République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire De Fin de Cycle

En vue d'obtention d'un diplôme de Master professionnel en

Informatique Spécialité : Administration et Sécurité des Réseaux

THÈME

Mise en place d'une architecture VPN MOBILE,

cas d'étude : Entreprise GPL NAFTAL de Bejaia

Réalisé par :

M^elle^ BORDJAH Nawal et M^elle^ BENHADDAD Zahra.

Soutenu devant les jurys composé de :

Président	**Mme. ALOUI Soraya**	**U. A/Mira Béjaïa.**
Examinateur	**M^r^. TOUAZI Djoudi**	**U. A/Mira Béjaïa.**
Encadrant	**Dr. YAICI Malika**	**U. A/Mira Béjaïa.**

Promotion 2021-2022

Remerciements

Nous tenons tout d'abord à remercier Dieu le tout puissant qui nous a donné la force et la patience d'accomplir ce modeste travail.

En second lieu, nous tenons à remercier notre encadrant M^{ME}**. YAICI MALIKA** pour avoir bien voulu nous accompagner tout au long de ce projet, pour son aide inestimable ses conseils et recommandations qui nous ont permis de réaliser ce travail. Qu'il trouve ici l'expression de notre profonde gratitude.

Et en formule de ce travail, nous tiendrons à remercier également le personnel de **NAFTAL** spécialement M.**CHEURFA HALIM** qui a eu l'amabilité de répondre à nos questions et de nous fournir ses précieux conseils.

Nos remerciements vont aussi à tous les membres de jury qui nous ont fait l'honneur d'accepter d'examiner ce travail et de l'enrichir.

Enfin nous tenons à remercier toutes les personnes qui ont contribué de près ou de loin au succès de ce présentprojet, trouvant aussi l'expression de nos profonds gratitudes et respects.

Dédicaces

Je dédie ce modeste travail à :

nos chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de notre études, A nos chères sœurs pour leurs encouragements permanents, et leur soutien moral, A notre chers frères pour leur appui et leur encouragement,

A toute notre famille pour leur soutien tout au long de notre parcours universitaire, Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible, Merci d'être toujours là pour nous.

Table des matières

Table des matières iv

Listes des abréviations vii

Introduction Géneral 1

1 Présentation de l'organisme d'accueil 3
- 1.1 Introduction . . . 3
- 1.2 Présentation de l'organisme d'accueil NAFTAL . . . 3
  - 1.2.1 **Historique de NAFTAL** . . . 3
  - 1.2.2 **Les activités principales de l'entreprise NAFTAL** . . . 4
  - 1.2.3 **Objectifs de l'entreprise NAFTAL** . . . 4
- 1.3 Présentation du district GPL NAFTAL Bejaia . . . 4
  - 1.3.1 **Les missions principales du District GPL** . . . 4
  - 1.3.2 **L'organigramme du District GPL** . . . 5
  - 1.3.3 Le rôle de chaque service de l'entreprise :[4] . . . 5
- 1.4 Etude du réseau informatique de l'entreprise : [4] . . . 6
  - 1.4.1 **Infrastructure matériel** . . . 6
  - 1.4.2 **Support de transmission** . . . 7
  - 1.4.3 **Gestion de la sécurité** . . . 7
  - 1.4.4 **Gestion des employés** . . . 9
  - 1.4.5 **Problématique et Solution proposée** . . . 9
- 1.5 conclusion . . . 9

2 La sécurité des réseaux informatique 10
- 2.1 Introduction . . . 10
- 2.2 Définition de sécurité des réseaux . . . 10
- 2.3 Les critères de sécurité . . . 10
  - 2.3.1 **Intégrité** . . . 11
  - 2.3.2 **Confidentialité** . . . 11
  - 2.3.3 **Non répudiation** . . . 11
  - 2.3.4 **L'authentification** . . . 11
  - 2.3.5 **Disponibilité** . . . 12
- 2.4 Terminologie de la sécurité informatique . . . 12
  - 2.4.1 **Vulnérabilité** . . . 12
  - 2.4.2 **Une attaque** . . . 12
  - 2.4.3 **Une contre-mesure** . . . 12

2.4.4 **Une menace** . . . 12
2.5 Les types d'attaques . . . 12
2.5.1 **Les attaques directes** . . . 12
2.5.2 Les attaques indirectes par rebond . . . 12
2.5.3 **Les attaques indirectes par réponse** . . . 13
2.6 Les éléments à sécuriser dans un réseau . . . 13
2.6.1 **Matériel** . . . 14
2.6.2 **Programme** . . . 14
2.6.3 **Données** . . . 14
2.7 La sécurité et Les solutions de la protection des données dans les transmissions [19] . . . 14
2.7.1 **Les solutions de sauvegarde** . . . 15
2.7.2 **Les connexions réseau** . . . 15
2.7.3 **Les mots de passe du disque dur** . . . 15
2.7.4 **Le chiffrement des données** . . . 15
2.8 Les dispositifs de protection . . . 15
2.8.1 **Antivirus** . . . 16
2.8.2 **Le pare-feu (firewall)** . . . 16
2.8.3 **Liste contrôle d'accès aux réseaux** . . . 16
2.8.4 **Les Réseaux Privé Virtual (VPN)** . . . 17
2.8.5 **Système de détection d'intrusion (IDS) [7]** . . . 17
2.8.6 **Le système de prévention d'intrusion (Intrusion Prévention System-IPS) :** . . . 18
2.8.7 **Le Proxy :** . . . 18
2.9 Conclusion : . . . 18

3 La généralité sur les réseaux privé virtuel(VPN) 19
3.1 Introduction . . . 19
3.2 Définitions des réseaux privés virtuel : . . . 19
3.3 Cas d'utilisation VPN . . . 19
3.4 Le fonctionnement des VPN : . . . 20
3.5 Les avantages des VPN[25] : . . . 20
3.6 Les inconvénients des VPN [26] : . . . 20
3.7 Les différents types des VPN : . . . 21
3.7.1 **VPN d'entreprise** . . . 21
3.7.2 **VPN operateur** . . . 23
3.8 Les protocoles de VPN : . . . 23
3.8.1 **Protocole PPP (Point To Point Protocol)** . . . 23
3.8.2 **Protocole PPTP (Point To Point Tunneling Protocol)** . . . 24
3.8.3 **ProtocoleL2F (Layer 2 Forwarding)** . . . 24
3.8.4 **Protocole L2TP (Layer 2 Tunneling Protocol)** . . . 24
3.8.5 **Protocole MPLS (Multi-Protocol Label Switching)** . . . 25
3.8.6 **Protocole SSL/ TLS (Secure Sockets Layer) / (Transport Layer Security)** . . . 25
3.8.7 **Protocole SSH (Secure Shell)** . . . 25
3.8.8 **Protocole IPSEC (Internet Protocol Security)** . . . 25
3.9 Les applications VPN existant . . . 25
3.9.1 **Open VPN** . . . 25
3.9.2 **Forticlient VPN** . . . 26
3.9.3 **Anyconnect Cisco** . . . 26

3.10 Conclusion 26

4 Configuration et Implémentation **27**
4.1 Introduction 27
4.2 Présentation de l'environnement de travail 27
4.2.1 **Installation de GNS3 sous Windows** 27
4.2.2 **Installation de VMware Workstation pro** 28
4.2.3 **Wireshark** 29
4.2.4 **Les machines virtuelles** 29
4.3 Architecture proposée 29
4.4 Tableaux des équipements d'interconnexion 30
4.5 Adressage 30
4.5.1 **Tableau d'adressage des équipements** 30
4.5.2 **Tableau des Vlans** 31
4.6 Configuration de base sur le serveur 32
4.6.1 **Distribuer une adresse IP fixe au serveur** 32
4.6.2 **Installer l'active directory dans le serveur** 32
4.6.3 **Configuration d'Active Directory** 33
4.6.4 **Installation de DHCP** 34
4.6.5 **Configuration DHCP** 35
4.6.6 **Configuration d'utile d'organisation NAFTAL** 38
4.7 Configuration infrastructure 40
4.7.1 **Configuration des ports au mode trunk** 41
4.7.2 **Configuration de Vlan Trunking Protocol (VTP)** 42
4.7.3 **Création les vlans** 43
4.7.4 **Affectation des ports pour les Vlans en mode accès** 45
4.7.5 **Configuration du routage inter_VLAN ET DHCP relais** . . 46
4.7.6 **Configuration de la route par défaut vers internet** 47
4.8 Configuration du Firewall 47
4.9 La configuration du serveur OpenVPN 51
4.9.1 **Création de certificat autorité (CA)** 52
4.9.2 **Création d'un certificat d'autorité "server"** 52
4.9.3 **Création des règles firewall pour le serveur et le client** . . . 54
4.9.4 **Téléchargement des applications pour les clients** 55
4.9.5 **Création d'un nouveau certificat pour l'utilisateur** 55
4.9.6 **La vérification des clients exportés** 57
4.10 Tests de configuration 57
4.10.1 **Test DHCP** 57
4.10.2 **La vérification de la connectivité** 58
4.10.3 **Ajouter l'utilisateur au domaine** 59
4.11 Tester la connectivité de routeur vers firewall 60
4.11.1 **Test de connection des clients OpenVPN (VPN Mobile)** . . 62
4.12 Conclusion 70

Conclusion générale **71**

Annexe **75**

Table des figures

1.1 Logo de l'entreprise NAFTAL . . . 3
1.2 L'organigramme du District GPL NAFTAL BEJAIA [4] . . . 5
1.3 Architecture du réseau GPL NAFTAL BEJAIA [4] . . . 8

2.1 Critères de sécurité [12] . . . 11
2.2 Attaque indirecte par rebond [13] . . . 13
2.3 Attaque indirecte par réponse [14] . . . 13
2.4 pare-feu (firewall)[11] . . . 16
2.5 Système de détection d'intrusion (IDS) [10] . . . 17

3.1 VPN site à site . . . 21
3.2 VPN poste à site [34] . . . 22
3.3 protocole L2TP [21] . . . 24

4.1 GNS3 . . . 28
4.2 L'interface graphique de VMware Workstation pro 16 . . . 28
4.3 L'interface graphique de wireshark . . . 29
4.4 Architecture de réseau proposée . . . 30
4.5 Configuration de serveur . . . 32
4.6 L'Installation active directory . . . 33
4.7 Les rôles AD DS et DNS . . . 34
4.8 Installation de DHCP . . . 34
4.9 Relier DHCP avec l'actif directory . . . 35
4.10 Nom et description de vlan . . . 35
4.11 Paramétrer les adresses des Vlan . . . 36
4.12 Exclusion des 10 premières adresses . . . 37
4.13 Les étendus des vlans configurer . . . 38
4.14 Création d'utile d'organisation . . . 38
4.15 Création d'utilisateur 1 . . . 39
4.16 Création d'utilisateur 2 . . . 39
4.17 Création de département commercial . . . 40
4.18 Relier les deux utilisateurs au département . . . 40
4.19 Configuration des interfaces aux mode trunk Switch distribution . . . 41
4.20 Configuration des interfaces trunk sur les switch d'Access . . . 42
4.21 Configuration de VTP en mode serveur . . . 42
4.22 Configuration de VTP en mode client . . . 43
4.23 création des vlans dans le switch SWD . . . 43
4.24 vérification des vlanscrées . . . 44

4.25 Affectation des ports pour les Vlans en mode accès . . . 45
4.26 Test d'affectation des ports au vlans . . . 45
4.27 Configuration du routage intervlan et dhcp relais . . . 46
4.28 Routage des Vlans vers l'internet . . . 47
4.29 Page d'accueil de pfsense . . . 47
4.30 configuration de pfSense . . . 48
4.31 changement de mot de passe . . . 48
4.32 changement du source de IPV4 . . . 49
4.33 Paramètre de Gateway vers les VLAN . . . 49
4.34 Création des routes vers les VLANS . . . 50
4.35 relier les VLANs vers l'internet . . . 50
4.36 interface de configuration du serveur openVPN . . . 51
4.37 Sélection de base de données locale . . . 52
4.38 1 Création de certificatautorité (CA) : . . . 52
4.39 Les informations générales sur le serveur openvpn . . . 53
4.40 Connexion de client vers infrastructure à travers internet . . . 53
4.41 Création des règles Firewall . . . 54
4.42 Création de serveur de connexion VPN . . . 54
4.43 téléchargement et L'installation openVPN . . . 55
4.44 Certificat user créer . . . 56
4.45 Création d'utilisateur zahra . . . 56
4.46 Certificat d'utilisateur zahra . . . 57
4.47 les clients Export . . . 57
4.48 Le pc a reçu une adresse ip Dynamic attribuer par le serveur dhcp . . . 58
4.49 Ping de pc vers serveur . . . 58
4.50 Joindre le domaine par l'utilisateur . . . 59
4.51 Les paramètres d'administrateur . . . 59
4.52 Ping routeur vers firewall . . . 60
4.53 Ping de serveur vers routeur et firewall . . . 61
4.54 Ping vers internet . . . 61
4.55 Installation openVPN . . . 62
4.56 Ping client vers internet . . . 63
4.57 Les paramètres d'utilisateur . . . 63
4.58 Utilisateur connecté . . . 64
4.59 Ping utilisateur vers serveur . . . 64
4.60 Test de création d'interface . . . 65
4.61 Création nouvelle session RDP . . . 65
4.62 Accès au serveur avec RDP . . . 66
4.63 les paramètres d'utilisateur Android . . . 67
4.64 l'utilisateur Android connecté . . . 68
4.65 Ping client Android vers serveur . . . 69
4.66 Vérification de connectivité sur firewall . . . 70
4.67 Vérification le trafic d'openVPN . . . 70

Liste des tableaux

1.1 Tableau les différentes caractéristiques de ces supports. 8

4.1 Les équipements 30
4.2 d'Adressage des équipements 31
4.3 Tableau des Vlans 31
4.4 Tableau de routage inter-Vlan 32

Listes des abréviations

ERDP : Entreprise de **R**affinage et de **D**istribution de **P**roduit **P**étrolier

GPL : Gaz de **P**étrole **L**iquéfié

FTP : File **T**ransfer **P**rotocole

SFP : Small **F**orm **F**actor **P**luggable

UTP : Personnel et **M**oyen **C**ommun

PMC : Unshielded **T**wisted **P**air

STP : Spanning **T**ree **P**rotocol

CPL : Classification **L**abelling **P**ackaging

IP : Internet **P**rotocole

CPU : Central **P**rocessing **U**nit

DHCP : Dynamic **H**ost**C**onfiguration

DNS : Domaine **N**ame **s**ystem

FTP : File **T**ransfer **P**rotocol

TRANSEC : Transmission **S**ecurity

COMSEC : Communication **S**ecurity

TSK : Transmission **S**ecurity Key

LPI : Faible **P**robability **I**nterception

LPD : Faible **P**robability **D**etection

VPN : Virtual **P**rivate **N**etwork

BIOS : **B**asic **I**nput **O**utput **S**ystem

OSI : **O**pen **S**ystem **I**nterconnexion

ACL : **A**ccess **C**ontrol **L**ist

IDS : **I**ntrusion **D**etection **S**ystem

RSA : **R**ivest **S**hamir **A**delman

TPM : **A**rusted **P**latform **M**odule

IPS : **I**ntrusion **P**revention **S**ystem

TCP : **T**ransmission **C**ontrôle **P**rotocole

ICMP : **I**nternet **C**ontrol **M**essage **P**rotocol

FAI : **F**ournisseur **D**'accés**I**nternet

ADSL : **A**symmetric **D**igital **S**ubscriber **L**ine

PPP : **P**oint To **P**oint **P**rotocol

IPX : **I**nternetwork **P**acket **E**xchange

Netbeui : **N**etBIOS **E**xtended **U**ser **I**nterface

PPTP : **P**oint to **P**oint **T**unneling **P**rotocol

L2TP : **L**eyer 2 **T**unneling **P**rotocol

L2F : **L**ayer **T**wo **F**orworking

LAC : **L**2tp **A**ccess **C**oncentrator

LNS : **L**2Tp **N**etwork **S**erver

Mpls : **M**ulti-**P**rotocol **L**abel **S**witching

Qos : **Q**uality **O**f **S**ervice

SSL : **S**ecure **S**ochets **L**ayer

TLS : **T**ransport **L**ayer **S**ecurity

HTTP : **H**yper **T**ext **T**ransfer **P**rotocol

HTTPs : **H**yper **T**ext **T**ransfer **P**rotocol **S**ecure

Ipsec : **I**nternet **P**rotocol **S**ecurity

Telnet : **T**erminal **N**etwork

IETF : **I**nternet **E**ngineering **T**ask **F**orce

IKE : **I**nternet **K**ey **E**xchange

CPA : **C**lé **P**ublique **A**uthentifié

RAM : **R**andom **A**ccess **M**emory

P2P : **P**eer to **P**eer

IPv6 : **I**nternet **P**rotocol **V**ersion 6

IOS : **I**nternetwork **O**perating **S**ystems

WAN : **W**ide **A**rea **N**etwork

AES : **A**dvanced **E**ncryption **S**tandard

SSH : **S**ecure **S**hell

ISP : **I**nternet **S**ervice **P**rovider

ESP : **E**ncapsulating **S**ecurity **P**ayload

AH : **A**uthentication **H**eader

Introduction Géneral

Les réseaux locaux d'entreprise sont des réseaux internes à une organisation, c'est-à-dire que les liaisons entre machines appartiennent uniquement à l'organisation. Ces réseaux sont de plus en plus souvent reliés à Internet par l'intermédiaire d'équipements d'interconnexion. Il arrive ainsi que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloignées via Internet.

Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne à une organisation car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

La première solution pour répondre à ce besoin de communication sécurisé consiste à relier les réseaux distants à l'aide de liaisons spécialisées. Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission.

Un bon compromis consiste donc à utiliser Internet comme support de transmission en utilisant un protocole d'encapsulation appelé " tunneling ", c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (VPN) pour désigner le réseau ainsi créé. Ce réseau est dit virtuel car il relie deux réseaux physiques (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données. Le système de VPN permet ainsi d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux. En contrepartie, il ne permet pas d'assurer une qualité de service comparable à une ligne louée dans la mesure où le réseau physique est public et donc non garanti. Comme la plus part des acteurs d'une entreprise sont souvent mobiles, l'utilisation d'un VPN mobile est aussi souhaité et nécessaire.

Dans le cadre du stage qu'on a entrepris au niveau de l'entreprise GPL NAFTAL, nous avons pu vérifier cette nécessité d'utiliser un VPN pour les clients externes et même un VPN mobile pour les clients en déplacement. Le manuscrit est organisé en quatre chapitres :

– Le premier chapitre s'intitule " " Présentation de l'organisme d'accueil ", qui est le

noyau de notre travail. Nous avons donné une présentation générale de l'organisme d'accueil ainsi que le service où nous avons effectué notre stage, de là, nous avons soulevé les différents problèmes rencontrés, et proposé une solution à ces derniers.
- Le deuxième chapitre est dédié à " la sécurité des réseaux informatiques ". En effet nous décrivons la sécurité des réseaux informatiques et présentons les différentes types d'attaques auxquelles un réseau peut être exposé et Les dispositifs de protection.
- Le troisième chapitre concerne " Les réseaux privé virtuel(VPN)". Dans ce chapitre, nous avons présenté les VPN, et les protocoles les plus communément utilisé et les applications existantes et plus précisément OpenVPN qui est l'application utiliser dans notre projet.

"Configuration et Implémentation" fera l'objet du quatrième chapitre dans lequel nous définirons les outils utilisés. Nous illustrerons également quelques captures de la configuration réalisée.

Enfin, nous conclurons ce travail en résumant les connaissances acquises durant la réalisation du projet.

Chapitre 1

Présentation de l'organisme d'accueil

1.1 Introduction

Dans ce chapitre, nous allons présenter la société de NAFTAL ou nous avons effectué un stage pour compléter notre projet de fin d'étude. Nous allons nous intéresser à la présentation de l'historique et les activités principale de l'entreprise ensuite les missions principales de GPL (Gaz De Pétrole Liquéfie) NAFTAL Bejaia, et enfin l'étude du réseau informatique de l'entreprise qui est notre objectif.

1.2 Présentation de l'organisme d'accueil NAFTAL

NAFTAL dont le logo est donné par la figure 1.1,est une entreprise pétrolière algérienne, spécialisée dans la distribution des produits pétroliers.

FIGURE 1.1 – Logo de l'entreprise NAFTAL

1.2.1 ***Historique de NAFTAL***

La société de raffinage et de distribution de produit pétrolier (ERDP) de SONATRACH a été créée par décret n°80/101 du 6 avril 1981. Début de la production le 1^{er} janvier 1982, responsable du raffinage et de la distribution des produits pétrolier. En août 1987, l'activité de raffinage est séparée de l'activité de distribution et transférée à une nouvelle entité NAFTEC.

Et ensuite NAFTAL est désormais seul responsable Produits pétroliers et dérivés, elle est rattachée à l'activité commercialisation. En 1998, elle devient une société par actions à 100% de SONATRACH [3].
Elle intervient également dans le domaine de :

- L'enfûtage des GPL (Gaz de Pétrole les Liquéfié).
- La formulation des bitumes.
- La distribution, le stockage et la commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatiques, GPL/carburant, produits spéciaux.
- Le transport des produits pétroliers.

1.2.2 Les activités principales de l'entreprise NAFTAL

NAFTAL a pour activités principales [1] :

♣ La commercialisation de carburants pour la motrice essence et diesel :
- Essence normale.
- Essence super.
- Essence super sans plomb.
- Gaz Oïl/CPL.

♣ Commercialisation des pneumatiques de grandes marques.
♣ Commercialisation d'une gamme de lubrifiants : ce dernier couvre toutes les applications d'un secteur automobile et industriel.
♣ Le traitement du gaz naturel ou gaz associés.
♣ Le raffinage du pétrole.
♣ La liquéfaction du gaz naturel.

1.2.3 Objectifs de l'entreprise NAFTAL

A travers son plan de développement NAFTAL vise deux objectifs principaux :

- Poursuivre la distribution des produits pétroliers.
- Améliorer la qualité des produits et services proposés.

1.3 Présentation du district GPL NAFTAL Bejaia

Dans cette partie on va présenter le district GPL NAFTAL Bejaia, les missions de district GPL et le rôle de chaque service.

1.3.1 Les missions principales du District GPL

Le District GPL est chargée des activités liées au transport, stockage, enfûtage, distribution, promotion et développement des GPL sur tout le territoire national. Elle a pour missions de :

- Commercialiser les GPL vrac et conditionner leurs emballages et accessoires.
- Veiller au respect des normes et consignes de sécurité sur toute la chaîne GPL (transport, installation d'enfûtage et de stockage, bouteilles, citernes, accessoires, etc ...).
- Organiser et développer le réseau commercial et de distribution.
- Développer et valoriser les GPL sous toutes ses formes particulièrement vrac et gaz carburant.
- Distribuer les GPL aux utilisateurs aux meilleures conditions de coût, de qualité, de délais et de sécurité.
- Moderniser les infrastructures pour améliorer la productivité, la sécurité et la gestion.

- Développer le partenariat et la coopération dans domaine des GPL.

1.3.2 L'organigramme du District GPL

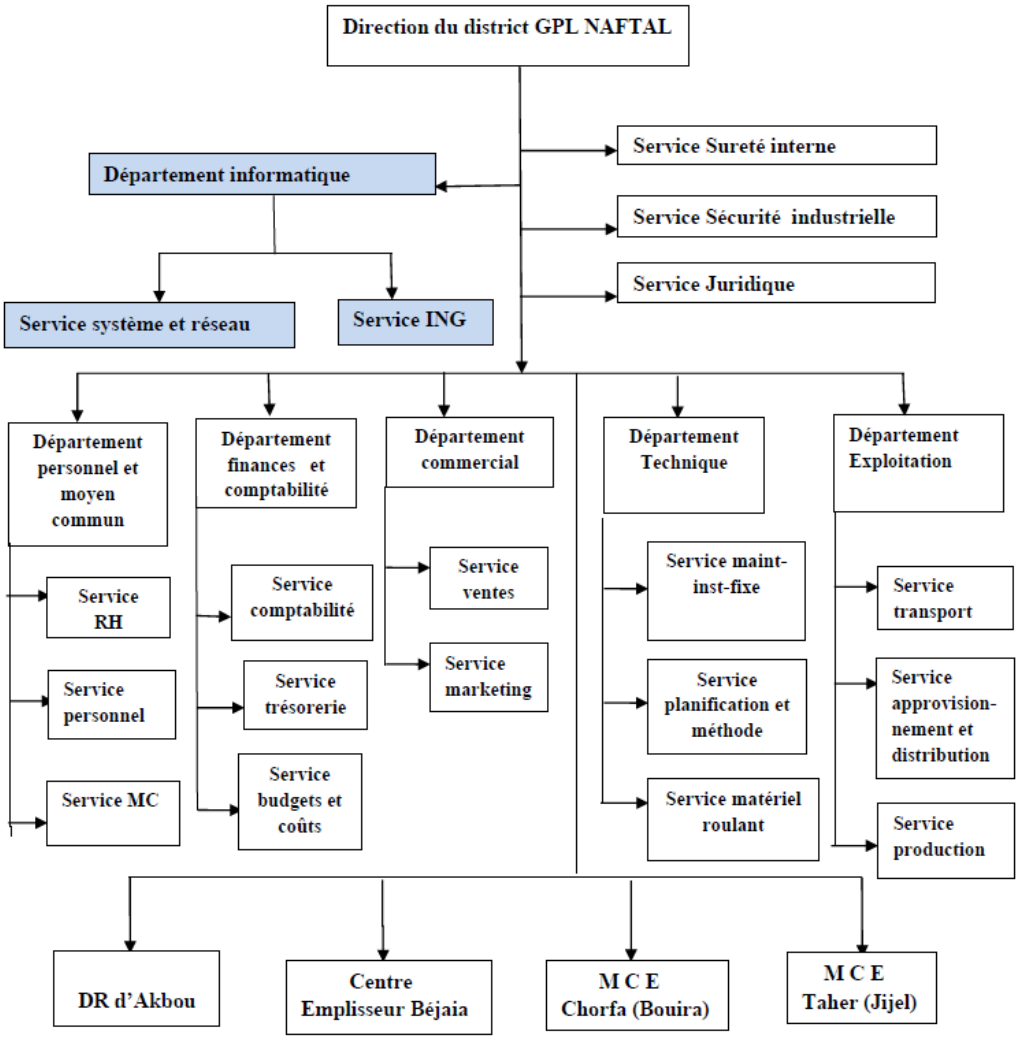


FIGURE 1.2 – L'organigramme du District GPL NAFTAL BEJAIA [4]

1.3.3 Le rôle de chaque service de l'entreprise :[4]

✓ **Services de sécurité :** Assurer la sécurité au sein de l'entreprise.
✓ **Services juridiques :** S'assurer que les documents signés ou en attente sont conformes
✓ **Service Sécurité Industrielle :** Ce service est chargé d'assurer la protection et la préservation des personnes, des actifs industriels et de l'environnement.
✓ **Département informatique :** responsable de la coordination des activités informatiques au niveau de la société NAFTAL.
✓ **Département des Opérations :** Responsable des tâches suivantes :
– Suivi de la performance des moyens de transport.
– Diriger et organiser les moyens de transport et élaborer un plan de distribution approprié.

  - Il est responsable du conditionnement du gaz butane en vrac en bouteilles de 13kg et 3kg.
  - Qu'il s'agisse de vrac ou de GPL, il s'assure que le produit est disponible pour les clients.

✓ **Département Technique :** Sa responsabilité est d'assurer la gestion du projet pendant les phases de recherche et de supervision de l'ingénierie.

✓ **Département du Commerce :** Responsable des diverses transactions entre l'entreprise et les clients, et responsable des études de marché sur l'environnement de commercialisation des produits.

✓ **Service Comptabilité Financière :** Ce service est responsable de l'ensemble des flux financiers de l'entreprise, s'assure de l'authenticité des comptes régionaux et de la cohérence des écritures comptables avec les flux physiques et financiers. La direction est composée de 3 directions de service :

♣ Direction financière en charge des recettes et des dépenses.

♣ Le service comptabilité générale qui gère les bilans et les inventaires.

♣ La Division du Budget et des Dépenses est chargée d'ajuster les budgets et les crédits provisoires d'investissement et de fonctionnement du District.

✓ **Département du Personnel et des Utilités Publiques :** Principalement chargé de la reconversion et de la promotion du personnel de l'entreprise.

1.4 Etude du réseau informatique de l'entreprise : [4]

1.4.1 ***Infrastructure matériel***

Le GPL NAFTAL de Bejaia dispose d'un vaste réseau informatique composé de 4 blocs distincts, chacun représentant un sous-réseau avec des commutateurs. Les blocs sont des armoires qui contiennent différents équipements, et chaque bloc est dans un département. Nous allons maintenant présenter les différents matériels réseaux utilisés dans chaque service.

1.4.1.1 La direction :

On retrouve l'armoire principale dans ce service, qui contient :

- **Routeur de marque Cisco 2911 :** permet d'interconnecter deux ou plusieurs réseaux. Les routeurs permettent aux messages d'être acheminés vers leurs destinations via leurs tables de routage.
- **Commutateur Cisco CATALYST 2960 :** ce commutateur est un commutateur autonome empilable à configuration fixe qui fournit un accès FastWire Speed Ethernet et Gigabit Ethernet.
- **Panneau de brassage :** Il connecte les ports de divers périphériques réseau aux extrémités des câbles réseau et des connecteurs situés sur le panneau de brassage. Cela garantit une commutation de haute qualité.
- **Deux tiroirs optiques :** Ces tiroirs sont utilisés pour les connexions de câbles afin d'assurer la distribution sur d'autres câbles ou appareils actifs. Par conséquent, ces fonctions principales sont la fixation, l'épissure et la terminaison des câbles. Toutes ces fonctions peuvent être réparties dans différents conteneurs.
- Agit comme une terminaison pour l'adaptateur entre le port Rj45 et le port SFP (Small Form Factor Pluggable).
- **Point d'accès (modem) :** il s'agit d'un appareil qui permet aux appareils sans fil de se connecter à un réseau filaire ou à Internet à l'aide d'une connexion radio. Il

est généralement connecté au routeur (via un réseau câblé), mais il peut également faire partie intégrante du routeur lui-même.

Cet armoire est reliée à l'armoire du service des ressources humaines par des câbles Rj45, et est relié à l'armoire du service commerce par fibre optique. En plus de cette armoire, nous avons constaté dans la gestion que le serveur est la partie la plus importante de toute l'architecture de l'entreprise.

1.4.1.2 Département commerciale

On retrouve dans l'armoire de ce département :
- Un tiroir optique.
- Un commutateur fibre optique CATALYST 3750.
- Un panneau de brassage.

Il est relié à celle de la direction par une fibre optique.

1.4.1.3 Service des ressources humaines

On retrouve dans l'armoire de ce département :
- Un commutateur Cisco 2911.
- Un panneau de brassage.

Il est connecté au service PMC et au service de gestion via des câbles Rj45 en cascade.

1.4.1.4 Service PMC (Personnel et Moyen Commun)

Dans l'armoire de ce service on trouve :
- Commutateur Cisco 2911.
- Un panneau de brassage.

L'armoire est connecté à service des ressources humaines via un câble en cascade Rj45.

L'architecture est également équipée d'une ligne ADSL qui sert de lien d'accès à Internet.

1.4.2 ***Support de transmission***

Pour connecter les différents appareils utilisés, NAFTAL a choisi deux supports :

1.4.2.1 Câble paire torsadée

Il existe deux types : les câbles Unshielded Twisted Pair (UTP), terminés par des connecteurs RJ45, et les câbles à paires torsadées blindées Spanning Tree Protocol (STP). L'objectif principal de ce câble est de limiter la sensibilité aux interférences.

1.4.2.2 Fibre Optique

C'est un fil en verre ou en plastique avec une âme très fine qui conduit la lumière et qui est utilisé pour l'inspection de la fibre, l'éclairage ou la transmission de données numériques. Le tableau 1 résume les différentes caractéristiques de ces supports.

1.4.3 ***Gestion de la sécurité***

Pour assurer la sécurité au sein du réseau, NAFTAL utilise plusieurs moyens :
- Des pares feux pour filtrer les paquets, accordant ainsi l'accès à certains types de trafic et en bloquant d'autres.

Désignation	Quantité
Prises réseaux RJ45 Catégorie 6	118
Câble de Postes souple 4 paires FTP 3m Catégorie 6	118
Câble de fibre optique souple 6 brins	150m
Tiroir optique avec jarretières	2
Coupleur de fibre optique	4

TABLE 1.1 – Tableau les différentes caractéristiques de ces supports.

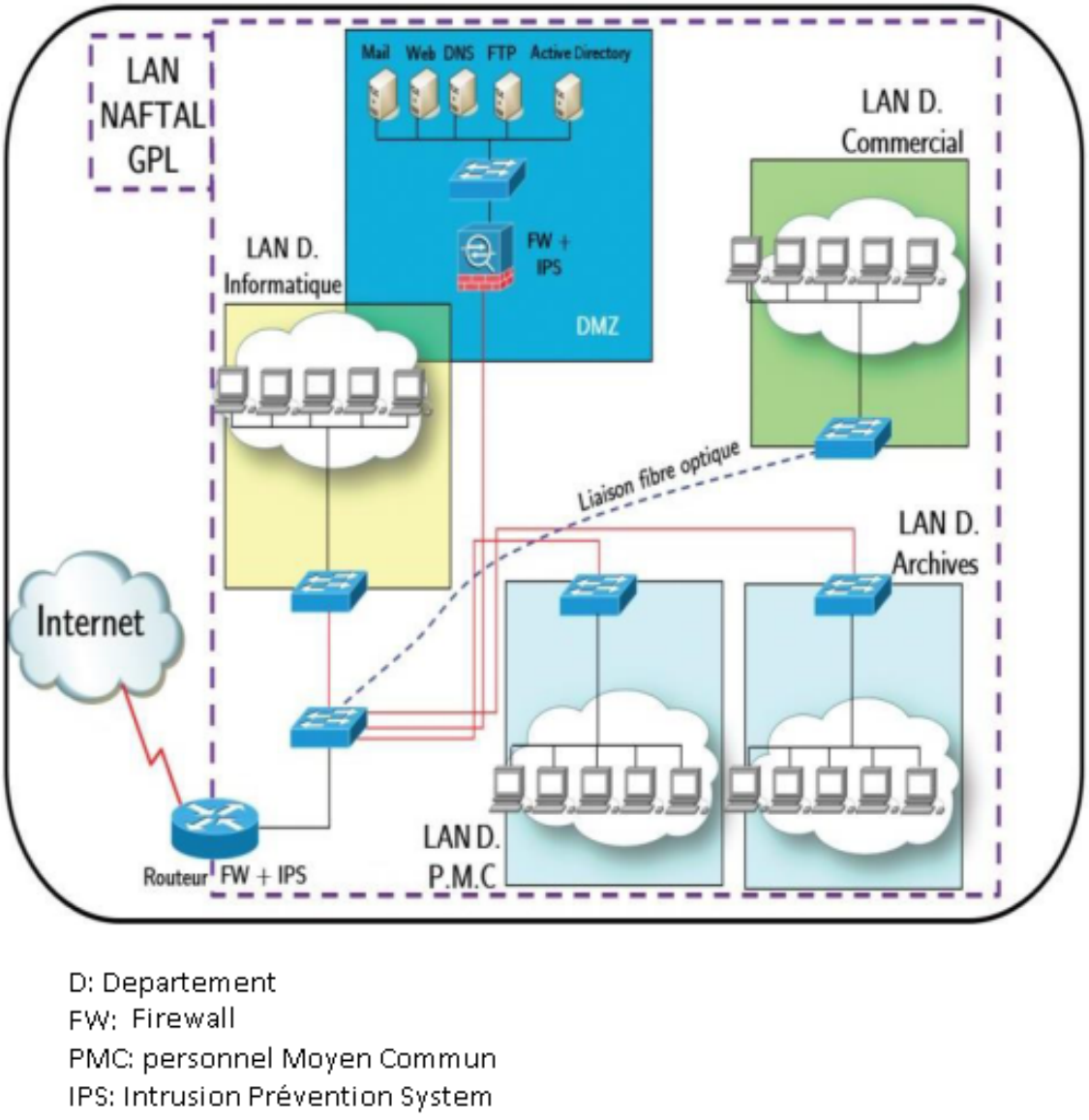


FIGURE 1.3 – Architecture du réseau GPL NAFTAL BEJAIA [4]

- Une application de sécurité (Kaspersky Security) pour surveiller l'état de leurs machines.
- Des contrôleurs de domaine "Active Directory", qui est un service d'annuaire développé par Microsoft pour les domaines Windows, pour localiser, sécuriser, gérer et organiser les ressources (fichiers, utilisateurs, groupes, périphériques et périphériques réseau). Et ceci pour faciliter la gestion de l'information.

1.4.4 ***Gestion des employés***

Chaque employé de cette entreprise a un compte sur son ordinateur qui a été créé par le service informatique à son arrivée, et ce compte est protégé par un mot de passe. L'authentification et l'autorisation de l'utilisateur à accéder à son poste de travail sont assurées par le serveur qui demande l'identifiant et le mot de passe lorsque l'employé allume son ordinateur. Le serveur fournira également aux employés des dossiers partagés auxquels quelques-uns peuvent accéder et d'autres non, selon la position de l'employé.

1.4.5 ***Problématique et Solution proposée***

Les applications et les systèmes distribués font de plus en plus partie intégrante du paysage d'un grand nombre d'entreprises. Ces technologies ont pu se développer grâce aux performances toujours plus importantes des réseaux locaux. Mais le succès de ces applications a fait aussi apparaître leur faiblesses.

En effet si les applications distribuées deviennent le principal outil du système d'information de l'entreprise, comment assurer leur accès sécurisé au sein de structures parfois réparties sur de grandes distances géographiques ?

Concrètement comment une succursale d'une entreprise peut-elle accéder aux données situées sur un serveur de la maison mère distant de plusieurs milliers de kilomètres ? Les VPN ont commencé à être mis en place pour répondre à ce type de problématique. Mais la mobilité des clients, des fournisseurs et même des employés rend l'utilisation de VPN insuffisant. C'est pour cela que nous avons choisi la solution de VPN mobile.

La démarche proposée : Après avoir analysé le contexte du système actuel, nous allons étudié quelles sont les principales caractéristiques des VPN à travers un certain nombre d'utilisation type. Nous nous intéresserons ensuite aux protocoles permettant leur mise en place. OpenVPN est un VPN, ou Private Virtual network, optimisé pour le télétravail. Il sécurise les accès distants aux applications d'entreprise, en créant un réseau privé virtuel. OpenVPN est utilisé pour pouvoir gérer n'importe quel réseau virtuel privé à partir d'un appareil Android, tout comme le ferais à partir de l'ordinateur avec le programme de bureau.

1.5 conclusion

Dans ce premier chapitre nous avons présenté l'organisme d'accueil, déterminé la problématique et la solution optimale proposée pour améliorer le VPN et la sécurité des réseaux de l'entreprise, ce qui nous mènera dans le chapitre suivant à détailler la sécurité des réseaux informatique.

Chapitre 2

La sécurité des réseaux informatique

2.1 Introduction

La sécurité engendre généralement le déploiement de moyens techniques , notamment de prévention. Ces dernières doivent prendre en compte la formation et la sensibilisation de solutions de tous les acteurs de l'entreprise sur les risques encourus. Ainsi il faut mettre en place une bonne politique de sécurité fondée sur la collaboration de l'ensemble des employés et l'utilisation d'équipements et techniques qui répondent aux exigences du système tout en assurant un blocage d'attaques informatiques de tout genre. Dans ce chapitre, nous aborderons les différents aspects liés à la sécurité informatique.

2.2 Définition de sécurité des réseaux

La sécurité des réseaux et de l'information est la capacité d'un réseau ou d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions illégales ou malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées ou transmises et des services connexes que ces réseaux et systèmes offrent ou qu'ils rendent accessibles [16].

2.3 Les critères de sécurité

La sécurité de l'information dans une entreprise est une question essentielle qui préoccupe aujourd'hui tous les dirigeants. Pour la mettre en place, il faut suivre quelques règles essentielles mais surtout, il faut veiller à respecter les critères majeurs en matière de sécurité. Ces critères majeurs sont au nombre de quatre, et vous pourrez les découvrir dans la figure 2-1 [8].

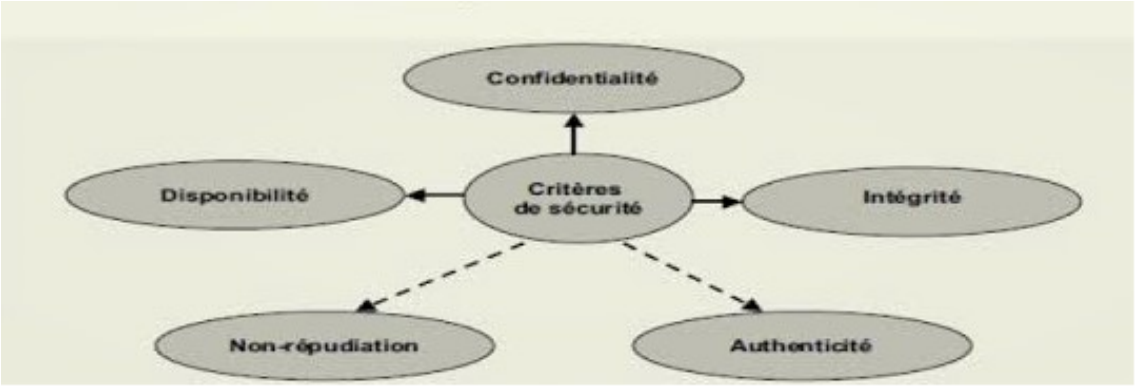


FIGURE 2.1 – Critères de sécurité [12]

2.3.1 ***Intégrité***

Le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions et services) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Une fonction de sécurité appliquée à une ressource pour contribuer à préserver son intégrité, permettra de la protéger plus ou moins efficacement contre une menace de corruption ou de destruction [18].

2.3.2 ***Confidentialité***

La confidentialité des données peut être définie comme la protection des données contre une divulgation non autorisée [7]. Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

- ✓ Limiter et contrôler leurs accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire.
- ✓ Les rendre incompréhensibles en les chiffrant à l'aide de moyens de déchiffrement pouvant y accéder.

2.3.3 ***Non répudiation***

C'est le fait de ne pas pouvoir nier ou rejeter qu'un événement (actions, transactions) a eu lieu [18]. A ce critère de sécurité peuvent être liées les notions suivantes :

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

2.3.4 ***L'authentification***

Elle a pour but de s'assurer que les données reçues proviennent bien de l'entité émettrice (vérification de l'identité d'un utilisateur)et pour celle de quelqu'un d'autre. [18].

2.3.5 ***Disponibilité***

Elle a pour but de s'assurer que l'information sur le système, soit disponible aux personnes autorisées (garantir l'accès aux données) [17].

2.4 Terminologie de la sécurité informatique

La sécurité informatique utilise un ensemble de terme bien spécifique et parmi ces termes [5] :

2.4.1 ***Vulnérabilité***

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

2.4.2 ***Une attaque***

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

2.4.3 ***Une contre-mesure***

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

2.4.4 ***Une menace***

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

2.5 Les types d'attaques

Les personnes malveillantes utilisent plusieurs techniques d'attaques qui peuvent être regroupées en trois familles différentes [18].

2.5.1 ***Les attaques directes***

C'est l'attaque la plus simple. Les pirates attaquent ses victimes directement depuis son ordinateur. En fait, les programmes de piratage qu'ils utilisent ne sont que peu configurable, et un grand nombre de ces programmes envoient des paquets directement à la victime.

2.5.2 Les attaques indirectes par rebond

Cette attaque est très prisée des hackers. En effet, le rebond a deux avantages :
✓ Masquer l'identité (l'adresse IP) du hacker
✓ Utiliser éventuellement les ressources de l'ordinateur intermédiaire car il est plus puissant (CPU, bande passante) pour attaquer.

Les paquets d'attaque sont envoyés à l'ordinateur intermédiaire qui répercute l'attaque vers la victime. D'où le terme de rebond ce que montre la figure 2-2.

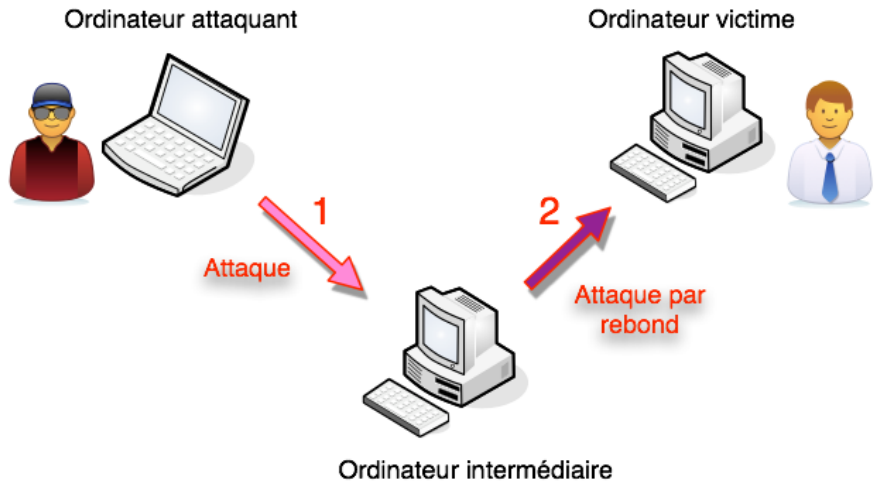


FIGURE 2.2 – Attaque indirecte par rebond [13]

2.5.3 ***Les attaques indirectes par réponse***

Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du hacker, mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime ce qu'est montré dans la figure2-3.

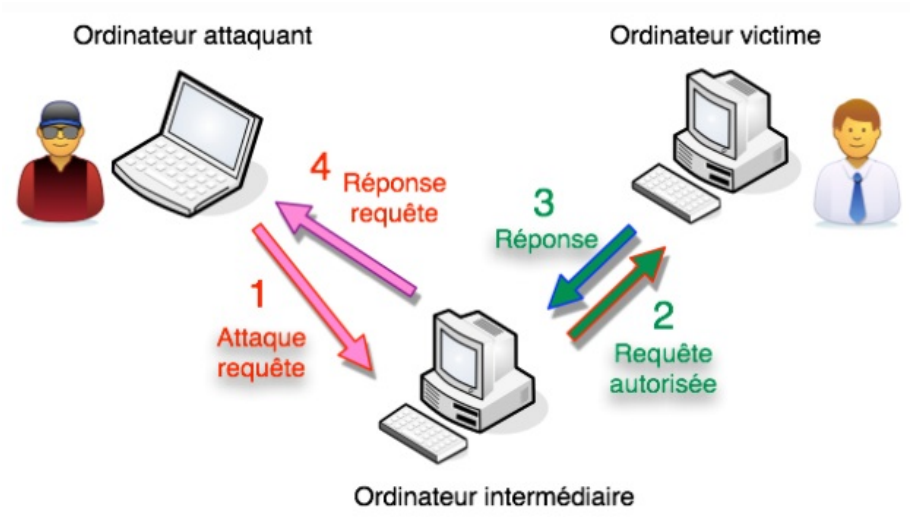


FIGURE 2.3 – Attaque indirecte par réponse [14]

2.6 Les éléments à sécuriser dans un réseau

Les réseaux sont constitués de divers équipements d'une part et de liens filaires ou non Filaires, qui les relient d'autre part. Toute où partie de ces équipements peuvent être gérés par des programmes adaptés et plusieurs sortes de données y sont stockées. Certaines d'entre elles peuvent être l'objet de transferts selon des protocoles appelés protocoles de réseaux.

La sécurité concerne celle du matériel, celle des programmes, celle des données et celle des protocoles. Avant de réaliser un système de sécurité, il faut spécifier d'abord les éléments à protéger. On dénombre trois types essentiels qui sont [5] :

2.6.1 ***Matériel***

Mis à part les ordinateurs que les réseaux relient, le matériel inclut aussi, les équipements intermédiaires comme les répéteurs, commutateurs, switch, routeurs, serveurs, modems, firewalls....etc. La limitation d'accès à chaque matériel participe à la sécurité de l'ensemble.

2.6.2 ***Programme***

Les programmes incluent les systèmes d'exploitation y compris les pilotes de périphériques ainsi que les logiciels programmés gérant les différents mécanismes de réseaux. Les services permettant une meilleure gestion à distance et plus d'autonomie, on parle dans ce cas-là de services réseau tels que : DHCP, DNS, FTP, etc.

2.6.3 ***Données***

On distingue deux sortes de données ; celles qui servent au fonctionnement du réseau comme les tables de routage, les bases de données des clients, les fichiers relatifs aux droits d'accès, etc. On retrouve aussi des données qui ne sont pas en rapport avec le Fonctionnement du réseau tels que : les documents et les archives.

2.7 La sécurité et Les solutions de la protection des données dans les transmissions [19]

La sécurité de la transmission (TRANSEC) est le processus visant à empêcher les transmissions de données d'être infiltrées, exploitées ou interceptées par un individu, une application ou un appareil. TRANSEC sécurise les données lors de leur déplacement sur un support de communication.

TRANSEC fait partie de la sécurité des communications (COMSEC) et est mis en œuvre et géré par plusieurs techniques.

Chaque flux de transmission est sécurisé par une clé de sécurité de transmission (TSK) et un algorithme cryptographique. Le TSK est un algorithme permettent la création d'une séquence pseudo-aléatoire au-dessus des données transmises. Les buts et objectifs clés de TRANSEC sont les suivants :

- ✓ Pour créer une faible probabilité d'interception (LPI) pour les transmissions.
- ✓ Pour créer une faible probabilité de détection (LPD) pour les mesures prises par TRANSEC.
- ✓ Pour assurer l'anti jam ou la résistance au brouillage.

Les ordinateurs portables mettent aussi en péril la sécurité des données. Tout d'abord, ils demandent la mise en place de solutions de sauvegarde adaptées : très peu de ces machines comportent plusieurs disques durs. Il est aussi difficile, vis-à-vis de l'aspect mobile, d'envisager le transport d'unité de sauvegarde externe importante [6]. Il faut donc se tourner vers des solutions de stockage légères ou en réseau.

2.7.1 ***Les solutions de sauvegarde***

On peut distinguer trois manières d'assurer la sauvegarde d'un ordinateur portable : les clés/unités de stockage USB, la synchronisation avec un serveur de sauvegarde et l'utilisation d'applications web.

Les clés USB ont pour avantage d'être utilisables tout le temps mais sont aussi très faciles à perdre. La clé USB contient suffisamment de données pour permettre à un pirate de s'y introduire. Il est donc impératif d'utiliser des solutions de chiffrement sur ce type de support.
Aussi,on peut securiser le portable avec l'empreinte digitale

Les deux autres solutions permettent une sauvegarde plus systématique des données mais soulèvent le problème de la sécurité des transferts [6].

2.7.2 ***Les connexions réseau***

L'utilisation d'un ordinateur induit très souvent des connexions à de multiples réseaux. Ainsi, le risque de se retrouver sur une connexion présentant des failles de sécurité s'accroît. De plus, certains IOS comme Windows XP ne permettent pas d'adapter automatiquement les règles de pare-feu. Ainsi, des machines configurées pour des connexions intranet peuvent se retrouver totalement accessibles lorsqu'elles sont connectées directement sur le web.

Par ailleurs, les ordinateurs portables utilisent majoritairement des connexions sans fil. La problématique des faux points d'accès et de la sécurisation des réseaux Wi-Fi se pose de façon bien plus cruciale que pour les PC de bureau. Il est donc fortement déconseillé de se connecter à un réseau sans fil non crypté et d'y envoyer des données personnelles. Dans le cadre d'une utilisation professionnelle, il est impératif de se connecter à un VPN (Réseau Privé Virtual) dès le début d'une session Wi-Fi [6].

2.7.3 ***Les mots de passe du disque dur***

La protection des données passent aussi par la mise en place de mot de passe au démarrage de la machine. Un mot de passe à l'ouverture de la session est un minimum. Il peut aussi s'agir d'un mot de passe sur le BIOS ou mieux, sur le disque dur. Son avantage sur les autres mots de passe est qu'il empêche toute intrusion.

La perte de ce mot de passe entraînera presque à coup sûr l'impossibilité de se servir de ce disque dur [6].

2.7.4 ***Le chiffrement des données***

Sur ce point, il existe des solutions logicielles et matérielles. De nombreuses applications permettent la création de containers cryptés dans lesquels l'utilisateur va stocker ses documents. Les systèmes d'exploitation proposent aussi d'encrypter complètement la partition du disque système. On trouve des solutions matérielles avec des disques durs embarquant un système de cryptage à la volée [6].

2.8 Les dispositifs de protection

Les principaux dispositifs permettant de sécuriser un réseau contre les attaques sont :

2.8.1 ***Antivirus***

Logiciel censé protéger ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire [9].

2.8.2 ***Le pare-feu (firewall)***

Un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent et filtrer le trafic en fonction des informations contenues dans les couches 2 et 3 de modèle OSI. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits.

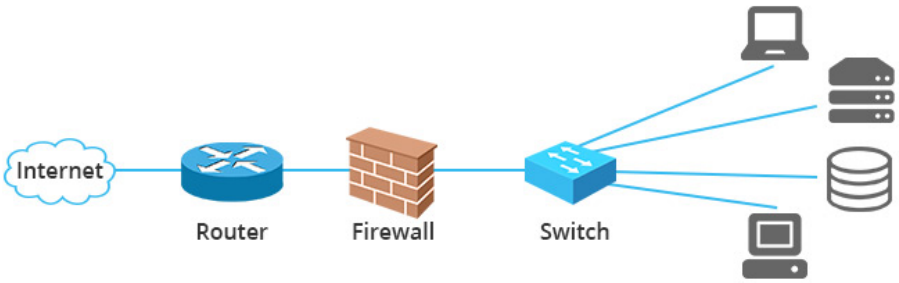


FIGURE 2.4 – pare-feu (firewall)[11]

Le pare-feu n'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système, et ne protège pas contre une attaque venant du Réseau intérieur (qui ne le traverse pas) [9].

2.8.2.1 Le filtrage simple de paquets

C'est le plus vieux dispositif de filtrage réseau, introduit sur les routeurs. Il regarde chaque paquet indépendamment des autres et le compare à une liste de règles préconfigurées. [15]

2.8.2.2 Le filtrage dynamique de paquets

Certains protocoles dits " à états " comme TCP introduisent une notion de connexion. Les pares-feux à états vérifient la conformité des paquets à une connexion en cours. Ils savent aussi filtrer intelligemment les paquets ICMP qui servent à la signalisation des flux IP. [15]

2.8.2.3 Le filtrage applicatif

Dernière génération de pare-feu, ils vérifient la complète conformité du paquet à un protocole attendu. Par exemple, ce type de pare-feu permet de vérifier que seul le protocole HTTP passe par le port TCP 80. Ce traitement est très gourmand en temps de calcul dès que le débit devient très important. [15]

2.8.3 ***Liste contrôle d'accès aux réseaux***

Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers. Une ACL est un ensemble de conditions qui sont

applique au trafic circulant via une interface de routeur. Elle indique au routeur les types des paquets à accepter ou à rejeter. Les ACL permettent de sécuriser l'accès d'un réseau en entrée comme en sortie [5].

2.8.4 ***Les Réseaux Privé Virtual (VPN)***

Il correspond à une liaison permanente, distante et sécurisée entre deux sites d'une organisation. Cette liaison autorise la transmission de données cryptées par le biais d'un réseau non sécurisé, comme internet. En d'autres termes, un réseau privé virtuel est l'extension d'un réseau privé qui englobe les liaisons sur des réseaux partages ou publics, tels qu'internet. Il permet d'échanger des données entre deux ordinateurs sur un réseau partagé ou public, selon un mode qui émule une liaison privée point à point. Le VPN est basésur la rechnique du tunnelling comme processus d'encapsulation,de transmission et de désencapsulation,consiste à contruire un chemin virtuel après avoir identifié l'émetteur et le destinataire et la source chiffre les donnée et les achemine en empruntant ce chemin virtuel.

2.8.5 ***Système de détection d'intrusion (IDS) [7]***

La détection d'intrusion est définie comme étant l'ensemble des pratiques et des mécanismes utilisés qui permettent de détecter des problèmes pouvant conduire à des violations de la politique de sécurité.

La notion d'intrusion est à considérer au sens large et comprend les notions d'anomalies et l'usage abusif des ressources.

Un système de détection d'intrusion (IDS, Intrusion Détection System) analyse les données pour détecter celles qui pourraient conduire à des incidents ou à des intrusions. Selon la localisation (sur l'infrastructure réseau ou dans un système hôte) et le champ d'action, les systèmes de détection d'intrusion se distinguent en :

- Systèmes de détection d'intrusion bases sur le réseau sont les plus courants. Ils examinent le trafic réseau en transit pour détecter des signes d'intrusion.
- Systèmes bases sur l'hôte examinent l'activité des utilisateurs et des processus sur la machine locale dans le but de trouver des signes d'intrusion.

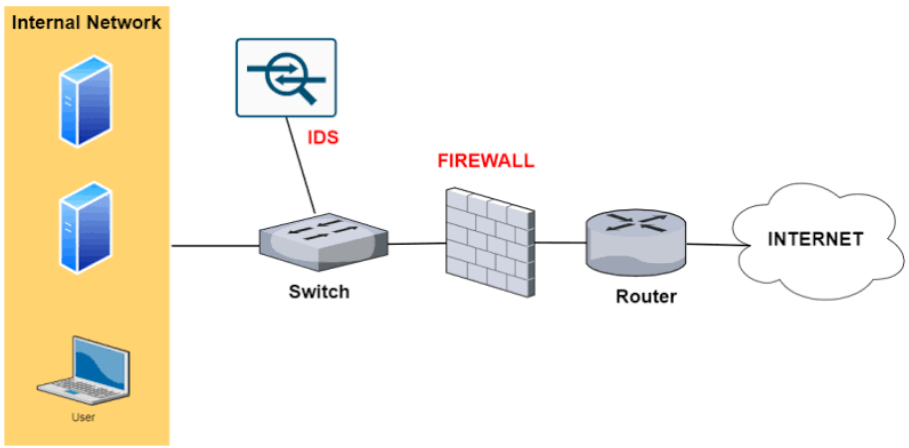


FIGURE 2.5 – Système de détection d'intrusion (IDS) [10]

2.8.6 ***Le système de prévention d'intrusion (Intrusion Prévention System-IPS) :***

Le système de prévention d'intrusion (IPS) est un dispositif de sécurité qui surveille les activités du réseau et/ou du système informatique à la recherche des comportements indésirables afin de les empêcher à produire des incidents de sécurité.

L'IPS est considéré comme la prochaine étape dans l'évolution du système de détection d'intrusion (IDS). Il peut également être un Software ou un Hardware qui a la capacité de prévenir les menaces et les attaques, qu'elles soient connues ou inconnues, et de les empêcher d'interrompre le fonctionnement du réseau ou système informatique.

2.8.7 ***Le Proxy :***

Un proxy (mandataire) est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.

Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement Internet. On appelle aussi (proxy) un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services.

Le proxy se situe au niveau de la couche application (HTTP, FTP, SSH, etc. de niveau 7).

2.9 Conclusion :

Dans ce chapitre, nous avons défini les notions fondamentales et les stratégies de sécurité des réseaux informatiques à prendre pour remédier aux attaques. Le prochain chapitre sera consacré aux VPN (Virtuel Privat Network).

Chapitre 3

La généralité sur les réseaux privé virtuel(VPN)

3.1 Introduction

La plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission.

Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole de "tunnellisation", c'est-à-dire encapsulant les données à transmettre de façon chiffrée.

Nous parlons alors de réseau privé virtuel (Virtual Privat Network) pour désigner le réseau ainsi artificiellement créé.

Dans ce chapitre nous allons détailler le VPN.

3.2 Définitions des réseaux privés virtuel :

Un réseau privé virtuel est un tunnel sécurisé à l'intérieur d'un réseau (Internet notamment). Il permet d'échanger des informations de manière sécurisée et anonyme en utilisant une adresse IP différente de celle de votre ordinateur [20].

Le VPN fournit un tunnel sécurisé de bout en bout entre un client et un serveur et permet d'identifier et d'autoriser l'accès ainsi que chiffrer tous trafic circulant dans le réseau [21].

3.3 Cas d'utilisation VPN

On peut trouver plusieurs cas 'd'utilisation d'un VPN dont :

- **Connexion à distance pour les utilisateurs mobiles :**
  Il suffit de se connecter depuis des appareils mobiles pour obtenir une connectivité sécurisée pour les Smartphones, les tablettes, les ordinateurs portables (accès facile pour les utilisateurs mobiles).

Les utilisateurs communiquent en toute sécurité grâce à une technologie de cryptage éprouvée, à une authentification à deux facteurs et à un couplage utilisateur-appareil pour éliminer les menaces à la sécurité du réseau.

- **Connexion à distance pour les utilisateurs télétravailleurs :** L'utilisation d'un VPN ouvre un tunnel sécurisé entre le poste de travail à distance et le réseau de votre entreprise. Pour que les utilisateurs puissent travailler en toute sécurité en dehors du bureau, les administrateurs informatiques doivent pouvoir limiter l'accès VPN à certains ordinateurs portables autorisés de l'entreprise. Toute tentative d'accès à partir d'une autre machine doit alors être refusée [22].
- **Connexion de sites distants :**
  Quelle que soit la distance entre les sites, ils communiquent autour d'un réseau local étendu (WAN), accessible également pour les utilisateurs mobiles. Le VPN via internet (ipsec ,ssl) ou via opérateur privé (MPLS) garantit la sécurité des données sans nuire à la communication et la mutualisation des services (téléphonie, logiciel métier, messagerie, visioconférence ...) entre les sites[23].

3.4 Le fonctionnement des VPN :

Le VPN repose sur un protocole de tunnelisation qui est un protocole permettant de chiffrer les données par un algorithme cryptographique entre les deux réseaux [24].
Le VPN n'est qu'un concept, ce n'est pas une implémentation. Il se caractérise par les obligations suivantes :

- authentification des entités communicantes : le serveur VPN doit pouvoir être sûr de parler au vrai client VPN.
- authentification des utilisateurs : seuls les bonnes personnes doivent pouvoir se connecter au réseau virtuel. On doit aussi pouvoir conserver les logs de connexions.
- gestion des adresses : tous les utilisateurs doivent avoir une adresse privée et les nouveaux clients vont obtenir une facilement.
- cryptage du tunnel : les données échangées sur Internet doivent être cryptées entre le client VPN et le serveur VPN.
- les clés de cryptage doivent être régénérées souvent (automatiquement).
- le VPN peut supporter tous les protocoles afin de réaliser un vrai tunnel comme s'il y avait réellement un câble entre les deux réseaux.

3.5 Les avantages des VPN[25] :

Parmi les principaux avantages des VPN on cite :
– une couverture géographique mondiale.
– le coût de fonctionnement le plus bas du marché (tarifs calculés sur la plus courte distance au point d'accès opérateur).
– offre des garanties de sécurité (utilisation de tunnels).
– solution pour la gestion des postes nomades (grands nombres de points d'accès).

3.6 Les inconvénients des VPN [26] :

– la qualité de service et les délais d'acheminement n'est pas garantie
– les performances ne sont pas toujours au rendez-vous.
– Ne pas savoir si le chiffrement fournit par le VPN est robuste.

3.7 Les différents types des VPN :

Selon l'entité qui contrôle le VPN, on peut distinguer deux grandes catégories de VPN : les VPN d'entreprise et les VPN d'opérateur. Chacun d'eux a ses avantages et ses inconvénients, et ils ne s'excluent pas mutuellement car il n'est pas rare d'avoir les deux dans la même entreprise.

Nous allons ci-dessous les définir et présenter les différents avantages et inconvénients de chacune d'elles.

3.7.1 ***VPN d'entreprise***

Dans ce cas, l'entreprise conserve la maîtrise de l'implantation des VPN entre ses différents points de présence et entre les postes de travail situés à l'extérieur de l'entreprise et le site principal.

Il existe trois types de VPN d'entreprise et qui sont : les VPN site à site, les VPN poste à site, et VPN poste à poste.

3.7.1.1 VPN site a site :

VPN site à site aussi appelés router to router est utilisé pour relier au moins deux ou plusieurs sites entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants voir la figure 3-1.

Certaines données très sensibles peuvent être amenées à transiter sur le VPN.

Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées.

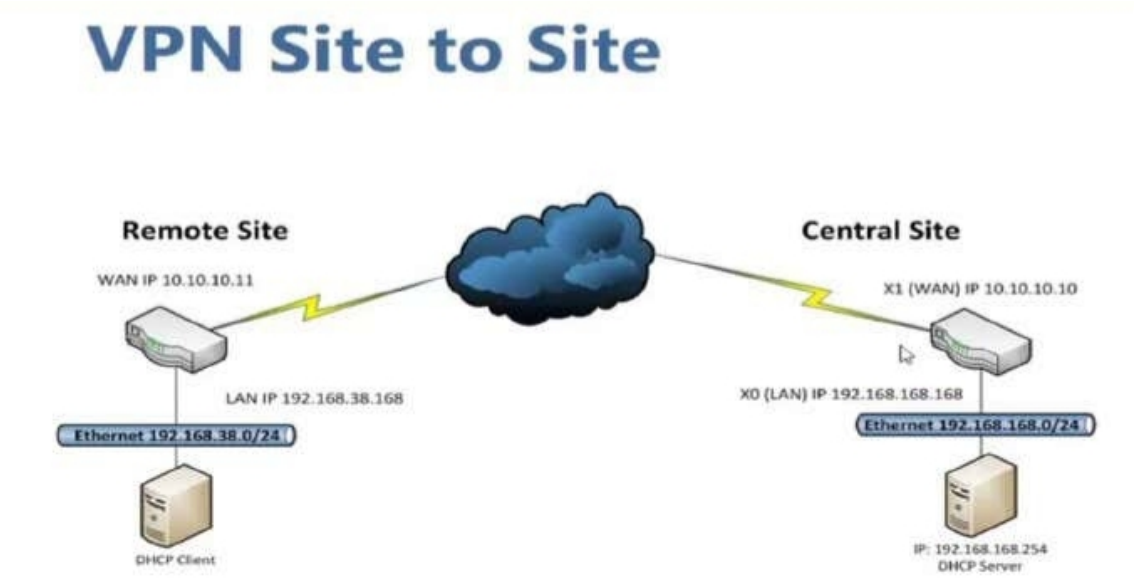


FIGURE 3.1 – VPN site à site

Les avantages de VPN site à site :
Parmi tous les avantages que présente VPN site à site, nous citons :

- il permet de garantir la sécurité et l'intégrité des données échangées entre des différents sites de l'entreprise.
- Il permet à deux machines de réseaux différents de connecter en utilisant uniquement des adresses privées.

Les inconvénients de VPN site à site :

- Il ne protège pas la conversation de bout en bout car le flux n'est chiffré qu'entre les deux extrémités du tunnel (routeur ou pare-feu).
- Il n'y a pas de protection des données entre le poste et le firewall car le tunnel n'est établi qu'entre les deux firewalls.

3.7.1.2 VPN poste à site :

Un utilisateur distant a simplement besoin d'un client VPN installé sur son ordinateur personnel pour se connecter au site de l'entreprise via sa connexion internet. Le développement de l'ADSL favorise ce genre d'utilisation.

La figure 3-2 montre un exemple d'utilisation de VPN poste à site, dans la quelle explique comment un VPN permettre à des postes isolés (poste à la maison, commerciaux itinérants) d'accéder au site principal à l'aide d'une connexion VPN à la demande. **Les**

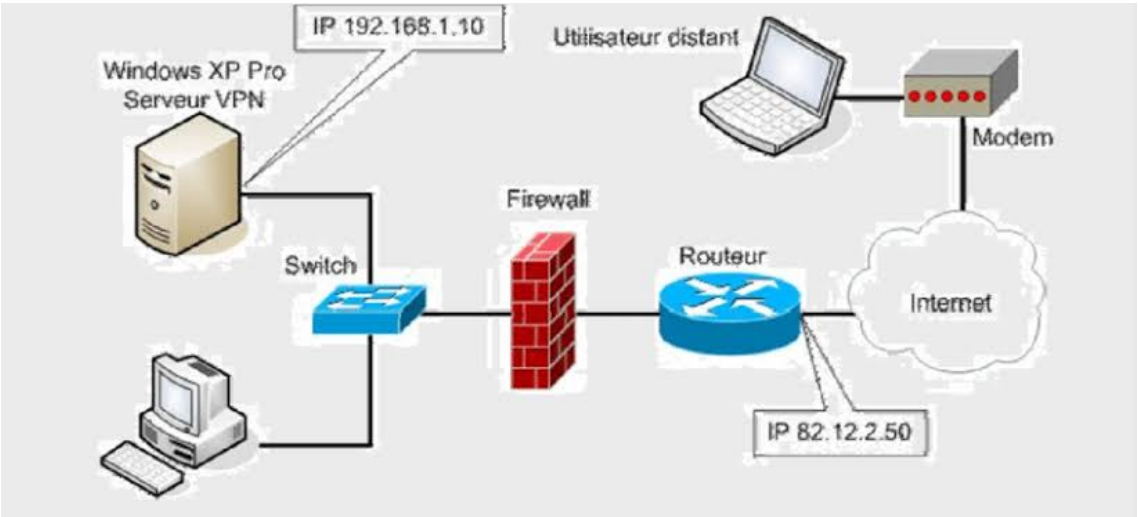


FIGURE 3.2 – VPN poste à site [34]

avantages de VPN poste à site :

- Transférer les données entre le poste distant et site central de manière sécurisée grâce à l'authentification.
- Il permet potentiellement à n'importe quel poste mobile distant qu'elle soit isolée ou sur un réseau de se connecter à une ou plusieurs machine d'un autre réseau en utilisant seulement les adresses privés.

Les inconvénients de VPN poste à site :

- Aucun cryptage n'est fourni en dehors du pare-feu du site central.
- Nécessite souvent l'installation d'un logiciel sur la station distante.

3.7.1.3 VPN poste à poste :

C'est le cas d'utilisation le plus simple. Il s'agit de mettre une relation entre deux serveurs. Le cas d'utilisation peut être le besoin de synchronisation de base de données entre deux serveurs d'une entreprise disposant de chaque côté d'un accès internet. L'accès réseau complet n'est pas indispensable dans ce genre de situation [27].

Avantages de VPN poste à poste :

- Il permet de protéger la conversation de bout en bout. Il est donc particulièrement indiqué dans des contextes où est requis de confidentialité.
- Il désigne une conversation entre deux postes d'utilisateurs que la connexion entre un poste de travail et un serveur.

Les inconvénients de VPN poste à poste :

- l'utilisation de protocoles de VPN en maillage d'un nombre important de postes puisse avoir un impact négatif sur les performances de ceux-ci.
- Les postes constituant les extrémités doivent pouvoir se contacter quand ils sont sur le même réseau local.

3.7.2 ***VPN operateur***

Lors de l'interconnexion de plusieurs sites d'une même entreprise avec des engagements de performance et de disponibilité, il serait plus judicieux de faire appel à l'opérateur, mais évidemment plus cher, afin que l'opérateur dispos d'un réseau dédié entre tous les sites.

Dans le cas d'un VPN opérateur, le réseau utilisé est basé sur les infrastructures IP privées et managées d'un opérateur de télécommunications et permettent un transport direct et natif des flux IP. La sécurité et la qualité de service sont alors assurés par le réseau de l'opérateur (technologies MPLS ou IP Sec). Les VPNs IP opérateurs cumulent les avantages du protocole IP et ceux des VPN traditionnels comme le Frame Relay (sécurité et classes de service) [32].

3.8 Les protocoles de VPN :

Les protocoles VPN représentent les processus et les ensembles d'instructions sur lesquels se basent les fournisseurs VPN pour s'assurer que les utilisateurs VPN bénéficient de communications stables et sécurisées entre le client VPN et le serveur VPN. Nous allons présenter ci- dessous les protocoles les plus communément utilises avec les VPN.

3.8.1 ***Protocole PPP (Point To Point Protocol)***

PPP (Point to Point Protocol) est un protocole qui permet de transférer des données sur un lien synchrone ou asynchrone. Il est full duplex et garantit l'ordre d'arrivée des paquets.

Il encapsule les paquets IP (Internet Protocole), Ipx (Internet PacketEXchange) et Netbeui(NetBIOS Extended User Interface) dans des trames PPP, puis transmet ces paquets encapsulés au travers de la liaison point à point.

PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau [28].

3.8.2 ***Protocole PPTP (Point To Point Tunneling Protocol)***

Le protocole PPTP est un protocole qui utilise une connexion PPP à travers un réseau IP en créant un réseau privé virtuel (VPN).

Le principe du protocole PPTP est de créer des paquets et de les encapsuler dans les datagrammes IP. Le tunneling PPTP se caractérise par une initialisation du client, une connexion de clôture entre client et serveur ainsi que par la clôture du tunnel par le serveur [28].

3.8.3 ***ProtocoleL2F (Layer 2 Forwarding)***

L2F fournit un tunnel sécurisé entre utilisateurs distants et la passerelle VPN Authentification et le chiffrement basée sur PPP, ils composent de [39] :

- Tunnel L2F entre l'ISP (Internet Service Provider) et le serveur d'accès distant
- Connexion PPP entre le client et l'ISP, que l'ISP fait suivre au serveur d'accès distant via le tunnel L2F.

3.8.4 ***Protocole L2TP (Layer 2 Tunneling Protocol)***

L2TP est un protocole réseau de la couche liaison de données qui permet de créer des réseaux privés virtuels entre un opérateur et les fournisseurs d'accès à internet, issu de la convergence des protocoles PPTP et L2F.

Il permet l'encapsulation des paquets PPP au niveau de la couche 2 et 3[28].

L2TP repos sur 2 concepts qui sont :

- **L2TP accès concentrateur(LAC) :**
  Il sert à fournir un moyen physique pour se connecter à un ou plusieurs LNS par le protocole L2TP. Il est responsable de l'identification et construit le tunnel vers les LNS. Il se trouve obligatoirement dans l'infrastructure du FAI de chaque utilisateur du VPN.
  Cela est donc très lourd (et cher) à mettre en place dans la mesure où il faut louer une place dans un serveur de connexion du fournisseur d'accès internet(FAI).
- **L2TP network server(LNS) :**
  Il assure la communication entre le réseau auquel il est connecté et les LAC vers lesquels il a un tunnel. Il se trouve généralement dans l'entreprise ou le service auquel appartient l'utilisateur distant.
  Voir la figure ci-dessous.

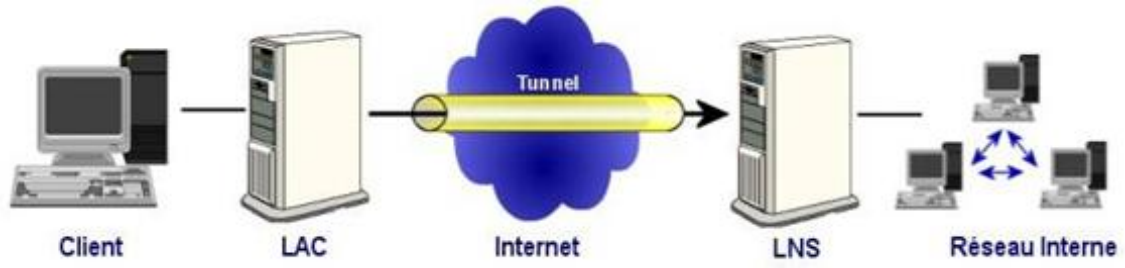


FIGURE 3.3 – protocole L2TP [21]

3.8.5 ***Protocole MPLS (Multi-Protocol Label Switching)***

MPLS (Multi-Protocol Label Switching) est un protocole de niveau 3 (réseau) qui permet d'établir un tunnel privé au sein d'un réseau public, il est utilisé par les fournisseurs d'accès à l'Internet pour proposer à leurs clients un moyen de créer un réseau privé entre plusieurs sites d'une même entreprise [29].

3.8.6 ***Protocole SSL/ TLS (Secure Sockets Layer) / (Transport Layer Security)***

Ce sont des protocoles permettant de sécuriser les échanges sur internet. Développé à l'origine sous le nom SSL par Netspace, l'IETF en reprend le développement en le rebaptisant TLS. Ce sont des protocoles très largement utilisé car les protocoles de la couche application, comme http , n'ont pas besoin d'être profondément modifiés pour utiliser une connexion sécurisée. Ils sont seulement implémentés au-dessus de ces protocoles, ce qui donne pour le http : Https. Il permet l'utilisation d'un navigateur Web comme client VPN [30].

3.8.7 ***Protocole SSH (Secure Shell)***

Ce protocole était souvent utilisé pour protéger des communications de type console (équivalent de Telnet) ou transferts de fichiers (de type FTP notamment). Son essor est limité à la fois par le succès grandissant de SSL/TLS et par son champ d'application plus restreint [31].

3.8.8 ***Protocole IPSEC (Internet Protocol Security)***

IPSEC est un protocole transportant des paquets (couche 3), issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP. Il est associé au protocole IKE pour l'échange des clés. Garantit la sécurité de transmission et l'authentification des utilisateurs sur les réseaux publics, offre la confidentialité et l'intégrité des données. Par conséquent, il peut être mis en œuvre indépendamment des applications qui s'exécutent sur le réseau [33]. Le protocole IP Sec est basé sur deux modules :

3.8.8.1 AH (Authentication Header)

concernant l'intégrité, l'authentification et la protection contre le rejeu des paquets à encapsuler [35].

3.8.8.2 ESP (Encapsulating Security Payload)

définissant le chiffrement de paquets. ESP fournit la confidentialité, l'intégrité, l'authentification et la protection contre le rejeu [35].

3.9 Les applications VPN existant

Dans ce qui suit les applications VPN les plus utilisés dans les grandes entreprises

3.9.1 ***Open VPN***

OpenVPN est un VPN open source. Il est conçu pour créer des réseaux privés virtuels (Virtual Privat networks) au-dessus d'internet en vue d'assurer la sécurité d'une

connexion, et ainsi empêcher la fuite ou la captation des données échangées entre le navigateur et une application ou un serveur distant. OpenVPN est aussi le nom du protocole de chiffrement mis en œuvre par l'application. [36]

3.9.2 ***Forticlient VPN***

Cette application FortiClient VPN de FortiNet permet de créer une connexion sécurisée de réseau privé virtuel (VPN) à l'aide de connexions IPSec ou SSL VPN "Mode tunnel" entre unappareil Android et le pare-feu FortiGate. La connexion sera entièrement cryptée et tout le trafic sera envoyé via le tunnel sécurisé, l'application FortiClient prend en charge le FortiToken. [37]

3.9.3 ***Anyconnect Cisco***

Le client VPN Cisco AnyConnect est une application logicielle pour la connexion à un réseau privé virtuel (VPN) qui fonctionne sur différents systèmes d'exploitation et configurations matérielles. Cette application logicielle permet aux ressources distantes d'un autre réseau de devenir accessibles comme si l'utilisateur était directement connecté à son réseau, mais de manière sécurisée. Le client Cisco AnyConnect Secure Mobility offre une nouvelle façon innovante de protéger les utilisateurs mobiles sur des plates-formes informatiques ou de Smartphones, offrant une expérience plus transparente et toujours protégée pour les utilisateurs finaux et une application complète des politiques pour les administrateurs informatiques. Cette application prend en charge les protocole Ipsec(Internet Protocol Security) et SSL(Secure Sockets Layer). [38]

3.10 Conclusion

Les réseaux VPN sont la meilleure solution pour les entreprises pour la réalisation de leurs réseaux étendus car ils combinent la sécurité de l'information à des prix les plus bas. L'avantage des approches par MPLS/IPSEC est la souplesse de d'installation et de dépannage du VPN.

Chapitre 4

Configuration et Implémentation

4.1 Introduction

Ce chapitre consiste à mettre en œuvre les solutions proposées pour la réalisation de notre projet, en exposant les différentes configurations nécessaires à implémenter sur le LAN. Comme nous n'avons pas pu utiliser le réseau de NAFTAL, (à cause de de droits d'accès), nous avonc été obligé de simuler sur GN3 un sous-réseau qui nous permettra d'utiliser le VPN mobile avec OpenVPN.

Ces configurations consistent en la configuration des VLANs, VTP et le routage inter vlan, ensuite la configuration du serveur de gestion et administration (AD), DNS et DHCP, et enfin la configuration de la partie VPN et VPN Mobile en se basant sur le logiciel open source GNS 3, l'hyperviseur VMware Workstation et l'application Open VPN. Pour présenter les configurations que nous avons réalisées, nous nous sommes servies des captures d'écran qui illustrent les étapes de la configuration afin d'éclaircir chaque composant de cette dernière et son fonctionnement. Enfin, des tests de validation sont effectués pour confirmer le bon fonctionnement du réseau seront réalisés.

4.2 Présentation de l'environnement de travail

4.2.1 ***Installation de GNS3 sous Windows***

GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques. [1]

Pour installer GNS3 (logo donné en figure 4.1), il faut tout d'abord télécharger le fichier exécutable, ensuite le lancer et suivre les étapes d'installation jusqu'à la fin puis cliquer sur le bouton "Finish".

FIGURE 4.1 – GNS3

4.2.2 ***Installation de VMware Workstation pro***

VMware Workstation est un outil de virtualisation il permet de créer de nouvelles machines virtuelles, transformer un PC en une machine virtuelle et effectuer un déploiement en masse.

Afin de créer les machines utilisateurs virtuelles au sein du même pc, nous allons installer VMware Workstation en suivant les étapes d'installations (donnés dans l'annexe ?)jusqu'à la fin puis cliquer sur le bouton "terminer". La figure 4.2 présente L'interface graphique de VMware Workstation pro.

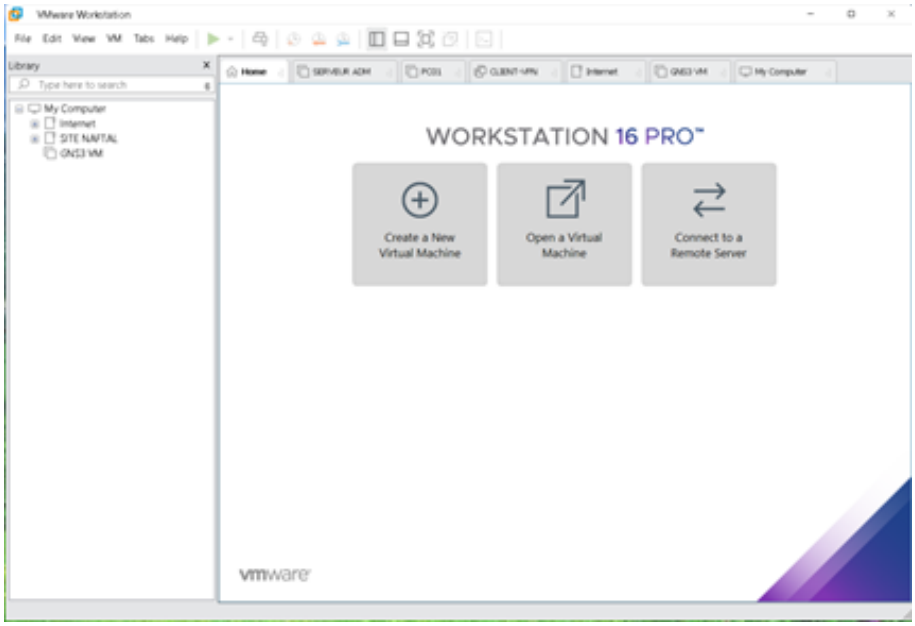


FIGURE 4.2 – L'interface graphique de VMware Workstation pro 16

4.2.3 ***Wireshark***

Wireshark est un analyseur de protocole réseau gratuit et open source qui permet aux utilisateurs de parcourir de manière interactive le trafic de données sur un réseau informatique. La figure 4.3 présente L'interface graphique de Wireshark.

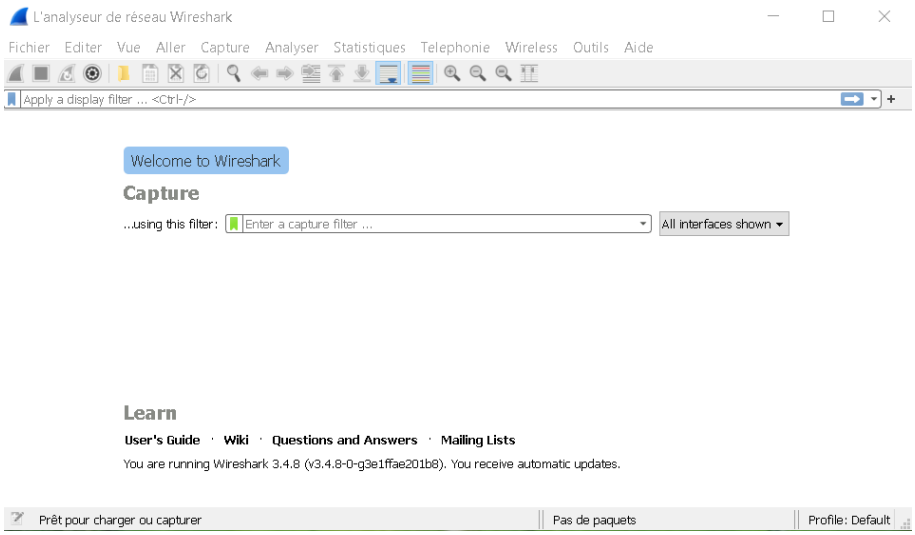


FIGURE 4.3 – L'interface graphique de wireshark

4.2.4 ***Les machines virtuelles***

4.2.4.1 Le pfSense

pfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états Packet Filter ainsi que des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques.

Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise.

4.2.4.2 Windows serveur 2022

Windows Server 2022 est l'actuel système d'exploitation commercialisé par Microsoft et destiné aux serveurs. Le système offre une sécurité multicouche avancée, des fonctionnalités hybrides avec Azure et une plateforme d'application flexible.

4.2.4.3 Windows 10

Windows 10 est un système d'exploitation de la famille Windows NT développé par la société américaine Microsoft.

4.3 Architecture proposée

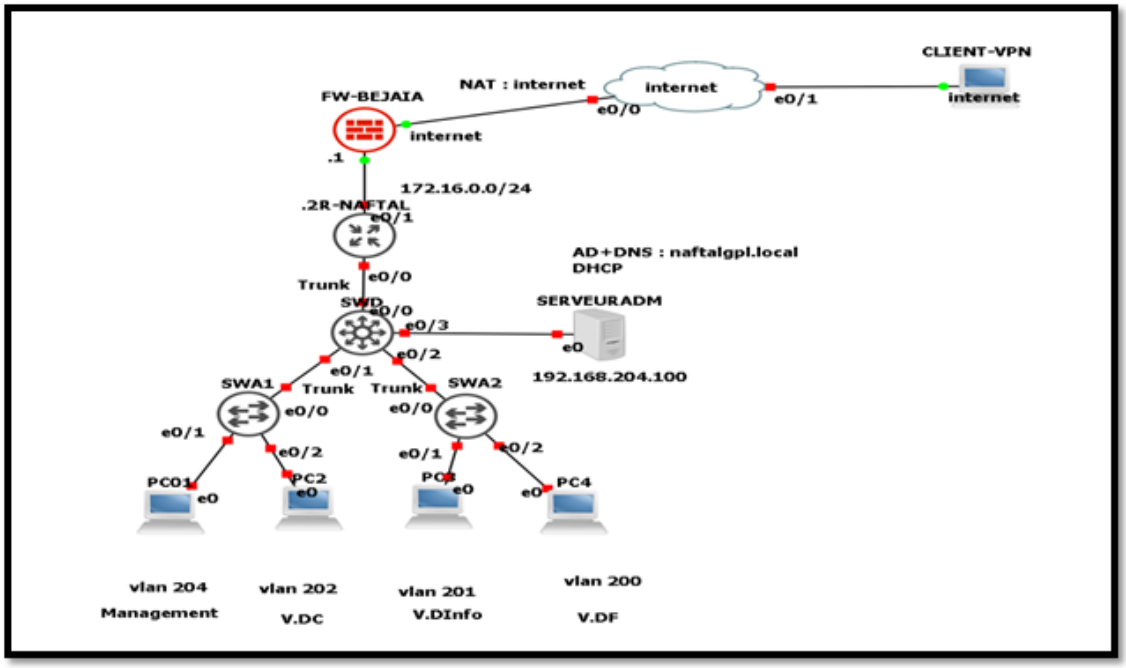


FIGURE 4.4 – Architecture de réseau proposée

4.4 Tableaux des équipements d'interconnexion

Equipement	**Fournisseur**	**Nom équipement**	**Système**
Routeur Cisco2911	Cisco	R-NAFTAL	los
Switch Cisco2911	Cisco	Switch distribution	los
Switches catalyst 2960	Cisco	Switch accès 1 et 2	los
Pfsense	Netgate	FW-Bejaia	FREE BSD
Serveur DELL R830	DELL	Serveur ADM	WINDOWS

TABLE 4.1 – Les équipements

4.5 Adressage

4.5.1 Tableau d'adressage des équipements

Device	interface	Adresse ip	Description	passerelle
R-naftal	E0/0	Sous interfaces	Connecter au SWD	//
	E0/1	172.16.0.2/24	connecter au pfsense	//
Switch distribution SWD	E0/0	En mode trunk	Connecter au routeur	//
	E0/1	En mode trunk	Connecter au SWA1	//
	E0/2	En mode trunk	Connecter au SWA2	//
	E0/3	VLAN 204	Connecter au serveur	//
Serveur	E0	192.168.204.100/24	Connecter au SWD	//
Switch accès 1 SWA1	E0/0	En mode trunk	connecter au SWD	//
	E0/1	En mode accès	connecter au vlan 204	//
	E0/2	En mode accès	connecter au vlan 202	//
Switch accès 2 SWA2	E0/0	En mode trunk	connecter au SWD	//
	E0/1	En mode accès	connecter au vlan201	//
	E0/2	En mode accès	connecter au vlan 200	//
pfsense	E0/0	NAT	connecter a internet	//
	E0/1	172.16.0.1/24	connecter au routeur	172.16.0.1
Client-vpn	E0/1	Open vpn (internet)	connecter a internet	//
D.F	E0	DHCP	connecter au vlan 200 et vlan Voice	//
D.info	E0	DHCP	connecter au vlan 201 et vlan Voice	//
D.C	E0	DHCP	Connecter au vlan 202 et vlan Voice	//
management	E0	DHCP	connecter au vlan 204 et vlan Voice	//

TABLE 4.2 – d'Adressage des équipements

4.5.2 ***Tableau des Vlans***

Nom vlans	**IP vlans**	**Réseau/préfixe**
Département finances	200	192.168.200.0/24
Département informatique	201	192.168.201.0/24
Département commercial	202	192.168.202.0/24
Vlan voix	203	192.168.203.0/24
Vlan management	204	192.168.204.0/24
Vlan native	99	//////////////////

TABLE 4.3 – Tableau des Vlans

4.5.2.1 Tableau de routage inter-vlan

Equipements	Encapsulation 802.1q	Interface	Adresse IP /préfixe
R-NAFTAL	200	0/0.200	192.168.200.1/24
	201	0/0.201	192.168.201.1/24
	202	0/0.202	192.168.202.1/24
	203	0/0.203	192.168.203.1/24
	204	0/0.204	192.168.204.1/24

TABLE 4.4 – Tableau de routage inter-Vlan

4.6 Configuration de base sur le serveur

4.6.1 Distribuer une adresse IP fixe au serveur

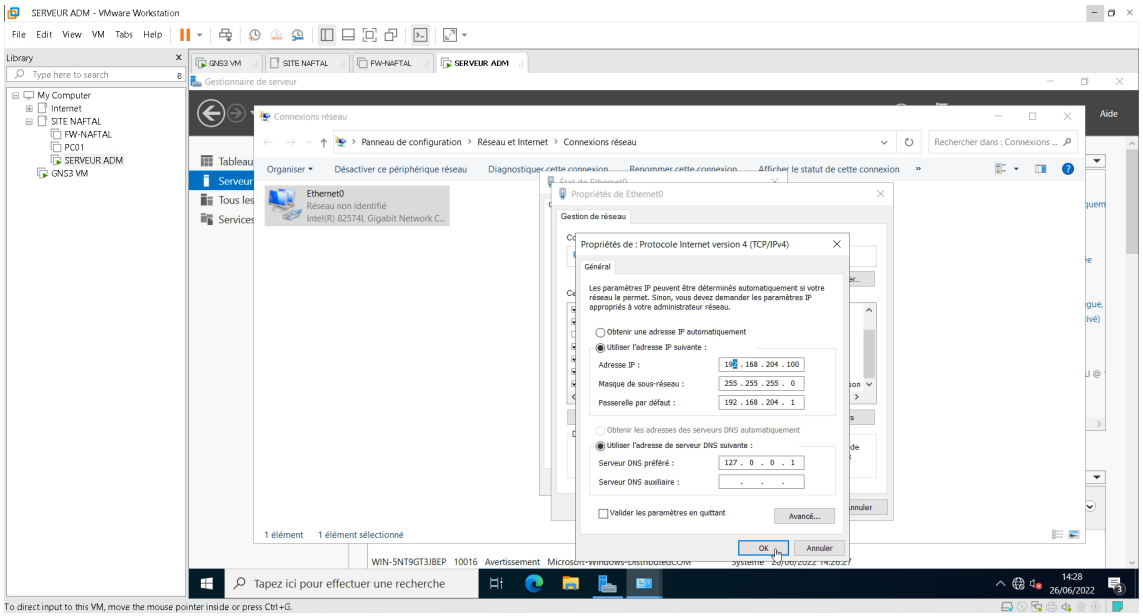


FIGURE 4.5 – Configuration de serveur

4.6.2 Installer l'active directory dans le serveur

Sur la machine Windows serveur 2022 nous avons installé un contrôleur de domaine dont le nom de domaine est Naftalgpl.local.

Pour commencer l'installation, il va falloir ajouter le Service de Rôle Active Directory, lancer l'installation et ajouter les fonctionnalités qui nous manquent.
Voici les étapes d'installation aclive directory. Dans le gestionnaire de serveur :

- on choisit ajouter des rôles et fonctionnalités.
- On sélectionne le serveur destination.
- On choisi le rôle active directory.
- On lance l'installation.

Le DNS sera installé automatiquement en parallèle avec l'active directory.

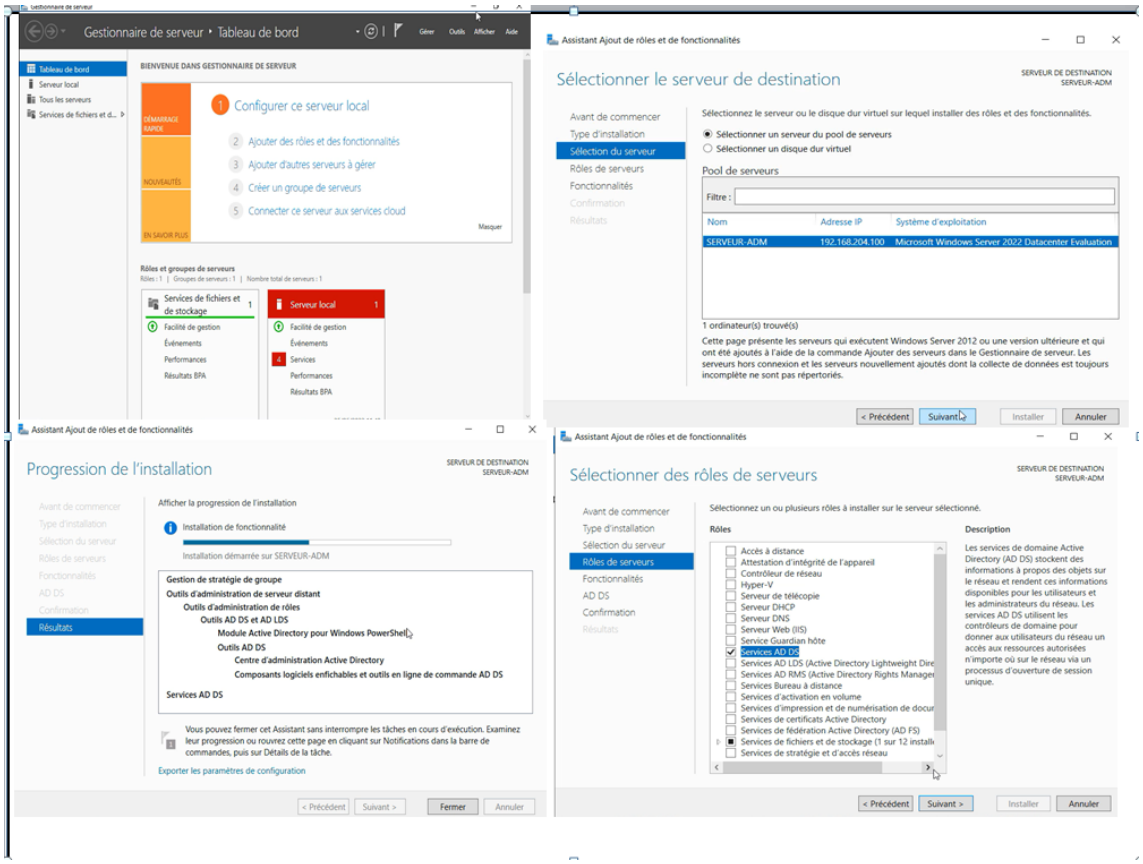


FIGURE 4.6 – L'Installation active directory

4.6.3 ***Configuration d'Active Directory***

Maintenant nous allons commencer la configuration de notre Active Directory. La première étape consiste à créer une nouvelle foret, nommé naftalgpl.local. Le nom affecté, Windows nous demande de choisir le niveau fonctionnel de notre foret Active Directory.

Dans notre exemple, nous mettrons un niveau fonctionnel 2016. Windows nous propose ensuite d'installer des options supplémentaires, tel qu'un serveur DNS compatible avec notre Active Directory. Le domaine créé naftalgpl.local est notre premier contrôleur de domaine catalogue global activé. Lorsque les services sont installés et configurés, on clique sur FIN et le système devra redémarrer. A la fin de l'installation on aura les deux rôles installés comme le montre la figure 4.7 :

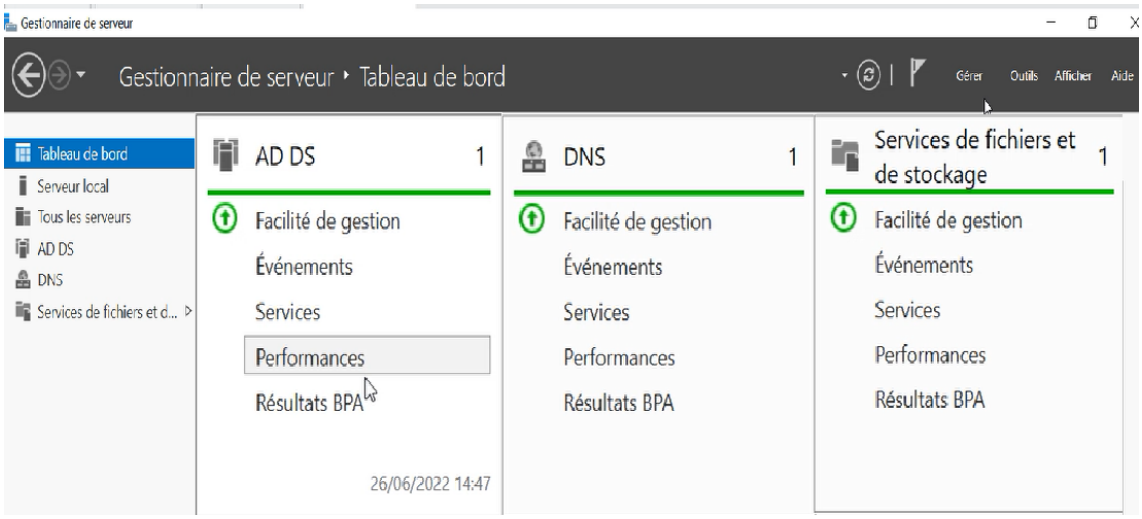


FIGURE 4.7 – Les rôles AD DS et DNS

4.6.4 Installation de DHCP

Nous avons installé DHCP server sur la machine Windows server 2022 Pour commencer l'installation, il va falloir ajouter le Service de DHCP Server et ajouté les fonctionnalités necessaires.

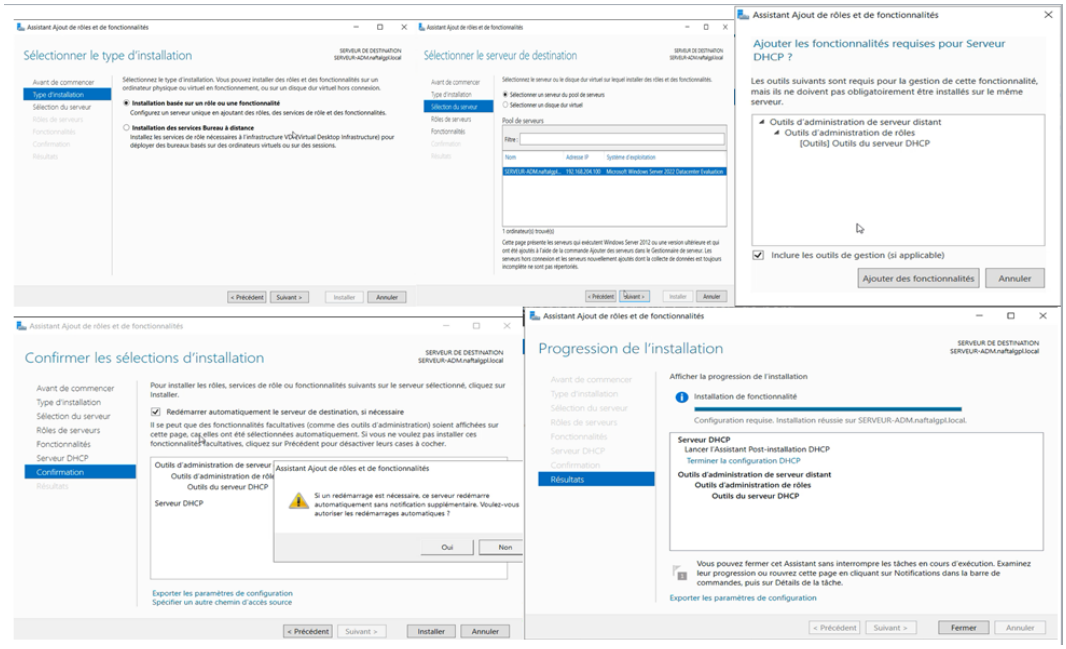


FIGURE 4.8 – Installation de DHCP

Pour relier le DHCP avec l'active directory il suffit de valider le nom d'utilisateur pour autoriser la relation.

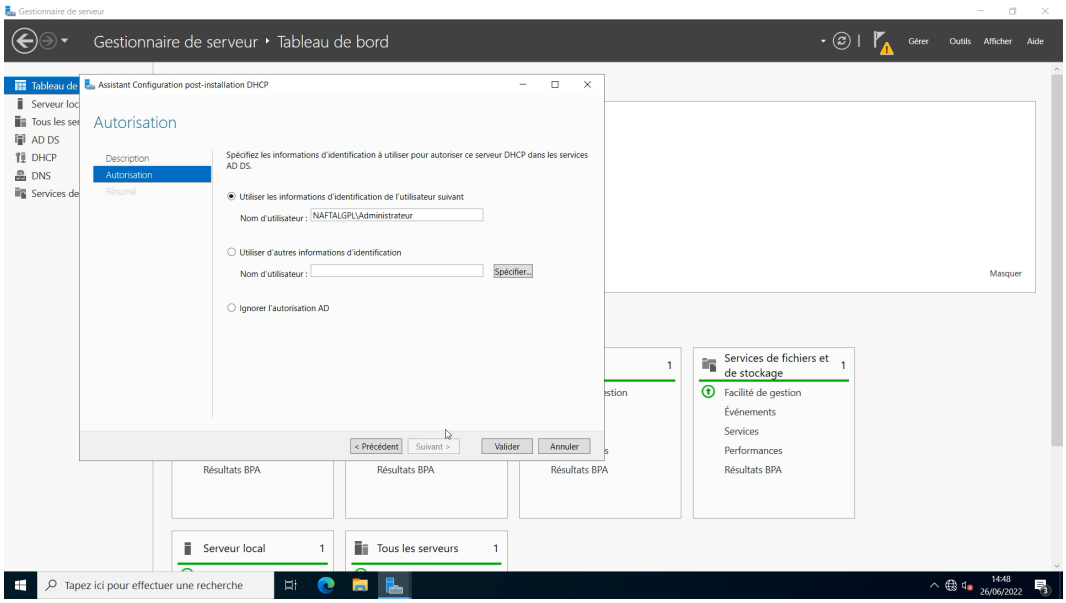


FIGURE 4.9 – Relier DHCP avec l'actif directory

4.6.5 Configuration DHCP

Pour créer un pool d'adresse pour chaque Vlan (distribution des adresses pour chaque vlan) on clique sur IPV4.
Etape1 : donner le nom et la description de vlan

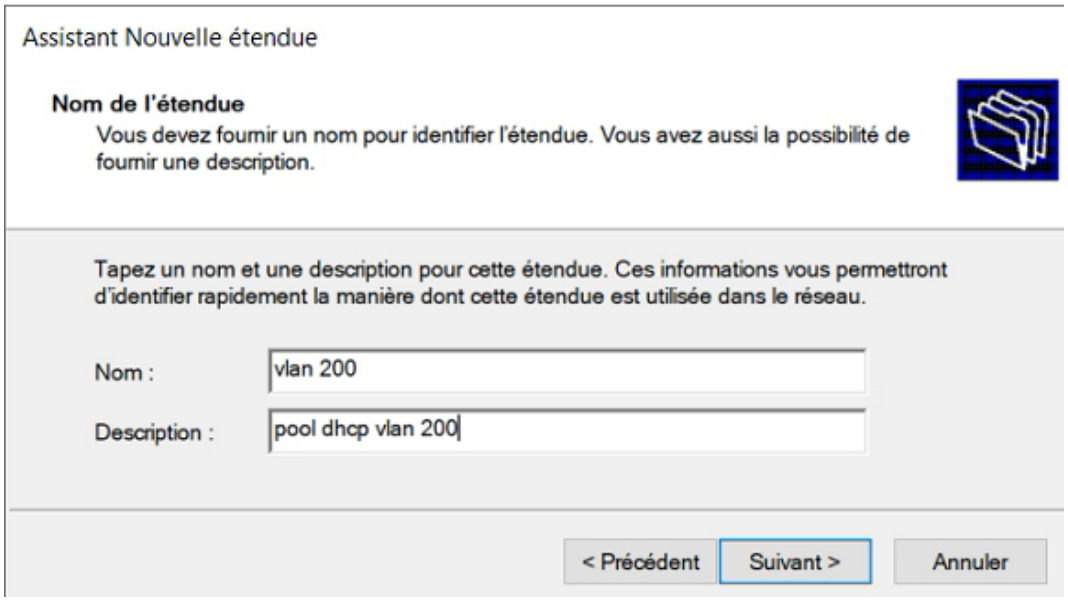


FIGURE 4.10 – Nom et description de vlan

Etape2 : distribution des adresses pour les vlans

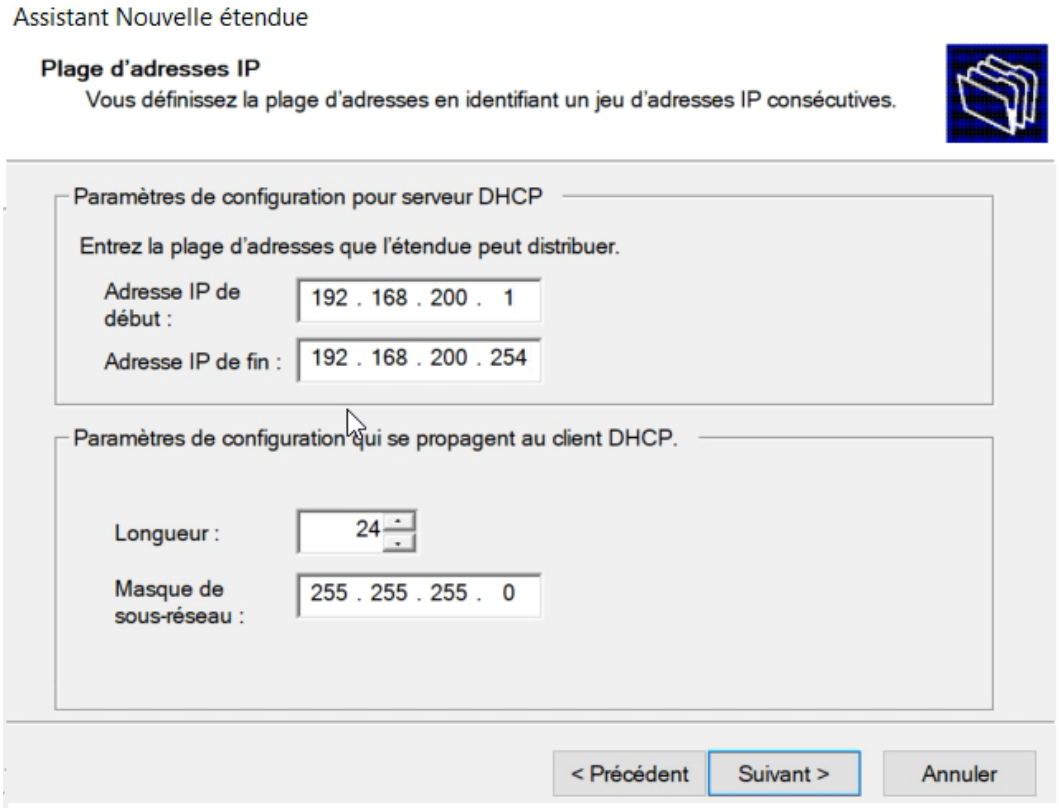


FIGURE 4.11 – Paramétrer les adresses des Vlan

Etape3 : On va exclure les 10 premières adresses par exemple la passerelle qui sont réservé pour les serveurs statiques.

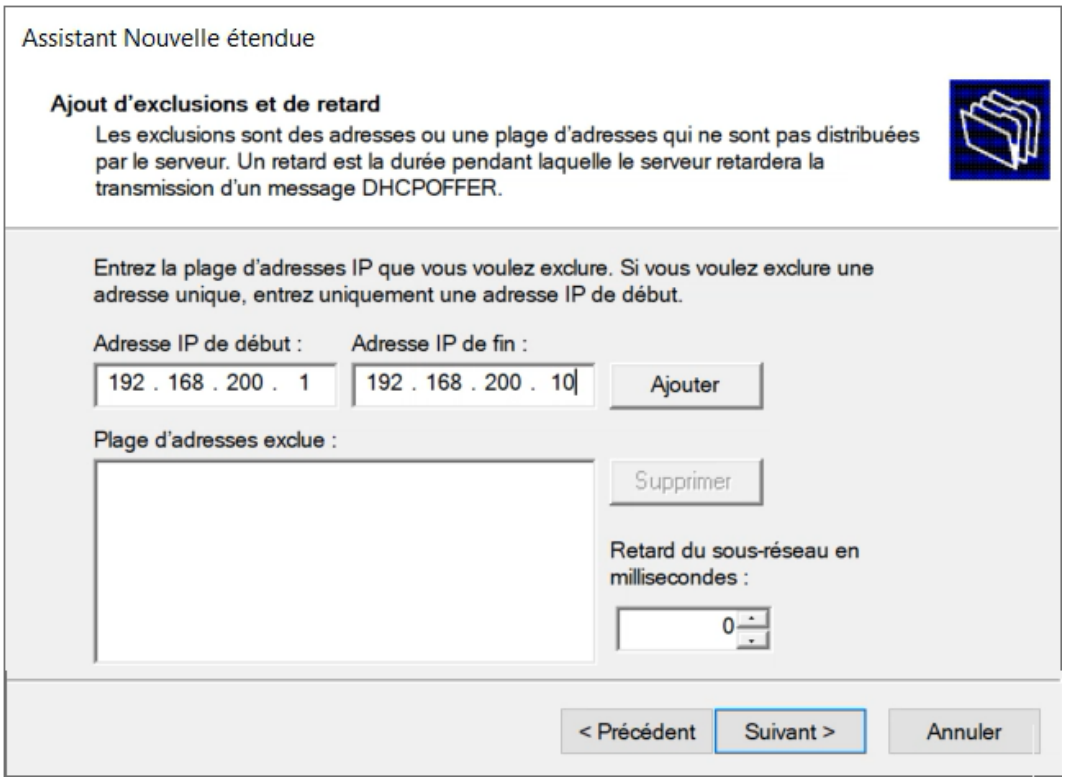


FIGURE 4.12 – Exclusion des 10 premières adresses

Ensuite on active l'étendu et configurer les options (la Gateway, DNS, la passerelle)
- Configurer la passerelle 192.168.200.1
- 8.8.8.8 pour les configurer sur internet et c'est la même méthode pour les autres étendu. C'est de cette manière qu'on na configurer tous les vlans sur le serveur DHCP (tous les étendu sont activer) (voir figure 4.13).

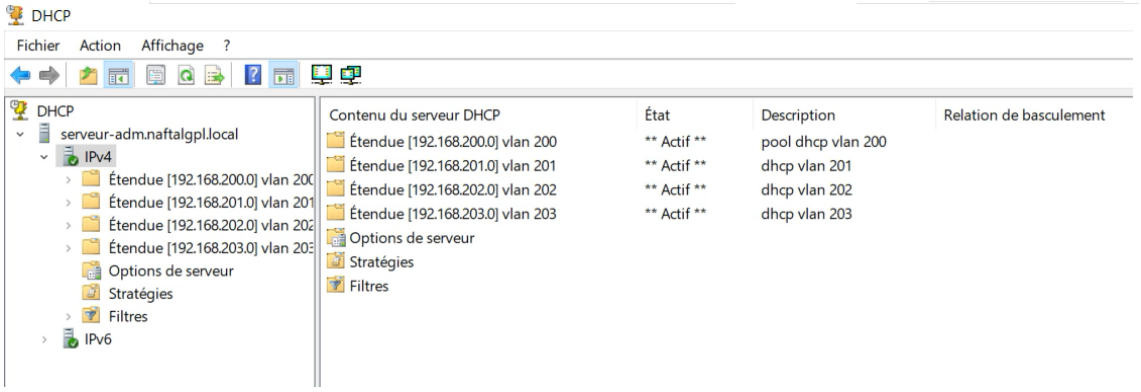


FIGURE 4.13 – Les étendus des vlans configurer

4.6.6 Configuration d'utile d'organisation NAFTAL

Créer l'utile d'organisme NAFTAL GPL Bejaia dans laquelle on crée les utilisateurs

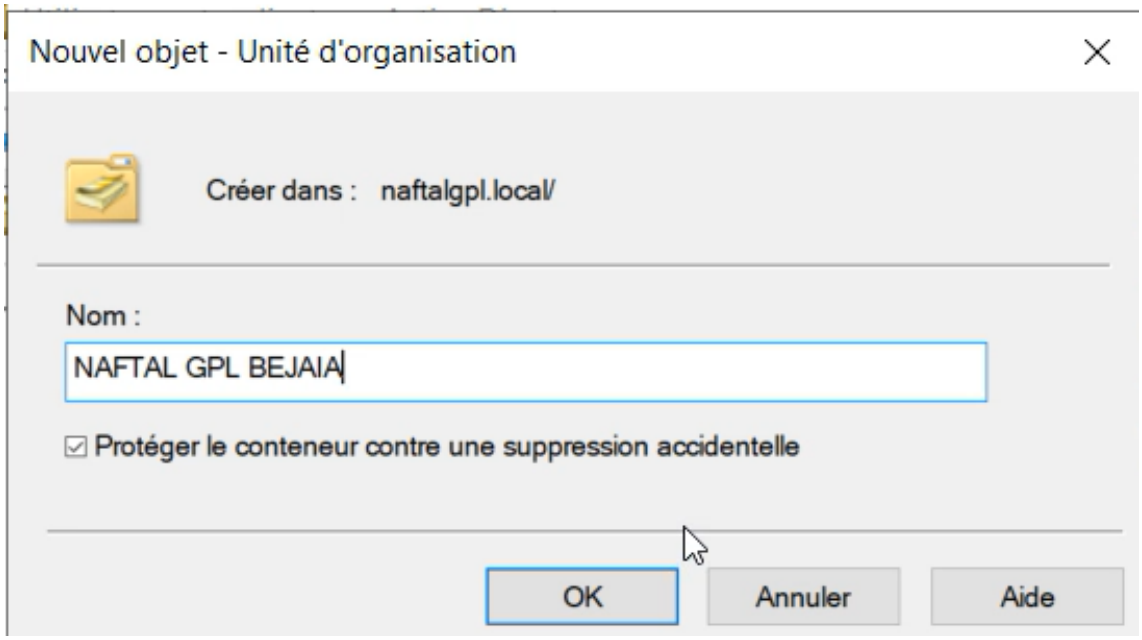


FIGURE 4.14 – Création d'utile d'organisation

La création des utilisateurs par le serveur active directory

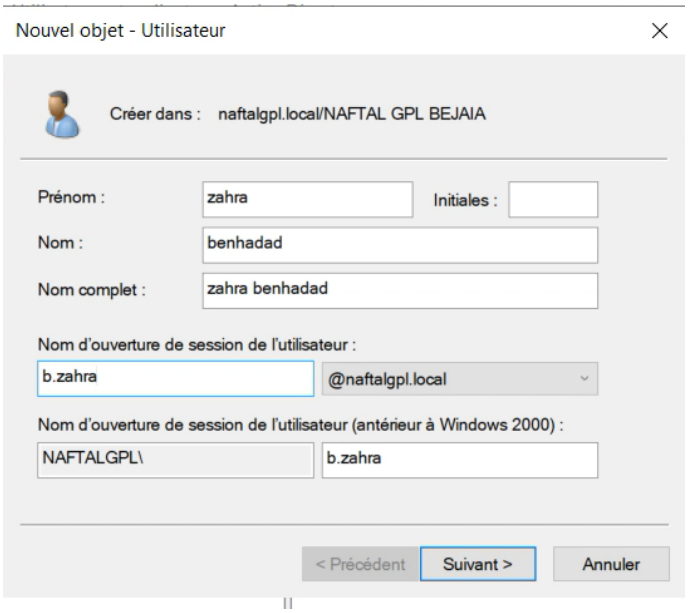


FIGURE 4.15 – Création d'utilisateur 1

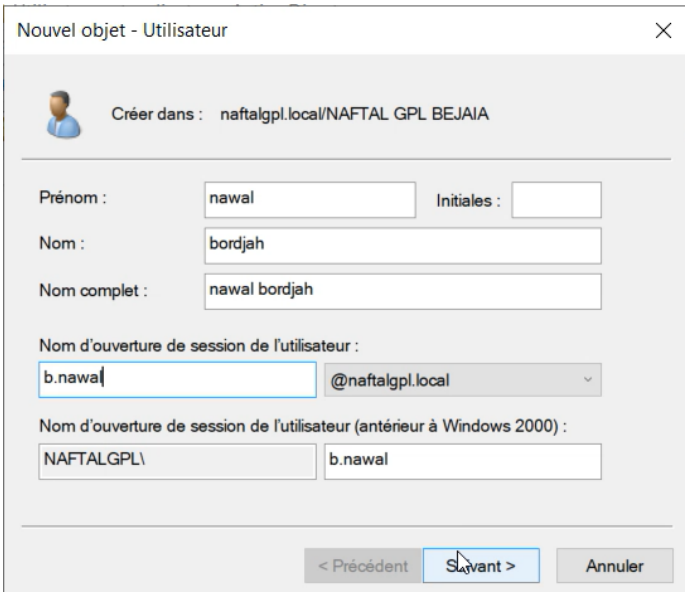


FIGURE 4.16 – Création d'utilisateur 2

Créer les départements de l'entreprise comme département commercial et informatique.

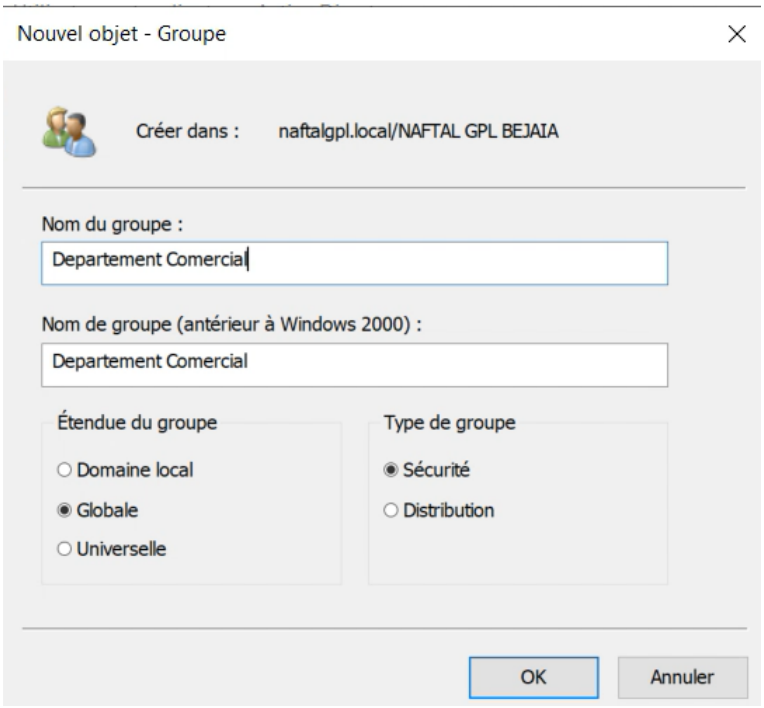


FIGURE 4.17 – Création de département commercial

On crée les autres départements de la même façon. Relier les deux utilisateurs 1 et 2 au département informatique :

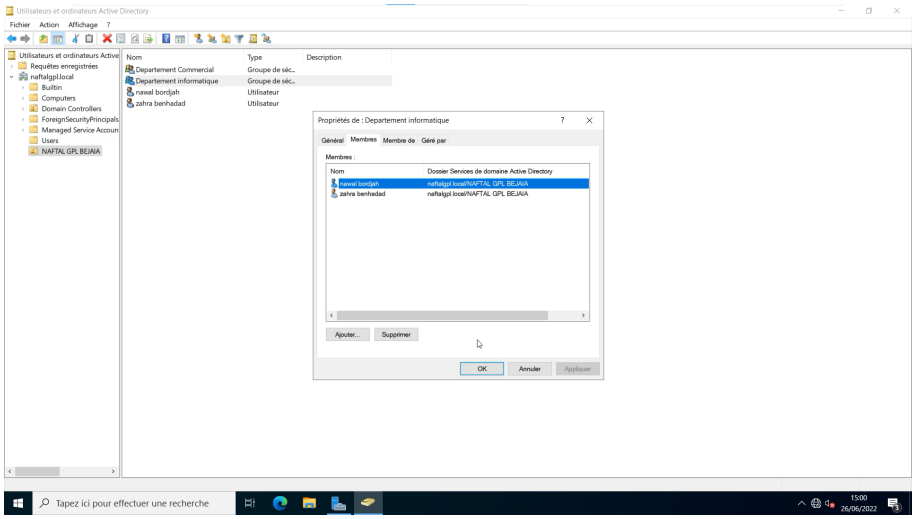
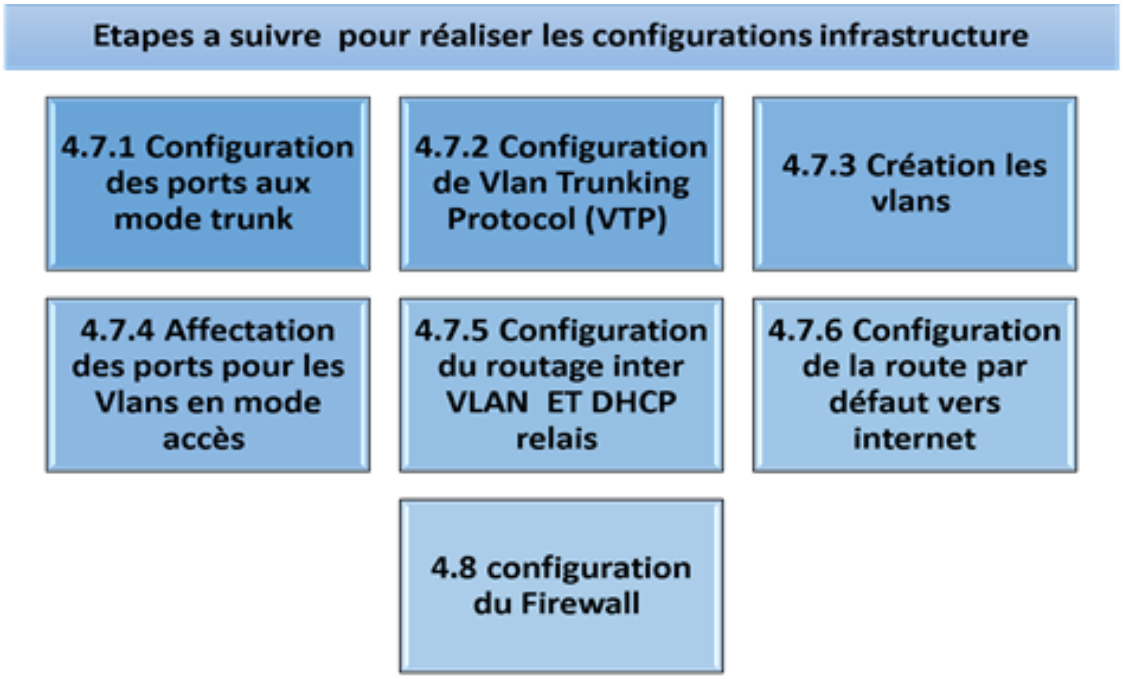


FIGURE 4.18 – Relier les deux utilisateurs au département

4.7 Configuration infrastructure

Configurertoutes les interfaces des switches en mode trunk pour configurer de telle sorte que l'on peut y faire circuler des trames Ethernet modifiées comportant des informations

relatives au VLAN sur lequel elles transitent.



4.7.1 Configuration des ports au mode trunk

- Switch Distribution

```
SWD#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD(config)#inter
SWD(config)#interface range eth
SWD(config)#interface range ethernet 0/1-2
SWD(config-if-range)#swit
SWD(config-if-range)#switchport tru
SWD(config-if-range)#switchport trunk enc
SWD(config-if-range)#switchport trunk encapsulation do
SWD(config-if-range)#switchport trunk encapsulation dot1q
SWD(config-if-range)#swit
SWD(config-if-range)#switchport mode tr
SWD(config-if-range)#switchport mode trunk
SWD(config-if-range)#exit
SWD(config)#
```

FIGURE 4.19 – Configuration des interfaces aux mode trunk Switch distribution

- Switch Access

```
SWA1(config)#in
SWA1(config)#interface  eth
SWA1(config)#interface  ethernet 0/0
SWA1(config-if)#sw
SWA1(config-if)#switchport tr
SWA1(config-if)#switchport trunk en
SWA1(config-if)#switchport trunk encapsulation do
SWA1(config-if)#switchport trunk encapsulation dot1q
SWA1(config-if)#sw
SWA1(config-if)#switchport mo
SWA1(config-if)#switchport mode tr
SWA1(config-if)#switchport mode trunk
SWA1(config-if)#
SWA1(config-if)#end
SWA1#
SWA1#wr
*Jun 26 14:59:33.713: %SYS-5-CONFIG_I: Configured from console by console
```

FIGURE 4.20 – Configuration des interfaces trunk sur les switch d'Access

4.7.2 Configuration de Vlan Trunking Protocol (VTP)

Le VTP facilite la gestion des VLANs, il a trois modes de configuration :
- **Mode serveur :** Centraliser les commandes dans le switch de distribution.
- **Mode client :** Appliquer la configuration dans les switches d'accès.
- **Mode transparence :** diffuser la configuration des switches.

♦ Configuration de VTP en mode serveur :

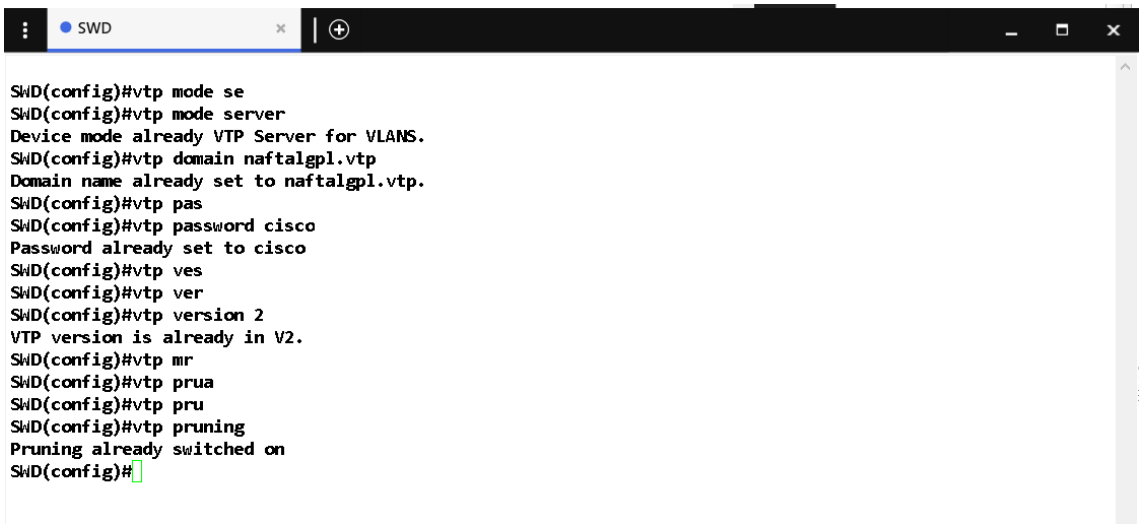


FIGURE 4.21 – Configuration de VTP en mode serveur

♦ Configuration de VTP en mode client :

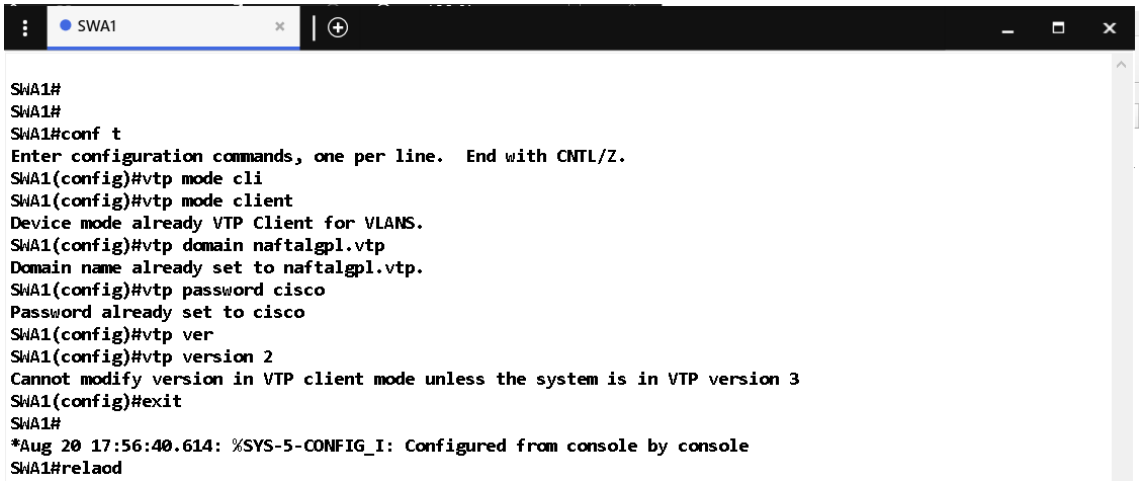


FIGURE 4.22 – Configuration de VTP en mode client

4.7.3 Création les vlans

♦ Switch distribution :

Après la configuration du serveur VTP, on passe à la création des vlans ce dernier va diffuser pour les Clients VTP qui va appliquer la configuration.

```
SWD#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD(config)#
SWD(config)#vlan 200
SWD(config-vlan)#name D.F
SWD(config-vlan)#vlan 201
SWD(config-vlan)#name D.INF
SWD(config-vlan)#vlan 202
SWD(config-vlan)#name D.C
SWD(config-vlan)#
SWD(config-vlan)#vlan 203
SWD(config-vlan)#name voice
SWD(config-vlan)#vlan 204
SWD(config-vlan)#name management
SWD(config-vlan)#vlan 99
SWD(config-vlan)#name native
SWD(config-vlan)#
SWD(config-vlan)#
SWD(config-vlan)#end
SWD#
```

FIGURE 4.23 – création des vlans dans le switch SWD

♦ La vérification des vlans crées sur le switch distribution :
Tous les vlans sont reçu la configuration (voir figure 4.24).

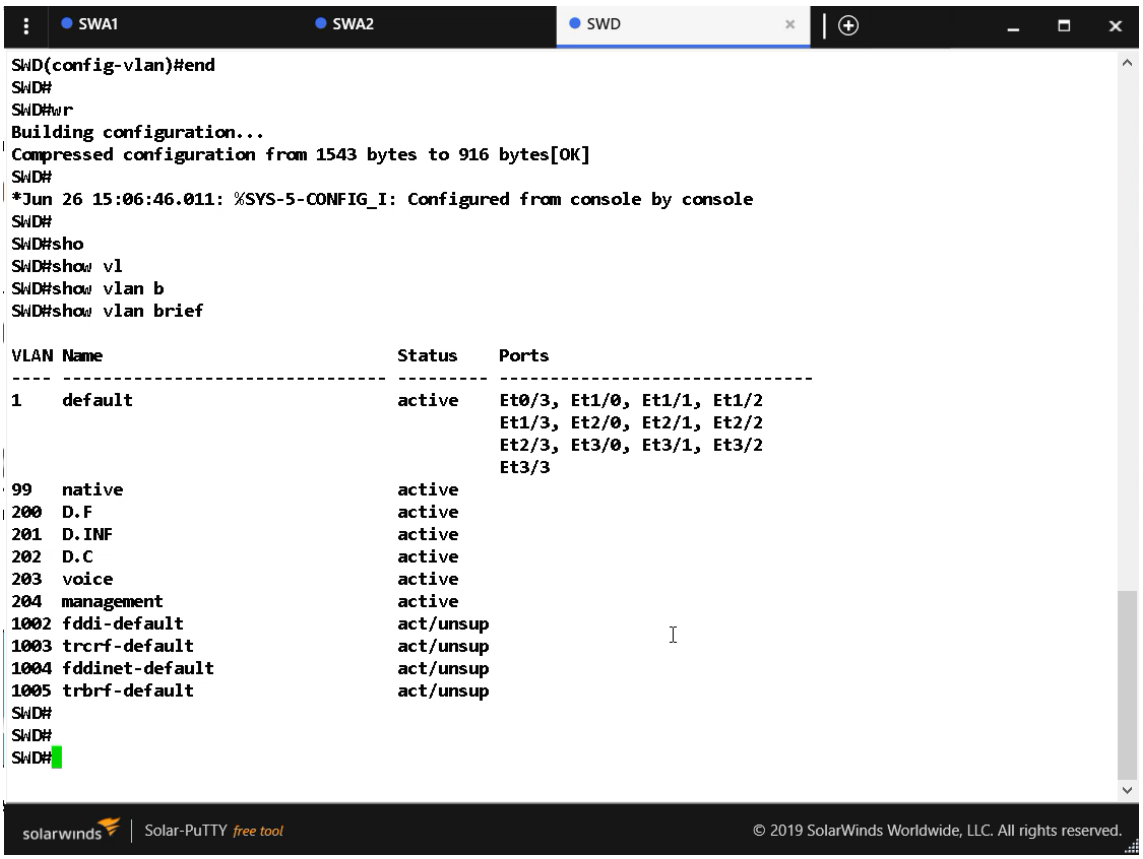


FIGURE 4.24 – vérification des vlanscrées

4.7.4 Affectation des ports pour les Vlans en mode accès

Tousles ports doivent avoir un accès vocal (tous les départements doivent avoir la téléphonie).

```
SWA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA1(config)#interfa
SWA1(config)#interface eth
SWA1(config)#interface ethernet 0/1
SWA1(config-if)#swit
SWA1(config-if)#switchport mode ac
SWA1(config-if)#switchport mode access
SWA1(config-if)#swit
SWA1(config-if)#switchport acce
SWA1(config-if)#switchport access vlan
SWA1(config-if)#switchport access vlan 204
SWA1(config-if)#swit
SWA1(config-if)#switchport voi
SWA1(config-if)#switchport voice vlan 203
SWA1(config-if)#
```

FIGURE 4.25 – Affectation des ports pour les Vlans en mode accès

♦ Test d'affectation des ports au vlans

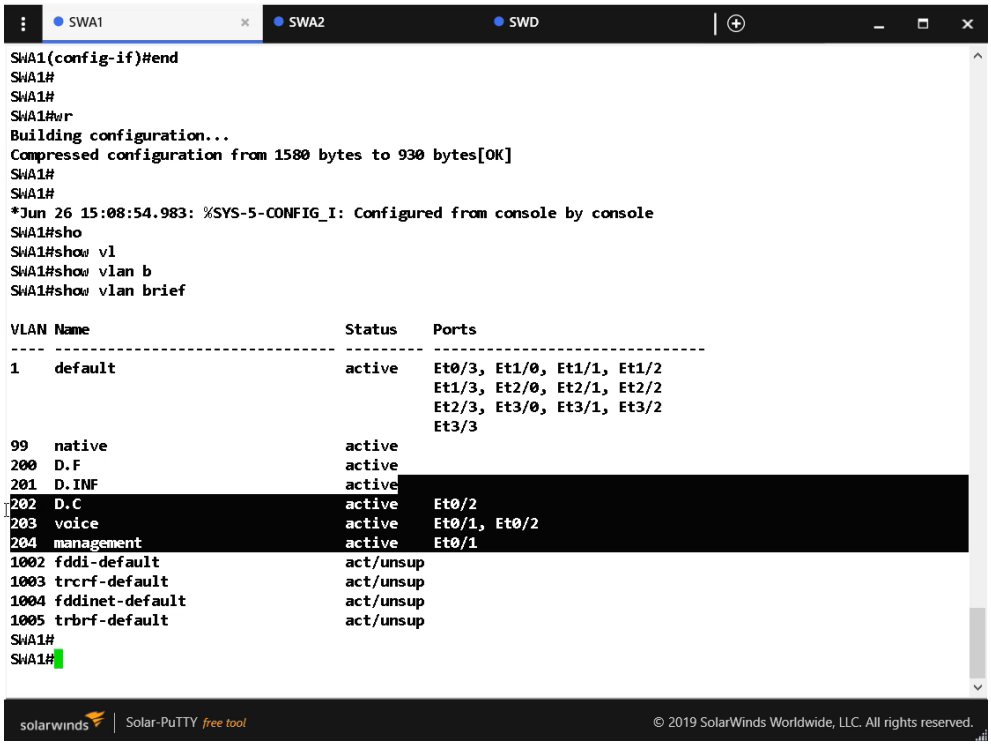


FIGURE 4.26 – Test d'affectation des ports au vlans

Ensuit les mêmes étapes pour le switch d'accès 2 et le switch distribution (SWD n'a pas besoin de voix).

4.7.5 Configuration du routage inter_VLAN ET DHCP relais

Les étapes des configurations comme suit :

- Création des sous interfacespour chaque vlan .
- Configuration de l'encapsution 802.1Q pour chaque interface
- Configuration des adresses " passerelle par défaut pour chaque vlan33 "
- Configuration de l'agent relais pour chaque sous interface afin de permettre les diffusions des message DHCP en indiquant a chaque sous interface l'adresse ip du serveur avec la commande ip helper-address 192.168.204.100 ;

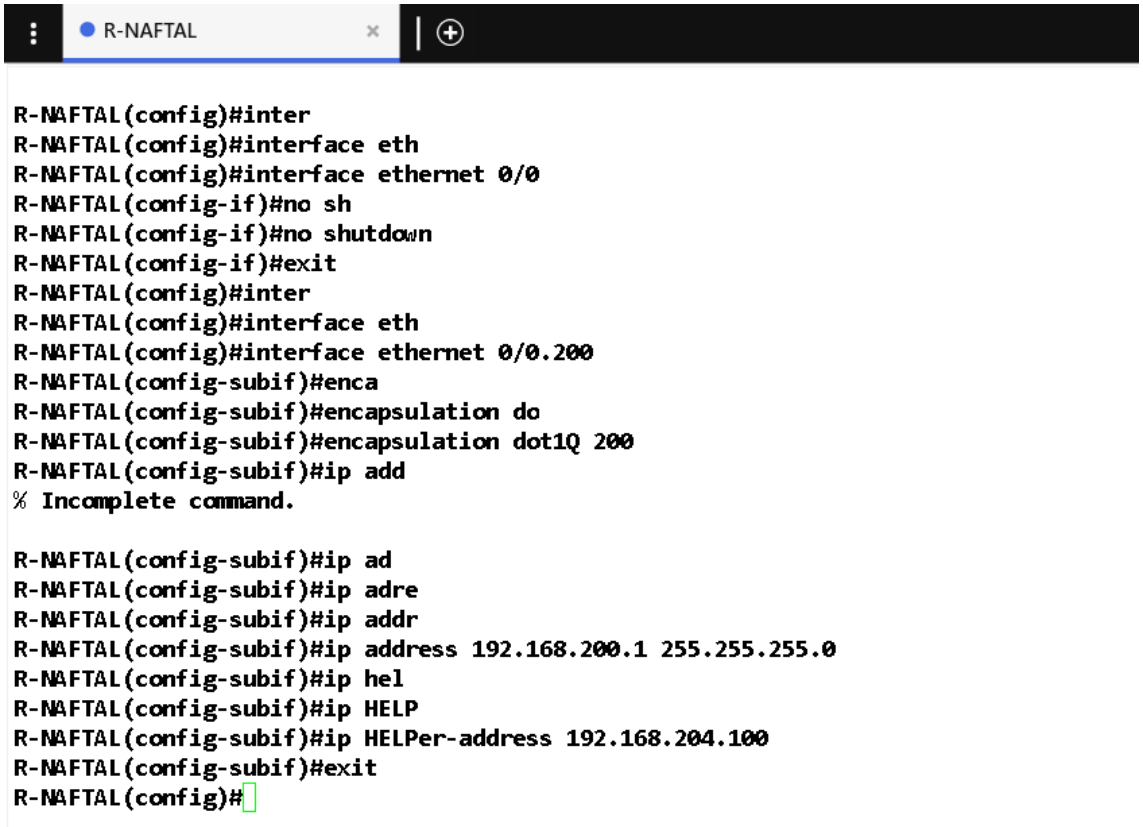


FIGURE 4.27 – Configuration du routage intervlan et dhcp relais

4.7.6 Configuration de la route par défaut vers internet

Afin de router le Traffic des vlans vers internet, nous devons configurer la route par défaut en utilisant la commande ip route 0.0.0.0 0.0.0.0 et indiquer l'interface de sortie vers internet.

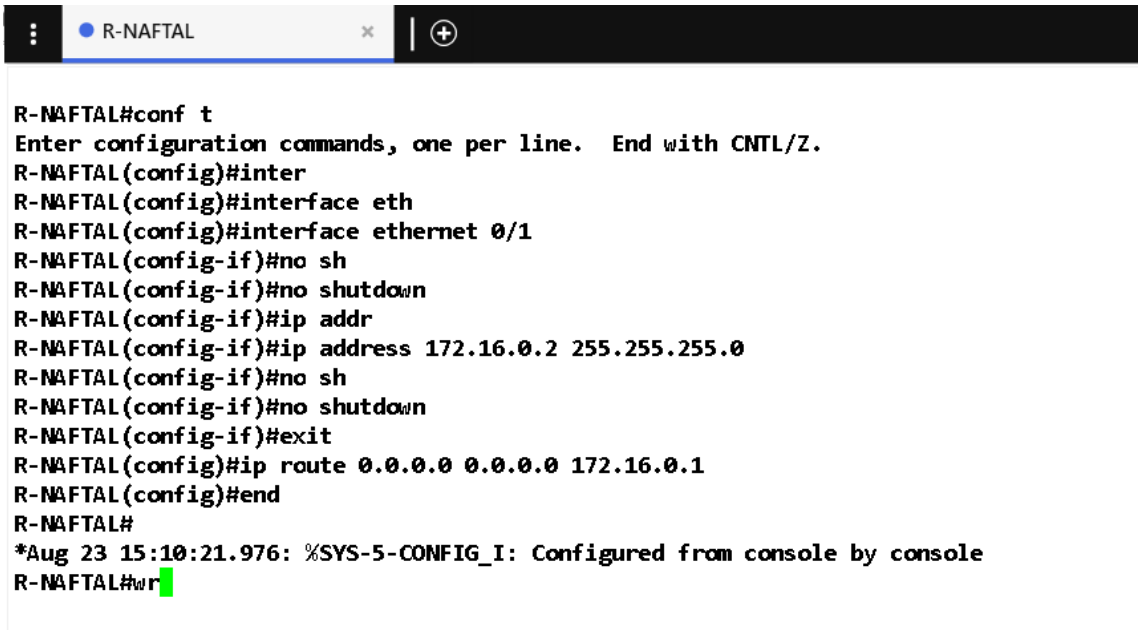


FIGURE 4.28 – Routage des Vlans vers l'internet

4.8 Configuration du Firewall

♦ **étape 1 :** sur pfSense saisir user Name et mot de passe

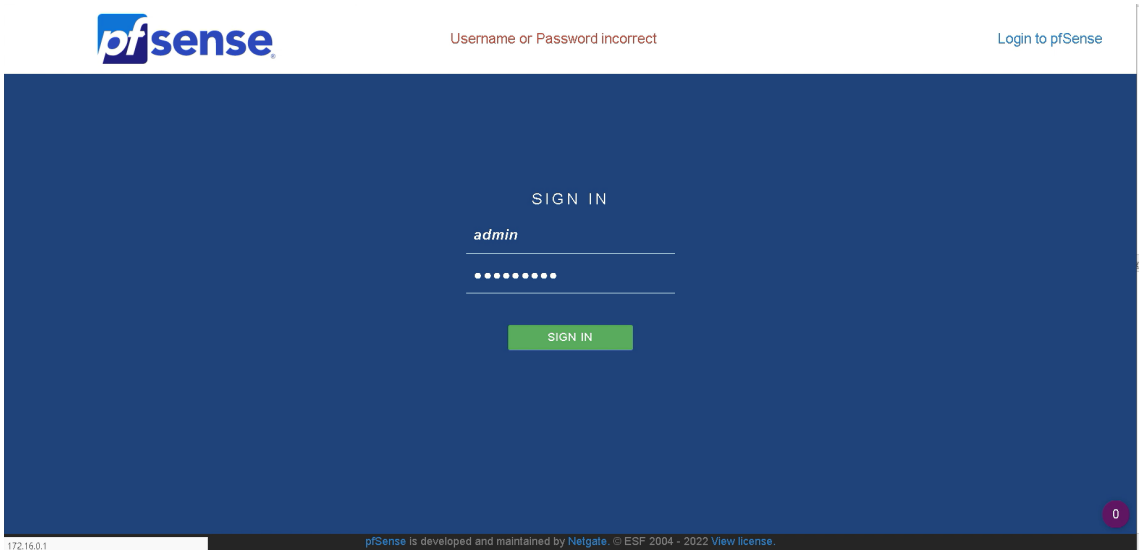


FIGURE 4.29 – Page d'accueil de pfsense

♦ **étape 2 :** configuration de pfSense en donnant le hostname, domaine, DNS et DNS connecté à internet.

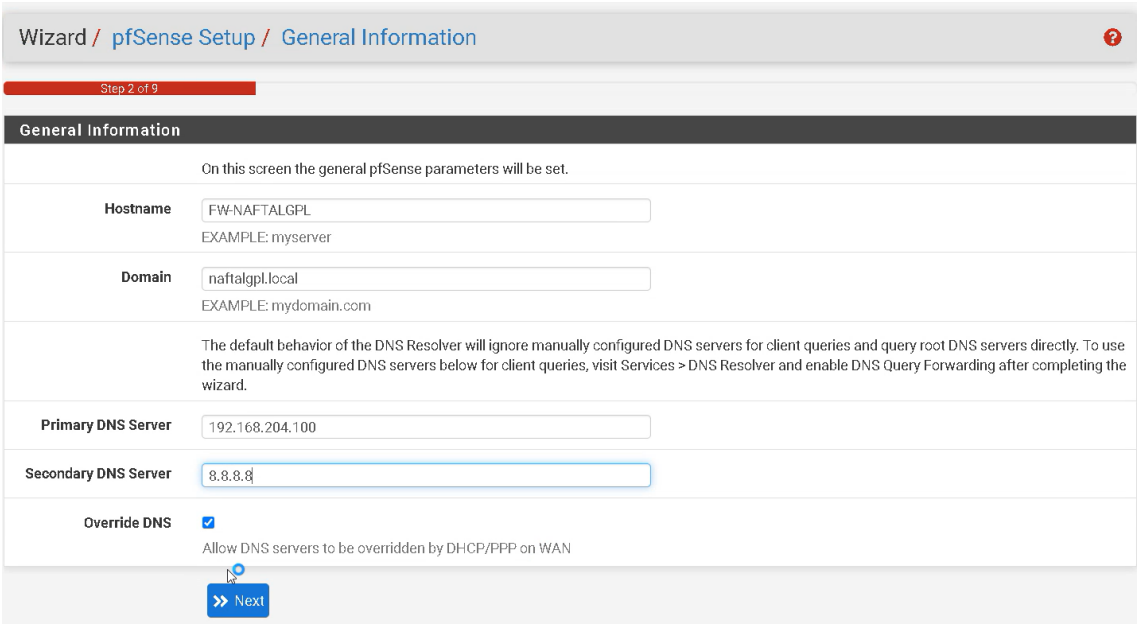


FIGURE 4.30 – configuration de pfSense

♦ **étape 3 :** changer le mot de passe de pfSense

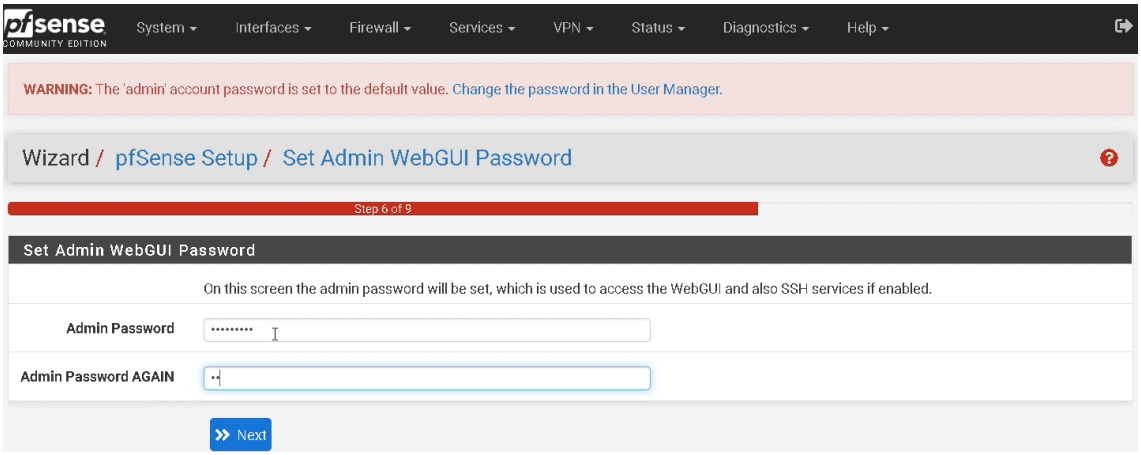


FIGURE 4.31 – changement de mot de passe

♦ **étape 4 :** dans cette étape on va préciser les vlans sur la partie firewall, ensuite on va autoriser que le IPV4 , puis on change la source, au lieu de Lannet, on met Any.

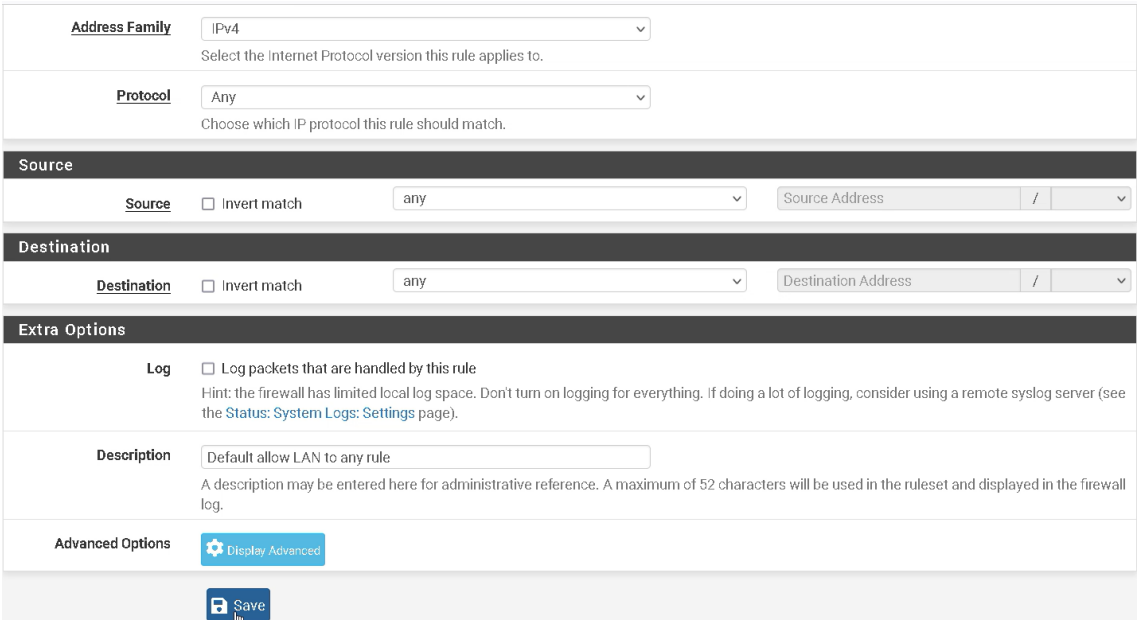


FIGURE 4.32 – changement du source de IPV4

♦ **étape 5 :** Paramétrer la Gateway vers les VLANs
D'abord on va donner un nom pour la Gateway ensuite adresse IP de routeur NAFTAL pour donner un accès vers internet.

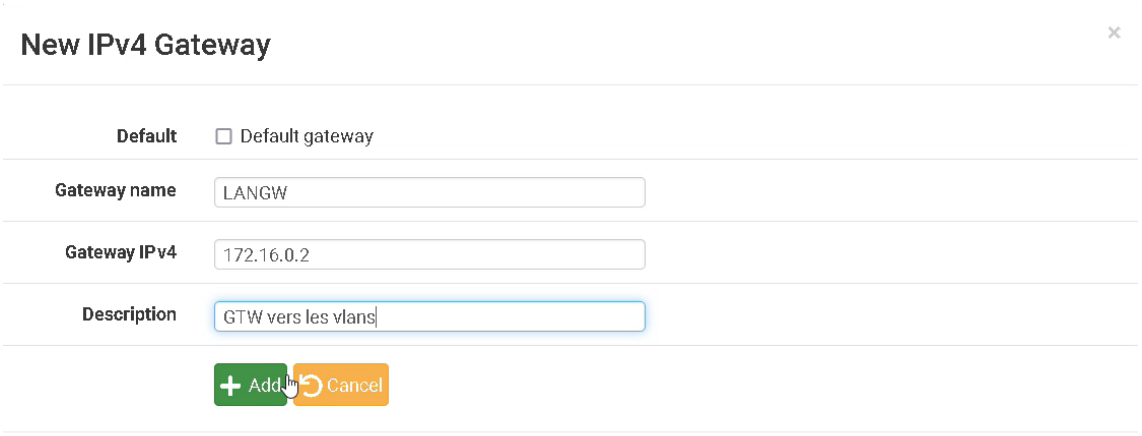


FIGURE 4.33 – Paramètre de Gateway vers les VLAN

♦ **étape 6 :** créer des routes vers les Vlans, on donne l'adresse destination puis la Gateway qu'on a créé avant, et la route vers vlan 200 par exemple, suivre les mêmes étapes pour les autres vlans.

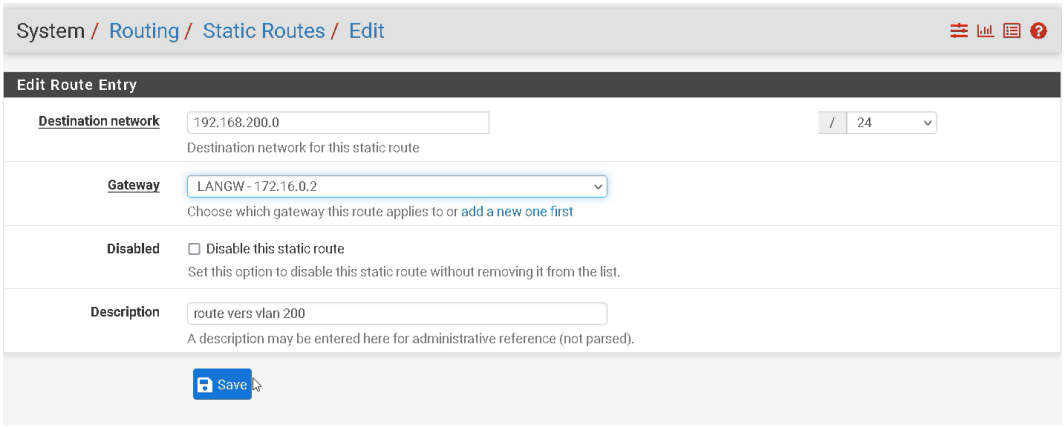


FIGURE 4.34 – Création des routes vers les VLANS

♦ **étape 7 :** Afficher les cinq vlans routé vers l'internet

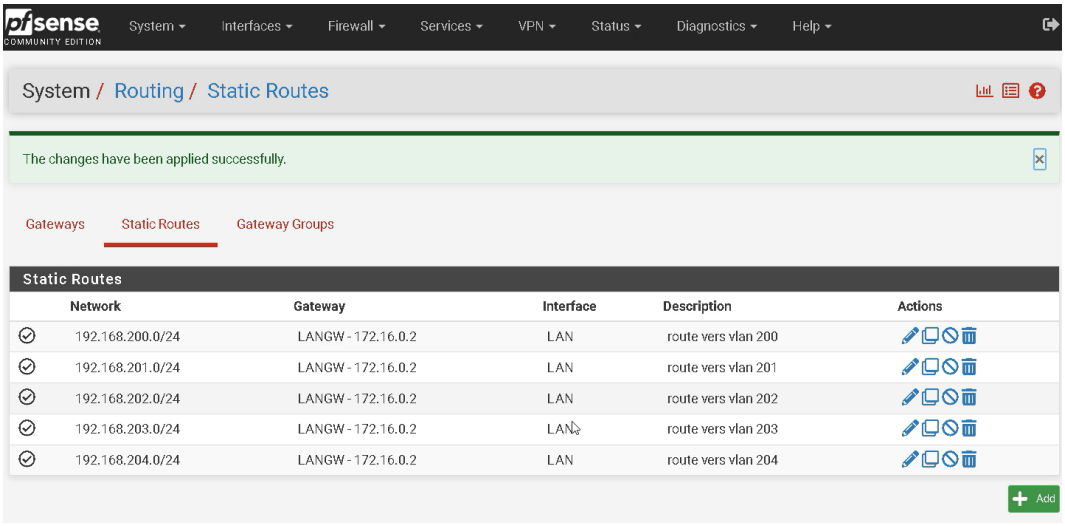
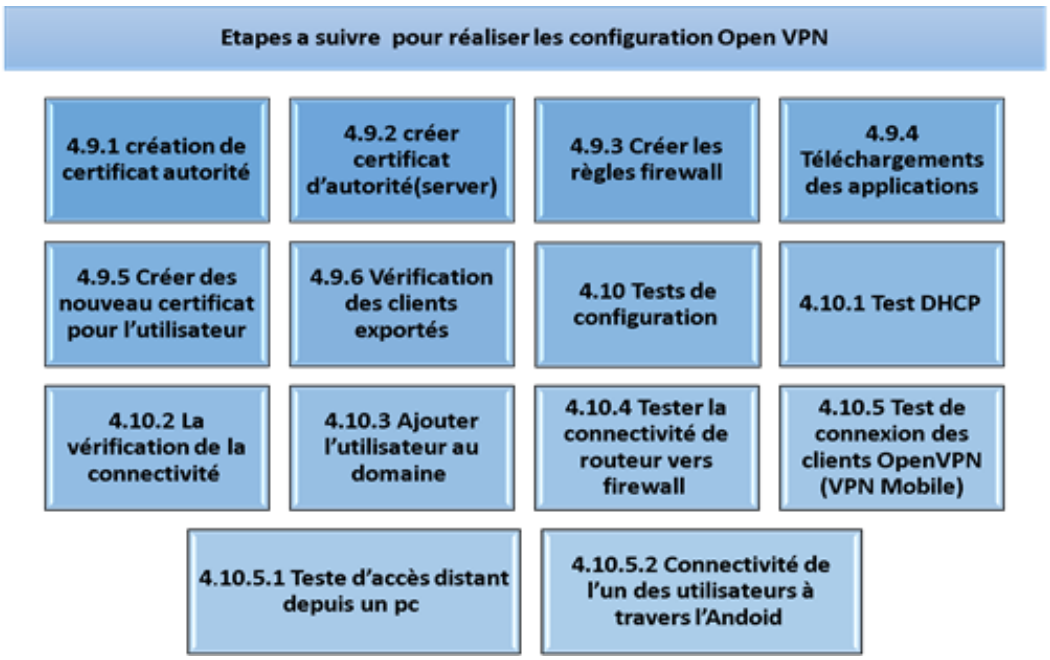


FIGURE 4.35 – relier les VLANs vers l'internet

4.9 La configuration du serveur OpenVPN



Sur le tableau de bord de notre firewall pfsense on va cliquer sur le volet VPN puis OpenVPN, par la suite on va lancer le wizards afin de créer notre serveur OpenVPN

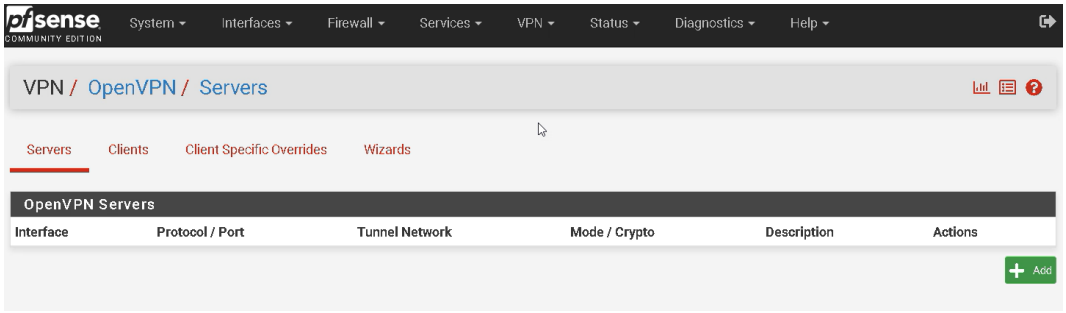


FIGURE 4.36 – interface de configuration du serveur openVPN

Ensuite on va choisir l'utilisateurs local pour les connexions Vpn Mobile

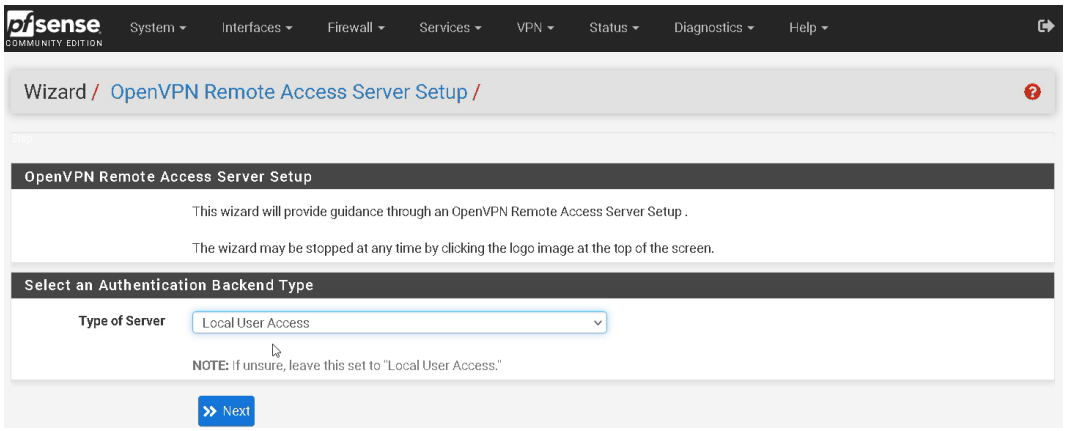


FIGURE 4.37 – Sélection de base de données locale

4.9.1 Création de certificat autorité (CA)

Pour une authentification plus sécurisé on utilise une authentification par certificat (nom d'utilisateur et mot de passe).

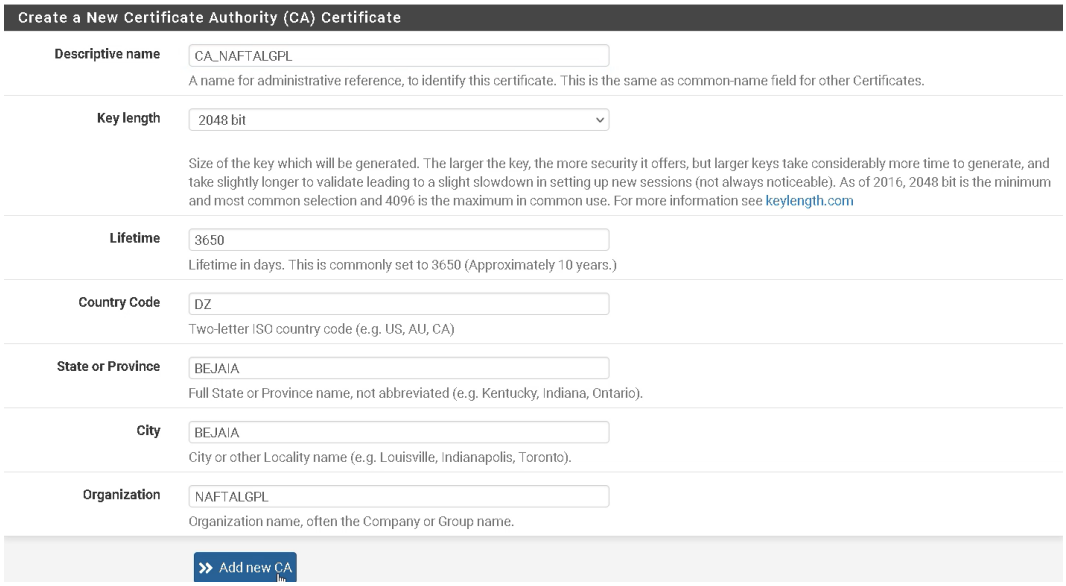


FIGURE 4.38 – 1 Création de certificatautorité (CA) :

4.9.2 Création d'un certificat d'autorité "server"

On suit les mêmes étapes pour créer certificat de serveur vpn. Les informations générales sur le serveur openvpn : on utilise l'interface WAN dans le serveur pour avoir une large connectivité vers internet, baseé sur le protocole UDP only pour une connexion client to site, avec les algorithmes de chiffrements pour assurer la confidentialité, l'intégrité et l'authentification.

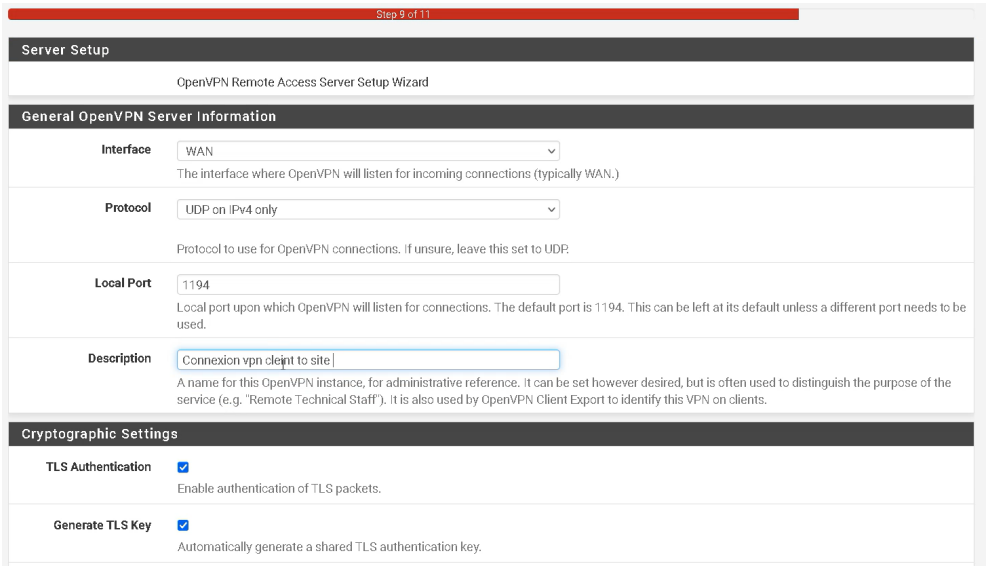


FIGURE 4.39 – Les informations générales sur le serveur openvpn

Par la suite on va paramètrer l'afféctation du pool dynamique des adresses ip pour nos clients VPN mobile suivi par les options de ce dernier (domain, dns, netbios ... etc)

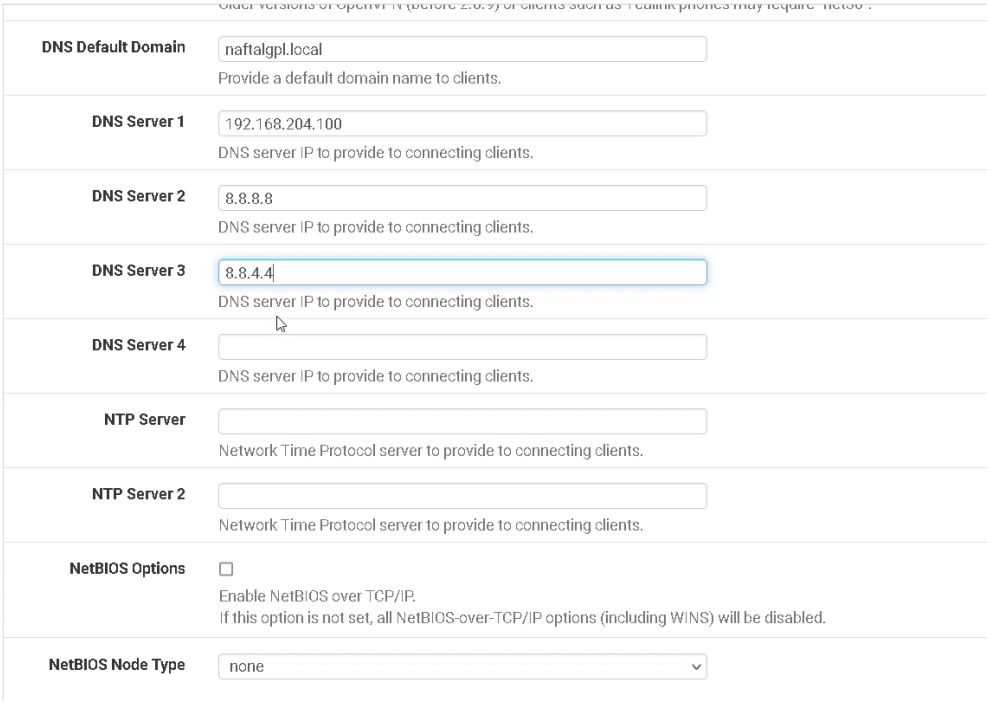


FIGURE 4.40 – Connexion de client vers infrastructure à travers internet

4.9.3 Création des règles firewall pour le serveur et le client

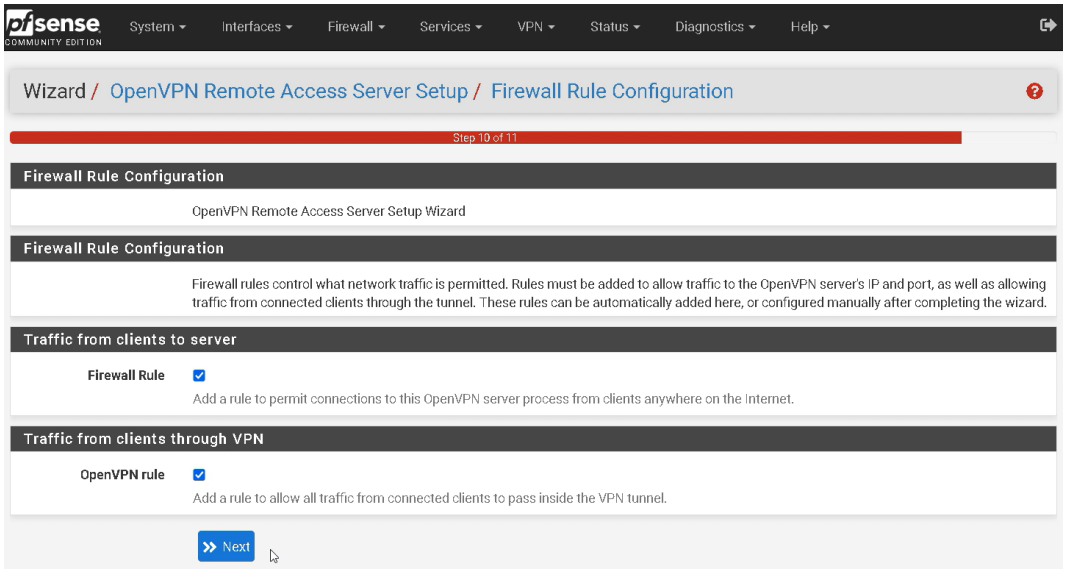


FIGURE 4.41 – Création des règles Firewall

Le serveur de connexion VPN est créé ce qui est montré dans la figure 4.42.

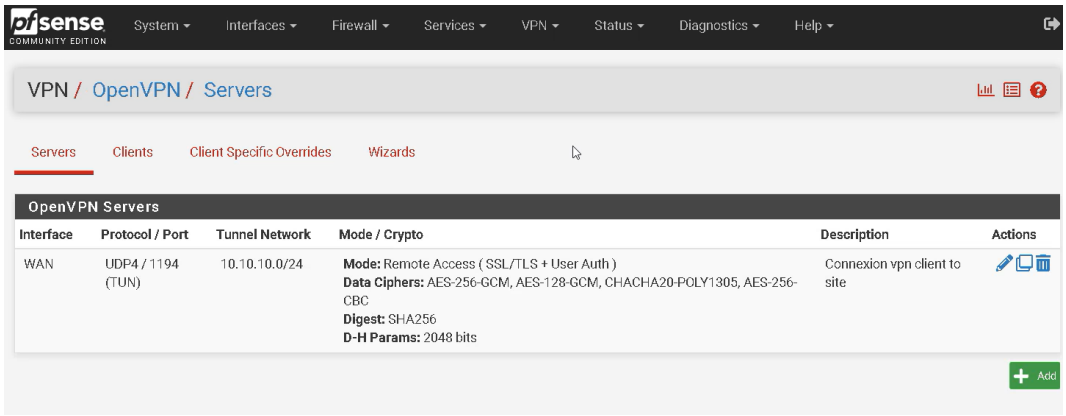


FIGURE 4.42 – Création de serveur de connexion VPN

4.9.4 Téléchargement des applications pour les clients

Pour télécharger une application on clique sur system puis en choisi package manager, ensuite available packages on aura tous les applications existantes.

On télécharge l'application openvpn puis l'installer qui sera préconfigurer pour les utilisateurs.

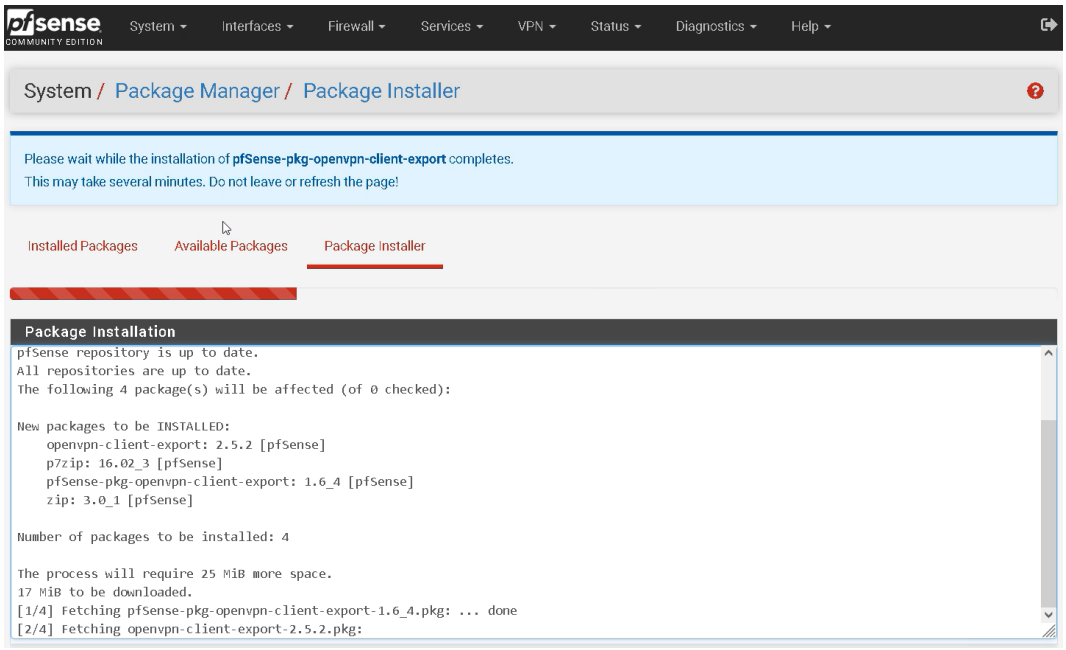


FIGURE 4.43 – téléchargement et L'installation openVPN

4.9.5 Création d'un nouveau certificat pour l'utilisateur

Pour créer un nouveau certificat user on donne un nom puis on choisi certificat d'autorité CA_NAFTALGPL et le nom de domaine naftalgpl.local et l'organisation NAFTALGPL enfin on sauvegarde

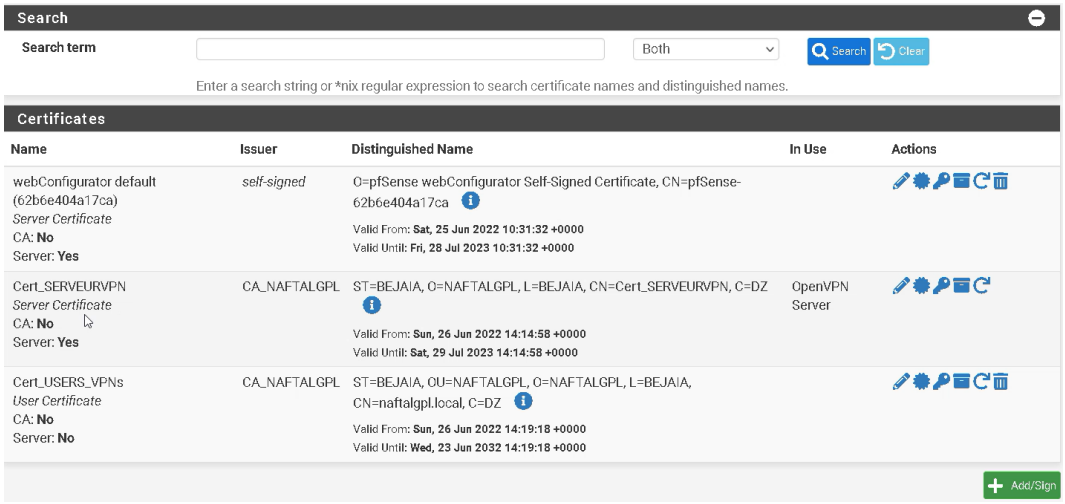


FIGURE 4.44 – Certificat user créer

Création de nouveau utilisateur : sur system puis user on donne les informations de l'utilisateur comme nom et mot de passe

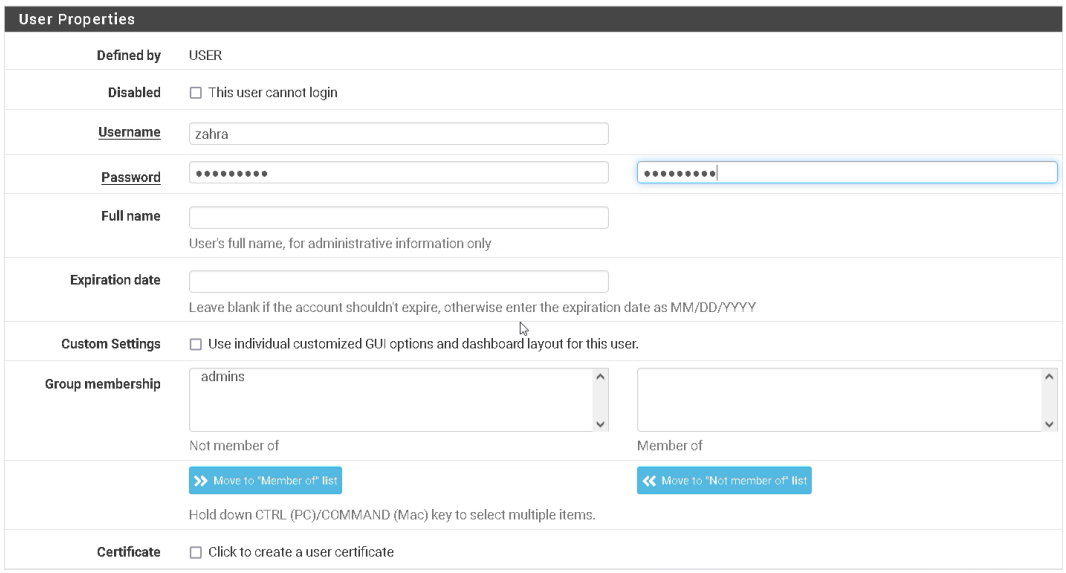


FIGURE 4.45 – Création d'utilisateur zahra

Après on donne le certificat à l'utilisateur avec l'username et certificat d'authority.

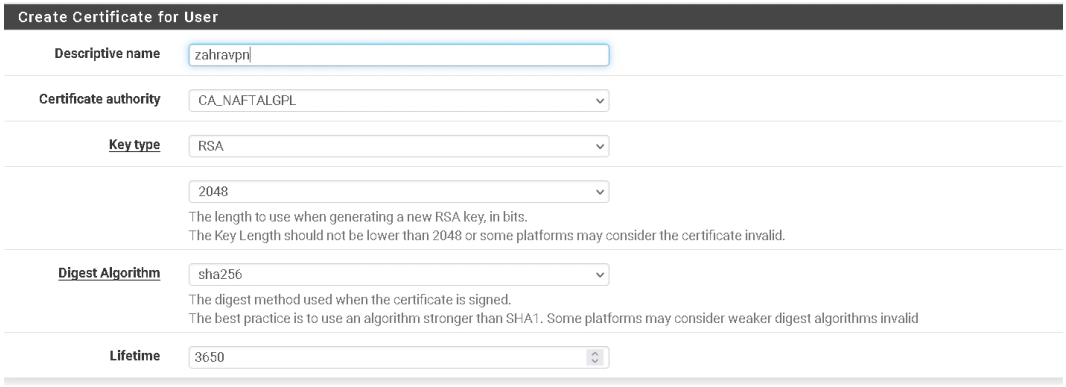


FIGURE 4.46 – Certificat d'utilisateur zahra

Ensuite les mêmes étapes pour créer d'autres utilisateurs.

4.9.6 ***La vérification des clients exportés***

On clique sur VPN puis open VPN pour voir que les clients exportés sont ajouté dans laquelle on trouve la configuration des utilisateurs.

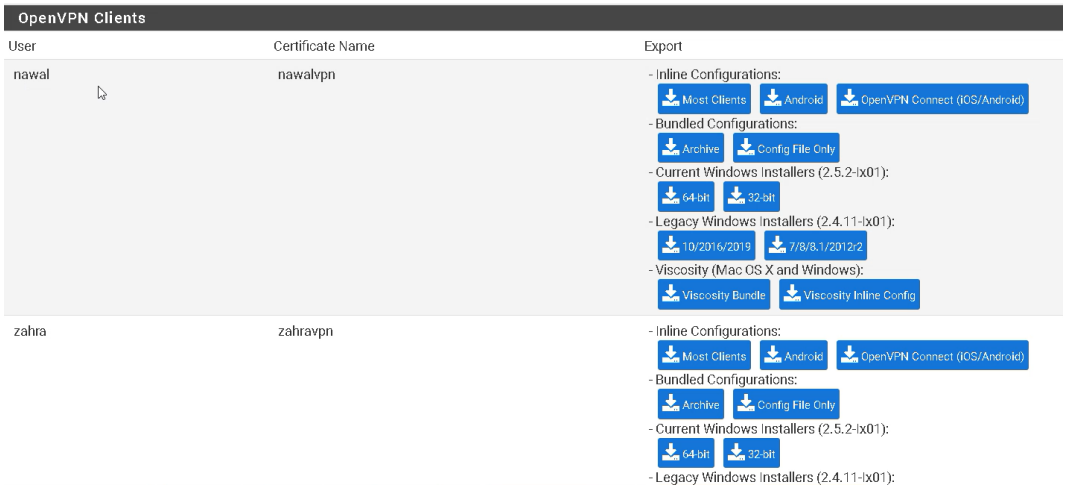


FIGURE 4.47 – les clients Export

4.10 Tests de configuration

4.10.1 ***Test DHCP***

Sur nos station de travail on lance la commande ip dhcp afin de tester le fonctionnement de notre serveur DHCP Notre serveur est fonctionnel (voir figure 4.48)

```
PC4>
PC4>
PC4>
PC4> ip dhcp
DDD
Can't find dhcp server

PC4> ip dhcp
DORA IP 192.168.200.11/24 GW 192.168.200.1

PC4>
```

FIGURE 4.48 – Le pc a reçu une adresse ip Dynamic attribuer par le serveur dhcp

4.10.2 ***La vérification de la connectivité***

Test de connectivité des clients vers le serveur active directory et DNS

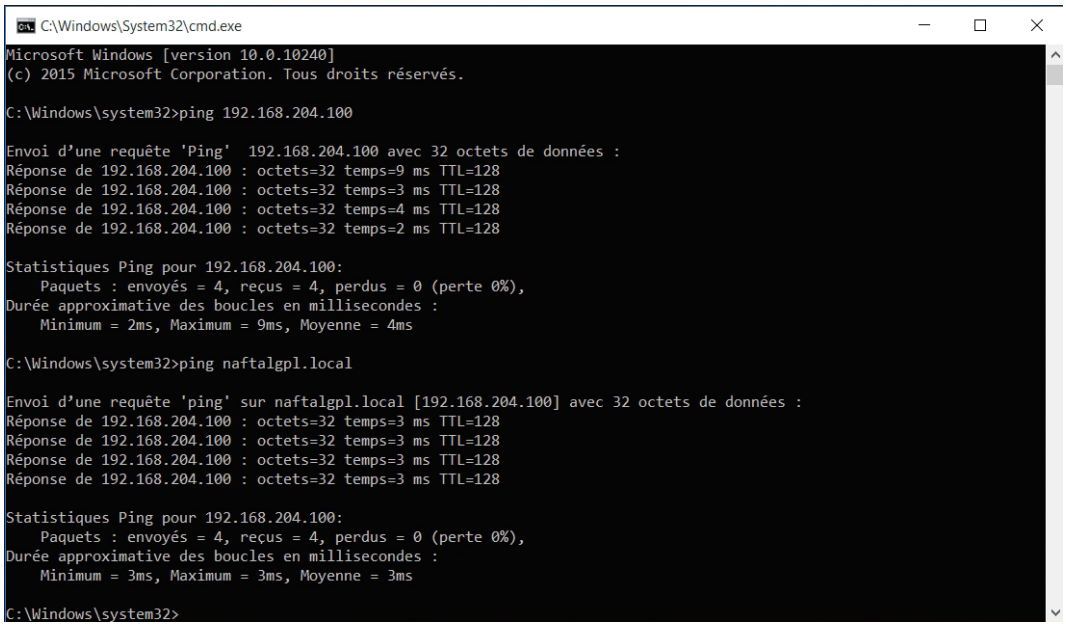


FIGURE 4.49 – Ping de pc vers serveur

4.10.3 ***Ajouter l'utilisateur au domaine***

on va joindre le domaine sur le nom des utilisateurs par donne le nom d'utilisateur et le mot de passe. Ensuit on donne le domaine (NAFTALGPL.LOCAL).

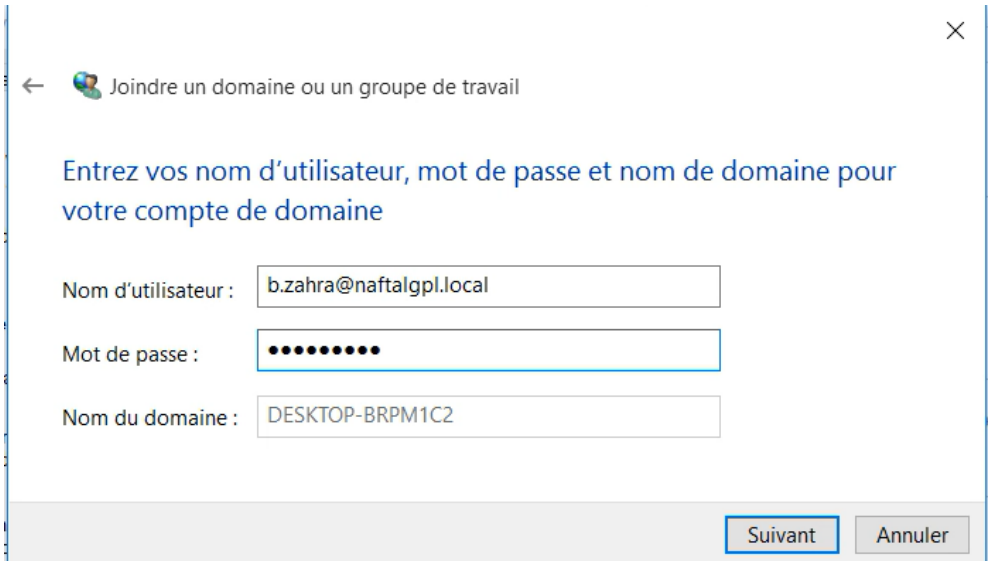


FIGURE 4.50 – Joindre le domaine par l'utilisateur

On doit disposer d'un mot de passe administrateur qui va autoriser l'utilisateur d'entrer au domaine (voir la figure 4.51)

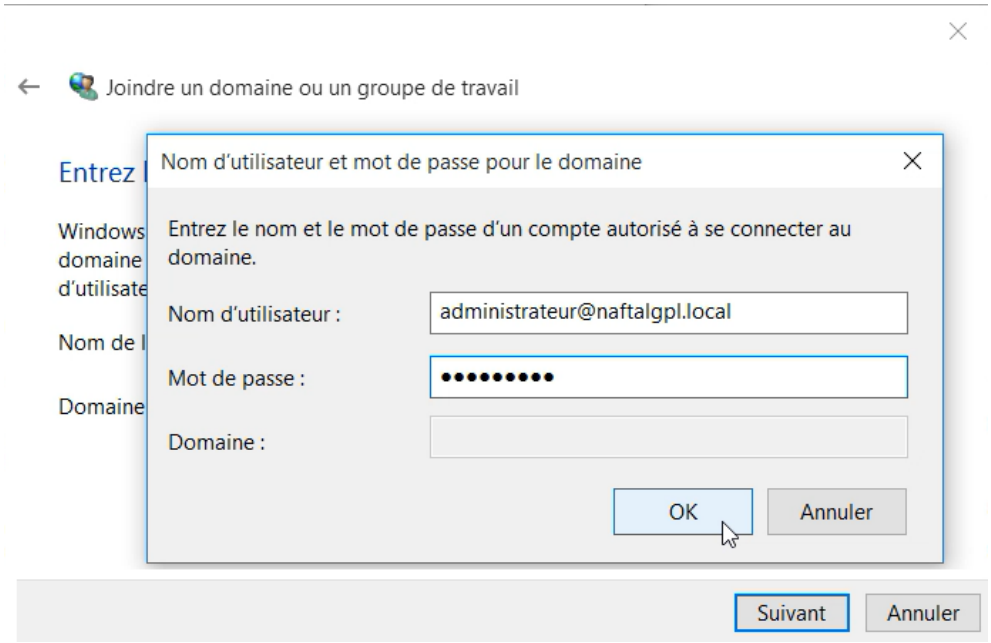


FIGURE 4.51 – Les paramètres d'administrateur

4.11 Tester la connectivité de routeur vers firewall

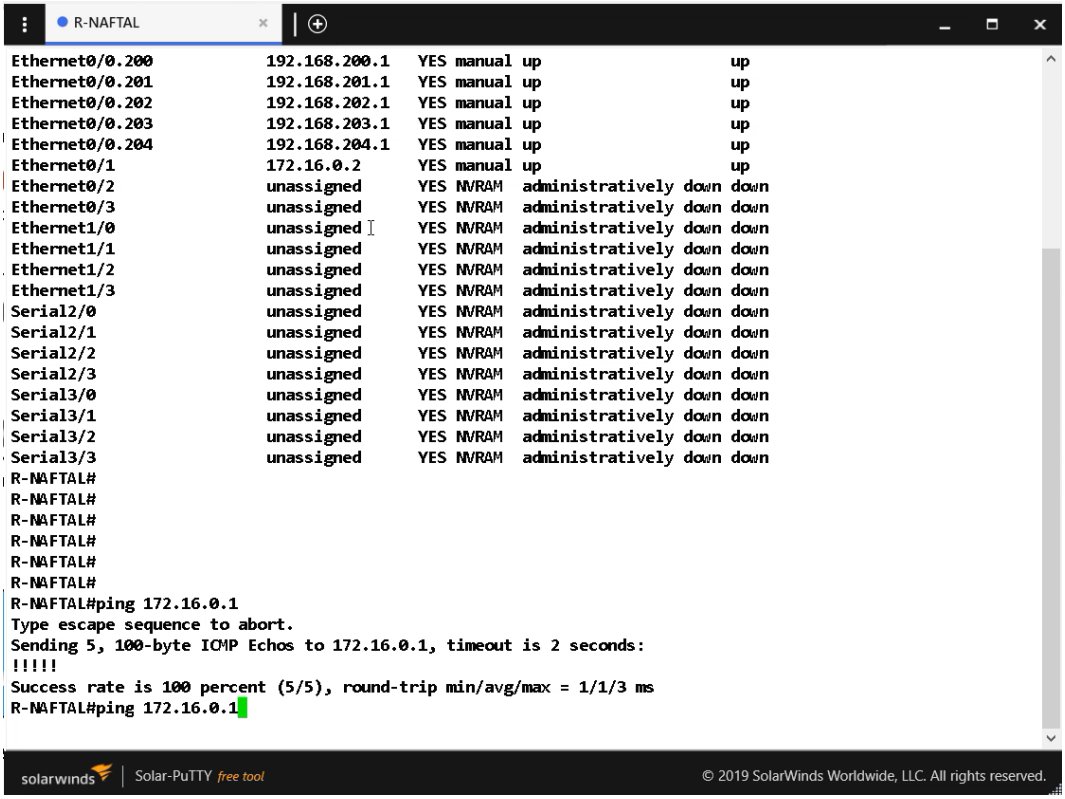


FIGURE 4.52 – Ping routeur vers firewall

Test de connectivité du server vers le firewall

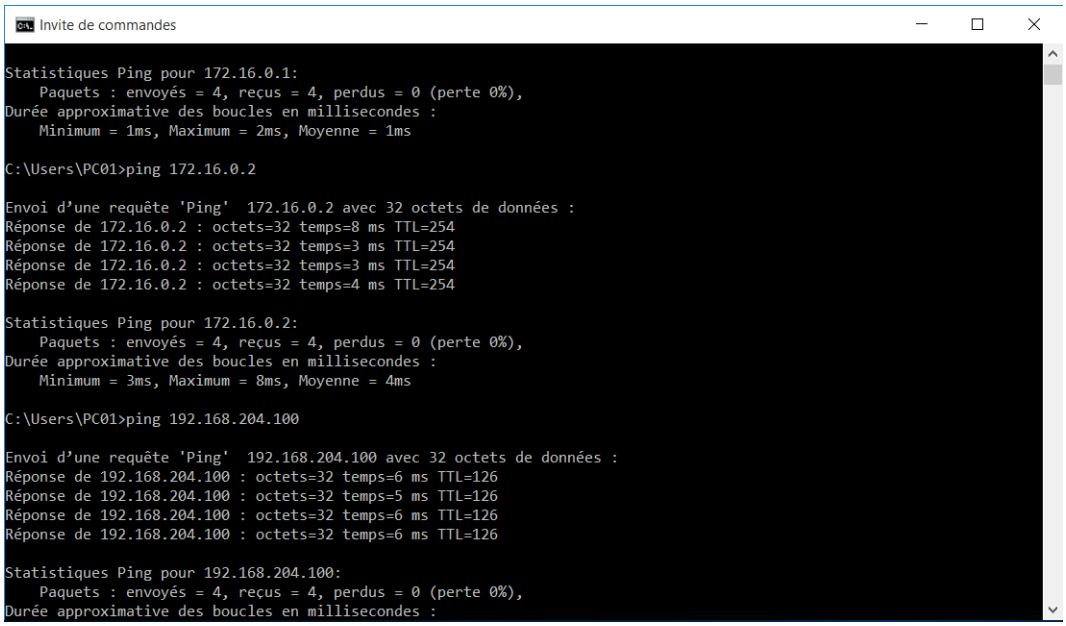


FIGURE 4.53 – Ping de serveur vers routeur et firewall

Test de connectivité vers internet

On va lancer un ping vers le serveur de google par exemple : 8.8.8.8

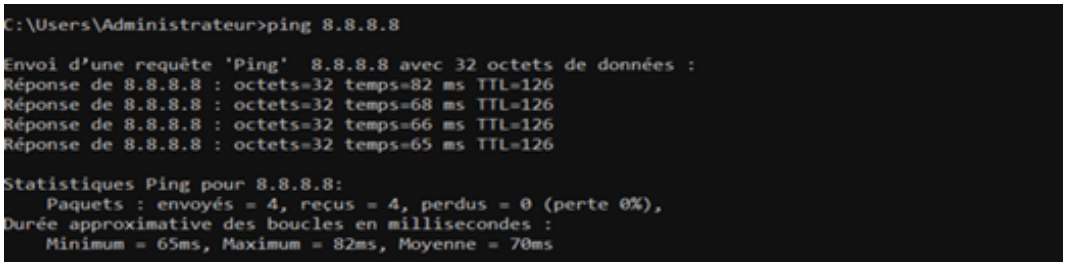


FIGURE 4.54 – Ping vers internet

4.11.1 ***Test de connection des clients OpenVPN (VPN Mobile)***

Après avoir exporté les clients on passe au téléchargement des packages (Windows, Android) pour finir la pré-configurations des clients.
L'installation de l'application sous Windows :

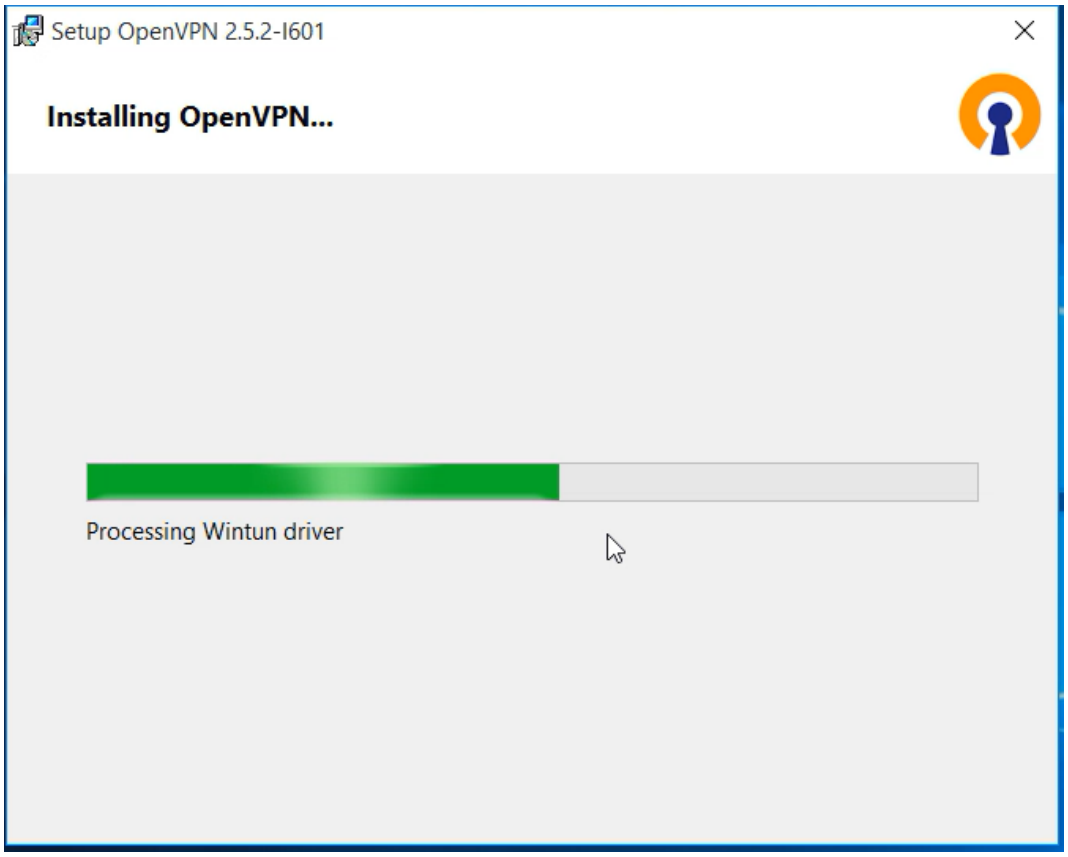


FIGURE 4.55 – Installation openVPN

Le test de connectivité entre le client vpn et internet (Ping 8.8.8.8).

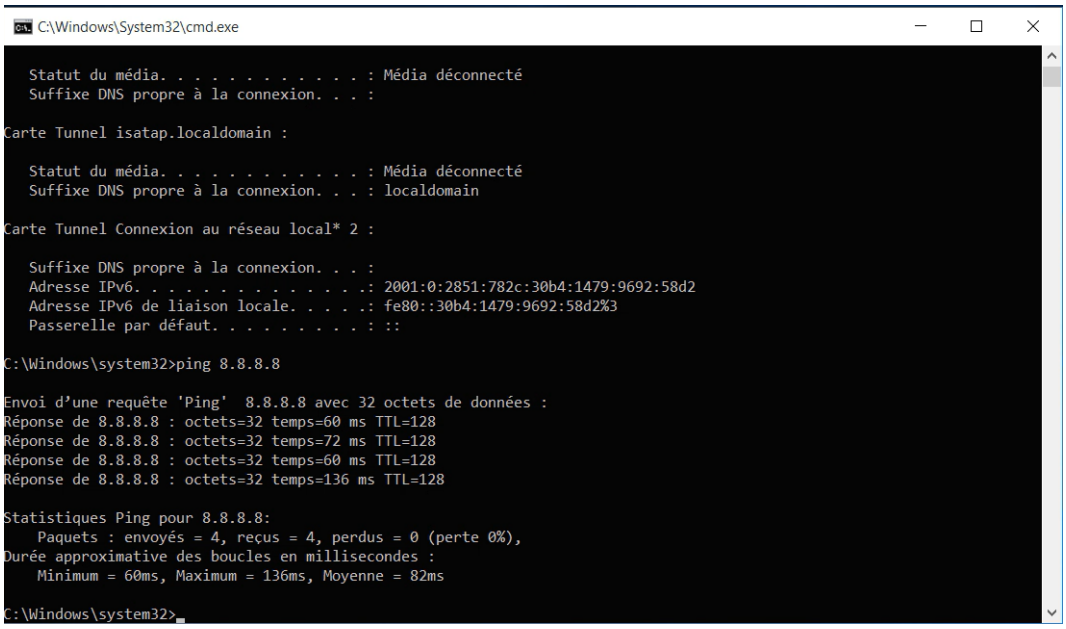


FIGURE 4.56 – Ping client vers internet

L'un des utilisateurs va se connecter après la fin d'installation du l'application.

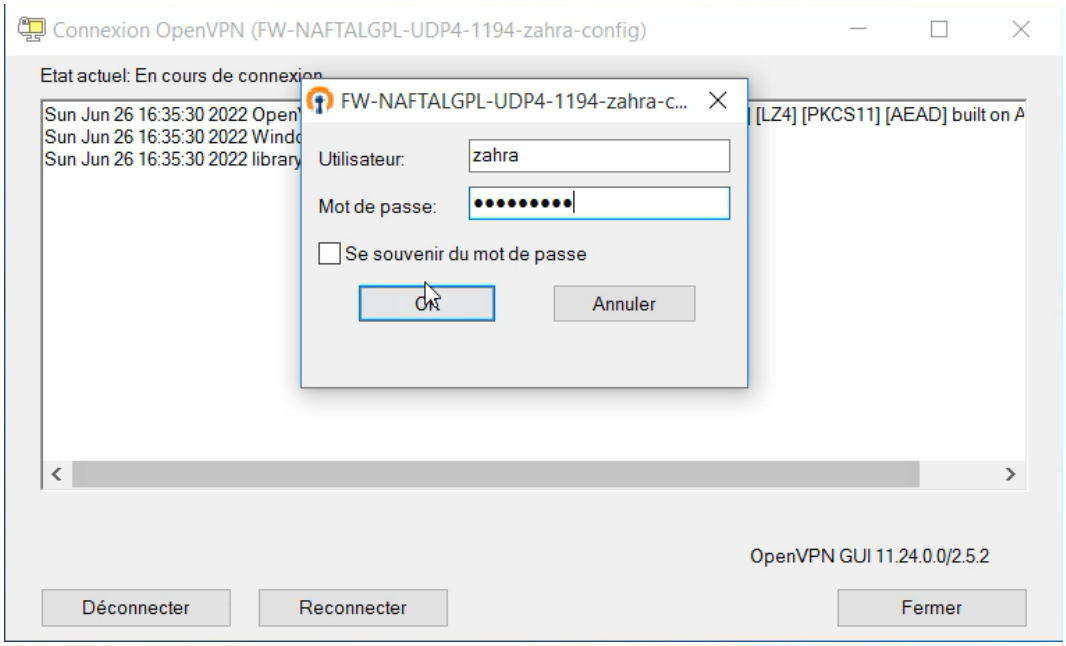


FIGURE 4.57 – Les paramètres d'utilisateur

On consulte le statut de Firewall pour vérifier que l'utilisateur est connecté, ce qui est montré dans la figure 4.58.

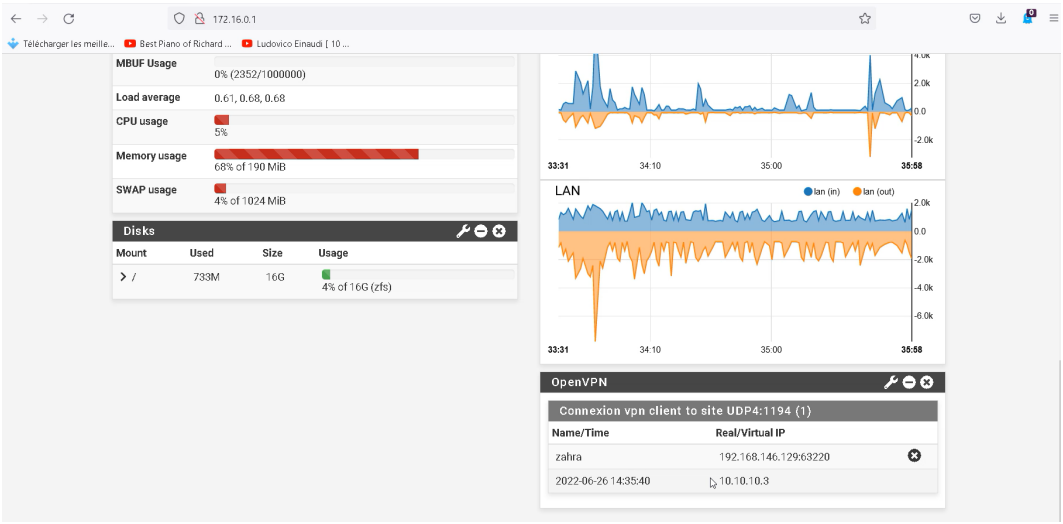


FIGURE 4.58 – Utilisateur connecté

4.11.1.1 Teste d'accès distant depuis un pc

Vérification de connectivité d'utilisateur vers le serveur par internet (Ping 192.168.204.100).

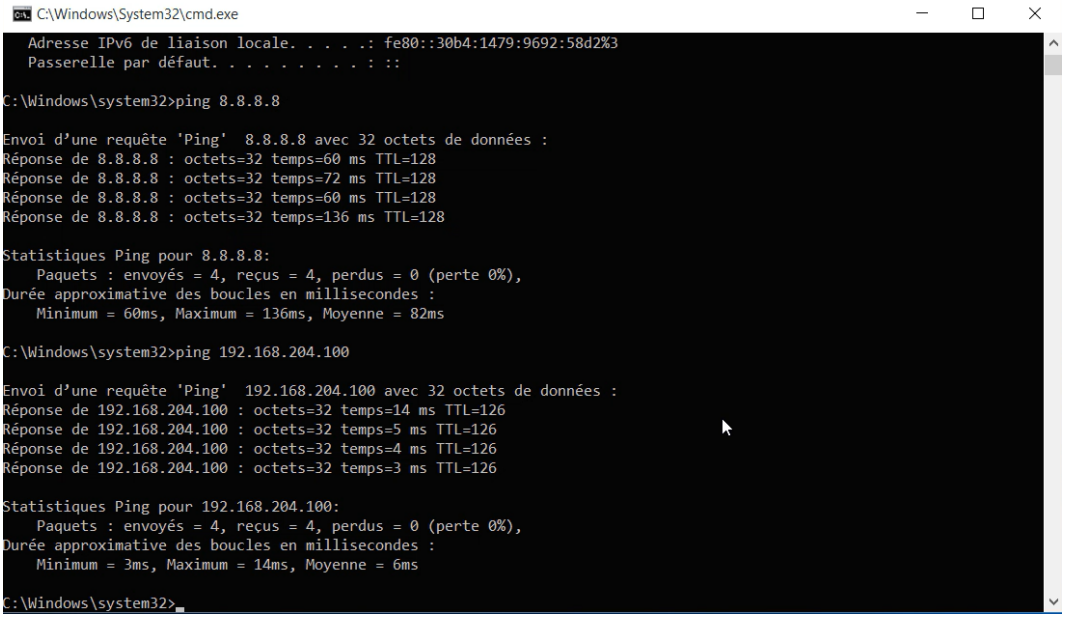


FIGURE 4.59 – Ping utilisateur vers serveur

Test de création de nouvelle interface (tunnel VPN).

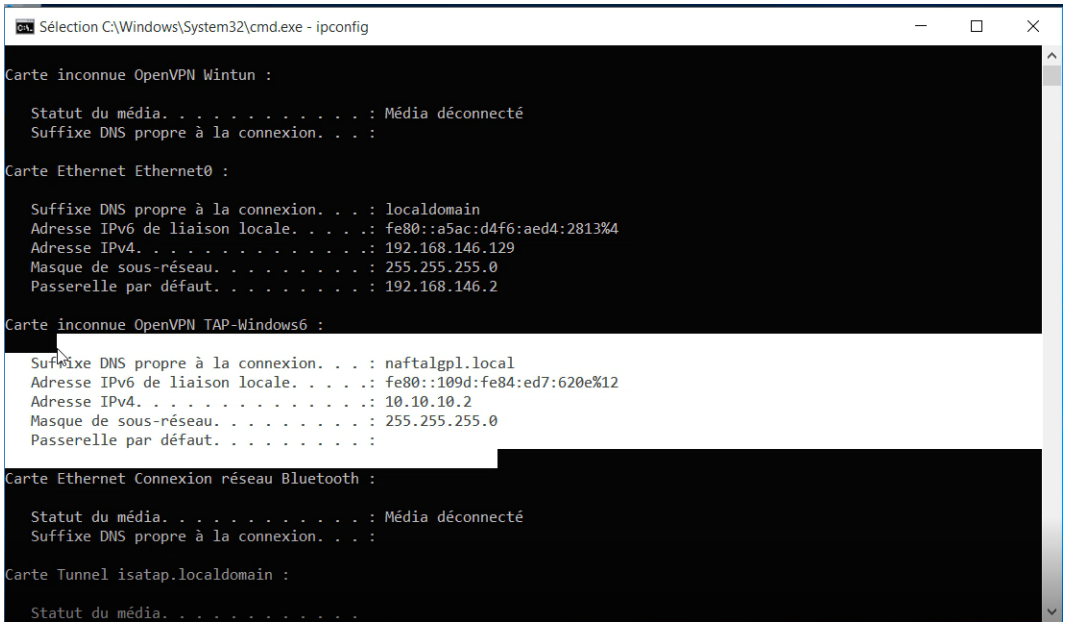


FIGURE 4.60 – Test de création d'interface

L'accès à distance avec RDP (Microsoft Remote Desktop) :L'utilisateur utilise le RDP comme moyen d'accès à distance au serveur de l'entreprise. Dans le RDP on crée une nouvelle session on donne le nom de serveur, username, domaine et le mot de passe.

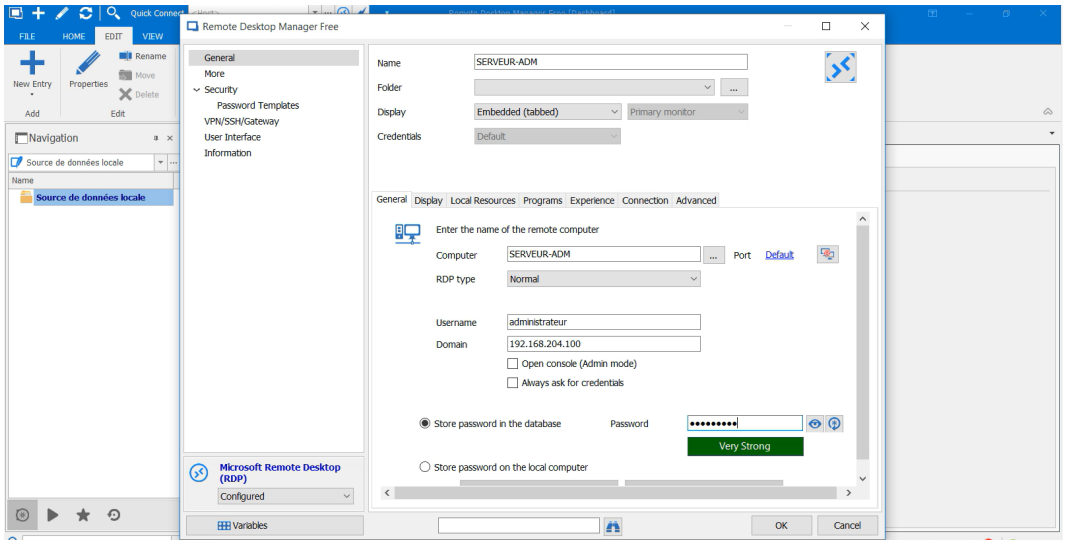


FIGURE 4.61 – Création nouvelle session RDP

Enfin pour lancer la session on clique deux fois sur SERVEUR-ADM Voir ça dans la figure 4.62.

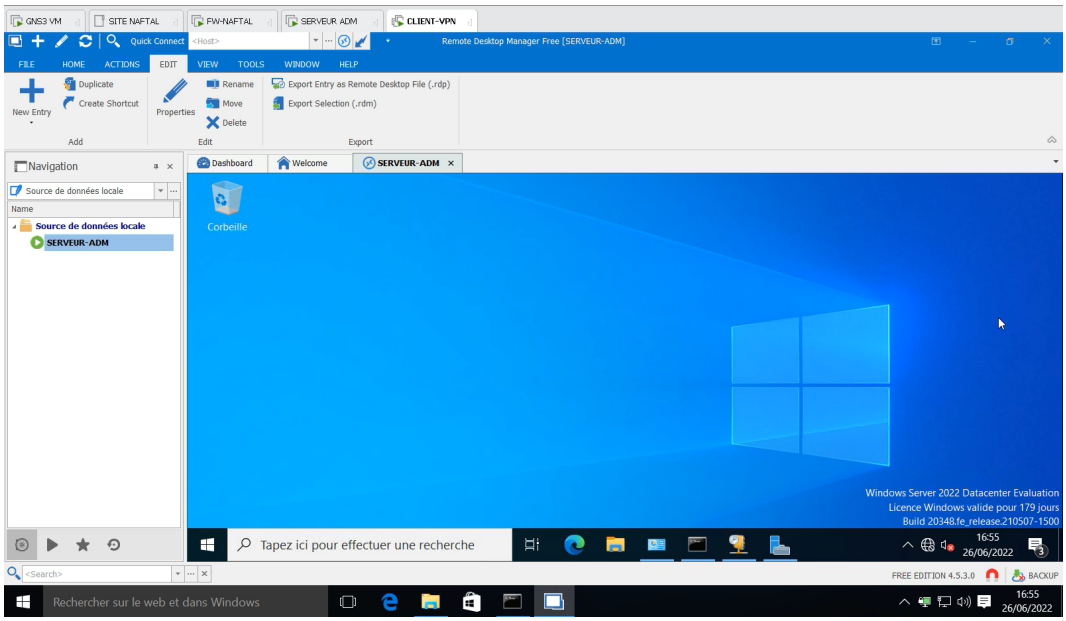


FIGURE 4.62 – Accès au serveur avec RDP

4.11.1.2 Connectivité de l'un des utilisateurs à travers l'Andoid

Après avoir installé l'application OpenVPN sur Android et paramétré l'utilisateur on passe à :

- **Connecter l'utilisateur par le saisi de son nom et mot de passe.**

FIGURE 4.63 – les paramètres d'utilisateur Android

- **L'utilisateur est connecté au VPN voir ça dans la figure 4.64.**

FIGURE 4.64 – l'utilisateur Android connecté

- **Teste d'accès distant telephone portable Android :**

Test connectivité d'utilisateur Android vers serveur

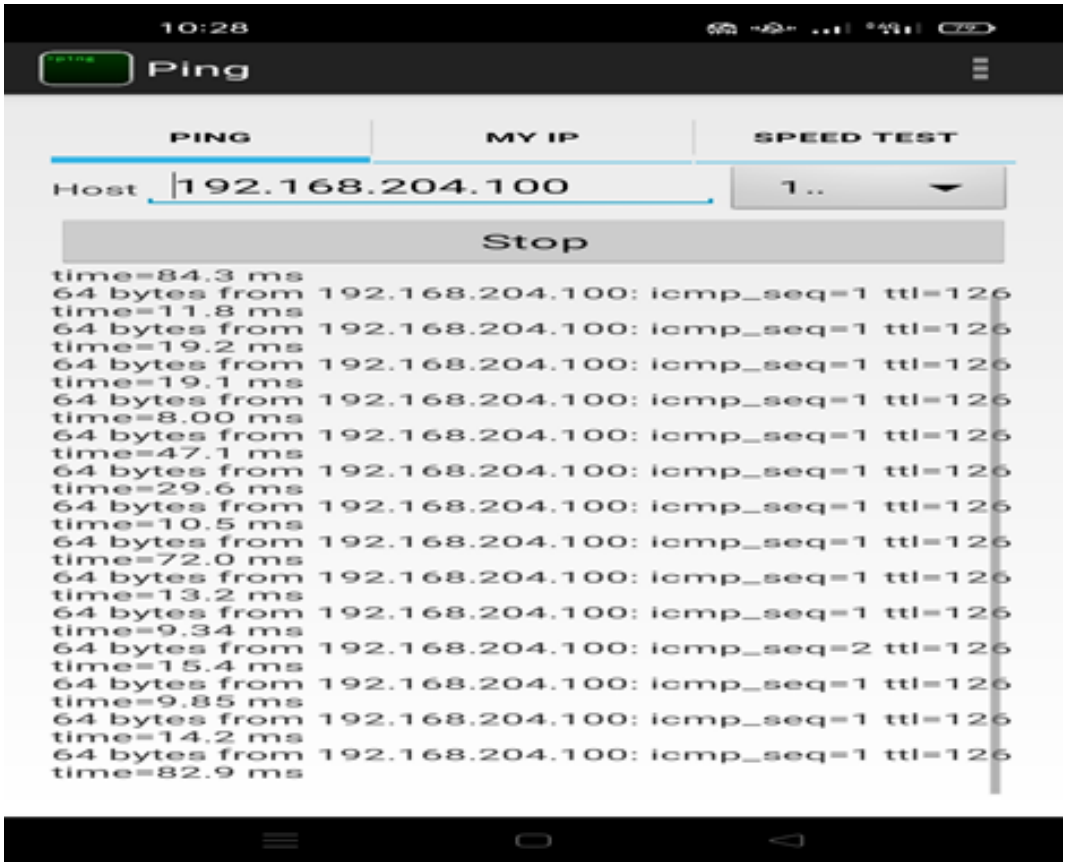


FIGURE 4.65 – Ping client Android vers serveur

La vérification de connectivité de deux utilisateurs l'un sur Android et l'autre sur Windows au niveau de firewall.

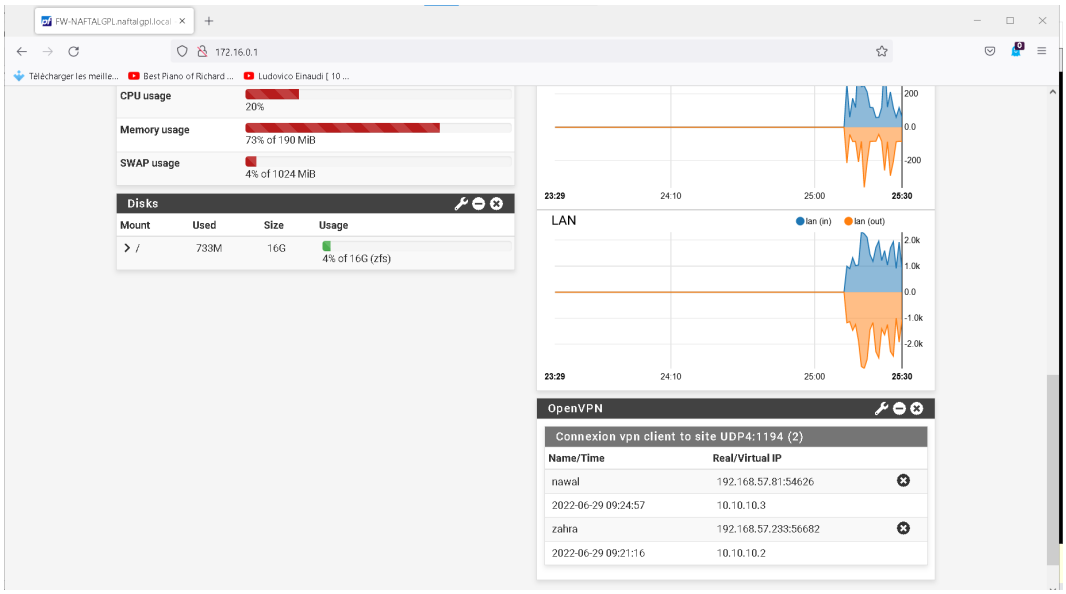


FIGURE 4.66 – Vérification de connectivité sur firewall

•Vérification le trafic d'openVPN sur Wireshark :

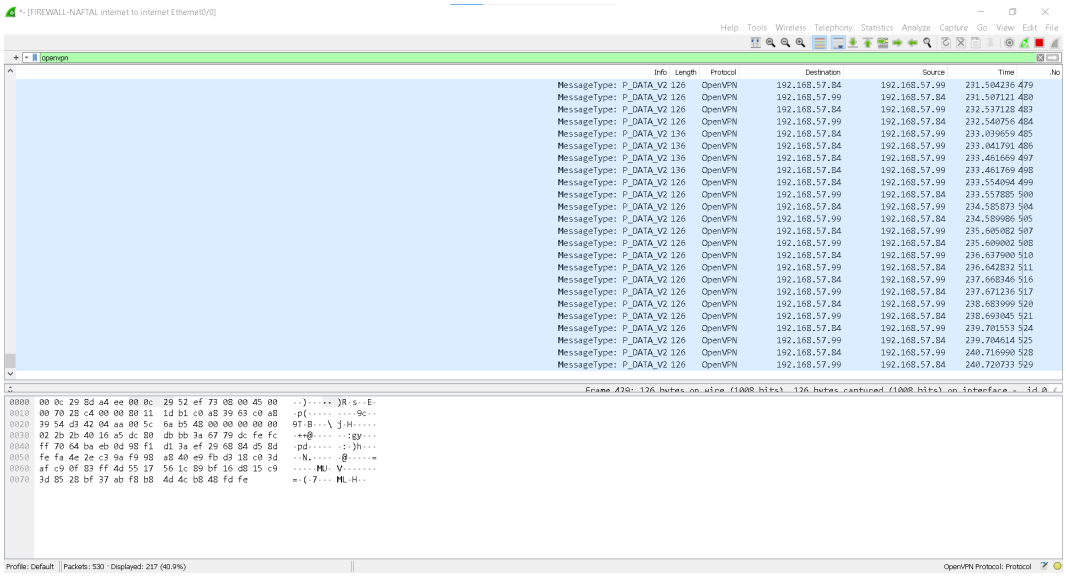


FIGURE 4.67 – Vérification le trafic d'openVPN

4.12 Conclusion

Dans ce dernier chapitre, nous avons présenté la solution mise en place avec les détails de l'installation et la configuration des différents équipements et les tests de validation pour nous assurer que notre objectif a bien été atteint.

Conclusion générale

Les VPN ont pris un certain pourcentage du développement d'Internet. En fait, avec l'avènement de la technologie sans fil, des problèmes de sécurité et de confidentialité sont apparus. Ces problèmes de sécurité sont une préoccupation majeure, en particulier lors de l'échange de données sensibles. Une solution VPN peut résoudre ce problème et assurer une communication fluide et sécurisée. Nos recherches nous ont donné une idée approximative des différentes possibilités requises pour déployer un VPN. Dans ce cas, nous avons constaté qu'il existe un grand nombre de protocoles, de technologies et d'architectures pour déployer ce concept, et le choix de la solution VPN dépend encore des besoins d'utilisation et de l'investissement financier que nous y ferons. Dans notre projet, nous avons choisi une solution VPN mobile(poste à site) avec l'application OpenVPN.Cette solution crée un réseau privé sécurisé qui non seulement garantit une communication efficace et sécurisée entre les postes distants et les sites de l'entreprise, mais offre également aux télétravailleurs la possibilité d'accéder à distance au réseau de l' entreprise.

En raison de droits d'accès que L'entreprise GPL NAFTAL a refusé de nous octroyer , nous n'avons pas pu mettre en pratique cette solution au niveau de l'entreprise et nous avons décidé de la simuler sur la plateforme GNS3.

Malgré cela, nous avons réussi à établir toutes les étapes nécessaire à mettre en pratique notre solution, et par la même apprendre de nouveaux concepts, logiciels ou environnements de travail.

Enfin, nous tenons à souligner que ce travail nous donne l'opportunité d'approfondir nos connaissances dans les domaines de la sécurité informatique, du transfert de données et du déploiement d'architectures VPN mobile.

Evidemment la perspective principale de notre travail serait que GPL NAFTAL puisse profiter de nos résultats, et même inclure un moyen d'authentification pour les clients externes par exemple : serveur radius, LDAP, etc.

Bibliographie

Bibliographie

[1] https ://www.naftal.dz/fr/index.php/produits/particuliers/gpl consulter le 22/06/2022.

[2] https ://www.Inr-dz.com/2022/04/16/mise-a-disposition-de-2-300-tpe-sur-le-reseau-naftal/ consulter le 23/06/2022.

[3] https ://www.naftal.dz/fr/index.php/a-propos-de-naftal/historique Consulter le 23/06/2022.

[4] document interne d'entreprise NAFTAL GPL Bejaia consulter le 17/05/2022.

[5] Laurent Bloch et Christophe Wolfhugel "Sécurité informatique principe et méthode", EYROLLES 2eme Edition, 2005.

[6] Jean- FrancoisPillou et Jean-Phylippe Bay "tout sur la sécurité informatique", Dunod 4eme Edition, 2016.

[7] SolongeGhernaouti-Hélie "sécurité informatique et réseaux" EYROLLES 3eme Edition, 2012.

[8] Https ://www.wavesoft.it/fr/quels-sont-les-criteres-majeurs-de-securite-des-si/ Consulter le 03/06/2022.

[9] Bernard Cousin "sécurité des réseaux informatique", Université de Rennes 1, https ://www.slideshare.net/simomans/1-securitedesreseaux2-p Consulter le 14/05/2022.

[10] https ://images.app.goo.gl/KMNmFnoLQzdusvwdA Consulter le 20/05/2022.

[11] https ://images.app.goo.gl/T6GMMdKzAnSaXwXd6 Consulter le 20/05/2022.

[12] https ://images.app.goo.gl/bwzqS397NR3tMqNC7 Consulter le 20/05/2022.

[13] https ://images.app.goo.gl/pHd1KpfgXuHKRMQa8 Consulter le 20/05/2022.

[14] https ://images.app.goo.gl/dh7jEt3zatHg12Kg8 Consulter le 20/05/2022.

[15] Raphael Yende " Le sécurité informatique et crypto", support de cours de master, Université Congo-Kinshasa, 2018.

[16] Https ://www.Marche-public.fr/Terminologie/Entrees/securite-reseaux-information.htm. Consulter le 04/05/2022.

[17] BahoniThisiri et Sahi Sara "Solution VPN d'accès distant a l'intranet de l'université de Bejaia : Application au réseau VLAN de scolarité" mémoire Master 2, Université de Bejaia,2017/2018.

[18] Mehoubi Mohamed et MedjaniNacer "Sécurisation d'une infrastructure LAN /WAN à base d'équipement Cisco" Mémoire Master 2, Université de Tizi Ouzou, 2015.

[19] Http ://fr.theastrologypage.com. Consulter le 28/05/2022

[20] https ://www.futura-sciences.com/definitions/connection-vpn-1819/ consulté 15/04/2022.

[21] https ://www.frameip.com/vpn/ consulter le 15/04/2022.

[22] https ://www.isdecisions.fr/teletravail-securiser-sessions-rdp-vpn consulter le 03/06/2022.

[23] https ://www.koesio.com/communications/connectivite/interconnexion-de-sites consulter le 03/06/2022.

[24] Rahmani Tinhinane, Sadaoui Fadhila " Étude et mise en place d'un réseau VPN " mémoire master 2, université Mouloud Mammeri de Tizi Ouzou, 2016/2017.

[25] C Pham " VPN et solutions pour l'entreprise ",Université de Pau et des pays de l'Adour, département informatique, 2001/2002, Www.univ-pau.fr/ cpham. Consulter le 07/04/2022.

[26] https ://www.Vpnoverview.com/fr/infos-vpn/inconvenients-vpn consulter le 24/04/2022.

[27] https ://www.editions.eni.fr/open/mediabook.aspx ?idR=514693bd82511bcae374604dddb5c870 consulter le 06/05/2022.

[28] n'djoli Jacques et Elidrissi Ilias, Exposé d'administration des réseaux sur Linux, les VPN,

[29] Laurent Bloch et Christophe Wolfhugel. "Sécurité informatique principe et méthode", EYROLLES 2eme Edition, 2005.

[30] Solange Ghernaouti -Hélie "sécurité informatique et réseaux" EYROLLES 3eme Edition, 2012.

[31] J.PARCHIER, "les VPN, fonctionnement et mise en œuvre ", éditions ENI, 2011.

[32] Documentation technique Orange Developer " Généralités sur les VPNs ", https ://developer.orange.com/tech_guide/documentation-technique-reseaux-orange-france/#les-vpnconsulter le 13/06/2022.

[33] Djedjiga Benzid" Le réseau privé virtuel(VPN) sur les réseaux mailles sans fil WMN "Mémoire de fin d'étude, Université du Québec MONTREAL, 2014.

[34] https ://www.cnmtelecom.net/wp-content/uploads/sites/758/2016/02/vpn-classique.jpg consulter 09/04/2022.

[35] Jean-François Pillou, Jean Philippe Bay "tout sur la sécurité informatique" DONOD 4eme Edition.

[36] https ://www.journaldunet.fr/web-tech/guide-de-l-entreprise-digitale/1506369-openvpn-tout-savoir-sur-le-vpn-open-source-pour-les-pros/#openvpn-cest-quoiConsulter le 24/07/2022.

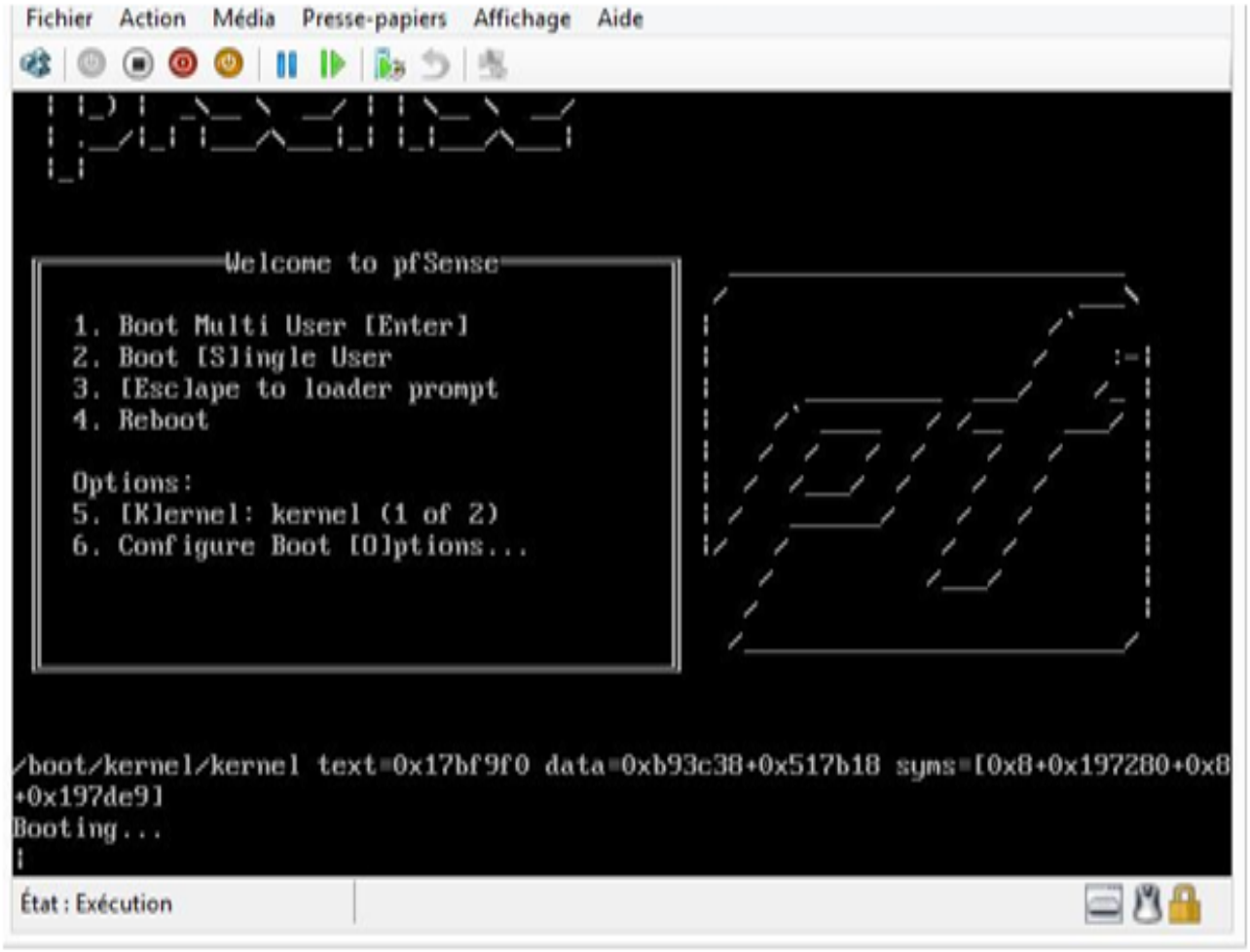
[37] https ://apksshare.com/forticlient-vpn-apk-mod-premium-download-6-4-4-0484/ consulter le 24/07/2022.

[38] https ://www.cisco.com/c/fr_ca/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5467-anyconnect-secure-mobility-client-software-frequently-asked.html#f1 consulter le 24/07/2022.

[39] Loudni "Les Réseaux Privés Virtuels(VPN) ", https ://-loudni.users.greyc.fr/Enseignement/Cours/TRc8/CM/CM3_VPN.pdf. Consulter le 07/04/2022.

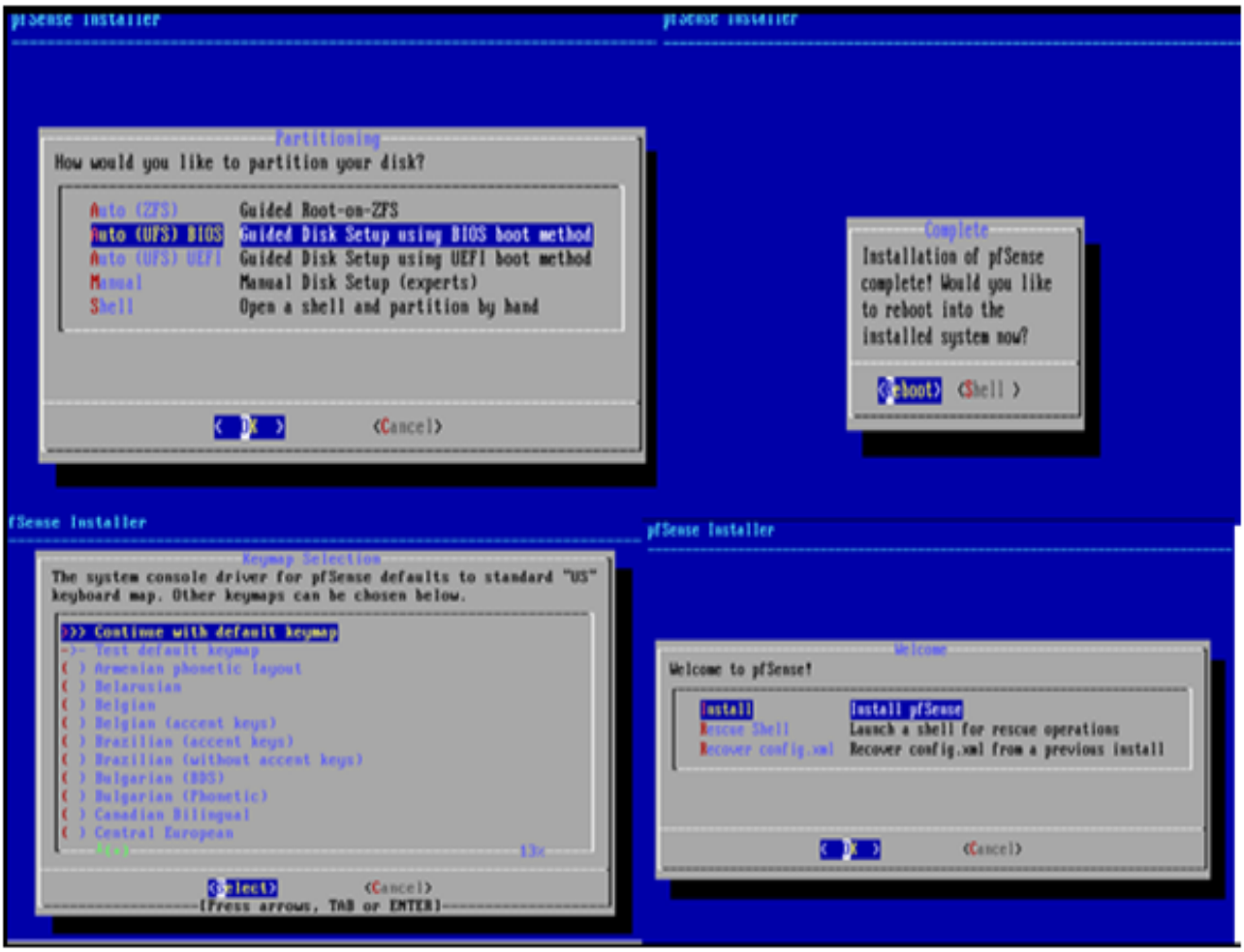
Annexe

Les étapes d'installation de pfSense :
Dans cette partie nous allons voir les différentes étapes d'installations de pfSense :
Démarrer la VM, Accepter la licence.



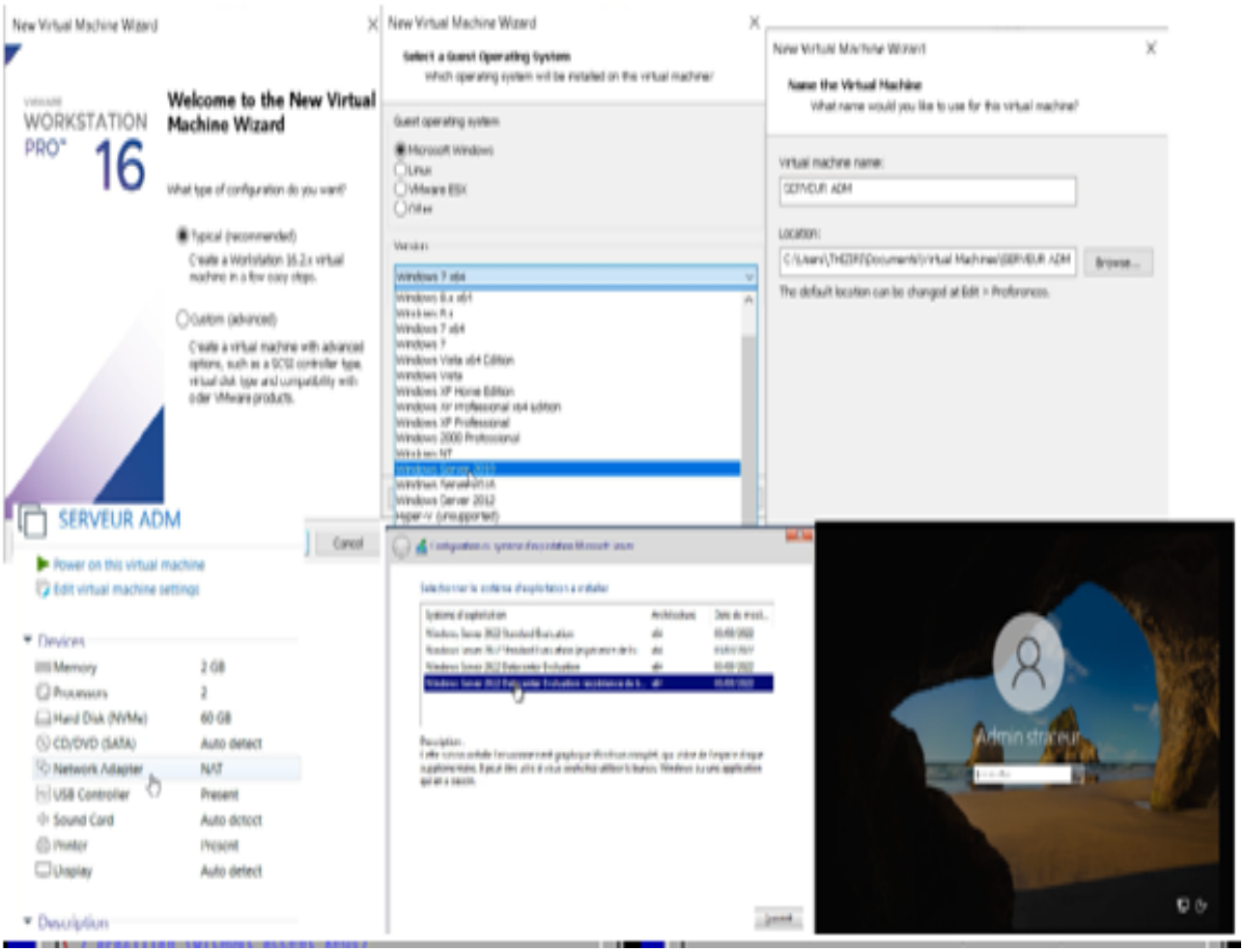

pfSense Installer
Copyright and distribution notice
pfSense is Copyright 2004-2017 Rubicon Communications, LLC (Netgate).
pfSense is a federally registered trademark of Electric Sheep Fencing, LLC. Any unauthorized use of this trademark is prohibited by state and federal law and international law. Refer to our Trademark Usage Guidelines for how to properly use the marks. All rights reserved.
Absolutely No Commercial Distribution Is Allowed.
<Accept>

Install PFSense : OK, select.



Les étapes d'installation de serveur Windows 2022

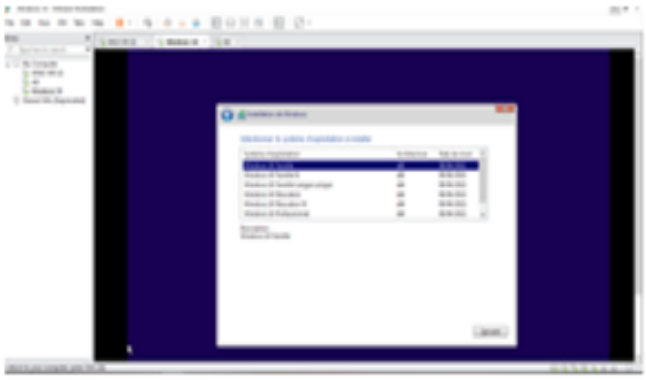
Dans cette partie nous allons voir les différentes étapes d'installations de Windows Server 2022.

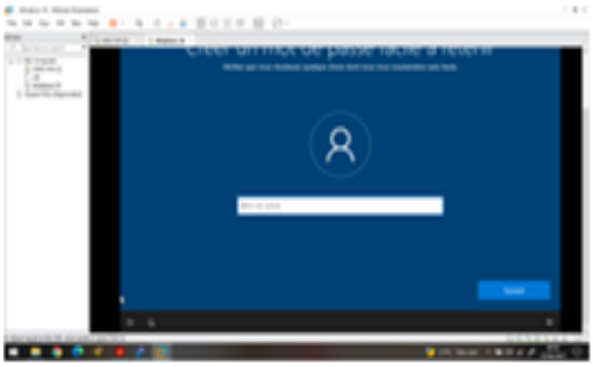


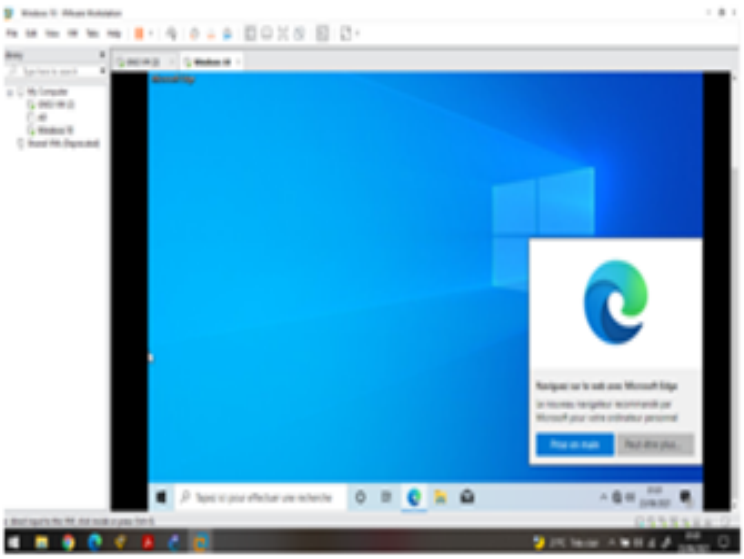
Les étapes d'installation de Windows 10 :

Nous avons créé une machine après avoir ajouté l'image de Windows 10 sur VMware.
A qui on a attribué les caractéristiques suivantes :

- Allocation de la mémoire pour la machine fixé à 2GB
- Deux processeurs
- Disque dur 30GB








Windows 10
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 1 GB
Processors 2
Hard Disk (NVMe) 30 GB
CD/DVD (SATA) Using file C:\Use...
Network Adapter Custom (VMnet0)
Network Adapter 2 NAT
Network Adapter 3 Custom (VMnet0)
Network Adapter 4 Custom (VMnet0)
USB Controller Present
Sound Card Auto detect
Serial Port Using named pi...
Display Auto detect
Description
Type here to enter a description of this virtual machine.

Résumé

Aujourd'hui, les entreprises placent la sécurité au cœur de leurs priorités. La sécurité informatique est essentielle au fonctionnement normal des réseaux informatiques, et la sélection des politiques de sécurité à utiliser est également essentielle. A cet effet, plusieurs mécanismes de sécurité ont été développés et mis à la disposition des administrateurs pour renforcer la sécurité du réseau et le rendre plus efficace et robuste.

Notre travail consiste à mettre en place une architecture VPN mobile sécurisée avec le protocole SSL pour l'entreprise GPL NAFTAL de Béjaia. Cette solution permettra aux clients distants de l'entreprise de s'interconnecter via des tunnels sécurisés utilisant l'infrastructure réseau publique (Internet).

Afin de mettre en pratique l'étude réalisée sur les VPN mobile, nous avons établi une simulation avec le simulateur GNS3 où nous avons réalisé la configuration des routeurs de la topologie proposée en réseau. Et pour finir, nous avons utilisé l'application Openvpn sur Windows et Android pour sécurise les accès distants aux applications d'entreprise, en créant un réseau privé virtuel.

Abstract

Today, companies place security at the heart of their priorities. Computer security is essential to the normal operation of computer networks, and the selection of security policies to be used is also essential. To this end, several security mechanisms have been developed and made available to administrators to strengthen network security and make it more efficient and robust. Our job is to set up a secure mobile VPN architecture with the SSL protocol for the GPL NAFTAL company in Béjaia.

This solution will allow remote enterprise clients to interconnect through secure tunnels using the public network infrastructure (Internet). In order to put into practice the study carried out on mobile VPNs, we established a simulation with the GNS3 simulator where we carried out the configuration of the routers of the proposed network topology. And finally, we used Openvpn application on Windows and Android to secure remote access to corporate applications, by creating a virtual private network.