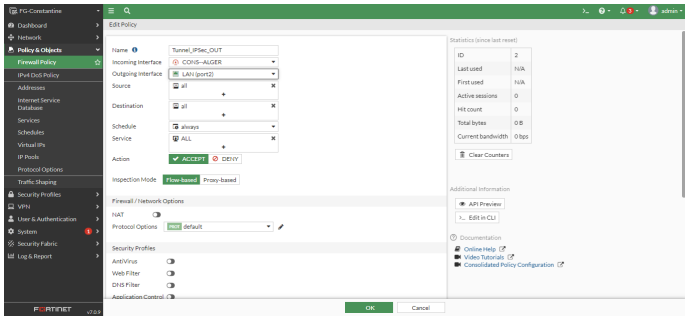


FIGURE 4.43 – Création d'une policie sortante de tunnel Constantine-Alger.

4. **Tunnel VPN entre Alger-Constantine** Pour le tunnel Alger-Constantine nous ferons les mêmes étapes q'on a fait sur le tunnel Constantine-Alger sur le fortigate de Alger, Voici une figure qui illustre la configuration de tunnel. 4.44

Après on a continué à créer une route statique de constantine au tunnel Ager-Constantine et deux policies d'entrés"IN1" port le port2 ET "IN2" pour le port3 de Alger et une policie de sortie "OUT".

4.3.3 Création de tunnel GRE

Tunnel GRE Sétif-Bejaia Pour créer ce tunnel il faut accéder au routeur de sétif, nous créerons une interface "tunnel 1", l'attribuer une addresse IP, lui donner l'addresse source de routeur de sétif et l'addresse destination de fortigate de Bejaia et donner aussi les routes vers les trois VLANs de Bejaia. (Voir Figure 4.45)

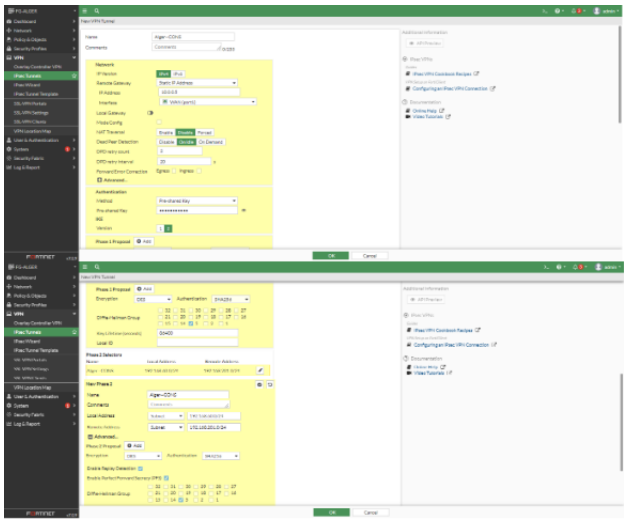


FIGURE 4.44 – Création de tunnel Alger-Constantine.

```
setif(config)#interface Tunnel1
setif(config-if)# ip address 10.10.10.2 255.255.255.252
setif(config-if)# ip mtu 1400
setif(config-if)# ip tcp adjust-mss 1360
setif(config-if)# tunnel source 10.0.0.9
setif(config-if)# tunnel destination 10.0.0.1
setif(config-if)#end
setif#
setif#conf t
*May 20 08:46:37.815: %SYS-5-CONFIG_I: Configured from console by console
setif#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
setif(config)#ip route 172.17.10.0 255.255.255.0 10.10.10.1
setif(config)#ip route 172.17.11.0 255.255.255.0 10.10.10.1
setif(config)#ip route 172.17.12.0 255.255.255.0 10.10.10.1
setif(config)#
setif(config)#end
```

FIGURE 4.45 – Configuration de tunnel Sétif-Bejaia.

Tunnel GRE Bejaia-Sétif Grace à la commande "config system gre-tunnel"qu'on va l'utiliser sur le fortigate de Bejaia on peut spécifier divert paramètres pour configurer le tunnel GRE. Donc on va créer un tunnel "GRE-B-S" qui sort de Bejaia(port1) vert Sétif .(Voir Figure 4.59)

Pour terminer la configuration de tunnel GRE entre Sétif et Bejaia on ajoutons sur le fortigate de Bejaia les policies du firewal "IN" et "OUT" et une route statique de sétif vert le tunnel.

4.3.4 Création de tunnel SSL

La création de tunnel SSL se résume en indiquant l'interface et le port, la création d'une certificat avec l'interface publique et le DHCP lui donne les addresses par défaut. (Voir Figure 4.47)

Nous créerons un groupe VPN-SSL. (Voir Figure 4.48)

Création d'une policie SSL Nous créerons une politique de sécurité qui porte le nom "SSL-VPN" qui va etre de tunnel SSL au réseau externe. (Voir Figure 4.49)

Création d'une connexion VPN SSL Al'utilisation de l'application FortiClient Nous pouvons créer facilement des utilisateur pour se connecter à distance.

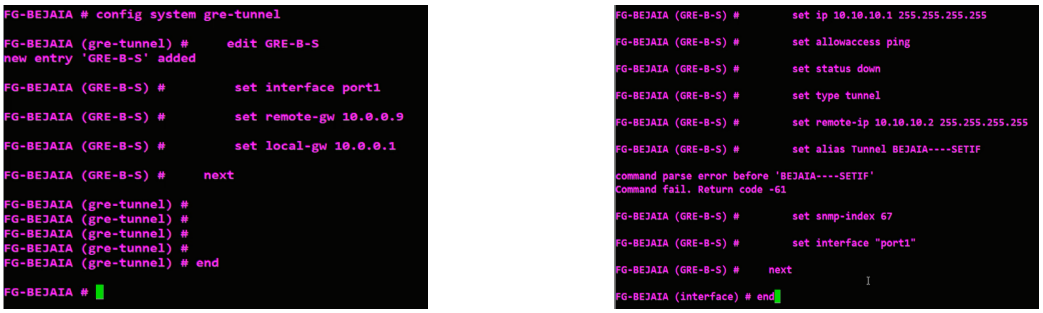


FIGURE 4.46 – Configuration de tunnel Bejaia-Sétif

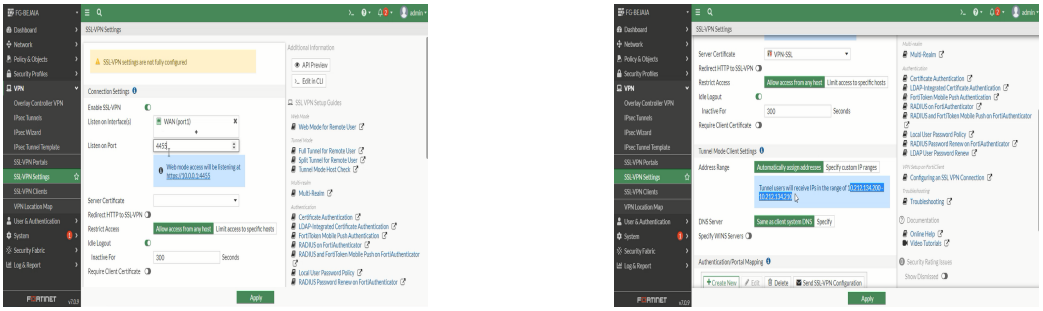


FIGURE 4.47 – Création de tunnel SSL

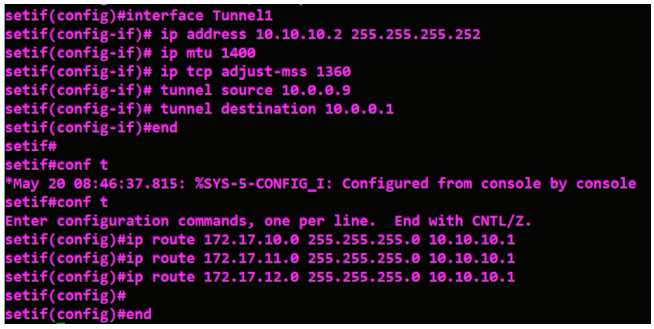


FIGURE 4.48 – Configuration de tunnel Sétif-Bejaia.

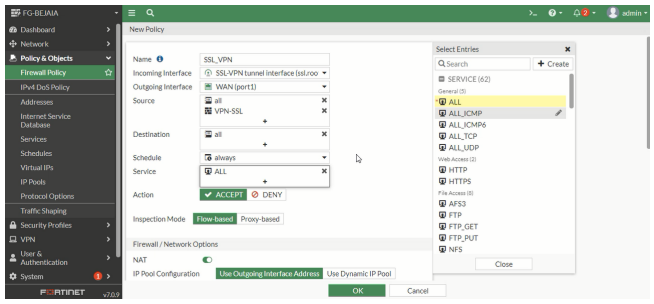


FIGURE 4.49 – Création d'une policy SSL.

4.3.5 Configuration de l'Active Directory(AD)

La première étape consiste à configurer le nom de la machine et l'addresse du serveur local (Voir Figure 4.51

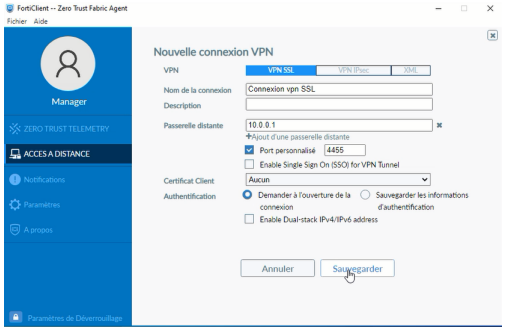


FIGURE 4.50 – Création d'une connexion VPN SSL.

- Nom de la machine est SER-AD
- L'adresse IPv4 c'est une adresse statique de classe C : 172.17.10.100

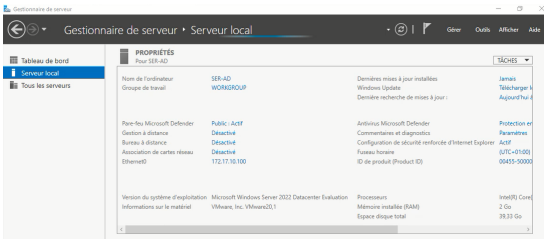


FIGURE 4.51 – Configuration du serveur local

La deuxième étape comprend l'ajout du role d'Active Directory au serveur local , pour cela nous allons(Voir Figure 4.52)

- Depuis le gestionnaire de serveur,cliquer sur ajouter des roles et fonctionalités.
- Sélectionner le type d'installation "installation basée sur un role ou fonctionnalité".
- Notre serveur est le seule du réseau, le choisir dans le pool de serveurs.
- Cocher le role service AD DS (Active Directory Domain Service).

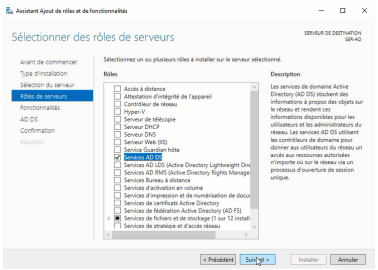


FIGURE 4.52 – L'ajout du role AD DS.

Après l'installation d'Active Directory Domain Service, le système va se redémarrer automatiquement, l'assistant nous demande de créer une nouvelle foret sous le nom (Voir Figure 4.53)

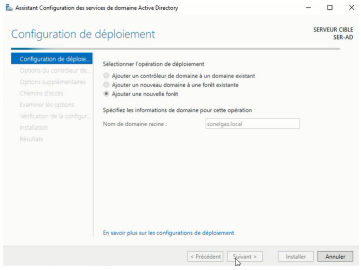


FIGURE 4.53 – L'ajout d'une nouvelle foret

L'orsque la foret et le domaine seront créés, le niveau fonctionnel de la nouvelle foret est sélectionné par défaut, et nous laissons cocher l'ajout de la fonctionnalité du serveur DNS. Puis insérer le mot de passe du mode de restauration du service d'annuaire (Voir Figure 4.54)

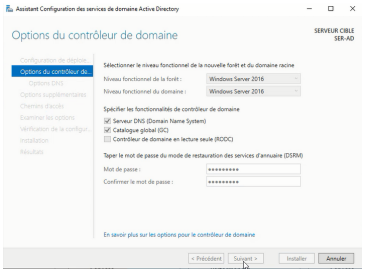


FIGURE 4.54 – Option de controleur de domaine.

Après la configuration, le serveur redémarre automatiquement. A présent, les outils de gestion d'Active Directory sont présents dans le menu outils, notre domaine est crée et l'ouverture d'une session s'effectue avec le compte d'administration du domaine SONELGAZ \ Administrateur.(Voir Figure 4.55)

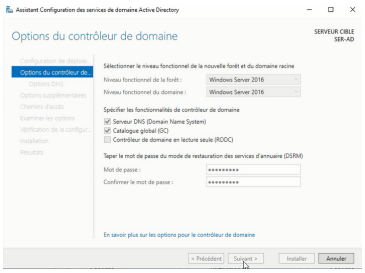


FIGURE 4.55 – Ouverture de la session Administration.

4.3.6

4.3.7 Tableau d'adressage des vlans et le routage inter-VLANs

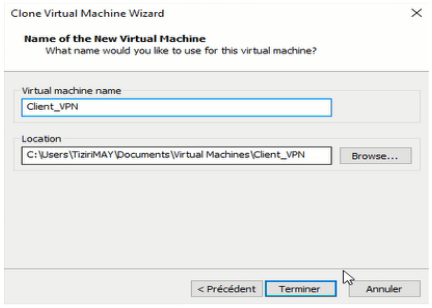
Dans ce tableau nous citons les Vlans qui existent dans les deux sites Bejaia et Alger.

Nom du VLAN	ID du VLAN	Adresse IP	Gteway
VLAN 10 DGI	10	172.17.10.0/24	
VLAN 11 DT-G-E	11	172.17.11.0/24	
VLAN 12 DGRH	12	172.17.12.0/24	
VLAN 100 DGI	100	172.18.100.0/24	
VLAN 101 DT-G-E	101	172.18.101.0/24	
VLAN 102 DGRH	102	172.18.102.0/24	

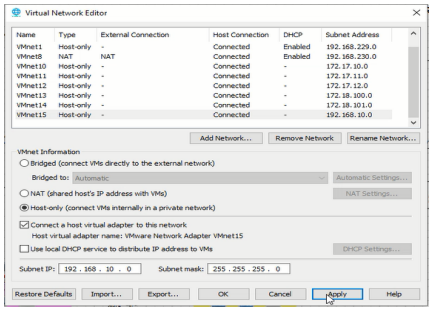
TABLE 4.3 – Tableau d'adressage des VLANs et le routage inter-VLANs.

4.3.8 Création d'un client VPN

Dans le Vmware nous clonerons un autre PC pour créer une intrface virtuelle et nous l'apelons Client-VPN.(voir Figure 4.60)
Après nous l'attribuons une addresse IP à l'interface et la carte réseau qui convient.(Voir Figure 4.56b)



(a) Création du client-VPN



(b) Attribution d'une addresse

4.4 Création d'un tunnel VPN IPsec "Client to site"

En accédons au fortigate de Bejaia, nous allons crée un tunnel Client to Site et l'attribuons un mot de passe. (Voir Figure 4.57)
Dans l'étape prècedente nous avons besois d'un groupe VPN, (Voir la figure 4.58a) qui se constitue des utilisateurs VPN qu'on doit les créer comme la figure 4.58b le montre.
Après nous ajoutons les utilisateurs VPN que nous avons créer au groupe.
La prochaine étape nous attribuons l'interface intervlan de Bejaia comme une interface locale et le pool d'adressage. (Voir Figure 4.59)

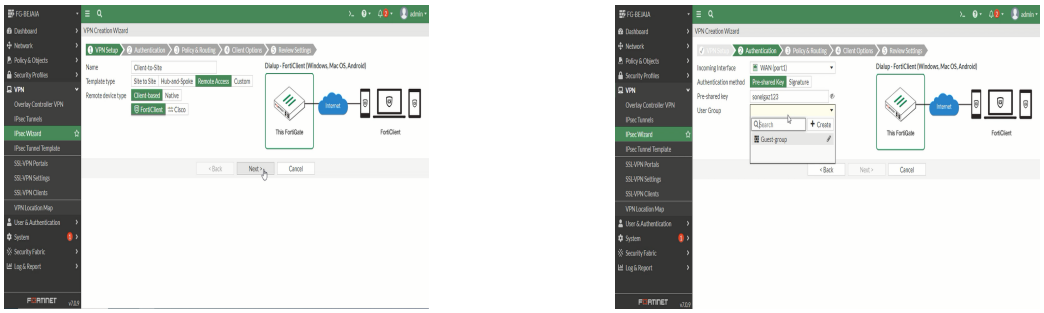
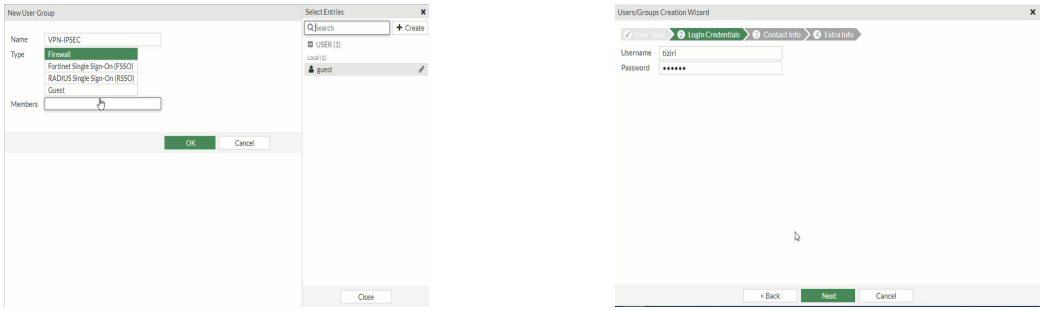


FIGURE 4.57 – Création et sécurisation de tunnel IPsec Client to site



(a) Création d'un groupe VPN (b) Création d'un utilisateur VPN

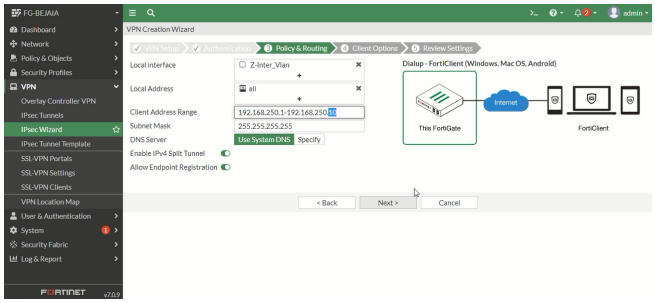


FIGURE 4.59 – Attribution des addreses au tunnel.

4.5 Configuration VPN à travers l'application FortiClient

Nous accéedons à l'application puis cliquons sur "Acces à distance", après choisissons VPN IPsec et remplissons les informations qui sont dans la figure 4.60

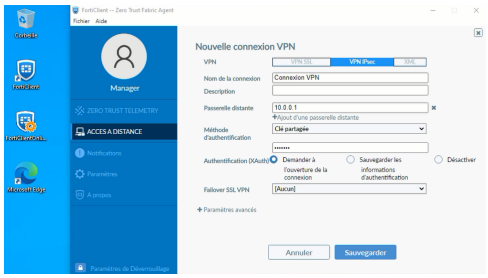


FIGURE 4.60 – Configuration VPN.

Connecter les clients au réseau VPN

Pour connecter un client au réseau il s'agit d'intoduire toutes les informations illustré dans la figure 4.61

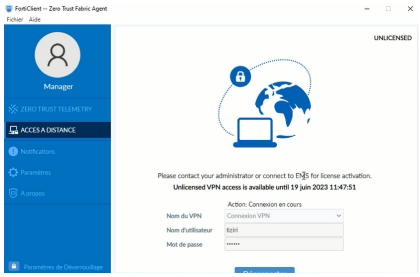


FIGURE 4.61 – Connexion des clients.

Après la connexion une page qui va s'afficher, Pour montrrer que le VPN est bien connecté.(Voir Figure4.62)

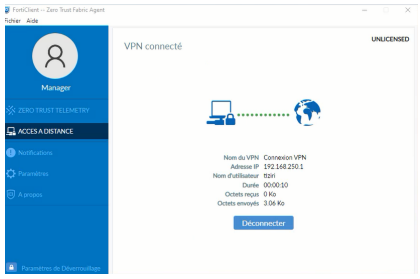


FIGURE 4.62 – Connexion des clients.

En but de visualiser et d'analiser le traffic réseau sécurisé entre un client et un serveur nous faisons une capture Wireshark pour le protocole ESP

La capture ESP sur wireshark Pour faire la capture il s'uffit juste d'aller sur l'architecture et de cliquer un clique droit sur un tunnel qui est reliè au réseau WAN, puis nous choisissons "Start Capture"et directement la capture se déclenche (Voir Figure 4.63)

Les communication entre le client et le serveur sont chiffrés grace au protocole ESP

4.6 Partie test

4.6.1 Les tests de site de bejaia

Nous vérifions la connexion vers le site de Béjaia en effectuant un ping à partir de PC CLIENT-VPN avec l'adresse IP «10.0.0.1» et la connexion intrnet à partir d'un PC CLIENT-VPN (Voir Figure4.64)

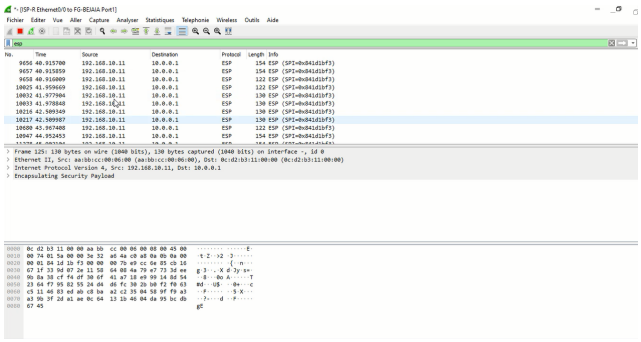


FIGURE 4.63 – La capture de protocole ESP sur Wireshark.

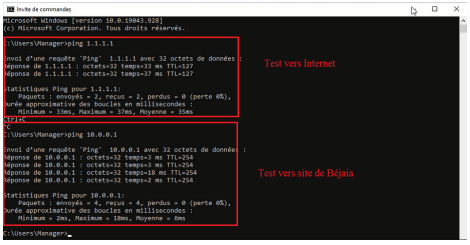


FIGURE 4.64 – Ping entre CLIENT-VPN et Bejaia .

4.6.2 Les tests de site d'Alger

A partir du firewal d'Alger nous vérifions la connection avec le site de Bejaia. (Voir Figure 4.65)

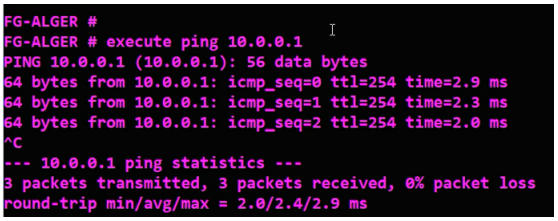


FIGURE 4.65 – Ping entre Alger et Bejaia.

Nous faisons un test DHCP d'un PC d'Alger. (Voir Figure 4.66)

FIGURE 4.66 – Test DHCP.

4.6.3 Les Tests de site de Sétif.

Nous vérifions la connectivité du routeur de Sétif avec chaque VLAN de Bejaia

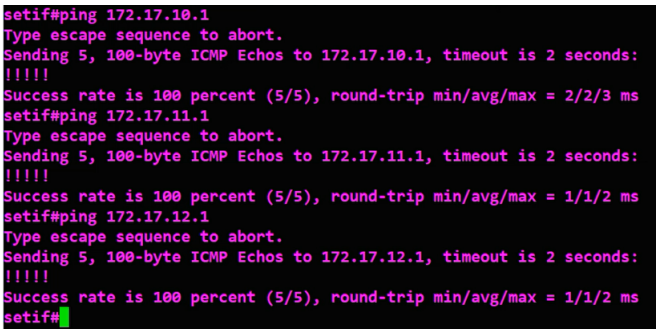


FIGURE 4.67 – Test entre le site Sétif et INTER-VLAN BEJAIA.

4.7 Conclusion

Au cours de ce chapitre, nous avons abordé la phase implémentation de notre projet, nous avons débuté par présenter les outils que nous avons utilisés, à savoir GNS3 et VMWARE, pour créer notre environnement de travail. Ensuite, nous avons détaillé les différentes étapes de configuration des solutions proposées, en mettant l'accent sur les aspects liés à la sécurité. Enfin, nous avons effectué des tests afin de s'assurer du bon fonctionnement de nos configurations.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

Au terme de ce projet, nous avons pu exploiter nos connaissances théoriques et pratiques pour étudier l'architecture réseau de l'entreprise SONELGAZ de Bejaia et maître en place une amélioration à cette dernière. Ainsi, Après la présentation du présent projet suivie de l'étude générale de l'architecture réseau de SONELGAZ, Nous avons élaboré une solution à retenir pour avoir une architecture mieux adaptée aux besoins de l'entreprise, qui répond à un pourcentage important aux exigences de sécurité et nous avons pu mettre en œuvre quelques-unes.

La mise en place du réseau local virtuel (VLAN) nous a permis de segmenter le réseau de SONELGAZ, afin d'augmenter les performances du réseau et remédier aux attaques qui peuvent se produire à l'intérieur de l'entreprise. La mise en place de VPN site-à-site placés dans une entreprise permet aux réseaux privés de se relier et de s'étendre entre eux a travers internet en toute sécurité ainsi que la réduction du coût des infrastructures réseaux, cette dernière est basée sur le protocole IPsec est considérée comme l'un des facteurs clés de réussite qui sont en constente évolution, ainsi nous avons implémenté le protocole GRE permet d'établir une connexion fiable et efficace entre les différentes partie d'une infrastructure réseau .

En conséquence, nous avons exposé un travail divisé en deux grandes parties, à savoir l'approche théorique sur les généralités à propos des réseaux informatiques, la sécurité informatique et VPN où nous avons basé de façon claire sur les notions, le fonctionnement ainsi que les différents protocoles utilisés pour la mise en œuvre de réseau VPN et quant à la deuxième partie, elle est consacrée à la finalisation du projet, laquelle nous avons solutionné par une solution VPN site-à-site qui consiste à mettre au point une liaison permanente, distante et sécurisée entre sites du SONELGAZ à savoir Béjaia, Alger, Setif, Constantine et aussi nous avons segmenté le réseau local en plusieurs LAN virtuels, pour réduire les domaines de collisions et éviter les congestions. Ce qui permet de renforcer la sécurité au niveau du réseau local.

Pour la réalisation de ce travail, nous avons utilisé le GNS 3 avec le VMWARE WORKSTATION PRO 17 pour simuler l'architecture étudiée. Aussi nous avons présenté notre environnement de travail et les outils qui nous ont servi pour implémenter notre simulation et vérifier son bon fonctionnement.

En termes de perspectives, nous envisageons d'améliorer notre travail en implémentant une solution VPN IPsec afin d'améliorer la sécurité du réseau et se protéger contre les éventuelles attaques.

Ainsi que, ce mémoire nous a permis d'acquérir une expérience personnelle et professionnelle très bénéfique. Ce fut une occasion pour notre groupe de se familiariser avec l'environnement du travail et de la vie professionnelle, d'élargir et d'approfondir nous connaissances sur l'administration et sécurité des réseaux informatiques.

BIBLIOGRAPHIE

[1] cour sur les réseaux informatiques transmission de l'information spécialité si. *Lycée Jules Ferry Versailles*.

[2] cour sur notions de base sur les réseaux informatiques. *1ère année BTS SRI*.

[3] `https://www.ordinateur.cc/rÃ©seaux/Autre-RÃ©seaux-informatiques/78502.html.`, (Consulté le 03 Mars 2023).

[4] interêt de vpn. `https://www.journaldugeek.com/vpn/faq/avantages-inconvenients/.`, (Consulté le 03 Mars 2023).

[5] mongosukulu. `https://www.mongosukulu.com/index.php/contenu/informatique-et-reseaux/reseaux-informatiques/639-les-equipements-reseaux-informatiques.`, (Consulté le 03 Mars 2023).

[6] mongosukulu. `https://www.journaldugeek.com/vpn/faq/avantages-inconvenients/`, (Consulté le 03 Mars 2023).

[7] Site officiel de sonelgaz. `https://www.sonelgaz.dz/fr.`, (Consulté le 03 Mars 2023).

[8] `https://web.maths.unsw.edu.au/~lafaye/CCM/initiation/types.htm`, (Consulté le 1 Mars 2023).

[9] Jean-Paul Archier and Jean-Paul Archier. *Les VPN : fonctionnement, mise en oeuvre et maintenance des réseaux privés virtuels*. Editions ENI, 2013.

[10] Philippe Atelin. *Réseaux informatiques : notions fondamentales : normes, architecture, modèle OSI, TCP/IP, Ethernet, Wi-Fi,...* Editions ENI, 2009.

[11] Dr Nadjia Khatir.Dr Abdelkader Belhadri. cours sur les réseaux informatiques. *Ecole Supérieure en Génie Electrique et Energétique d'Oran*, 2021.

[12] Jean-François Carpentier. *La sécurité informatique dans la petite entreprise : l'état de l'art et bonnes pratiques*. Editions ENI, 2009.

[13] Joe Casad and Bob Willsey. *TCP/IP*. CampusPress France, 1999.

[14] MOINDJIE Said Mouhamed. cours sur les réseaux informatique, les équipements d'interconnexions. *site de la technologie*, consulté le 04 mars 2023.

[15] Mme Labraoui N. Sécurité informatique.chapitre 1 : Notions fondamentales. *Master 1 Réseaux et systèmes distribués*, 2020.

[16] préface de Michel .solange Ghrnaouti-Hélie. Sécurité informatique et réseaux. *2éme édition.*

RÉSUMÉ

Ce mémoire présente une étude approfondie sur la mise en place d'une politique de sécurité pour un VPN interconnectant plusieurs sites, reliant la direction générale de SONELGAZ à Alger avec les sites de Sétif, Béjaia et Constantine.
L'objectif principal de ce mémoire est de concevoir et de mettre en place une architecture de sécurité robuste pour le VPN à multi-sites, reliant efficacement les différentes entités de l'organisation. En utilisant des technologies telles que l'IPsec,le GRE,SSL et d'autre mécanisme de sécurité, nous visons à garantir un niveau élevé de protection des données et des communications au sein du réseau VPN et d'ouvrir un accés aux ressources de l'entreprise pour les utilisateurs situés en dehors de l'infrastructure de SONELGAZ grace à l'accée à distance par le tunnel client-to-site.
En conclusion ce travail propose une approche complète pour la mise en place d'une politique de sécurité avancée dans un environnement VPN à multi-sites. Les résultats et les recommandations présentés ici permettront aux organisations de renforcer leur sécurité, d'améliorer leur résiliences face aux menaces et de garantir la confidentialité des données sensibles dans leur réseau VPN.

Mots clés : GRE, IPsec, SONELGAZ, SSL, VPNs.

ABSTRACT

This thesis presents an in-depth study on the implementation of a security policy for a multi-site VPN, connecting the headquarters of SONELGAZ in Algiers with the sites in Sétif, Béjaia, and Constantine.
The main objective of this thesis is to design and implement a robust security architecture for the multi-site VPN, effectively connecting the different entities of the organization. By utilizing technologies such as IPsec, GRE, SSL, and other security mechanisms, we aim to ensure a high level of data and communication protection within the VPN network and provide access to company resources for users located outside the SONELGAZ infrastructure through remote client-to-site tunneling.
In conclusion, this work proposes a comprehensive approach for the implementation of an advanced security policy in a multi-site VPN environment. The results and recommendations presented here will enable organizations to strengthen their security, enhance resilience against threats, and ensure the confidentiality of sensitive data within their VPN network..

Key words : GRE, IPsec, SONELGAZ, SSL, VPNs.