République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Béjaïa

Faculté des Sciences Exactes

Département d'Informatique

Mémoire de fin de cycle

En vue de l'obtention d'un Master Professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Etude et Mise en place d'une infrastructure réseau intranet sécurisée Cas Station de Pompage Béni-Mansour (rattachée à la SONATRACH Béjaia)

Réalisé par :
BOULAOUAD HADIL
CHELFINI DAOUIA

Soutenu devant le jury composé de :

Président :	*M^r SALHI* Nadir
Examinateur :	*M^r MOHAMMEDI* Mohamed
Encadrant :	*M^r TOUAZI* Djoudi

Année Universitaire : 2021/2022

REMERCIEMENTS

Nos remerciements vont à Dieu le tout puissant de nous avoir donné la force, la volonté et le courage de réaliser ce modeste travail.
Nous tenons à remercier en premier lieu notre encadrant Mr TOUAZI DJOUDI, pour son encadrement, sa disponibilité et ses orientations qui nous ont permis de mener ce travail.
Nos remerciements les plus vifs vont tout particulièrement à notre encadrant de stage Mr ARKOUB MALEK pour son encadrement et orientation avec toute rigueur tout au long de notre stage au sein de SONATRACH.
Nous tenons à remercier Mr DJEBARI YASSINE pour ses orientations, ses encouragements et ses conseils. Nous tenons également à remercier les membres du jury d'avoir consacré leurs temps à la lecture et à la correction de ce mémoire.
Nous remerciements les plus particuliers à nos parents, en qui nous avons puisé tout le courage, la volonté et la confiance, nous leur serons éternellement reconnaissants.

DÉDICACES

Je dédie ce travail

À mes chers parents, aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consentis pour mon instruction et mon bien-être. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis toujours. Puisse Dieu, le très haut, vous accorde santé, bonheur et longue vie.

À mes chers frères Adem, Mohammed-Raid et ma chère sœur Alaa qui ont su être là au moindre besoin.

À mes chers oncles et tantes pour leur soutien tout au long de mon parcours universitaire.

À ma chère amie Abdoune Katia, merci pour ta présence tout au long de ma préparation, je suis tellement chanceuse de t'avoir.

À ma chère binôme et amie Daouia, ta présence est remarquable tout au long de notre parcours et notre préparation de mémoire.

Je tiens également à exprimer ma profonde gratitude à toute ma famille et tous ceux qui ont participé du pré ou du loin à la réalisation de ce travail.

HADIL.

DÉDICACES

Je dédie ce travail

À mes chers parents, aucune dédicace ne saurait exprimer mon respect, mon amour éternel et ma considération pour les sacrifices que vous avez consentis pour mon instruction et mon bien-être. Je vous remercie pour tout le soutien et l'amour que vous me portez depuis toujours. Puisse Dieu, le très haut, vous accorde santé, bonheur et longue vie.

À mes chers oncles, tantes , cousins et cousines pour leur soutien et aide tout au long de ce travail.

À ma chère amie Betta Farida, merci de ta présence tout au long de l'élaboration du travail.

À ma chère binôme et amie Hadil, ta présence est remarquable tout au long de notre parcours et notre préparation de mémoire.

À tout les personnes qui ont participé du pré et du loin à la réalisation de ce travail.

DAOUIA.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ACL Access Control List.

AD Active Directory.

BDM Business Development et Marketing.

BOOTP Bootstrap Protocol.

CME Call Manager Express.

DARPA Defense Advanced Research Project Agency USA.

DHCP Dynamic Host Configuration Protocol.

DNS Domain Name System.

DoS Denial Of Service.

DRGB Direction Régionale de Transport de Bejaia.

FTP File Transfer Protocol.

H-IDS Host Based Intrusion Detection System.

HSRP Hot Standby Router Protocol.

HTTP Hypertext Transfer Protocol.

IDS Intrusion Detection System.

IETF Internet Engineering Task Force.

IPS Intrusion Prevention System.

IPX Internetwork Packet Exchange.

IP Internet Protocol.

ISO International Organization for Standardization.

ISP Internet Service Provider.

LACP Link Aggregation Control Protocol.

LAN Local Area Network.

LS Ligne Spécialisée.

MAC Media Access Control.

MAN Metropolitan Area Network.

N-IDS Network Based Intrusion Detection System.

OSI Open System Interconnection.

P2P Peer To Peer (égal à égal).

PAgP Port Aggration Protocol.

PAN Personal Area Network.

RFC Requests For Comments .

RTC Région de Transport Centre.

RTE Région de Transport Est.

RTH Région de Transport de Haoued-el-Hamra.

RTO Région de Transport Ouest.

SBM Station de Béni-Mansour.

SNMP Simple Network Management Protocol.

TCP/IP Transmission Control Protocol/Internet Protocol.

TCP Transmission Control Protocol.

TRC Transport par Canalisations.

VLAN Virtual Local Area Network.

VPN Virtual Private Network.

VTP Virtual Trunking Protocol.

WAN Wide Area Network.

Introduction Générale

De nos jours, le développement industriel invoque le développement des infrastructures réseaux utilisées dans chaque entreprise où les réseaux informatiques occupent une place très importante. Ces derniers permettent de partager les ressources logicielles ou matérielles et rendront l'exploitation et la maintenance de ses ressources moins coûteuses.

La sécurité des réseaux informatiques et particulièrement celle des réseaux locaux est en évolution ceci est dut à l'ouverture des systèmes informatiques sur internet. Les menaces peuvent se produire au niveau externe comme au niveau interne, de ce fait les entreprises doivent protéger leurs réseaux en implémentant le maximum des techniques de sécurités.

L'entreprise SONATRACH de Bejaia fait partie de celles qui utilisent les outils informatiques les plus robustes pour la gestion et la sécurisation de leur réseau. L'objectif de notre projet de fin d'étude consiste à installer et configurer un réseau local au compte de l'entreprise Sonatrach, Station Beni-Mansour qui ne dispose pas d'un réseau local et utilise des méthodes classiques de la gestion d'information.

Notre mémoire est structuré en quatre chapitres : Le premier intitulé « Généralités sur les réseaux informatiques » consiste à définir brièvement quelques notions de bases sur les réseaux informatiques. Le deuxième intitulé «la sécurité des réseaux informatique » porte l'impact de la sécurité informatique sur les réseaux en exposant les objectifs ainsi que les stratégies de sécurité. Le troisième titré « Présentation de l'organisme d'accueil » a pour but en premier lieu de présenter la société nationale des hydrocarbures (SONATRACH) généralement et la RTC de Bejaia, son système informatique ainsi qu'une étude sur notre thème la station Beni-Mansour en abordant sa problématique, ses objectifs et les différentes solutions permettant de sécuriser le réseau. Le dernier intitulé « Réalisation » est consacré à la définition des différents outils et logiciels ayant servis à l'élaboration de notre implémentation, tout en expliquant les configurations établies ainsi que les tests.

Enfin, nous terminerons notre travail par une conclusion générale qui résumera les points accomplis dans ce travail et nos perspectives.

Chapitre 1

Généralités sur les réseaux informatiques.

1.1 Introduction :

À l'heure actuelle la communication et la technologie sont les maîtres mots de notre société où l'avenir des réseaux informatiques se grandit et se développe. L'intégration des réseaux locaux et grande distance dans le système d'information et de communication de l'entreprise a conduit au concept de réseau d'entreprise, dans lequel l'utilisateur a accès à toutes les ressources informatiques, grâce à une réelle distribution des applications.

Ce chapitre a pour objectif de présenter en premier lieu les réseaux informatiques en général leurs significations, objectifs, classifications ainsi que le modèle OSI et TCP/IP. Puis la définition des différents équipements et supports utilisés dans les réseaux locaux. Ensuite, nous décrivons les protocoles relatifs au traitement des données.

1.2 Définition d'un réseau informatique :

Un réseau informatique est un moyen de communication qui a pour fonction de permettre à des individus ou à des groupes de partager des informations ou des services et d'échanger des données. Ce dernier est constitué des équipements appelés nœuds qui utilisent des protocoles ou langages compréhensibles par tous afin d'assurer la communication entre eux.[1]

1.3 L'utilité des réseaux informatiques :

- Partage des ressources physiques tel que : imprimantes, modem, CD-Rom, disque dur.
- Partage des ressources logicielles qui permet l'accès de plusieurs utilisateurs à des applications sans avoir besoin de les installer.
- Communication entre les personnes distantes tel que : messagerie, chat, visioconférence.
- Réduction des coûts.
- Recherche d'informations : internet.

1.4 Les différents types des réseaux :

Afin de relier les ordinateurs entre eux, plusieurs types de réseaux sont employés. On peut les classifier selon leur taille, c'est-à-dire en fonction de la distance maximale parcourue par l'information entre deux machines. On distingue :

1.4.1 PAN (Personal Area Network)

Le réseau personnel est un réseau informatique formé autour d'une personne. Il peut être utilisé pour établir la communication entre ces appareils personnels afin de se connecter à un réseau numérique et à internet.[2]

1.4.2 LAN (Local Area Network)

Un réseau local est un réseau informatique situé sur un même site. C'est un système de communication de données limité à une zone géographique restreinte tel qu'une entreprise, un bâtiment, une salle informatique qui utilise des débits de l'ordre de quelques Mbits/s jusqu'au Gigabits/s.[2]

1.4.3 MAN (Metropolitan Area Network)

Le réseau métropolitain, appelé aussi réseau fédérateur est une infrastructure réseau publique ou privée qui permet l'interconnexion de plusieurs réseaux locaux LAN géographiquement proches (au maximum quelques dizaines de kilomètres) à des débits importants.[2]

1.4.4 WAN (Wide Area Network)

Le réseau étendu est constitué des réseaux locaux voir des réseaux métropolitains. Il est destiné comme son nom l'indique à transporter des données numériques sur des distances à l'échelle d'un pays, d'un continent. [2]

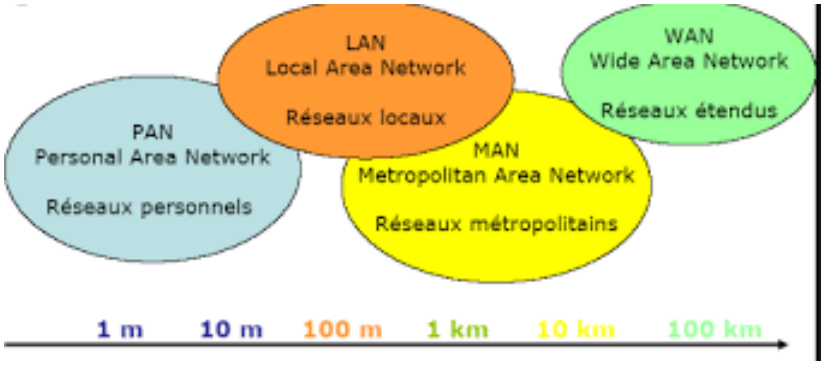

FIGURE 1.1 – Les Types des réseaux.

1.5 Architecture des réseaux :

Afin de permettre le transfert des données, On distingue généralement deux types d'architecture de réseaux bien différents, ayant tout de même des similitudes :

1.5.1 Les réseaux poste à poste (Peer to Peer/ égal à égal) :

L'architecture poste à poste (architecture P2P) est une architecture de réseau informatique couramment utilisée dans laquelle chaque poste de travail, ou nœud, a les mêmes capacités et responsabilités. Elle est souvent comparée et opposée à l'architecture classique client/serveur, dans laquelle certains ordinateurs sont dédiés au service des autres.[3]

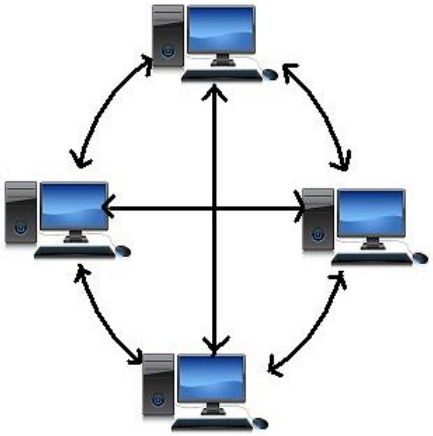

FIGURE 1.2 – Architecture poste à poste.

1.5.2 Les réseaux organisés autour de serveurs (client/serveur) :

L'architecture client/serveur est un modèle informatique dans lequel plusieurs composants travaillent dans des rôles strictement définis pour communiquer. Le serveur héberge, fournit et gère la plupart des ressources et des services qui seront consommés par le client. Dans ce type d'architecture à ressources partagées, un ou plusieurs ordinateurs clients sont connectés à un serveur central via un réseau ou une connexion Internet.[3]

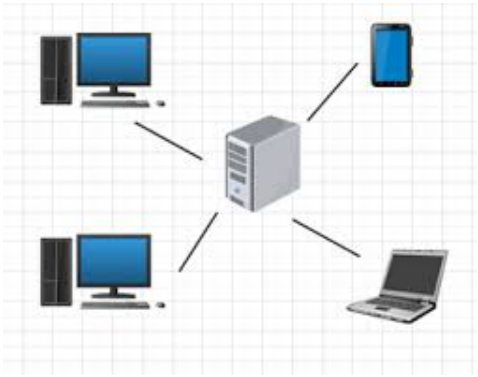

FIGURE 1.3 – Architecture client/serveur.

1.6 Topologie des réseaux :

Le mot topologie désigne la structure des réseaux en termes de liens d'interconnexion entre stations.On peut distinguer :

- La topologie logique : représente la façon dont les hôtes communiquent entre eux par le support. Les topologies logiques les plus courantes sont : Ethernet, token ring.
- La topologie physique : représente la manière dont les équipements du réseau sont arrangés physiquement.

1.6.1 Topologie en bus :

C'est l'organisation la plus simple d'un réseau ou tous les équipements sont reliés à un câble commun.Les transmissions se font donc par un seul lien sur lequel un seul ordinateur a le droit d'émettre des données à la fois.

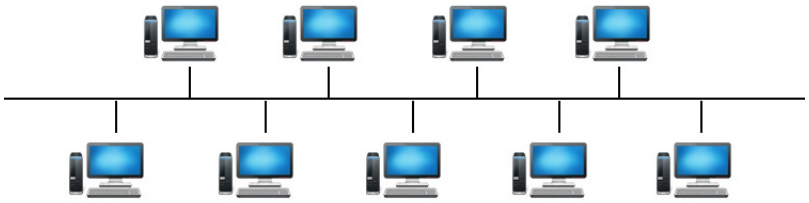

FIGURE 1.4 – Topologie en bus.

1.6.2 Topologie en anneau :

Son principe consiste à relier chaque nœud à ses deux nœuds adjacents formant une boucle fermée qui se caractérise par une connexion circulaire de la ligne de communication.

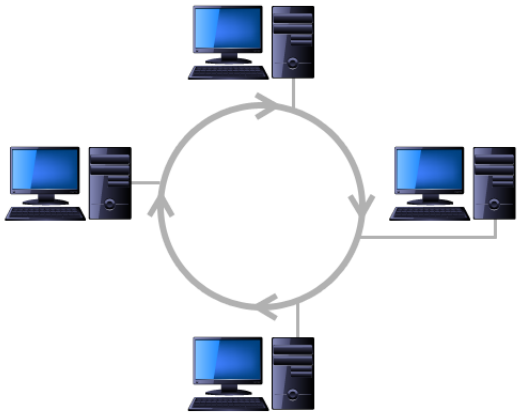

FIGURE 1.5 – Topologie en anneau.

1.6.3 Topologie en étoile :

Tous les périphériques du réseau sont connectés à un nœud central appelé concentrateur (Hub) par lequel transitent toutes les données formant une étoile.

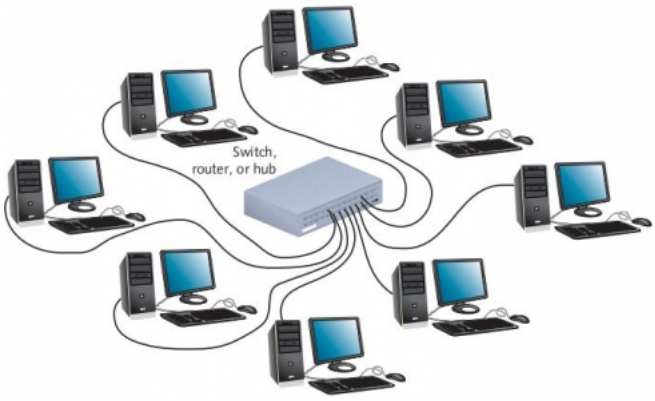

FIGURE 1.6 – Topologie en étoile.

1.7 Les alternatives de raccordements des réseaux :

1.7.1 Équipements d'interconnexion

— **Les unités hôtes :** les hôtes sont des unités directement connectées à un segment de réseau, nous pouvons les retrouver sous forme d'ordinateurs, de serveurs, de scanners ou d'imprimantes.[4]

— **Le concentrateur :** le concentrateur (appelé Hub en anglais) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Son rôle c'est de prendre les données binaires parvenant d'un port et les diffuser sur l'ensemble des ports.[4]

— **Le pont (bridge) :** le pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole.[4]

— **Les commutateurs :** comme le concentrateur, le commutateur (en anglais Switch) est un élément matériel qui permet de relier plusieurs ordinateurs entre eux. Sa seule différence avec le Hub, il est capable de connaître l'adresse physique des machines qui lui sont connectés et d'analyser les trames reçues pour les diriger vers la machine de destination.[4]

— **Les passerelles :**La passerelle est un système matériel et logiciel permettant de relier deux réseaux, servant d'interfaces entre deux protocoles différents.[4]

— **Les routeurs :** le routeur est un matériel de communication de réseau informatique qui permet de choisir le chemin qu'un message va emprunter. Il est utilisé pour relier des réseaux locaux de technologie différente (par exemple Ethernet et token ring). Il intervient sur la couche réseau.[4]

1.7.2 Les supports de transmission :

Afin que les informations circulent au sein d'un réseau, il est nécessaire de relier les différentes unités de communications à l'aide d'un support de transmission. Un support de transmission est un canal physique qui permet de relier des ordinateurs et des périphériques.

— **Les câbles à paires torsadées :** Les câbles à paires torsadées (twisted pair cables) sont des câbles constitués au moins de deux brins de cuivres entrelacés en torsade et recouverts des isolants. [5]

— **Les câbles coaxiaux :** Le câble coaxial est composé d'un fil de cuivre entouré successivement d'une gaine d'isolation, d'un blindage métallique et d'une gaine extérieure.[5]

— **Les câbles à fibre optique :** La fibre optique permet de transmettre des données sous forme d'impulsions lumineuses avec un débit nettement supérieur à celui des autres supports de transmissions filaires. Elle est constituée du cœur, d'une gaine optique et d'une enveloppe protectrice.[5]

— **Transmission sans fil :** Aucun support filaire n'est utilisé, il s'agit des réseaux sans fil. Des ondes sont utilisées pour transporter l'information.[5]

1.8 Le modèle OSI (Open System Interconnection) :

Le modèle d'interconnexion des systèmes ouverts conçus dans les années 1970 par l'Organisation internationale de normalisation -ISO-, est un cadre conceptuel qui décrit le fonctionnement d'un système de réseau ou de télécommunication. Ce modèle est constitué de 7 couches, dont les 4 premières sont dites basses et les 3 supérieures dites hautes.

- **La couche physique :** Cette couche comprend les équipements physiques impliqués dans le transfert de données, tels que les câbles et les commutateurs. C'est à son niveau où les données sont converties en un flux de bits, c'est-à-dire une chaîne de 1 et de 0.
- **La couche liaison de données :** Cette couche facilite le transfert de données entre deux dispositifs sur le même réseau. Comme la couche réseau, elle est également responsable du contrôle de flux et du contrôle d'erreurs dans les communications intra-réseau.Elle définit également une méthode d'accès au support.
- **La couche réseau :** Cette couche est chargée de faciliter le transfert de données entre deux réseaux différents.
- **La couche transport :** Cette couche est responsable de la communication de bout en bout entre les deux appareils. Elle est également responsable du contrôle de flux, du contrôle d'erreurs et du contrôle de congestion.
- **La couche session :** Cette couche est responsable de l'ouverture et la fermeture de la communication entre les deux appareils.
- **La couche présentation :** Cette couche est principalement responsable de la traduction, du cryptage et de la compression des données.
- **La couche application :** C'est la seule couche qui interagit directement avec les données de l'utilisateur. Les applications logicielles telles que les navigateurs Web et les clients de messagerie électronique s'appuient sur la couche application pour initier les communications.

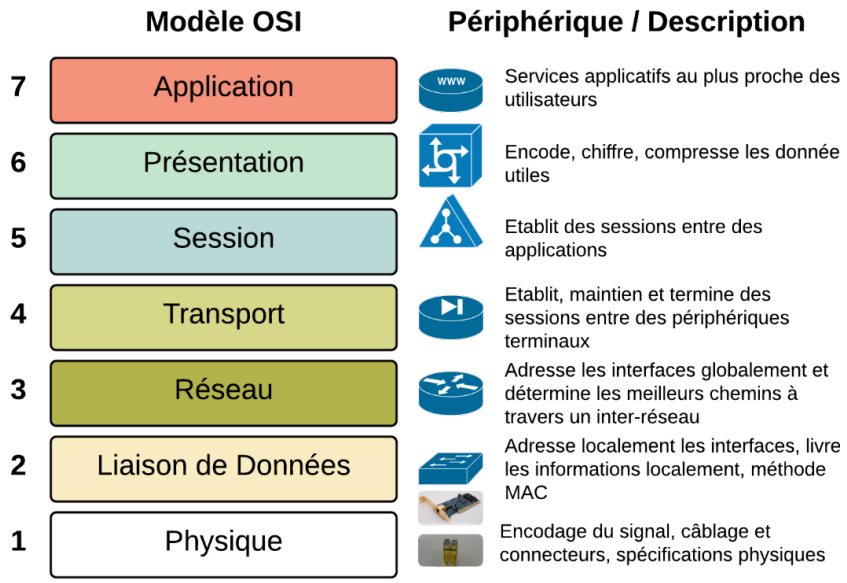

FIGURE 1.7 – Le modèle OSI

1.9 Le modèle TCP/IP :

Le modèle de référence TCP/IP est une suite de protocoles de communication a quatre couches utilisées pour interconnecter des périphériques réseaux sur Internet qui a été développé par la DARPA (Defense Advanced Research Project Agency USA).

Le protocole Internet (IP) est le système d'adressage de l'Internet et a pour fonction principale de transmettre des paquets d'informations d'un dispositif source à un dispositif cible. L'IP est le principal moyen d'établir des connexions réseau et constitue la base de l'Internet. Ces fonctionnalités nécessitent un autre protocole, généralement c'est le TCP.[6]

Les quatre couches du modèle TCP /IP sont :

— **La couche accès réseau (Network interface layer) :** Recouvre la couche physique et la couche liaison de données du modèle OSI. Elle sert d'interface avec le support de transmission et détermine la façon dont les données doivent être acheminées.

— **La couche internet (internet layer) :** Sert d'interconnecter des réseaux hétérogènes distants dans un mode non connecté. Son rôle est d'assurer l'adressage et le routage des paquets dans le réseau.

— **La couche transport (transport layer) :**Assure la transmission des données et la correction des erreurs lors de l'acheminement des données dans le support de communication.

— **La couche application :** Définit les protocoles d'application TCP/IP.Le rôle important de cette couche est le choix du protocole de transport à utiliser.[7]

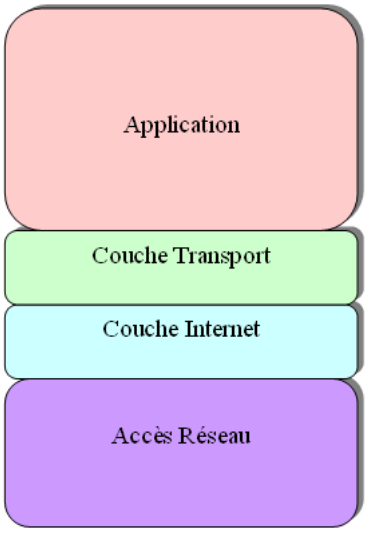

FIGURE 1.8 – Le modèle TCP/ IP.

1.10 Les protocoles :

1.10.1 Le VTP (Virtual Trunking Protocol)

Definition :

VTP est un protocole de liaison propriétaire de CISCO qui s'applique au niveau de la couche liaison de données du modèle OSI. Il est chargé de gérer les VLANs d'une manière centralisée et évite ainsi aux administrateurs du réseau de se connecter autant de fois qu'il y a de commutateurs dans un réseau pour ajouter, modifier ou supprimer la configuration d'un appelé serveur VTP, afin de distribuer ces informations de configuration VLAN d'un bout à l'autre du réseau commuté. Ce protocole réduit les délais d'administration et de maintenance des réseaux VLAN.[8]

Principe de fonctionnement :

Le protocole VTP définit la notion de domaine VTP où ce dernier est composé d'un ou plusieurs équipements interconnectés qui partagent le même nom. Il regroupe des commutateurs pour échanger leurs informations de configurations envoyés par le serveur VTP de chaque domaine concerné et plus dans un environnement VTP, un commutateur peut assurer un des trois rôles qui définissent les trois modes de fonctionnement suivants :

- **Mode serveur VTP :** Un commutateur en mode serveur est chargé de diffuser la configuration aux commutateurs du domaine VTP en envoyant des messages connus sous le nom « trames VTP », c'est le seul commutateur du domaine capable d'ajouter, supprimer ou renommer des VLAN dans le domaine VTP concerné.[8]
- **Mode client VTP :** Un commutateur en mode client est chargé d'appliquer la configuration émise par un commutateur en mode serveur, ce mode ne donne pas la possibilité de créer, modifier

ou supprimer des informations VLAN. Donc, il faut d'abord appliquer la modification au sein du serveur VTP pour qu'elle se propage aux différents commutateurs en mode client du même domaine VTP.[8]

- **Mode transparent VTP :** Un commutateur en mode transparent ne fait que diffuser les annonces VTP et les configurations du domaine VTP auquel il appartient à travers ses ports de liaison sans prendre en comptes leurs contenus.[8]

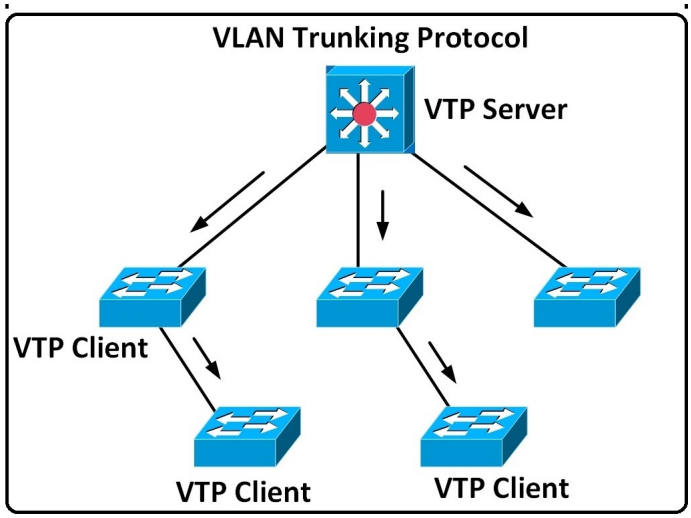

FIGURE 1.9 – Le protocole VTP.

1.10.2 Le protocole DHCP

Le protocole de configuration dynamique des hôtes (DHCP) est un protocole client/serveur qui automatise l'attribution d'adresses IP à des hôtes fixes et mobiles connectés avec ou sans fil. Les RFC 2131 et 2132 définissent le DHCP comme une norme de l'IETF (Internet Engineering Task Force) basée sur le protocole BOOTP (Bootstrap Protocol), un protocole avec lequel le DHCP partage de nombreux détails de mise en œuvre (qui est devenu obsolète car il ne fonctionne que sur les réseaux IPv4.). Le protocole DHCP permet aux hôtes d'obtenir les informations de configuration TCP/IP requises auprès d'un serveur DHCP.

1.11 Le protocole IP :

Internet Protocol IP est le protocole de base qui constitue internet avec le protocole TCP, car il est responsable de l'adressage d'ensemble des terminaux connectés au réseau et l'acheminement des paquets de données (datagrammes) entre les hôtes. Le protocole IP est considéré comme non fiable car il assure seulement la livraison des datagrammes.

1.11.1 Adressage IP :

L'adresse IP ou l'adresse logique désigne une machine en tant que membre d'un réseau ou d'un sous-réseau. Chaque interface possède une adresse IP fixée par l'administrateur du réseau ou attribuée d'une façon dynamique via des protocoles tels que le DHCP. Il existe des adresses IP de version 4 (IPv4) et de version 6 (IPv6). La version 4 est la plus utilisé, elle est codée sur 32 bits notée en général « a.b.c.d » qui représente des entiers entre 0 et 255 et chaque valeur représente une suite de 8 bits. L'adresse IP d'une machine va en conséquence être composée de 2 parties : le net-id (la partie fixe) et le host-id (la partie variable).

Classes d'adresses IP :

Il existe cinq classes d'adressage IP disponibles :

- **Classe A :**le premier bit est à « 0 ».
- **Classe B :**le premier bit est à « 10 ».
- **Classe C :**le premier bit est à « 110 ».
- **Classe D :**le premier bit est à « 1110 », réservée aux groupes de multidiffusion.
- **Classe E :**le premier bit est à « 1111 », réservée pour une utilisation future.

— **Adresse réseau :** Chaque réseau IP a une adresse qui est celle obtenue en mettant tous les bits de l'host-id à 0. Un réseau IP est complètement défini par son adresse de réseau et son masque de réseau.

— **Adresse de diffusion :** Cette adresse permet à une machine d'envoyer un datagramme à toutes les machines d'un réseau. Cette adresse est celle obtenue en mettant tous les bits de l'host-id à 1.

— **Adresse de bouclage (loopback) :** Les adresses de 127.0.0.0 à 127.255.255.255 sont également interdites. Les adresses 127.0.0.0 à 127.255.255.255 s'appellent l'adresse de boucle locale (loopback en anglais) et désigne la machine locale (localhost).

Les adresses Privées :

Un certain nombre de ces adresses IP sont réservées pour un usage interne aux entreprises (RFC 1918[3]) Elles ne doivent pas être utilisées sur l'internet où elles ne seront de toute façon pas routées. Il s'agit des adresses :

- **Classe A :** de 10.0.0.0 à 10.255.255.255.
- **Classe B :** de 172.16.0.0 à 172.31.255.255.
- **Classe C :** de 192.168.0.0 à 192.168.255.255.

Les adresses IP privées contrastent avec les adresses IP publiques, qui sont celles que l'on utilise sur le réseau public Internet et ne peuvent pas être utilisées dans un réseau domestique ou professionnel.

1.12 Le routage IP :

Le routage est le processus permettant, à un datagramme d'être acheminé vers le destinataire, lorsque celui-ci n'est pas sur le même réseau physique que l'émetteur.

1.12.1 Les types de routage :

On distingue :

- **Routage statique :** si les routes sont fixées manuellement par l'administrateur réseau.
- **Routage dynamique :** si les tables de routages sont automatiquement mises à jour pour tenir compte d'une modification du réseau global (panne de routeur, nouvelle route, ...).[9]

1.13 Conclusion

Dans ce chapitre nous avons présenté les réseaux informatiques d'une façon générale en citant les critères basiques qui montrent le rôle et la description d'un réseau informatique.

Chapitre 2

La sécurité des réseaux informatiques

2.1 Introduction

Chaque système informatique dans un réseau local a besoin d'implémenter des techniques de sécurité, afin de garantir le bon fonctionnement de ce réseau en gérant les droits d'accès aux ressources concernées et maintenant la confiance dans les relations d'échange. Ce chapitre sera dédié aux différents termes de sécurité.

2.2 La sécurité des systèmes informatiques :

La sécurité informatique désigne les processus et les outils conçus et déployés pour protéger les informations sensibles contre toute modification, perturbation, destruction ou inspection au sein du système d'information.

2.3 Principes de la sécurité informatique :

- **Authentification :** L'authentification a pour objectif de vérifier l'identité des processus communicants, il s'agit donc de s'assurer que celui qui se connecte correspond au nom indiqué.[10]
- **Intégrité des données :** C'est un ensemble des mécanismes garantissant qu'une information n'a pas été modifiée.[10]
- **Confidentialité des données :** C'est un ensemble de mécanismes permettant à une communication de données de rester privée entre un émetteur et un destinataire. La cryptographie ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données.[10]
- **Non répudiation :** C'est un mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.[10]
- **Disponibilité :** C'est un ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles, que ces dernières concernent l'architecture réseau, la bande passante, le plan de sauvegarde, etc..[10]

2.4 Les attaques :

2.4.1 Définition d'une attaque :

Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.[11]

2.4.2 Buts des attaques

- Obtention d'un accès au système.

- Vol des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- Récupération des données bancaires.
- Information sur l'organisation (entreprise de l'utilisateur, etc.).
- Trouble du bon fonctionnement d'un service.
- Utilisation du système de l'utilisateur comme « rebond » pour une attaque.
- Utilisation des ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

2.4.3 Conséquences des attaques

Les conséquences des attaques sont de divers ordres parmi eux :

- **Accès physique :** il s'agit d'un cas où l'attaquant à accès aux locaux, éventuellement même aux machines :
  - ✓ Coupure de l'électricité.
  - ✓ Extinction manuelle de l'ordinateur.
  - ✓ Vandalisme.
  - ✓ Ouverture du boîtier de l'ordinateur et vol de disque dur.
  - ✓ Ecoute du trafic sur le réseau.[11]
- **Interception de communications :**
  - ✓ Vol de session (session hijacking).
  - ✓ Usurpation d'identité.
  - ✓ Détournement ou altération de messages.[11]
- **Déni de service :** il s'agit d'attaques visant à perturber le bon fonctionnement d'un service. On distingue habituellement les types de déni de service suivant :
  - ✓ Exploitation de faiblesses des protocoles TCP/IP.
  - ✓ Exploitation de vulnérabilité des logiciels serveurs.[11]
- **Intrusions :**
  - ✓ Balayage de ports.
  - ✓ Elévation de privilèges : ce type d'attaque consiste à exploiter une vulnérabilité d'une application en envoyant une requête spécifique, non prévue par son concepteur, ayant pour effet un comportement anormal conduisant parfois à un accès au système avec les droits de l'application.
  - ✓ Maliciels (virus, vers et chevaux de Troie).[11]
- **Ingénierie sociale :**
  - ✓ Perte des informations.

- ✓ Le vol ou la perte de données sensibles.
- ✓ La création de brèches dans un système de sécurité.
- ✓ L'exposition à un chantage (ransomware...).[11]

- **Trappes :** il s'agit d'une porte dérobée dissimulée dans un logiciel, permettant un accès ultérieur à son concepteur. [11]

2.4.4 Les attaques actives

Les attaques actives sont les attaques dans lesquelles l'attaquant tente de modifier l'information ou crée un faux message. La prévention de ces attaques est assez difficile en raison d'un large éventail de vulnérabilités physiques, de réseaux et de logiciels. Au lieu de la prévention, il met l'accent sur la détection de l'attaque et la récupération de toute perturbation ou retard causé par celui-ci.

Les formes des attaques actives

Les attaques actives sont sous forme :

- L'interruption dans laquelle un attaquant non autorisé essaie de se présenter comme une autre entité.
- La modification implique une modification du message original.
- La fabrication provoque des attaques de déni de service (DOS) dans lesquelles l'attaquant s'efforce d'empêcher les utilisateurs d'accéder à certains services, auxquels ils sont autorisés ou, en termes simples, l'attaquant accède au réseau, puis verrouille l'utilisateur autorisé.[12]

2.4.5 Les attaques Passives

Définition

Les attaques passives sont les attaques où l'attaquant se met en écoute non autorisée, en surveillant simplement la transmission ou la collecte d'informations. L'oreille indiscrète n'apporte aucun changement aux données ou au système.

Les formes des attaques passives

Au moment du transit, le message est sous une forme inintelligible qui ne peut être comprise par les pirates. C'est la raison pour laquelle, dans les attaques passives, la prévention est plus préoccupante que la détection. Les attaques passives empêchent les ports ouverts qui ne sont pas protégés par des pare-feu. L'attaquant recherche continuellement les vulnérabilités et une fois qu'il est trouvé, l'attaquant accède au réseau et au système.[12]

2.5 Type d'attaques

2.5.1 Les logiciels malveillants

Un logiciel malveillant est un logiciel qui est installé sur un ordinateur sans le consentement de son propriétaire.

2.5.2 Attaque de reconnaissance

La reconnaissance est la découverte non autorisée des systèmes, de leurs adresses et de leurs services, ou de leurs vulnérabilités. Il s'agit d'une collecte d'informations qui, dans la plupart des cas, précède un autre type d'attaque.[13]

2.5.3 Attaque d'accès

L'accès au système est la possibilité pour un intrus d'accéder à un périphérique qui ne dispose pas d'un compte ou d'un mot de passe. La pénétration dans un système implique généralement l'utilisation d'un moyen de piratage, d'un script ou d'un outil exploitant une vulnérabilité connue de ce système ou de l'application attaquée.[13]

2.5.4 Attaque par déni de service (Dos)

L'attaque par déni de service (DoS) est la forme d'attaque la plus répandue et aussi la plus difficile à éliminer. Dans la communauté des pirates, ce type d'attaque est même considéré comme trivial et est peu prisé, car son exécution demande peu d'efforts. [13]

2.6 Mécanisme de défense

2.6.1 Antivirus

Définition

Un logiciel antivirus est un programme ou un ensemble de programmes conçus pour prévenir, rechercher, détecter et supprimer les virus logiciels et autres logiciels malveillants tels que les vers, les chevaux de Troie, les logiciels publicitaires, etc.[14]

Fonctionnalités d'un Antivirus

Plusieurs sociétés différentes fabriquent des logiciels antivirus et ce qu'elles proposent peut varier, mais toutes remplissent certaines fonctions essentielles :

- Analyse des fichiers ou des répertoires spécifiques à la recherche de tout logiciel malveillant ou de modèles malveillants connus.

- Programmation des analyses qui s'exécutent automatiquement pour vous
- Lancement à tout moment une analyse d'un fichier particulier ou de l'ensemble de votre ordinateur, ou encore d'un CD ou d'une clé USB.
- Suppression tout code malveillant détecté, parfois, vous serez informé d'une infection et il vous sera demandé si vous souhaitez nettoyer le fichier, d'autres programmes le feront automatiquement en coulisses.[14]

2.6.2 Chiffrement

Définition

Le chiffrement désigne la conversion des données depuis un format lisible dans un format codé. Les données chiffrées ne peuvent être lues ou traitées qu'après leur déchiffrement. C'est l'élément fondamental de la sécurité des données. C'est le moyen le plus simple et le plus efficace de s'assurer que les informations du système informatique ne peuvent être ni volées ni lues par quelqu'un qui souhaite les utiliser à des fins malveillantes.[15]

Les techniques de chiffrement les plus courantes

Les deux principales techniques de chiffrement sont le chiffrement symétrique et asymétrique :

— **Chiffrement symétrique :**Également appelé chiffrement à clé privée. La clé utilisée pour encoder est la même que celle utilisée pour décoder, ce qui convient parfaitement pour les utilisateurs individuels et les systèmes fermés. Autrement, la clé doit être envoyée au destinataire, ce qui augmente le risque de compromission si elle est interceptée par un tiers. Cette méthode est plus rapide que la méthode asymétrique.[15]

— **Chiffrement asymétrique :** cette méthode utilise deux clés différentes (publique et privée) mathématiquement reliées. Concrètement, les clés se composent uniquement de grands nombres qui ont été couplés entre eux mais ne sont pas identiques, d'où le terme asymétrique. La clé privée est tenue secrète par le propriétaire et la clé publique est soit partagée parmi les destinataires autorisés, soit mise à disposition du public à grande échelle.[15]

2.6.3 Pare-feu

Définition d'un pare-feu :

Un pare-feu est un outil informatique matériel ou logiciel conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise). Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.[16]

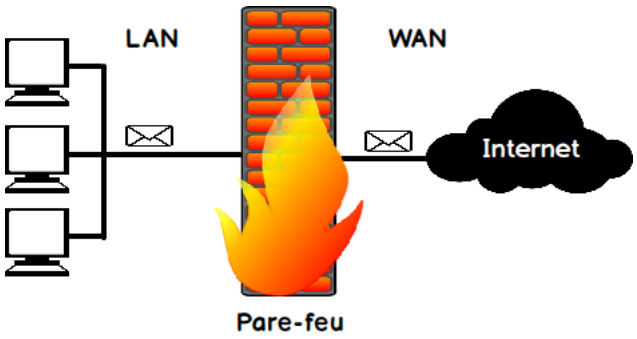

FIGURE 2.1 – Le parefeu.

Objectifs d'un pare-feu

Le Pare-feu peut jouer trois rôles :

- ✓ Bloquer les attaques et les infections en amont, notamment, le firewall peut bloquer les Trojans-Downloader, empêchant ainsi d'installer la charge utile.
- ✓ Bloquer les connexions établies par un Trojan et potentiellement les connexions vers le serveur de contrôle.
- ✓ Bloquer les infections automatiques provenant de machines infectées (vers) qui visent des services réseaux potentiellement vulnérables sur l'ordinateur. [16]

Le fonctionnement d'un pare-feu

Le fonctionnement d'un pare-feu repose sur un ensemble de règles prédéfinies permettant :

- ✓ D'autoriser la connexion (allow).
- ✓ De bloquer la connexion (deny).
- ✓ De rejeter la demande de connexion sans avertir l'émetteur (drop).
- ✓ Autoriser uniquement les communications ayant été explicitement autorisées : « Tout ce qui n'est pas explicitement autorisé est interdit ».
- ✓ D'empêcher les échanges qui ont été explicitement interdits.[16]

2.6.4 Proxy

Le Serveur Proxy (serveur Mandataire) est un intermédiaire entre les ordinateurs d'un réseau local et Internet. Utilisé la plupart du temps par le web, il s'agit alors d'un proxy HTTP qui permet :

- ✓ D'accélérer la navigation : mémoire cache, compression de données, filtrage des publicités ou des contenus lourds.
- ✓ La journalisation des requêtes (login).
- ✓ Le filtrage et l'anonymat.
- ✓ La sécurité des réseaux locaux. [17]

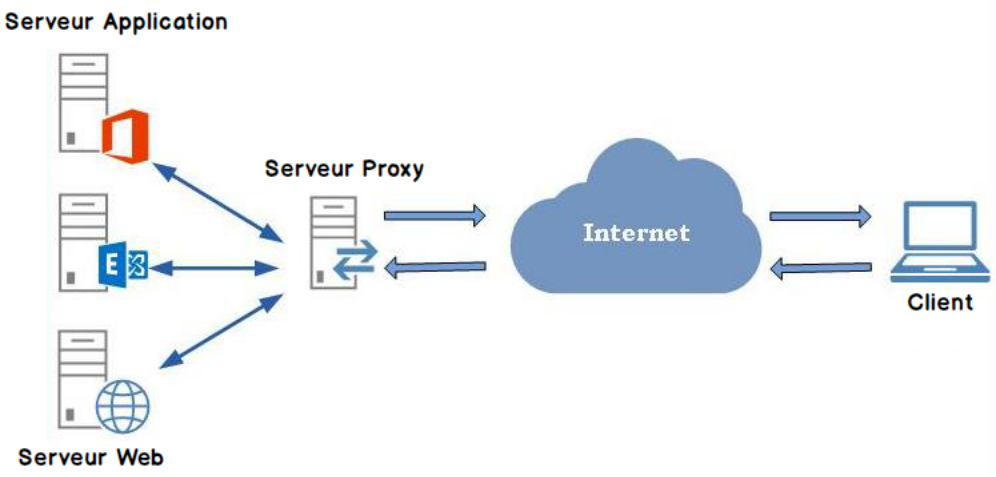

FIGURE 2.2 – Le proxy.

2.6.5 Système de détection d'intrusion

Définition

Il s'agit d'un logiciel de sécurité qui surveille l'environnement réseau pour détecter toute activité suspecte ou inhabituelle et alerte l'administrateur si quelque chose se produit.

Utilité du Système de détection d'intrusion

Les services informatiques des organisations déploient le système pour obtenir des informations sur les activités potentiellement malveillantes qui se produisent dans leurs environnements technologiques. En outre, il permet aux informations d'être transférées entre les départements et les organisations d'une manière de plus en plus sûre et fiable. À bien des égards, il s'agit d'une mise à niveau d'autres technologies de cyber sécurité telles que les pare-feu, l'antivirus, le cryptage des messages, etc.[18]

2.6.6 Système de prévention d'intrusion

Définition :

Système de prévention d'intrusion est un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion. Il existe deux grandes familles distinctes d'IDS :

— Les N-IDS (Network Based Intrusion Detection System), ils assurent la sécurité au niveau du réseau.

— Les H-IDS (Host Based Intrusion Detection System), ils assurent la sécurité au niveau des hôtes.[18]

2.7 La sécurité des réseaux

2.7.1 Réseaux locaux virtuels

Définition

Un VLAN est un ensemble de périphériques ou de nœuds de réseau qui communiquent entre eux comme s'ils constituaient un seul réseau local. Les VLAN regroupent logiquement les stations dans des domaines de diffusion distincts, indépendamment de leur emplacement physique. Ils facilitent ainsi la conception, l'administration et la gestion du réseau. Lorsque les VLAN sont bien configurés, le réseau s'adapte rapidement et simplement a la réorganisation des stations ou des utilisateurs. [19]

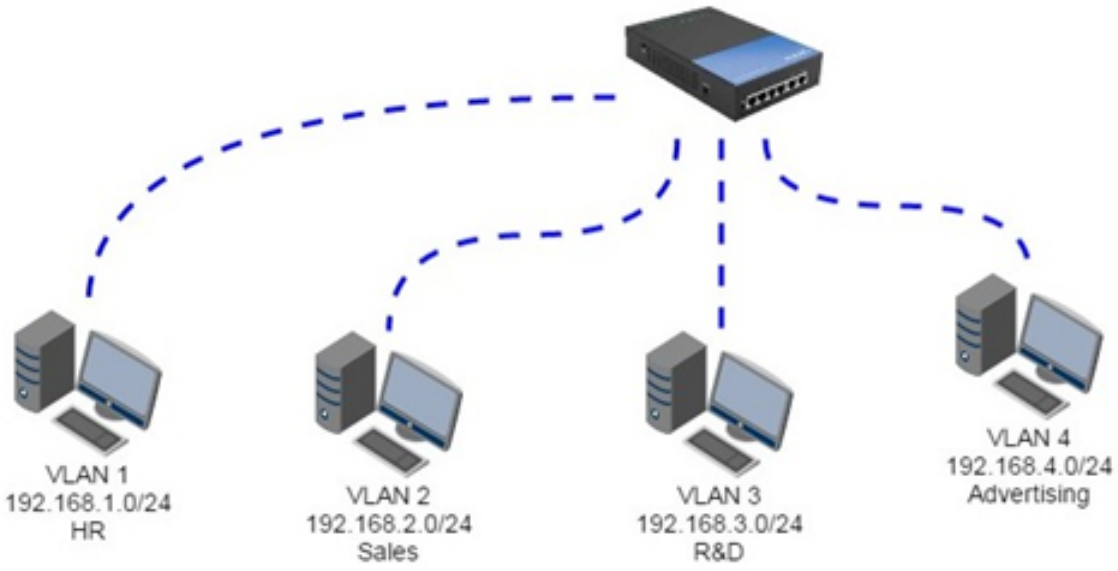

FIGURE 2.3 – Les VLANs.

Types de VLANs

Les VLANs différent selon les informations utilisées pour regrouper les stations. Il en existe trois niveaux, respectivement basés sur le port, l'adresse MAC, et sous réseau ou protocole.

— **VLAN de niveau 1 :**Aussi appelés VLAN par port, définit un réseau virtuel en fonction des ports de raccordement sur le commutateur.

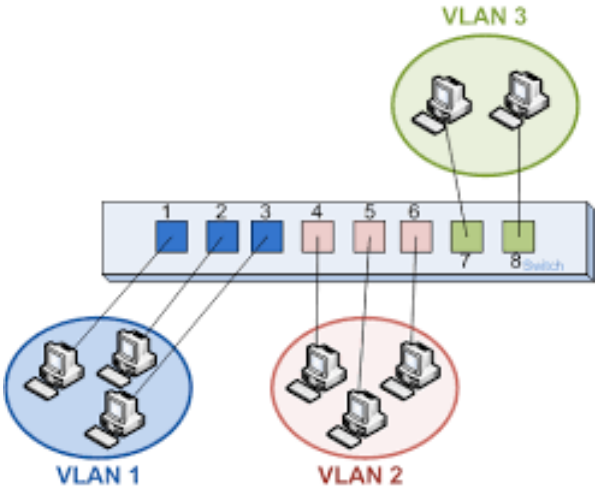

FIGURE 2.4 – Les VLANs par port.

— **VLAN de niveau 2 :**également appelé VLAN MAC, consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.

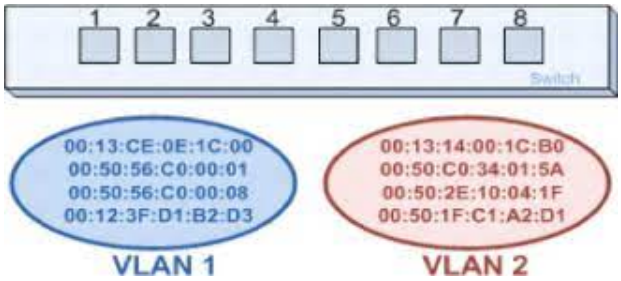

FIGURE 2.5 – Les VLANs par adresse MAC.

— **VLAN de niveau 3 :**on distingue plusieurs types de VLAN de niveau 3 :

✓ **Le VLAN par sous-réseau :**Il associe des sous réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.

✓ **Le VLAN par protocole :** permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

Avantages des VLANs :

— **Augmentation des performances :**La segmentation créée par les VLAN réduit la taille des domaines de broadcast et de ce fait le nombre de collisions sur ces domaines.

— **Réduction des coûts :**L'utilisation de VLAN permet de simplifier l'administration du réseau.

— **Gestion simplifié des projets et d'applications :**les VLANS rassemblent des utilisateurs et des périphériques de réseaux pour prendre en charge des impératifs commerciaux ou géographiques.

— **Gain de sécurité :**les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.

— **Optimisation de la bande passante :**en réalisant des réseaux disjoints, donc en réalisant des domaines de collision disjoints.

2.7.2 Les lignes louées ou spécialisés

Définition

On appelle lignes "louées" des lignes spécialisées (notées parfois LS) qui permettent la transmission de données à moyens et hauts débits (64 Kbps à 140 Mbps) en liaison point à point ou multipoints (service Transfix).[20]

Le besoin d'une ligne spécialisée

Pour obtenir une connexion à Internet, il faut, en règle générale, payer un abonnement auprès d'un prestataire Internet ou un service en ligne. Le prix de cette connexion dépend de la vitesse de transfert des données.[20]

2.7.3 Les réseaux privés virtuels VPNs

Définition

Un VPN est une solution de communication sécurisée et chiffrée entre deux réseaux ou entre un utilisateur individuel et un réseau. Il consiste en un tunnel logique établi entre deux entités, permettant de rendre invisible de l'extérieur les données qui y circulent.[21]

L'utilité des VPNs

Un VPN peut être utilisé par une entreprise pour :

✓ Les accès de télémaintenance.

✓ L'interconnexion de ses sites distants.

✓ La communication avec ses clients, fournisseurs ou partenaires.

✓ La connexion des nomades au réseau de l'entreprise.

Les types de VPNs

Parmi les types de VPN :

- **VPN site à site :**autrement dit Intranet VPN, c'est une solution utilisé pour relier deux ou plusieurs sites distants d'une entreprise entre eux via un support Internet avec une relation sécurisée, ce cas d'utilisation est l'un des cas les plus fréquents dans le réseau d'entreprise. Pour réaliser cette solution on aura besoin d'un routeur ou d'un pare-feu situé aux frontières.[22]

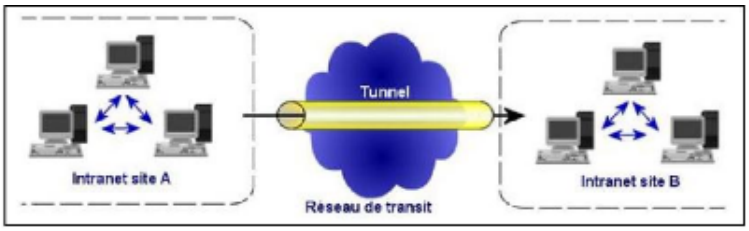

FIGURE 2.6 – VPN site à site.

- **VPN poste à site :** autrement dit VPN d'accès, ce type de VPN est aussi l'une des solutions les plus fréquemment utilisées. Elle consiste à permettre aux utilisateurs distants de se communiquer et d'accéder aux ressources de leurs réseaux d'entreprise avec un tunnel sécurisé. Afin de mettre en place cette solution on a besoin :
  - Du coté site central : mise en place d'un router, pare-feu ou d'un concentrateur SSL implémenté au frontière du réseau local.
  - Du coté poste de travail distant : installation d'un logiciel qui gère le type de protocole choisi et qui doit être compatible avec le matériel implémenté dans le site central.[22]

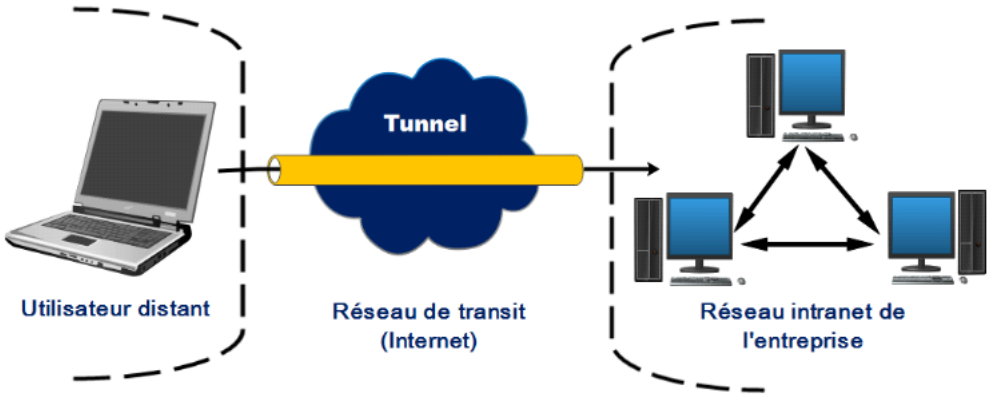

FIGURE 2.7 – VPN poste à site.

- **VPN poste à poste :** c'est le cas le plus simple, il s'agit de relier deux poste (dans le cas le plus général un poste et un serveur) et ceci se fait dans le cas où les deux postes se trouvent dans le même réseau local ou entre deux postes distant reliés eu même par un VPN site à site.[22]

2.7.4 EtherChannel :

L'Etherchannel qui est aussi connu sous l'appellation d'agrégation de liens est une technologie qui permet de regrouper plusieurs liens physiques en un seul lien logique. L'agrégation des liens (= EtherChannel) a pour objectif d'augmenter la vitesse de la bande passante, il est possible de regrouper jusqu'à 8 interfaces physiques, la seule condition est que les types de ports doivent être identiques sur ce même lien, par exemple, il n'est pas possible de regrouper deux ports FastEthernet et deux ports Gigabit Ethernet dans un EtherChannel. Il existe deux types de protocoles d'agrégation de lien :

— **Protocole PAgP (Port Aggration Protocol) :** est un protocole propriétaire de Cisco qui facilite la création automatique d'EtherChannel, quand une liaison EtherChannel est configurée grâce à PAgP, des paquets PAgP sont envoyés entre les ports compatibles EtherChannel pour négocier la formation d'un canal. Quand PAgP identifie des liaisons ethernet associées, il groupe les liaisons dans un EtherChannel.

— **Protocole LACP (Link Aggregation Control Protocol) :** LACP est un protocole de couche de liaison de données défini dans la norme IEEE 802.3ad. Il fournit une méthode pour contrôler le regroupement de plusieurs ports physiques pour former un seul canal logique. LACP permet à un commutateur de négocier un regroupement automatique en envoyant des paquets LACP à l'homologue, en étant une norme IEEE, il peut être utilisé pour faciliter les EtherChannels dans les environnements multi-fournisseurs.

2.7.5 Le protocole HSRP

Le protocole HSRP (Hot Standby Router Protocol) est un protocole propriétaire de CISCO, qui assure la redondance d'un sous-réseau local. Dans HSRP, deux routeurs ou plus donnent l'illusion d'un routeur virtuel. HSRP fonctionne selon un modèle actif-secondaire ou il permet de configurer deux routeurs ou plus en tant que routeurs en attente et un seul routeur en tant que routeur actif à la fois. Tous les routeurs d'un même groupe HSRP partagent une seule adresse MAC et une seule adresse IP, qui sert de passerelle par défaut vers le réseau local. Le routeur actif est responsable de la transmission du trafic. S'il tombe en panne, le routeur en attente assume toutes les responsabilités du routeur actif et achemine le trafic.

2.8 Conclusion

Ce chapitre a été dédié à la sécurité des réseaux ou nous avons défini la sécurité des systèmes informatiques et ses principes, les attaques et leurs types, les mécanismes de défense et enfin la sécurité des réseaux.

Chapitre 3

Présentation de l'organisme d'accueil.

3.1 Introduction

L'étude de l'organisme d'accueil est une étape importante qui sert à représenter les contraintes sous lesquelles se réalisera notre projet. Dans ce chapitre, nous allons présenter l'entreprise SONATRACH, citer les différents départements qui la constituent et donner quelques informations qui nous seront utiles pour notre approche sur le domaine et le milieu où nous souhaitons travailler.

3.2 Présentation de l'organisme d'accueil

3.2.1 Présentation de Sonatrach :

L'entreprise Sonatrach est l'acronyme de « Société Nationale pour le Transport et la Commercialisation des Hydrocarbures » est une entreprise publique algérienne qui a été créé le 31 Décembre 1963 par le décret n°63/491. Les statuts ont été modifiés par le décret n°66/292 du 22 Septembre 1966, et SONATRACH devient "Société nationale pour la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures", cela a conduit à une restructuration de l'entreprise dans le cadre d'un schéma directeur approuvé au début de l'année 1981 pour une meilleure efficacité organisationnelle et économique, de ces principes Sonatrach a donné naissance à 17 entreprises : (NAFTAL, ENIP, ENAC,...etc).Après sa restructuration en 1982 et sa réorganisation en 1985, Sonatrach s'est recentrée sur ses métiers de base que constituent les activités suivantes :

— Exploration et recherche.

— Exploration des gisements d'hydrocarbures.

— Le transport par canalisation.

— La liquéfaction et la transformation de GAZ.

— La commercialisation.

Au fil des années, Sonatrach est devenue un puissant élément d'intégration nationale et de stabilité économique et sociale surnommé la major africaine de l'industrie pétrolière.

3.2.2 Organisation :

Afin de réaliser les objectifs visées Sonatrach est divisée en cinq activités, chaque activité exerce ses métiers, développe son portefeuille d'affaires et contribue dans son domaine de compétences au développement des activités internationales de la société, qui sont représentées par l'organigramme suivant :

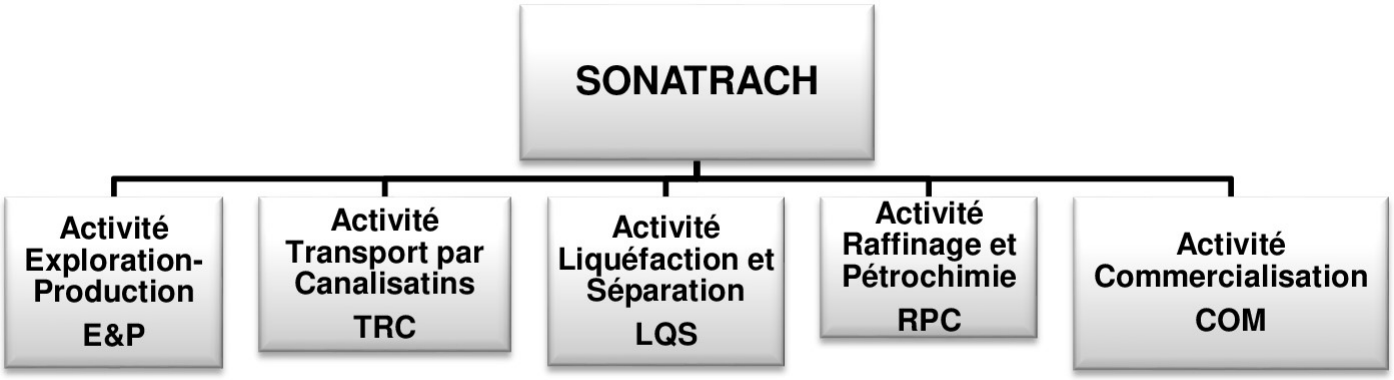

FIGURE 3.1 – Les activités de Sonatrach

3.3 Présentation de la branche de transport par canalisations TRC :

L'activité transport par canalisations (TRC) est chargée de l'élaboration et de l'application des politiques et stratégies en matière de transport des hydrocarbures par canalisations, dans le cadre des objectifs stratégiques de la Société. Elle assure le transport des hydrocarbures depuis les pôles de production au sud vers les pôles de demande et de transformation au nord (marché national et exportation).
L'Activité TRC couvre plusieurs domaines :

- La gestion et l'exploitation des ouvrages de transport des hydrocarbures.
- La maintenance, l'entretien et la protection des ouvrages et canalisations.
- L'installation de chargements portuaires.
- Les études et le développement, à l'exception des études relevant de la Direction Corporate Business Development et Marketing (BDM) et la réalisation de projets relevant de la Direction Centrale Engineering et Project Management.

La Sonatrach possède cinq régions de l'activité de transport par canalisations :

- Région de Transport Est RTE (skikda).
- Région de Transport Centre RTC (Bejaia).
- Région de Transport Ouest RTO (Arzew).
- Région de Transport de Haoued-el-Hamra RTH (centre distribution).
- Région de Transport d'In Aminas.

3.4 Présentation de la direction régionale de transport de Bejaia RTC :

La direction régionale de transport de Bejaia est l'une des cinq régions de transport par canalisations de la Sonatrach, qui se situe au nord de Bejaia (arrière port) à l'entrée de la ville. La RTC est chargée du transport, stockage et la livraison des hydrocarbures. Les hydrocarbures transportés à travers les canalisations gérées et exploitées par la DRGB sont :

- ✓ Le GAZ naturel.
- ✓ Le pétrole brut.
- ✓ Le condensat.

3.4.1 Organisation de la RTC :

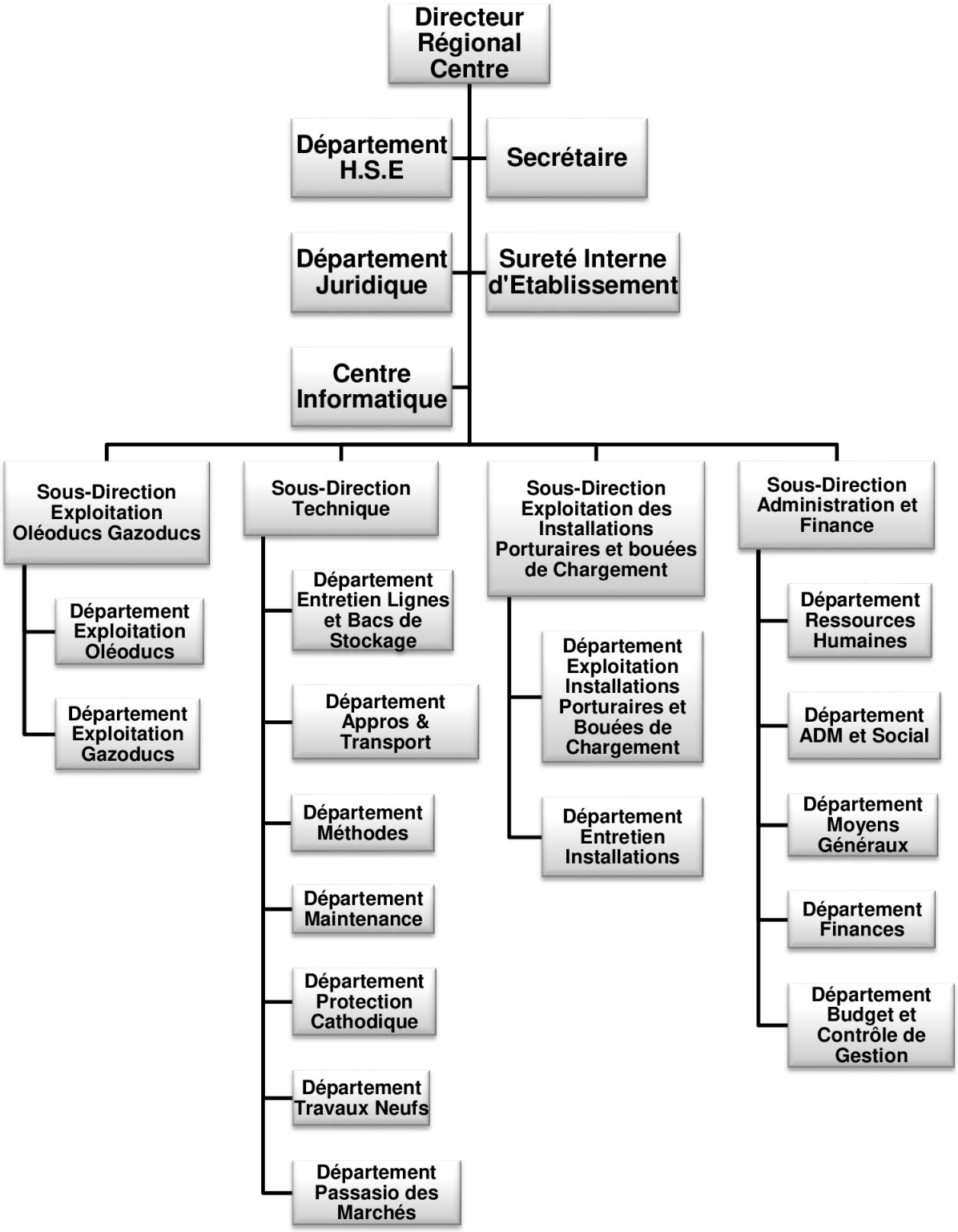

FIGURE 3.2 – Organigramme de la RTC

3.4.2 Définition des services :

- **Direction régionale :** dirigé par un directeur régional aidée par des assistants et secrétariat.
- **Secrétariat.**
- **Sureté interne d'établissement :** A pour mission de protéger et de sauvegarder le patrimoine humain et matériel de la DRGB.
- **Centre informatique :** : Regroupe un ensemble des moyens d'exploitation et de développement des applications informatiques pour l'ensemble des structures de la DRGB, ainsi que la gestion du réseau informatique interne.
- **Sous-Direction Exploitation Oléoducs Gazoducs :** Elle est organisée en deux départements :
  - ✓ Département Exploitation Oléoducs.
  - ✓ Département Exploitation Gazoducs.
- **Sous-Direction Technique :** Assurer la maintenance, la protection des ouvrages, l'approvisionnement, l'étude et le suivi de projets pour la réalisation de travaux neufs. Elle est organisée en sept départements :
  - ✓ Département Entretien Lignes et Bacs de Stockage.
  - ✓ Département Appros et Transport.
  - ✓ Département Méthodes.
  - ✓ Département Maintenance.
  - ✓ Département de protection cathodique.
  - ✓ Département Travaux Neufs.
  - ✓ Département Passation des Marchés.
- **Sous-Direction Exploitation des Installations Portuaires et bouées de Chargement :** Elle est chargée de l'exploitation des installations de la région, et de maintenir le fonctionnement des trois ouvrages en effectuant des réparations en cas de fuite, de Sabotage ou de panne pour les stations de pompage. Elle est organisée en deux départements :
  - ✓ Département Exploitation Installations Portuaires et Bouées de Chargement.
  - ✓ Département Entretien Installations.
- **Sous-Direction Administration et Finance :** : Elle a pour mission la gestion des ressources humaines et les moyens généraux et d'effectuer la gestion financière, le budget et le contrôle de gestion de la RTC. Elle est organisée en cinq départements :
  - ✓ Département Ressources Humaines.
  - ✓ Département ADM et Social.
  - ✓ Département Moyens Généraux.
  - ✓ Département Finances.
  - ✓ Département Budget et Contrôle de Gestion.

3.5 Présentation du centre informatique :

3.5.1 Structure :

Le centre informatique est composé de trois services, qui sont illustrées dans le schéma suivant :

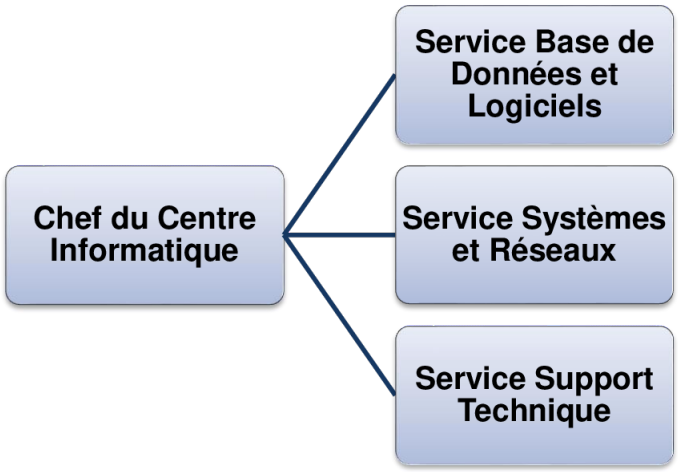

FIGURE 3.3 – Organigramme du centre informatique.

3.5.2 Rôle des services :

Chaque service joue un rôle et effectue des tâches spécifiques, on définit :

Service base de données et logiciels :

Ce service est dirigé par un chef (ingénieur SI) et des ingénieurs systèmes d'information.

Base de données :

Son rôle est :

- L'administration des bases des données de l'entreprise.
- Installation, configuration et exploitation du système de gestion de base de données SGBD et ses bases.
- Gérer la sauvegarde, la restauration et la migration des données.
- Assure la cohérence et la qualité des données introduites par les utilisateurs.

Logiciels :

- Etude et conception des systèmes d'information.
- Développement et maintenance des applications informatiques pour la RTC.
- Déploiement des applications et formations des utilisateurs.

Service Système et Réseaux :

Ce service est dirigé par un chef (ingénieur système (SIQ)), un ingénieur système distribué (SPD) et un ingénieur d'informatique industriel (SIQ).

Système :

- L'administration des serveurs.
- Installations des logiciels sur les serveurs.
- Orientation des travaux de l'équipe de développement par une bonne utilisation des ressources de l'ordinateur.
- Mise en œuvre des nouvelles versions de logiciels.

Réseaux :

- Définir les droits d'accès à l'utilisation du réseau.
- Assure la surveillance permanente pour détecter et prévenir les pannes.
- Etude et choix de l'architecture du réseau à installer et la participation à sa mise en place.

Service Support Technique :

Ce service est dirigé par un chef de support technique.

- Assistance aux utilisateurs en cas de problèmes software et hardware.
- Installation des logiciels de gestion, technique et bureautique.
- Formation aux nouveaux produits installés.

3.6 État des lieux

3.6.1 Présentation du réseau RTC :

Le réseau informatique de la RTC de Bejaia est constitué de deux bâtiments, l'ancien bâtiment qui dispose de topologie physique en étoile étendue et le nouveau bâtiment dont la topologie physique est hybride (en étoile et en anneaux). Le type de lien entre ces deux derniers est la fibre optique.

3.6.2 Infrastructure réseau :

L'architecture physique du réseau LAN de Sonatrach RTC est installée suivant le modèle hiérarchique qui divise le réseau en trois couches ou niveaux distinctes : couche cœur ou noyau (Core layer), couche distribution (Distribution layer) et couche d'accès (Access layer). Au niveau des stations rattachées à la Sonatrach RTC un réseau LAN est réalisé afin de faciliter la communication entre les utilisateurs des stations et l'utilisation des ressources centralisées au niveau de la DRGB. Le raccordement des stations au réseau Sonatrach RTC est réalisé à travers une ligne spécialisée de boucle fibre optique propriété de la SONATRACH.

3.6.3 Analyse du parc informatique

Le tableau suivant montre les différents équipements informatiques existant au niveau de l'entreprise Sonatrach RTC Béjaia.

Périphériques utilisés	Appellation
Commutateur cœur	Cisco Catalyst 9407
Commutateur distribution	Cisco Catalyst 3850
Commutateur accès	Cisco Catalyst 9200
	Cisco Catalyst 2960
	Cisco Catalyst 3550
	Cisco Catalyst 3850
CME(Call Manager Express)	Routeur 2900
ISP(Internet Service Provider)	Cloud PT
Terminal PC	PC bureau DELL, Laptop
Téléphonie IP	IP Phone 7960
Autres équipements	Serveurs, imprimantes, Access Point

TABLE 3.1 – Tableau du parc inforamtique existant.

3.7 Problématique et solutions proposées

3.7.1 Présentation de station de pompage Béni-Mansour :

L'activité principale de la station de pompage est la réception et le pompage des hydrocarbures liquides (pétrole brut et condensat) transportés par l'oléoduc depuis le Terminal Départ jusqu'au Terminal Arrivée. La station de pompage Béni-Mansour est l'une des plus importantes à l'échelle nationale en matière de transport par canalisations de pétrole brut. Réalisé au 27 juin 2006, elle est située à la commune de Taourirt (Wilaya de Bouira) à 107 km sud-ouest de la wilaya de Béjaia. Cette station permet le transport du brut vers la raffinerie de Sidi Arcine (Alger) sur un trajet de 135 km. La station est alimentée par un piquage au niveau du pipeline OB1 qui véhicule du pétrole brut du site Haoued EL Hamra vers le terminal pétrolier de Béjaia. La station a pour objectifs :

- Le pompage de brut vers la raffinerie d'Alger.
- Assurer un débit continuel avec une pression bien déterminée selon la demande des terminaux ou bien les exigences de la station.
- Contrôle du passage du condensat et du brut vers le terminal pétrolier de Béjaia.

3.7.2 Plan station Béni-Mansour avant l'installation des équipements :

La figure suivante montre le plan de la station de Béni-Mansour avant la mise en place des équipements.

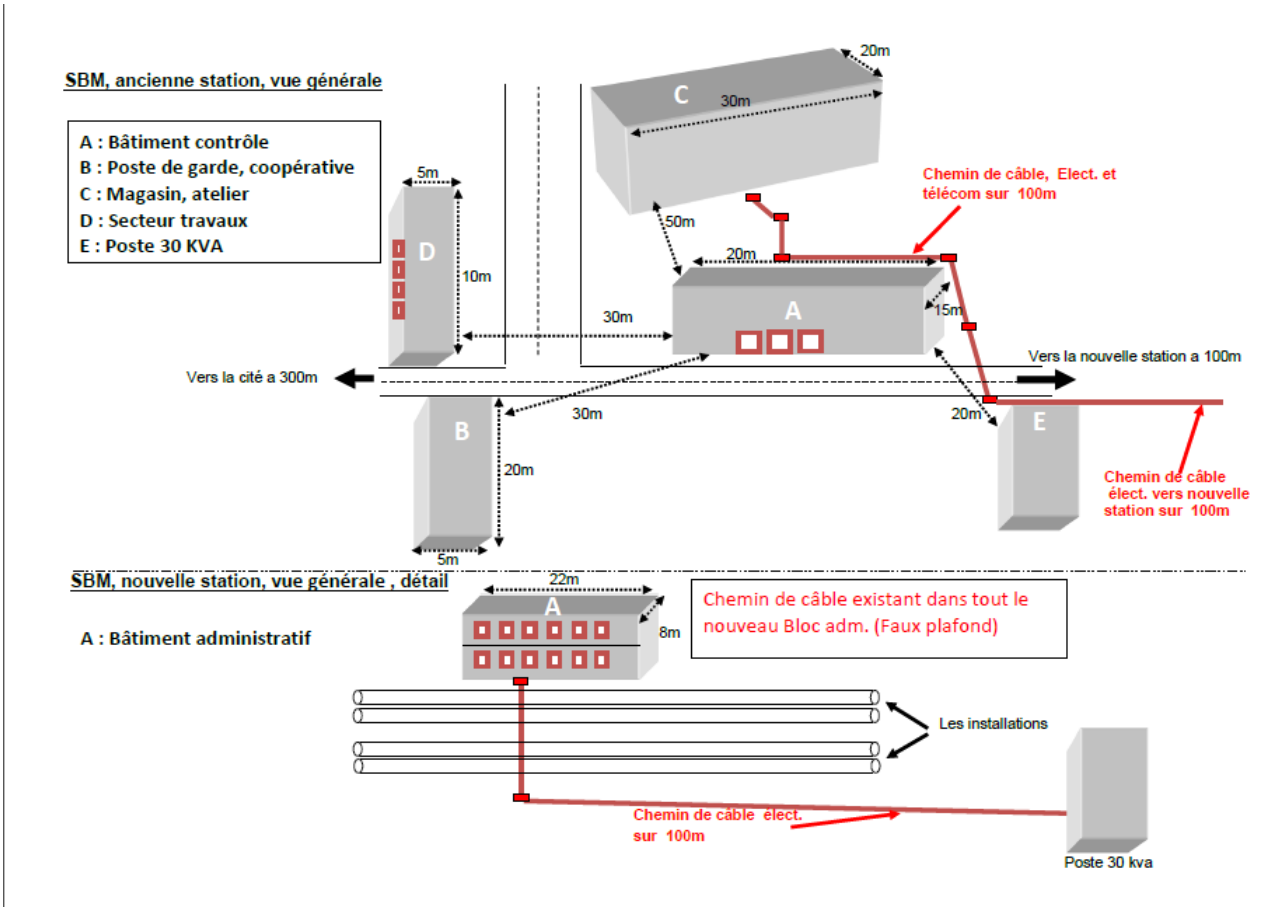

FIGURE 3.4 – Le Plan de la station Béni-Mansour avant l'installation.

3.7.3 Problématique

Au cours de notre stage,on a constaté que la station Beni-Mansour ne dispose pas auparavant d'un réseau local et continue à utiliser les méthodes de gestion de l'information classiques qui sont souvent moins efficaces et performantes. nous avons pu mettre le point sur ces questions :

- L'absence d'une architecture réseau. nous incite à questionner comment on peut concevoir une infrastructure réseau fiable et optimiser les performances, la disponibilité du réseau et la capacité d'extension du réseau ?
- Comment organiser les différents services du réseau local ?
- Comment éliminer les risques d'attaques depuis l'extérieur contre le réseau interne ?
- Comment relier le réseau de la station Béni-Mansour à le site de Sonatrach béjaia ? et comment assurer la sécurisation de la liaison entre ces deux sites ?

3.7.4 Solutions proposées

Notre objectif à travers ce projet est de mettre en place une architecture réseau sécurisée et l'interconnecter au site de béjaia. Pour cela nous avons proposé des solutions en prennant compte des problèmes évoqués auparavant :

— Proposer une architecture réseau en utilisant le modèle hiérarchique en couches.

— Segmentation des VLANs pour la bonne organisation du réseau local.

— Mettre en place d'une solution de pare-feux en exploitant ses différents fonctionnalités.

— Mettre en place une liaison VPN afin de connecter les deux sites Béni-Mansour et Sonatrach Béjaia pour permettre le transfert des données d'une façon privée et sécurisée.

3.7.5 Proposition de placement des équipements :

Le tableau suivant montre notre proposition pour l'emplacement des switchs de distribution et d'accès, ainsi que le routeur.

Bâtiment		Nombre d'utilisateurs	Equipements
Nouvelle station	A	23	Switch distribution Switch d'accès Routeur
Ancienne station	A	16	Switch d'accès.
	C	06	Switch d'accès.
	D	08	Switch d'accès.

TABLE 3.2 – Tableau de proposition d'emplacement des équipements.

Plan station Béni-Mansour après l'installation des équipements :

La figure ci-dessous montre le plan de la station de Béni-Mansour après l'installation des switchs de distribution et d'accès, ainsi que le routeur.

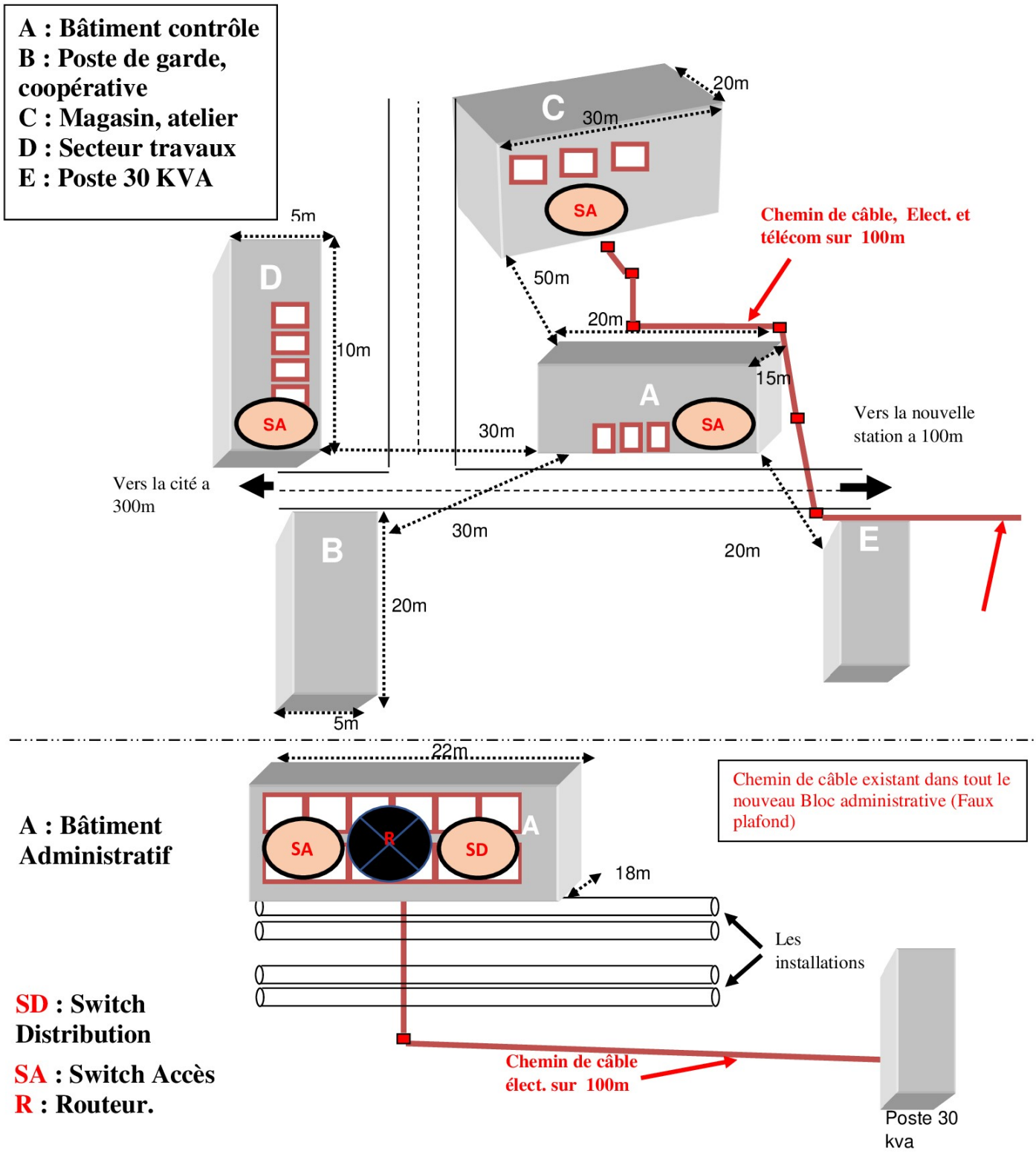

FIGURE 3.5 – Plan de Station Béni-Mansour après l'installation

3.8 Conclusion

À travers ce chapitre, nous avons présenté l'organisme d'accueil ainsi le service informatique de l'entreprise dans lequel nous avons effectué notre stage, l'état des lieux ainsi la problématique et les solutions proposées pour la station BENI-MANSOUR. Le chapitre suivant sera consacré à la réalisation.

Chapitre 4

Réalisation

4.1 Introduction

Ce chapitre sera dédié à la partie réalisation qui consistera à mettre en œuvre un réseau local pour la station de Beni-Mansour et le connecter avec la RTC afin d'augmenter le degré de partage des ressources matérielles et logicielles d'une part et permettre une communication et une fluidité de la circulation de l'information d'autre part.

4.2 Présentation de l'environnement de travail

L'environnement de travail désigne l'ensemble des conditions matérielles et humaines qui composent le cadre du travail.

4.2.1 Partie logiciels :

Présentation du simulateur GNS3 (Graphical Network Simulator)

GNS3 est un logiciel libre permettant l'émulation des équipements informatiques (routeur, switch, pc, ...) Ou la simulation de réseaux informatiques. Son avantage par rapport aux autres simulateurs est qu'il est proche de la réalité.

FIGURE 4.1 – Gns3.

Présentation de VMWARE

VMware Workstation est une solution logicielle professionnelle, puissante et complète qui permet de gérer l'ensemble des machines virtuelles locales ou sur le réseau. C'est la solution ultime de virtualisation pour émuler et gérer plusieurs systèmes d'exploitation.

FIGURE 4.2 – VMWare Workstation.

4.2.2 Partie hardware

Pare-feu FortiGate

FortiGate est une gamme de boitiers de sécurité UTM (appliance sécurité tout en un) comprenant les fonctionnalités firewall, Antivirus, système de prévention d'intrusion (IPS), VPN (IPSec et SSL), filtrage Web, Antispam et d'autres fonctionnalités : QoS, virtualisation, compression de données.

Avantages du Fortigate

— Une sécurité ultra-rapide, de bout en bout.

— Défense cohérente en temps réel avec FortiGuard Services.

— Une excellente expérience utilisateur grâce aux unités de traitement de la sécurité.

— Efficacité opérationnelle et workflow automatisé.[23]

Pare-feu ASA

Le par feu ASA est l'un des outils de sécurité les plus utilisés au sein des entreprises afin de garantir plusieurs fonctionnalités dont :

✓ Supervision du système, Filtrage des paquets, Filtrage et inspection applicative, Network Adresse, Translation (NAT), DHCP, Routage, Implémentation, Layer 3 ou Layer 2, Support VPN, Groupe d'objets (Object groups), Filtrage du trafic de botnets, Haute disponibilité, Support AAA.

Les équipements utilisés dans l'architecture

Le tableau suivant, montre les équipements utilisées afin de réaliser notre architecture, ainsi que leurs images.

Les stations	Les équipements	Les images
RTC Bejaia	Pare-feu FortiGate	
	Routeur(R1+R2)	IOU L3
	Switchs distribution	IOU L2
	Switch d'accés	IOU L2
	Serveur Windows	Windows Server 2022
Station Béni-Mansour	Pare-feu ASA	
	Routeur	IOU L3
	Switch distribution	IOU L2
	Switch d'accès	IOU L2

TABLE 4.1 – Tableau des équipements utilisés dans l'architecture proposée.

4.2.3 Partie software

— **Windows server 2022 :** Windows Server 2022 est une version du système d'exploitation Microsoft destiné aux serveurs, sortie en août 2021. Le système offre une sécurité multicouche avancée et une plateforme d'application flexible.

— **Windows 7 :** Windows 7 est la dernière version du système d'exploitation Windows de Microsoft qui succède à Windows Vista. Windows 7 possède le noyau amélioré de son prédécesseur.

— **Wireshark :** Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie.

— **Putty :** PuTTY est un émulateur de terminal doublé d'un client pour les protocoles SSH, Telnet, rlogin, et TCP brut. Il permet également d'établir des connexions directes par liaison série RS-232.

4.3 L'architecture proposée

La figure suivante illustre l'architecture du réseau que nous avons réalisé pour la station de Béni-Mansour et l'entreprise Sonatrach Béjaia sous le logiciel GNS3.

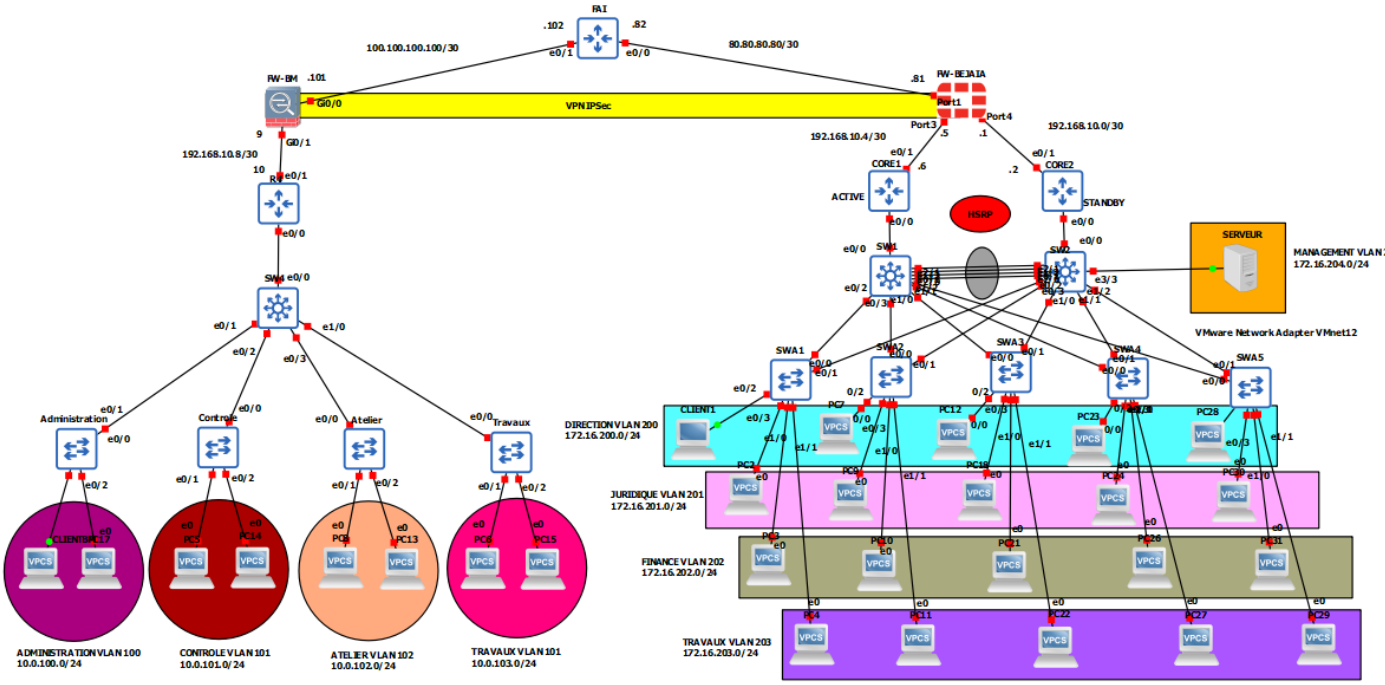

FIGURE 4.3 – Architecture proposée.

4.4 Plan d'adressage

4.4.1 Tableau d'adressage des VLANs

Site 1 : Station de Béni-Mansour

Les VLANs que nous avons proposé pour la station Béni-Mansour sont illustrés dans le tableau suivant, ainsi que les adresses IP.

VLAN ID	Nom du VLAN	Adresse IP
100	Administration	10.0.100.1/24
101	Contrôle	10.0.101.1/24
102	Atelier	10.0.102.1/24
103	Travaux	10.0.103.1/24

TABLE 4.2 – Tableau d'adressage des VLANs de la station Béni-Mansour.

Site 2 : Réseau LAN de RTC

Les VLANs de l'entreprise Sonatrach Béjaia sont illustrés dans le tableau ci-dessous, ainsi que leurs adresses IP.

VLAN ID	Nom du Vlan	Adresse IP	Adresse IP
200	Direction	172.16.200.1/24	172.16.200.2/24
201	Juridique	172.16.201.1/24	172.16.201.2/24
202	Finance	172.16.203.1/24	172.16.203.2/24
203	Technique	172.16.204.1/24	172.16.204.2/24
204	Management	172.16.205.1/24	172.16.205.2/24

TABLE 4.3 – Tableau d'adressage des VLANs du réseau LAN de RTC.

4.4.2 Tableau d'adressage des équipements

Le tableau ci-dessous, montre l'attribution des adresses IP aux interfaces des routeurs et des pare-feux pour les deux sites, la station Béni-Mansour et la Sonatrach Béjaia.

Equipements	Interface	Adresse IP
Routeur SBM (R1-SBM)	E0/0 E0/1	Encapsulation dot1Q 192.16.10.10/30
Routeur 1 RTC (CORE1-RTC)	E0/0 E0/1	Encapsulation dot1Q 192.168.10.6/30
Routeur 2 RTC (CORE2-RTC)	E0/0 E0/1	Encapsulation dot1Q 192.168.10.2/30
Routeur FAI	E0/0 E0/1	80.80.80.82/30 100.100.100.102/30
Pare-feu FortiGate	Port1 Port3 Port4	80.80.80.81/30 192.168.10.5/30 192.168.10.1/30
Pare-feu ASA	G0/0 G0/1	100.100.100.101/30 192.168.10.9/30

TABLE 4.4 – Tableau d'adressage des équipements.

4.5 Installation des systèmes et préparation du lab

4.5.1 Installation de GNS3

Pour installer GNS3, 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 ». La figure suivante représente l'interface de GNS3.

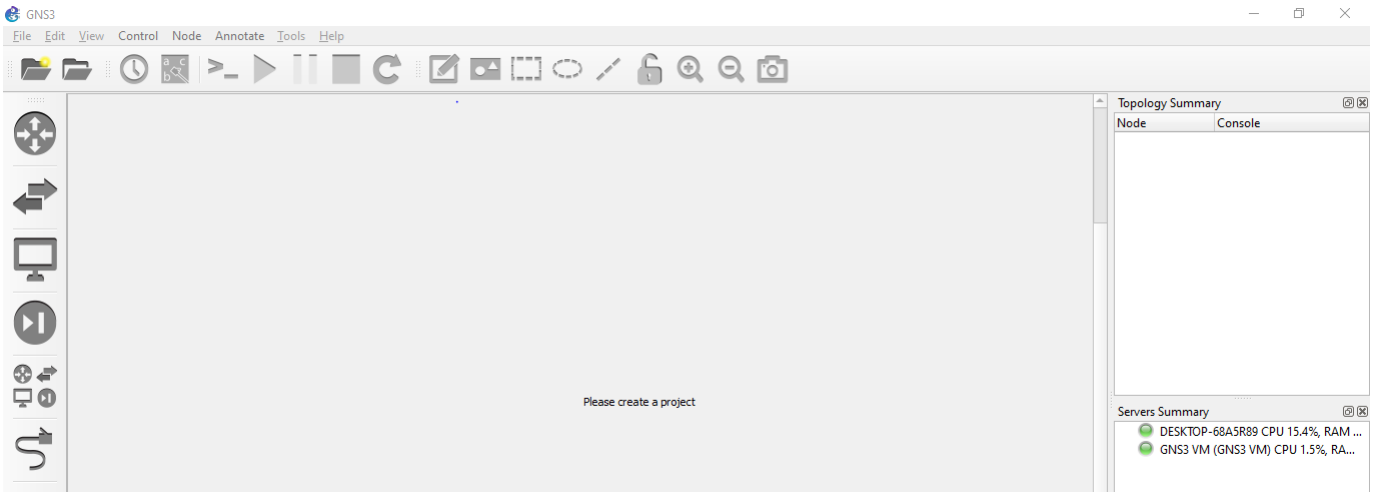

FIGURE 4.4 – Interface de GNS3.

4.5.2 Installation de VMware Workstation version 16

Afin de créer les machines utilisateurs virtuelles au sein du même pc, nous sommes appelés à installer VMware Workstation. Après l'installation de VMware une page d'accueil apparaîtra.

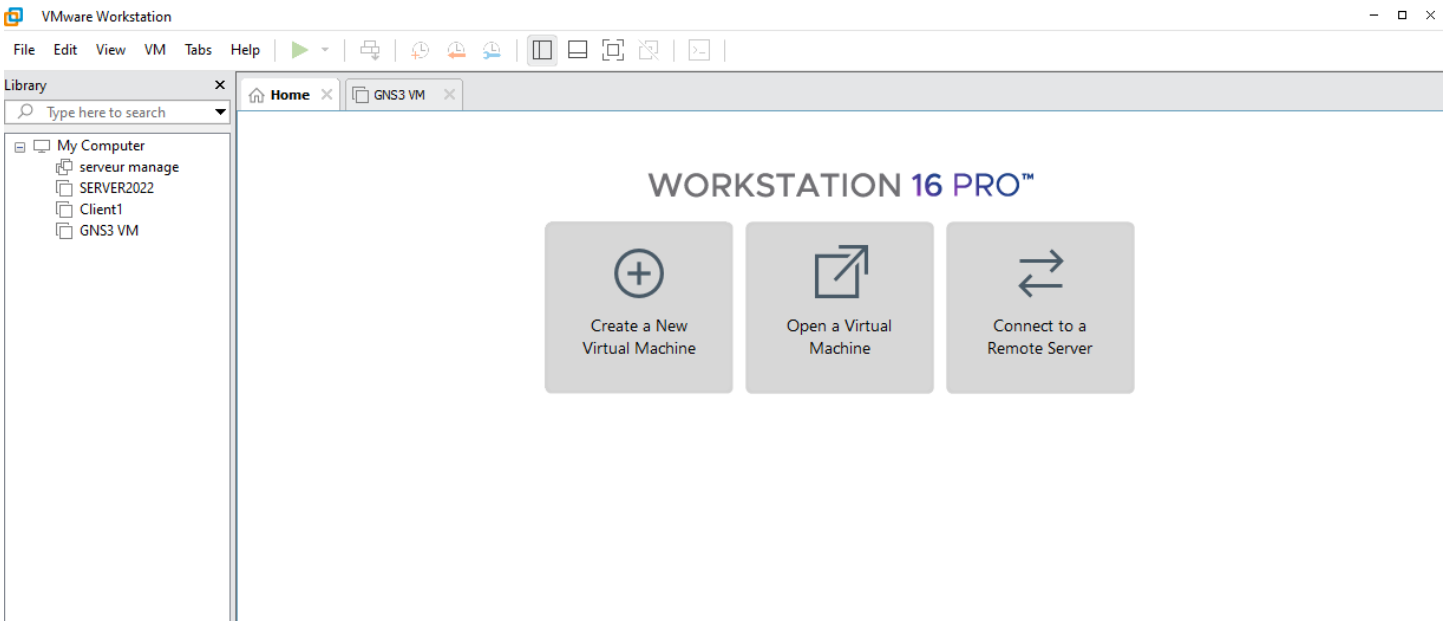

FIGURE 4.5 – Interface de VMWare Workstation Pro version 16.

4.5.3 Installation du Windows 7 sous VMware Workstation

Nous avons créé une machine après avoir ajouté l'image de Windows 7 sur VMware.

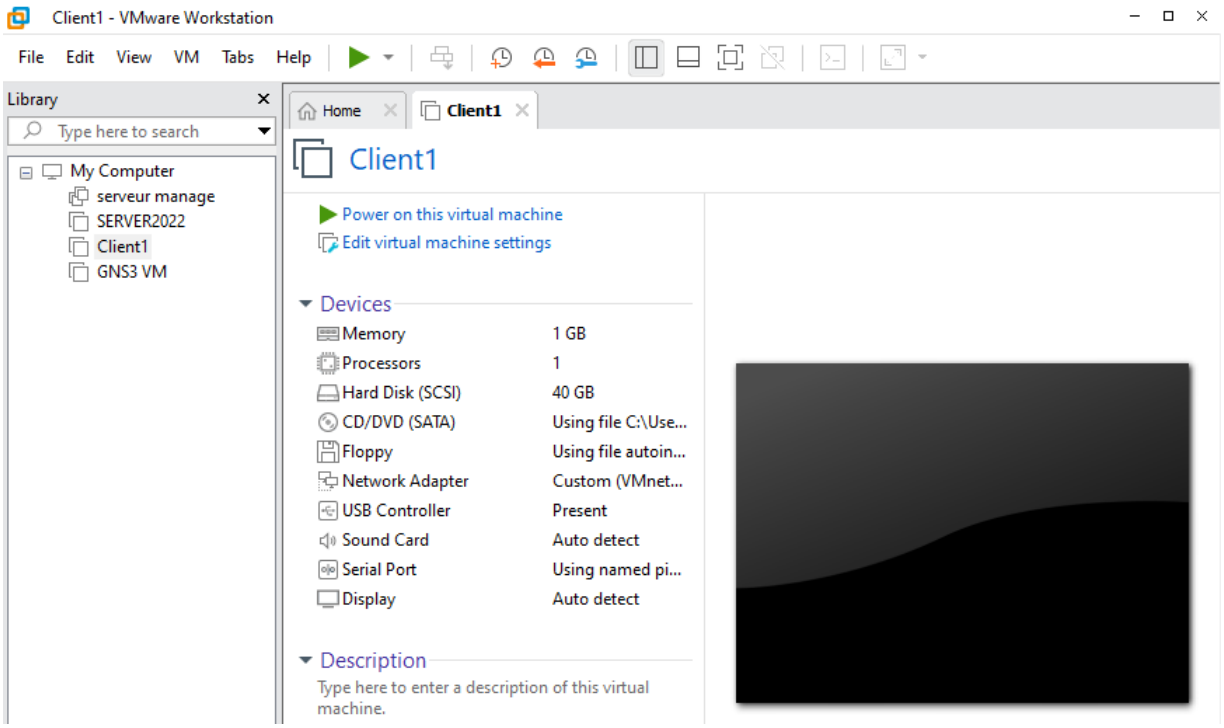

FIGURE 4.6 – Création de la machine virtuelle Windows 7.

4.5.4 Installation de la machine virtuelle Windows Server 2022

On installe la machine virtuelle Windows Server 2022, aprés avoir ajouter son image sur VMWare Workstation et en suit les étapes.

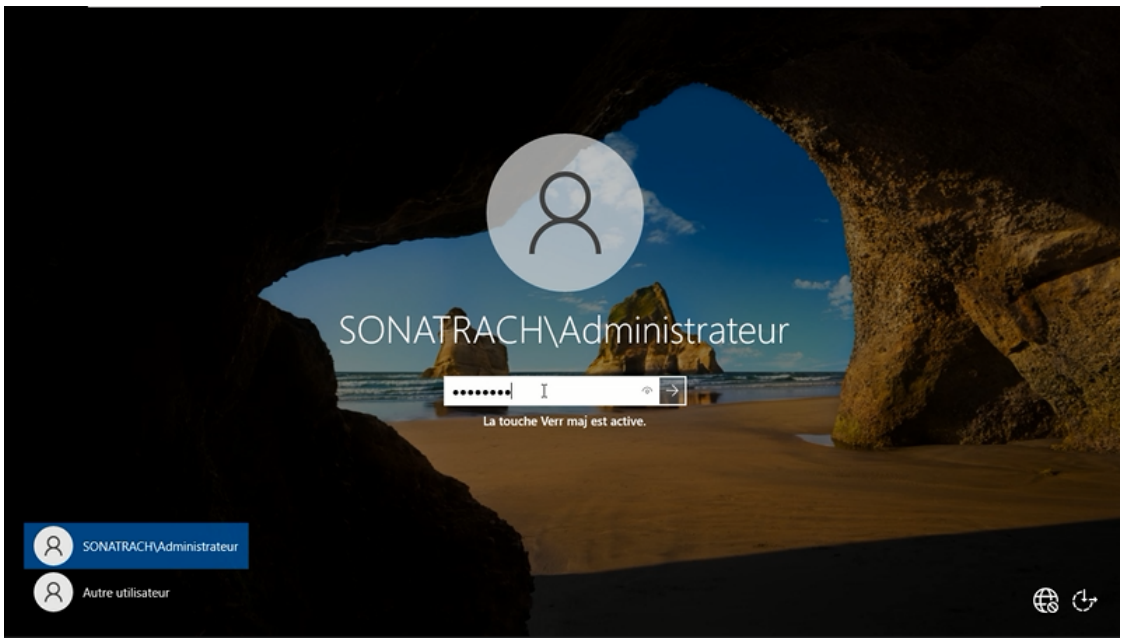

FIGURE 4.7 – La machine virtuelle Windows Server 2022 après l'installation de l'active directory.

4.5.5 Installation de l'active directory

Définition de l'active directory

C'est un service d'annuaire utilisé dans un environnement windows server. Il s'agit d'une structure de base de données qui partage des informations d'infrastructure pour gérer l'authentification et l'autorisation des utilisateurs et des machines sur les réseaux.

Sur la machine Windows serveur 2022 nous avons installé un contrôleur de domaine dont le nom de domaine est sonatrach.lan. La figure suivante montre l'interface du gestionnaire de serveur après l'installation des fonctionnalitées :

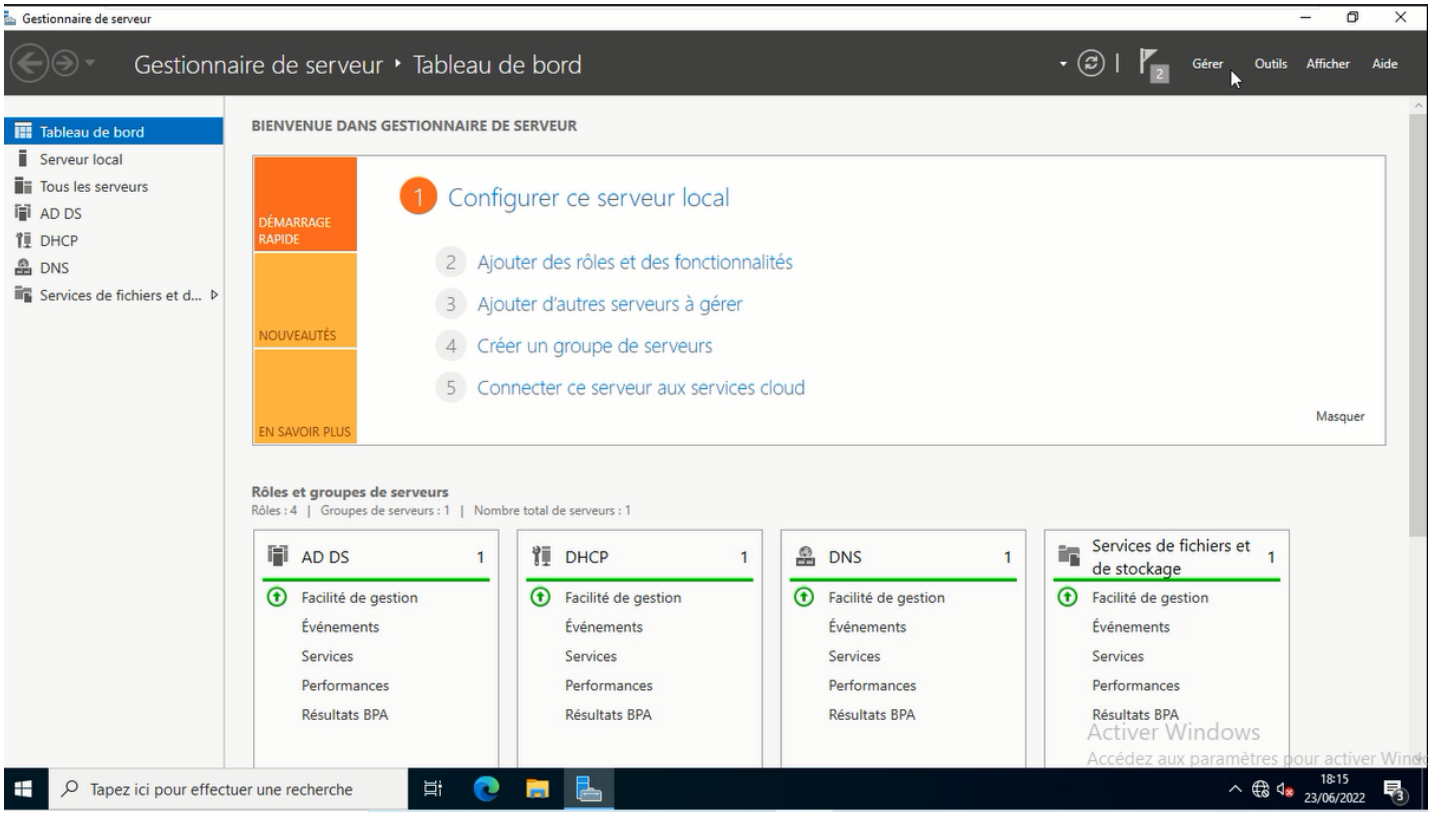

FIGURE 4.8 – Les rôles AD DS et DNS installés.

4.6 Configuration des équipements

Commençant par la configuration des commutateurs qui se réalisera au niveau de la console de chacun d'entre eux, en introduisant des commandes spécifiques. Dans ce qui suit, nous allons présenter un exemple de chaque configuration qui nous permettra de mettre en œuvre l'architecture proposée.

4.6.1 Partie 1 : Réseau de la station Béni-Mansour

Configuration du base :

Elle consiste à effectuer ces configurations suivantes dans le mode de configuration globale des périphériques qu'on accède avec la commande « configure terminal » ou « conf t » :

— Configuration du hostname et la console :

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname R1-SBM
R1-SBM(config)#line console 0
R1-SBM(config-line)#password SBM
R1-SBM(config-line)#login
R1-SBM(config-line)#exit
R1-SBM(config)#enable password SBM
R1-SBM(config)#exit
```

FIGURE 4.9 – Configuration du hostname et la console au niveau du "R1-SBM".

— Configuration du SSH

```
R1-SBM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-SBM(config)#ip domain-name sonatrach
R1-SBM(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R1-SBM.sonatrach

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1-SBM(config)#
*Jul 10 06:41:40.583: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1-SBM(config)#ip ssh version 2
R1-SBM(config)#service password-encryption
R1-SBM(config)#username admin password 0 p@55w0rd
R1-SBM(config)#line vty 0 4
R1-SBM(config-line)#login local
R1-SBM(config-line)#transport input ssh
R1-SBM(config-line)#exit
```

FIGURE 4.10 – Configuration du SSH au niveau du "R1-SBM".

Configurations des interfaces trunks :

Les liens en mode trunk représentent les liaisons entre les commutateurs ou entre un commutateur et un routeur. Les interfaces à configurer dans ce cas sont les liaisons entre l'ensemble des commutateurs de la couche d'accès et le commutateur distribution, ainsi que la liaison entre le commutateur de distribution et le routeur du réseau.

— **Le switch distribution**

```
SWD1-SBM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1-SBM(config)#interface range e0/0-3, e1/0
SWD1-SBM(config-if-range)#switchport trunk encapsulation dot1q
SWD1-SBM(config-if-range)#switchport mode trunk
SWD1-SBM(config-if-range)#
```

FIGURE 4.11 – Configuration des liens trunk au niveau du switch distribution "SWD1-SBM".

— **Le switch d'accès**

```
Administration#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Administration(config)#interface e0/0
Administration(config-if)#switchport trunk encapsulation dot1q
Administration(config-if)#switchport mode trunk
Administration(config-if)#exit
```

FIGURE 4.12 – Configuration des liens trunk au niveau du switch d'accès "Administration".

Configuration du protocole VTP :

Le serveur VTP : Il permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs clients du réseau. Il sera configuré au niveau du switch distribution.

```
SWD1-SBM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1-SBM(config)#vtp mode server
Device mode already VTP Server for VLANS.
SWD1-SBM(config)#vtp domain sbm
Changing VTP domain name from NULL to sbm
SWD1-SBM(config)#vtp password cisco
Setting device VTP password to cisco
SWD1-SBM(config)#vtp version 2
SWD1-SBM(config)#exit
```

FIGURE 4.13 – Configuration du serveur VTP au niveau du switch distribution "SWD1-SBM".

Les clients VTP : La configuration des clients VTP sera au niveau de tous les commutateurs de couche accès (switch d'accès) du réseau LAN.

```
Administration#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Administration(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
Administration(config)#vtp domain sbm
Changing VTP domain name from NULL to sbm
Administration(config)#vtp password cisco
Setting device VTP password to cisco
Administration(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
Administration(config)#exit
Administration#
```

FIGURE 4.14 – Configuration du client VTP au niveau du switch d'accès "Administration".

Création des VLANs :

La configuration des VLANs est faite au niveau du commutateur de la couche distribution c'est-à-dire le switch distribution du réseau.

```
SWD1-SBM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1-SBM(config)#vlan 100
SWD1-SBM(config-vlan)#name Administration
SWD1-SBM(config-vlan)#exit
SWD1-SBM(config)#vlan 101
SWD1-SBM(config-vlan)#name Controle
SWD1-SBM(config-vlan)#exit
SWD1-SBM(config)#vlan 102
SWD1-SBM(config-vlan)#name Atelier
SWD1-SBM(config-vlan)#exit
SWD1-SBM(config)#vlan 103
SWD1-SBM(config-vlan)#name Travaux
SWD1-SBM(config-vlan)#exit
SWD1-SBM(config)#
```

FIGURE 4.15 – Création des VLANs au niveau du switch distribution "SWD1-SBM".

Configuration des interfaces Access

Les ports auxquels nous connectons des PCs, sont dits des ports Access. Ces ports vont être assignés aux différents VLANs existants qui sont configuré sur tous les commutateurs d'accès.

```
Administration#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Administration(config)#interface range e0/1-2
Administration(config-if-range)#switchport mode access
Administration(config-if-range)#switchport access vlan 100
Administration(config-if-range)#exit
```

FIGURE 4.16 – Configuration des ports access au niveau du switch d'accès "Administration".

Configuration des routeurs

Routage inter-VLANs :

La subdivision de l'interface reliant le routeur et le commutateur Distribution, a pour but, d'accomplir la communication entre les différents VLANs (communication entre- VLAN). En effet, subdiviser l'interface en un nombre de sous interfaces, dépendant du nombre de VLAN qui existent, en leur affectant, ainsi, des adresse IP et des masques de sous-réseaux pour chacune d'elles.

```
R1-SBM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-SBM(config)#interface e0/0.100
R1-SBM(config-subif)#encapsulation dot1q 100
R1-SBM(config-subif)#ip address 10.0.100.1 255.255.255.0
R1-SBM(config-subif)#no shutdown
R1-SBM(config-subif)#exit
R1-SBM(config)#interface e0/0.101
R1-SBM(config-subif)#encapsulation dot1q 101
R1-SBM(config-subif)#ip address 10.0.101.1 255.255.255.0
R1-SBM(config-subif)#no shutdown
R1-SBM(config-subif)#exit
R1-SBM(config)#interface e0/0.102
R1-SBM(config-subif)#encapsulation dot1q 102
R1-SBM(config-subif)#ip address 10.0.102.1 255.255.255.0
R1-SBM(config-subif)#no shutdown
R1-SBM(config-subif)#exit
R1-SBM(config)#interface e0/0.103
R1-SBM(config-subif)#encapsulation dot1q 103
R1-SBM(config-subif)#ip address 10.0.103.1 255.255.255.0
R1-SBM(config-subif)#no shutdown
R1-SBM(config-subif)#exit
```

FIGURE 4.17 – Configuration des sub-interfaces au niveau du routeur SBM "R1-SBM".

Configuration de DHCP :

La configuration du DHCP est faite au niveau du routeur de la station Béni-Mansour, en créant tout d'abord des plages d'adresses qui comporteront les noms des VLANs et attribuera des adresses sur ces plages pour chaque VLAN avec une exclusion réservée à la passerelle par défaut des VLANs.

```
R1-SBM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-SBM(config)#ip dhcp pool vlan 100
R1-SBM(dhcp-config)#network 10.0.100.0 255.255.255.0
R1-SBM(dhcp-config)#default-router 10.0.100.1
R1-SBM(dhcp-config)#exit
R1-SBM(config)#ip dhcp pool vlan 101
R1-SBM(dhcp-config)#network 10.0.101.0 255.255.255.0
R1-SBM(dhcp-config)#default-router 10.0.101.1
R1-SBM(dhcp-config)#exit
R1-SBM(config)#ip dhcp pool vlan 102
R1-SBM(dhcp-config)#network 10.0.102.0 255.255.255.0
R1-SBM(dhcp-config)#default-router 10.0.102.1
R1-SBM(dhcp-config)#exit
R1-SBM(config)#ip dhcp pool vlan 103
R1-SBM(dhcp-config)#network 10.0.103.0 255.255.255.0
R1-SBM(dhcp-config)#default-router 10.0.103.1
R1-SBM(dhcp-config)#exit
R1-SBM(config)#exit
```

FIGURE 4.18 – Configuration du DHCP au niveau du routeur SBM "R1-SBM".

Confguration des interfaces du routeur et le routage statique

Après avoir configuré la première interface avec Encapsulation Dot1Q, on configure l'autre interface du routeur avec une adresse IP et un massque du sous-réseau, puis on réalise le routage statique par défaut qui consiste à router n'importe quel réseau vers n'importe quel (0.0.0.0) par la passerelle de sortie du routeur.

```
R1-SBM#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1-SBM(config)#interface e0/1
R1-SBM(config-if)#ip address 192.168.10.10 255.255.255.252
R1-SBM(config-if)#no shutdown
R1-SBM(config-if)#exit
R1-SBM(config)#
*Jul 10 06:51:36.611: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Jul 10 06:51:37.620: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
 to up
R1-SBM(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.9
R1-SBM(config)#exit
```

FIGURE 4.19 – Configuration d'interface et le routage statique au niveau du "R1-SBM".

4.6.2 Configuration du pare-feu ASA

Tout d'abord, on configure les interfaces du pare-feu ASA au niveau de la console.

```
FW-SBM(config)# interface g0/0
FW-SBM(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
FW-SBM(config-if)# no shutdown
FW-SBM(config-if)# ip address 100.100.100.101 255.255.255.252
FW-SBM(config-if)# exit
FW-SBM(config)# interface g0/1
FW-SBM(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
FW-SBM(config-if)# no shutdown
FW-SBM(config-if)# ip address 192.168.10.9 255.255.255.252
FW-SBM(config-if)# exit
FW-SBM(config)# route inside 10.0.100.0 255.255.255.0 192.168.10.10
FW-SBM(config)# route outside 0.0.0.0 0.0.0.0 100.100.100.102
FW-SBM(config)# exit
```

FIGURE 4.20 – Configuration de la console du pare-feu ASA.

La prochaine étape consistera à configurer le pare-feu ASA que nous avons déjà installé ou l'authentification est nécessaire :

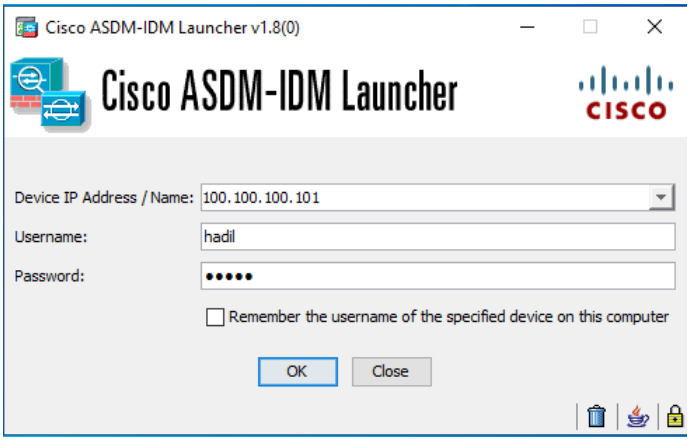

FIGURE 4.21 – Interface d'authentification du pare-feu ASA.

Après avoir introduit le mot de passe et le nom d'utilisateur (s'authentifier) l'interface d'accueil s'affichera comme suit :

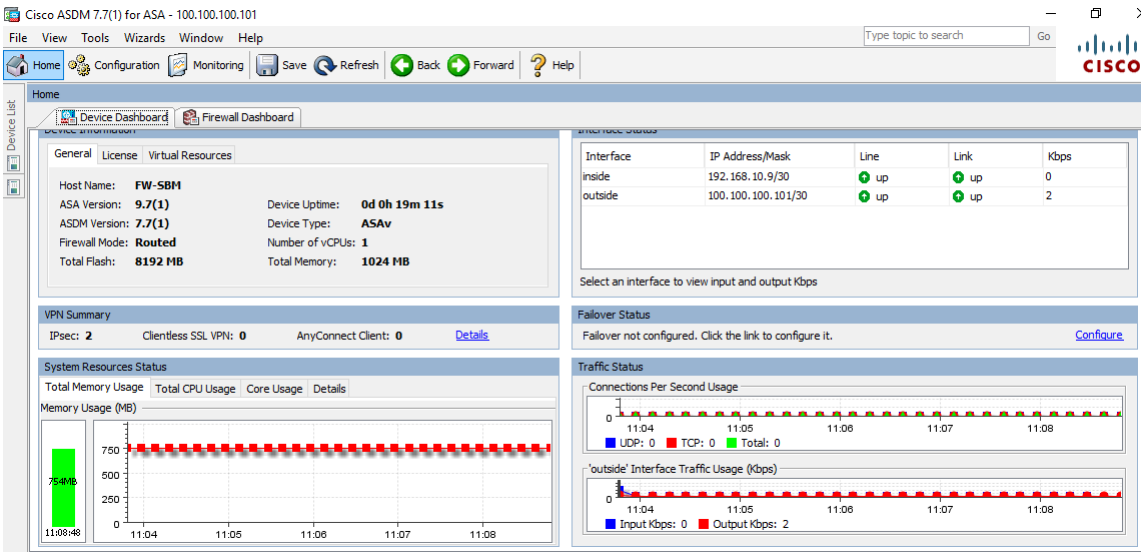

FIGURE 4.22 – Interface d'accueil du pare-feu ASA.

4.6.3 Partie 2 : Réseau LAN de la RTC :

Configurations des liens trunks :

— **Sur le switch distribution :** la configuration des liens trunks au niveau de la couche distribution se réalisera sur les deux switchs.

```
SWD1-RTC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1-RTC(config)#interface range e0/0-3, e1/0-3, e2/0-1
SWD1-RTC(config-if-range)#switchport trunk encapsulation dot1q
SWD1-RTC(config-if-range)#switchport mode trunk
```

FIGURE 4.23 – Configuration des liens trunks au niveau du switch distribution "SWD1-RTC".

— **Sur le switch d'accès :** la configuration des liens trunks au niveau de la couche accès se réalisera sur tous les autres switchs.

```
SWA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA1(config)#interface range e0/0-1
SWA1(config-if-range)#switchport trunk encapsulation dot1q
SWA1(config-if-range)#switchport mode trunk
```

FIGURE 4.24 – Configuration des liens access au niveau du switch d'accès "SWA1".

Configuration du protocole VTP :

— **Le serveur VTP :** sera réalisé au niveau des deux switchs distribution du réseau LAN.

```
SWD1-RTC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1-RTC(config)#vtp mode server
Device mode already VTP Server for VLANS.
SWD1-RTC(config)#vtp domain RTC
Changing VTP domain name from NULL to RTC
SWD1-RTC(config)#vtp password cisco
Setting device VTP password to cisco
SWD1-RTC(config)#vtp version 2
SWD1-RTC(config)#vtp pruning
Pruning switched on
SWD1-RTC(config)#exit
```

FIGURE 4.25 – Configuration du serveur VTP au niveau du switch distribution "SWD1-RTC".

— **Le client VTP :**sera réalisé au niveau de tout les switchs d'accès du réseau.

```
SWA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SWA1(config)#vtp domain RTC
Changing VTP domain name from NULL to RTC
SWA1(config)#vtp password cisco
Setting device VTP password to cisco
SWA1(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
SWA1(config)#exit
```

FIGURE 4.26 – Configuration du client VTP au niveau du switch d'accès "SWA1".

Création des VLANs :

La création des VLANs sera configuré au niveau du switch distribution qui va propager automatiquement aux autres switchs reliées.

```
SWD1-RTC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1-RTC(config)#vlan 200
SWD1-RTC(config-vlan)#name Direction
SWD1-RTC(config-vlan)#exit
SWD1-RTC(config)#vlan 201
SWD1-RTC(config-vlan)#name Juridique
SWD1-RTC(config-vlan)#exit
SWD1-RTC(config)#vlan 202
SWD1-RTC(config-vlan)#name Finance
SWD1-RTC(config-vlan)#exit
SWD1-RTC(config)#vlan 203
SWD1-RTC(config-vlan)#name Technique
SWD1-RTC(config-vlan)#exit
SWD1-RTC(config)#vlan 204
SWD1-RTC(config-vlan)#name Management
SWD1-RTC(config-vlan)#exit
```

FIGURE 4.27 – Création des VLANs au niveau du switch distribution "SWD1-RTC".

Configuration des interfaces des VLANs sous Windows Server 2022

Nous avons installé DHCP server sur la machine Windows server 2022. On va commencer par créer des étendus pour chaque VLAN déjà crée, nous allons des étapes comme la montre la figure suivante :

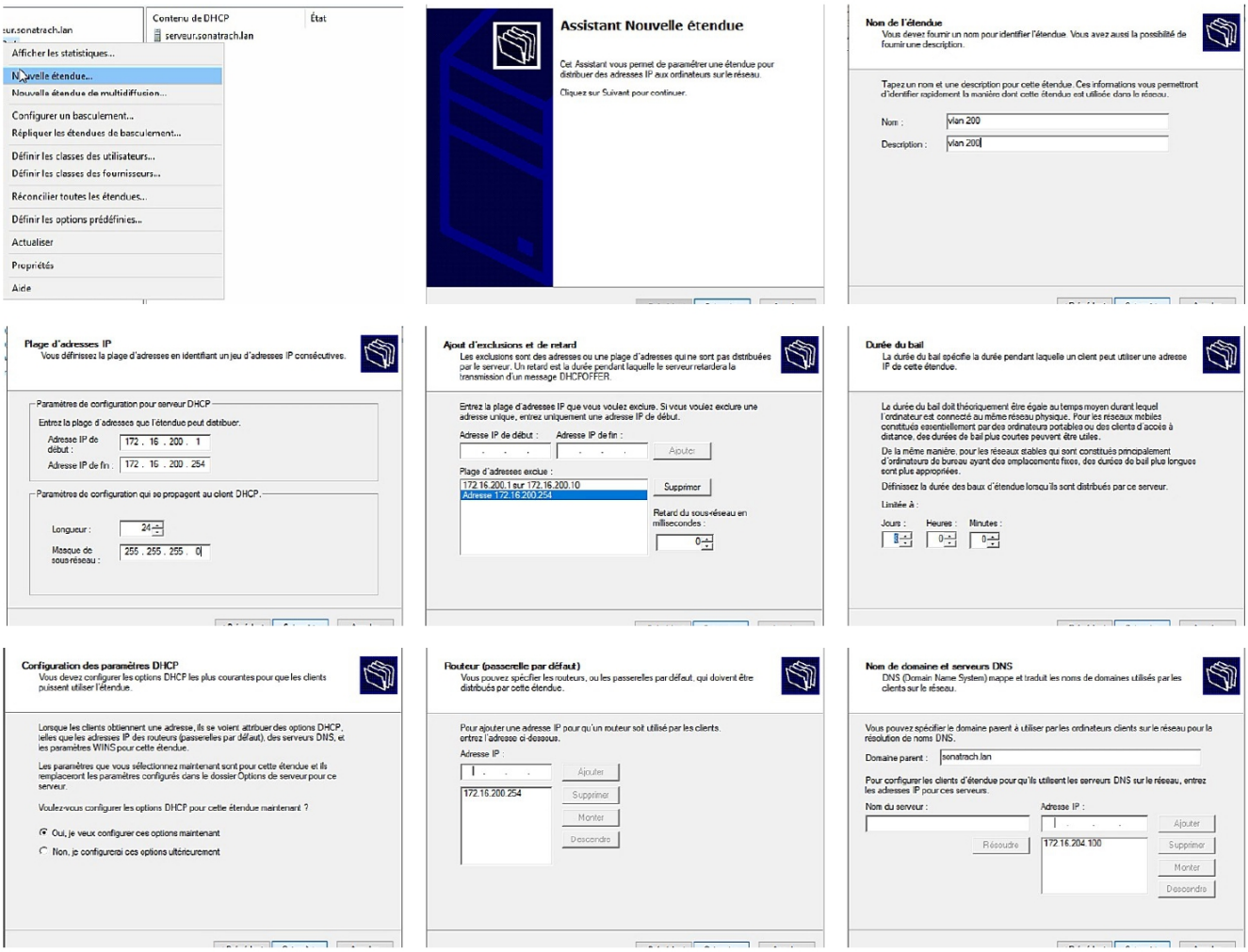

FIGURE 4.28 – Création de l'étendue des VLANs au niveau du Windows Server 2022.

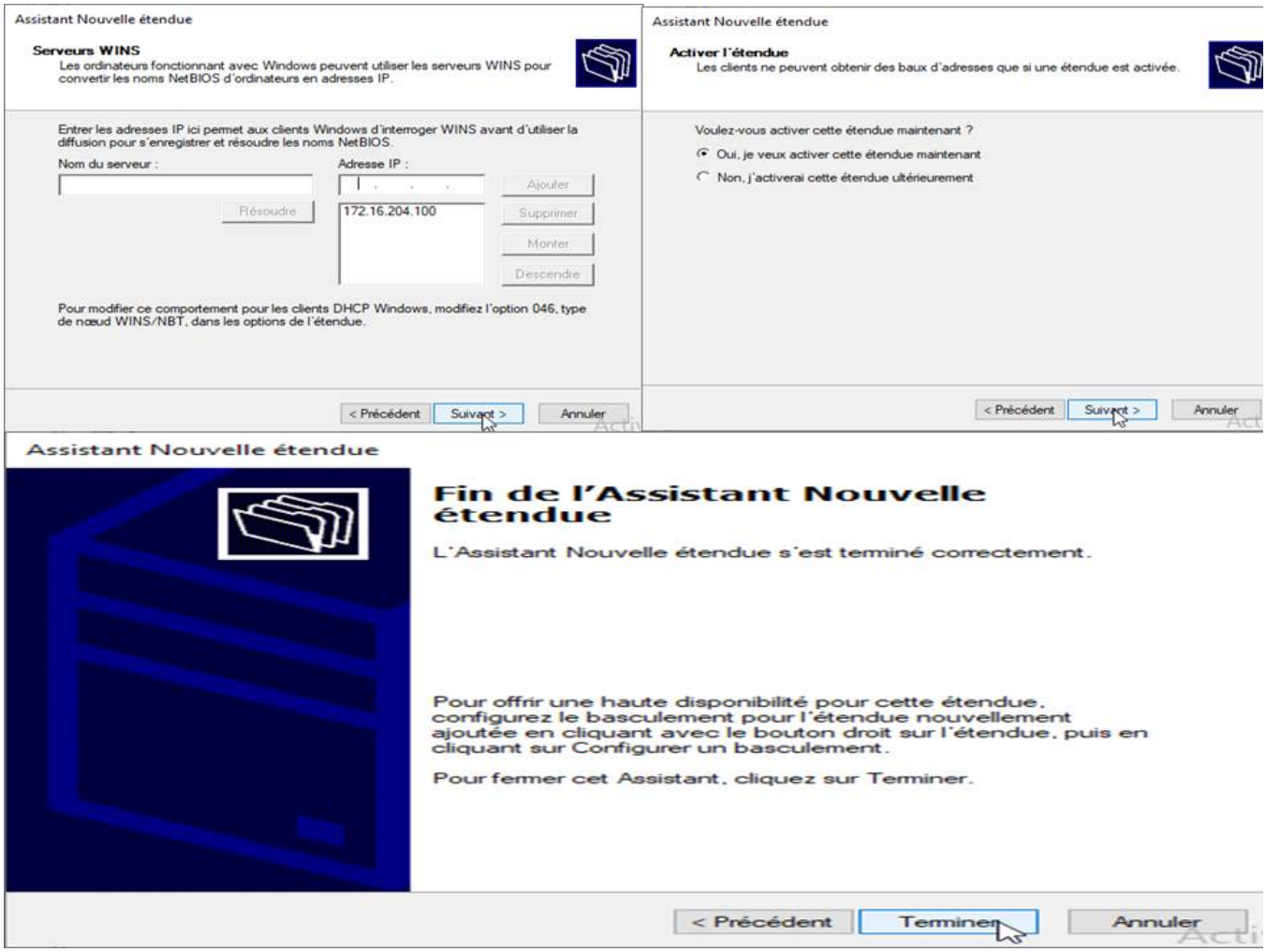

FIGURE 4.29 – Création de l'étendue des VLANs au niveau du Windows Server 2022.

la figure ci-dessous montre tous les étendues qu'on a créé :

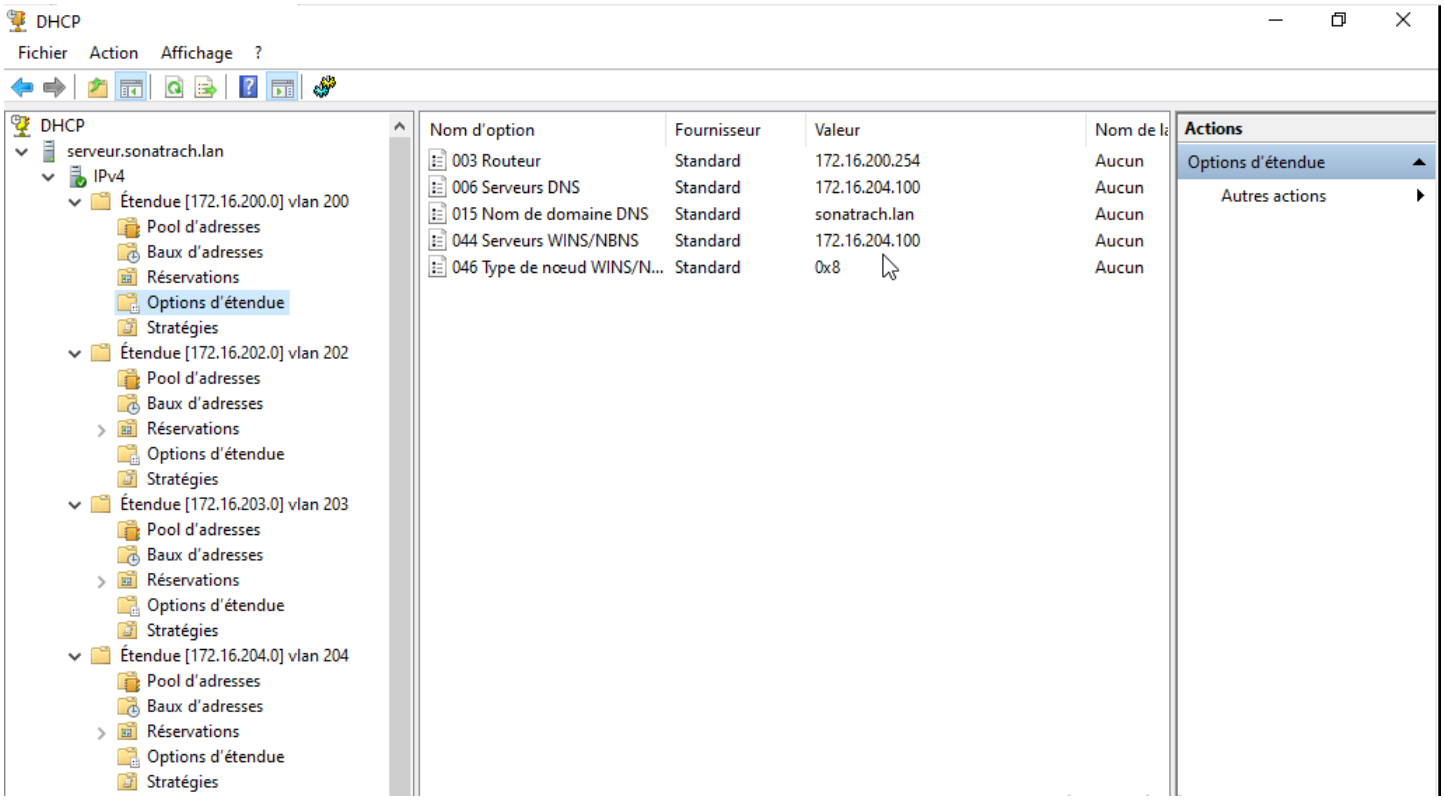

FIGURE 4.30 – Vérification des étendues crées au niveau du Windows Server 2022.

Configuration des interfaces Access

L'affectation des ports en mode Access aux VLANs crées se réalisera au niveau de tous les commutateurs d'accès du réseau RTC.

```
SWA1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA1(config)#interface e0/2
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport access vlan 200
SWA1(config-if)#exit
SWA1(config)#interface e0/3
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport access vlan 201
SWA1(config-if)#exit
SWA1(config)#interface e1/0
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport access vlan 202
SWA1(config-if)#exit
SWA1(config)#interface e1/1
SWA1(config-if)#switchport mode access
SWA1(config-if)#switchport access vlan 203
SWA1(config-if)#exit
```

FIGURE 4.31 – Configuration des ports Access au niveau du switch d'accès "SWA1".

Configuration d'EtherChannel

On a configuré l'etherchannel en ajoutant toutes les interfaces qui doit composer notre lien logique dans le même channel-group, on a créé un lien logique les deux switchs distributions du réseau LAN de RTC et on a configuré etherchannel en mode on.

— Sur le switch distribution SWD1

```
SWD1-RTC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1-RTC(config)#interface range e2/0-1, e1/3, e0/1
SWD1-RTC(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
```

FIGURE 4.32 – Configuration d'EtherChannel sur le switch distribution "SWD1-RTC".

— Sur le switch distribution SWD2

```
SWD2-RTC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD2-RTC(config)#interface range e2/0-1, e1/3, e0/1
SWD2-RTC(config-if-range)#channel-group 1 mode on
Creating a port-channel interface Port-channel 1
```

FIGURE 4.33 – Configuration d'EtherChannel sur le switch distribution "SWD2-RTC".

Configurations des routeurs

Routage inter-VLANs :

La configuration consiste à la subdivision de l'interface reliant le switch coeur et le switch distribution en un ensemble de sous-interfaces suivant le nombre des VLANs existants. Pour chaque sous-interface on l'as encapsulé avec le protocole 802.1Q en précisant l'id du VLAN, ensuite en lui attribue une adresse IP et un masque de sous-réseau.

— Sur les routeurs CORE1 et CORE2

```
CORE1-RTC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE1-RTC(config)#interface e0/0.200
CORE1-RTC(config-subif)#encapsulation dot1q 200
CORE1-RTC(config-subif)#ip address 172.16.200.1 255.255.255.0
CORE1-RTC(config-subif)#no shutdown
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.201
CORE1-RTC(config-subif)#encapsulation dot1q 201
CORE1-RTC(config-subif)#ip address 172.16.201.1 255.255.255.0
CORE1-RTC(config-subif)#no shutdown
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.202
CORE1-RTC(config-subif)#encapsulation dot1q 202
CORE1-RTC(config-subif)#ip address 172.16.202.1 255.255.255.0
CORE1-RTC(config-subif)#no shutdown
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.203
CORE1-RTC(config-subif)#encapsulation dot1q 203
CORE1-RTC(config-subif)#ip address 172.16.203.1 255.255.255.0
CORE1-RTC(config-subif)#no shutdown
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.204
CORE1-RTC(config-subif)#encapsulation dot1q 204
CORE1-RTC(config-subif)#ip address 172.16.204.1 255.255.255.0
CORE1-RTC(config-subif)#no shutdown
CORE1-RTC(config-subif)#exit
```

```
CORE2-RTC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE2-RTC(config)#interface e0/0.200
CORE2-RTC(config-subif)#encapsulation dot1q 200
CORE2-RTC(config-subif)#ip address 172.16.200.2 255.255.255.0
CORE2-RTC(config-subif)#no shutdown
CORE2-RTC(config-subif)#exit
CORE2-RTC(config)#interface e0/0.201
CORE2-RTC(config-subif)#encapsulation dot1q 201
CORE2-RTC(config-subif)#ip address 172.16.201.2 255.255.255.0
CORE2-RTC(config-subif)#no shutdown
CORE2-RTC(config-subif)#exit
CORE2-RTC(config)#interface e0/0.202
CORE2-RTC(config-subif)#encapsulation dot1q 202
CORE2-RTC(config-subif)#ip address 172.16.202.2 255.255.255.0
CORE2-RTC(config-subif)#no shutdown
CORE2-RTC(config-subif)#exit
CORE2-RTC(config)#interface e0/0.203
CORE2-RTC(config-subif)#encapsulation dot1q 203
CORE2-RTC(config-subif)#ip address 172.16.203.2 255.255.255.0
CORE2-RTC(config-subif)#no shutdown
CORE2-RTC(config-subif)#exit
CORE2-RTC(config)#interface e0/0.204
CORE2-RTC(config-subif)#encapsulation dot1q 204
CORE2-RTC(config-subif)#ip address 172.16.204.2 255.255.255.0
CORE2-RTC(config-subif)#no shutdown
CORE2-RTC(config-subif)#exit
```

FIGURE 4.34 – Configuration des sub-interfaces au niveau du routeur "CORE1-RTC" et le routeur "CORE2-RTC".

Configuration du DHCP relay :

On a configuré un DHCP relay avec l'adresse du notre serveur DHCP pour s'assurer que seul le serveur DHCP qui est sur le VLAN 204, qui va attribuer les adresses IP aux PCs. Cette configuration sera réalisé au niveau des deux routeurs du réseau.

```
CORE1-RTC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE1-RTC(config)#interface e0/0.200
CORE1-RTC(config-subif)#ip helper-address 172.16.204.100
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.201
CORE1-RTC(config-subif)#ip helper-address 172.16.204.100
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.202
CORE1-RTC(config-subif)#ip helper-address 172.16.204.100
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.203
CORE1-RTC(config-subif)#ip helper-address 172.16.204.100
CORE1-RTC(config-subif)#exit
```

FIGURE 4.35 – Configuration du DHCP relay au niveau du routeur "CORE2-RTC".

Configuration du HSRP :

Pour la mise en place du HSRP, on a défini une adresse IP qui sera l'IP du routeur virtuel sur chaque routeur, une priorité et un mode Actif sur le router 1 et un mode standby sur le routeur 2 de secours. Le routeur actif assure le rôle de passerelle par défaut pour le sous-réseau. S'il vient à tomber en panne, le routeur standby prendra le relai.

— Sur le routeur CORE1 et le routeur CORE2.

```
CORE1-RTC#conf t
Enter configuration commands, one per line.  End with
CORE1-RTC(config)#interface e0/0.200
CORE1-RTC(config-subif)#standby version 2
CORE1-RTC(config-subif)#standby 200 priority 110
CORE1-RTC(config-subif)#standby 200 ip 172.16.200.254
CORE1-RTC(config-subif)#standby 200 preempt
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.201
CORE1-RTC(config-subif)#standby version 2
CORE1-RTC(config-subif)#standby 201 priority 110
CORE1-RTC(config-subif)#standby 201 ip 172.16.201.254
CORE1-RTC(config-subif)#standby 201 preempt
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.202
CORE1-RTC(config-subif)#standby version 2
CORE1-RTC(config-subif)#standby 202 priority 110
CORE1-RTC(config-subif)#standby 202 ip 172.16.202.254
CORE1-RTC(config-subif)#standby 202 preempt
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.203
CORE1-RTC(config-subif)#standby version 2
CORE1-RTC(config-subif)#standby 203 priority 110
CORE1-RTC(config-subif)#standby 203 ip 172.16.203.254
CORE1-RTC(config-subif)#standby 203 preempt
CORE1-RTC(config-subif)#exit
CORE1-RTC(config)#interface e0/0.204
CORE1-RTC(config-subif)#standby version 2
CORE1-RTC(config-subif)#standby 204 priority 110
CORE1-RTC(config-subif)#standby 204 ip 172.16.204.254
CORE1-RTC(config-subif)#standby 204 preempt
CORE1-RTC(config-subif)#exit
```

```
CORE2-RTC#conf t
Enter configuration commands, one per line.  End with CN
CORE2-RTC(config)#interface e0/0.200
CORE2-RTC(config-subif)#standby version 2
CORE2-RTC(config-subif)#standby 200 ip 172.16.200.254
CORE2-RTC(config-subif)#exit
CORE2-RTC(config)#interface e0/0.201
CORE2-RTC(config-subif)#standby version 2
CORE2-RTC(config-subif)#standby 201 ip 172.16.201.254
CORE2-RTC(config-subif)#exit
CORE2-RTC(config)#interface e0/0.202
CORE2-RTC(config-subif)#standby version 2
CORE2-RTC(config-subif)#standby 202 ip 172.16.202.254
CORE2-RTC(config-subif)#exit
CORE2-RTC(config)#interface e0/0.203
CORE2-RTC(config-subif)#standby version 2
CORE2-RTC(config-subif)#standby 203 ip 172.16.203.254
CORE2-RTC(config-subif)#exit
CORE2-RTC(config)#interface e0/0.204
CORE2-RTC(config-subif)#standby version 2
CORE2-RTC(config-subif)#standby 204 ip 172.16.204.254
CORE2-RTC(config-subif)#exit
```

FIGURE 4.36 – Configuration du HSRP au niveau du routeur "CORE1-RTC" et "CORE2-RTC".

Configuration des interfaces du routeur

— Sur le routeur R1 (CORE1)

```
CORE1-RTC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE1-RTC(config)#interface e0/1
CORE1-RTC(config-if)#ip address 192.168.10.6 255.255.255.252
CORE1-RTC(config-if)#no shutdown
CORE1-RTC(config-if)#exit
```

FIGURE 4.37 – Configuration des interfaces du routeur "CORE1-RTC".

```
CORE1-RTC(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.5
CORE1-RTC(config)#exit
```

FIGURE 4.38 – Configuration de la route statique sur routeur "CORE1-RTC".

— Sur le routeur R2 (CORE2)

```
CORE2-RTC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CORE2-RTC(config)#interface e0/1
CORE2-RTC(config-if)#ip address 192.168.10.2 255.255.255.252
CORE2-RTC(config-if)#no shutdown
CORE2-RTC(config-if)#exit
```

FIGURE 4.39 – Configuration de l'interface du routeur "CORE2-RTC".

```
CORE2-RTC(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.1
CORE2-RTC(config)#exit
```

FIGURE 4.40 – Configuration de la route statique sur routeur "CORE2-RTC".

4.6.4 Configuration du pare-feu FortiGate

D'abord on configure les interfaces du pare-feu FortiGate au niveau de la console.

```
FW-BEJAIA # config system interface

FW-BEJAIA (interface) # edit port1

FW-BEJAIA (port1) # set mode static

FW-BEJAIA (port1) # set ip 80.80.80.81 255.255.255.252

FW-BEJAIA (port1) # set allowaccess ping http https

FW-BEJAIA (port1) # next

FW-BEJAIA (interface) # edit port3

FW-BEJAIA (port3) # set mode static

FW-BEJAIA (port3) # set ip 192.168.10.5 255.255.255.252

FW-BEJAIA (port3) # set allowaccess ping http https

FW-BEJAIA (port3) # next

FW-BEJAIA (interface) # edit port4

FW-BEJAIA (port4) # set mode static

FW-BEJAIA (port4) # set ip 192.168.10.1 255.255.255.252

FW-BEJAIA (port4) # set allowaccess ping http https

FW-BEJAIA (port4) # end
```

FIGURE 4.41 – Configuration des interfaces du pare-feu FortiGate.

La prochaine étape consistera à configurer le pare-feu FortiGate que nous avons déjà installé ou la configuration de la page d'authentification est nécessaire :
Tout d'abord il faut se rendre dans le site du pare-feu ou une configuration de la page d'authentification est nécessaire au début et ceux en y insérant quelques information sur l'entreprise suivi du mot de passe avec lequel accédera l'administrateur à FortiGate.

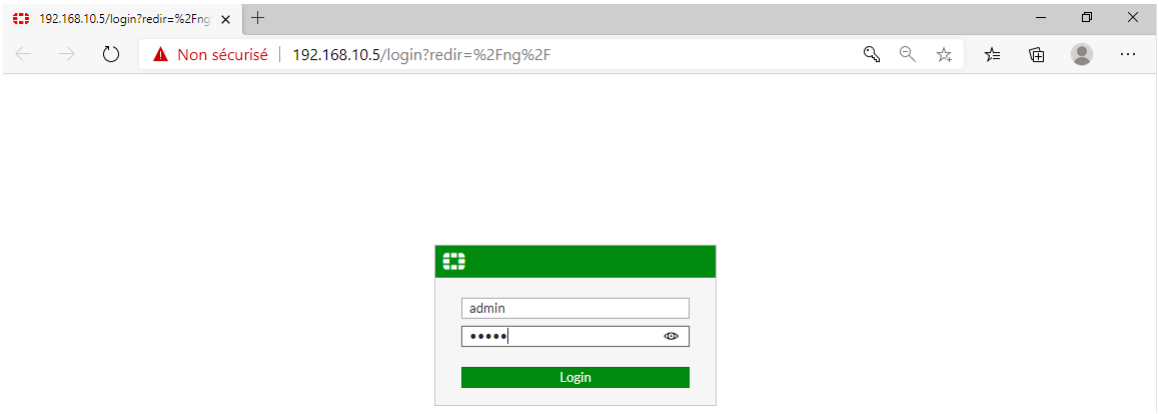

FIGURE 4.42 – L'interface d'authentification du pare-feu FortiGate.

Après avoir introduit le mot de passe et le nom d'utilisateur (s'authentifier) l'interface d'accueil s'affichera comme suit :

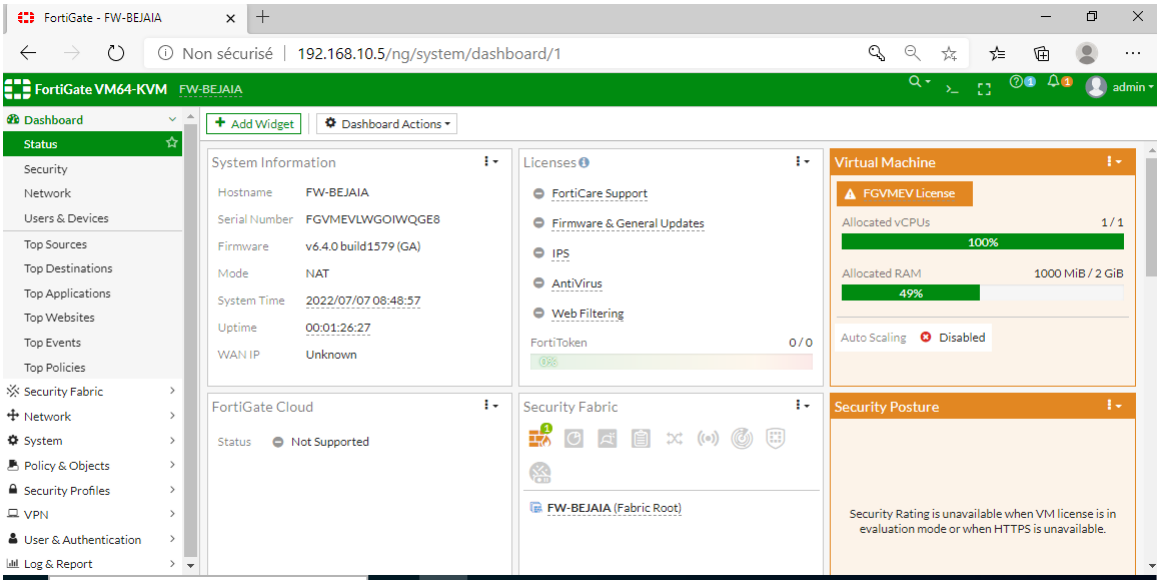

FIGURE 4.43 – L'interface d'accueil du pare-feu FortiGate.

4.6.5 Configuration du routeur R-FAI

On configure les interfaces du routeur en lui attribuent des adresses IP et des masques de sous-réseaux.

```
R-FAI#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-FAI(config)#interface e0/0
R-FAI(config-if)#ip address 80.80.80.82 255.255.255.252
R-FAI(config-if)#no shutdown
R-FAI(config-if)#exit
R-FAI(config)#interface
*Jul  1 18:10:22.766: %LINK-3-UPDOWN: Interface Ethernet0/0, c
*Jul  1 18:10:23.772: %LINEPROTO-5-UPDOWN: Line protocol on In
 to up
R-FAI(config)#interface e0/1
R-FAI(config-if)#ip address 100.100.100.102 255.255.255.252
R-FAI(config-if)#no shutdown
R-FAI(config-if)#exit
```

FIGURE 4.44 – Configuration des interfaces du routeur R-FAI.

4.7 Configuration du VPN site à site

Dans ce qui suit nous allons montrer la création du tunnel VPN IPSec entre le le site de Sonatrach RTC Béjaia et le site de Béni-Mansour.

4.7.1 Création du tunnel VPN au niveau du pare-feu FortiGate

Assistant de configuration VPN :

Pour créer le VPN sur le site de béjaia, il faut d'abord aller au VPN > IPSec Wizard > Create New IPSec tunnel. Puis on définit l'adresse de l'interface WAN ainsi que la clé partagée sur le tunnel entre les deux sites et sélectionner les réseaux distants et les réseaux locaux LAN.

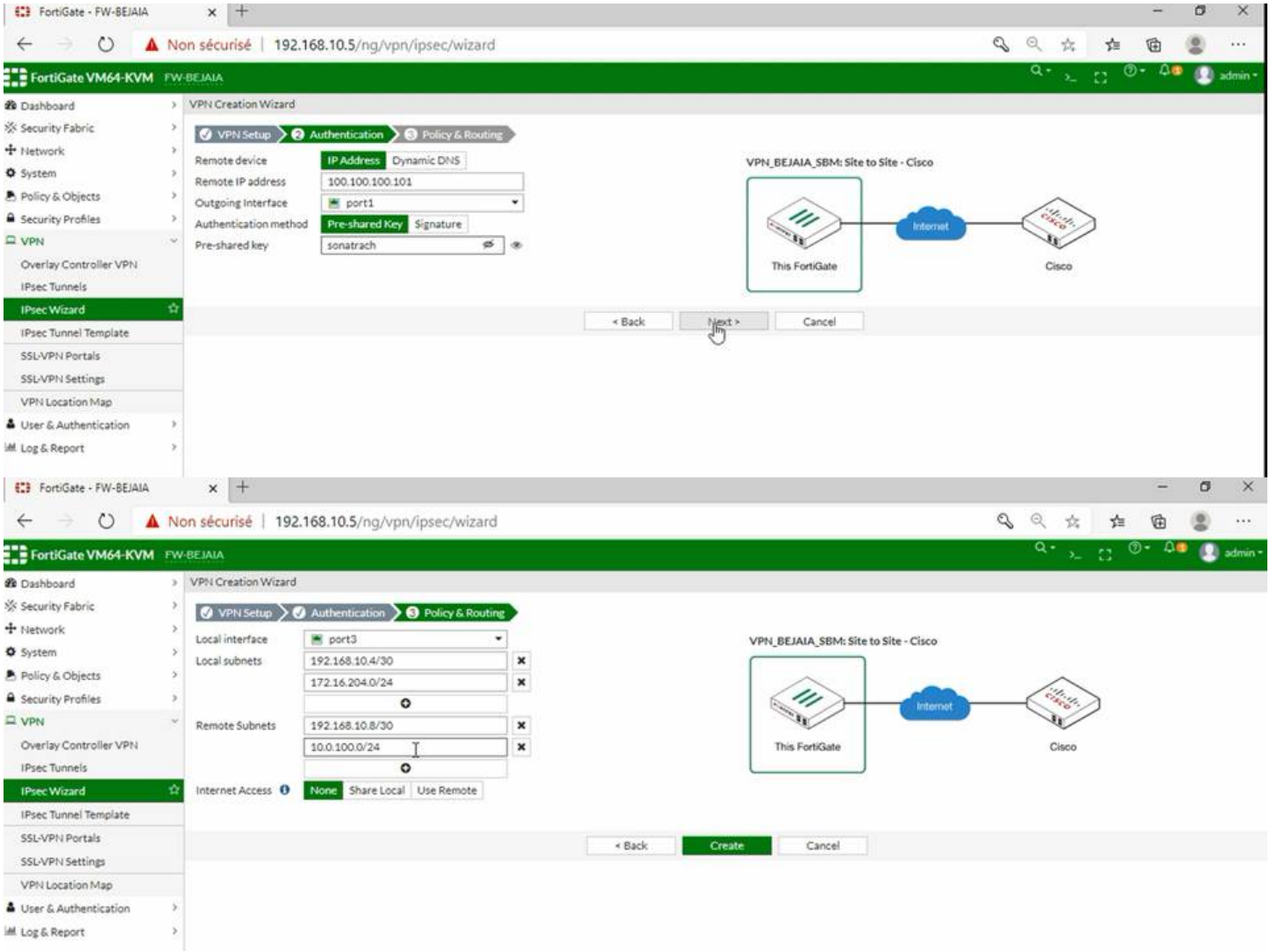

FIGURE 4.45 – La création du tunnel VPN au niveau du pare-feu FortiGate.

Par la suite on modifie les protocoles de cryptage de la clé partagée nécessaires pour le tunnel VPN.

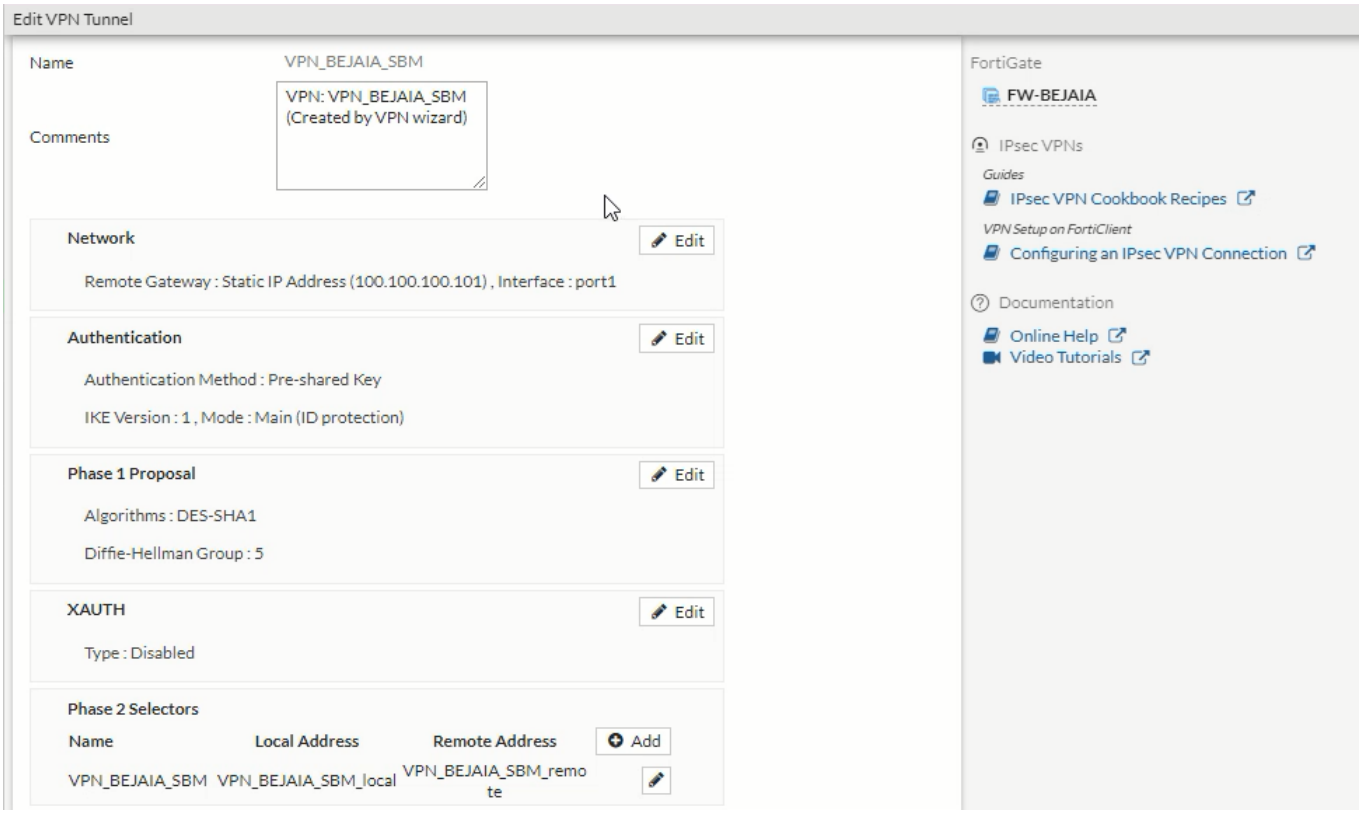

FIGURE 4.46 – La modification des protocoles de cryptage du tunnel VPN au niveau du pare-feu FortiGate.

Configuration du routage statique

On veut router le VLAN 204 qui est le management ou il y a le serveur, donc on a choisit le routage par interface pour acheminées les paquets vers le réseau distant.

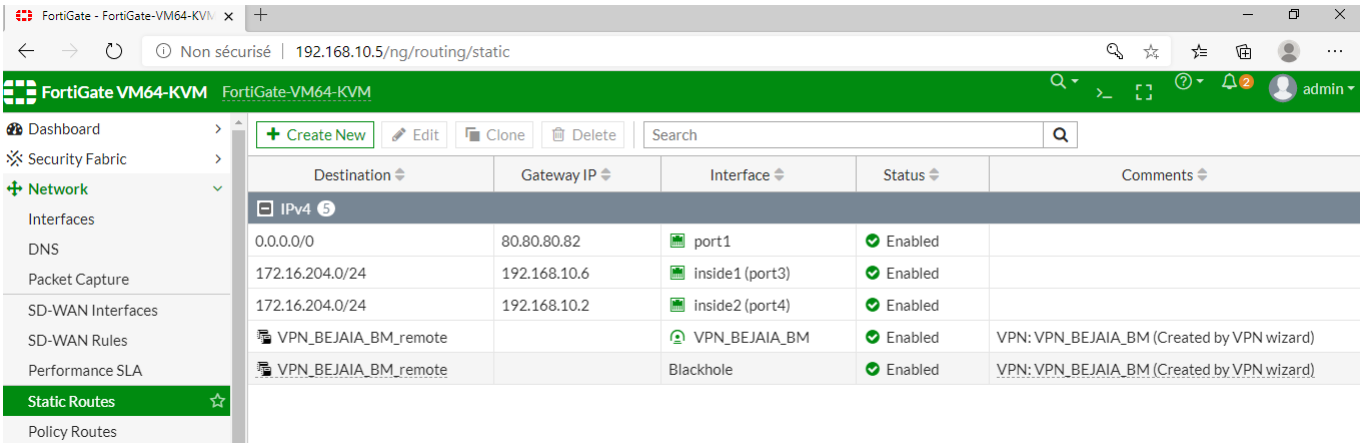

FIGURE 4.47 – Le routage statique au niveau du pare-feu FortiGate.

Vérification de la création du tunnel VPN

Pour vérifier que le tunnel VPN a été bien créé sur le pare-feu FortiGate, on va aller sur VPN > IPSec tunnel. le nom associé au tunnel doit être affiché.

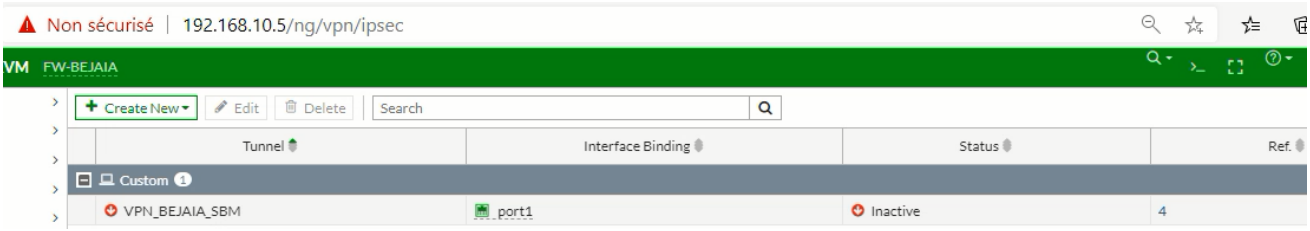

FIGURE 4.48 – Le tunnel VPN du pare-feu FortiGate.

4.7.2 Au niveau du pare-feu ASA.

Pour créer un tunnel VPN site-à-site sur le pare-feu ASA, on doit aller à Wizards > Site-to-Site Wizard.

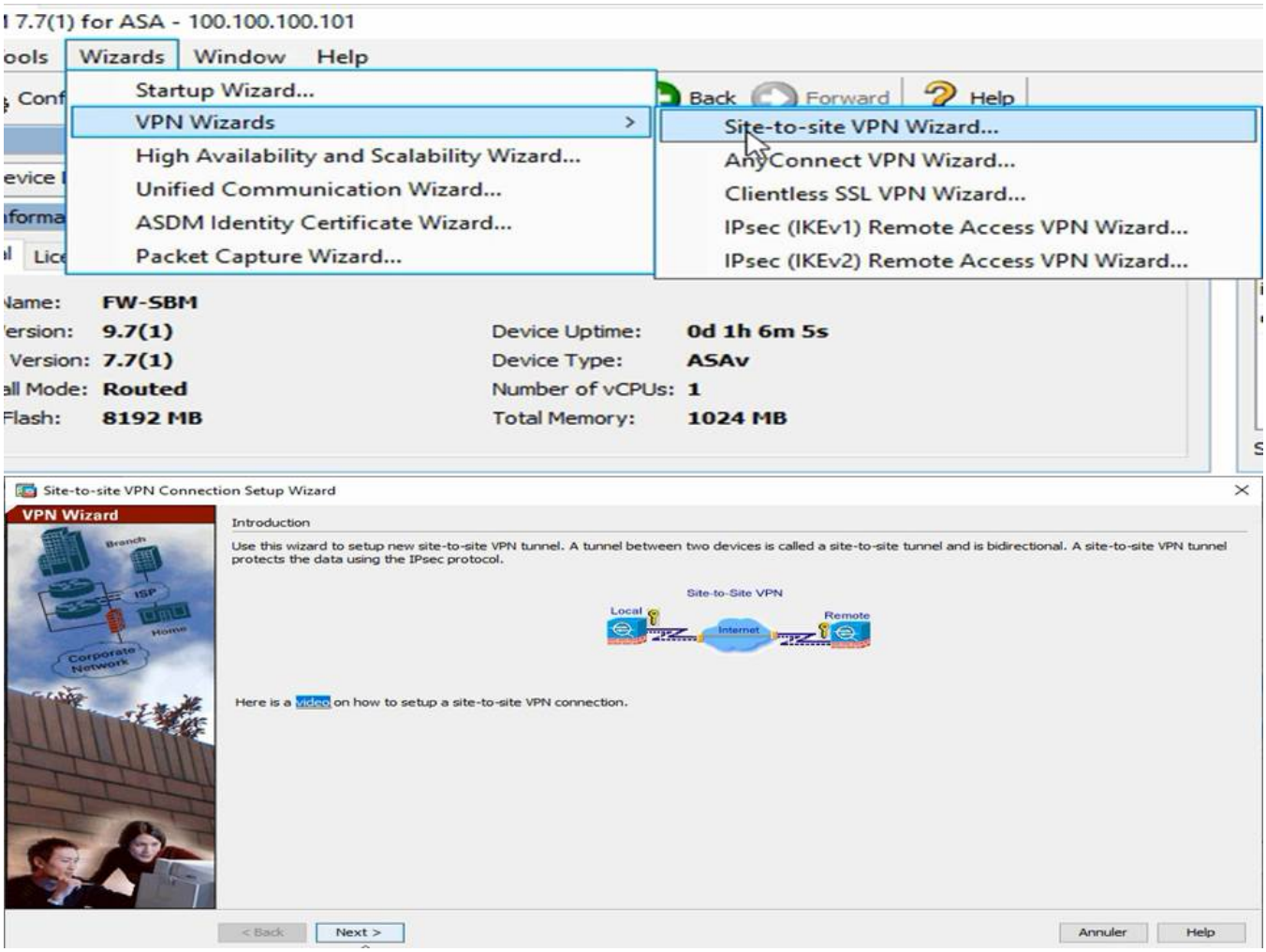

FIGURE 4.49 – La création du tunnel VPN au niveau du pare-feu ASA.

Puis on clique sur NEXT, une autre interface s'affiche pour saisir l'adresse de la passerelle distante, après un autre NEXT, une interface apparaîtra permettant de sélectionner les réseaux locaux qui sont le réseau de l'interface "inside" du pare-feu ASA. On autorise le VLAN 100 de sortir,puis on sélectionne le réseau distant qu'on veut atteindre qui est l'interface "port3" du pare-feu FortiGate et enfin on autorise le VLAN 204.

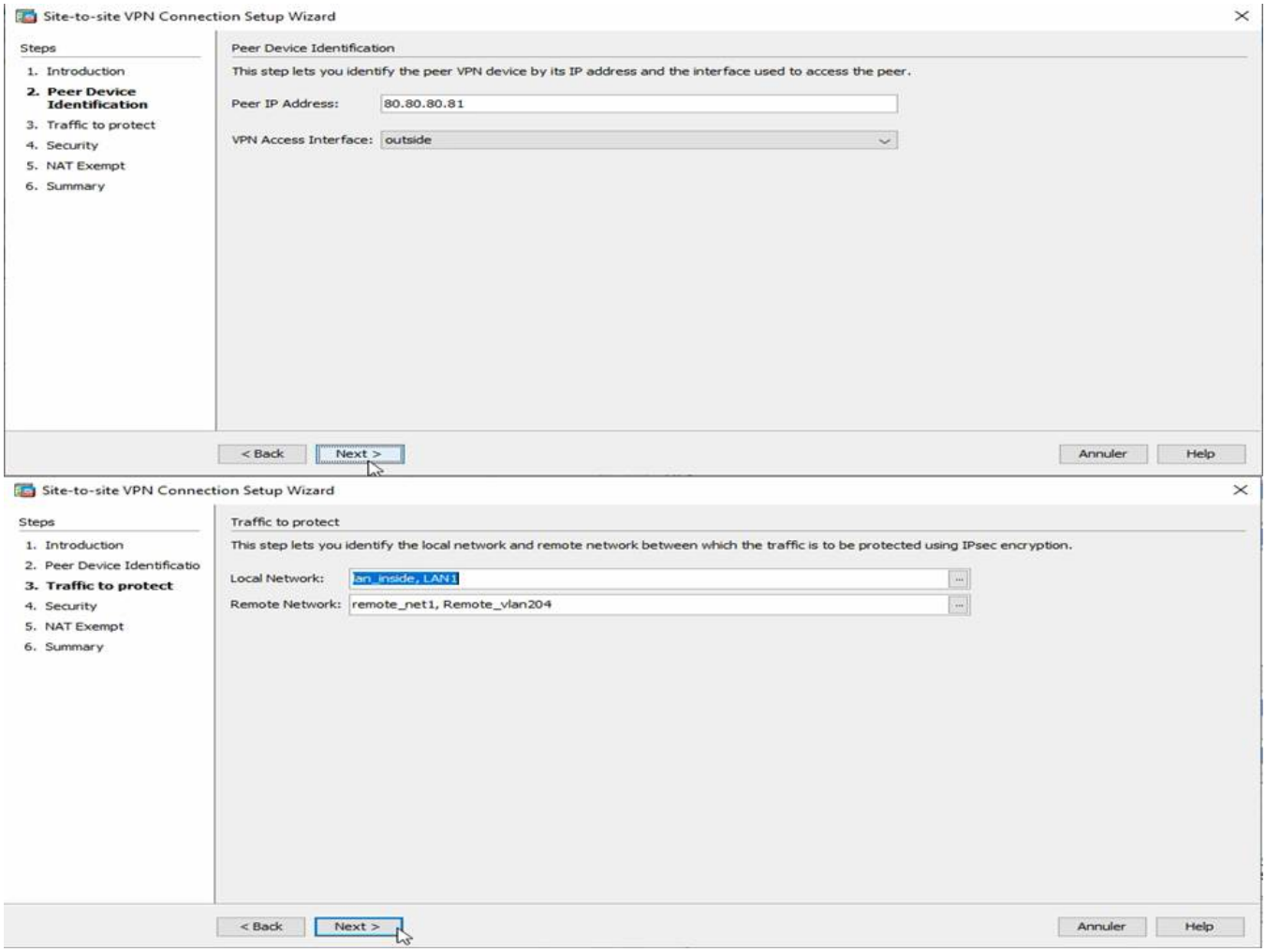

FIGURE 4.50 – La configuration des adresses du tunnel VPN au niveau du pare-feu ASA.

Par la suite on doit configuré la clé partagée, ainsi que les différents paramètres et protocoles de cryptage nécessaires pour le tunnel VPN et qui doivent être identiques à celles configuré au niveau du pare-feu de Béjaia.

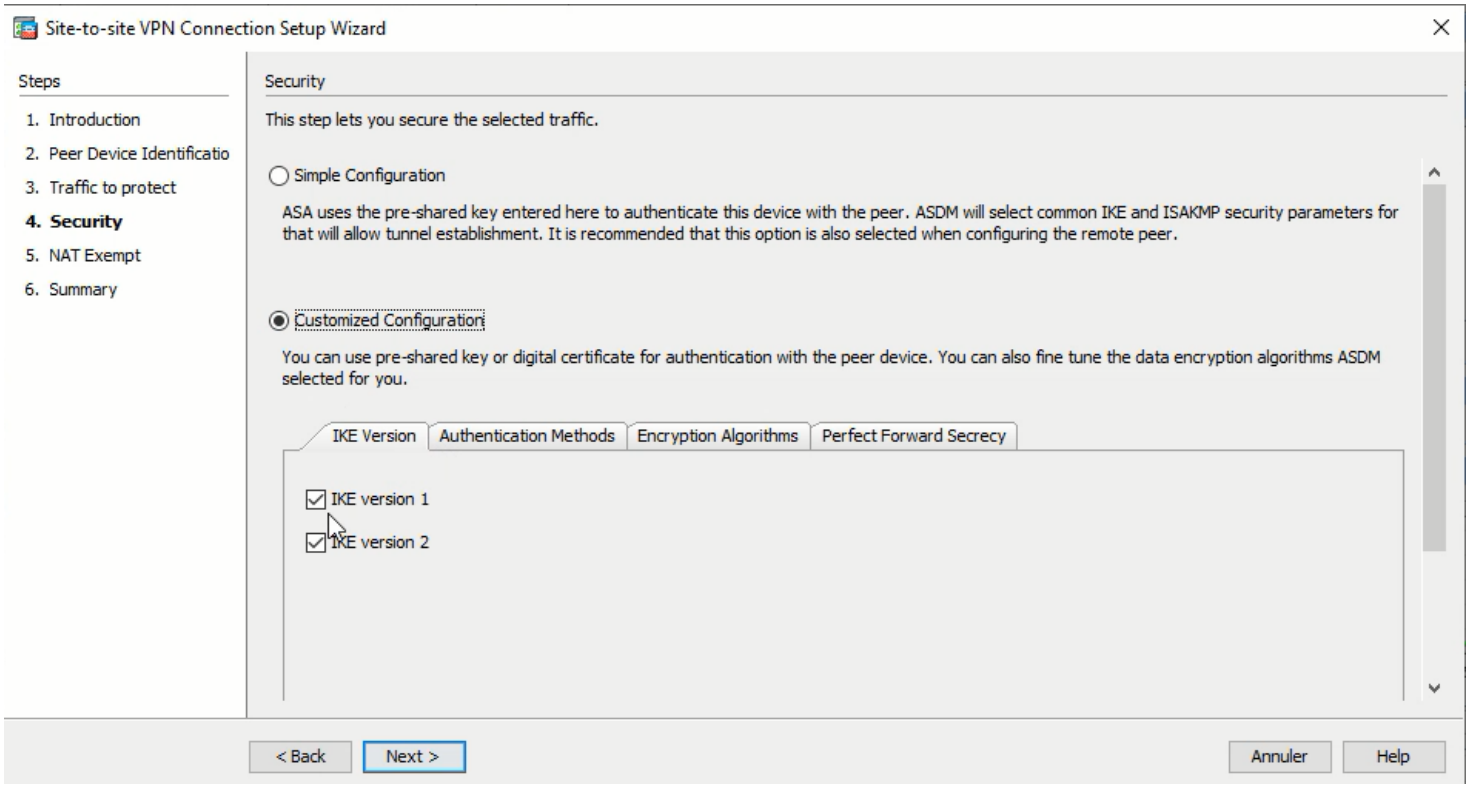

FIGURE 4.51 – La configuration des paramétres de cryptage du tunnel VPN au niveau du pare-feu ASA.

Vérification de la création du tunnel VPN

Afin de vérifier que le tunnel VPN à été crée au niveau du pare-feu ASA de la station Béni-Mansour, on sélectionne Configuration > Site-to-Site VPN > Connection Profiles. Ce que montre l'image suivante :

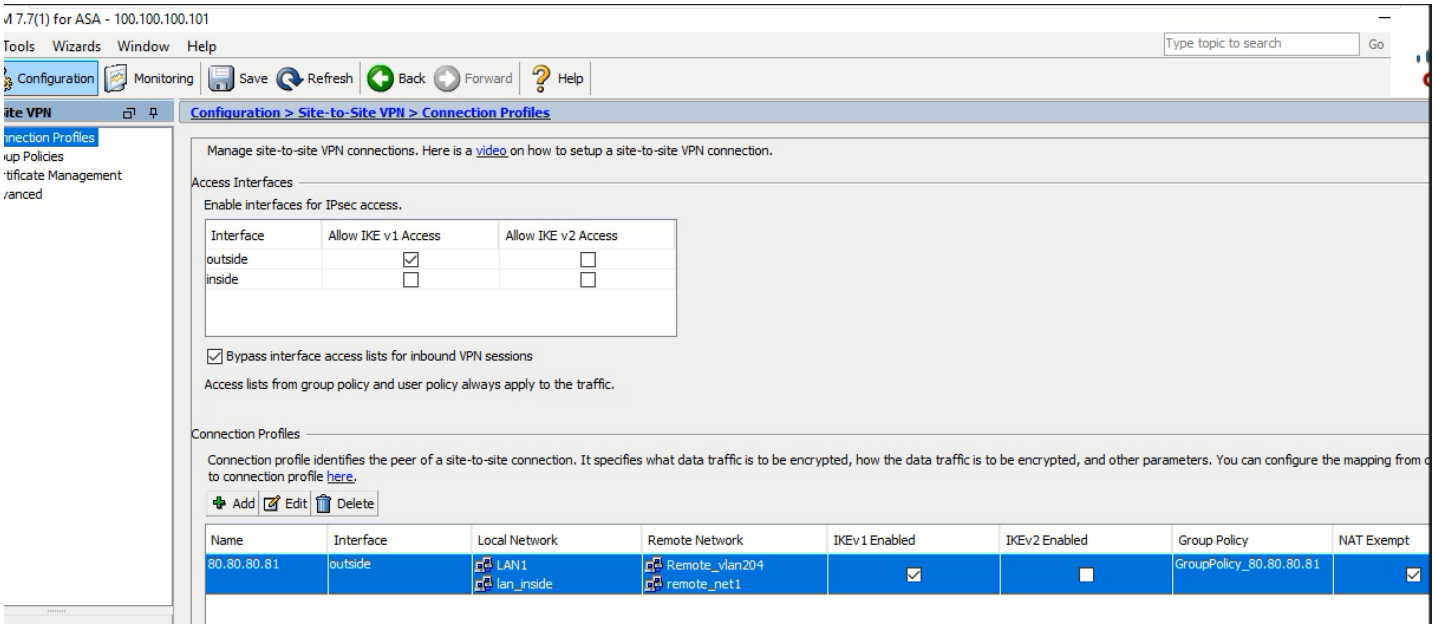

FIGURE 4.52 – La vérification de la création du tunnel VPN au niveau du pare-feu ASA.

4.7.3 Création des utilisateurs sur l'active directory

On a créé des comptes pour les utilisateurs, ainsi que des groupes et des ordinateurs pour les utilisateurs déjà crée sur les deux sites comme le montre la figure suivante :

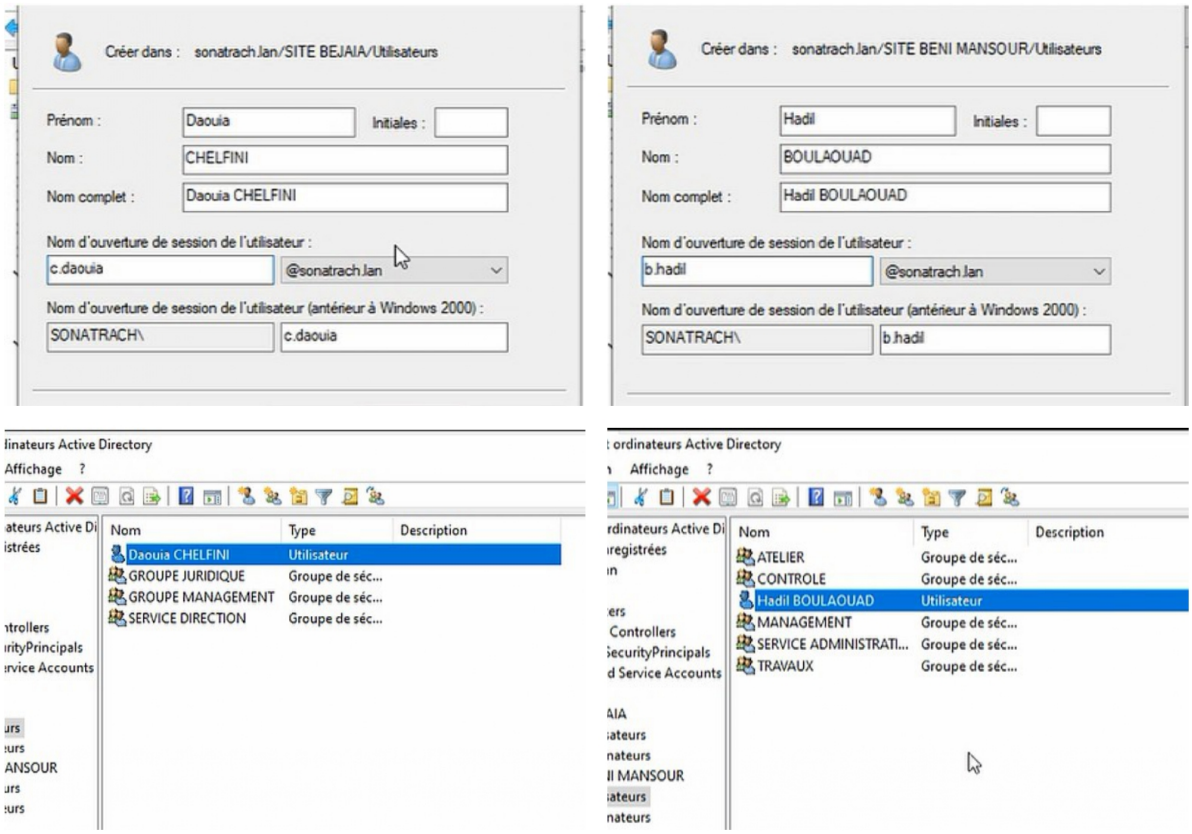

FIGURE 4.53 – La création des utilisateurs sur active directory.

Après avoir créer les groupes et les utilisateurs, on passe au GPO qui définissent les droits des utilisateurs, des stratégies de groupes qui sont applicables aux sites, domaines et UO. la figure suivante montre sa création :

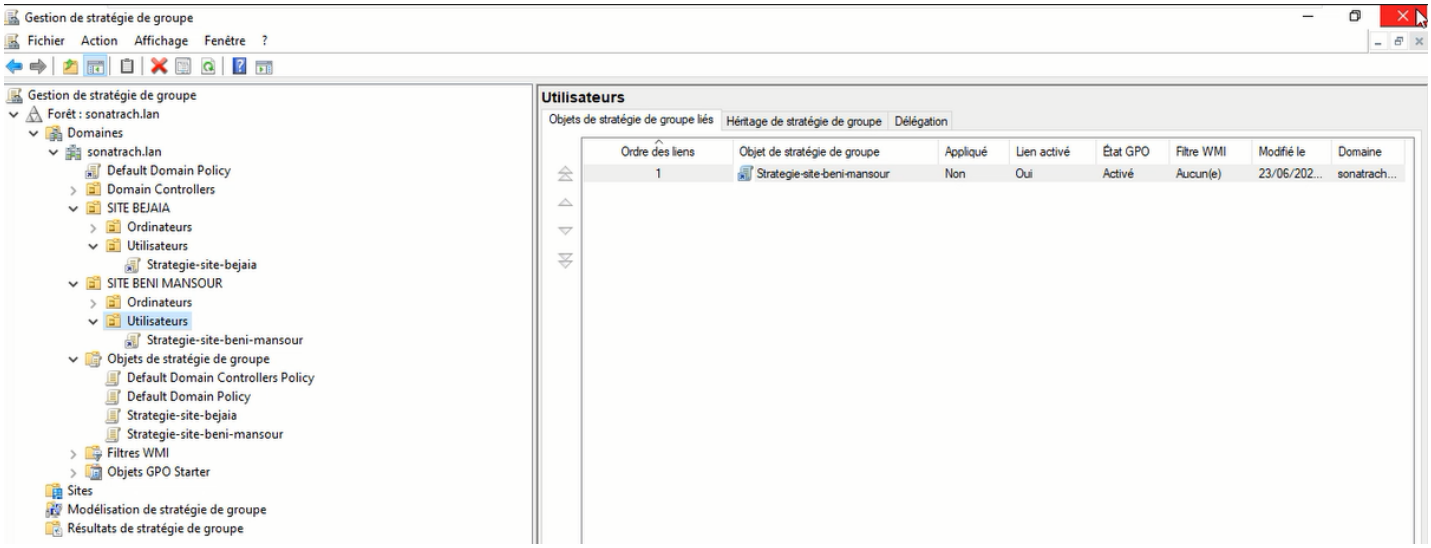

FIGURE 4.54 – La création des stratégies de groupe.

4.7.4 Configuration de l'accès à distance au serveur

Sur la machine cliente Windows 7 qui se situe dans le réseau du site de Béni-Mansour, on peut accéder au serveur située au niveau du réseau de la Sonatrach Béjaia.

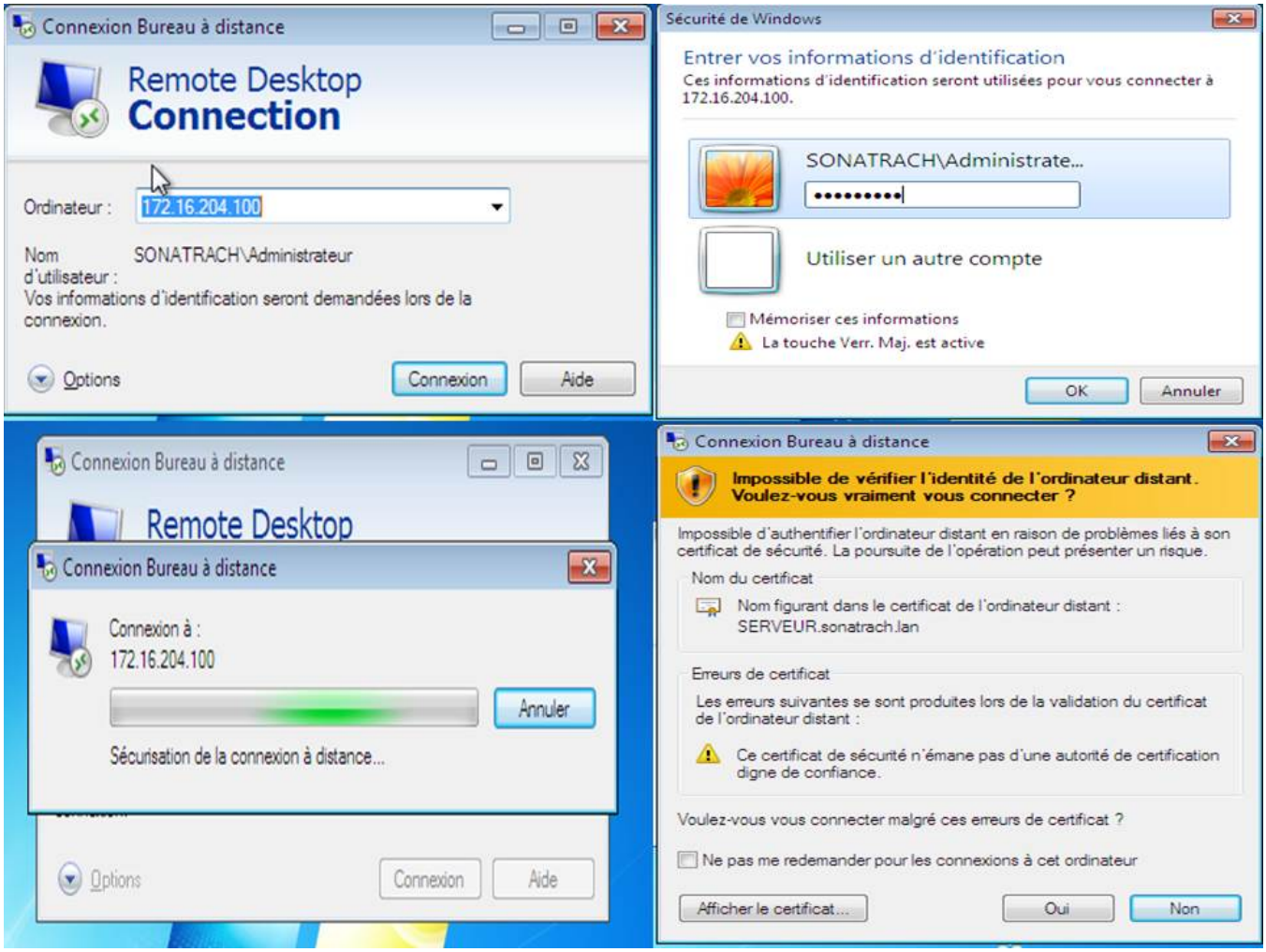

FIGURE 4.55 – La connexion à distance au serveur du béjaia.

4.7.5 Accès à distance au pare-feu FortiGate

Après avoir accéder au serveur de Sonatrach Béjaia, on peut également accéder à l'interface du pare-feu FortiGate.

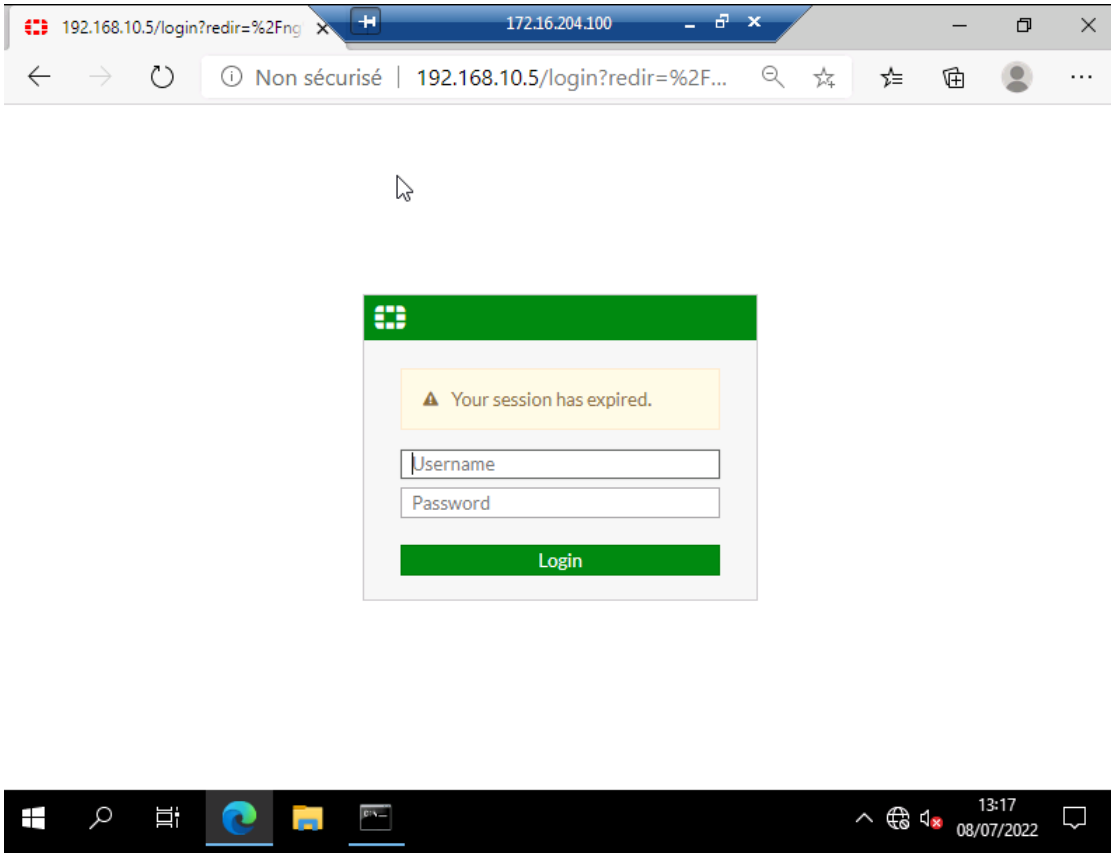

FIGURE 4.56 – L'accès à distance au pare-feu FortiGate.

4.7.6 Accès à distance au pare-feu ASA

On peut ainsi accéder à l'interface du pare-feu ASA, après avoir saisie le username et le mot de passe.

FIGURE 4.57 – L'accès à distance au pare-feu ASA.

4.8 Tests et Vérifications

Dans cette partie, l'ensemble des tests consiste à vérifier la validation des configurations en utilisant les commandes "Show" qui affiche selon la commande utilisé les différents configurations effectuées sur les équipements, et un autre phase qui consiste à vérifier l'accessibilité et la communication entre les utilisateurs en utilisant la commande "Ping" qui teste la réponse d'un équipement sur le réseau.

4.8.1 Vérification des configurations

Vérification de la configuration du protocole VTP

On vérifie l'activation du protocole VTP sur les switchs de la couche distribution et accès avec la commande "Show vtp status" sur la console des équipements.

— Sur le switch distribution "SWD1-SBM" en mode serveur et sur le switch d'accès "Administration" en mode client.

```
SWD1-SBM#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : sbm
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0600
Configuration last modified by 0.0.0.0 at 6-27-22 11:02:33
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 9
Configuration Revision            : 6
MD5 digest                        : 0x4E 0xA5 0x1C 0xDA 0x53 0xEC 0xD4 0x51
                                    0x30 0x1A 0xBA 0xBB 0xB0 0x91 0x5C 0xAF
Administration#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : sbm
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0900
Configuration last modified by 0.0.0.0 at 6-27-22 11:02:33

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 9
Configuration Revision            : 6
MD5 digest                        : 0x4E 0xA5 0x1C 0xDA 0x53 0xEC 0xD4 0x51
                                    0x30 0x1A 0xBA 0xBB 0xB0 0x91 0x5C 0xAF
```

FIGURE 4.58 – Vérification du protocole VTP en mode serveur et client respectivement sur "SWD1-SBM" et "Administration".

Vérification de la création des VLANs

Pour vérifier que les VLANs sont bien crées, on lance la commande "show vlan brief" sur les commutateurs du la couche distribution et accès.

— Sur le switch distribution "SWD1-SBM" et le switch d'accès "Administration"

```
SWD1-SBM#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/1, Et1/2, Et1/3, Et2/0
                                                Et2/1, Et2/2, Et2/3, Et3/0
                                                Et3/1, Et3/2, Et3/3
100  Administration                   active
101  Controle                         active
102  Atelier                          active
103  Travaux                          active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
Administration#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/3, Et1/0, Et1/1, Et1/2
                                                Et1/3, Et2/0, Et2/1, Et2/2
                                                Et2/3, Et3/0, Et3/1, Et3/2
                                                Et3/3
100  Administration                   active    Et0/1, Et0/2
101  Controle                         active
102  Atelier                          active
103  Travaux                          active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

FIGURE 4.59 – Vérification de la création des VLANs sur le switch distribution "SWD1-SBM" et le switch d'accès "Administration".

Vérification de la configuration des sub-interfaces du routeur

Pour savoir si les sub-interfaces possèdent des adresses IP correctes, on saisie la commande "show ip interface brief" sur la console du routeur.

```
R1-SBM#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES NVRAM  up                    up
Ethernet0/0.100            10.0.100.1      YES NVRAM  up                    up
Ethernet0/0.101            10.0.101.1      YES NVRAM  up                    up
Ethernet0/0.102            10.0.102.1      YES NVRAM  up                    up
Ethernet0/0.103            10.0.103.1      YES NVRAM  up                    up
Ethernet0/1                192.168.10.10   YES NVRAM  up                    up
Ethernet0/2                unassigned      YES NVRAM  administratively down down
Ethernet0/3                unassigned      YES NVRAM  administratively down down
Ethernet1/0                unassigned      YES NVRAM  administratively down down
Ethernet1/1                unassigned      YES NVRAM  administratively down down
Ethernet1/2                unassigned      YES NVRAM  administratively down down
 --More--
```

FIGURE 4.60 – Vérification de la configuration des sub-interfaces sur le routeur "R1-SBM".

Vérification d'EtherChannel

On vérifie la création d'Etherchannel et son fonctionnement en utilisant la commande "show etherchannel summary" sur la console des deux switchs distributions.

— Sur le switch distribution 1 et 2.

```
SWD1-RTC#show etherchannel summary
Flags:   D - down         P - bundled in port-channel
         I - stand-alone s - suspended
         H - Hot-standby (LACP only)
         R - Layer3       S - Layer2
         U - in use       N - not in use, no aggregation
         f - failed to allocate aggregator

         M - not in use, minimum links not met
         m - not in use, port not aggregated due to minimum links not met
         u - unsuitable for bundling
         w - waiting to be aggregated
         d - default port

         A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)           -        Et0/1(P)    Et1/3(P)    Et2/0(P)
                                  Et2/1(P)
SWD2-RTC#show etherchannel summary
Flags:   D - down         P - bundled in port-channel
         I - stand-alone s - suspended
         H - Hot-standby (LACP only)
         R - Layer3       S - Layer2
         U - in use       N - not in use, no aggregation
         f - failed to allocate aggregator

         M - not in use, minimum links not met
         m - not in use, port not aggregated due to minimum links not met
         u - unsuitable for bundling
         w - waiting to be aggregated
         d - default port

         A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)           -        Et0/1(P)    Et1/3(P)    Et2/0(P)
                                  Et2/1(P)
```

FIGURE 4.61 – Vérification de la configuration d'etherchannel sur le switch distribution "SWD1-RTC" et le switch distribution "SWD2-RTC".

Vérification de la configuration du HSRP

Pour vérifier l'application du protocole HSRP sur les deux routeurs avec les deux modes active et standby, on lance la commande "Show standby brief" sur la console de chacun.

— Sur le routeur 1 et le routeur 2.

```
CORE1-RTC#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/0.200   200  110 P Active  local           172.16.200.2    172.16.200.254
Et0/0.201   201  110 P Active  local           172.16.201.2    172.16.201.254
Et0/0.202   202  110 P Active  local           172.16.202.2    172.16.202.254
Et0/0.203   203  110 P Active  local           172.16.203.2    172.16.203.254
Et0/0.204   204  110 P Active  local           172.16.204.2    172.16.204.254
CORE1-RTC#
CORE2-RTC#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/0.200   200  100   Standby 172.16.200.1    local           172.16.200.254
Et0/0.201   201  100   Standby 172.16.201.1    local           172.16.201.254
Et0/0.202   202  100   Standby 172.16.202.1    local           172.16.202.254
Et0/0.203   203  100   Standby 172.16.203.1    local           172.16.203.254
Et0/0.204   204  100   Standby 172.16.204.1    local           172.16.204.254
CORE2-RTC#
```

FIGURE 4.62 – Vérification de la configuration de HSRP sur le routeur "CORE1-RTC" et le routeur "CORE2-RTC".

Vérification du protocle DHCP

On vérifie l'affectation des adresses IP aux ordinateurs du réseau par le protocole DHCP avec la commande "ip dhcp" lancé à partir des la console des PCs.

```
PC5> ip dhcp
DDORA IP 10.0.101.11/24 GW 10.0.101.1

PC5>
```

FIGURE 4.63 – Vérification d'affectation d'une adresse IP au "PC5".

4.8.2 Tests

La phase des tests consiste à effectuer des commandes "Ping" entre les équipements du réseau pour tester l'accessibilité. un utilisateur qui veut communiquer avec un autre émet avec le ping des paquets au destinataire. si ce dernier les reçoit alors le ping est réussi, sinon il a échoué.

Test intra-VLANs

On vérifie la communication entre les équipements situés en même VLAN, en effectuent un test « ping » entre le PC5 avec l'adresse IP « 10.0.101.11 » et le PC14 avec l'adresse IP «10.0.101.12 », tels que les deux se trouve dans le même VLAN 101 et commutateur d'accès « Contrôle ».

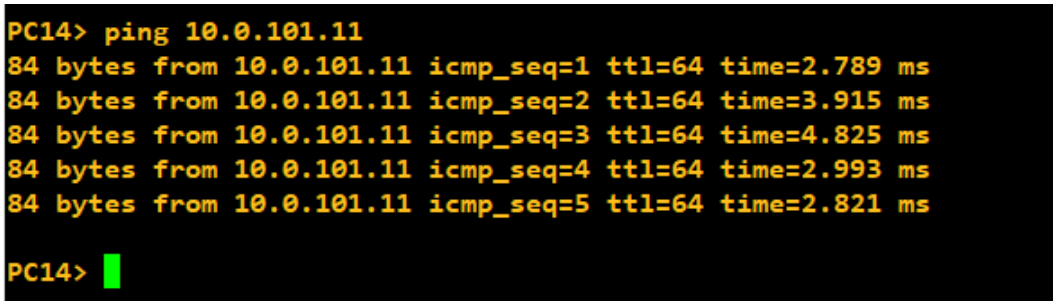

FIGURE 4.64 – Test ping intra-VLANs.

Test inter-VLANs

On vérifie la communication entre les équipements de VLANs différents, en effectuant un test « ping » entre le PC8 avec l'adresse IP «10.0.102.11 » qui se trouve dans le VLAN 102 au commutateur d'accès «Atelier» et le PC14 avec l'adresse IP «10.0.101.12 » qui se trouve dans le VLAN 101 au commutateur d'accès « Contrôle ».

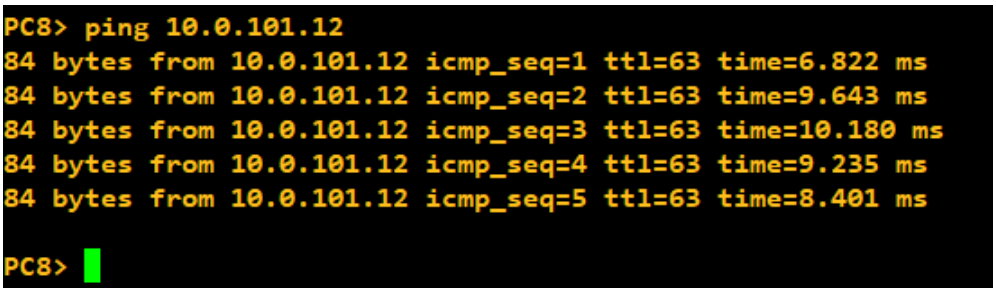

FIGURE 4.65 – Test ping inter-VLANs.

Test entre deux sites

On teste la connectivité entre le site de Béni-Mansour et celui de Sonatrach RTC Béjaia en appliquant un test ping entre les PCs de chacun d'entre eux. On effectue un ping entre le PC17 qui appartient au VLAN 100 du site Béni-Mansour vers le serveur de site de Sonatrach RTC béjaia.

```
PC17> ping 172.16.204.100
84 bytes from 172.16.204.100 icmp_seq=1 ttl=125 time=6.555 ms
84 bytes from 172.16.204.100 icmp_seq=2 ttl=125 time=16.007 ms
84 bytes from 172.16.204.100 icmp_seq=3 ttl=125 time=49.836 ms
84 bytes from 172.16.204.100 icmp_seq=4 ttl=125 time=16.793 ms
84 bytes from 172.16.204.100 icmp_seq=5 ttl=125 time=34.751 ms

PC17>
```

FIGURE 4.66 – Test ping entre les deux sites Béni-Mansour et Sonatrach Béjaia.

Capture Wireshark

On lance une capture wireshark sur le lien reliant les deux sites, la station Béni-Mansour et l'entreprise Sonatrach Béjaia et on séléctionne la trame "ISAKMP" qui correspond aux données cryptées.

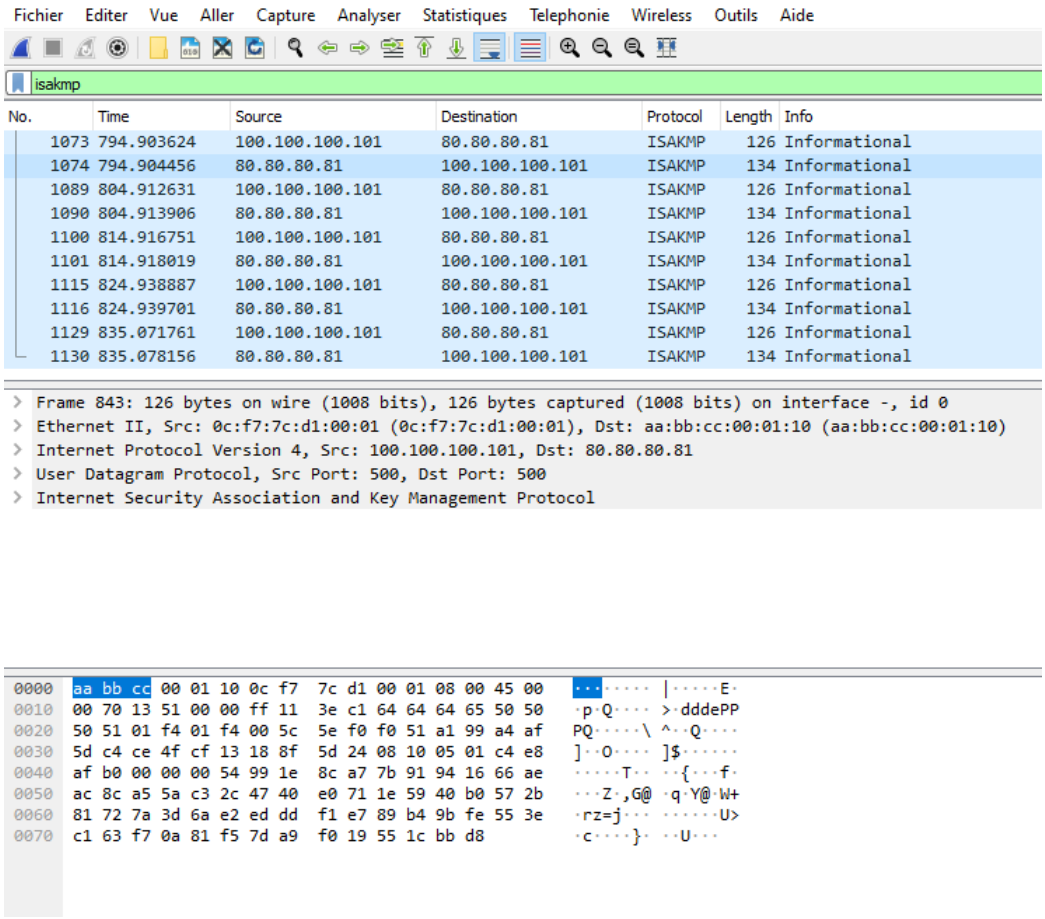

FIGURE 4.67 – Capture du traffic VPN sur Wireshark.

Conclusion Générale et Perspectives

Ce projet de fin d'études consiste à proposer une infrastructure réseau intranet sécurisée pour la station Beni-Mansour et l'interconnecter avec la RTC Bejaia en mettant en pratique les connaissances théoriques à travers des méthodes professionnelles utilisées dans l'entreprise SONATRACH.
Notre travail s'est porté sur les différentes techniques de sécurité dans un réseau local que nous avons configuré. Ces dernières répondent à un pourcentage important aux exigences de sécurité, d'où la protection du réseau des menaces internes ou externes.
Les attaques peuvent se produire à l'intérieur de l'entreprise (écoute sur le canal ou sur les ports), pour remédier à ce type d'attaque nous avons segmenté le réseau avec des VLANs.
Dans le but de protéger le réseau des attaques qui proviennent de l'extérieur (internet) nous avons placé un pare-feu pour empêcher les requêtes web de rentrer au réseau local afin de renforcer la sécurité. Par la suite, nous avons configuré la connexion des deux sites de Bejaia et Beni-Mansour avec un VPN IPsec, ce qui offre une sécurisation des informations échangées entre ces deux stations distantes.
Pour la réalisation de ce travail, nous avons utilisé le GNS 3 avec le VMWARE WORKSTATION PRO 16 pour simuler l'architecture étudiée. Aussi nous avons présenté notre environnement de travail et les outils qui nous ont servi pour implémenter notre simulation et vérifier son bon fonctionnement.
En termes de perspectives, nous envisageons d'améliorer notre travail en implémentant d'autres mécanismes de sécurité afin de se protéger contre les éventuelles attaques.

Annexes

Étapes d'installation du VMWare Workstation PRO 16

Pour installer le logiciel VMWare Workstation, il faut d'abord télécharger le fichier exécutable et lancer, après on suit les étapes d'installation jusqu'à la fin puis on clique sur "Finish". La figure suivante représente les différentes étapes :

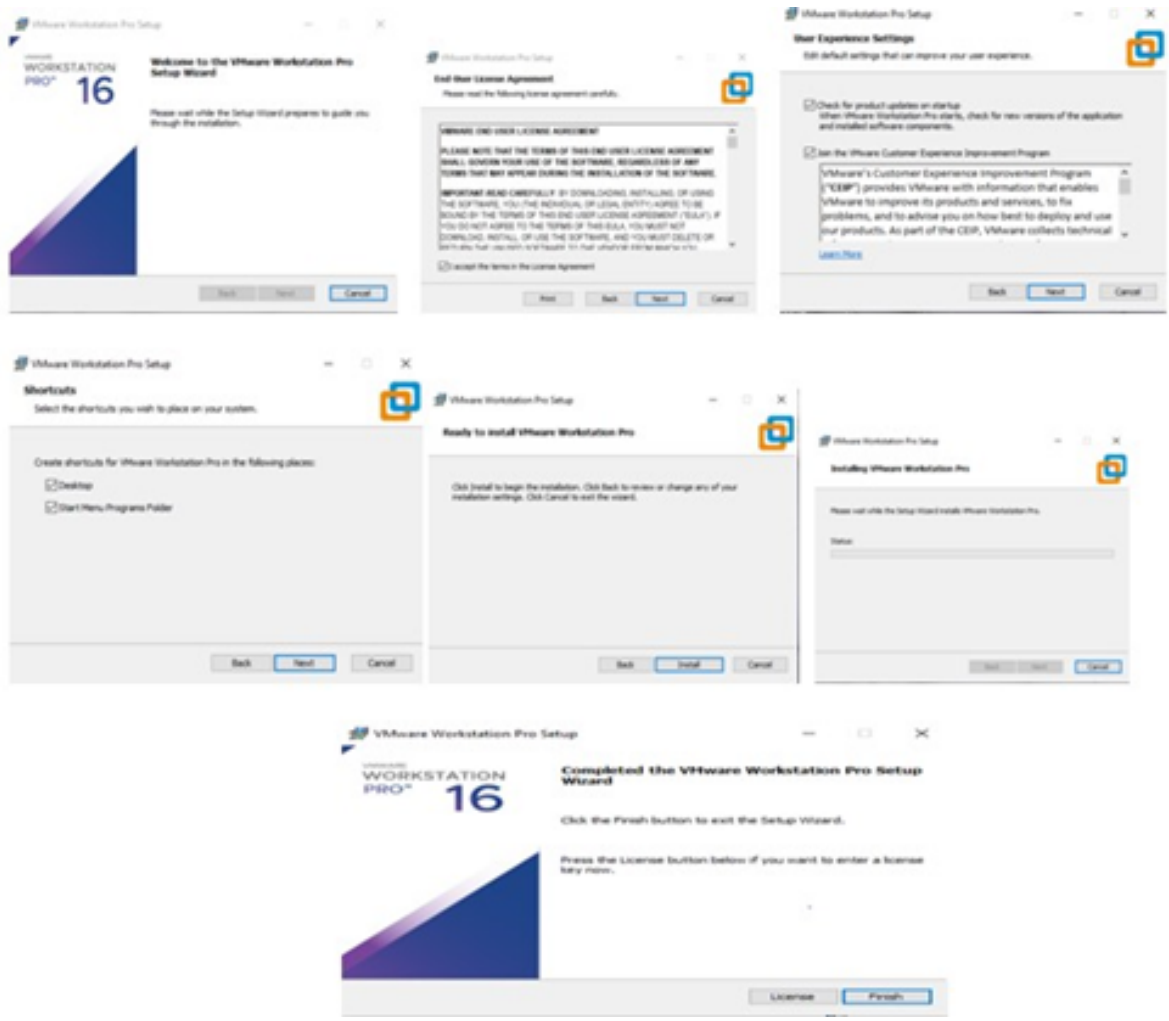

FIGURE 68 – Les étapes d'installation du VMWare Workstation PRO 16.

Installation de l'active directory sur Windows Server 2022

Sur la machine virtuelle on installe le contrôleur de domaine "Active Directory". Pour commencer l'installation, il va falloir ajouter le Service de Role Active Directory. Lancer l'installation et ajouter les fonctionnalités qui nous manquent.

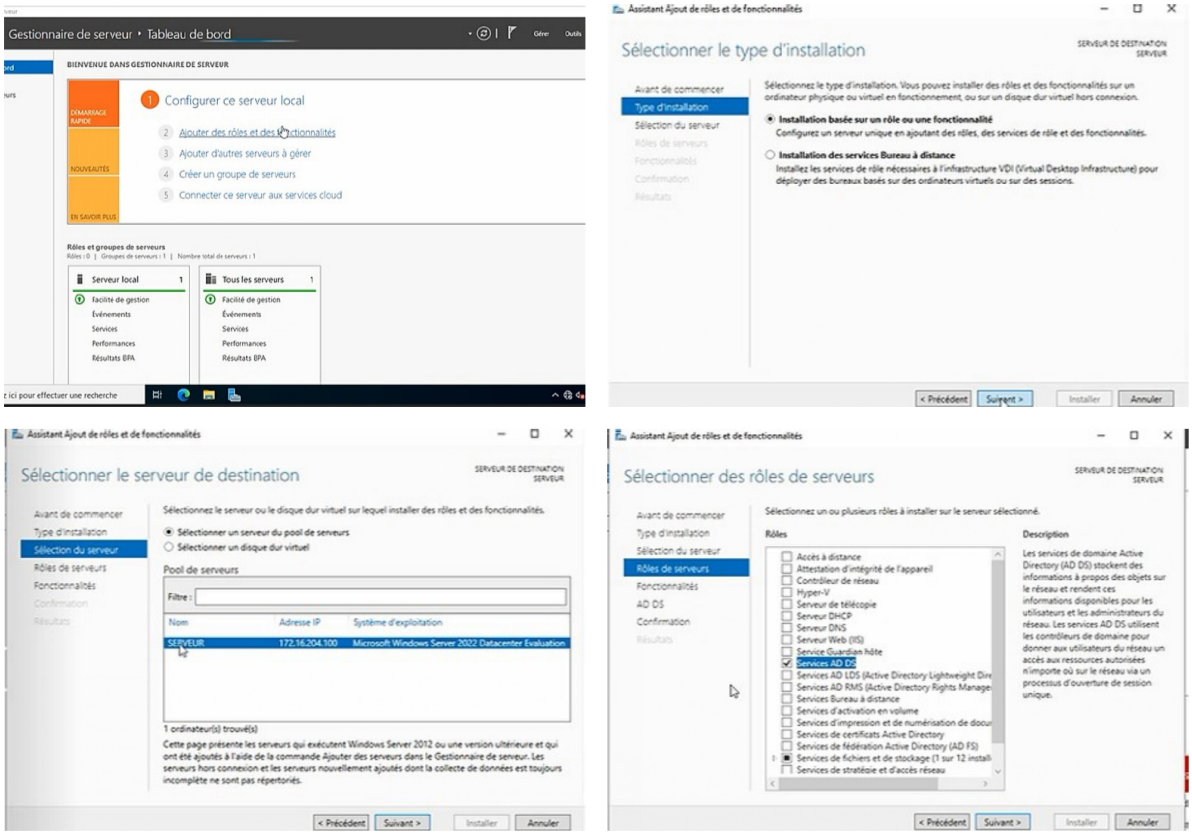

FIGURE 69 – Installation de l'active directory.

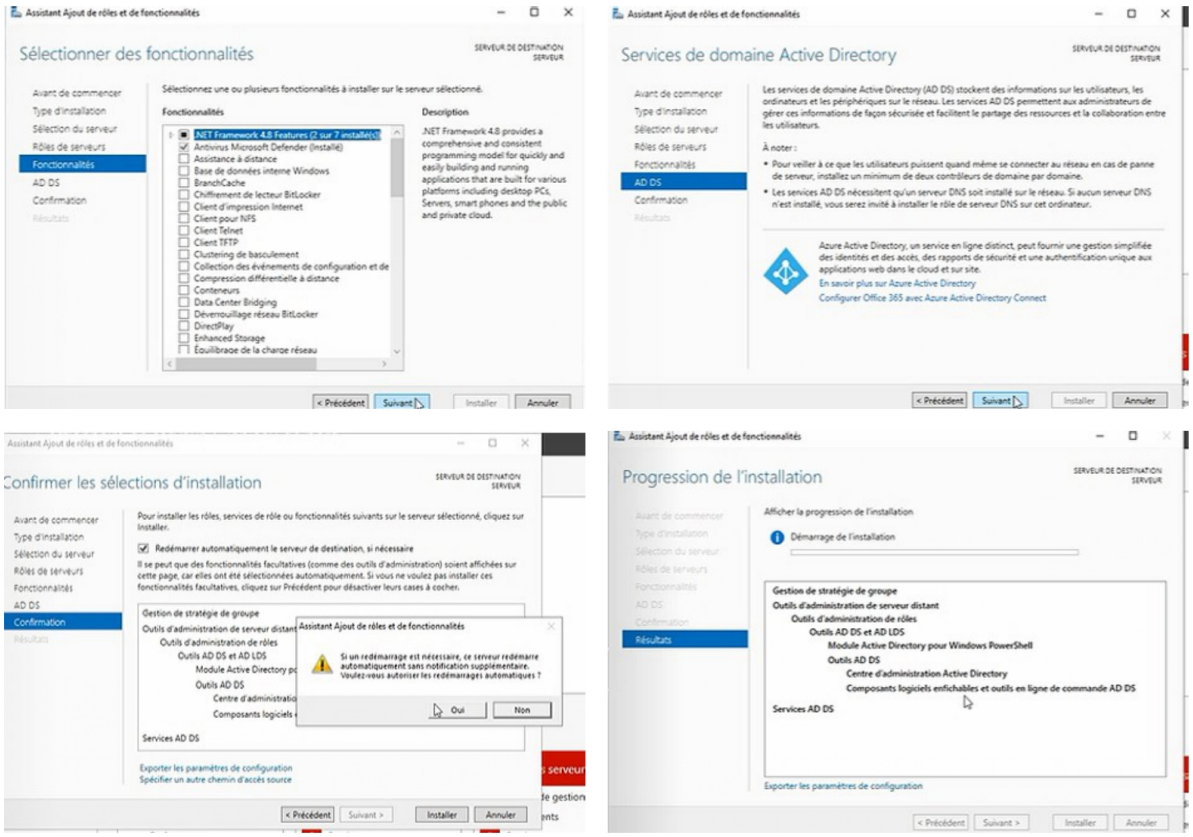

FIGURE 70 – Installation de l'active directory.

Installation de DHCP sous Windows Server 2022

Sur la machine virtuelle Windows Server 2022, Nous avons installé DHCP server Pour commencer l'installation, il va falloir ajouter le Service de DHCP Server et ajouté les fonctionnalités. Les figures suivantes montre les étapes de l'installation :

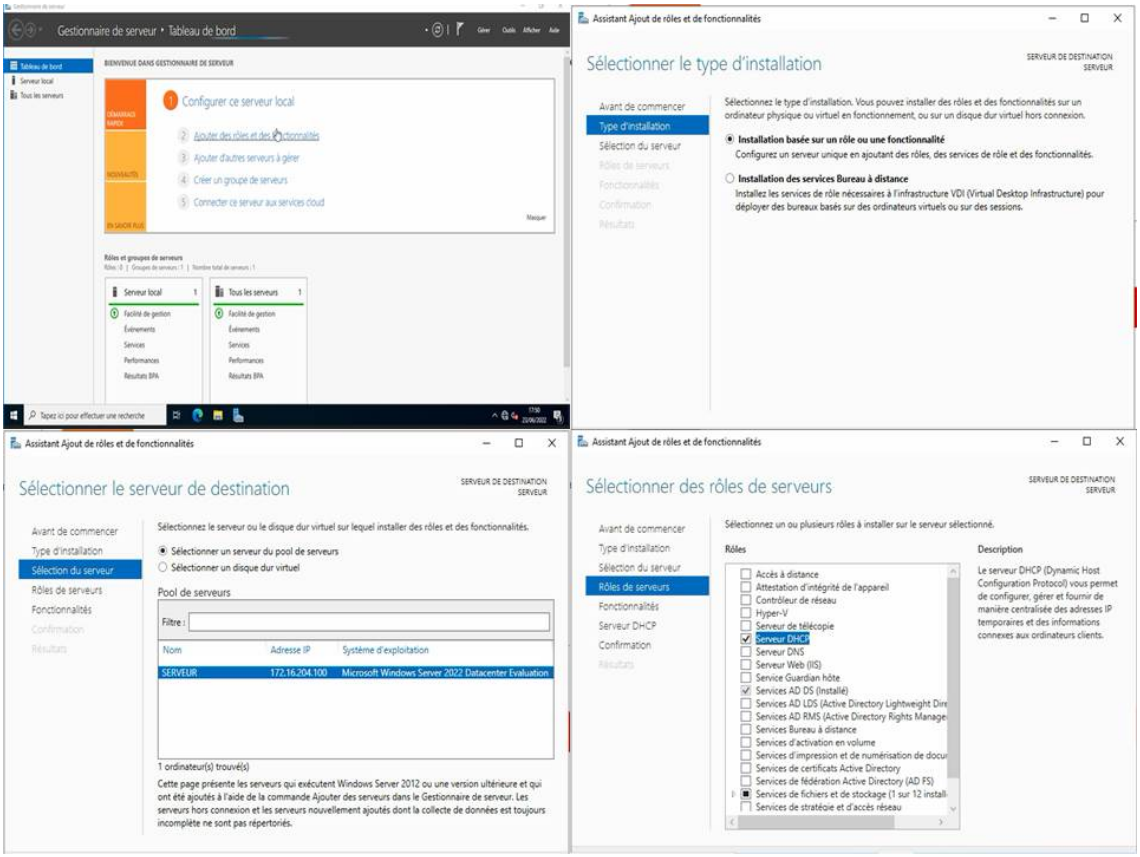

FIGURE 71 – Installation du DHCP.

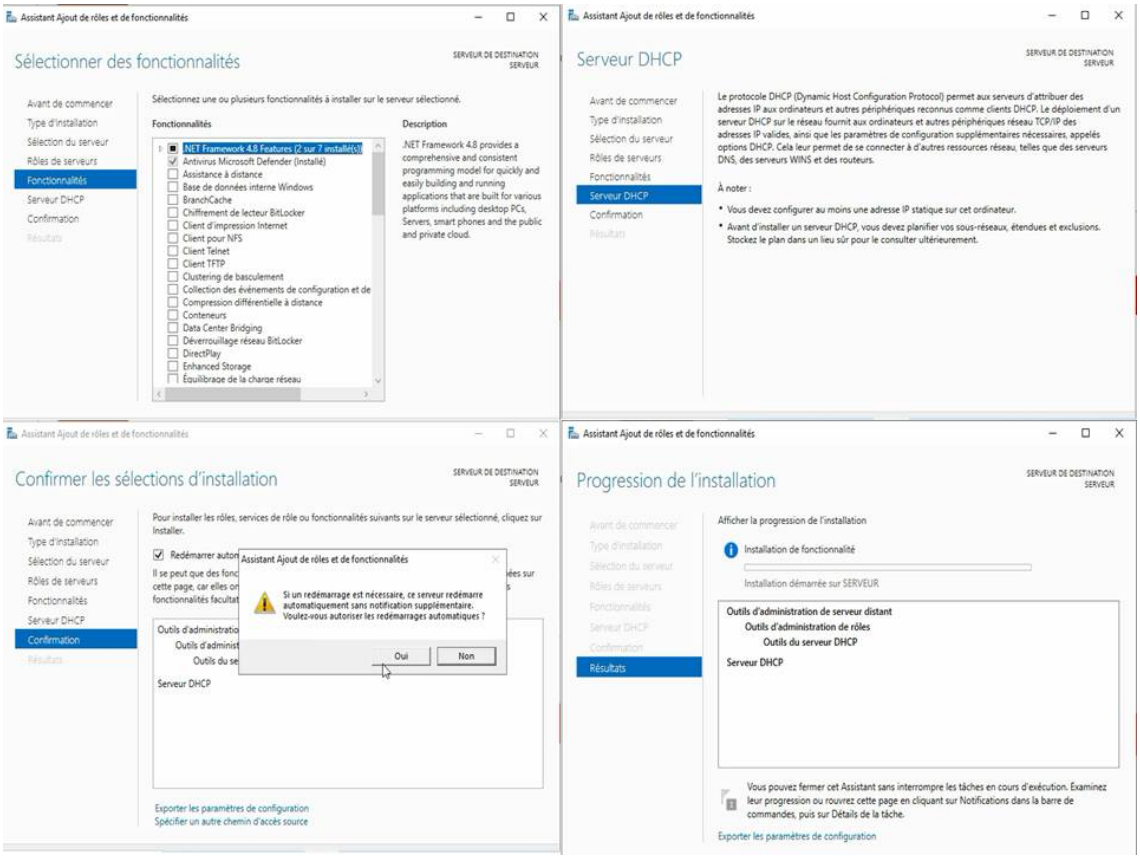

FIGURE 72 – Installation du DHCP.

Bibliographie

[1] Philippe Atelin, José Dordoigne, *Réseaux informatiques : Notions fondamentales (Normes, Architecture, Modèle ...)*, Éditions ENI, 2006.

[2] http://portail.lyc-la-martiniere-diderot.ac-lyon.fr/srv1/co/reseau_reseaux.html. (consulté le 05 juin 2022).

[3] https://www.techopedia.com (consulté le 05 juin 2022).

[4] https://www.mongosukulu.com/index.php/contenu/informatique-et-reseaux/reseaux-informatiques/639-les-equipements-reseaux-informatiques. (consulté le 05 juin 2022).

[5] https://www.hotosting.com/cresite/support-transmission.html. (consulté le 05 juin 2022).

[6] https://www.samomoi.com/reseauxinformatiques/modele_DOD.php (consulté le 07 juin 2022).

[7] https://portail.jacquenod.net/Web/Tutoriaux/normalisation.pdf (consulté le 07 juin 2022).

[8] *Meilleur pratique en matière de vlan*, livre blanc, IN, fluKe corporation, 2004. www.fluKenetworks.com (consulté le 07 juin 2022).

[9] http://tvaira.free.fr/bts-sn/reseaux/cours/cours-reseaux-routage-ip.pdf. (consulté le 07 juin 2022).

[10] C. Llorens L. Levier D. Valois. *Tableaux de bord de la sécurité.*, Groupe Eyrolles, 2003-2006, ISBN : 2-212-11973-9.

[11] https://web.maths.unsw.edu.au/~lafaye/CCM/attaques/attaques.htm (consulté le 14 juin 2022).

[12] https://waytolearnx.com/2018/07/difference-entre-attaque-active-et-attaque-passive.html. (consulté le 14 juin 2022).

[13] http://aidesecurite.blogspot.com/2013/03/types-dattaques-dun-reseau.html (consulté le 14 juin 2022).

[14] https://www.webroot.com/ca/en/resources/tips-articles/what-is-anti-virus-software (consulté le 14 juin 2022).

[15] https://www.kaspersky.fr/resource-center/definitions/encryption. (consulté le 19 juin 2022).

[16] https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html#~types-of-firewalls (consulté le 19 juin 2022).

[17] Sreven André, Brian Kenyon, and Erik Pack Birkholz, *Security Sage.s guide to hard-ening the network infrastructure*. Syngress, 2000.

[18] https://web.maths.unsw.edu.au/~lafaye/CCM/detection/ids.htm (consulté le 19 juin 2022).

[19] David Passmore and John Freeman, *The Virtual LAN Technology Report*, May 1998.

[20] https://web.maths.unsw.edu.au/~lafaye/CCM/technologies/tx.htm (consulté le 19 juin 2022).

[21] https://developer.orange.com/od-uploads/Generalites-sur-les-VPNs.pdf (consulté le 19 juin 2022).

[22] J. ARCHIER, *les vpn*. Éditions ENI, 552P, 2010.

[23] https://www.fortinet.com/products/next-generation-firewall (consulté le 21 juin 2022).

Résumé

Le réseau informatique est le cœur de l'entreprise, quelle que soit son secteur d'activité. Pour cela, les problèmes de sécurité doivent être réduit au minimum afin d'assurer l'activité de cette dernière. Dans notre travail, nous nous focalisons sur l'une des plus importantes technologies de réseau informatique, c'est l'installation, la configuration et la sécurisation d'un réseau local informatique pour la station Beni-Mansour et l'interconnecter avec la RTC Bejaia. L'objectif est d'assurer la communication entre les services des deux sites. À cet effet, nous avons segmenté notre réseau en VLANS comme nous avons configuré un VPN entre les deux sites BENI-MANSOUR et SONATRACH-BEJAIA, ainsi nous avons intégré plusieurs protocoles de sécurité(DHCP, VTP, HSRP,....). Pour la réalisation, notre simulation est faite à base du simulateur GNS3 et VMWARE.

Mots clés : réseau local,RTC, VLAN, VPN, DHCP, VTP, HSRP, GNS3, VMWARE.

Abstract

The computer network is the heart of the company, regardless of its sector of activity. For this, security problems must be reduced to a minimum in order to ensure the activity of the latter. In our work, we focus on one of the most important computer networking technologies, it is the installation, configuration and security of a computer local network for the Beni-Mansour station and interconnect it with the Bejaia RTC. The objective is to ensure communication between the services of the two sites. For this purpose, we have segmented our network into VLANS as we have configured a VPN between the two sites BENI-MANSOUR and SONATRACH-BEJAIA, as well as we have integrated several security protocols (DHCP, VTP, HSRP,....). For the realization, our simulation is made based on the GNS3 and VMWARE simulator.

Keywords : réseau local,RTC, VLAN, VPN, DHCP, VTP, HSRP, GNS3, VMWARE.