REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE ABDERRAHMANE MIRA -BEJAIA
FACULTE DES SCIENCES EXACTES
DEPARTEMENT INFORMATIQUE

Mémoire de fin de cycle

En vue de l'obtention du diplôme de Master professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Etude et mise en place d'une nouvelle stratégie de sécurité réseau et système
Cas d'étude : Entreprise SARL Laiterie SOUMMAM

Réalisé par

Mr HAMIDOUCHE Younes
Mlle KHALFI Yamina

Encadré par

Mme ADEL Karima

Encadrant de stage

Mr AMOURI Salah

Devant le jury composé de

Président : Mme YAICI Malika
Examinateur : Mr MOKTEFI Mohand

Promotion 2022-2023

Remerciements

Nous souhaitons exprimer nos sincères remerciements aux personnes et entités qui ont contribué à la réalisation de ce modeste travail, et nous tenons tout d'abord à exprimer notre gratitude envers DIEU tout puissant qui nous a accordé la santé, la volonté, et la patience, ainsi que Son précieux guidage tout au long de ce parcours.

Nous adressons nos plus chaleureux remerciements à notre promotrice, Mme ADEL Karima, pour avoir généreusement accepté de nous encadrer, pour ses orientations précieuses et sa disponibilité.

Nous sommes également très reconnaissants envers les membres du jury, le président Mme YAICI Malika, et l'examinateur Mr MOKTEFI Mohand, pour avoir consacré leur temps à l'évaluation de notre travail.

Nos remerciements s'étendent à l'ensemble des enseignants de notre faculté des sciences exactes, et plus particulièrement à ceux du département informatique, dont les enseignements ont joué un rôle fondamental dans notre formation tout au long de notre cycle d'études.

Nous exprimons nos sincères reconnaissances à Mr Hamitouche Lounis, gérant de la « laiterie SOUMMAM », pour nous avoir offert l'opportunité et les moyens nécessaires pour mener à bien notre travail.

Un grand merci à toute l'équipe de l'unité « Laiterie Soummam », notamment au Chef de service informatique, Mr Sebkhi Lyes, ainsi qu'au chef de la sécurité du réseau informatique, Mr Amouri Salah, et à toute l'équipe informatique pour leur soutien précieux pendant notre période de stage.

Nous exprimons notre profonde gratitude à Mr Djebbari Yassine, gérant de campus NTS, pour nous avoir accordé les ressources et l'assistance nécessaires à la réalisation de notre travail.

Un remerciement spécial et chaleureux va à nos très chers parents, dont le soutien, l'aide et les encouragements constants ont été d'une valeur inestimable tout au long de nos années d'études.

Enfin, nous tenons à remercier toutes les personnes qui, de près ou de loin, ont contribué à l'accomplissement de ce travail. Votre aide a été précieuse et nous en sommes profondément reconnaissants.

Dédicaces

Au nom de DIEU le tout puissant

En ce jour mémorable, je souhaite dédier ce travail :

A ma chère mère TOUNSI Hadjira

Aucun mot ne saurait exprimer pleinement l'amour et l'affection que je ressens pour toi. Ta présence inébranlable, ton encouragement et ton réconfort ont été mes piliers. Tes prières et tes bénédictions m'ont été d'un grand secours pour mener à bien mes études. Je te dédie ce travail pour exprimer ma gratitude envers les sacrifices que tu as consentis depuis ma naissance. Je ne pourrai jamais te remercier assez. Puisse le tout puissant te donner la santé, le bonheur et une longue vie.

A mon cher père Djamel

À travers toi, j'ai appris la valeur du travail acharné et de la responsabilité. Je prie pour que le Tout-Puissant te préserve une bonne santé et une vie longue et joyeuse.

A mes grands-parents TOUNSI Youcef et TALBI Ndjima

Une spéciale dédicace pour mon grand-père maternel, TOUNSI Youcef, qui nous a quittés avant de témoigner de ce moment de joie, Je te suis éternellement reconnaissante pour tes prières et ton encouragement. Tu resteras toujours dans mes pensées, que ton âme repose en paix. A ma grand-mère maternelle, le pilier restant, tu es chère à nos yeux Puisse Dieu te gratifier d'une longue vie et te garde pour nous.

A mes précieuse sœurs, Meriem et Rabia, et à mes frères Adel et Sifeddine
Pour votre encouragement, votre soutien moral et votre réconfort. Que nos liens fraternels se renforcent. Que Dieu vous protège tous.

A ma chère tante, Hassina
Aucune dédicace ne saurait exprimer pleinement mon amour, ma gratitude, mon respect et ma profonde reconnaissance pour ton soutien tout au long de mes années d'études. Que le Tout-Puissant te préserve et te donne la santé ainsi qu'une longue vie.

À mes précieux neveux, Shérine, Younes, et mon petit cousin Elias, *ma source de tendresse.*
A ma chère belle-sœur ***BOUBKER Ouarda****.*

A mes chères amies, Asma, Niscia, Fairouz et Inès
Pour avoir été à mes côtés, dans les bons moments comme dans les moments difficiles. Que DIEU le Tout Puissant vous bénisse.

A tous mes professeurs
Votre générosité et votre soutien méritent mon respect et ma sincère considération.

A mon partenaire d'étude et à sa famille

A tous ceux qui ont contribué à la réalisation de ce mémoire, MERCI.

Yamina

Dédicaces

En cette mémorable occasion de ma soutenance, je tien à dédier ce modeste travail

A ma très chère mère Hadjila
Quoi que je fasse ou que je dis, je ne saurai point te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les déférents obstacles. Ce modeste travail est le fruit de tous les sacrifices que tu as déployés pour mon éducation et ma formation. Puisse le tout puissant te donner Santé, bonheur et longue vie.

A mon très cher père Rabia
Aucune dédicace ne serait exprimée tout mon amour, ma reconnaissance, mon respect et ma profonde gratitude pour tes sacrifices, ta patience sans fin, ton soutien, ton encouragement durant toutes mes années d'études. Grâce à toi j'ai appris le sens du travail et de la responsabilité. Je te dois ce que je suis aujourd'hui et ce que je serais demain et je ferai toujours de mon mieux pour te rendre fier et ne jamais et décevoir. J'implore le tout puissant pour qu'il t'accorde une longue vie.

A mes précieuses chères sœurs
Thanina, Thilleli, kenza et Ouazna pour l'amour qu'elles me réservent, pour tous vos encouragement permanent, vos soutiens moraux et vos réconforts. Puisse nos liens fraternels se consolider et se pérenniser encore plus. Je vous souhaite une vie pleine du bonheur et de succès

A ma nièce Rima et mon neveu Ilyas
Les lumières de mes jours, la source de mes efforts les flammes de mon cœur mes vies que dieu vous protégé a jamais je vous aime beaucoup

A mes beau-frère Amar et Abasse

A la mémoire de mes grands parents

A mon grand-père maternel je leur souhaite une longue vie

A mes oncles et mes tentes

A tous mes cousins et cousines en générale, à Farhat en particulier en témoignage de l'amitié qui nous unit

A tous mes amis et Dassyne en particulier qui m'a toujours encouragée et à qui je souhaite plus de succès

A ma partenaire d'étude Yamina et toute sa famille

Younes

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AAA : Authentication Authorization Accounting.

AD : Active directory.

AD CS : Active Directory Certificate Service.

AD DS : Active Directory Domain Service.

AH : Authentication Header.

CA : Certificate Authority**.**

DDoS : Distributed Denial Of Service.

DHCP : Dynamic Host Configuration Protocol.

DMZ : Demilitarized Zone.

DNS : Domain Name System.

EAP : Extensible Authentication Protocol.

ESP : Encapsulating Security Payload.

FG-LS : Fortigate Laiterie Soummam.

FTP : File Transfer Protocol.

GNS3 : Graphical Network Simulator.

GPO : Group Policy Object.

ID : Identifiant.

IEEE : Institute of Electrical and Electronics Engineers.

IKE : Internet Key Exchange.

IP : Internet Protocol.

IPSec : Internet Protocol Security.

IPS/IDS : Intrusion Prevention System / Intrusion Detection System.

ISO : International Organization for Standardization.

ISP : Internet Service Provider.

LAN : Local Area Network.

LDD : Liaison de Données.

MAC : Media Access Control.

MAN : Metropolitan Area Network.

NAT : Network Address Translation.

NPS : Network Policy Server.

OSI : Open Systems Interconnexion.

PAN : Personal Area Network.

PEAP : Protected Extensible Authentication Protocol.

P2P : Peer To Peer.

RADIUS : Remote Access Dial In User Service.

SA : Security Association.

Sw-Dist : Switch-Distribution.

TACACS : Terminal Access Controller Access-Control System.

TCP : Transmission Control Protocol.

TCP/IP : Transmission Control Protocol/Internet Protocol.

TLS : Transport Layer Security.

UDP : User Datagram Protocol.

VLAN : Virtual Local Area Network.

VPN : Virtuel Private Network.

VTP : VLAN Trunking Protocol.

WAN : Wide Area Network.

Introduction générale

Avec l'avènement des technologies numériques et de la connectivité croissante, les réseaux informatiques jouent un rôle essentiel dans le bon fonctionnement des entreprises de tous secteurs. Hélas, la sécurité des réseaux est devenue une préoccupation primordiale pour assurer la confidentialité, l'intégrité et la disponibilité des données. Dans ce contexte notre mémoire de fin cycle vise à identifier les problèmes de sécurité existants dans le réseau local (LAN) de l'entreprise SARL Laiterie SOUMMAM et de proposer une solution efficace pour les résoudre. Pour atteindre cet objectif, nous avons structuré notre travail en quatre chapitres, chacun ciblant un objectif spécifique.

Le premier chapitre établira les fondements théoriques de notre mémoire. Dans un premier temps, nous aborderons les notions générales relatives aux réseaux informatiques. Ensuite, nous explorerons les concepts fondamentaux de la cybersécurité. Nous nous pencherons également sur les VLANs, en mettant en lumière les différents protocoles tels que VTP, qui facilite la distribution centralisée des déclarations VLAN à travers le réseau, ainsi que le routage inter-VLAN, permettant la communication entre les interfaces virtuelles segmentées des VLANs, et l'utilisation des private VLANs pour renforcer la sécurité de la DMZ mise en place dans l'entreprise. Enfin, nous nous concentrerons sur les deux modes de connexion, filaire (Ethernet) et sans fil (Wi-Fi), sur lesquels va se baser notre solution pratique. Ce chapitre vise principalement à doter les lecteurs de connaissances solides sur les réseaux informatiques et la sécurité informatique, afin de leur permettre de comprendre les enjeux spécifiques liés à la sécurité des réseaux locaux.

Le deuxième chapitre sera consacré à la présentation de l'organisme d'accueil, la SARL Laiterie SOUMMAM, avec un accent particulier sur son département informatique. Nous commençons par présenter la situation géographique de l'entreprise ainsi que ses activités, ensuite nous procéderons à une étude approfondie de l'existant afin de mettre en évidence les problèmes de sécurité liés au réseau de l'entreprise. À travers cette analyse, nous serons en mesure de cerner les faiblesses et les vulnérabilités qui pourraient mettre en péril la sécurité du réseau et proposons des solutions visant à renforcer la sécurité du réseau local de l'entreprise.

Le troisième chapitre, au cœur dans notre étude, expliquera le fonctionnement théorique des différents protocoles et systèmes de sécurité, ainsi que les méthodes et bonnes pratiques à appliquer pour renforcer la sécurité à chaque niveau d'un réseau LAN. Nous débuterons en définissant le modèle de conception du réseau que nous utiliserons dans notre mise en pratique,

puis nous explorerons les outils d'administration et de sécurité des réseaux informatiques tels que les VPN et l'authentification RADIUS. Ces méthodes permettront une administration efficace du réseau et garantiront une protection robuste contre les menaces internes et externes.

Enfin, le quatrième chapitre présentera la mise en œuvre concrète de notre solution visant à combler les failles de sécurité identifiées dans le réseau de la Laiterie SOUMMAM. Nous débuterons par la présentation de l'environnement de travail, de l'architecture proposée, ainsi que des équipements matériels utilisés. Ensuite, nous détaillerons l'installation des rôles sur notre serveur, tels qu'AD DS, DHCP, NPS, etc. Nous configurerons également les équipements de raccordement, le pare-feu Fortigate, et les rôles installés sur le serveur. Nous mettons en place diverses politiques de sécurité au niveau du pare-feu, notamment la politique de prévention des attaques DOS, destinée à bloquer les tentatives d'attaques visant à perturber le réseau de l'entreprise. Enfin, nous conclurons notre partie pratique par des tests, y compris des attaques DOS, afin de vérifier l'efficacité de notre solution.

Chapitre 1

Notions de base sur la sécurité des réseaux informatiques

1.1 Introduction

Ce chapitre explorera les fondements essentiels de la sécurité des réseaux informatiques. Pour ce faire, nous commencerons par présenter quelques concepts de base des réseaux informatiques, puis explorerons les concepts clés de la cybersécurité. Par la suite, nous approfondirons notre compréhension des VLANs et de leur rôle dans l'optimisation de la gestion des réseaux. Enfin, nous aborderons les modes de connexion Ethernet et Wi-Fi, vous préparant ainsi à évoluer aisément dans le domaine en perpétuelle évolution des technologies informatiques.

1.2 Généralités sur les réseaux informatiques

1.2.1 Définition

Un réseau informatique est l'interconnexion de deux à plusieurs terminaux (ordinateurs, imprimantes, scanner, etc.), qui sont reliés par des câbles et des équipements d'interconnexion (routeurs, commutateurs, hub, etc.) afin de partager des données, des ressources et des informations entre eux grâce à des protocoles de communication. Chaque appareil est identifié par son adresse IP, et peut être configuré de différentes manières pour répondre à des besoins spécifiques.

1.2.2 Types de réseaux

Trois termes sont souvent utilisés pour décrire les différents types de réseaux informatiques :

Intranet : est un réseau privé conçu pour un groupe restreint, inaccessible depuis Internet. Il facilite le partage sécurisé de ressources et d'informations au sein d'une organisation, favorisant la collaboration entre les employés. Cependant, sa mise en place requiert une solide infrastructure informatique et une équipe compétente en informatique.

Extranet : est un réseau qui s'étend au-delà du propre réseau d'une organisation, permettant un accès externe à certaines parties d'un intranet d'une entreprise, qui est sécurisée de manière à n'autoriser l'accès uniquement qu'aux personnes désignées [1]. Les extranets sont utilisés pour faciliter la collaboration et l'échange d'informations avec des partenaires.

Internet : est un réseau mondial accessible au public, reliant de nombreux dispositifs et permettant le partage d'informations à moindre coût. Il repose sur une architecture client-serveur et utilise le protocole TCP/IP. Internet offre divers services, notamment le World Wide Web, la messagerie électronique et le transfert de fichiers via FTP. Cependant, sa nature publique comporte des risques de sécurité, nécessitant des mesures de protection pour préserver la confidentialité des utilisateurs et des données.

1.2.3 Architecture réseau

Il est possible de distinguer deux modes de fonctionnement :

Paire à paire (en anglais Peer to Peer, ou P2P) : Le modèle P2P est un réseau informatique où chaque ordinateur agit à la fois en tant que client et serveur, permettant le partage direct de fichiers et de ressources entre ordinateurs sans nécessiter un serveur central. Cela facilite les échanges rapides entre les ordinateurs d'un réseau, couramment utilisé pour le partage de fichiers, le streaming vidéo, les jeux en ligne, et d'autres applications de pair à pair.

Client/serveur : est un modèle de communication entre ordinateurs dans lequel un ordinateur central appelé « serveur » met à disposition des services réseau aux utilisateurs. Le serveur est spécialisé dans la distribution et le stockage des ressources partagées des utilisateurs connectés au réseau. Le client désigne l'ordinateur qui accède aux ressources partagées mises à disposition par le serveur du réseau. Ce modèle est courant dans les réseaux informatiques, les applications Web, les bases de données, etc. Il présente des avantages comme la centralisation des données, la gestion facile, et la sécurité, mais peut aussi engendrer des coûts élevés et une dépendance au serveur.

1.2.4 Norme de communication OSI (Open System Interconnection)

Appelé modelé de référence OSI, basé sur une proposition développée par l'organisation internationale de normalisation (ISO), composé de sept couches. Chaque couche (n) fournit de nombreux services à la couche (n+1) et déroule des protocoles définis de manière unique à partir des services fournis par la couche (n-1).

La figure suivante présente les fonctionnalités fournit par chaque couche :

Une couche assurant la transmission de l'application demandée avec envoi de messages.	*7*	*couche application*	Gère les applications de types réseaux : courrier électronique, transfert de fichier, appel de procédure distantes…
	6	*couche présentation*	Assure une transparence en terme de codage (ex. *ASCII*).
	5	*couche session*	S'occupe de fiabiliser la communication utilisateurs, gère des tours de parole, synchronisation.
Une *couche de communication de base* permettant de transmettre physiquement en respectant un certain nombre de règles.	*4*	*couche transport*	Optimise l'utilisation de la couche réseau et assure des travaux de type fragmentation de message (ex. *TCP*).
	3	*couche réseau*	Offre un nombre de services dont un service d'adressage (*IP*) permettant d'atteindre son destinataire, un service de routages déterminant un chemin à l'intérieur du réseau maillé et un contrôle du flux pour ne pas saturer le réseau.
	2	*couche liaison de données*	Permet d'assurer une liaison fiable par une bonne synchronisation et une détection d'erreurs.
	1	*couche physique*	Emet des signaux assurant la bonne transmission.

Figure 1.1 : Couches modèle OSI [2].

1.3 La sécurité informatique

1.3.1 Définition

La sécurité informatique représente l'ensemble des moyens et des techniques mises en œuvre pour assurer l'intégrité et la non-diffusion involontaire des données transitant dans le système d'information. Ce dernier définit l'ensemble des données et des ressources (matérielles, logicielles et humaines) permettant de stocker et de faire circuler les informations qu'il contient. Il représente également le réseau d'acteur qui interviennent sur celui-ci, qui échangent les données, y accèdent et les utilisent [3].

1.3.2 Objectifs de la sécurité

La sécurité informatique vise les objectifs suivants :

La confidentialité : Assurer que les informations ne sont pas divulguées aux entités non autorisées à les connaitre, une entité peut être une personne, un site, une organisation, etc. pour garantir cet objectif on a souvent recours aux algorithmes de chiffrements.

L'intégrité : La garantie que les données émises sont exactement celles à la réception, autrement dit garantir qu'au cours de la communication les données ne sont pas modifiées, altérés ou détruits. Cela peut être accompli grâce à l'utilisation des fonctions de hachage.

La Disponibilité : Il s'agit d'un bon fonctionnement du système, l'accès à un service ou à une ressource doit être disponible pour les personnes autorisées, durant la plage d'utilisation, avec un temps de réponse acceptable. Pour assurer cela, des mesures de sécurité comme la tolérance aux pannes, la redondance, et les sauvegardes sont mises en place.

L'Authentification : L'authentification englobe deux aspects distincts : d'une part, prouver l'origine d'une information (l'auteur ou l'émetteur), et d'autre part, vérifier que l'identité de l'utilisateur correspond à celle déclarée, pouvant s'effectuer via divers moyens tels que mot de passe, carte à puce, certificat, empreinte digitale, ADN, etc.

La Non-répudiation : La propriété qui empêche un utilisateur de nier les opérations qu'il a réalisées. Par exemple : empêcher l'expéditeur ou le receveur de nier avoir transmis ou reçu un message. Généralement la non-répudiation est garantie grâce à la signature des données.

Le Contrôle d'accès : Limité l'accès à des ressources pour les entités du réseau, de tel sorte, à attribuer des droits d'accès selon différents privilèges et exiger l'authentification sur chaque entité, ainsi seuls les utilisateurs autorisés auront accès aux systèmes et aux données.

1.3.3 Politique de sécurité

1.3.3.1 Définition

C'est l'ensemble de règles, de procédures et pratiques, à suivre au sein d'un système spécifique, dont le but est de garantir que les objectifs de la politique soient satisfaits.

1.3.3.2 Objectifs [4]

L'objectif principal d'une politique de sécurité informatique est de fournir un cadre et des directives pour protéger les systèmes informatiques, les données et les informations sensibles d'une organisation contre les menaces et les risques. Voici quelques exemples :

- S'assurer que les utilisateurs observent les bonnes pratiques et les règles concernant l'utilisation des technologies de l'information.
- Réviser périodiquement les résultats des vérifications et contrôles, notamment pour y relever les anomalies et autres incidents.
- Recommander les actions à prendre pour corriger les situations anormales ou dangereuses.

1.3.4 Mise en place d'une politique de sécurité informatique [4]

Il existe deux philosophies pour la mise en place d'une politique de sécurité :

- Prohibitive : tout ce qui n'est pas explicitement autorisé est interdit.
- Permissive : tout ce qui n'est pas explicitement interdit est autorisé.

Voici les étapes clés à suivre pour établir une politique de sécurité informatique :

i. Identifier les risques et leurs conséquences.
ii. Évaluation des probabilités associées à chacune des menaces.
iii. Evaluation du coût d'une intrusion réussie.
iv. Élaborer des règles et des procédures à mettre en œuvre pour les risques identifiés.
v. Evaluation des coûts des contre-mesures.
vi. Surveillance et veille technologique sur les vulnérabilités découvertes.
vii. Actions à entreprendre et personnes à contacter en cas de détection d'un problème.

1.3.5 Attaques informatiques

Une attaque comme mentionné précédemment est l'exploitation d'une vulnérabilité dans un système, son origine peut être interne comme : un utilisateur malveillant, une erreur involontaire, etc. ou externe comme piratage informatique, virus, intrusion, etc. Il existe plusieurs attaques informatiques, divisés en quatre catégories.

- **Catégories d'attaques**
  - **Interruption :** L'objectif principal de cette attaque est de rendre indisponible un système ou un service.
  - **Interception :** vise la confidentialité, elle consiste à capturer ou à écouter des communications ou des données sensibles entre deux parties légitimes.
  - **Modification :** porte atteinte à l'intégrité des données, elle vise à altérer ou modifier les données ou les communications pendant leur transit.
  - **Fabrication :** C'est une attaque portée à l'authenticité, créer de fausses données, des identités ou des ressources dans le but de tromper les utilisateurs ou de compromettre un système.
- **Exemple d'attaques**
  - **DDoS (Distributed Denial Of Service) :** Une attaque par déni de service distribué vise à rendre un serveur ou un système hors service, en le submergeant par de multiples requêtes, le rendant ainsi indisponible pour les utilisateur légitimes.
  - **Man-in-the-Middle (l'homme du milieu)** : L'hacker s'interpose entre deux parties communicantes, intercepte et modifie les données échangées avant de les retransmettre a l'autre bout, en se faisons passer par une des parties communicantes.

- **Les attaques de phishing** : Il s'agit d'une technique frauduleuse utilisée par les hackers, en émettant des entités légitimes comme des entreprises ou des banques, dans le but d'inciter les utilisateurs (internautes) à divulguer des informations personnelles ou à effectuer des paiements.
- **Malware :** Les logiciels malveillants, comme les virus, vers, chevaux de Troie et ransomwares, sont des programmes conçus pour endommager ou compromettre un système informatique, généralement distribués par des moyens tels que pièces jointes, téléchargements douteux, sites Web malveillants ou supports de stockage infectés.
- **Attaques par force brute :** c'est une méthode utilisée par les attaquants, elle consiste à essayer toutes les combinaisons possibles pour deviner un mot de passe ou une clé de chiffrement, souvent avec l'aide de logiciels automatisés. Cela peut prendre beaucoup de temps, parfois plusieurs jours voire des années.
- **Spoofing (Mystification) :** C'est une technique d'intrusion qui implique la falsification d'adresse IP, en se faisons passer par une entité, dans le but de passer pare-feu.

1.4 Les VLANs (Virtual Local Area Networks)

1.4.1 Principe des VLANs

Le principe des VLANs est de regrouper des machines dans un ou plusieurs segments quel que soit leur emplacement physique [5]. Voici un exemple de ces segments :

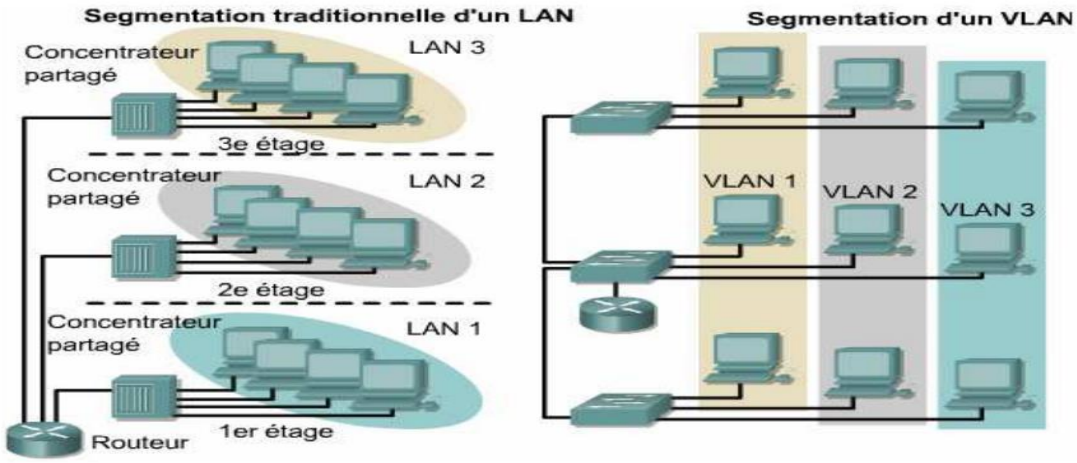


Figure 1.2 : Exemple de segmentation d'un LAN et d'un VLAN [6]..

Les VLANs sont couramment utilisés dans les entreprises pour améliorer la sécurité, faciliter la gestion des réseaux et optimiser les performances en isolant les groupes d'utilisateurs et en contrôlant le trafic.

1.4.2 Types de VLANs

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue :

- **VLAN de port :** Il associe les trames au VLAN en fonction du PVID du port d'accès. Il renforce la sécurité en limitant l'accès à un VLAN spécifique. L'administration peut être simplifiée en utilisant l'authentification 802.1X pour configurer dynamiquement les ports. Cette méthode est souvent utilisée dans les entreprises.
- **VLAN basé sur les adresses MAC :** Ils situent à la couche 2 du modèle OSI et dépendent des tables d'adresses MAC configurées sur les commutateurs ou les routeurs. Les adresses non déclarées sont associées au VLAN du PVID du port d'entrée ou au VLAN par défaut ou rejetée. Sensible au spoofing MAC, mais ce modèle reste plus modulaire et centralisé que le VLAN de port, offrant une flexibilité accrue.
    - **VLAN basé sur les protocoles :** Ils associent les trames à des VLAN en fonction du protocole de couche 3 utilisé (comme TCP/IP, IPX, AppleTalk), principalement pour la différenciation de service 802.1p, mais rarement utilisés en entreprise.
    - **VLAN basé sur les sous réseaux ou VLAN IP :** Ils associent les trames en fonction du sous-réseau IP de l'adresse source. Bien que cela permette une gestion centralisée, la désencapsulation des paquets est moins efficace que la gestion par adresse MAC ou par port. De plus, cela rend le réseau vulnérable aux attaques de spoofing IP, donc peu utilisé en entreprise en raison de ses limitations.

En résumé, les différents types de VLANs offrent une flexibilité de segmentation du réseau en fonction des besoins spécifiques d'une entreprise ou d'une organisation.

1.4.3 La norme 802.1Q

La norme 802.1Q est essentielle pour segmenter les réseaux Ethernet en utilisant des étiquettes VLAN, renforçant ainsi la gestion et la sécurité des réseaux LAN d'entreprise pour une infrastructure plus stable et flexible. Voici un exemple d'une trame Ethernet :

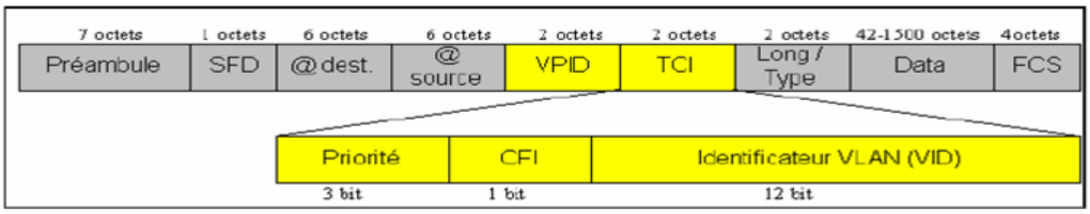


Figure 1.3 : Exemple d'une trame Ethernet [7].

802.1Q modifie les trames Ethernet en ajoutant 2 octets, créant ainsi des champs pour diverses fonctions. Elle identifie ces trames avec le champ VPID 0x8100 pour désigner la trame 802.1q. Son principal objectif est de permettre la communication entre les machines du même VLAN à travers divers équipements réseau. De plus, elle offre une priorisation de flux grâce à la norme 802.1p, un champ protocole pour une utilisation flexible, et un champ Vlan ID pour l'identification de VLANs, avec une capacité de jusqu'à 4096 VLANs.

1.4.4 Le VLAN Natif

Le VLAN natif est un VLAN qui est configuré sur les ports trunk, utilisé pour traiter les trames non marquées sur le lien 802.1Q afin d'éviter les attaques telles que le spoofing. Par défaut, il est le VLAN 1, mais peut être configuré sur un autre VLAN si nécessaire. Il doit être le même sur les deux extrémités d'un lien trunk pour communiquer correctement, il est donc important de le configurer avec soin.

1.4.5 Le protocole VTP (VLAN Trunking Protocol) [7]

1.4.5.1 Définition

Il permet de diffuser la déclaration des VLANs pour les ports trunk sur l'ensemble du réseau en réalisant une administration centralisée de ceux-ci. Ce protocole est propriétaire CISCO. Il fonctionne avec une architecture client-serveur.

1.4.5.2 Mode de fonctionnement

Le serveur tient à jour une table de VLANs déclarés. Cette table est diffusée à l'ensemble des clients étant sur le même domaine VTP. De ce fait chaque modification de la table est répercutée à l'ensemble des clients. Ainsi tous les VLANs définis sur le serveur pourront transiter par l'ensemble des ports trunk des switchs clients (sauf configuration contraire sur les interfaces).

Les matériels peuvent être en mode :

- **Server :** Il est associé à un domaine VTP. La déclaration des VLANs s'effectue sur le serveur. Il tient à jour la liste des VLANs déclarés et la diffuse à l'ensemble des clients.
- **Client :** Il est associé à un domaine VTP. Il reçoit la liste des VLANs, il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste.
- **Transparent :** Il est associé à aucun domaine VTP. Sa liste de VLAN est locale et n'est pas mis à jour lorsqu'il reçoit une trame VTP. Cependant il propage les listes de VLAN qu'il reçoit.

1.4.5.3 Paramètres

- **VTP password :** il est possible d'indiquer un mot de passe sur le serveur pour le domaine VTP. Dans ce cas les clients ne peuvent se mettre à jour que s'ils ont le même mot de passe. Ceci permet de déjouer les attaques consistant pour un pirate à se faire passer pour le VTP serveur.
- **VTP prunning :** le VTP prunning permet de faire des économies de bande passante. La fonction s'active à partir du switch server dans le but d'avertir le switch voisin de ne pas lui envoyer de trafic pour ce VLAN.

1.4.6 Le routage inter-vlan

Le routage inter-VLAN est essentiel car les VLANs fonctionnent au niveau 2 du modèle OSI. Pour permettre la communication entre les VLANs, il faut utiliser une passerelle de niveau trois, comme un routeur ou un commutateur multilayer. Ce routage est effectué entre des interfaces virtuelles, une par VLAN, similaire au routage entre des interfaces physiques. Il permet la communication entre tous les VLANs via un routeur en détagguant et retagguant les trames avec les bons identificateurs de réseau virtuel (VID).

1.4.7 Le private VLAN

Le VLAN privé (PVLAN) segmente les ports pour empêcher la communication directe entre eux, ne permettant la communication qu'avec un port uplink partagé ou un port communautaire. Cela économise des adresses IP et renforce la sécurité, utile pour les fournisseurs d'hébergement et les entreprises isolant des clients ou des utilisateurs (voir l'exemple sur la figure 1.4).

1.4.7.1 Types de VLAN dans un VLAN privé [8]

Au sein d'un réseau VLAN privé, les VLAN sont accessibles sous trois modalités :

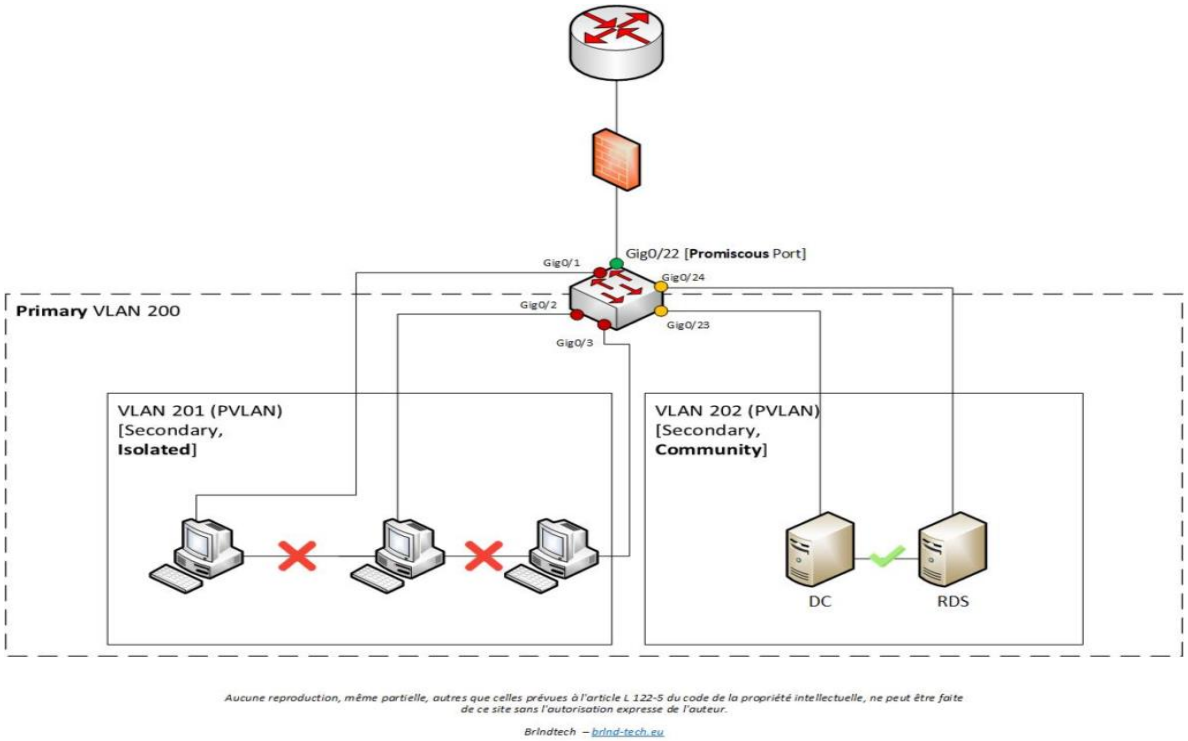
- **VLAN primaire :** Ce type de VLAN fait référence au VLAN d'origine, qui peut descendre des trames vers tous ses sous-VLAN (VLAN secondaires) à partir des ports promiscuous vers tous les ports connectés à l'hôte.
- **VLAN isolé :** En tant que VLAN secondaire, le VLAN isolé ne peut prendre en charge que les ports de commutation (ports isolés) au sein du VLAN isolé qui transmettent des données aux ports promiscuous du VLAN primaire. Même dans un même VLAN isolé, les ports isolés ne peuvent pas communiquer entre eux.
- **VLAN communautaire :** Le VLAN communautaire est également un type de VLAN secondaire. Les ports de commutation (ports communautaires) au sein d'un même VLAN

communautaire peuvent communiquer entre eux ainsi qu'avec les ports du VLAN primaire. Mais un tel type de VLAN est également incapable de communiquer avec d'autres VLAN secondaires, y compris d'autres VLAN communautaires.

1.4.7.2 Types de port du private VLAN [8]

Il existe trois types de port VLAN :

- **Port promiscuité :** ce type de port est capable d'envoyer et de recevoir des trames de n'importe quel autre port du VLAN. Il se connecte généralement à un commutateur de couche 3, un routeur ou d'autres dispositifs de passerelle.
- **Port isolé :** Existant dans un sous-VLAN, le port isolé se connecte à un hôte et ne peut communiquer qu'avec des ports promiscuous.
- **Port communautaire :** Le port communautaire réside également dans un sous-VLAN et se connecte à un hôte. Cependant, il ne peut dialoguer qu'avec les ports promiscuous et les autres ports communautaires du même sous-réseau.



Aucune reproduction, même partielle, autres que celles prévues à l'article L 122-5 du code de la propriété intellectuelle, ne peut être faite de ce site sans l'autorisation expresse de l'auteur.
Brindtech – brind-tech.eu

Figure 1.4 : Visualisation d'un VLAN primaire 200 composé de 2 sous VLAN 201(isolated) et 202(community) [9].

1.4.8 Avantages du VLAN

Parmi les avantages liés à la mise en œuvre d'un VLAN, on retiendra notamment :

- La flexibilité de segmentation du réseau.
- La simplification de la gestion.

- Le renforcement de la sécurité.
- La régulation de la bande passante.
- Réduction de la diffusion du traffic sur le réseau [10].

1.5 Modes de connexion

Les objets connectés, comme par exemple les composants du réseau, doivent pouvoir communiquer entre eux. Pour ce faire, ils vont devoir établir une connexion, un lien entre les appareils. Le lien entre deux équipements peut-être une connexion de type filaire, infrarouge ou par ondes radio.

La connexion filaire, repose sur l'utilisation de câbles physiques pour la transmission des données, offrant une stabilité et une fiabilité inégalées, illustré par des technologies telles qu'Ethernet.

La connexion sans-fil, élimine le besoin des câbles avec l'utilisation des ondes radios, comme le Wi-Fi, apportant une flexibilité inestimable, mais avec des considérations de sécurité particulières.

1.5.1 Connexion filaire (Ethernet)

Ethernet est une technologie de réseau câblé qui a vu le jour dans les années 1970 grâce à la collaboration de Xerox, Intel et Digital Equipment Corporation. Elle est définie par les normes de l'IEEE (Institute of Electrical and Electronics Engineers). Au fil des années, Ethernet a évolué. En 1985 IEEE a modifié la norme Ethernet pour produire la norme 802.3, qui est compatible avec les normes ISO. Cette technologie opère dans la couche physique et la sous-couche MAC de la couche LDD (Liaison de Données) du modèle OSI. Elle est couramment utilisée dans les réseaux LAN et offre une variété de vitesses de transmission allant de 10 Mbps à 100 Gbps, en utilisant différents types de câbles tels que le câble Ethernet torsadé et la fibre optique. Ethernet repose généralement sur une topologie en étoile, où les appareils se connectent à un commutateur ou un routeur central, garantissant une gestion centralisée du trafic et une fiabilité de la connexion.

1.5.2 Connexion sans fil (WI-FI)

Le Wi-Fi, qui signifie "Wireless Fidelity", est un ensemble de normes et technologies de connexion sans fil qui permet à des appareils électroniques d'accéder à internet et d'échanger des renseignements entre eux, ce qui crée un réseau. Il utilise des fréquences radio pour envoyer des signaux entre les appareils.

Il existe deux modes de connexion : le mode infrastructure et le mode Ad-Hoc.

- **Le mode infrastructure :** Pour fonctionner le mode infrastructure a besoin d'un point d'accès (AP) qui peut par exemple être un routeur Wifi. Chaque ordinateur à l'aide de sa carte réseau va se connecter à cet AP. C'est en général le mode qui est utilisé chez les particuliers et entreprise.
- **Le mode Ad-Hoc :** Dans le mode Ad-Hoc, chaque ordinateur fait office d'émetteur et de récepteur. La connexion entre chaque ordinateur ne nécessite aucun matériel particulier à part une carte réseau Wifi. Ce mode est très pratique dans le cas d'une connexion rapide entre ordinateur.

Ainsi un téléphone portable, avec un accès Wifi peut devenir émetteur Wifi pour un PC Portable. Il passe en mode Ad-Hoc afin de partager la connexion internet [11].

1.6 Conclusion

Dans ce chapitre, nous avons établi les bases pour notre exploration du domaine de la sécurité des réseaux informatiques. En fournissant des informations cruciales, l'objectif de ce chapitre est de fournir à nos lecteurs une base solide et exhaustive. Cela les aidera à mieux comprendre les complexités et les défis auxquels les organisations sont confrontées dans ce monde numérique en constante mutation.

Chapitre 2

Présentation de l’organisme d’accueil, problématiques et solutions proposées

2.1 Introduction

Dans ce chapitre, nous présenterons l'organisme d’accueil, nous allons donc commencer par présenter l’entreprise « SARL Laiterie SOUMMAM » puis nous nous intéresserons particulièrement au département informatique, ainsi nous ferons une étude de l’existant pour soulever les problèmes relatifs à la sécurité du réseau de l’entreprise et enfin proposer une solution pour résoudre ces problèmes.

2.2 Présentation de la SARL Laiterie Soummam

2.2.1 Création et évolution

La Laiterie La Laiterie Soummam a été créée en 1993 à Akbou, en Algérie, et a connu une croissance significative grâce à son esprit innovant. En 1995, elle a triplé sa capacité de production, atteignant 240 000 pots par jour. En 2000, un nouveau site de production a été inauguré dans la Zone industrielle TAHARACHT, marquant une étape clé pour Soummam et permettant d'atteindre une capacité de 1 000 000 pots par jour en 2001.

En 2002, l'entreprise a acquis un nouveau terrain et construit un deuxième bâtiment pour accueillir six nouvelles lignes de production. La capacité de production a été portée à 2 400 000 pots par jour en 2003 avec la mise en service d'une nouvelle chaîne de production de fromage frais. L'expansion s'est poursuivie avec la construction d'un quatrième bâtiment en 2008, suivi d'un cinquième bâtiment en 2015, portant la capacité de production à 8 millions de pots/jour.

En 2018, Soummam a élargi sa gamme de produits en lançant des spécialités fromagères fondues et des préparations fromagères. Aujourd'hui, l'entreprise offre plus de 2 000 emplois permanents et génère plus de 10 000 emplois indirects. Elle est reconnue pour sa qualité de production et propose une large gamme de produits dans différents emballages et contenances. La Laiterie Soummam continue d'innover et de consolider sa position en tant qu'acteur majeur de l'industrie laitière en Algérie.

2.2.2 Situation géographique

La SARL LAITERIE SOUMMAM est située à la zone d'activité d'AKBOU qui contient plus de 50 entreprises agroalimentaires et considéré comme l'un des pôles économiques de la vallée de la SOUMMAM. Elle se situe aux bordures de la route nationale N°26, menant à la pénétrante de l'autoroute « est-ouest ». Elle est implantée au nord de l'Algérie à 200 km à l'est de la capitale Alger et à 60 km du chef-lieu de la wilaya de Béjaïa, grande ville côtière abritant le 2ème port commercial du pays. La figure suivante montre la localisation exacte de l'entreprise.

Figure 2.1 : Image satellitaire de la position exacte de la SARL laiterie SOUMMAM.

2.2.3 La structure de l'entreprise

SARL Laiterie Soummam est une entreprise spécialisée dans la production et la distribution de produits laitiers. Elle adopte une structure organisationnelle hiérarchique avec plusieurs départements fonctionnels, et utilise une infrastructure informatique pour soutenir ses opérations quotidiennes et faciliter la communication et la gestion des données au sein de l'entreprise. Elle utilise des applications et systèmes informatiques spécialisés pour gérer ses processus internes.

2.2.4 Organigramme de l'entreprise

L'organigramme suivant illustre l'ensemble des services de la SARL laiterie SOUMMAM

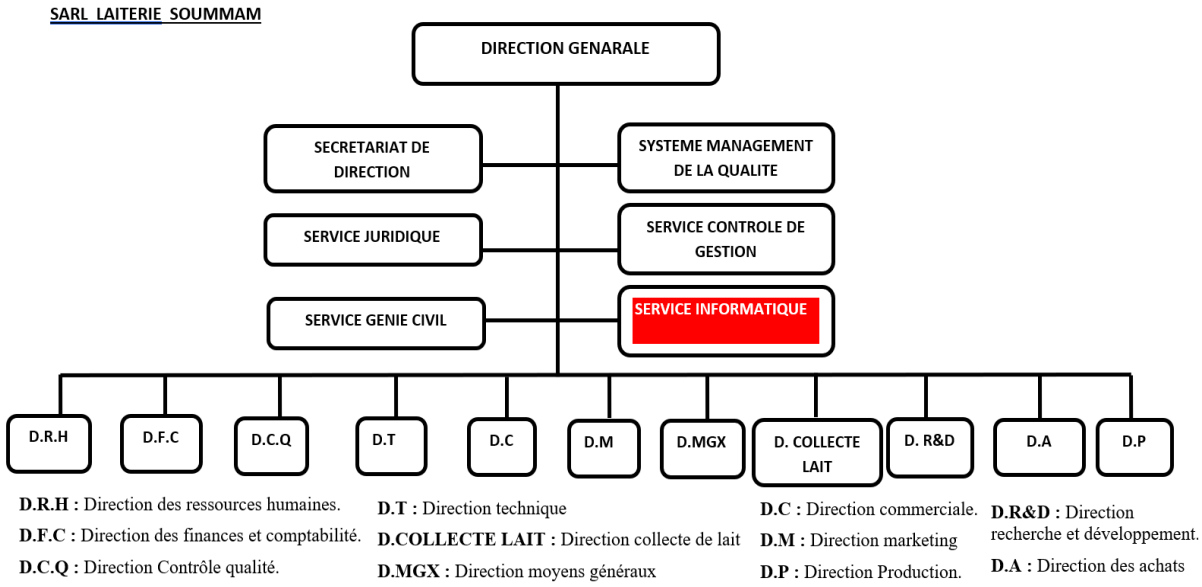


Figure 2.2 : Organigramme de la SARL LAITERIE SOUMMAM.

2.2.5 Les activités et les objectifs de l'entreprise

La Laiterie SOUMMAM est une entreprise spécialisée dans le secteur agro-alimentaire, dont l'activité principale est la production et la commercialisation de dérivés du lait. Parmi son assortiment de produits figurent les yaourts Fort, Acti+, Céréalo, B'nina, J'nina, Mamzoudj, Olé, Yago et Aladin, ainsi que les fromages frais P'tit Soummam (nature et aromatisés), les crèmes dessert et d'autres produits laitiers comme fromage frais, L'ben et Raibe. L'entreprise exerce également des activités secondaires telles que :

- La commercialisation du lait frais et dérivés ;
- Promouvoir les produits associés à l'industrie de l'alimentation humaine ;
- La collecte de lait cru (qui présente le projet le plus important pour l'entreprise) ;
- La distribution de céréales et d'aliments du bétail au niveau de la vente en gros ;
- La distribution d'outils, de fournitures et d'équipements agricoles en grandes quantités.

La figure suivante montre un exemple de différents produits fabriqué par l'entreprise :

Figure 2.3 : Les différents produits de la LAITERIE SOUMMAM [12].

2.3 Présentation du service d'accueil (Service informatique)

2.3.1 Organisation

L'organisation du service informatique d'une entreprise vari selon la taille de cette dernière. Une société extérieure s'occupe du réseau dans les petites entreprises, une personne suffit à gérer le réseau d'une entreprise moyenne, mais dans les grandes entreprises, comme dans notre cas, le service contient plusieurs personnes : à sa tête le chef de service informatique, ceux qui s'occupent de la maintenance matérielle, d'autres qui s'occupent de la maintenance logicielle et une personne s'occupe de la sécurité du réseau de l'entreprise.

2.3.2 Activité du département informatique

Ce service a la charge du parc informatique de l'entreprise. Les personnes y travaillant ont pour rôle la configuration des machines, veillent à la sécurité du réseau et des données, à la maintenance des postes informatique ainsi qu'à l'installation et la mise à jour des logiciels.

2.3.3 Expérience acquise

Notre stage au sein du département informatique de la SARL Laiterie Soummam a été une expérience riche en enseignements. Nous avons eu l'opportunité de travailler sur des aspects cruciaux de la sécurité informatique, notamment la gestion de l'Active Directory, la configuration de certificats numériques, et l'administration d'une multitude d'équipements, tels que les commutateurs, les pare-feu FortiGate, et les routeurs. L'équipe informatique nous a impressionnés par son sérieux et son organisation, ce qui a grandement contribué à notre apprentissage. Nous avons également eu l'occasion de mettre en pratique nos compétences en travaillant au sein du data center, où nous avons participé au montage et au démontage des pièces informatiques sur les ordinateurs, tout en suivant de près les bonnes pratiques en matière de sécurité et de maintenance logicielle. Cette expérience nous a inculqué une grande prudence concernant la sécurité du réseau et nous a préparés à être des professionnels compétents et responsables dans le domaine de la sécurité informatique.

2.4 Etude de l'existant

2.4.1 Architecture du réseau

La figure suivante schématise l'architecture actuelle du réseau de l'entreprise :

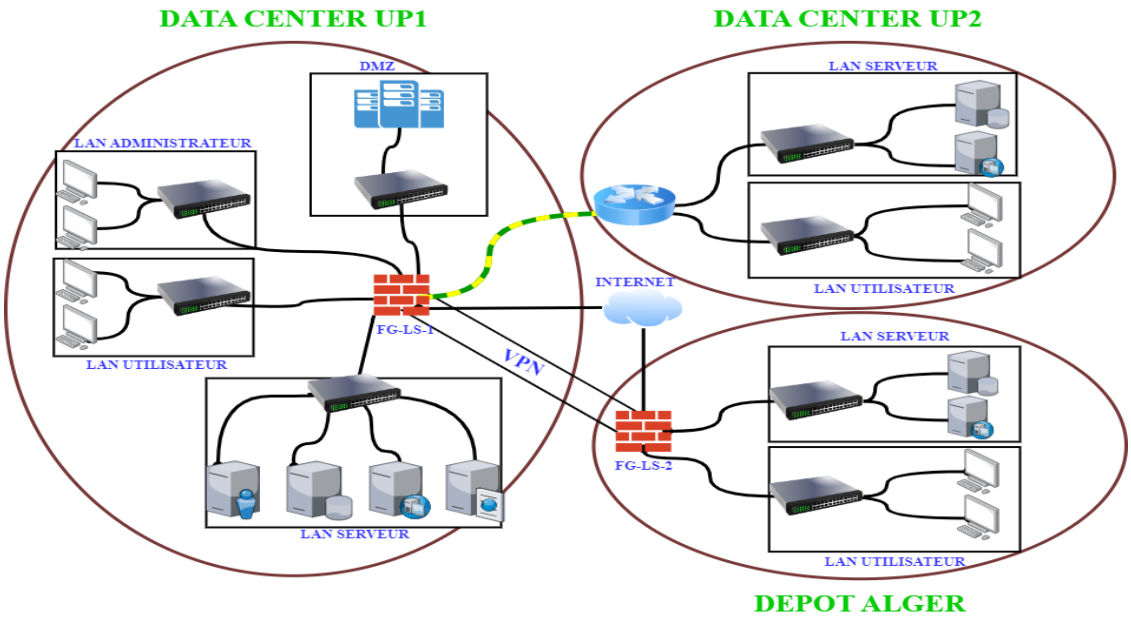


Figure 2.4 : Architecture actuelle du réseau de l'entreprise.

Le schéma architectural adopté par l'entreprise est une architecture en étoile physique, où chaque département est directement connecté au pare-feu central. Cette structure est mise en œuvre sur deux sites situés à Akbou : UP1 à Taharacht et UP2 dans la zone d'activité, qui sont reliés via une liaison en fibre optique. En outre, l'entreprise possède un dépôt à Alger.

2.4.2 Présentation du réseau

L'entreprise SARL Laiterie SOUMMAM gère aujourd'hui un réseau comptant 400 postes de travail. Pour assurer une gestion optimale de son réseau, elle combine différents types de commutateurs tels que ceux de Cisco, Mikrotik et HP. Pour répondre à ses besoins en matière de stockage et de traitement de données, elle exploite à la fois des serveurs physiques et virtuels. En parallèle, elle a mis en place divers points d'accès Wi-Fi gérés par un contrôleur Wi-Fi et soutenus par un pare-feu Fortigate. Ce dernier lui permet de protéger son réseau contre les menaces extérieures. Un Fortigate est en place au niveau du premier site, UP1, l'autre est opérationnel au dépôt d'Alger. Pour sécuriser la communication entre ces deux points, un réseau privé virtuel (VPN) de type site-à-site a été configuré via le protocole SSL. Elle a également choisi d'utiliser l'antivirus "Kaspersky Total Security" sur chaque poste de travail connecté au réseau, qui offre une protection contre plusieurs types d'attaques, notamment les malwares, les virus, le phishing et les attaques de type Man-in-the-Middle. En adoptant ces mesures de sécurité, l'entreprise renforce la robustesse de son réseau face aux menaces émergentes.

En ce qui concerne le service extranet de l'entreprise, La laiterie Soummam possède un site web accessible à l'adresse : https://www.soummam-dz.com/.

2.4.3 Inventaire des équipements matériels (hardware)

L'équipement	Nombre	La marque	Description
Serveur	30	HP Entreprise	 C'est un ordinateur puissant conçu pour répondre aux besoins de performance, fiabilité et sécurité des entreprises. Il dispose de composants matériels de haute qualité, une gestion avancée, une évolutivité flexible et des fonctionnalités de sécurité avancées, assurant une disponibilité maximale et une réduction des temps d'arrêt pour les applications et services essentiels de l'entreprise.
Pare-feu	4	Fortigate 100 E	 C'est un pare-feu nouvelle génération (NGFW) de Fortinet, leader en sécurité réseau. Il dispose de 20 ports GE RJ45, dont 2 ports WAN, 1 port DMZ, 1 port Mgmt, 2 ports HA, et 14 ports switch, avec 2 couples médias partagés (2 ports GE RJ45 et 2 fentes SFP). Le nombre maximum de FortiAP (Total / Tunnel) : 64 / 32 [13]. La SARL Laiterie SOUMMAM l'utilise avec deux appareils en mode de répartition (load balancing) de charge pour améliorer disponibilité, performances, et résilience du réseau.
Routeur	3	Cisco 1900	 C'est est une série de routeurs Cisco ISR destinés aux petites et moyennes entreprises, offrant une connectivité sécurisée et flexible avec des options de personnalisation en fonction des besoins spécifiques du réseau.
Switch	65	Cisco Catalyst 2960	 Il s'agit d'un commutateur de couche 2 du modèle OSI, il est conçu pour les entreprises, Ethernet, la vitesse de transmission 10/100/1000Mb/s, il fournit jusqu'a 48 ports, facile à configuré, stratégies de sécurité avancées, listes de contrôle d'accès (ACL).
		Mikrotk CRS328-24P-4S+	 C'est un commutateur Gigabit Ethernet de gestion avancée pour les réseaux d'entreprise. Il offre 24 ports Gigabit Ethernet PoE (Power over Ethernet) et 4 ports SFP (Small Form-factor Pluggable) + pour une connectivité optique haute vitesse. Avec ses fonctionnalités de gestion VLAN, de routage, de gestion de la bande passante et de sécurité, il garantit des performances optimales et une protection efficace pour le réseau d'entreprise.
		HP 2510G et 2530G	 Le switch HP 2510G et 2530G sont des commutateurs Ethernet de Hewlett Packard Enterprise (HPE). Ils offrent une connectivité réseau avancée, une transmission de données rapide et fiable, ainsi que des fonctionnalités de gestion et de sécurité pour

			optimiser les performances et protéger le réseau.
Points d'accès	65	TP-LINK, D-Link et Aruba	TP-LINK, D-Link et Aruba sont des dispositifs de connectivité sans fil. TP-LINK est abordable et adapté aux utilisateurs domestiques et de petites entreprises. D-Link offre des performances élevées et une sécurité avancée. Aruba est haut de gamme, conçu pour les déploiements à grande échelle, avec des performances élevées et une gestion avancée de la sécurité. 
Contrôleur WIFI	1	Aruba	Aruba est une solution de gestion centralisée pour les réseaux sans fil, offrant une connectivité sécurisée et stable. La « SARL Laiterie SOUMMAM » utilise le contrôleur virtuel Aruba Instant, basé sur le cloud, pour gérer et contrôler ses points d'accès sans fil de manière flexible. Cette solution simplifie l'administration du réseau sans fil en offrant des fonctionnalités avancées de gestion et de contrôle d'accès. 
Postes de travail	400		Ordinateurs de bureau et des laptops utilisés par les employés de la « SARL Laiterie SOUMMAM » offrant ainsi les outils nécessaires à ces personnels pour exceller dans leurs tâches quotidiennes.

Tableau 1.1 : Présentation des équipements.

La laiterie Soummam possède un site web accessible à l'adresse : https://www.soummam-dz.com/.

2.5 Problématiques

Après des séances de travail effectuée au sein de l'entreprise, avec le responsable de la sécurité, nous avons identifié les failles et problèmes du réseau local, notamment :

- La surcharge du pare-feu dû au fait que tous les équipements soient reliés directement à lui, cela implique de jouer plusieurs rôles notamment celui d'un routeur.
- Il est difficile de gérer chaque switch indépendamment, cela cause une perte de temps.
- La plupart des ports de commutateur se trouvent sur le VLAN natif (par défaut (1)), ce qui risque d'augmenter les domaines de diffusion et compromettre la sécurité, allant à l'encontre de l'objectif de la micro-segmentation du réseau avec les VLANs.
- La DMZ présente une vulnérabilité en termes de sécurité, créant une faille pour les attaques extérieures au réseau local.
- Dans des conditions qui nécessitent le télétravail, comme la période du covid 19, la connexion à distance sur le site de l'entreprise n'est pas sécurisée.

- Les informations d'identification des utilisateurs sont stocké localement sur chaque équipement réseau, cela crée un risque de compromission si un appareil est compromis.
- Aucun contrôle d'accès ni de journalisation des tentatives d'authentification pour les ports Ethernet des switchs et routeurs installés à travers les différents sites de l'entreprise, ce qui augmente les risques d'attaque par force brute ou d'usurpation d'identité.
- Absence de contrôle d'accès pour certains sites Web gourmands en bande passante qui réduit la vitesse à laquelle les employés travaillent (YouTube, Facebook, etc.).

2.6 Solutions proposées

Le défi clé d'une architecture réseau sécurisée est de contrôler l'accès aux ressources depuis le réseau local et l'extérieur tout en minimisant les vulnérabilités aux attaques ou aux fuites d'informations. Nous avons proposé des solutions pour résoudre les problèmes évoqués :

- La mise en place d'une architecture virtuelle, dans laquelle on ajoute quelques équipements tel que le switch de distribution qui permet de gérer tous les autres switchs du réseau, ainsi qu'un routeur pour configurer le routage inter-vlan et le NAT.
- Création et configuration des VLAN d'une manière plus sécurisé, avec l'utilisation du VTP et la configuration du mode trunk sur les ports des commutateurs.
- Utilisation des VLAN privé pour mieux sécuriser et isolé la DMZ du réseau local.
- Mettre en place un système d'authentification RADIUS centralisé qui permet également la gestion des autorisations d'accès et la journalisation des tentatives d'authentification.
- Optimiser la solution du pare-feu Fortigate, qui consistera à le configurer en fonction des besoins d'accès et de filtrage au réseau internet, en organisant les utilisateurs en groupes distincts. De plus établir un lien VPN entre les clients distants et le site local afin de contrôler et de sécurisé tout accès à distance au réseau local.

2.7 Conclusion

Ce chapitre nous a donné un bref aperçu de l'entreprise, en premier lieu une présentation générale, ensuite nous avons mené une étude sur le réseau existant en passant par l'architecture en place et les équipements installés, ce qui nous a permis de trouver toutes les failles ou anomalies dans le réseau. Nous avons conclu notre chapitre, en proposons une solution pour renforcer la sécurité du réseau de l'entreprise. Dans le prochain chapitre, nous entamerons les modes de sécurisation des réseaux locaux.

Chapitre 3

Modes de sécurisation des réseaux locaux

3.1 Introduction

Dans ce chapitre, nous allons étudier les modes de sécurité du LAN par niveau, et prendre le modèle OSI comme référence. Pour chaque couche nous allons présenter une ou plusieurs méthodes pour garantir une meilleure administration et une sécurité optimale. Ces méthodes vont nous permettre d'atteindre tous les objectifs de la sécurité vu précédemment, et contrer un maximum d'attaques malveillantes venant de l'extérieur ou de l'intérieure du réseau.

3.2 Modèle de conception réseaux

Il existe différents modèles de conception réseau, notamment : le modèle en étoile, le modèle en bus ainsi que le modèle hiérarchique. Dans notre solution nous avons opté pour le modèle hiérarchique pour diverses raisons : ce modèle combine les caractéristiques des deux autres modèles cités (en étoile et en bus) avec plus d'autres caractéristiques qui permettent de mieux sécuriser le réseau. Les réseaux d'entreprise privilégient souvent ce modèle hiérarchique, qui se compose de trois couches distinctes, chacune ayant des rôles définis. Sa mise en place assure l'évolutivité, une grande disponibilité et une gestion simplifiée.

La figure suivante montre un exemple de ce modèle hiérarchique qui comprend les trois couches (core, distribution et access) que nous allons définir par la suite.

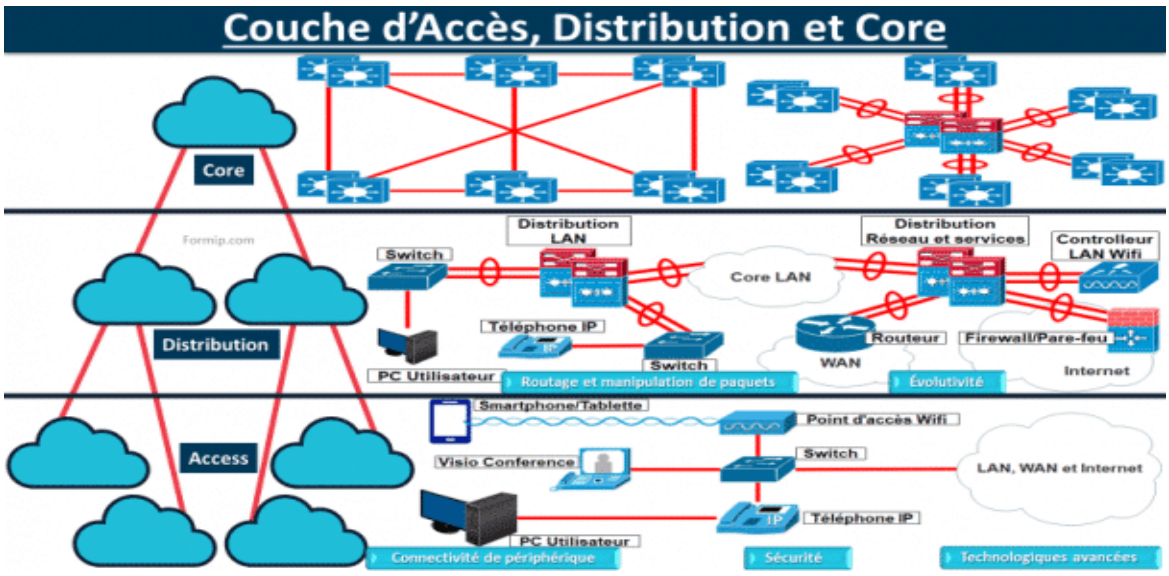


Figure 3.1 : Les trois couches core, distribution et access [14].

➢ **Définition de chaque couche**

- **Couche core :** Elle constitue le cœur du réseau, assurant une connectivité rapide entre les commutateurs de distribution et les autres réseaux d'entreprise, tout en étant adaptable aux changements. Les routeurs sont couramment employés pour cette connectivité, et l'utilisation de commutateurs et routeurs haut de gamme garantit une disponibilité et des performances optimales.
- **Couche distribution :** Elle fait le lien entre la couche d'accès et la couche cœur en agrégeant et distribuant le trafic. Elle utilise des technologies comme le VLAN et le routage pour permettre une communication sécurisée entre les périphériques de la couche d'accès et l'accès aux services réseau de manière organisée et sécurisée.
- **Couche access :** Elle relie les périphériques de l'utilisateur final (ordinateurs, imprimantes, téléphones IP) au réseau via des technologies telles qu'Ethernet et Wi-Fi, et permet la communication entre ces eux et l'accès aux services réseau. Elle comprend généralement des équipements comme des concentrateurs, des commutateurs et des ponts, avec des ports configurés selon les besoins en ports d'accès ou de tronc(trunk).

3.3 Outils d'administration des réseaux informatiques

3.3.1 AD (Active directory)

AD est un service de gestion d'annuaire développé par Microsoft. Son rôle principal est de fournir une base centralisée pour la gestion des identités et des ressources au sein d'un environnement informatique, généralement au sein d'un réseau d'entreprise.

Avec Windows Server 2008, le champ d'application d'AD s'est considérablement élargi. Il est devenu un parapluie pour un certain nombre de technologies qui vont au-delà de ce qu'AD était dans Windows Server 2000 et Windows Server 2003 [15], voici les composant que contient l'AD depuis Windows serveur 2008 :

- Services de Domaine Active Directory.
- Active Directory Lightweight Directory Services.
- Services de fédération Active Directory.
- Services de certificats Active Directory.
- Services de gestion des droits de l'Active Directory.

3.3.1.1 AD DS (Active Directory Domain Service)

Nous parlons d'un annuaire LDAP, une structure hiérarchique stockant des informations sur des objets du réseau (serveurs, groupes, comptes utilisateur, etc.). Les informations stockées peuvent être : des mots de passe, des numéros de téléphone, etc. Mais le champ d'application d'AD DS va au-delà d'un simple annuaire, c'est un outil de sécurité et d'administration puissant et flexible qui a pour objectif de centraliser deux fonctionnalités essentielles : l'identification et l'authentification des utilisateurs au sein d'un système d'information. Grâce aux stratégies de groupe (GPO), une fonctionnalité intégrée dans AD DS, nous pouvons gérer efficacement le comportement des clients finaux et leurs droits d'accès.

3.3.1.2 AD CS (Active Directory Certificate Service)

AD CS permet de déployer une infrastructure à clés publiques (PKI) pour émettre et gérer des certificats numériques qui garantissent la confidentialité avec le chiffrement, l'intégrité avec la signatures numériques et l'authentification en associant des clés de certificats à des comptes d'ordinateur ou d'utilisateur. Voici les composants clé que contient AD CS : CA (Certificate Authority), inscription des certificats, révocation des certificats, modèles de certificats et inscription web.

Une autorité de certification est chargée d'attester de l'identité des utilisateurs, d'authentifier une entité et de se porter garante de cette identité en émettant un certificat signé numériquement. L'autorité de certification peut également gérer, révoquer et renouveler des certificats [16].

3.3.2 DNS (Domain Name System)

DNS fait partie d'une série de protocoles répondant aux normes du secteur, qui inclut le protocole TCP/IP standard. Il s'agit d'une base de données hiérarchisée distribuée, utilisée sur les réseaux IP pour la résolution et le mappage des noms d'hôtes et des adresses IP aux utilisateurs et aux ordinateurs [17]. C'est-à-dire : il permet aux gens d'accéder aux sites web en utilisant des noms faciles à retenir, plutôt que de devoir se souvenir des adresses IP numériques.

3.3.3 Relation entre DNS et AD DS

AD DS utilise DNS comme mécanisme d'emplacement, les contrôleurs de domaine utilisent DNS pour se localiser les uns les autres [17].

3.3.4 Le protocole DHCP (Dynamic Host Configuration Protocole)

La saisie manuelle des paramètres de la carte réseau pose beaucoup de problèmes : un temps significatif pour la saisie, la charge administrative et les erreurs de la saisie ce qui implique des

problèmes de communication entre les différentes machines. La solution pour tous ces problèmes n'est d'autre que le service DHCP. Dans les réseaux d'entreprise, ce service est un outil couramment utilisé pour la surveillance et la gestion efficace et automatique des adresses IP, adresse et masque réseau, adresse DNS et la passerelle par défaut.

Voici un exemple illustré du fonctionnement de DHCP :

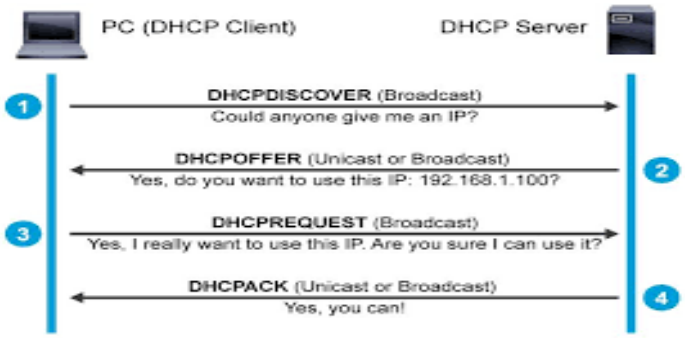


Figure 3.2 : Démonstration DHCP.

- La découverte est la première étape. Le client DHCP émet en diffusion un premier message de demande d'une adresse IP. Le type de ce message est DHCPDISCOVER.
- En fonction des serveur DHCP existant et attient par la diffusion, ces derniers offrent au client une adresse IP disponible associée une durée d'utilisation (bail), à travers un message de type DHCPOFFER
- Dans la troisième étape, le client choisi une adresse parmi les offres reçues, puis émet un DHCPREQUEST en mode diffusion pour demander l'autorisation d'utilisation de cette adresse auprès du serveur offrant cette dernière, ainsi les autres serveurs DHCP apprennent qu'ils n'ont pas été sélectionnés.
- La quatrième et dernière étape est la transmission d'un message DHCPACK par le serveur DHCP sélectionné pour accorder l'utilisation de l'adresse IP.

3.4 Outils de la sécurité des réseaux informatiques

Pour garantir la sécurité de l'infrastructure réseau d'une entreprise, il est essentiel de disposer de divers logiciels et matériels, que nous examinerons dans la suite de ce document :

3.4.1 Les réseaux privés virtuelle VPN (Virtual Private Network)

Les VPN sont un moyen fiable de protéger la communication réseau en établissant un tunnel crypté entre différents points de connexion. Leur utilisation principale est de protéger les communications Internet, permettant aux utilisateurs de se connecter à distance à un réseau

privé avec une sécurité renforcée. Voici une description détaillée du fonctionnement des VPN et de leurs différents types :

3.4.1.1 Fonctionnement

Pour établir une communication sécurisée entre les points de connexion, les VPN utilisent des protocoles de cryptage (tunneling). Cela crée un tunnel sécurisé pour l'échange de données, garantissant l'intégrité et la confidentialité des informations transmises.

Voici une schématisation du fonctionnement général des VPN :

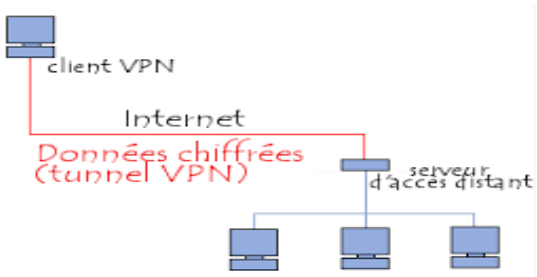


Figure 3.3 : Tunnel VPN [18].

1. L'utilisateur se connecte à Internet à partir de son ordinateur ou appareil mobile.
2. L'utilisateur lance le client VPN et entre les informations d'authentification pour se connecter au serveur VPN.
3. Le client VPN établit une connexion sécurisée (tunnel) avec le serveur VPN à travers Internet.
4. Toutes les données échangées entre l'utilisateur et le serveur VPN sont cryptées.
5. Le serveur VPN transfère les données vers le réseau privé.
6. Les données sont ensuite traitées sur le réseau privé, puis envoyées au serveur VPN.
7. Le serveur VPN crypte les données et les envoie à l'utilisateur via la connexion VPN sécurisée.

3.4.1.2 Types de VPN

Il existe principalement deux types de VPN : les VPN d'accès à distance (démontré sur la figure 3.4) et les VPN de site à site (démontrer sur la figure 3.5).

VPN d'accès à distance : Un VPN d'accès à distance (Client-to-site) permet à un utilisateur de se connecter à un réseau privé et d'accéder à ses services et ressources à distance. Cela est utile pour les entreprises et les utilisateurs individuels, car il leur permet de contourner les restrictions régionales sur Internet et d'accéder aux sites Web bloqués. Les utilisateurs VPN privés utilisent des services VPN pour améliorer leur sécurité et leur confidentialité sur Internet.

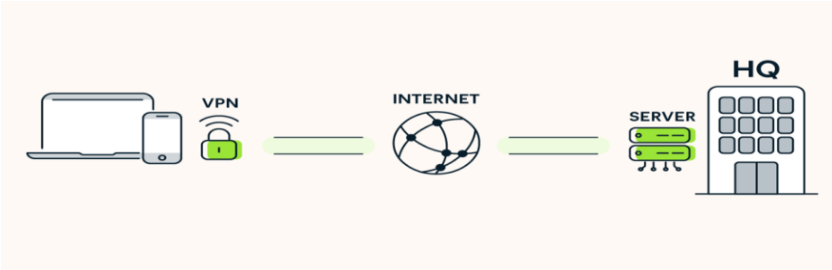


Figure 3.4 : VPN d'accès à distance [19].

VPN de site à site : Les VPN de site à site sont utilisés par les entreprises ayant des bureaux dans différentes zones géographiques pour connecter le réseau d'un site de bureau à un autre. Les VPN basés sur l'intranet relient plusieurs bureaux dans la même entreprise, tandis que les VPN extranets se connectent au bureau d'une autre entreprise. Les VPN de site à site créent un pont virtuel entre les réseaux de bureaux géographiquement éloignés, les connectent via Internet et maintiennent une communication sécurisée et privée entre réseaux. La communication entre les deux routeurs ne commence qu'après la validation de l'authentification.

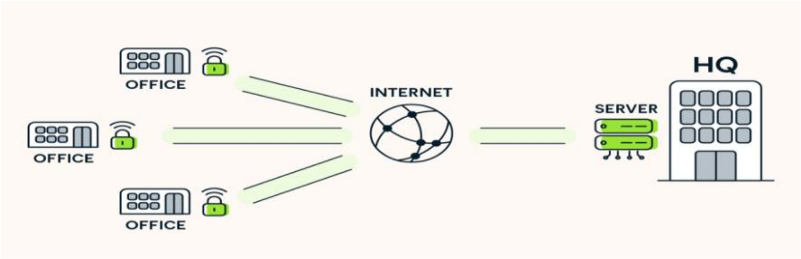


Figure 3.5 : VPN site-à-site [19].

3.4.1.3 Intérêt des VPNs

Les VPN assurent la confidentialité et la sécurité des communications en cryptant les données Ils permettent également d'accéder à du contenu en ligne restreint et à des sites Web bloqués dans diverses régions, contournant ainsi les restrictions géographiques.

3.4.1.4 Les protocoles de tunneling

Il existe différents protocoles dit de tunneling permettant la création des réseaux VPN.

3.4.1.4.1 Le protocole SSL

SSL (Secure Sockets Layer) est un protocole de sécurité développé par Netscape en 1994 qui aide à sécuriser les échanges de données entre un client et un serveur sur Internet. Il utilise un système de cryptage pour protéger les données sensibles et un certificat SSL pour assurer l'identité du serveur. Il a été remplacé par le protocole Transport Layer Security (TLS), mais est encore largement utilisé.

Les données confidentielles sont protégées pendant qu'elles transitent entre le clavier du client et le serveur du site comme si elles passaient dans un tuyau à part, comme illustré dans les 2 schémas suivants :

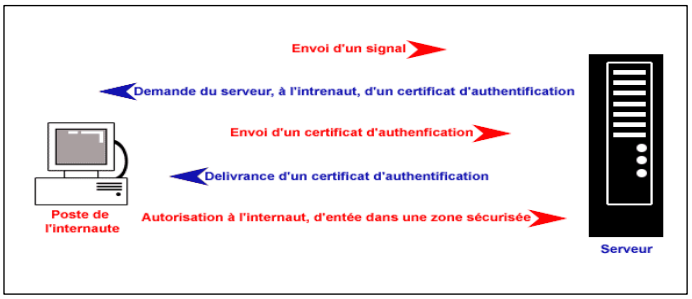


Figure 3.6 : Processus de dialogue avec SSL [20].

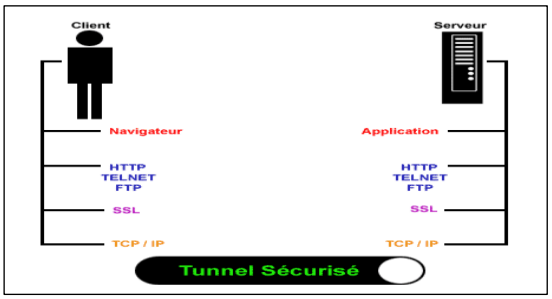


Figure 3.7 : Architecture de réseau utilisant SSL [20].

➢ Les avantages du protocole SSL

- Authentification du serveur garantie par l'usage de certificats et d'algorithme à clé publique.
- Fiabilité de la connexion. L'intégrité des messages échangés est assurée par l'ajout de code d'authentification des messages (MAC) calculé à l'aide de fonction de hachage non réversible
- Confidentialité de la connexion. Elle est assurée par un chiffrement à clé symétrique négocié au cours de la phase de dialogue initial.

➢ Les inconvénients du protocole SSL

- Coût du certificat : Il est possible d'obtenir un certificat SSL gratuit, mais ce n'est pas recommandé pour de nombreuses raisons. Selon le type de certificat que vous achetez, le prix variera un peu. Cependant, si l'on considère le niveau de sécurité supplémentaire, le coût n'est pas vraiment prohibitif pour la plupart des sites Web [21].

3.4.1.4.2 Le protocole IPSec

IPSec est un protocole de sécurité de la couche 3 qui crée des VPN sécurisés en chiffrant les données transmises via un protocole de cryptage. Il renforce la sécurité du protocole IP en assurant la confidentialité, l'intégrité et l'authentification des échanges, basé sur 3 modules clés :

- **L'IP Authentification Header (AH) :** assure l'authentification et l'intégrité en vérifiant que l'adresse source est légitime à l'aide d'un code d'authentification de message (MAC). Il garantit également l'intégrité des données pendant leur transfert.
- **L'Encapsulating Security Payload (ESP) :** permet le chiffrement des données pour rendre le contenu du paquet confidentiel. L'émetteur encapsule les données, les chiffre

à l'aide d'algorithmes tels que DES, Triple DES, RC5 ou IDEA, et ajoute éventuellement des bits de bourrage.

- **Les Associations de sécurité (SA) :** définissent les échanges de clés et les paramètres de sécurité. Elles incluent des informations sur le traitement des paquets IP, les protocoles AH et/ou ESP à utiliser, les modes de tunnel ou de transport, les algorithmes de sécurité et les clés. Les clés peuvent être échangées manuellement ou via le protocole IKE (Internet Key Exchange), qui facilite l'accord mutuel sur les SA entre les parties.

L'IPSec, malgré son impact sur le temps de traitement et le volume des paquets, garantit la sécurité des communications en offrant une protection anti-rejeu, essentielle dans des environnements axés sur la confidentialité et l'intégrité des données.

➢ Avantages du protocole IPSec

Le protocole IPSec offre une interopérabilité garantie grâce à sa normalisation par des RFC (Request for Comments), ce qui le distingue des autres solutions et lui confère plusieurs avantages, notamment :

- Économie de bande passante : IPSec intègre la compression des en-têtes des données transmises, ce qui permet de réduire la consommation de bande passante. De plus, il n'utilise pas de techniques d'encapsulation lourdes telles que les tunnels PPP sur lien SSH.
- La protection des protocoles de bas niveau tels que ICMP, IGMP, RIP, etc.
- IPSec permet une évolution continue car les algorithmes de chiffrement et d'authentification sont spécifiés séparément du protocole lui-même.

L'interconnexion IPSEC offre à l'entreprise une solution fiable, économique et rapide pour établir des connexions sécurisées entre différents sites. C'est pourquoi nous avons choisi cette solution pour relier le siège social de "SARL Laiterie Soummam" à un site distant situé à Alger. Notre solution comprend également un accès au système d'information local pour les télétravailleurs de l'entreprise grâce au protocole VPN IPSec. Cette méthode assure un contrôle et une sécurité optimaux pour ces connexions, en utilisant simplement Internet, quel que soit le débit ou l'emplacement des utilisateurs.

3.4.1.5 Les avantages et inconvénients d'un VPN

➢ Avantages

Les VPN présentent principalement les avantages suivants :

- La sécurité : Les VPN permettent de crypter les données qui transitent sur le réseau, ce qui renforce la sécurité des communications et protège contre les attaques externes.
- Accès distant : Les VPN permettent aux employés de travailler à distance en se connectant au réseau de l'entreprise de manière sécurisée.
- Les économies de couts.
- La flexibilité Dans le cas d'une entreprise ou d'une administration ayant plusieurs localisations, l'ajout d'un nouveau site se fait simplement en le connectant à Internet et en l'incluant sur le VPN d'entreprise. Il sera ainsi très facilement intégré sur l'intranet d'entreprise.

➢ **Inconvénients**

Parmi les désavantages des VPN, nous pouvons citer :

- Ralentissement possible de vitesse.
- Pas de protection contre les cookies.
- La complexité de la gestion et la mise en place d'un VPN dans certains cas.
- La dépendance à internet.

3.4.2 Les Firewalls

3.4.2.1 Concept

Un pare-feu (Firewall ou Coupe-feu) est un élément de sécurité d'un réseau qui peut être : un ordinateur, un routeur ou un matériel propriétaire. C'est une combinaison d'éléments matériels et logiciels (propriétaires, shareware ou freeware) permettant de protéger un ordinateur ou un réseau d'ordinateurs, seulement contre des intrusions extérieures provenant d'un réseau tiers (notamment Internet) en contrôlant le trafic réseau entrant et sortant. Il existe deux grandes catégories de pare-feu : Firewall de paquet et Firewall de nouvelle génération.

3.4.2.2 Firewall de paquet

Le pare-feu joue le rôle de filtre et peut donc intervenir à plusieurs niveaux du modèle OSI. Il existe deux types de base : le Pare-feu sans état et le Pare-feu avec état.

3.4.2.2.1 Firewall sans état (Stateless)

C’est le type le plus ancien et le plus basique. Il ne s’attache que pour examiner les paquets IP indépendamment les uns les autres. Il décide d’accepter ou de rejeter les paquets en fonction des informations des deux couches, réseau et transport (voir figure 3.8) (adresse IP source et destination, ports source et destination, protocoles, etc.). Ce type de firewall connais bien des limites, le manque de souplesse et la difficulté à gérer certains protocoles tel que TCP et FTP.

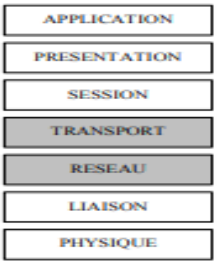


Figure 3.8 : Niveau du modèle OSI stateless.

3.4.2.2.2 Firewall avec état (Statefull)

Il s'agit d'une amélioration du pare-feu sans état qui intègre la capacité de maintenir un suivi des sessions et des connexions en utilisant des tables d'état internes. Ce pare-feu opère sur les trois couches du modèle OSI : 3, 4 et 5 (voir figure 3.9). Néanmoins, cette évolution comporte quelques inconvénients, notamment un coût plus élevé par rapport à la version sans état, une configuration plus complexe, et la gestion délicate du suivi des connexions.

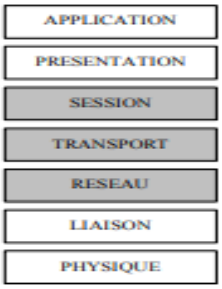


Figure 3.9 : Niveau du modèle OSI stateful.

3.4.2.3 Pare-feu de nouvelle génération NGFW

Les firewalls de nouvelle génération fonctionnent sur la couche 7 du modèle OSI (voir figure 3.10), ils offrent des fonctionnalités avancées telles que le filtrage d'applications, la prévention des intrusions, une sécurité avancée et la segmentation de réseau. Cela permet aux organisations de mieux protéger leur réseau. Le Pare-feu applicatif (proxy au mandataire) est un exemple de pare-feu NGFW.

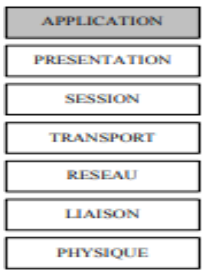


Figure 3.10 : Niveau modèle OSI NGFW.

3.5 Architecture et déploiement

Au sein d'une architecture réseau, on peut identifier divers éléments tels que des interfaces réseau, une zone démilitarisée (DMZ), un pare-feu d'application, un système de prévention et de détection d'intrusions (IPS/IDS), le réseau interne, ainsi que le réseau intranet, entre autres.

Voici un exemple de l’architecture :

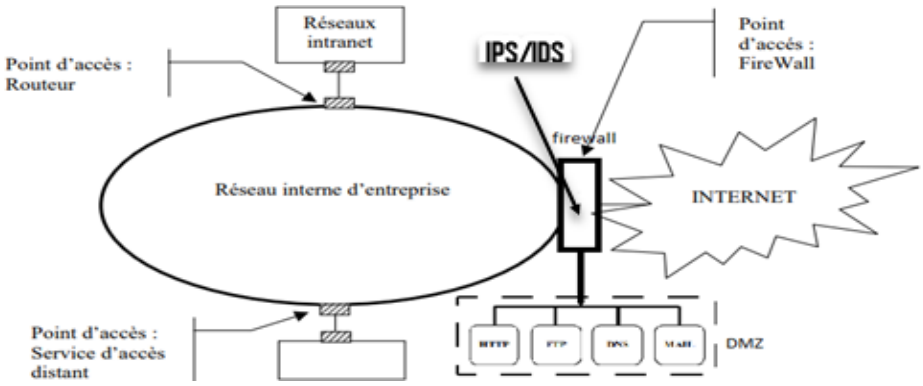


Figure 3.11 : Architecture d'un pare-feu.

3.5.1 La DMZ (Demilitarized Zone)

C'est une zone intermédiaire entre le réseau interne de l'entreprise et Internet, où les serveurs accessibles au public sont hébergés. Le firewall est placé entre la DMZ et Internet pour protéger les serveurs de la DMZ contre les attaques externes.

3.5.2 Service d'accès distant

Ces services sont couramment utilisés pour permettre aux employés d'accéder au réseau de l'entreprise à partir de chez eux ou lorsqu'ils sont en déplacement. Les services d'accès distant peuvent être configurés pour permettre l'accès à des applications spécifiques ou à l'ensemble du réseau de l'entreprise. Un point d'accès sans fil peut être utilisé pour fournir un accès Wi-Fi à des employés travaillant à distance.

3.5.3 NAT (Network Address Translation)

Le NAT est une technique de réseau, créé pour traduire les adresses IP entre les réseaux locaux et internet. Il est généralement effectué par un routeur ou une passerelle, qui agit comme un intermédiaire entre le réseau local et internet, on retrouve aussi ce mécanisme sur les pares-feux. Lorsqu'un appareil du réseau local envoie une demande à Internet, le NAT modifie l'adresse source privée par une adresse IP publique unique et routable. Une fois la réponse est reçue, il inverse la traduction en remplaçant l'adresse IP publique par l'adresse IP privée de l'appareil d'origine, on parle alors de mappage d'adresse. Le NAT agit comme une barrière entre le réseau local et Internet, masquant les adresses IP internes et rendant les appareils du réseau local moins visibles aux attaques potentielles provenant de l'extérieur.

3.5.4 IPS/IDS (Intrusion Prevention System / Intrusion Detection System)

Tout d'abord c'est quoi une intrusion ? Une intrusion signifie non seulement une pénétration des systèmes informatique, mais aussi toute tentatives d'exploitation non autorisé.

D’un côté, Un IDS est un composant matériel ou logiciel (intégrer sur le pare-feu), qui surveille le trafic réseau, les journaux de systèmes et d’autre source de données afin de détecter des activité suspectes sur l’environnement cible (un réseau LAN). Cette détection se base soit sur le comportement des machines soit sur des signatures (scénario) fournies par l'éditeur de la solution et qui doivent être mises à jour régulièrement, on parle d'une base de connaissance.

D’un autre côté, l’IPS va au-delà de la simple détection d’intrusion, il peut aussi bloquer ou modifier le trafic afin de neutraliser l'attaque, Cependant, il faut faire très attention à ne pas bloquer du trafic ou activité légitime.

3.6 Authentification RADIUS

3.6.1 Historique

Le protocole RADIUS (Remote Authentication Dial-In User Service) a été créé en 1991 par Livingston Entreprises. Il est utilisé pour l'identification des clients des FAI (Fournisseurs d'accès à Internet) pour la connexion à distance. Ses capacités de comptabilisation des accès (accounting) ont permis la journalisation des accès et leur facturation. Par la suite il est largement utilisé en entreprise pour l’identification des client finals wifi et filaire.

3.6.2 AAA (Authorization, Authentication, Accounting)

L'architecture AAA est conçue pour garantir un accès sécurisé aux ressources réseau en contrôlant l'identité des utilisateurs et leur niveau d'accès autorisé, ainsi que pour assurer la traçabilité des actions effectuées sur le réseau. Le protocole radius utilise cette architecture.

3.6.2.1 Authentication (Authentification)

L’authentification fait référence au processus de validation de l’identité de l’utilisateur en faisant correspondre les informations d’identification fournies par l’utilisateur (par exemple, un couple identifiant/mot de passe ou un certificat), à ceux configurés sur le serveur AAA. Si les informations d’identification correspondent, l’utilisateur est authentifié dans le cas contraire l’authentification va échouer.

3.6.2.2 Authorization (Autorisation)

Après l’authentification suit l’autorisation, si l’utilisateur est authentifié et la demande d’accès correspond à celle configurer sur le serveur AAA, ce dernier accorde l’accès au réseau et au ressources demandé par l’utilisateur.

3.6.2.3 Accounting (Comptabilité)

La fonction de comptabilité permet l'enregistrement d'informations, sur les ressources et service auxquels l'utilisateurs accèdent lorsqu'il est sur le réseau. En incluant la quantité de temps système utilisé, la quantité de données envoyées, ou la quantité de données reçues par l'utilisateur au cours d'une session.

3.6.3 RADIUS et TACACS+

RADIUS est l'un des nombreux systèmes du protocoles AAA, TACACS+ et diamètre appartiennent aussi à cette famille.

3.6.3.1 RADIUS

RADIUS est un protocole client-serveur permettant de centraliser des demandes d'authentification provenant des clients et des équipements réseau (comme un point d'accès wifi ou un commutateur) sur un serveur radius. A la réception de la demande le serveur consulte la base de données ou sont stocké les informations relatives à l'utilisateur, qui peut être un AD DS, une base LDAP ou une base de données SQL. Ces bases ou annuaires peuvent se trouver sur le serveur lui-même ou sur un serveur tiers.

3.6.3.2 TACACS+

Famille de protocoles AAA apparue dans le monde Unix. TACACS+ (Terminal Access Controller Access-Control System+) est la dernière version du protocole mis au point par la société CISCO. Se basant sur le même principe que radius vis-à-vis la centralisation de l'authentification.

3.6.3.3 Avantages d'utilisé TACACS+

TACACS+ crypte tous les paquets assurant une sécurité supérieure à RADIUS, qui ne crypte que les mots de passe. D'une part il permet de contrôler l'autorisation des commandes, impliquant un contrôle granulaire de l'autorisation. D'autre part il permet d'utiliser différents protocoles d'authentification et d'autorisation, ce qui améliore la flexibilité. Enfin TACACS+ prend en charge la comptabilité de commande et plusieurs niveaux de privilèges [22].

3.6.3.4 Avantages d'utiliser RADIUS

En premier lieu, RADIUS fonctionne avec pratiquement tous les routeurs et commutateurs, tandis que TACACS+ ne fonctionne qu'avec les périphériques Cisco. En second lieu il prend en charge 802.1x, le contrôle d'accès réseau est basé sur les ports, contrairement à TACACS+. En dernier lieu RADIUS est meilleur à des fins comptables [22].

3.6.4 Fonctionnement du protocole Radius

La figure suivante montre un exemple du fonctionnement de RADIUS et de la 802.1x :

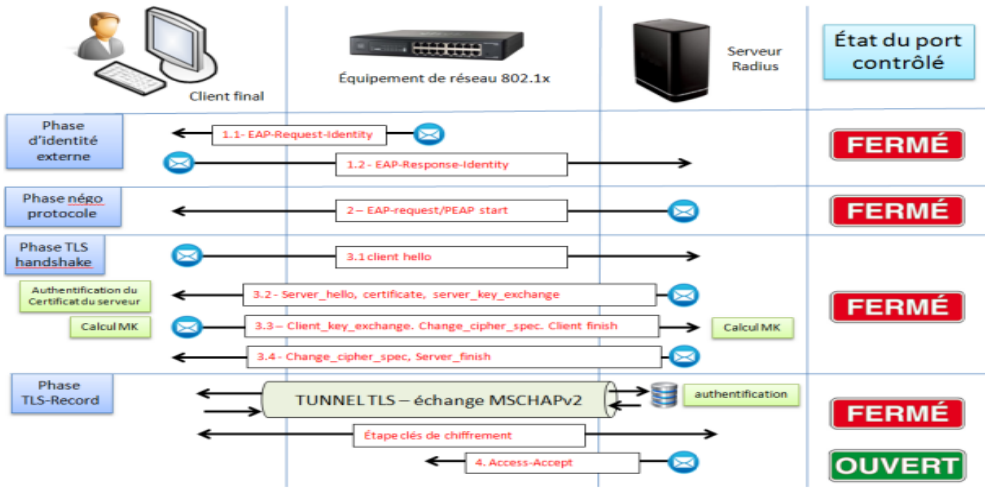


Figure 3.12 : Fonctionnement RADIUS [23].

- La première étape appelée phase d'identité externe qui consiste à l'identification du client finale ou de l'utilisateur : le client RADIUS demande au client final son identité avec la requête 1.1. Ensuite le client final répond par la requête 1.2 en envoyant son nom d'utilisateur, le client transfère à son tour la même requête vers le serveur radius.
- La deuxième étape comme son nom l'indique c'est une négociation entre le serveur et le client final par l'intermédiaire client RADIUS sur le protocole d'authentification a utilisé (PEAP par exemple).
- Après que le client final et le serveur se mettent d'accord sur le choix du protocole, suit la troisième étape comme nous le montre la figure 28 c'est l'échange entre ces deux entités via le protocole choisit. Durant cet échange Le serveur envoie son choix d'algorithme, ainsi que son certificat et sa clé publique au client final. Un tunnel chiffré est établi entre les deux pour permettre de protéger l'échange du mot de passe
- Dans La dernière étapes les échanges liés au protocole de validation du mot de passe vont être effectués dans le tunnel TLS. Ainsi si les informations fournis par le client final correspondent le serveur va donc accorder l'autorisation par la requête 4.

3.6.5 Limite Radius

- RADIUS a été conçu sur des liaisons lentes et peu sûres, c'est la raison du choix du protocole UDP.
- Son identification est basée sur le seul principe du couple (nom, mot de passe).
- Il assure un transport en clair, seul le mot de passe est chiffré par hachage.

- Il n’assure pas des mécanismes d’identification du serveur.
- Il est strictement client-serveur [24].

3.6.6 La norme 802.1x

Le protocole 802.1x est une solution standard de sécurisation de réseaux mise au point par l'IEEE en 2001. Il permet d'authentifier un utilisateur souhaitant accéder à un réseau (câblé ou Wifi) grâce à un serveur central d'authentification qui peut être un serveur RADIUS : un serveur Microsoft, Cisco ou un produit libre comme FreeRADIUS ou encore un serveur TACACS dans le monde fermé des équipements Cisco. L'autre nom de 802.1x est "Port-based Network Access Control" ou "User Based Access Control". Ce standard permet de sécuriser l'accès à la couche 2 (liaison de donnée) du réseau grâce à la gestion des ports Ethernet. 802.1x a recours au protocole EAP [23].

3.6.7 Le protocole EAP et PEAP/TLS

- EAP (Extensible Authentification Protocol) est la couche protocolaire de base de l'authentification. C’est un support universel permettant le transport de différentes méthodes d'authentification, alors que le port de connexion est fermé à toute autre forme de communication. C'est un protocole extensible, au sens où il va permettre l'évolution de méthodes d'authentification transportées, de plus en plus sûres au cours du temps. Parmi ces méthodes on trouve PEAP.
- PEAP (Protected Extensible Authentication Protocol) est un protocole de transfert sécurisé d'informations d'authentification. Il a été mis au point par Microsoft, Cisco et RSA. Il ne nécessite pas de certificat sur les postes clients, contrairement à EAP/TLS. MS-CHAP s'appuie sur PEAP
- TLS (Transport Layer Security) est un protocole de sécurité de couche transport utilisé pour établir une connexion sécurisée entre le client et le serveur
- Dans le contexte de PEAP/TLS, EAP est encapsulé dans un protocole d'authentification sécurisé PEAP, lui-même encapsulé dans une session TLS pour fournir une authentification mutuelle entre le client et le serveur.

3.7 Conclusion

Après avoir approfondi ce chapitre, nous avons pu observer les différentes techniques utilisées pour protéger un réseau local contre les attaques malveillantes. Afin d'acquérir une compréhension globale de ces méthodes et de leurs applications pratiques, nous proposons notre solution dans le prochain chapitre.

Chapitre 4

Réalisation

4.1 Introduction

A travers ce chapitre nous allons combler les failles de sécurité du réseau de l'entreprise « SARL LAITERIE SOUMMAM », grâce à la mise en œuvre de notre solution. Nous sommes en phase final de notre projet, ici nous allons détailler toutes les étapes que nous avons suivis et qui nous ont permis d'arriver au résultat final. Cela sera complété par des captures d'écran pertinentes, et en suivant une méthodologie idéale, dans le but de permettre à nos lecteurs une meilleure compréhension pour chaque étape que nous avons réalisé.

4.2 Environnement de travail (présentation des outils de travail)

Afin de concrétiser notre architecture réseau, nous avons sélectionné du matériel spécifique. Pour cela, nous avons utilisé un ordinateur ASUS Vivobook. De plus, nous avons opté pour "VMware Workstation 17 Pro" comme outil de virtualisation pour les stations de travail et les serveurs. Pour la création et la simulation de notre réseau virtuel, nous avons utilisé "Graphical Network Simulator 3". Ainsi, en combinant le matériel utilisé, GNS3 et VMware Workstation, nous avons pu mettre en place notre solution de manière efficace et adaptée à nos besoins.

4.2.1 Matériel utilisé

Afin de pouvoir configurer l'architecture souhaitée. Pour la gestion du pare-feu Fortigate et du serveur d'authentification RADIUS, nous avons utilisé un ordinateur ASUS Vivobook doté d'une mémoire RAM de 16 Go. Nous avons également choisi le système d'exploitation Windows 11 afin de garantir la compatibilité avec les environnements requis (voir figure 4.1). Ce choix de matériel et de système d'exploitation nous a permis de créer un environnement adapté à nos besoins et d'assurer un fonctionnement optimal de notre solution.

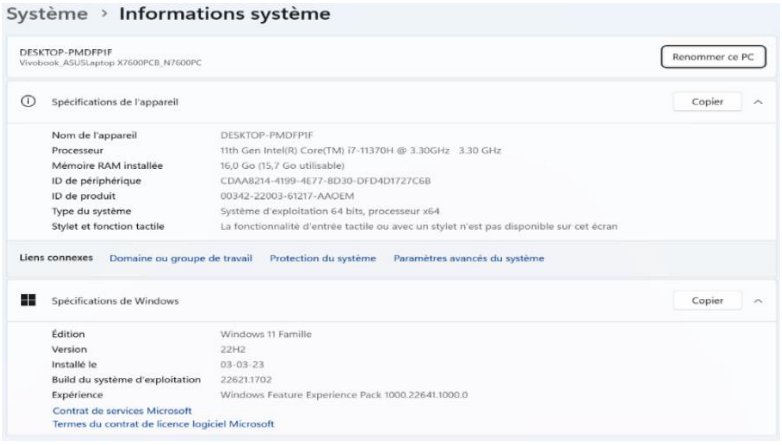


Figure 4.1 : Le PC utilisé.

4.3 Présentation des équipements matériels (Hardware)

Equipement	Modèle	Caractéristiques
Serveur	HP Entreprise	• L'architecture du serveur est conçue pour être solide et résiliente. • La gestion et l'administration ont été simplifiées. • Les mesures de sécurité ont été renforcées. • Prise en charge de la virtualisation. • La fiabilité et la stabilité du matériel.
Pare-feu	Fortigate	• Sécurité à plusieurs niveaux • Gestion centralisée • Fonction VPN • La haute disponibilité • Gestion simplifiée des politiques de sécurité
Routeur	Cisco 1900	• L'appareil dispose d'une large gamme d'options de connectivité, notamment des ports Ethernet, des ports série et des interfaces WAN. • Les fonctions de sécurité sont très avancées. • La disponibilité de modules d'extension permet l'extensibilité. • L'inclusion de fonctionnalités avancées telles que le routage dynamique, la virtualisation du réseau et la qualité de service (QoS).
Switch	Cisco Catalyst 2960	• Le modèle spécifique du système détermine le nombre de ports disponibles, qui varie de 8, 24 à 48 ports. • Les fonctionnalités de gestion des réseaux sont avancées. • La technologie qui permet la gestion à distance est entièrement prise en charge. • La technologie Power over Ethernet (PoE) est prise en charge.

Tableau 4.1 : Présentation des équipements Hadware utilisés.

4.4 Architecture proposée

Dans le cadre de ce mémoire, nous avons proposé une architecture hiérarchique à trois couches pour illustrer les outils d'administration et de sécurité couramment utilisés dans les

réseaux informatiques d'entreprises. Cette architecture comprend la couche cœur de réseau, la couche distribution et la couche d'accès, chacune ayant des besoins et des exigences spécifiques en termes de matériel, de configurations et de solutions. Bien que la mise en place de cette architecture puisse sembler complexe initialement, elle offre une efficacité accrue, une stabilité, une réflexion approfondie et une économie à long terme. Voici un schéma démontrant l'architecture du réseau que nous avons proposé :

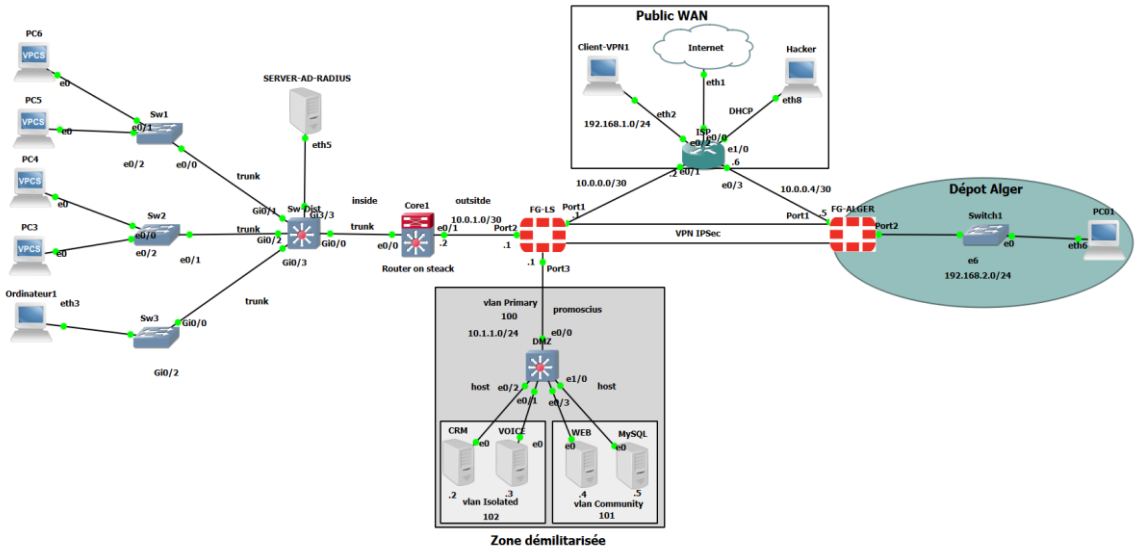


Figure 4.2 : Topologie du réseau.

4.5 Tableau d'adressage des VLANs et routage inter-VLANs

4.5.1 Tableau des VLANs

VLAN	Nom	Sous-réseau	Plage d'adresses
50	DRH	172.18.50.0/24	172.18.50.11 - 172.18.50.254
51	DI	172.18.51.0/24	172.18.51.11 - 172.18.51.254
52	DC	172.18.52.0/24	172.18.52.11 - 172.18.52.254
53	DP	172.18.53.0/24	172.18.53.11 - 172.18.53.254
54	DFC	172.18.54.0/24	172.18.54.11 - 172.18.54.254
55	DT	172.18.55.0/24	172.18.55.11 - 172.18.55.254
56	Data center	172.18.56.0/24	172.18.56.11 - 172.18.56.254
57	VoIP	172.18.57.0/24	172.18.57.11 - 172.18.57.254
58	Manager(server)	172.18.58.0/24	172.18.58.11 - 172.18.58.254
66	Native	//////////////////////	//////////////////////

Tableau 4.2 : Plan d'adressage des VLANs.

Dans ce tableau chaque VLAN est associé à un sous-réseau distinct avec une plage d'adresses IP spécifiques.

4.5.2 Routage inter-VLANs

Nous avons configuré Le routage inter-VLANs sur le router Core1, qui est relié directement au switch Sw-Dist, ce dernier contiens tous les VLANs. La technique que nous avons utilisée est "router on a stick" (routeur sur un tronçon) c'est une approche de routage inter-VLAN qui utilise un seul lien physique entre un commutateur et un routeur pour permettre le routage entre plusieurs VLAN. Pour cela nous avons choisi l'interface Ethernet 0/0 pour que tout le trafic inter-VLAN passe par ce lien.

4.6 Tableau d'adressage des équipements

Équipement	Interface	Adressage
Routeur ISP	e0/2	192.168.1.1/24
	e0/1	10.0.0.2/30
	e0/3	10.0.0.6/30
	e1/0	192.168.2.1/24
Pare-feu FG-LS	Port 1	10.0.0.1/30
	Port 2	10.0.1.1/30
	Port 3	10.1.1.1/24
	Port 10	192.168.124.10/24
Routeur Core1	e0/1	10.0.1.2/30
	e0/0.50	172.18.50.1/24
	e0/0.51	172.18.51.1/24
	e0/0.52	172.18.52.1/24
	e0/0.53	172.18.53.1/24
	e0/0.54	172.18.54.1/24
	e0/0.55	172.18.55.1/24
	e0/0.56	172.18.56.1/24
	e0/0.57	172.18.57.1/24
	e0/0.58	172.18.58.1/24
Switch Sw-Dist	e3/3	172.18.58.3/24
Switch Sw1	e0/1	172.18.55.11/24
	e0/2	172.18.54.11/24
Switch Sw2	e0/0	172.18.53.11/24
	e0/2	172.18.52.11/24
Switch Sw3	e0/1	172.18.51.11/24
	e0/2	172.18.50.11/24

Tableau 4.3 : Plan d'adressage des équipements.

4.7 Phase 1 : Installations

Pour chaque installation, nous allons illustrer puis décrire les étapes les plus importantes (il existe plusieurs étapes mais nous allons montrer que les étapes clé).

4.7.1 Installation des rôles sur le serveur

Afin de mettre en œuvre le système d'authentification RADIUS, nous avons besoin d'installer plusieurs rôles sur notre serveur, à savoir AD DS, DHCP, NPS et AD CS. L'installation est presque la même pour tous les rôles, pour cela nous allons diviser cette partie en deux : la première va contenir les étapes en commun, la deuxième quant à elle contiendra ce qui diffère.

4.7.1.1 Les étapes en commun

Dans cette partie nous allons illustrer quelques étapes clé qui sont en commun des différentes installations des rôles.

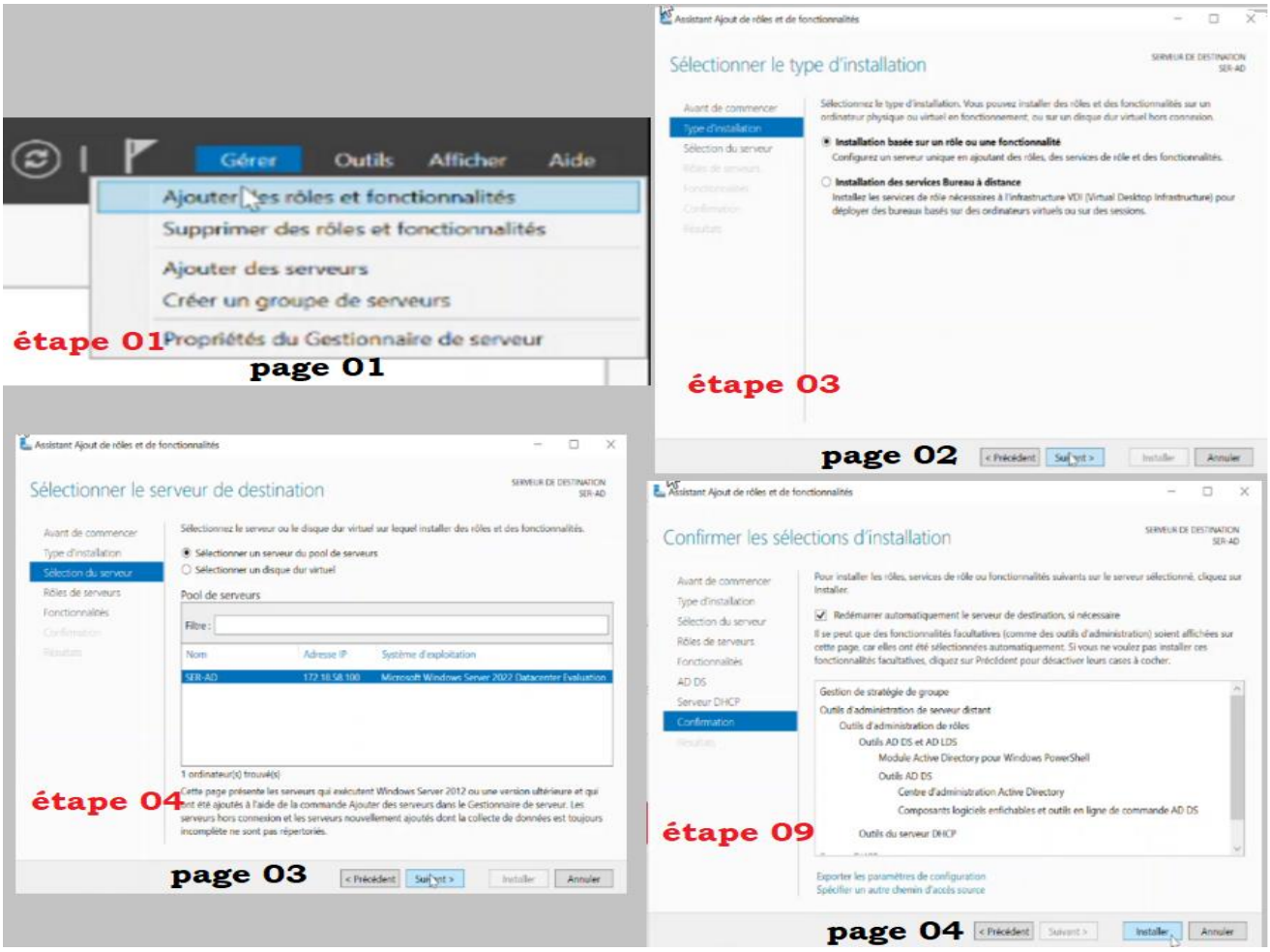


Figure 4.3 : Installation des rôles.

➢ **Description des étapes**

- Dans le gestionnaire de server nous pointons la souris sur « gérer » puis nous allons effectuer un clic droit sur « ajouter les rôles et fonctionnalités ».
- Dans La page 02 nous devons choisir le type d'installation, dans notre cas : « installation basé sur un rôle ou fonctionnalité ».

- Dans l'étape 4 nous devons sélectionner l'emplacement de l'installation, nous allons cocher la première option (sur le serveur).
- La page 04 représente l'étape de confirmation des différentes sélections d'installation.

4.7.1.2 Les étapes qui diffèrent

Selon le rôle installé, voici les étapes qui diffèrent entre les différents rôles.

a) AD DS + DHCP

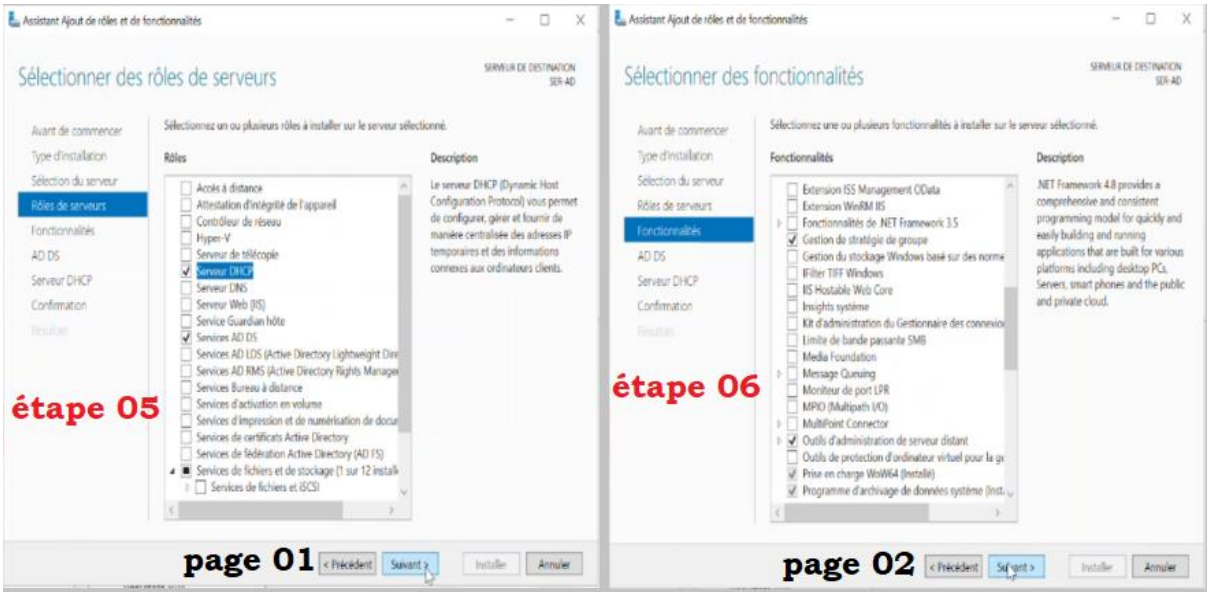


Figure 4.4 : Installation des rôles AD DS+DHCP.

➢ **Description des étapes**

- Dans la page 01 nous devant choisir le rôle à installer : DHCP pour l'attribution des adresses automatique et AD DS pour la gestion des utilisateurs.
- Dans la page 02, il est essentiel d'intégrer les fonctionnalités nécessaires, notamment la gestion de stratégie de groupe, une fonction très utile qui permet d'automatiser et d'appliquer des stratégies à des groupes spécifiques ou à l'ensemble des utilisateurs.

b) AD CS

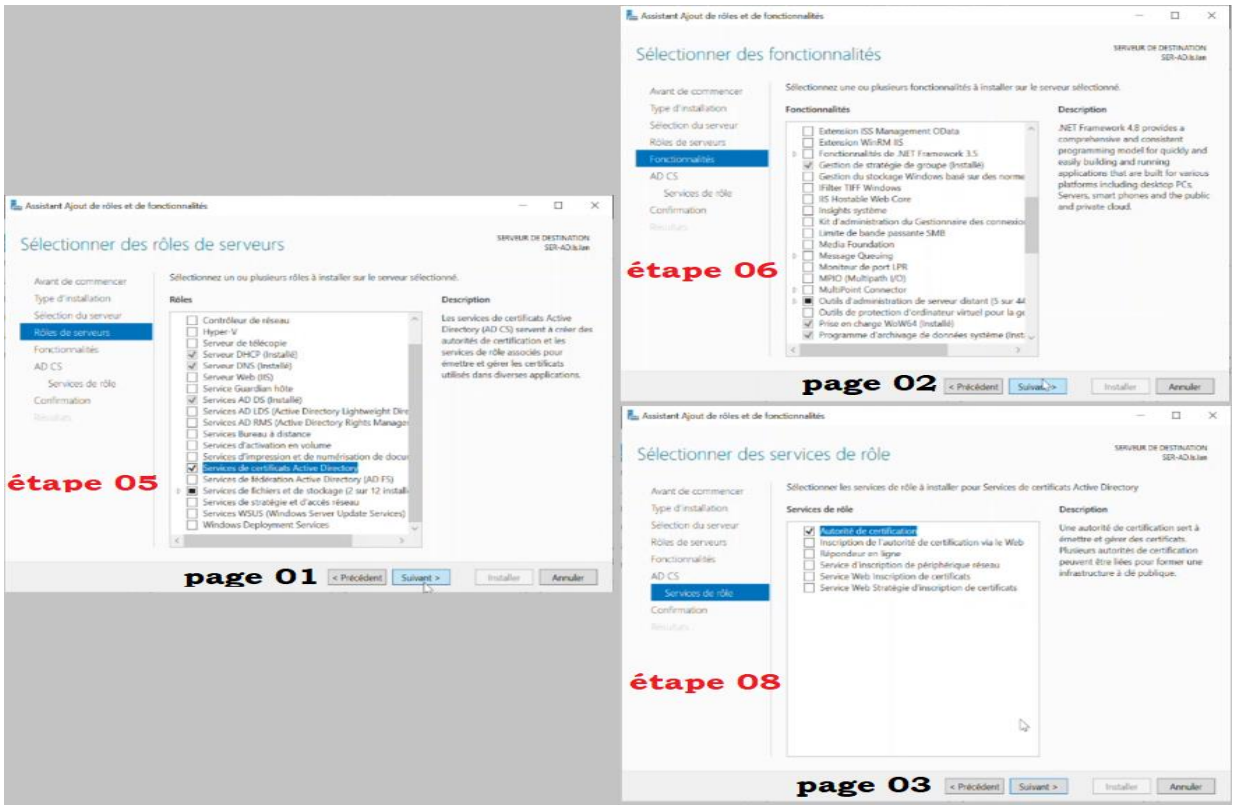


Figure 4.5 : Installation du rôle AD CS.

c) NPS (Network Policy Server)

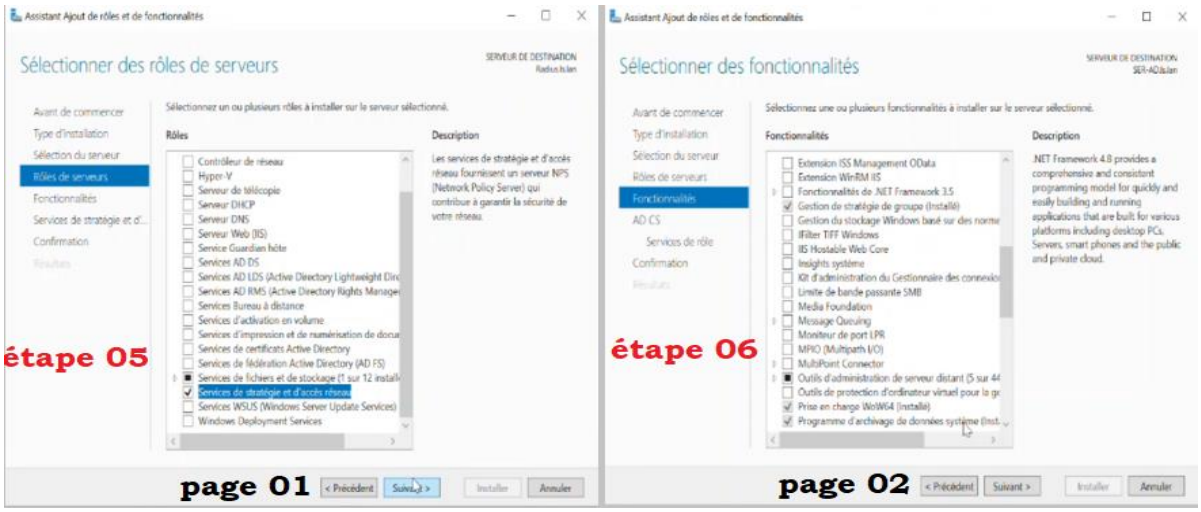


Figure 4.6 : Installation du rôle NPS.

➢ **Description des étapes**

- NPS en français services de stratégie et d'accès réseau, c'est la case que nous allons cocher dans la liste des rôles à installer qui figure dans la page 01.
- La page 02 représente la liste des fonctionnalités.

4.7.2 Configuration des rôles

Avant de conclure l'installation de certains rôles, il est impératif de les configurer préalablement. On pourrait considérer cela comme la phase finale de l'installation des rôles.

4.7.2.1 AD DS

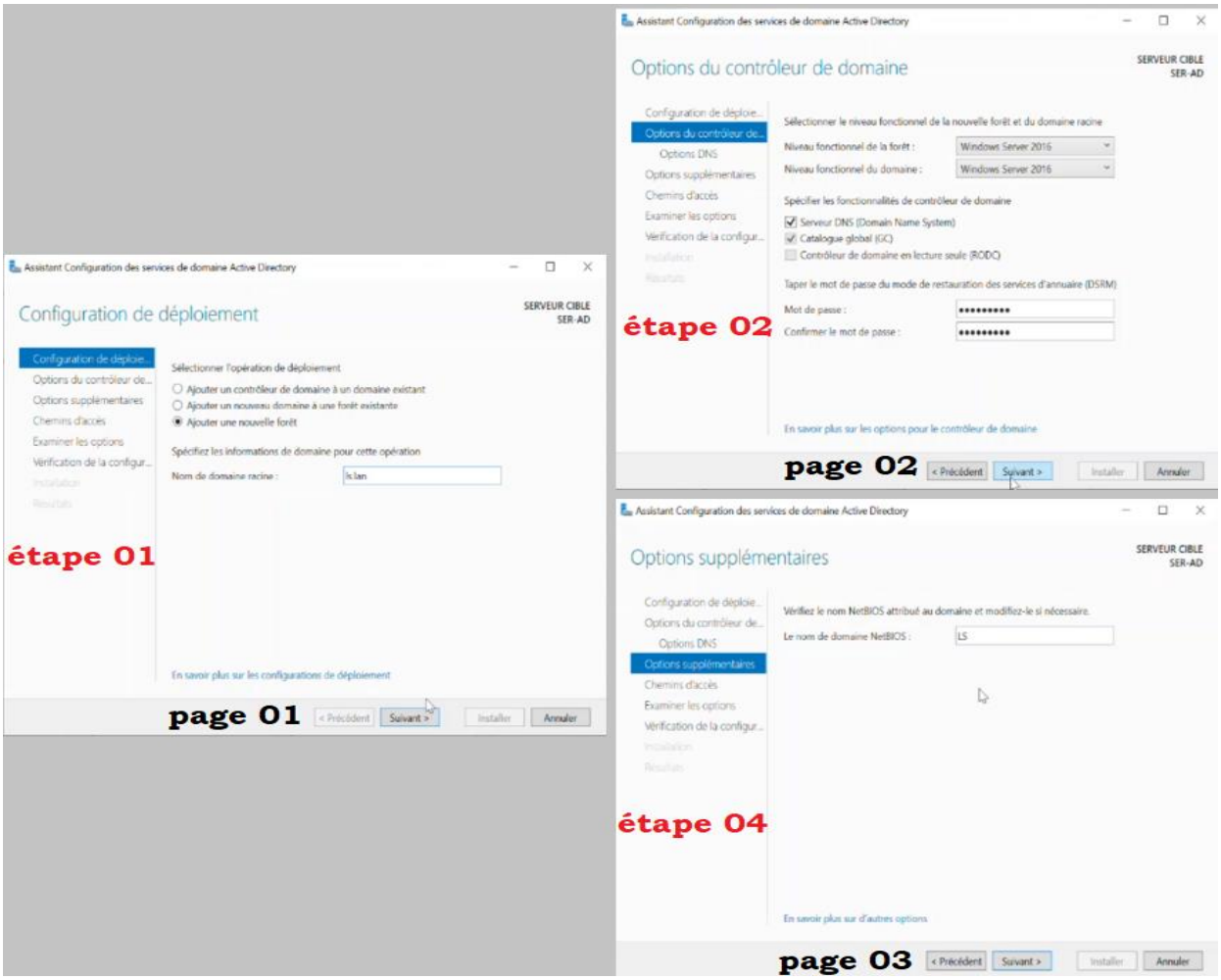


Figure 4.7 : Configuration AD DS.

➢ **Description des étapes**

- Après avoir installé le rôle AD DS, nous entamons la phase de configuration, au cours de laquelle nous créons et nommons un nouveau domaine, regroupant l'ensemble des serveurs et des postes de travail. Pour ce faire, nous choisissons l'option "Ajouter une nouvelle forêt", comme illustré sur la page 01.
- Dans la deuxième étape nous allons configurer les options du contrôleur de domaine : le niveau fonctionnel (de la forêt et du Domain), les fonctionnalités et le mot de passe.

4.7.2.2 AD CS

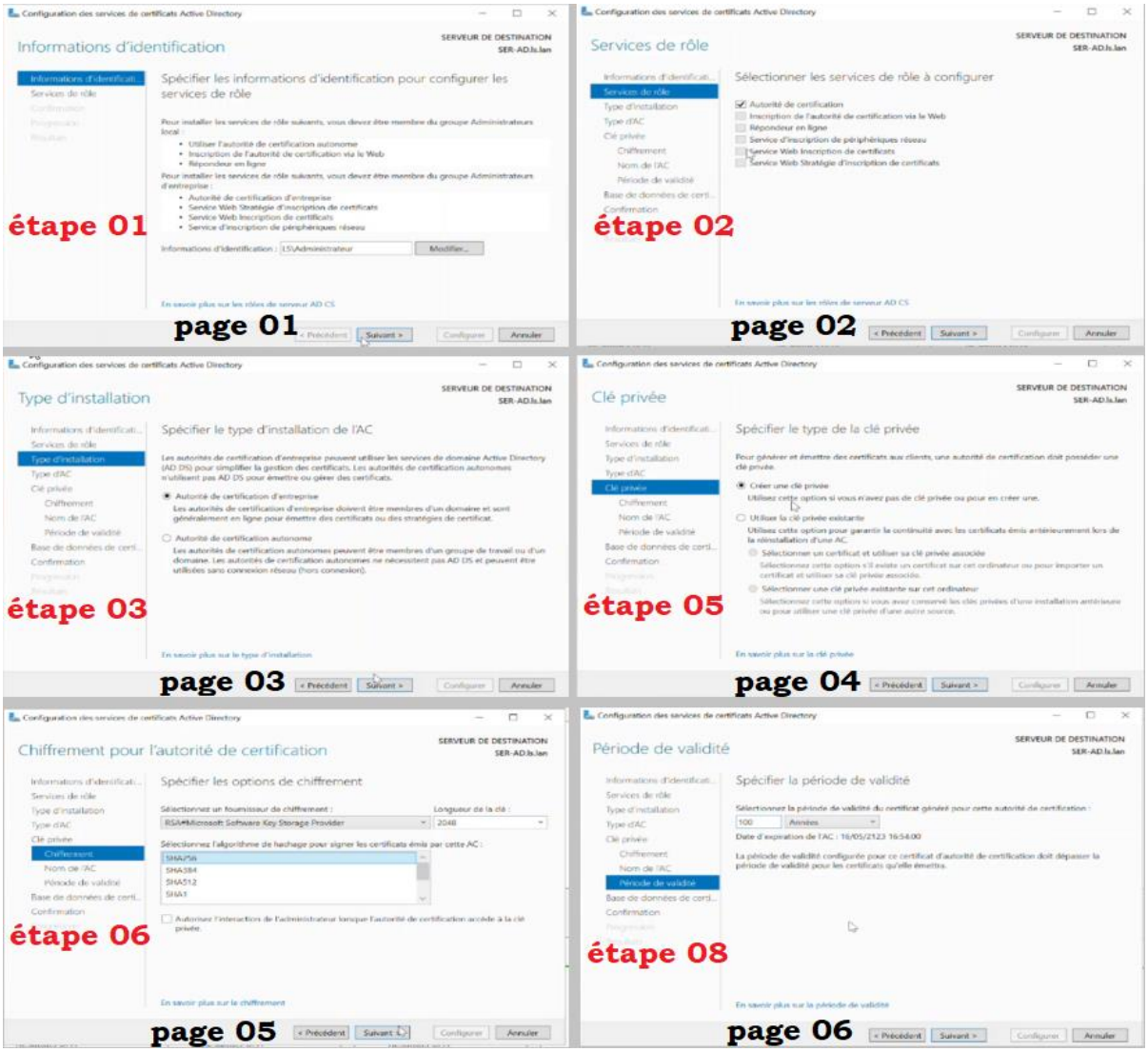


Figure 4.8 : Configuration AD CS.

➢ **Description des étapes**

- La première étape sert à s'informer et s'identifier.
- Dans la deuxième étape, nous choisissons le service de rôle à configurer, à savoir l'« Autorité de certification ».
- Pour le type d'installation sur la page 03 nous choisissons « autorité de certification d'entreprise ».
- L'attribution des certificats s'effectue grâce au chiffrement RSA, pour cela, il est nécessaire de générer une clé privée à la page 04.
- L'étape 06 est la spécification des options de chiffrement dans laquelle nous allons spécifier la longueur de la clé « 2048 » et l'algorithme de chiffrement « SHA256 ».
- Dans l'étape 08 nous devons spécifier la période de validité de l'autorité de certificat.

4.8 Phase 2 : Configurations

4.8.1 Configuration des équipements

Nous procéderons à une série de configurations pour les différents équipements du réseau local de la SARL Laiterie Soummam, notamment les routeurs et les commutateurs. Pour illustrer cela, nous fournirons un exemple de chaque configuration. Afin de faciliter ces configurations, nous avons dédié un PC à chaque VLAN, permettant ainsi une gestion plus efficace et spécifique de chaque segment du réseau.

4.8.1.1 Configuration des commutateurs

La configuration des switchs du réseau débute par la mise en place des noms pour chaque commutateur, suivie de la configuration des différents VLAN existants. Pour assurer une connectivité sécurisée, nous utiliserons des liens trunk et sécuriserons le VLAN natif. De plus, nous configurerons les interfaces des commutateurs en prenant en compte les protocoles à implémenter, tels que le protocole VTP. Enfin, nous nous pencherons sur la configuration du private VLAN dans la zone démilitarisée (DMZ), permettant ainsi de renforcer la sécurité et l'isolation des ressources dans cet environnement spécifique.

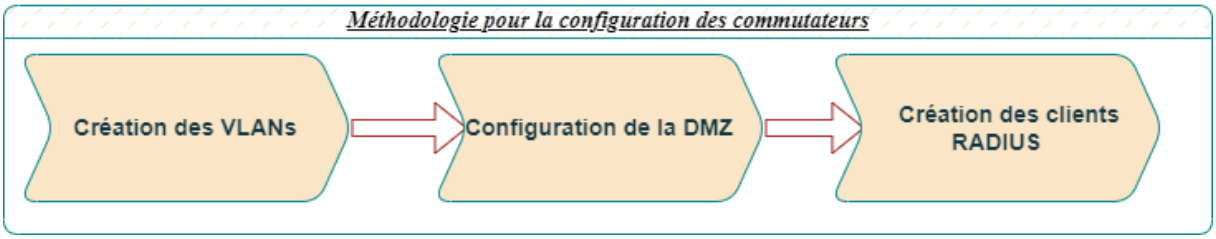


Figure 4.9 : Etapes de configurations des commutateurs.

4.8.1.2 Configuration des interfaces trunk et sécurisation du VLAN Natif

Le mode trunk sur un réseau permet le transport de trames provenant de différents VLAN. Le VLAN natif, quant à lui, représente le VLAN par défaut utilisé pour acheminer le trafic non marqué avec un identifiant de VLAN spécifique. Dans ce qui suit, nous allons configurer les interfaces trunk entre deux switchs ainsi qu'entre le switch distributeur et le routeur (pour le passage du routage inter-vlan). De plus, nous allons sécuriser le VLAN natif en l'associant au VLAN 66 afin de renforcer la sécurité au niveau 2 du réseau. Les commandes suivantes seront utilisées pour effectuer cette configuration :

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

```
Sw-Dist#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw-Dist(config)#interface range gigabitEthernet 0/1-3
Sw-Dist(config-if-range)#switchport trunk encapsulation  dot1q
Sw-Dist(config-if-range)#switchport mode trunk
Sw-Dist(config-if-range)#switchport trunk native vlan 66
Sw-Dist(config-if-range)#switchport trunk allowed vlan 50-58,66
```

```
Sw-Dist#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      1
Gi0/1       on               802.1q         trunking      66
Gi0/2       on               802.1q         trunking      66
Gi0/3       on               802.1q         trunking      66

Port        Vlans allowed on trunk
Gi0/0       1-4094
Gi0/1       50-58,66
Gi0/2       50-58,66
Gi0/3       50-58,66

Port        Vlans allowed and active in management domain
Gi0/0       1,50-58,66
Gi0/1       50-58,66
Gi0/2       50-58,66
Gi0/3       50-58,66

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       none
Gi0/1       none
```

Figure 4.10 : Configuration et vérification trunk sur le switch distibution Sw-Dist.

```
sw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw1(config)#interface ethernet 0/0
sw1(config-if)#switchport trunk encapsulation dot1q
sw1(config-if)#switchport mode trunk
sw1(config-if)#switchport trunk native vlan 66
sw1(config-if)#switchport trunk allowed vlan 50-58,66
sw1(config-if)#end
```

```
sw1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      66

Port        Vlans allowed on trunk
Et0/0       50-58,66

Port        Vlans allowed and active in management domain
Et0/0       50-58,66

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       50-58,66
```

```
sw2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw2(config)#interface ethernet 0/1
sw2(config-if)#switchport trunk encapsulation dot1q
sw2(config-if)#switchport mode trunk
sw2(config-if)#switchport trunk native vlan 66
sw2(config-if)#switchport trunk allowed vlan 50-58,66
sw2(config-if)#do wr
```

```
sw2#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       on               802.1q         trunking      66

Port        Vlans allowed on trunk
Et0/1       50-58,66

Port        Vlans allowed and active in management domain
Et0/1       50-58,66

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       50-58,66
```

```
sw3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw3(config)#interface gigabitEthernet 0/0
sw3(config-if)#switchport trunk encapsulation dot1q
sw3(config-if)#switchport mode trunk
sw3(config-if)#switchport trunk native vlan 66
sw3(config-if)#switchport trunk allowed vlan 50-58,66
sw3(config-if)#end
```

```
sw3#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       on               802.1q         trunking      66

Port        Vlans allowed on trunk
Gi0/0       50-58,66

Port        Vlans allowed and active in management domain
Gi0/0       50-58,66

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       50-58,66
```

Figure 4.11 : Configuration et vérification trunk sur les 3 switchs d'accès Sw1,Sw2 et Sw3.

4.8.1.3 Configuration d'un domaine VTP

Dans cette phase de configuration, nous allons mettre en place le protocole VTP (VLAN Trunking Protocol) sur les quatre commutateurs mit en place selon les étapes suivantes :

Le commutateur de distribution, Sw-Dist, sera configuré en tant que serveur VTP afin de distribuer les VLAN créés et leurs paramètres aux commutateurs clients.

Les commutateurs d'accès, Sw1, Sw2 et Sw3, seront configurés en tant que clients VTP pour recevoir les informations des VLANs propagées par le serveur.

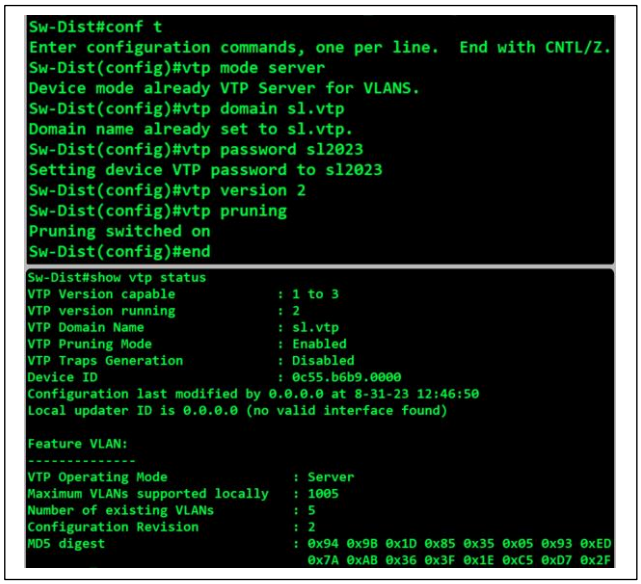


Figure 4.12 : Configuration VTP Serveur sur le switch de distribution Sw-Dist et Vérification.

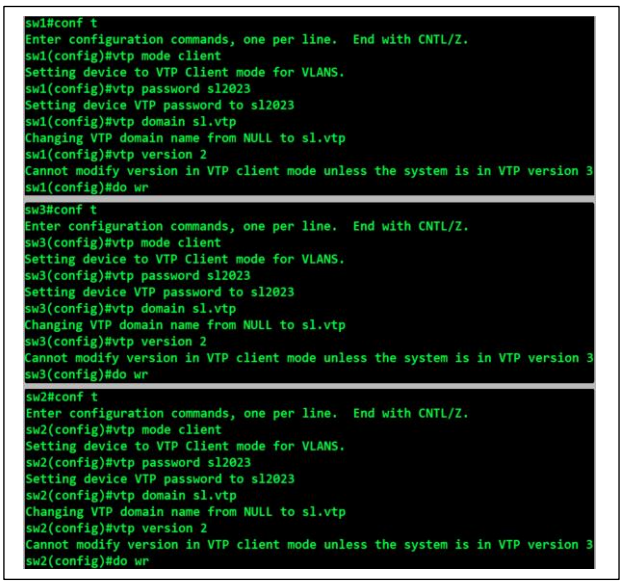


Figure 4.13 : Configuration VTP Client sur les trois switchs d'accès : Sw1, Sw2 et Sw3.

4.8.1.4 Création des VLANs

Les VLANs sont créés au niveau du commutateur Sw-Dist à l'aide des commandes illustrées dans la Figure 4.14 (nous allons procéder de la même manière pour la création du reste des VLANs de notre réseau).

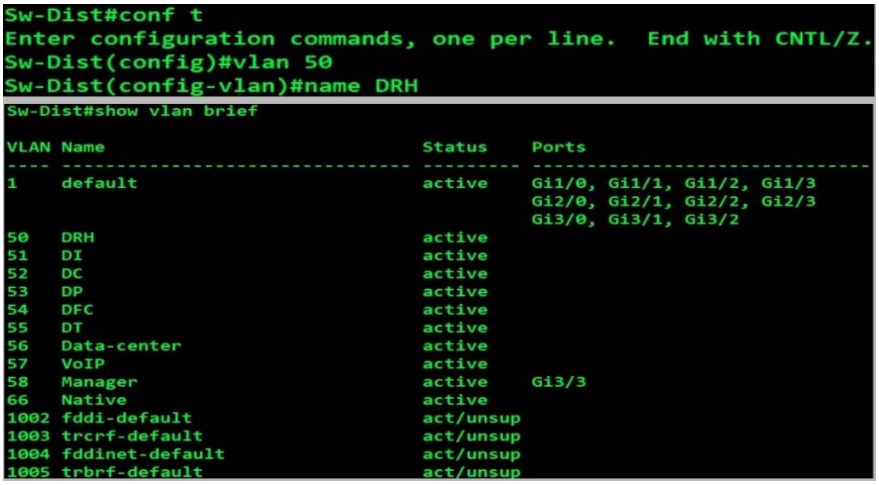


Figure 4.14 : Création du VLAN DRH et affichage des VLANs créer sur le switch Sw-Dist.

4.8.1.5 Configuration des interfaces Access

Nous allons maintenant procéder à la configuration des interfaces d'accès, qui sont configurées pour recevoir uniquement les paquets qui leur sont destinés.

La capture d'écran ci-dessous présente les différentes commandes utilisées pour configurer l'interface e0/2 du commutateur d'accès Sw1. Les mêmes étapes sont suivies pour la configuration des interfaces des commutateurs Sw2 et Sw3.

```
sw3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw3(config)#interface gigabitEthernet 0/2
sw3(config-if)#switchport mode access
sw3(config-if)#switchport access vlan 50
sw3(config-if)#end
```

Figure 4.15 : Configuration Access sur le switch d'accès Sw3.

4.8.1.6 Configuration de la DMZ

Dans cette section, nous allons mettre en place les private-VLANs en suivant la procédure suivante : Tout d'abord, nous allons configurer le VTP en mode transparent pour diffuser les VLANs que nous souhaitons ajouter sur les autres commutateurs. Cela signifie que le VTP du réseau local ne s'appliquera pas dans la DMZ, mais laissera les VLANs passer vers un autre VTP. Ensuite, nous créerons nos VLANs (100 pour le primary, 101 pour le community et 102 pour l'isolated). Enfin, nous configurerons les interfaces (Host et Promiscuous) du switch DMZ.

```
DMZ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DMZ(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
DMZ(config)#vlan 100
DMZ(config-vlan)#private-vlan primary
DMZ(config-vlan)#private-vlan association 101,102
DMZ(config-vlan)#exit
DMZ(config)#vlan 101
DMZ(config-vlan)#private-vlan community
DMZ(config-vlan)#exit
DMZ(config)#vlan 102
DMZ(config-vlan)#private-vlan isolated
DMZ(config-vlan)#exit
```

Figure 4.16 : Création du priavte-VLAN.

```
DMZ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
DMZ(config)#interface range ethernet 0/1-2
DMZ(config-if-range)#switchport mode private-vlan host
DMZ(config-if-range)#switchport private-vlan host-association 100 102
DMZ(config-if-range)#exit
DMZ(config)#interface range ethernet 1/0, ethernet 0/3
DMZ(config-if-range)#switchport mode private-vlan host
DMZ(config-if-range)#switchport private-vlan host-association 100 101
DMZ(config-if-range)#exit
DMZ(config)#interface ethernet 0/0
DMZ(config-if)#switchport mode private-vlan promiscuous
DMZ(config-if)#switchport private-vlan mapping 100 101,102
DMZ(config-if)#end
```

Figure 4.17 : Configuration des interfaces Host et Promiscuous.

4.8.1.7 Configuration des clients Radius

- Configuration des services de sécurité AAA sur le switch sw3 :

La figure suivante montre un exemple de création et de configuration d'un nouveau model AAA sur un switch (sw3) qui est client radius

```
sw3(config)#aaa new-model
sw3(config)#aaa authentication dot1x default group radius
sw3(config)#aaa authorization network default group radius
```

Figure 4.18 : Configuration AAA sur le switch sw3.

- Spécification des informations à propos du serveur radius :

```
sw3(config)#radius server radius
sw3(config-radius-server)#address ipv4 172.18.58.100
sw3(config-radius-server)#key 123456
sw3(config-radius-server)#exit
```

Figure 4.19 : configuration du serveur radius.

Nous avons spécifié sur le commutateur sw3 le nom de notre serveur RADIUS (radius), ensuite son adresse IP (172.18.58.100) et la clé partagée (123456) entre le serveur RADIUS et le client RADIUS.

- Configuration de la norme 802.1x sur le switch :

```
sw3(config)#dot1x system-auth-control
sw3(config)#interface gigabitEthernet 0/2
sw3(config-if)#switchport nonegotiate
sw3(config-if)#authentication port-control auto
sw3(config-if)#dot1x pae authenticator
sw3(config-if)#authentication host-mode multi-domain
sw3(config-if)#end
```

Figure 4.20 : Configuration DOT1X sur le switch sw3.

La figure précédente montre un exemple de configuration de la norme 802.1x sur le switch « sw3 » Afin de permettre la communication entre le switch et l'équipement terminal. Tout d'abord nous avons activé la 802.1x ensuite sur l'interface gigabitEthernet 0/2 nous avons désactivé toute autre négociation sur le port, nous avons également configuré les paramètres d'authentification notamment le port-control (auto), ainsi que le host-mode (multi-domain) afin de permettre l'authentification de plusieurs VLAN.

4.8.1.8 Configuration des routeurs

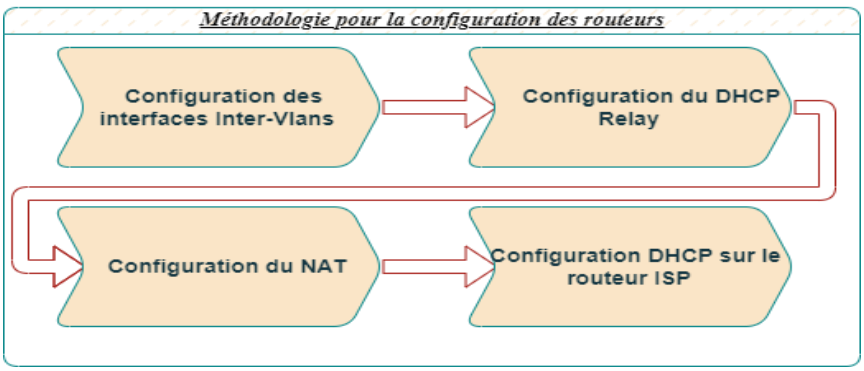


Figure 4.21 : Etapes de configurations des routeurs (Core1 et ISP).

4.8.1.9 Configuration du routeur core1

Après avoir configuré les commutateurs de notre réseau local, nous passerons à la configuration du routeur-on-stick Core1, connecté au commutateur de distribution du LAN. L'objectif est d'établir une communication entre les VLANs (routage inter-vlan). Dans ce scénario, les VLANs utilisent un même port physique du routeur, qui est divisé en plusieurs interfaces virtuelles. Pour chaque sous-interface, nous les avons encapsulées avec le protocole 802.1q en spécifiant l'ID du VLAN correspondant. Ensuite, nous leur avons attribué une adresse IP, un masque et avons configuré un DHCP Relay avec l'adresse de notre serveur DHCP. Cela garantit que seul le serveur DHCP situé dans le VLAN 58 attribuera les adresses IP. Enfin, nous passons à la configuration du NAT. Cette étape vise à traduire les adresses IP privées du réseau local en adresses IP publiques, permettant ainsi une communication sécurisée avec des réseaux distants de l'entreprise. Nous avons choisi de configurer le NAT au niveau du routeur (Core1) afin de ne pas surcharger le pare-feu. Toutes ces configurations sont présentées en détail dans les figures suivantes :

```
Core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core1(config)#interface ethernet 0/0.50
Core1(config-subif)#encapsulation dot1Q 50
Core1(config-subif)#ip address 172.18.50.1 255.255.255.0
Core1(config-subif)#ip helper-address 172.18.58.100
Core1(config-subif)#end
```

Figure 4.22 : Configuration du routage inter-vlan pour le vlan 50 et création de l'agent Relay DHCP pour cette étendue.

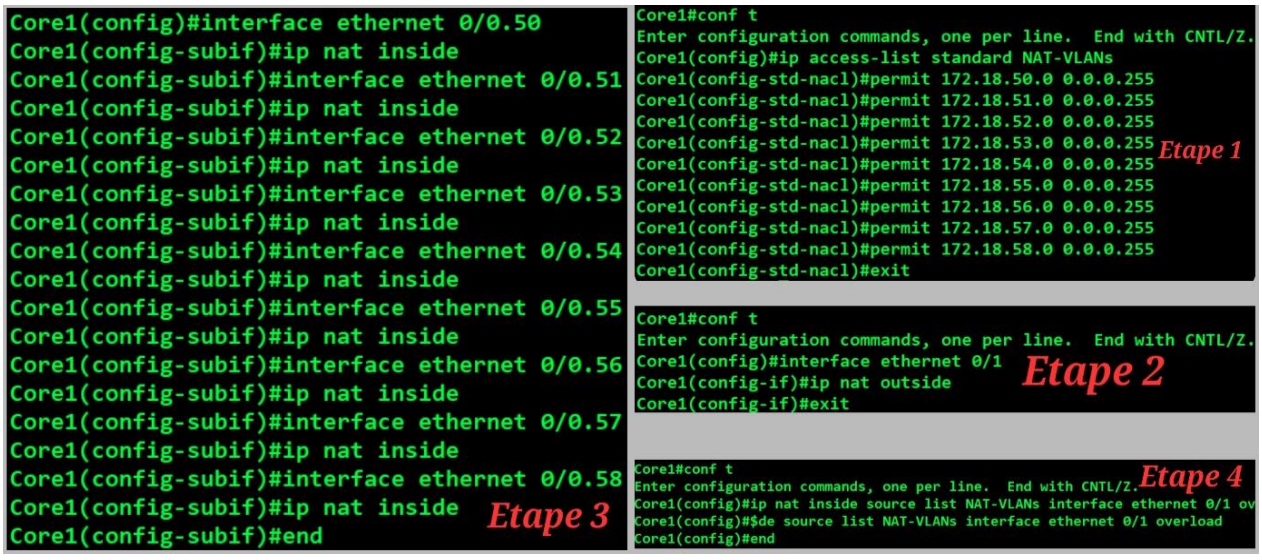


Figure 4.23 : Configuration du NAT au niveau du routeur Core1.

4.8.1.9.1 Configuration du routeur R1 (ISP)

Le routeur R1 joue le rôle de fournisseur de services Internet (ISP) dans notre réseau. Il permet à notre réseau local d'accéder à Internet et de profiter des services offerts par notre fournisseur d'accès Internet. Nous allons configurer ce routeur afin de connecter les clients distants de notre

entreprise à notre réseau local grâce à des connexions VPN. Pour ce faire, nous allons configurer le service DHCP pour les réseaux locaux distants et ceci après avoir effectué les configurations de base tel que la configuration des interfaces liées aux pares-feux de Béjaia et celui d'Alger.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
R1(config)#ip dhcp pool lan
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
R1(dhcp-config)#end
```

Figure 4.24 : Configuration DHCP dans le routeur R1(ISP).

4.8.2 Configuration du pare-feu fortigate

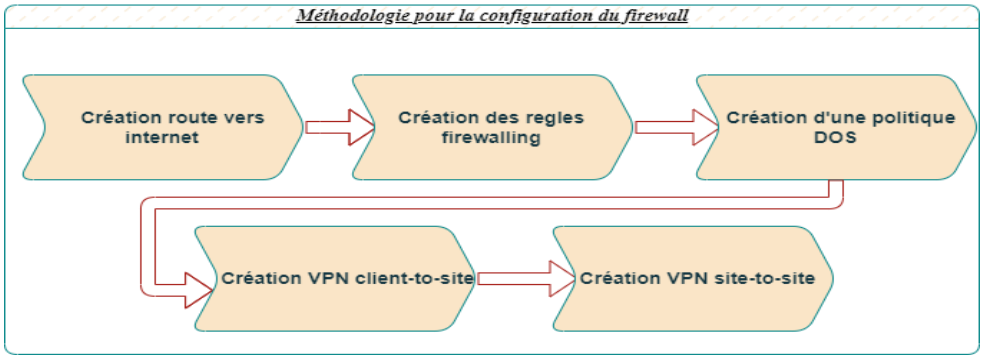


Figure 4.25 : Etapes configurations sur le pare-feu.

4.8.2.1 Mise en place

Une fois la configuration de base est terminée (tel que l'attribution des noms aux deux pare-feux déjà installés, ainsi que la configuration des interfaces des ports existants), on garde Fortigate allumé et on accède à l'interface Web. La figure en dessous montre que notre connexion LAN est bien configurée. Fortigate connecté sur l'adresse 10.0.1.1.

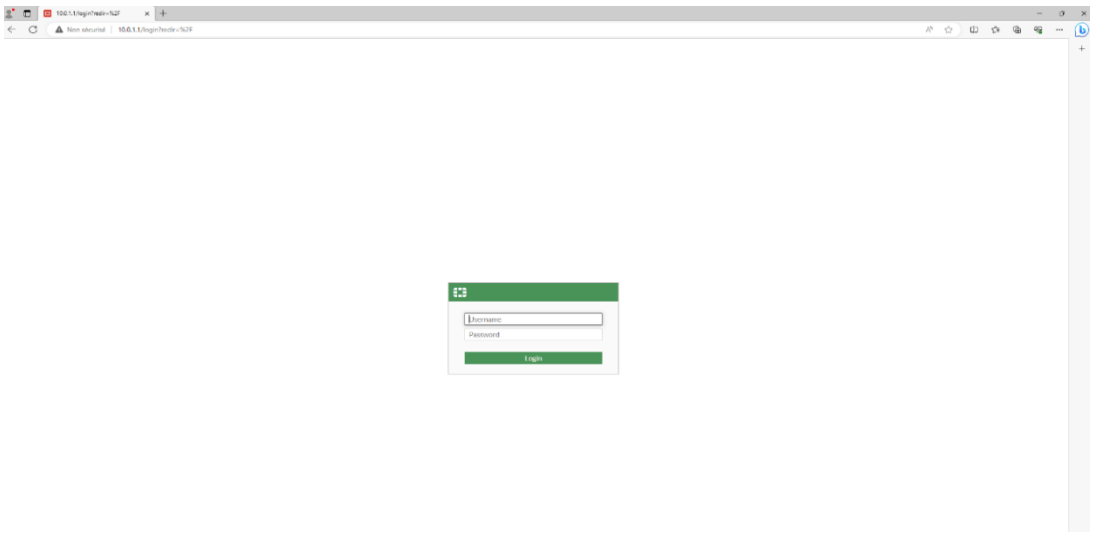


Figure 4.26 : Portail de connexion du fortigate.

4.8.2.2 Création route vers internet

Dans cette étape, nous mettrons en place une route statique vers Internet. Il s'agit d'une route par défaut qui permettra aux utilisateurs du réseau local de se connecter et d'accéder à Internet.

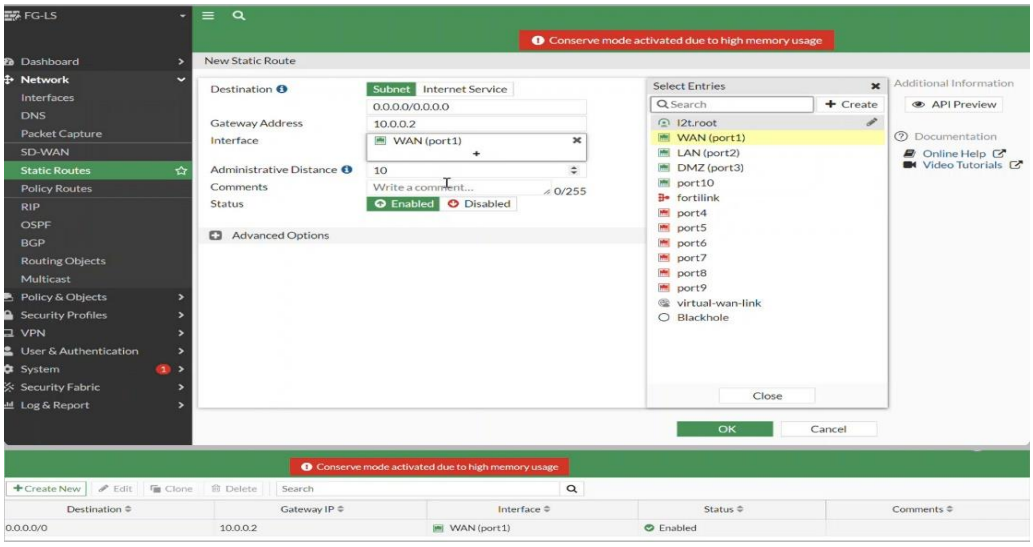


Figure 4.27 : Routage vers Internet et affichage de la route créer.

4.8.2.3 Création de la règle de pare-feu (firewalling)

Dans cette étape, nous configurons une règle de politique nommé « Policy-internet » qui autorise l'accès à Internet. Par défaut, tous les accès sont refusés (implicit deny). Pour ceci nous allons donc spécifier que l'interface d'entrée est le LAN et l'interface de sortie est le WAN. Cette règle s'applique à tous les VLAN (réseaux) et leur permet d'accéder à toutes les adresses. La règle est active en permanence (always) pour permettre une connexion à tout moment. Tous les protocoles sont autorisés (ALL). Les autres configurations du Fortigate sont laissées par défaut.

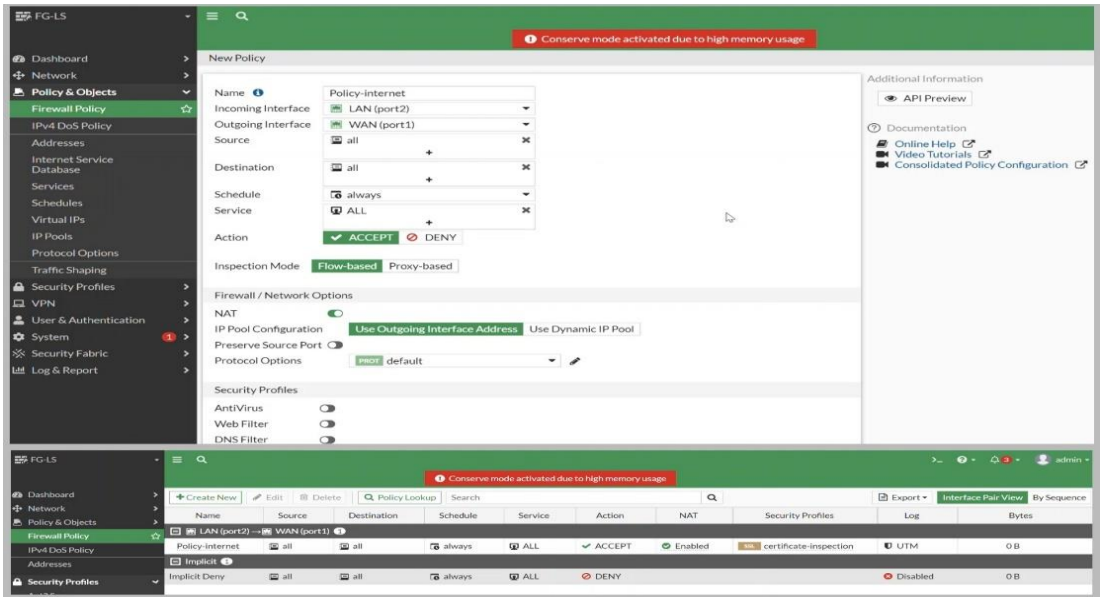


Figure 4.28 : Règle firewall pour autoriser à Internet et affichage de la politique créer.

4.8.2.4 Création d'une politique DOS

Afin de prévenir et de bloquer les attaques visant à perturber notre réseau, nous avons mis en place une politique DOS IPv4 sur notre pare-feu. La configuration de cette politique est illustrée dans la figure ci-dessous.

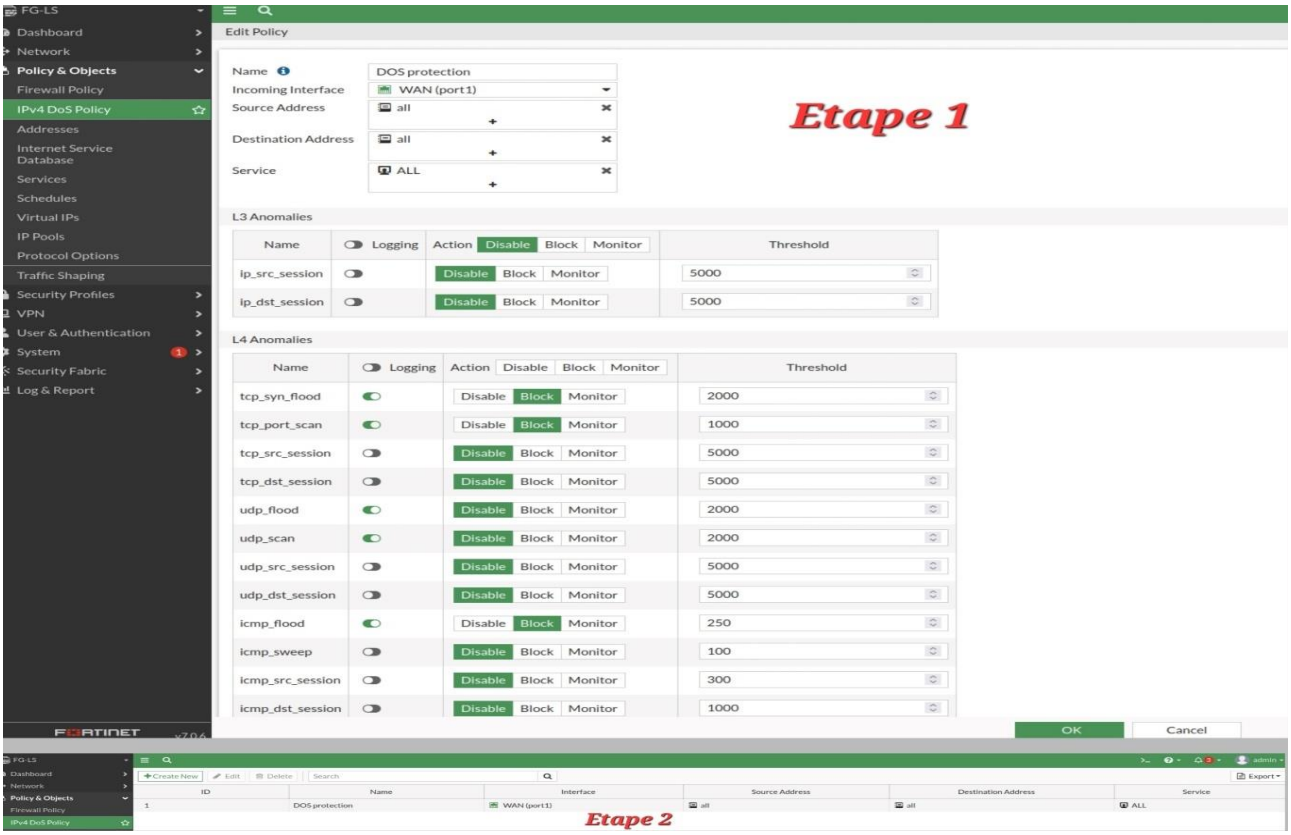


Figure 4.29 : Création d'une politique DOS et affichage.

Dans la première étape, nous avons défini le nom de la politique (DOS protection), spécifié l'interface à laquelle elle s'applique (por1), et activé les types d'attaques que nous voulons contrer, à savoir tcp-syn-session, tcp-port-scan, udp-flood, udp-scan et icmp-flood. La deuxième étape est l'affichage de la politique créée dans l'étape 1.

4.8.2.5 Création d'un VPN IPSec pour client-to-site

Dans cette étape, nous réalisons différentes actions. Pour configurer le portail VPN-SSL, nous commençons par désactiver la redirection, ce qui permet aux clients d'accéder directement au portail. Ils peuvent y télécharger des applications et bénéficier de fonctionnalités telles que le monitoring. De notre côté, nous avons également accès à ces fonctionnalités. Nous activons la fonction de téléchargement de FortiClient, facilitant ainsi l'installation de FortiClient sur les appareils des clients. Cela leur permet de se connecter de manière sécurisée et à distance au réseau local de l'entreprise en utilisant FortiClient (voir Figure 4.30).

Ensuite nous mettons en place notre tunnel IPSec. Tout d'abord, nous créons un nouveau tunnel IPSec de type client à site que nous appelons "vpnctsIpsec". Nous configurons la clé privée de bout en bout pour assurer la sécurité du tunnel. Ensuite, nous paramétrons notre VPN en utilisant le chiffrement DES et l'authentification SHA256 dans la phase 1 (phase d'authentification), ainsi que les algorithmes DES et SHA384. Nous utilisons le groupe 5 de Diffie-Hellman avec une longueur de 1024. Ces paramètres s'appliquent également à la phase de l'ESP (phase 2) (voir Figure 4.31). Par la suite, nous créons des groupes qui pourront se connecter via le VPN-IPSec en leur attribuant le portail VPN-IPSec créé au début. Plus spécifiquement, nous créons le groupe "VPN-LS" et ajoutons les deux utilisateurs (membres) qui auront accès au VPN-SSL (voir Figure 4.32).

Enfin, nous établissons une règle de firewalling dans laquelle nous désactivons le NAT afin de garantir la traçabilité des clients utilisant leurs adresses IP. Nous surveillons également les sessions des clients et générons des logs pour recevoir des notifications sur leurs activités lorsqu'ils se connectent à distance (voir Figure 4.33).

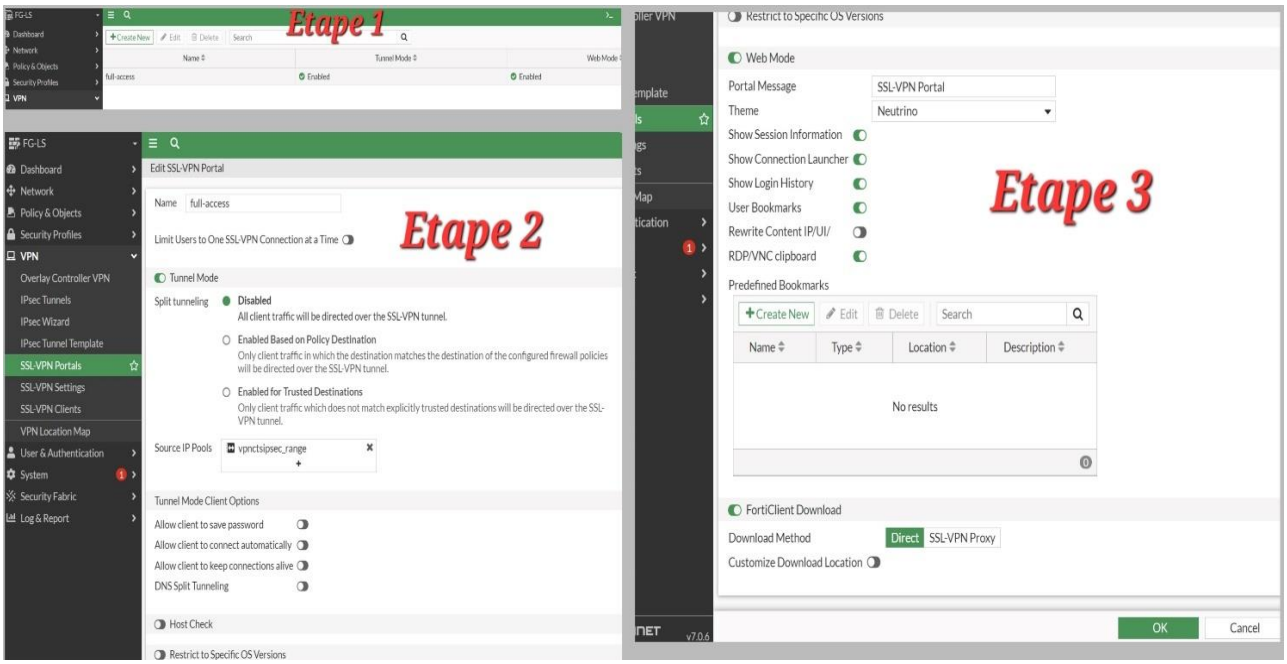


Figure 4.30 : Déctivation de la redirection et activation de FortiClient Download.

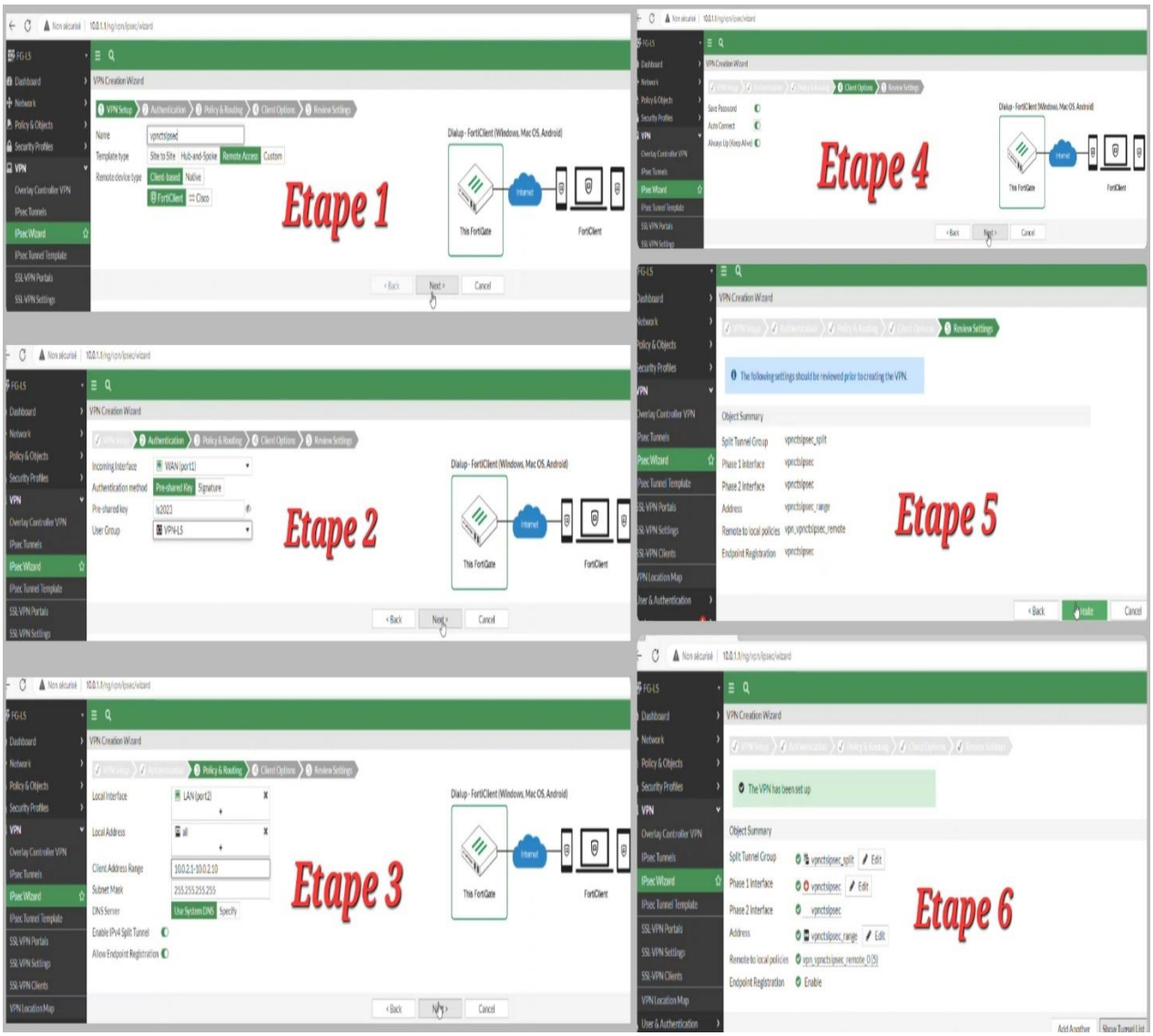


Figure 4.31 : Création tunnel IPSec client-to-site et affichage.

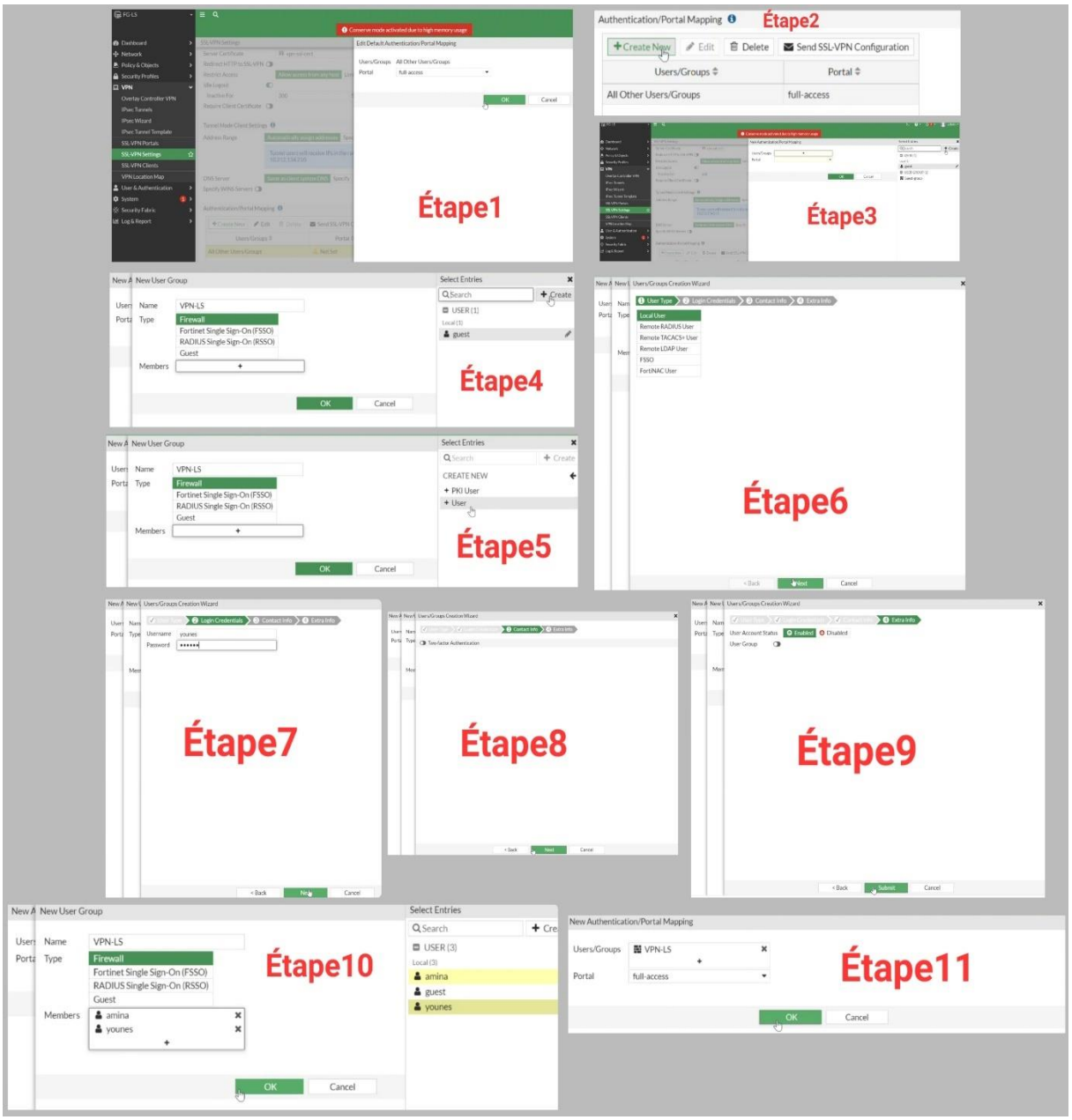


Figure 4.32 : Création d'un groupe.

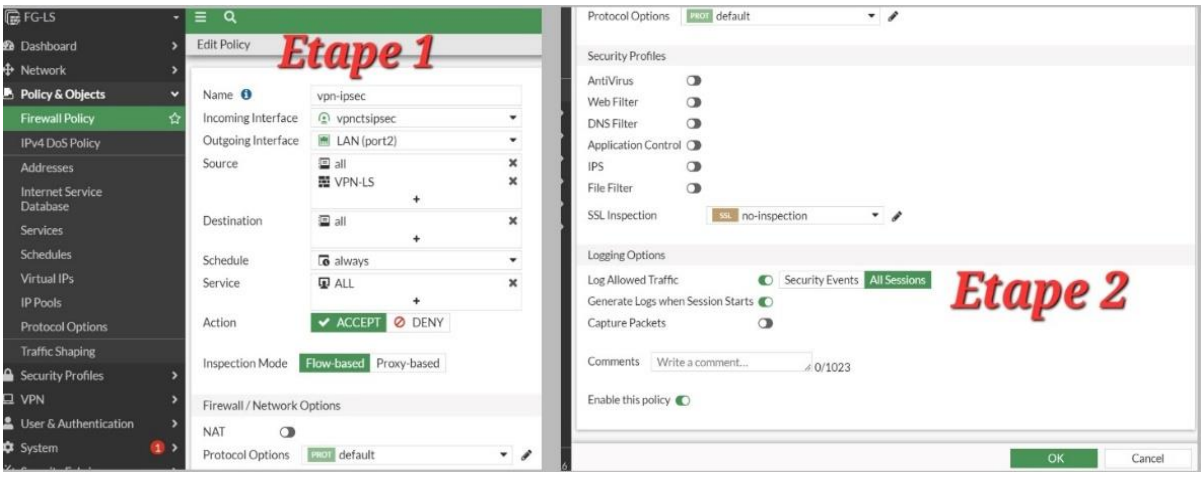


Figure 4.33 : La règle Firewalling établie.

4.8.2.6 Création d’un VPN IPSec pour site-to-site

Dans cette étape, nous mettons en place notre tunnel IPSec. Tout d'abord, nous créons un nouveau tunnel IPSec de type site à site que nous appelons "BEJAIA-ALGER". Nous configurons la clé privée de bout en bout pour assurer la sécurité du tunnel (voir Figure 4.34). Ensuite, nous paramétrons notre VPN en utilisant le chiffrement DES et l'authentification SHA256 dans la phase 1 (phase d'authentification), ainsi que les algorithmes DES et SHA384. Nous utilisons le groupe 5 de Diffie-Hellman avec une longueur de 1024. Ces paramètres s'appliquent également à la phase de l'ESP (phase 2) (voir Figure 4.35).

Ces configurations nous permettent de créer une route statique par défaut vers le réseau distant situé à Alger (remote). Cela signifie qu'une route est créée dans le tunnel pour atteindre ce réseau (voir Figure 4.36). Elles nous permettent également de créer une politique d'entrée-sortie dans la section "Policy & Objects". Pour le trafic entrant, une politique est configurée pour le tunnel vers le réseau local (LAN), tandis que pour le trafic sortant, une politique est mise en place pour le LAN vers le tunnel (voir Figure 4.37).

Enfin, nous activons la connexion du tunnel IPSec. Pour cela nous passons de l'état "inactive" à l'état "up" en effectuant les actions suivantes : cliquer deux fois sur le tunnel IPSec créé, cliquer une fois sur l'état "inactive" et autoriser les deux phases du tunnel. Cette activation se fait automatiquement, même de l'autre bout. Il est important de souligner que cette étape est également réalisée sur le FortiGate situé à Alger, en appliquant les mêmes configurations (voir Figure 4.38).

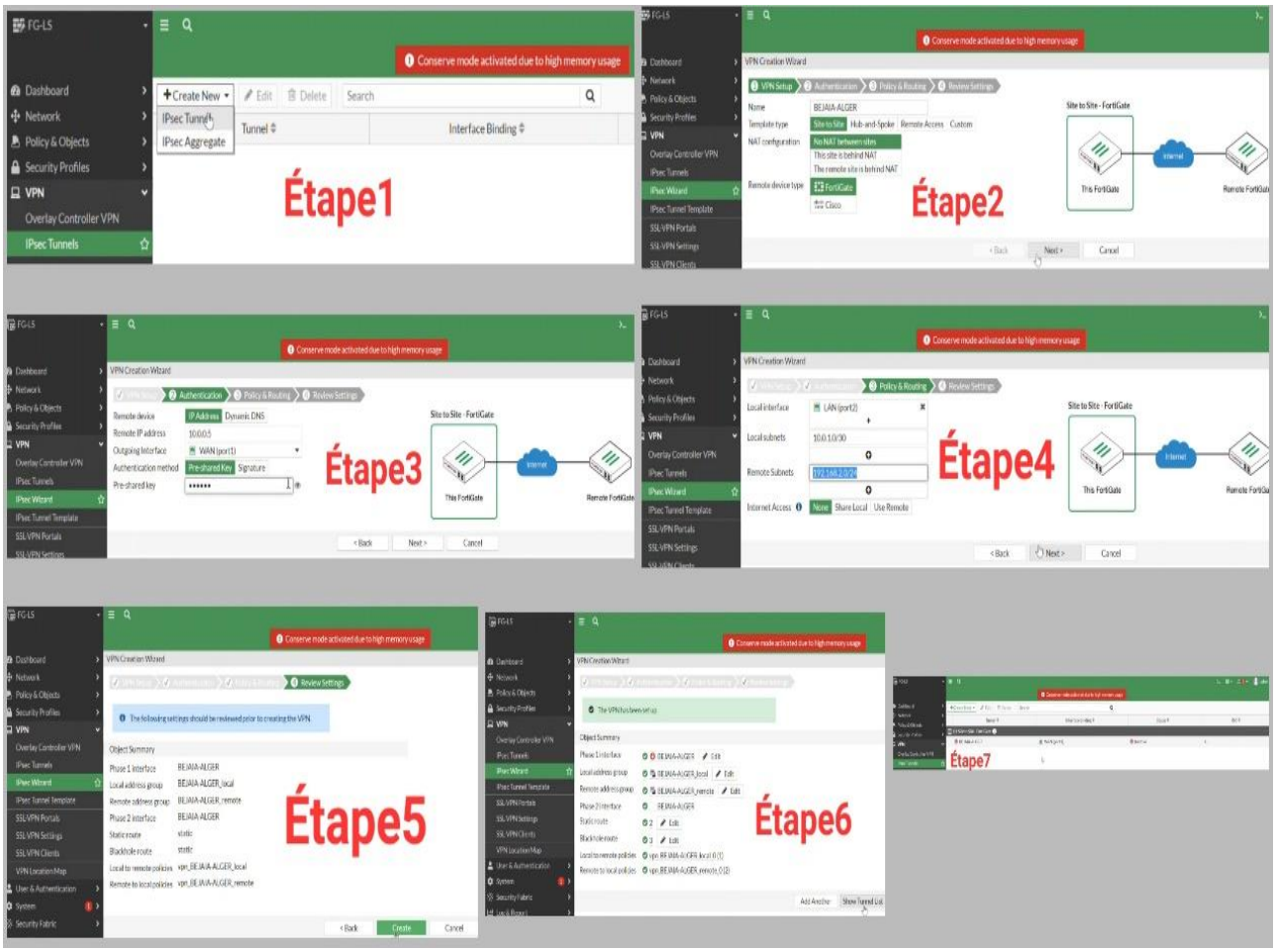


Figure 4.34 : Création tunnel IPSec site-to-site et affichage.

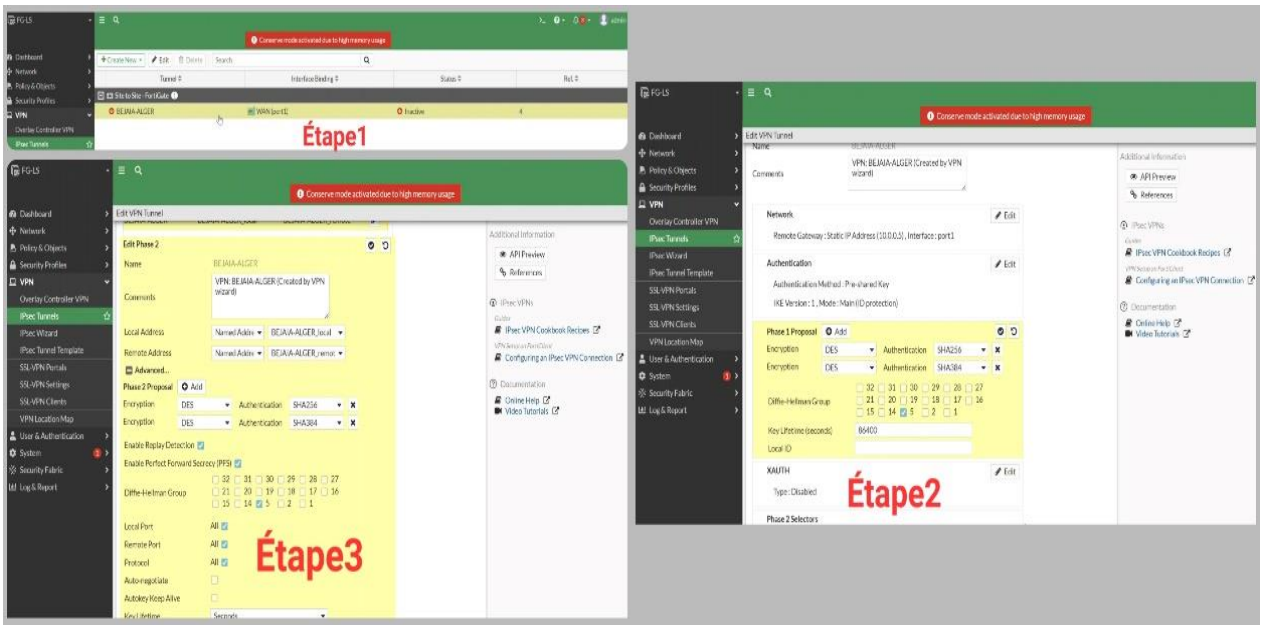


Figure 4.35 : Paramétrage du tunnel VPN (site-to-site).

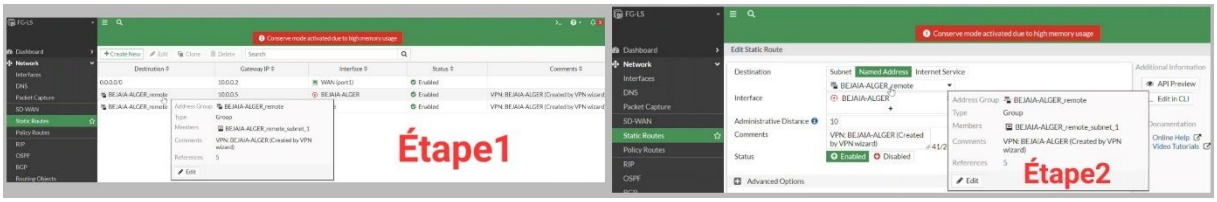


Figure 4.36 : Route statique créer qui mène vers remote (Alger).

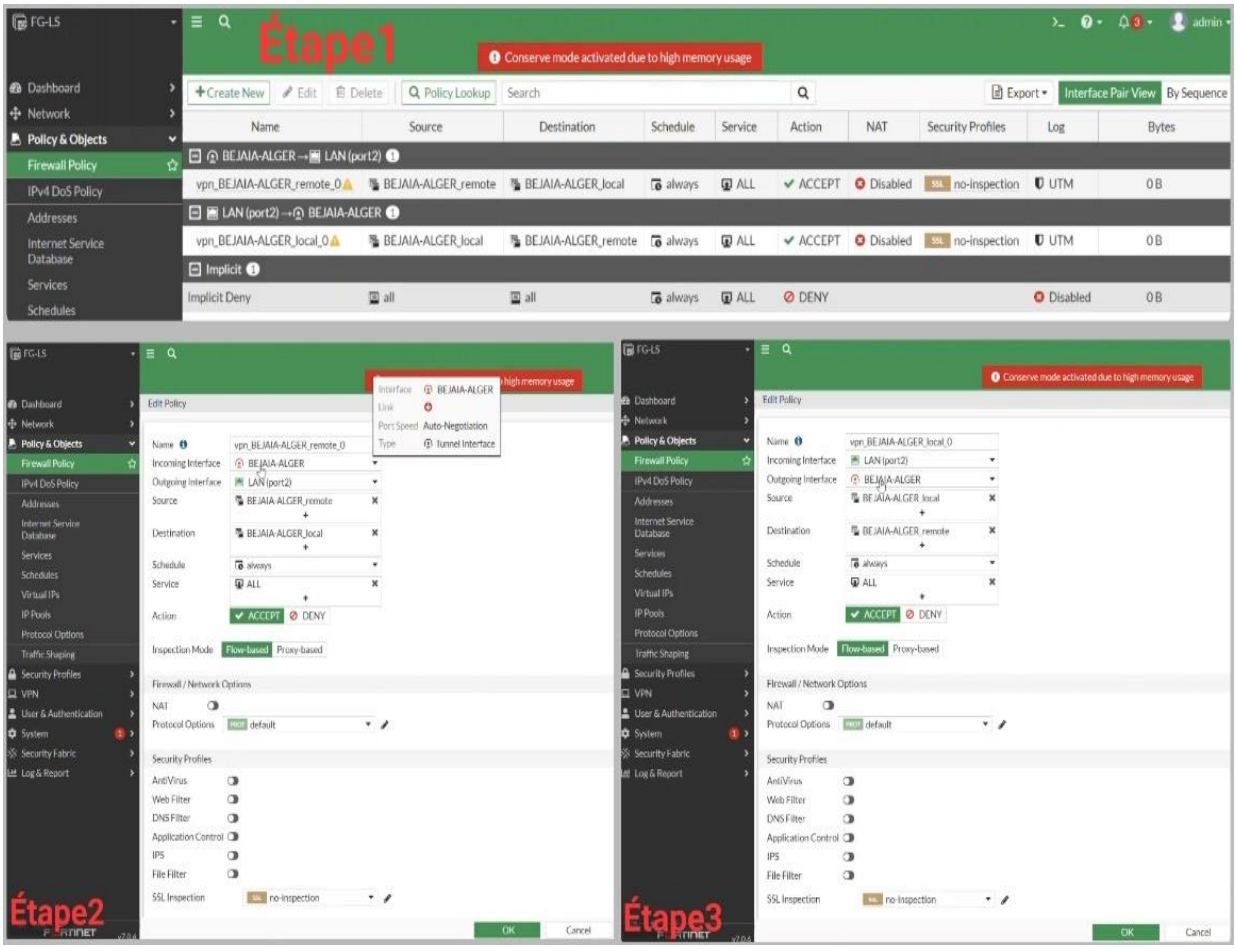


Figure 4.37 : Politique d'entrée-sortie créer vers LAN(Etape2) et vers tunnel (Etape3).

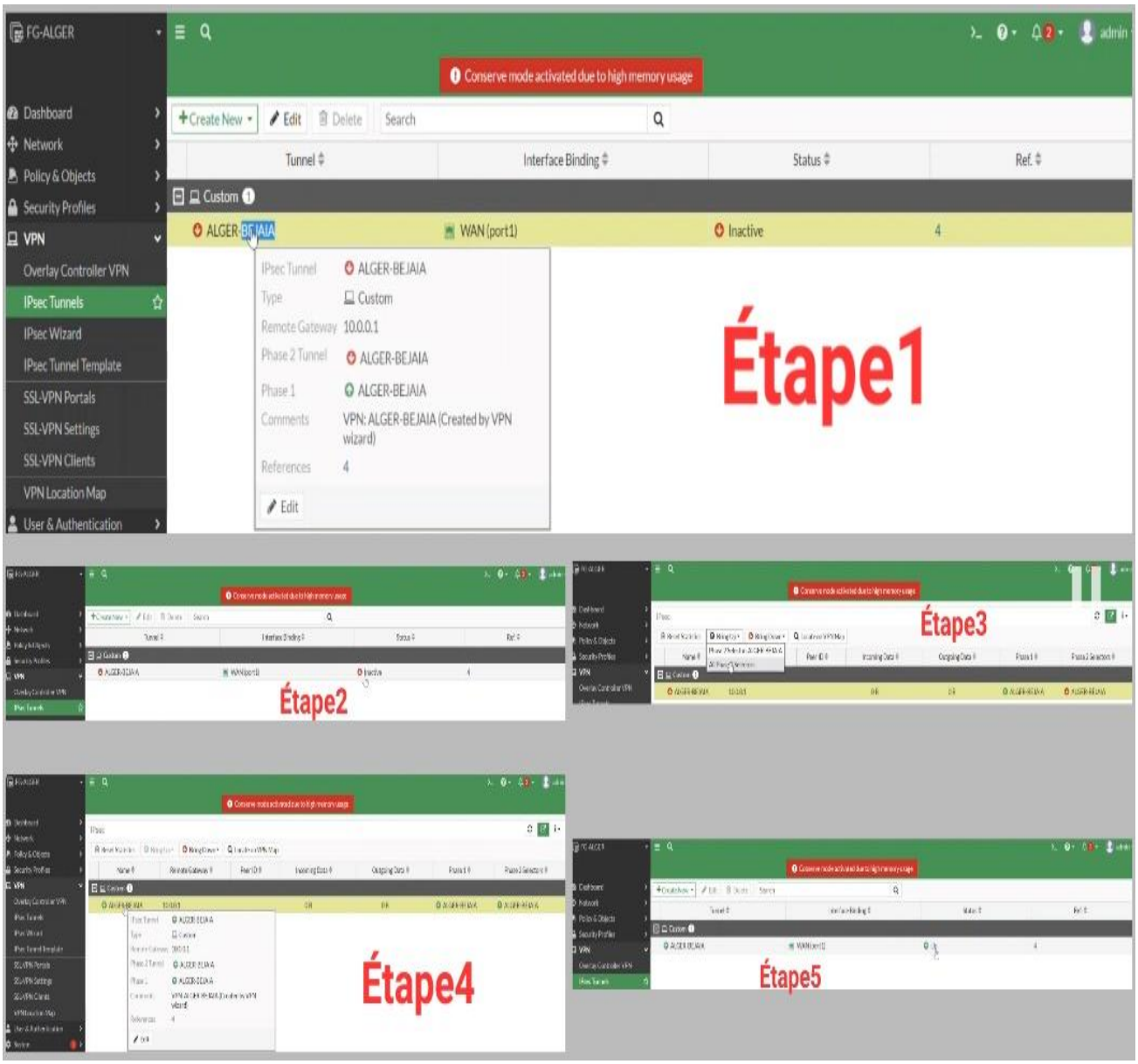


Figure 4.38 : Activation de la connexion du tunnel IPSec et affichage.

4.8.3 Configuration du serveur « radius »

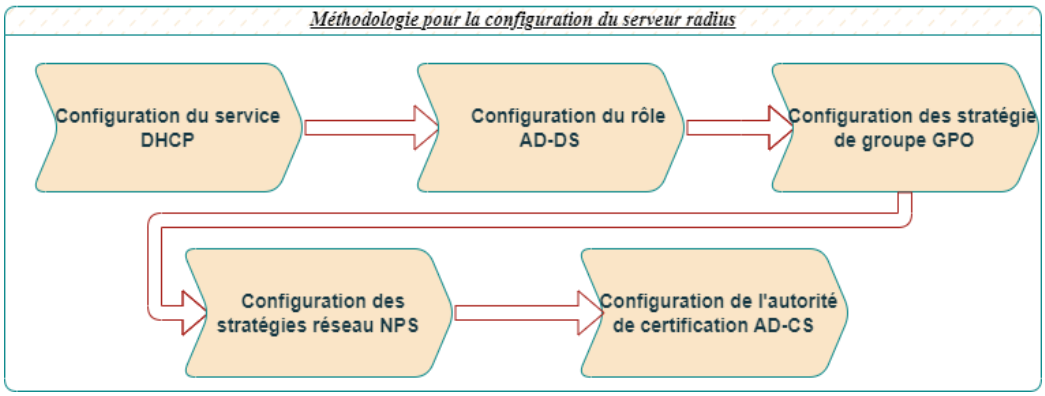


Figure 4.39 : Etapes suivis pour la configuration de notre serveur (radius).

4.8.3.1 DHCP

Dans le but de sécuriser les postes de travail, attribuer des adresses IP pour ces derniers d'une manière automatique et évité tout conflits d'adresse ou de fausse adresse, nous avons configurer le service DHCP.

Nous avons créé pour chaque VLAN une étendue (pool d'adresse) voici un exemple pour le VLAN DRH :

4.8.3.1.1 Création de l'étendue

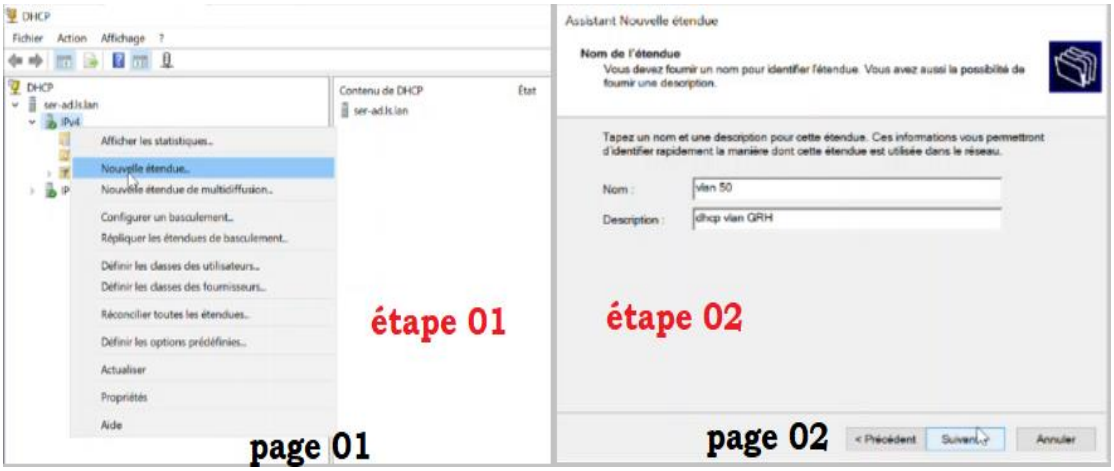


Figure 4.40 : Création d'une nouvelle étendue.

- **Description des étapes**
  - Dans le gestionnaire de serveur nous mettons le curseur sur « outil », ensuite nous effectuons un clic droit sur « DHCP ». L'interface de la page 01 va s'afficher. Nous effectuons un clic gauche sur « IPV4 » puis un clic droit sur « nouvelle étendue » afin de créer un pool d'adresse pour le VLAN 50.
  - Sur la page 02 nous allons nommer notre étendue et mettre une description.

4.8.3.1.2 Configuration des options de l'étendue

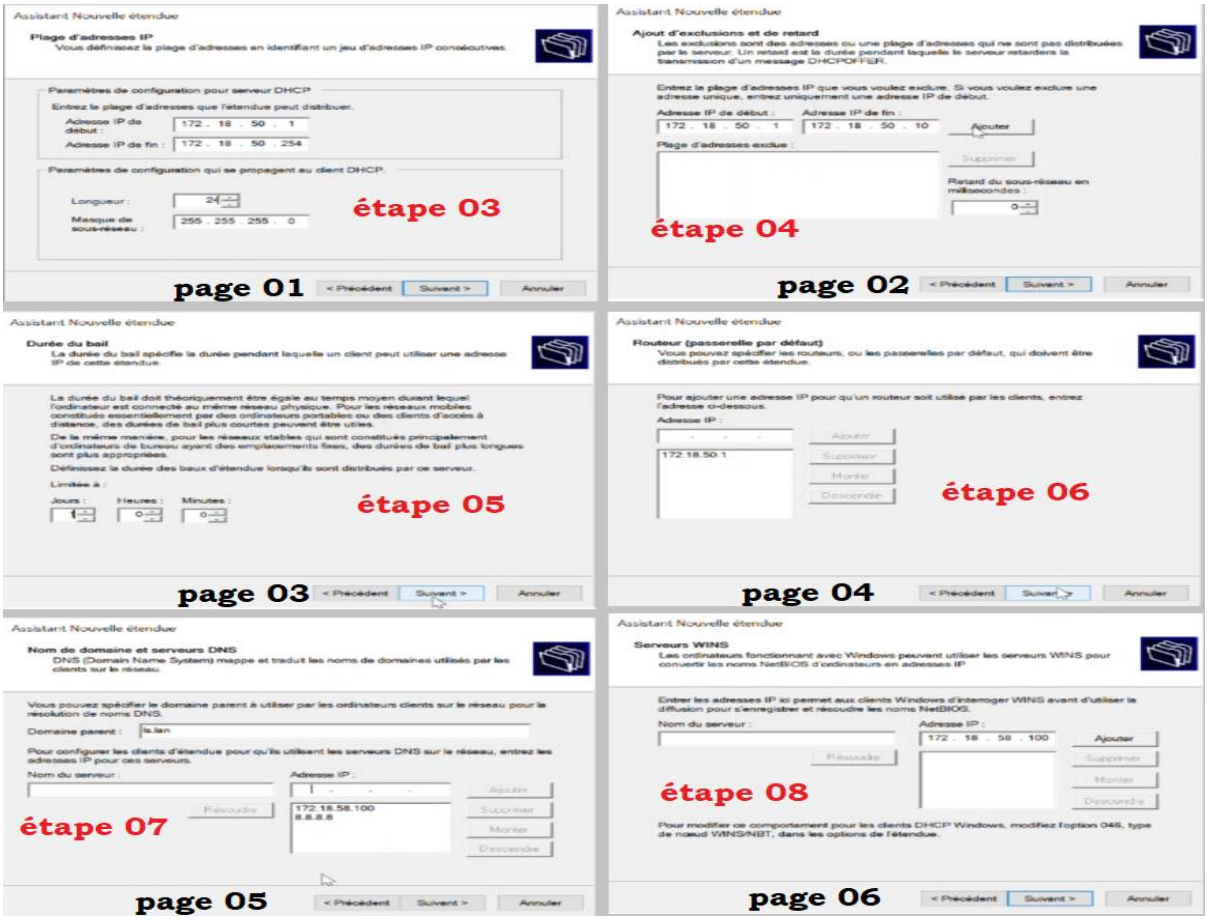


Figure 4.41 : Configuration DHCP.

➢ **Description des étapes**

- L'étape qui suit la création est celle de la spécification des adresses début, fin ainsi que le masque du réseau, que nous avons illustré dans la page1.
- Dans la page 02 nous avons exclu les 10 premières adresses pour les configurer statiquement.
- Ensuite nous avons spécifier une journée pour le bail dans la page3.
- Nous avons ajouté l'adresse de la passerelle par défaut dans la page 04.
- Dans la page 5, nous avons spécifié le nom de domaine ainsi que l'adresse DNS.
- Dans l'étape 8 nous avons spécifier l'adresse du serveur WINS qui sert à traduire les noms NetBIOS

4.8.3.2 AD DS

Pour une meilleure gestion et organisation, nous avons créé un système hiérarchique pour contenir les utilisateurs de l'entreprise. Dans ce qui suit nous allons donner quelques exemples qui nous ont permis de réaliser de cette architecture.

4.8.3.2.1 Création d'une unité d'organisation

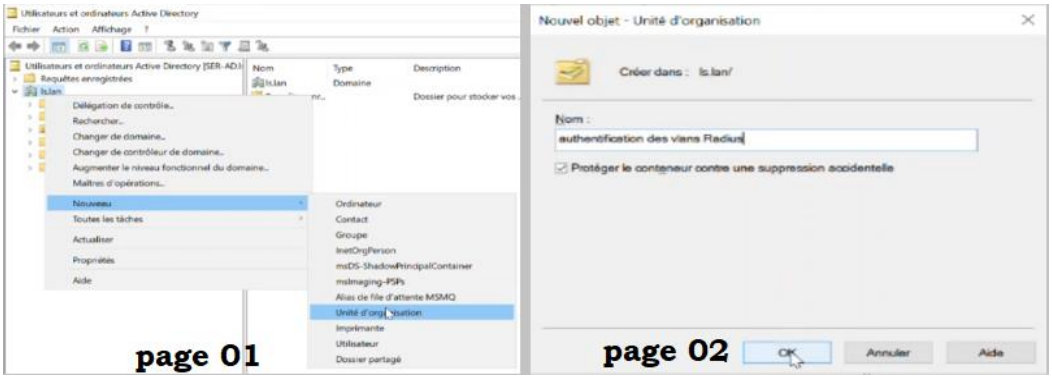


Figure 4.42 : Création de l'unité d'organisation.

➢ **Description des étapes**

- Dans cette partie nous avons créé l'unité d'organisation principale qui contiendra plusieurs groupes selon les départements de l'entreprise. Dans le gestionnaire de serveur puis sur « outil » suivi d'un clic droit sur « utilisateur et ordinateur Active Directory », l'interface de la page 01 s'affichera. Un clic droit sur « ls.lan » (qui représente le domaine de l'entreprise) puis glisser la souris sur « nouveau » et effectuer un clic droit sur « unité d'organisation ».
- L'étape suivante comme nous l'avons montré sur la page 02 c'est de nommé notre unité d'organisation.

4.8.3.2.2 Création des groupes de travail

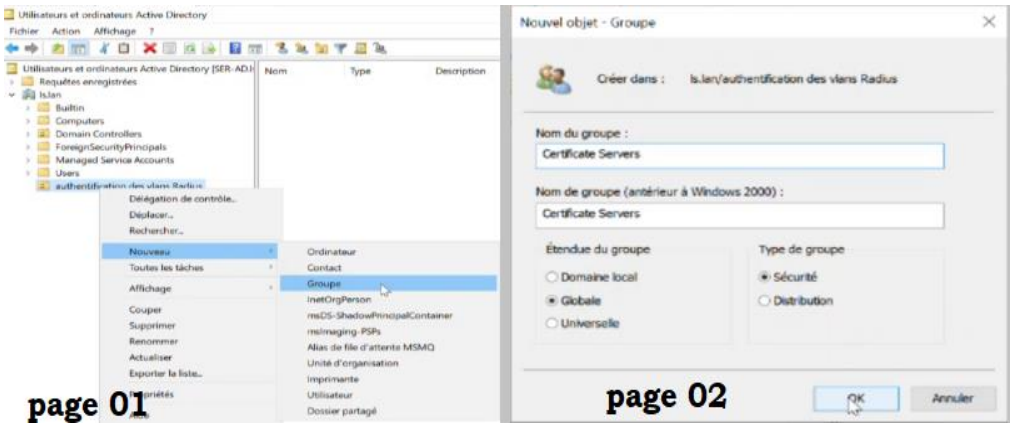


Figure 4.43 : Création d'un groupe de travail.

➢ **Description des étapes**

- Pour chaque département nous avons créé un groupe de travail qui va contenir tous les utilisateurs de ce département, et nous avons également créer deux groupes l'un pour contenir les clients(ordinateurs), l'autre les serveurs, pour les utiliser par la suite dans

l'attribution des certificats. Un clic gauche sur notre unité principal un glissement du curseur sur « Nouveau » suivi d'un clic droit sur « Groupe ».

- Dans la page 02 nous avons donné un nom au groupe et spécifier son type et son étendue.

4.8.3.2.3 Création d'un ordinateur

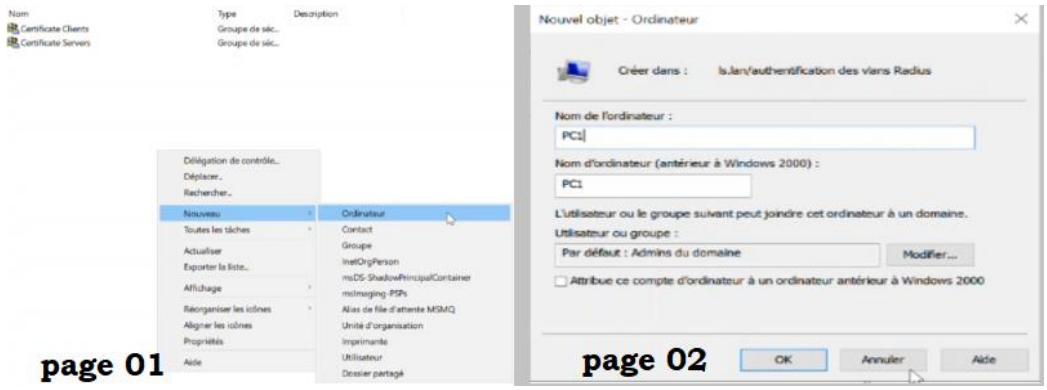


Figure 4.44 : Création d'un ordinateur.

➢ **Description des étapes**

- Afin de garantir une sécurité optimale, notre solution RADIUS (l'authentification des clients) se base sur les noms des ordinateurs et pas sur les utilisateurs, c'est-à-dire que les droits d'accès au réseau sont attribués grâce au nom de l'ordinateur client. Un clic droit sur l'unité d'organisation puis sur « Nouveau » on clique sur « Ordinateur ».
- Dans la page 02 nous avons nommé le nouvel ordinateur.

4.8.3.2.4 Affectation des membres du groupe

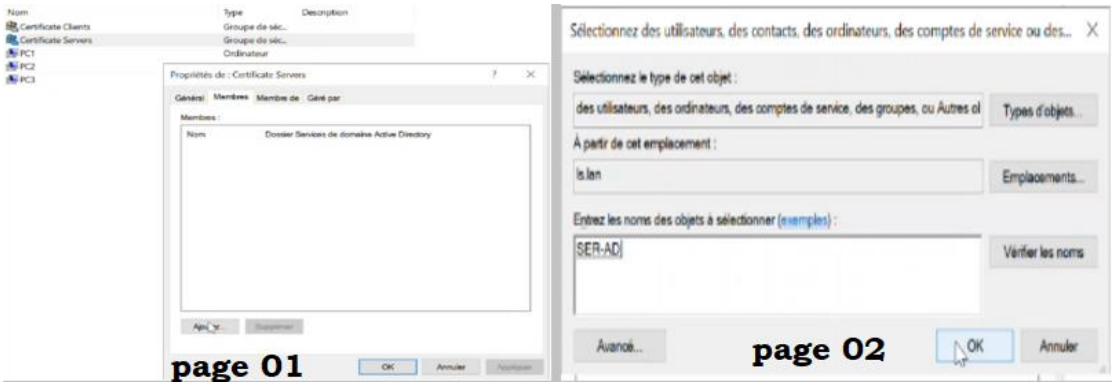


Figure 4.45 : Ajout d'un ordinateur au groupe.

➢ **Description des étapes**

- Chaque ordinateur doit appartenir à son groupe (son département). Nous allons faire un double clic sur le groupe pour voir les propriétés du groupe, puis dans « Membres » on clique sur « Ajouter ».
- Sur la page 02 il faut spécifier le type d'objet à ajouter, son emplacement et son nom.

4.8.3.3 GPO (Group Policy Object)

Comme nous l'avons déjà dit précédemment les GPO nous aident dans la configuration automatique des ordinateurs du réseau. Nous allons commencer par la configuration globale ensuite créé une stratégie pour les clients RADIUS.

4.8.3.3.1 Stratégie globale

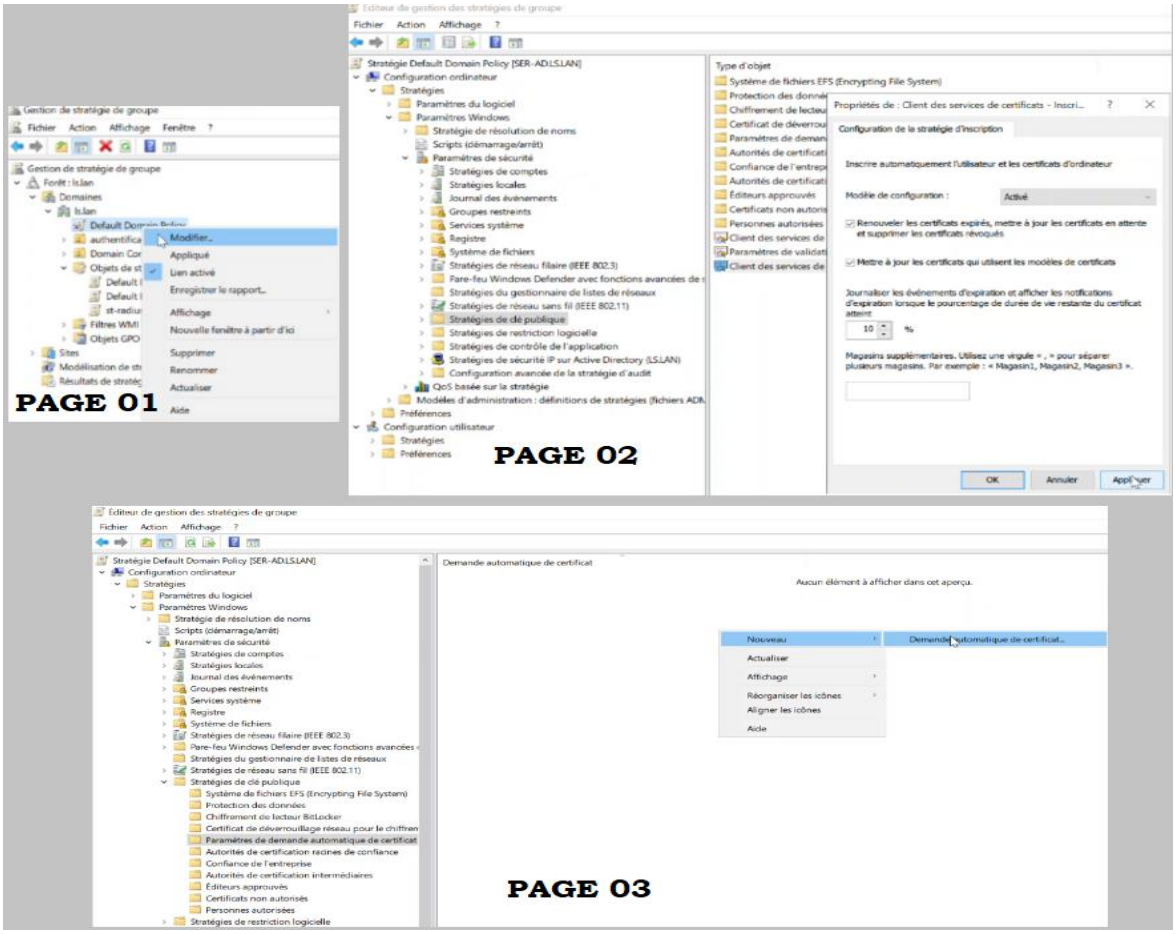


Figure 4.46 : Stratégie globale.

➢ **Description des étapes**

- Pour modifier la stratégie, nous allons faire un clic gauche sur « Default Domain Policy » suivi d'un clic droit sur « Modifier », comme illustré dans la page 01.
- En suivant l'arborescence illustré sur la page 02, nous allons effectuer un double clic sur « Clients des services de certificats – inscription automatique » pour modifier la configuration : nous avons activé le modèle de configuration puis cocher les deux options pour la mise à jour automatique des certificats. Avant de fermer l'interface, nous avons appliqué les modifications.
- Dans l'étape suivante (page03) nous avons créé la demande automatique des certificats pour les ordinateurs dans le dossier « paramètre de demande automatique de certificat ».

4.8.3.3.2 Stratégie radius

a) Création

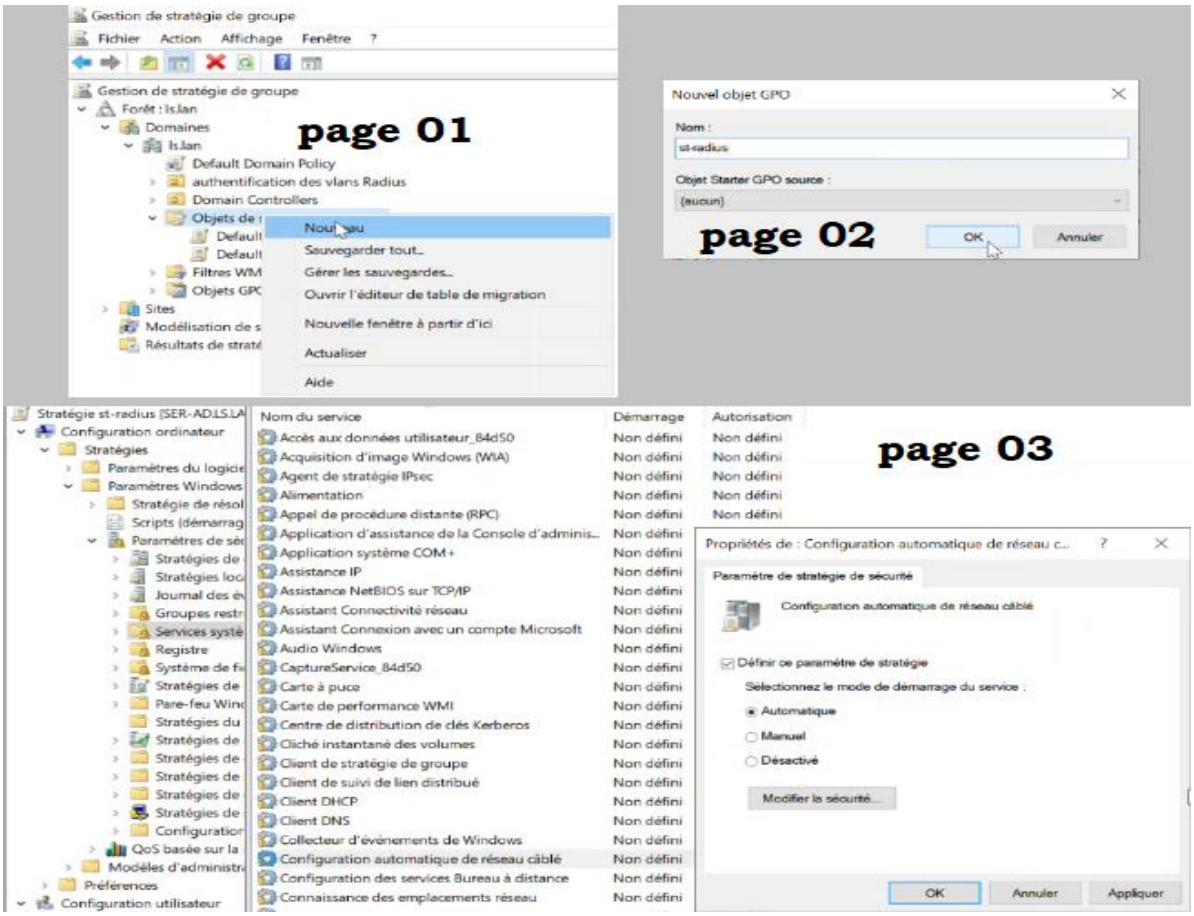


Figure 4.47 : Création d'une nouvelle stratégie.

- **Description des étapes**

  La première condition pour les clients afin d'avoir un accès au réseau avec le système d'authentification RADIUS, c'est de supporter et activé la norme 802.1x. pour cela nous avons créé une nouvelle stratégie comme montré dans les deux premières pages, ensuite dans la page 03 nous avons activé automatiquement cette norme pour l'ensemble des clients.

b) Stratégie filaire

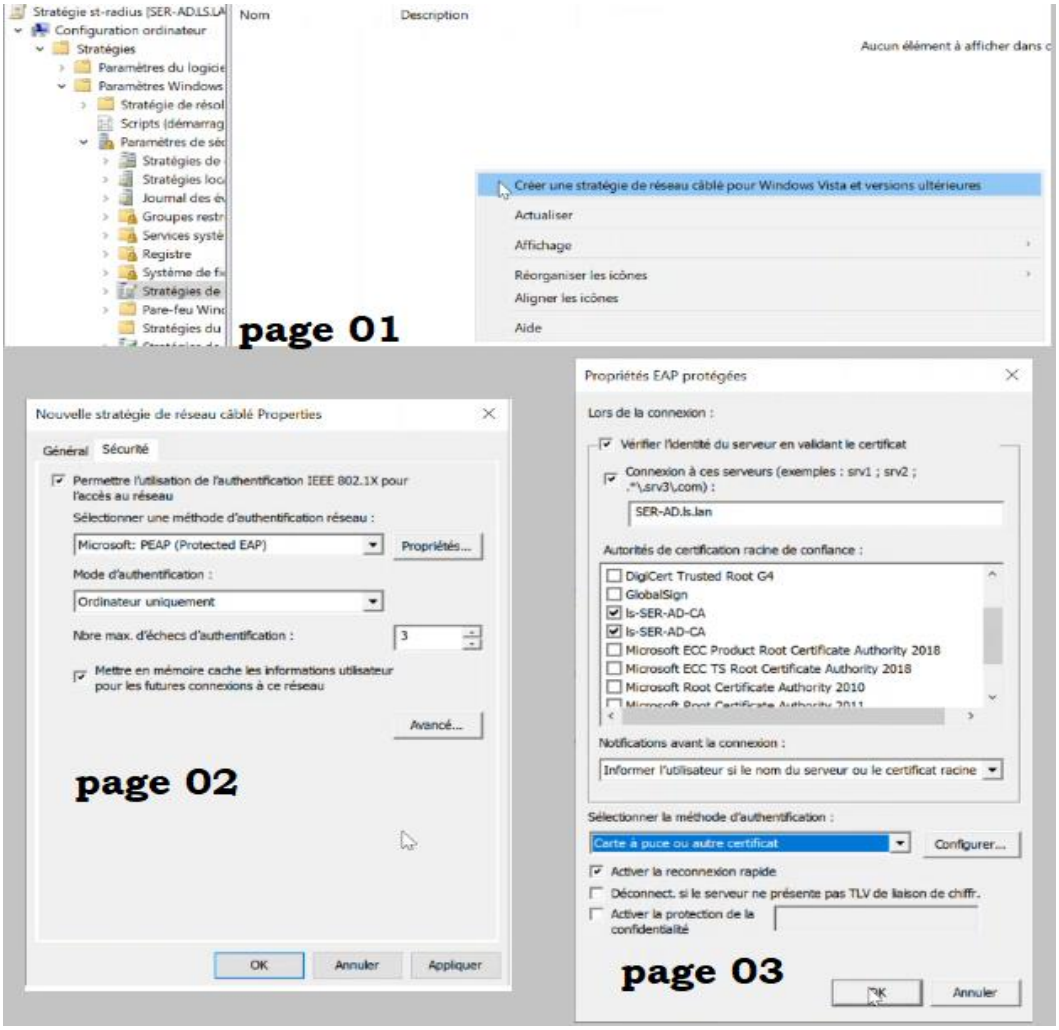


Figure 4.48 : Stratégie filaire.

➢ **Description des étapes**

- Sur notre stratégie RADIUS et en suivant l'arborescence montré dans la page 01 nous avons créé une nouvelle stratégie pour les connexions filaires.
- Sur la page 02 nous avons configuré les paramètres de sécurité de notre stratégie : la méthode d'authentification (PEAP), le mode d'authentification (ordinateur) et le nombre de tentative de connexion que nous avons mis à 3.
- Nous avons configuré les paramètres de la méthode d'authentification PEAP que nous avons illustré sur la page 03.

c) Stratégie sans file

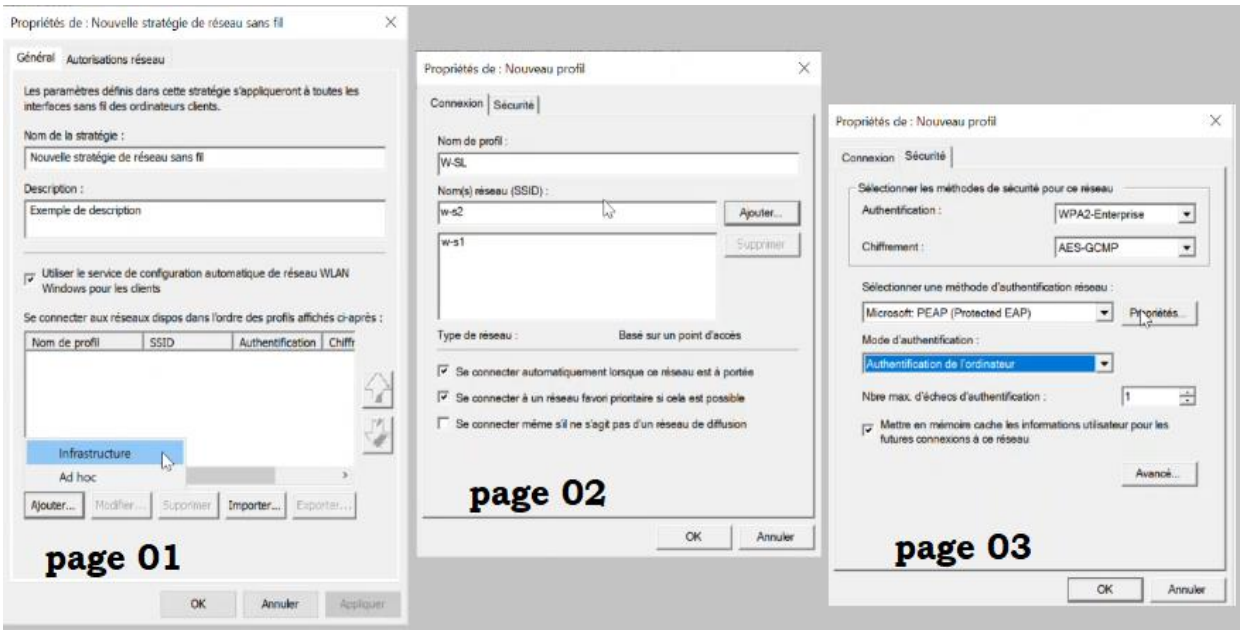


Figure 4.49 : Stratégie sans file.

➢ **Description des étapes**

- En suivant les mêmes étapes pour la création de la stratégie filaire nous avons créé une stratégie sans file. La figure 75 montre les étapes de configuration.
- La première interface après la création de la stratégie est celle de la page 01, où nous avons ajouté un nouveau profile (infrastructure).
- Sur la page 02 nous avons ajouté les points d'accès (SSID) de l'entreprise.
- Dans la page 03 nous avons configuré les paramètres de sécurité des points d'accès du réseau : authentification (WPA2 Entreprise) et chiffrement (AES-QCMP).
- De la même manière que la stratégie filaire nous avons configuré les paramètres de sécurité pour la connexion au réseau sur cette stratégie.

4.8.3.4 NPS (Network Policy Server)

Avant de commencer à configurer le système d'authentification RADIUS, faut d'abord inscrire le serveur sur Active Directory, la figure suivante montre cela :

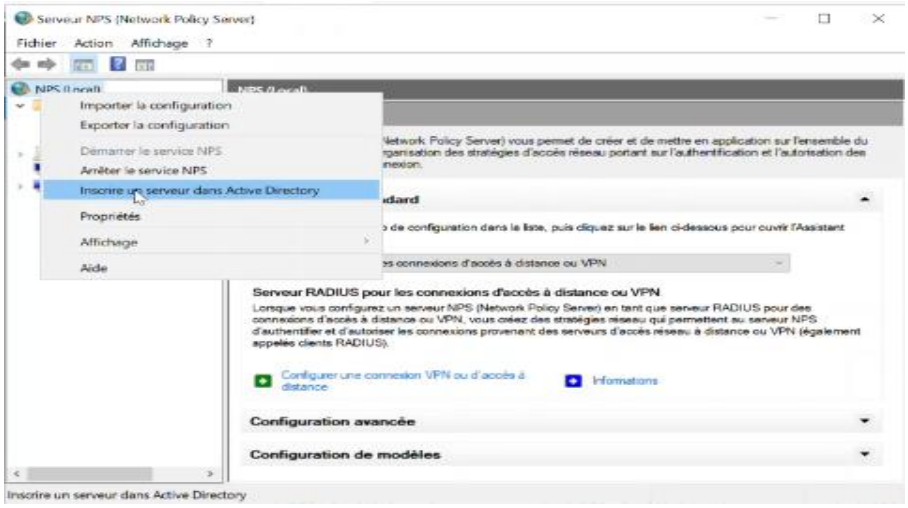


Figure 4.50 : Inscription sur Active Directory.

4.8.3.4.1 Stratégie filaire 802.1x

Ici nous allons configurer une stratégie réseau filaire (la 802.1x).

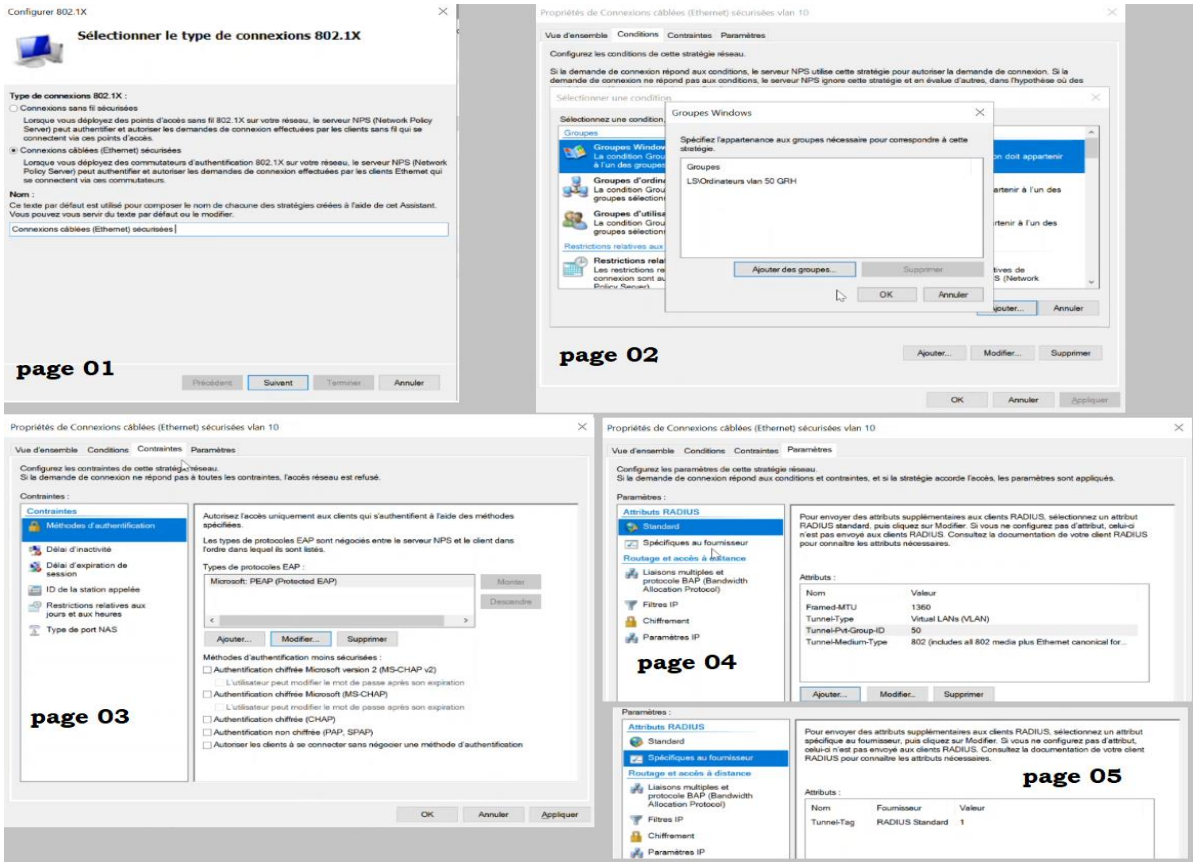


Figure 4.51 : Configuration stratégie réseau.

➢ **Description des étapes**

- Sur la première interface après l'ouverture du rôle NPS, nous allons cliquer sur le bouton en vert, écrit juste à côté « configurer 802.1x » afin de configurer une stratégie réseau filaire.

- La page 01 est l'interface résultante, nous avons donné un nom à notre stratégie et spécifié sa nature (connexion câblé).
- Pour chaque VLAN nous avons créé une stratégie de connexion afin de mieux contrôler les droits d'accès au réseau et au ressources du réseau.
- Sur la page 02 nous avons ajouté le groupe Windows qui contient les ordinateurs (clients) du VLAN.
- La méthode d'authentification comme nous l'avons déjà spécifié auparavant c'est le PEAP, nous avons donc ajouter notre méthode et supprimer toutes les autres comme illustré sur la page 03.
- Les deux dernières pages montrent les attributs relatifs à notre stratégie, à savoir : alléger la MTU (1360), précisé le Tunnel-type (VLAN), spécifié le VLAN de notre stratégie Tunnel-Pvt-Group-ID (50), précisé le Tunnel-Médium-Type (802.1x) et enfin tagué tous les paquets pour les reconnaitre quand ils passe par le routeur Tunnel-Tag (1).

4.8.3.4.2 Stratégie de demande de connexion

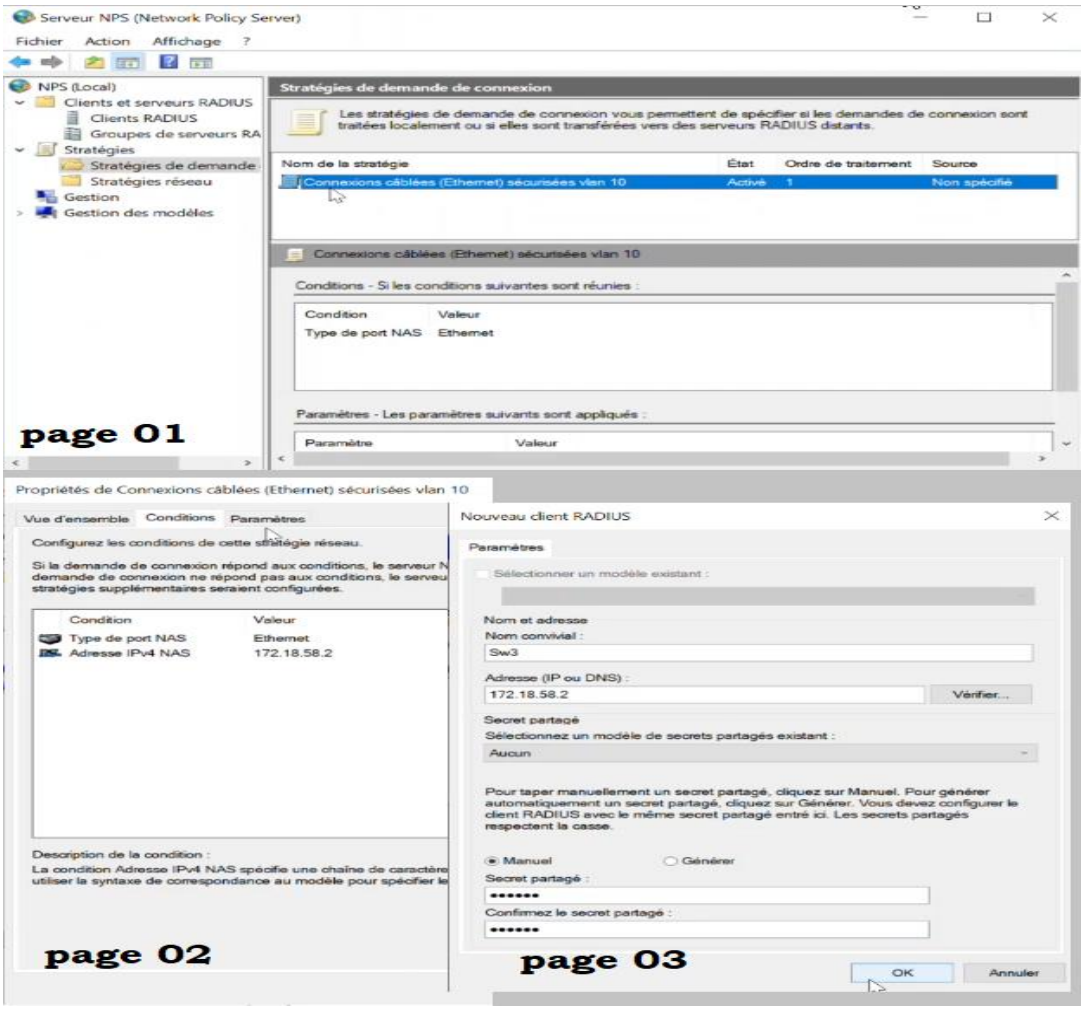


Figure 4.52 : Configuration stratégie de demande de connexion.

➢ **Description des étapes**

- En effectuant un clic droit sur « stratégie de demande de connexion » nous allons ajouter une nouvelle stratégie.
- Nous avons paramétré notre stratégie comme illustré sur la page 02 : spécifier le « Type de port NAS » (Ethernet) (le NAS est le client radius) ainsi que l'« Adresse IPV4 du client RADIUS » sur l'adresse du switch (172.18.58.2).
- Un clic droit sur « Client RADIUS » dans la barre à droite sur l'interface principale de NPS (voir la page 01), va nous permettre d'ajouter un nouveau client. Dans la page 03 nous avons configuré le nom du client, son adresse IP et un mot de passe partagé entre le client et le serveur RADIUS.

4.8.3.5 AD CS

Pour éviter les attaques de l'homme du milieu, nous avons mis en place une autorité de certificat, qui distribue les certificats pour les clients du réseau.

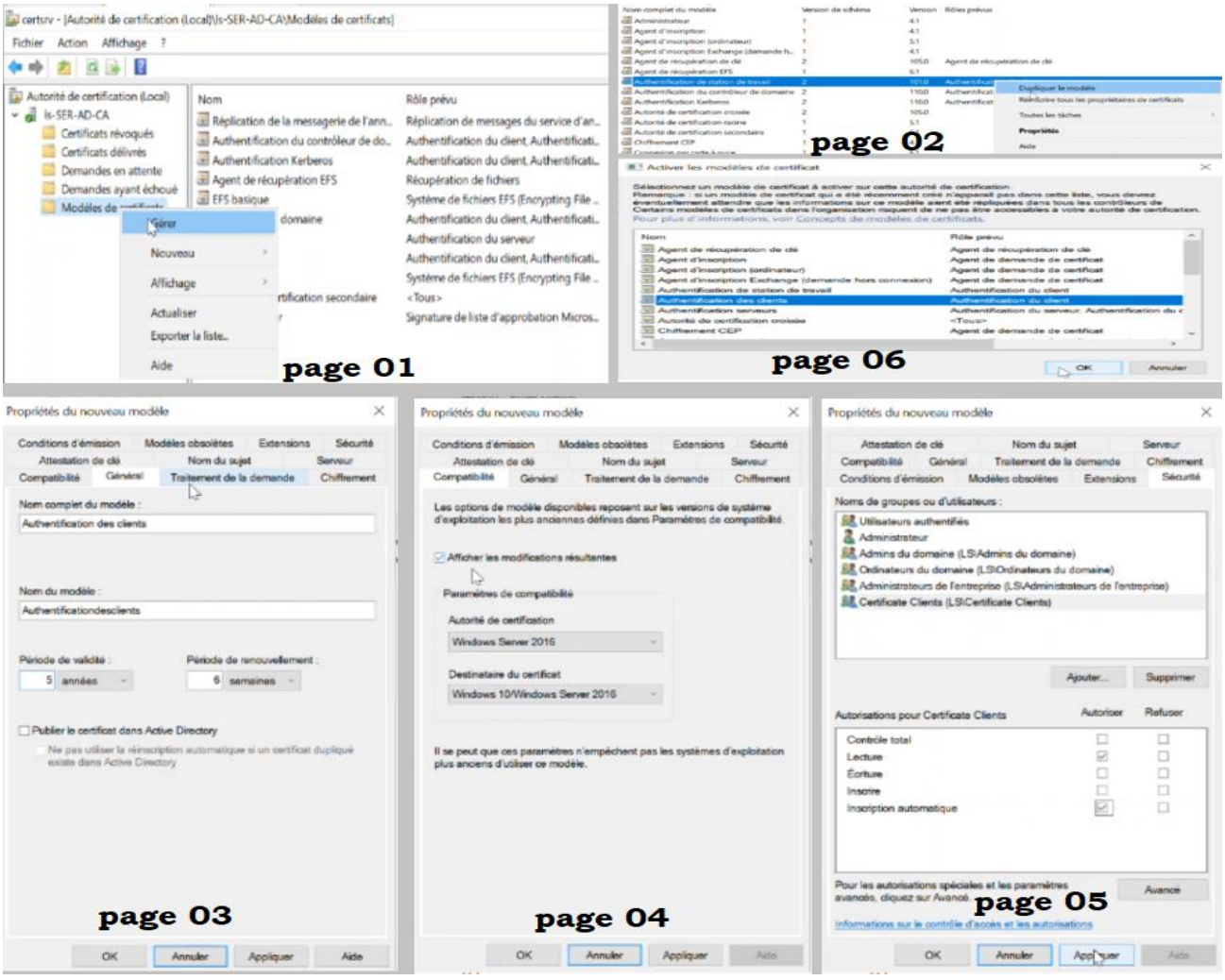


Figure 4.53 : Configuration de AD CS.

➢ **Description des étapes**

- En premier lieu nous avons créé deux modèles de certificat, un pour la certification des clients serveurs et l'autre pour la certification des clients. Dans le gestionnaire de serveur puis sur « Outils » puis un clic droit sur « Autorité de certification », l'interface de la page 01 s'affiche. Nous avons dupliqué les certificats existant et conçu pour ces rôles, les deux premières pages montrent les étapes à suivre pour la création.
- En second lieu nous avons configuré et modifié les paramètre des certificats.
- Dans la page 03 nous avons configurer les paramètres généraux à savoir le nom du modèle et sa période de validité sur 5 ans.
- Dans la page 04 nous avons modifier la compatibilité pour « l'autorité de certificat » et « le demandeur de certificat » selon les systèmes d'exploitation des serveurs et ordinateurs que nous avons installé.
- Dans la page 05 nous avons configuré la sécurité : activé l'inscription automatique des clients et ajouter le groupe concerné par le modèle de certificat, appliqué toutes les modifications puis fermer.
- La dernière étape est d'ajouter les deux certificats créés dans la liste des modèles de certificats : bouton droit sur « Modèles de certificat » puis sur « Nouveau » suivi d'un clic droit sur « Modèles de certificat à délivrer ». En dernier lieu comme nous l'avons montré dans la page 06 il suffit de sélectionner le modèle et de cliquer sur « Ok ».

4.9 Phase 3 : Tests

4.9.1 Test de connectivité

4.9.1.1 La connectivité entre le serveur VOICE et le Firewall de Béjaïa

Nous effectuerons un test de connectivité en utilisant la commande ping depuis un serveur (VOICE) situé dans la DMZ du réseau local de l'entreprise vers son pare-feu (FG-LS). Ce test nous permettra de vérifier si le serveur est capable d'établir une communication réussie avec le pare-feu, ce qui implique sa capacité à se connecter à l'extérieur du réseau via ce pare-feu.

Figure 4.54 : Test de connectivité entre le serveur VOICE vers FG-LS.

4.9.1.2 La connectivité entre l'ORDINATEUR1 et le routeur Core1

Dans cette étape, nous allons tester la connectivité entre le client final (ORDINATEUR1) déjà authentifier par RADIUS qui appartient donc au réseau local de l'entreprise, et le routeur du réseau local (Core1), ceci grâce à la commande ping depuis ce pc afin de vérifier l'établissement de la communication entre les 2 ainsi que le routage inter-vlan en effectuant des pings vers les adresses de différents Vlans existant dans l'entreprise.

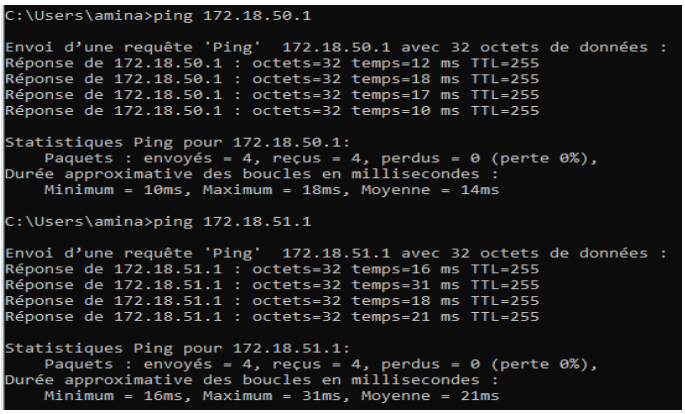


Figure 4.55 : Test de connectivité entre ORDINATEUR1 et Core1.

4.9.1.3 La connectivité entre le PC01 et Core1 avec capture wireshark

Dans cette étape, nous effectuons deux tests. Nous testons la connectivité en utilisant la commande ping depuis un PC (PC01) du réseau d'Alger vers le routeur du réseau local de l'entreprise "SARL Laiterie SOUMMAM",afin vérifier si la communication entre les deux réseaux est établie. Ensuite, nous capturons le trafic ESP à l'aide de Wireshark. Nous observons que les informations sont chiffrées de bout en bout, partant de l'adresse 10.0.0.5 jusqu'à l'adresse 10.0.0.1. Cette observation confirme que les données sont sécurisées pendant leur transmission à travers le tunnel IPSec. Ces tests nous permettent de vérifier à la fois la connectivité entre les réseaux et le bon fonctionnement du chiffrement des données dans le tunnel IPSec.

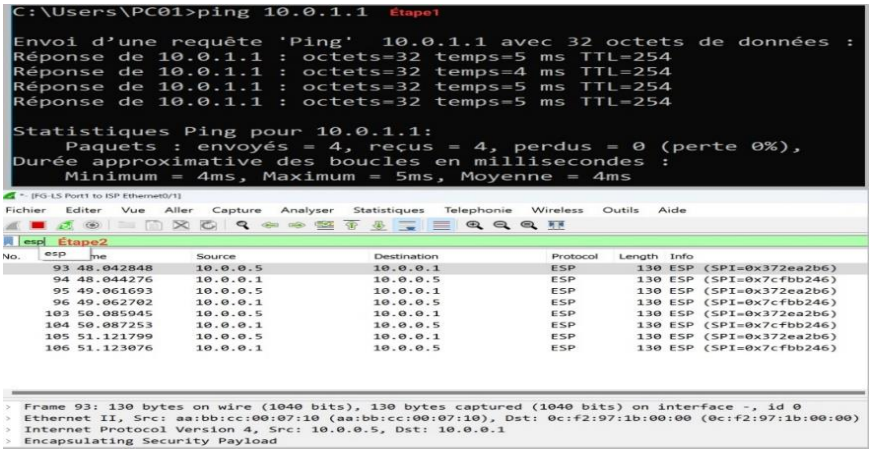


Figure 4.56 : Ping PC01 vers Core1 avec capture du trafique ESP.

4.9.1.4 La connectivité entre différents points du réseau

Dans cette étape, nous effectuons plusieurs tests de connectivité pour vérifier la communication entre différents points du réseau. Tout d'abord, nous utilisons la commande ping depuis un ordinateur (PC01) du réseau d'Alger vers le pare-feu du réseau local de Béjaia. Cela nous permet de vérifier si l'ordinateur est capable d'établir une communication avec le réseau LAN de Béjaia.

Ensuite, nous effectuons un test similaire en utilisant un serveur firewall de Béjaia pour envoyer un ping vers le firewall d'Alger. Cette étape nous permet de vérifier la connectivité entre les deux firewalls.

Enfin, nous réalisons un dernier test en utilisant un serveur firewall d'Alger pour envoyer des pings vers Internet et vers le firewall de Béjaia. Cette étape nous permet de vérifier si la communication vers l'extérieur et vers le réseau de Béjaia est établie avec succès.

Ces tests de connectivité nous permettent de s'assurer que la communication entre les différents points du réseau est fonctionnelle et que les échanges de données se déroulent correctement.

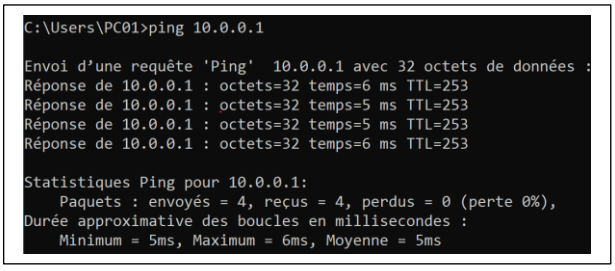


Figure 4.57 : Test de connectivité du PC01 vers FG-LS.

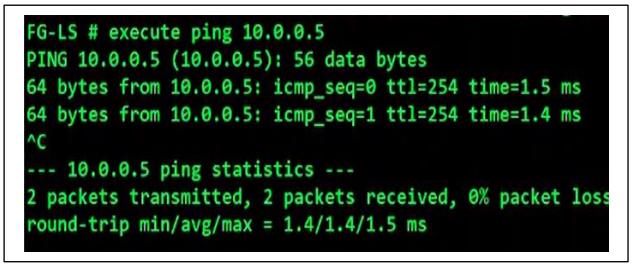


Figure 4.58 : Test de connectivité du FG-LS vers FG-ALGER.

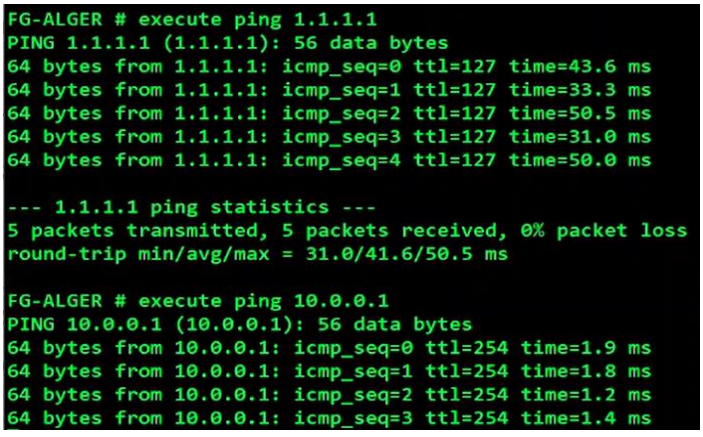


Figure 4.59 : Test de connectivité du FG-ALGER vers internet et vers FG-LS.

4.9.2 Test DHCP

Ici nous avons tester le service DHCP mise en place sur le serveur « SER-AD », avant la configuration de la stratégie RADIUS :

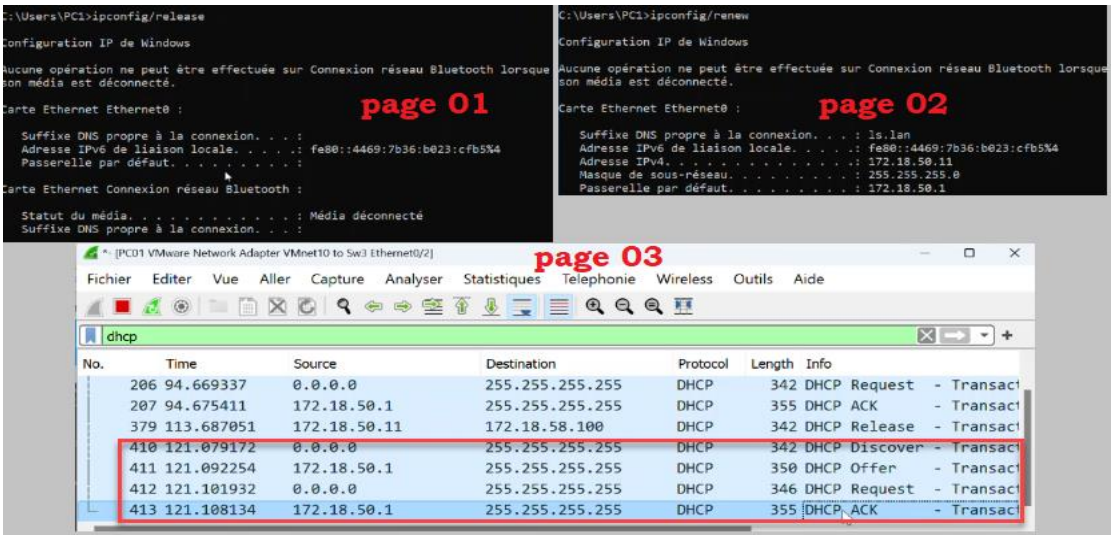


Figure 4.60 : Test DHCP.

Sur les deux premières pages nous avons supprimé puis renouvelé la configuration réseau à travers l'invité de commande de l'ordinateur PC1. Ce dernier est connecté sur le port Ethernet 0/2 qui est affecté pour le VLAN 50. Grâce au service DHCP l'ordinateur a bien reçu un nouvelle configuration réseau de la part du serveur comme nous l'avons montré sur la page 02. Nous pouvons voir les paquets échanger entre le switch 'sw3' et l'ordinateur 'PC1' en capturant le trafic par Wireshark, La page 03 montre ce trafique avec un filtre DHCP, nous pouvons voir les quatre paquets Discover, Offer, Request et ACK échangé entre le serveur et l'ordinateur.

4.9.3 Test RADIUS

Lors du teste de notre solution d'authentification RADIUS, nous avons pu faire des captures d'écran qui montrent la réussite de notre test.

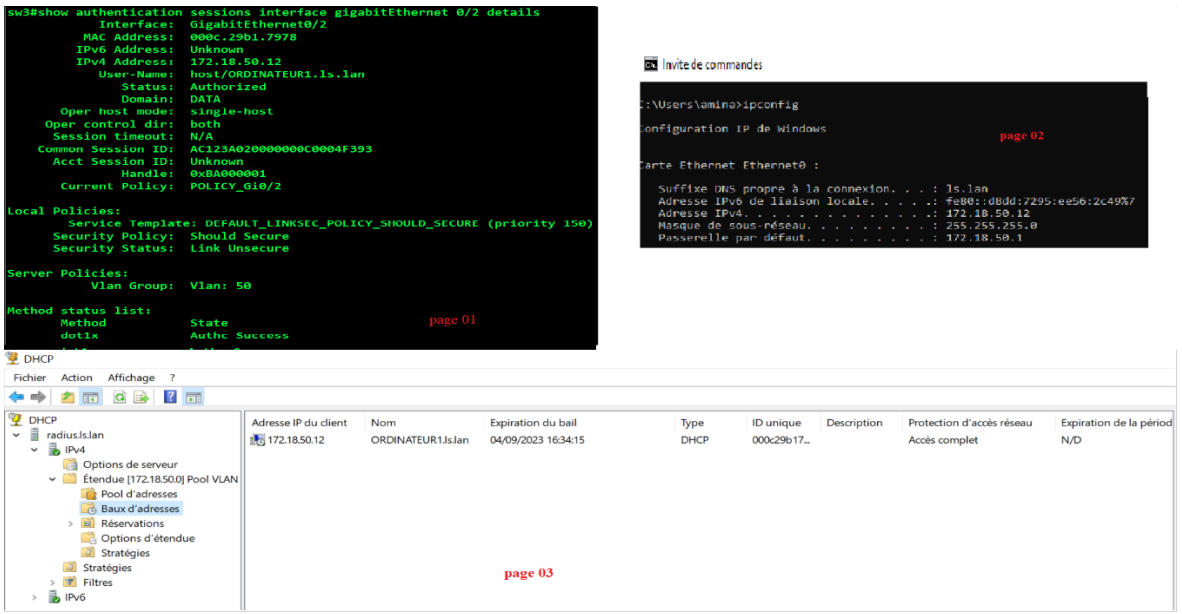


Figure 4.61 : Test d'authentification RADIUS.

➢ **Description de la figure**

- Dans la page 01 de la figure précédente nous avons pu observer les détails de l'authentification du client final (ORDINATEUR1) sur l'interface g0/2 du commutateur « sw3 » qui est client RADIUS, la connexion est autorisée.
- Sur la page 2 on peut voir aussi que le client a bien reçu une adresse IP de la part du serveur après avoir été autorisé par ce dernier.
- La page 3 nous montre que le service DHCP a attribué une adresse pour notre client final.

En allant sur l'observateur d'événements du serveur, sur les services de stratégie et d'accès réseau (NPS), après la tentative d'accès au réseau de l'entreprise par le client final, nous avons capturé l'écran comme montrer dans la figure suivante :

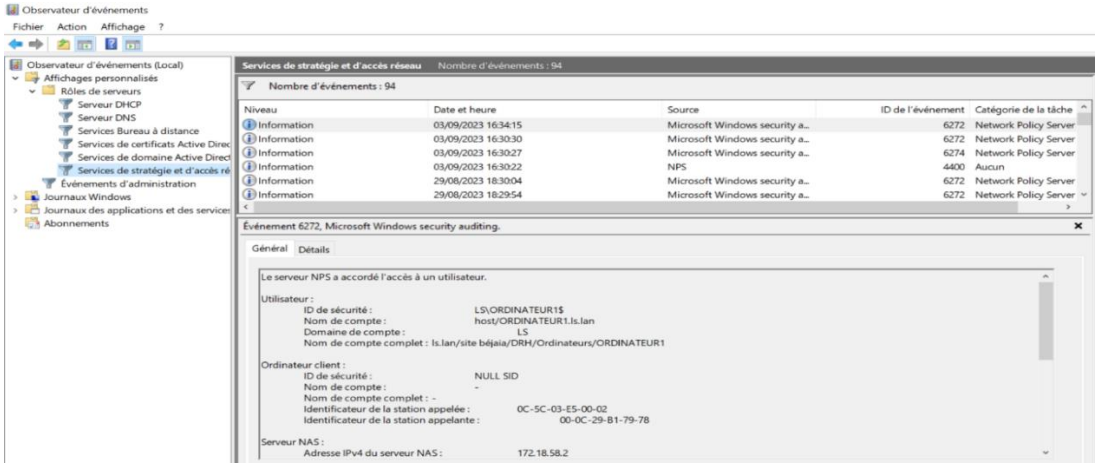


Figure 4.62 : Accès autorisé à l'utilisateur.

La note d'information nous informe que le serveur NPS a accordé l'accès à un utilisateur en précisant toutes les informations le concernant (ID de sécurité, Nom de compte, Domain de compte, nom complet de compte, le vlan auquel il appartient…etc.) ainsi que celles de la connexion (source, évènement, date, catégorie…etc.). Comme nous pouvons également voire plus de détails dans la rubrique (Détails).

4.9.4 Test VPN

4.9.4.1 Adresse attribuer au client distant par DHCP

Dans cet exemple, nous pouvons constater que la fonction d'attribution DHCP mise en place par le routeur ISP fonctionne avec succès. En effet, elle a attribué une adresse IP, en l'occurrence "192.168.1.12", au client distant (Client-VPN). Cette attribution d'adresse IP permet au client distant de se connecter au réseau et de bénéficier d'une communication réseau réussie.

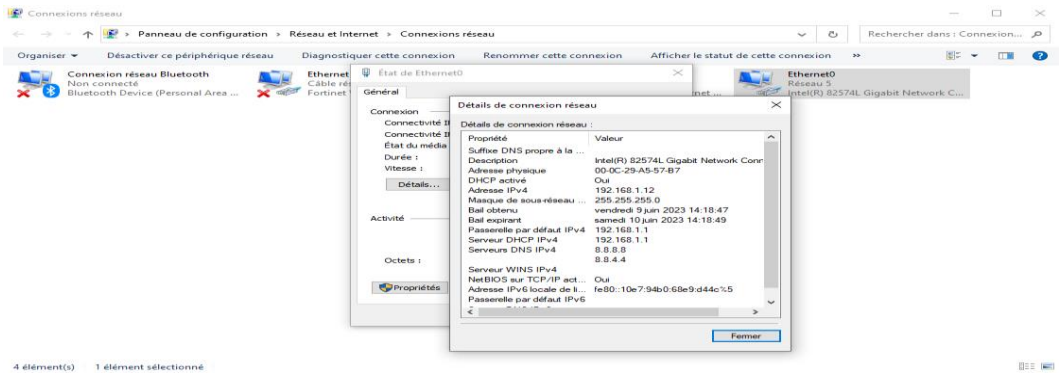


Figure 4.63 : Adresse attribué par DHCP au Client-VPN.

4.9.4.2 Connexion VPN établie client-to-site

Dans cette étape, nous allons configurer la connexion VPN pour un membre du groupe que nous avons créé (par exemple, Younes). Cette connexion permettra à Younes de se connecter au réseau local de l'entreprise en utilisant le tunnel IPSec que nous avons créé avec une clé partagée. Ainsi, Younes pourra établir une connexion sécurisée et accéder aux ressources du réseau local de l'entreprise.

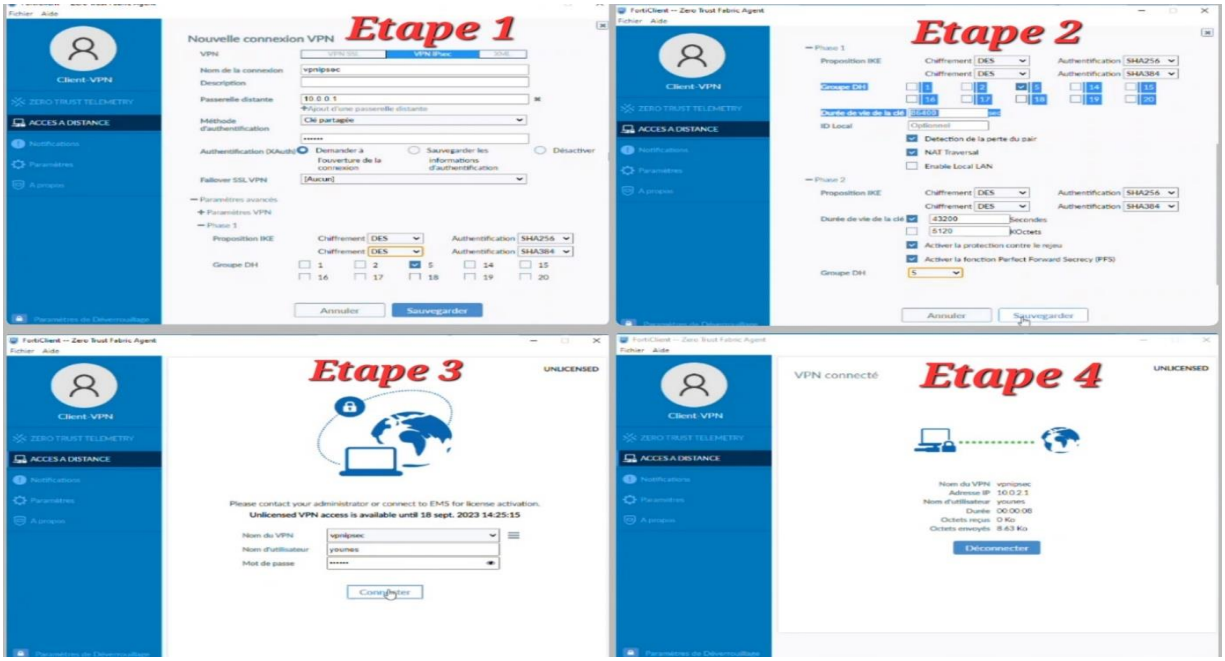


Figure 4.64 : Test connexion VPN via le tunnel IPSec.

4.9.5 Attaque DOS

Afin de mettre à l'épreuve notre politique DOS IPv4 configurée sur le pare-feu Fortigate, nous avons choisi de simuler une attaque DOS à l'aide d'un système Ubuntu Kali Linux qui ne fait pas partie du réseau de l'entreprise. Les captures d'écran ci-dessous présentent cette attaque en cours et attestent de manière évidente que notre pare-feu a réussi à la détecter et à la contrer de manière efficace, garantissant ainsi la continuité des services réseau.

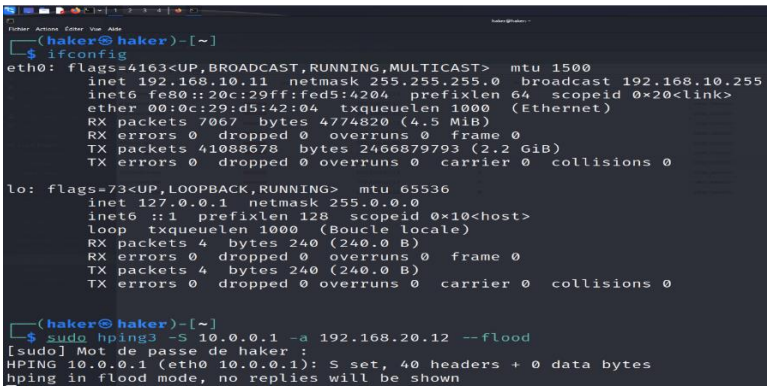


Figure 4.65 : Attaque DOS avec kali linux.

Au cours de cette attaque simulée, nous avons utilisé la commande HPING3 pour cibler l'adresse réseau 10.0.0.1 tout en masquant l'adresse source réelle (192.168.10.11) derrière une adresse falsifiée (192.168.20.12).

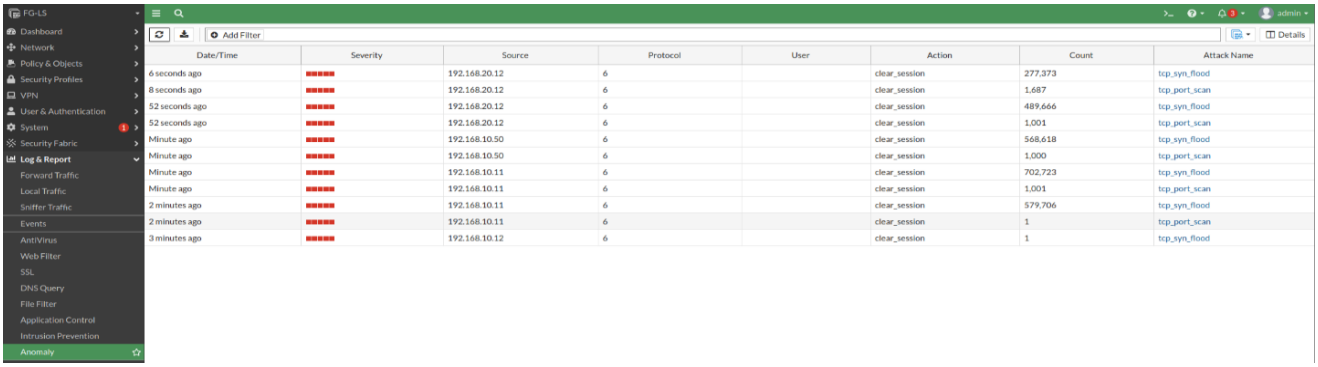


Figure 4.66 : Journal d'anomalies du pare-feu

Suite à cette attaque, nous avons consulté le journal d'anomalies du pare-feu, qui indique qu'une attaque tcq-port-scan et tcq-syn-flood a été détectée en provenance de l'adresse source 192.168.20.12. En réponse à cette attaque, le pare-feu a fermé la session pour contrer la menace.

4.10 Conclusion

Ce dernier chapitre met en pratique les concepts des chapitres précédents en déployant et sécurisant l'architecture réseau. Après avoir identifié les éléments et outils nécessaires, nous avons détaillé les étapes de mise en œuvre et configuration pour chaque équipement et serveur, avec une simulation sous GNS3. Cette application concrète reflète notre passage de la théorie à la pratique, montrant notre compétence à mettre en œuvre les concepts et à concevoir une infrastructure réseau sécurisée. En suivant ces étapes, nous avons établi une architecture réseau solide et conforme aux normes de sécurité. Ce chapitre pratique offre des exemples concrets aux lecteurs, illustrant la mise en place d'une telle architecture. Parallèlement, il a renforcé nos compétences et compréhension des pratiques de sécurité réseau.

Conclusion générale

À l'issue de notre étude dédiée à la sécurisation du réseau local de l'entreprise SARL LAITERIE SOUMMAM, il est clair que la préservation de la sécurité des données et des systèmes revêt une importance capitale dans l'environnement informatique. Notre analyse approfondie de l'infrastructure existante nous a permis d'identifier diverses vulnérabilités et de proposer des solutions appropriées afin de renforcer la sécurité du réseau.

La mise en place de VLANs basés sur le protocole VTP, conjointement avec d'autres protocoles de sécurité exposés dans notre projet, ainsi que l'adoption d'une solution d'authentification RADIUS, ont apporté des améliorations significatives à l'architecture du réseau, tout en offrant un contrôle précis sur l'accès des utilisateurs. De plus, la configuration d'un pare-feu et d'un VPN a garanti un accès sécurisé au réseau de l'entreprise, même à distance, renforçant ainsi la protection des données et des ressources sensibles.

La réalisation de ce projet a apporté une contribution significative à l'entreprise SARL LAITERIE SOUMMAM, tout en enrichissant nos connaissances des mécanismes et des protocoles de sécurité. Notre étude approfondie du fonctionnement de ces éléments nous a permis d'acquérir des compétences pratiques et théoriques précieuses pour notre parcours professionnel.

La sécurisation du réseau local demeure un impératif fondamental pour toute entreprise soucieuse de préserver la confidentialité de ses informations et de gagner la confiance de ses clients. En mettant en pratique les recommandations formulées dans notre étude, SARL LAITERIE SOUMMAM pourra établir un environnement réseau à la fois sûr, fiable et résistant aux attaques. De plus, afin de poursuivre cette démarche de sécurisation, nous suggérons également d'explorer la mise en place d'une supervision réseau proactive. Cette solution permettra la détection précoce de comportements anormaux ou de tentatives d'intrusion, renforçant ainsi la vigilance continue face aux menaces potentielles.

Bibliographie

[1] « Internet, Intranet et Extranet : comment les différencier ? - Ceralis ». *https://www.ceralis.fr/*, https://www.ceralis.fr/internet-intranet-et-extranet-comment-les-differencier/. Consulté le 18 août 2023.

[2] Aurélien Esnard, « Introduction aux Réseaux », MIAGE L3, Université de Bordeaux, http://www.labri.fr/~esnard (page consulté le 26/08/2023)

[3] Grégory Epiphane. ACISSI. Sécurité informatique Ethical Hacking Apprendre l'attaque pour mieux se défendre. ENI Editions. Nantes : Septembre 2017.

[4] Nadia BATTAT, « Les systèmes de sécurité », M2 ASR, Université Abderrahmane Mira, Bejaia, 2020/2021.

[5] Liste des Cours de BTS IG 2 éme année AMSI option Réseau, « Les LAN »,

http://perso.modulonet.fr/~placurie/AMSI2.htm. Consulté le 06 septembre 2023

[6] C. Français, "CCNA 3 v7.02 (ENSA) Réponses Français - Enterprise Networking, Security, and Automation," *CCNA Réponses - Questions et réponses aux Examens*, Nov. 09, 2022. https://ccnareponses.com/ccna-3-v7-02-ensa-reponses-francais-enterprise-networking-security-and-automation/

[7] *Les Vlans : les protocoles de transport et de contrôle*. http://igm.univ-mlv.fr/~dr/XPOSE2006/SURZUR-DEFRANCE/vtp.html. Consulté le 18 août 2023.

[8] « Qu'est-Ce Qu'un VLAN Privé et Comment Fonctionne-t-Il ? | Communauté FS ». *Knowledge*, 24 septembre 2019, https://community.fs.com:7003/fr/blog/what-is-private-vlan-and-how-it-works.html. Consulté le 18 août 2023.

[9] Sauvageot-Berland, Geoffrey. « Présentation des Private VLAN pour améliorer la sécurité de votre réseau ». *Le Guide Du SecOps*, 31 mai 2020, https://le-guide-du-secops.fr/2020/05/31/presentation-des-private-vlan-pour-ameliorer-la-securite-de-votre-reseau/. Consulté le 18 août 2023

[10] *VLAN - Réseaux virtuels*. https://web.maths.unsw.edu.au/~lafaye/CCM/internet/vlan.htm. Consulté le 18 août 2023.

[11] malekalmorte. « La connexion sans fil - Wi-Fi : comment ça marche et le dossier ». *malekal.com*, 26 octobre 2020, https://www.malekal.com/la-connexion-sans-fil-wifi-comment-ca-marche-et-le-dossier/. Consulté le 20 septembre 2023.

[12] *Qui sommes nous | Soummam*. http://www.soummam-dz.com/qui-sommes-nous.html. Consulté le 18 août 2023.

[13] Fortinet, « Fortinet_FortiGate-100 E », Mars 2017, les Etats Unis, https://www.exclusive-networks.com/ma/wp-content/uploads/sites/2/2020/12/Fortinet_FortiGate-100E_FR.pdf. Consulté le 03 septembre 2023.

[14] Soulages, Damien. « Couche d'Accès, Distribution et Core ». *Formip*, 2 septembre 2019, https://formip.com/acces-distribution-core/. Consulté le 18 août 2023.

[15] "Cours complet windows server 2016 pdf | PDFprof.com," https://pdfprof.com/FR_PDF/PDF_1PDFprof_Doc__Document_Gratuits_PDF_Free.php?q=-1PDF57476-cours+complet+windows+server+2016+pdf.

[16] Robinharwood. (n.d.). Documentation sur les services de certificats Active Directory. Microsoft Learn. https://learn.microsoft.com/fr-fr/windows-server/identity/ad-cs/. Consulté le 28 août 2023.

[17] JasonGerend. *Domain Name System (DNS)*. 10 janvier 2022, https://learn.microsoft.com/en-us/windows-server/networking/dns/dns-top. Consulté le 20 août 2023.

[18] *VPN - Réseaux Privés Virtuels (RPV)*. https://web.maths.unsw.edu.au/~lafaye/CCM/initiation/vpn.htm. Consulté le 18 août 2023.

[19] « Qu'est-ce qu'un VPN et comment fonctionne-t-il ? » *Qu'est-ce qu'un VPN et comment fonctionne-t-il ?*, https://www.avast.com/fr-fr/c-what-is-a-vpn. Consulté le 18 août 2023.

[20] Cahen ©1997, Murielle. « Avocate Paris cabinet avocat conseil juridique ». *Avocat Paris*, https://www.murielle-cahen.com/. Consulté le 18 août 2023.

[21] « Avantages et inconvénients de SSL / HTTPS / TLS ». *SSL.com*, https://www.ssl.com/fr/article/avantages-et-inconv%C3%A9nients-de-ssl-https-tls/. Consulté le 5 septembre 2023.

[22] Authors, Rublon. *RADIUS vs. TACACS+: What's the Difference? - Rublon*. https://rublon.com/blog/radius-vs-tacacs/. Consulté le 18 août 2023.

[23] YOUNESS-LA, "Authentification 8021x V10," *dokumen.tips*, 25 September 2022, https://dokumen.tips/documents/authentification-8021x-v10.html?page=1.

[24] Getting Started with GNS3 | GNS3 Documentation. (n.d.). Disponible depuis https://docs.gns3.com/docs/. Cosulté le 18 août 2023.

[25] *Getting Started with GNS3 | GNS3 Documentation*. https://mother.github.io/docs/. Cosulté le 18 août 2023.

[26]Timalsina R. 15+ hping3 command examples in Linux [Cheat Sheet] | GoLinuxCloud.

2022 ; Disponible sur : https://www.golinuxcloud.com/hping3-command-in-linux/#Introduction_to_hping3_command. Consulté le 06 septembre 2023.

Résumé

Notre mémoire se focalise sur la sécurisation du réseau local de SARL LAITERIE SOUMMAM, en mettant l'accent sur l'installation et la configuration de solutions de sécurité. Nous avons mis en œuvre l'authentification basée sur RADIUS pour contrôler l'accès au réseau, et segmenté le réseau en VLANs pour renforcer la sécurité. De plus, un pare-feu Fortigate a été déployé pour fournir l'authentification et le filtrage nécessaires. En utilisant GNS3 et une VMWARE, nous avons testé et validé nos solutions. Cette étude renforcera la fiabilité du réseau de SARL LAITERIE SOUMMAM, préservant la confidentialité des données et assurant une activité ininterrompue.

Abstract

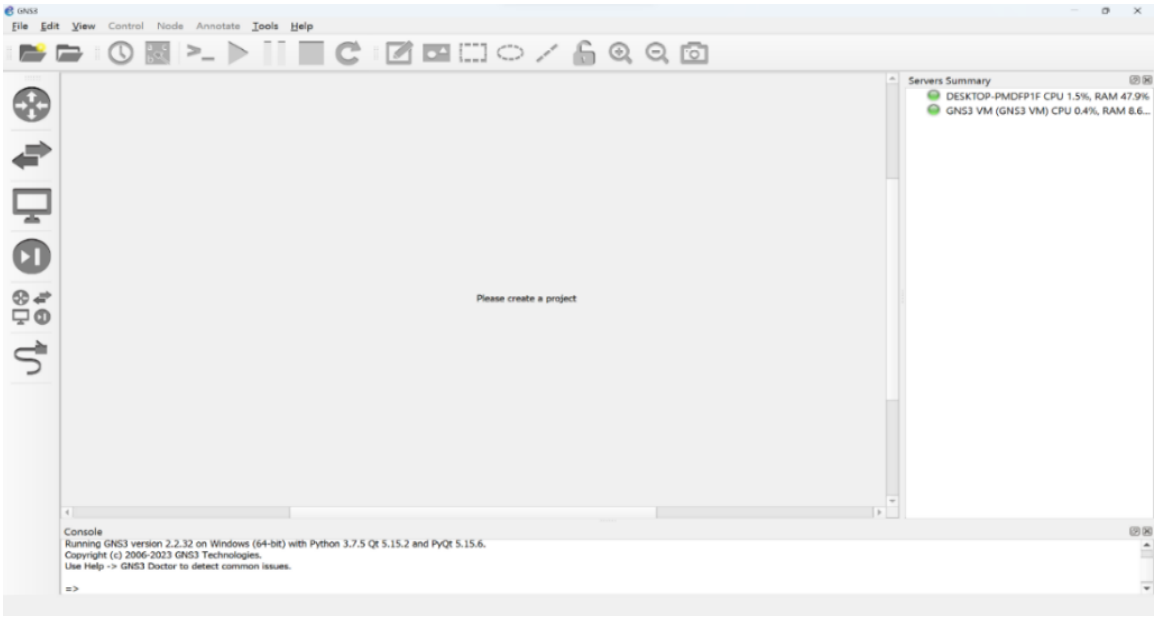
Our thesis focuses on securing the local network of SARL LAITERIE SOUMMAM, emphasizing the installation and configuration of security solutions. We implemented RADIUS-based authentication for network access control and segmented the network into VLANs to enhance security. Furthermore, a Fortigate firewall was deployed to provide necessary authentication and filtering. Using GNS3 and VMWARE, we tested and validated our solutions. This study will bolster the reliability of SARL LAITERIE SOUMMAM's network, preserving data confidentiality and ensuring uninterrupted operations.

Annexe

Annexe 1 : GNS3 (Graphical Network Simulator 3)

- **Définition**

GNS3 est utilisé par des centaines de milliers d'ingénieurs réseau dans le monde entier pour émuler, configurer, tester et dépanner des réseaux virtuels et réels. GNS3 est un logiciel open source gratuit que vous pouvez télécharger à partir de http://gns3.com [25].



Interface principale de GNS3.

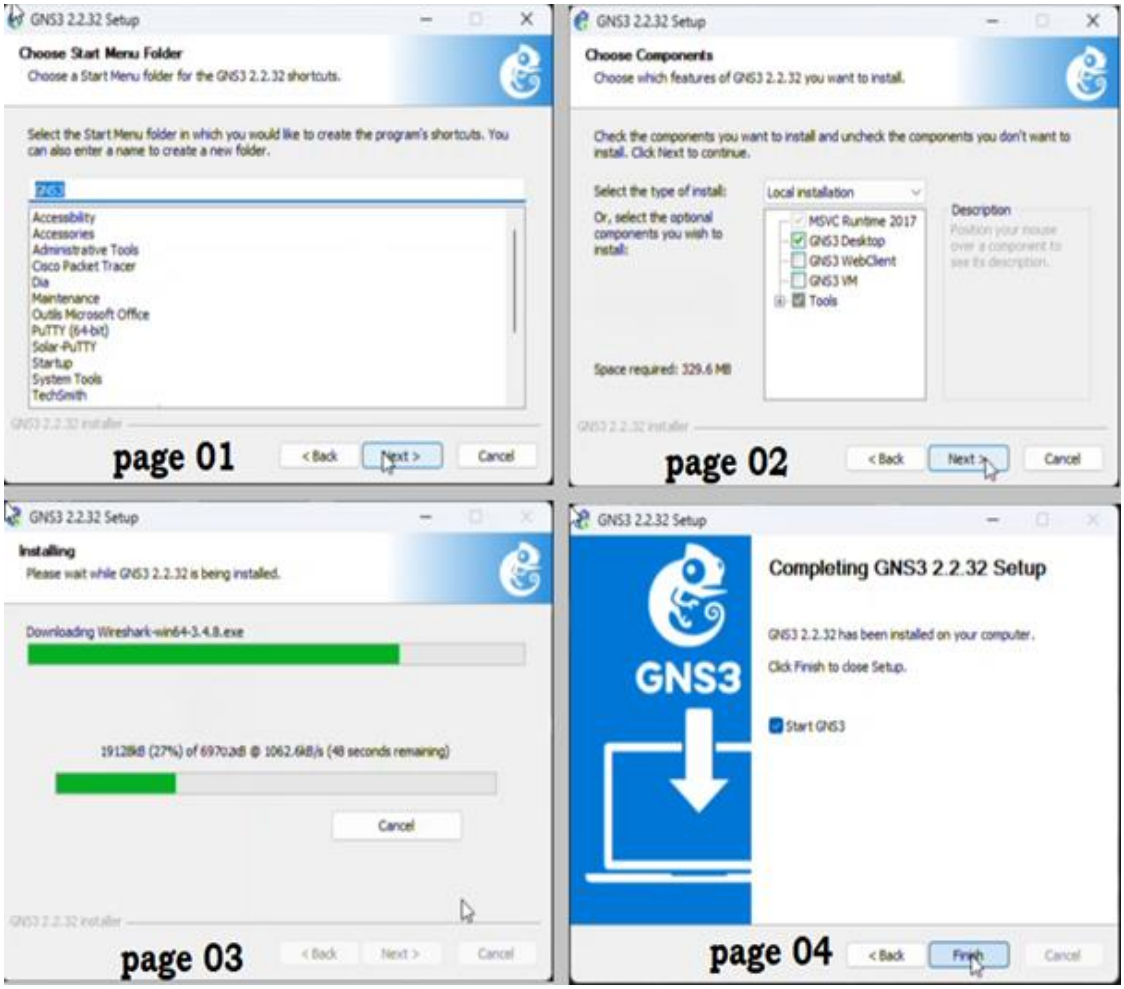
- **Architecture**

GNS3 se compose de deux composants logiciels :

- GNS3 GUI (Graphical User Interface) : est l'interface utilisateur graphique de GNS3, qui facilite la création, la configuration et la gestion des topologies réseau virtuelles. D'autre part elle permet de tester et de dépanner les configurations réseau sans avoir besoin du matériel réel. Enfin la GUI offre la possibilité d'enregistrer et charger des projets, les partager avec d'autres utilisateurs et travailler sur plusieurs projets simultanément.
- La machine virtuelle GNS3 (VM) : les périphériques créés doivent être hébergés et exécutés par un processus serveur. Pour cela nous avons le choix entre le pc sur lequel le logiciel est installé, la VM GNS3 locale a l'aide d'un logiciel de virtualisation [26].

- **Installation de GNS3 :**

Ci-dessous les étapes clé à suivre pour l'installation de GNS3

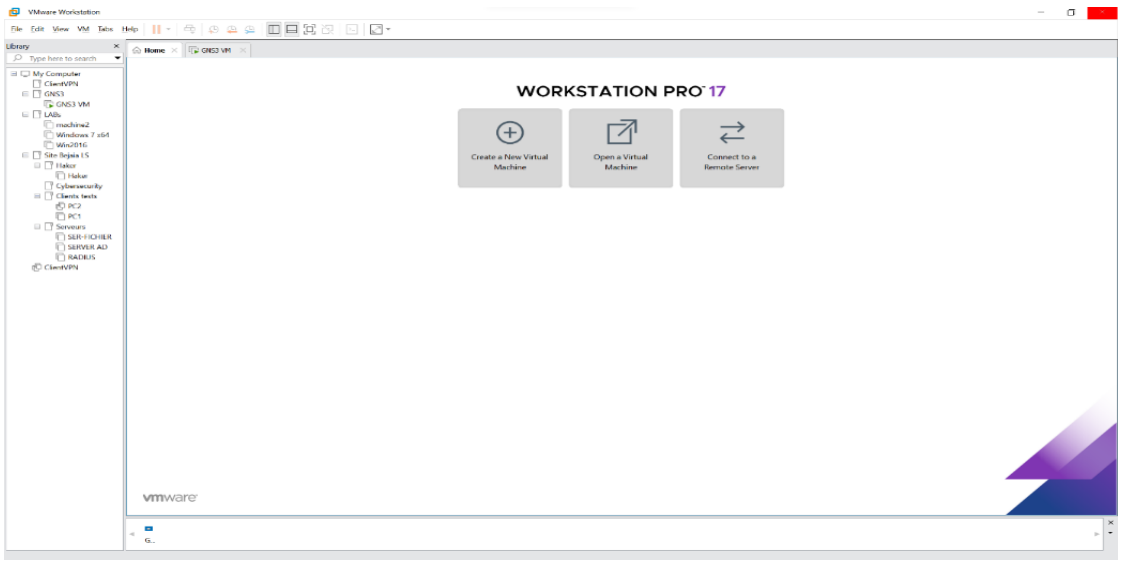


Installation GNS3

Annexe 2 : VMWARE WORKSTATION 17 PRO

- **Définition :**

VMware Workstation 17 Pro est un logiciel de virtualisation puissant qui permet d'exécuter plusieurs systèmes d'exploitation sur un seul ordinateur. Il offre un environnement isolé pour tester des applications, développer des logiciels ou exécuter des machines virtuelles pour diverses utilisations.

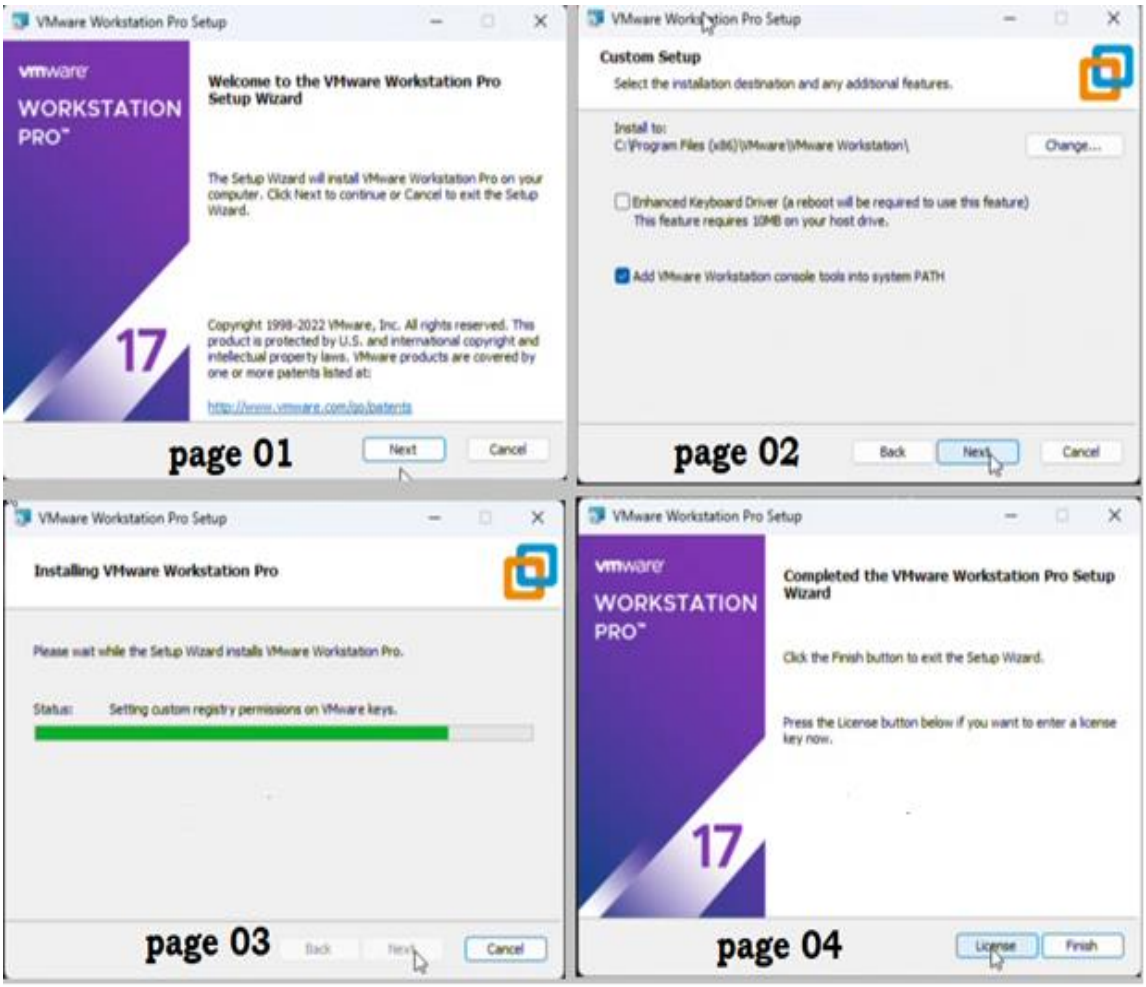


Interface principale de VMWare Workstation 17 pro.

Les caractéristiques clés de VMware Workstation 17 Pro incluent la possibilité d'exécuter plusieurs systèmes d'exploitation sur une seule machine, offrant ainsi une polyvalence pour les tests et le développement. Il fournit une isolation complète des machines virtuelles, permettant aux utilisateurs de travailler dans des environnements sécurisés sans interférence avec le système hôte. Avec des fonctionnalités réseau avancées, il permet aux utilisateurs de configurer des réseaux virtuels personnalisés pour tester des scénarios complexes. Les snapshots et les clones facilitent la gestion des configurations et des environnements de test. Enfin, VMware Workstation Pro offre des performances optimisées, garantissant une exécution fluide et réactive des machines virtuelles, même lorsqu'elles sont exécutées simultanément.

- **Installation de VMWARE WORKSTATION :**

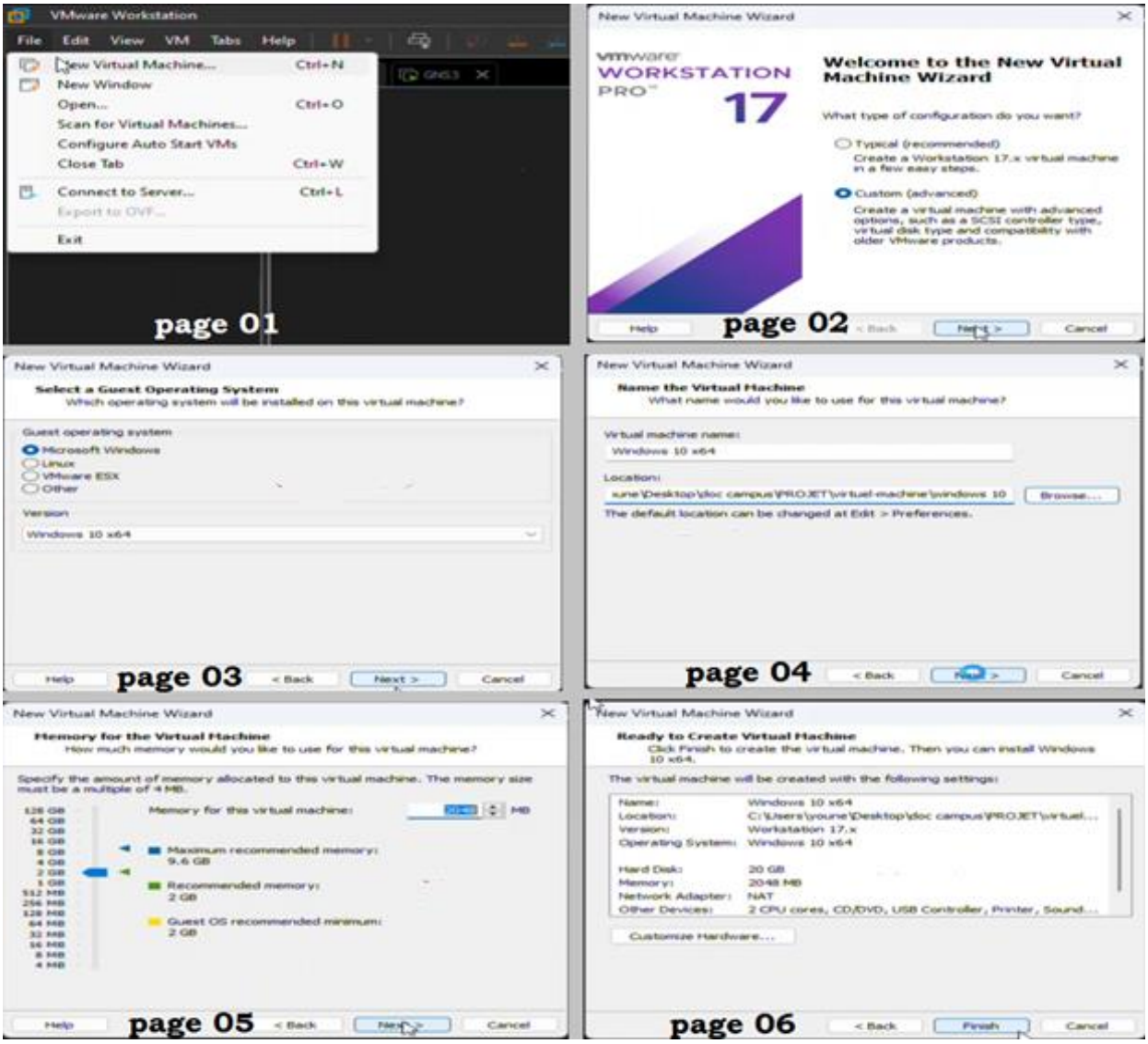
Après avoir télécharger ensuite ouvrir le fichier d'installation de VMWARE WORKSTATION 17 PRO voici quelques étapes à suivre lors de l'installation :



Installation VMWare Works Station 17 pro

Annexe 3 : création d'une machine virtuelle

Après l'installation des équipements de travail nous passons à l'installation des machines virtuels (Vms). La figure ci-dessus nous montre un exemple pour la création d'une VM qui contienne le système d'exploitation (Windows 10 professionnel).



Création d'une VM

Pour créer cette VM tout d'abord nous allons ouvrir VMware Workstation, pointer avec la souris sur « File » ensuite un seul clic sur « New Virtual Machine ». la figure précedente nous montre les paramaitre a configurer pour notre VM : choisir le type d'installation, spécifier le système d'exploitation, Nommé la VM, spécifier l'emplacement de l'installation et la mémoire RAM de la VM en Mégabit.

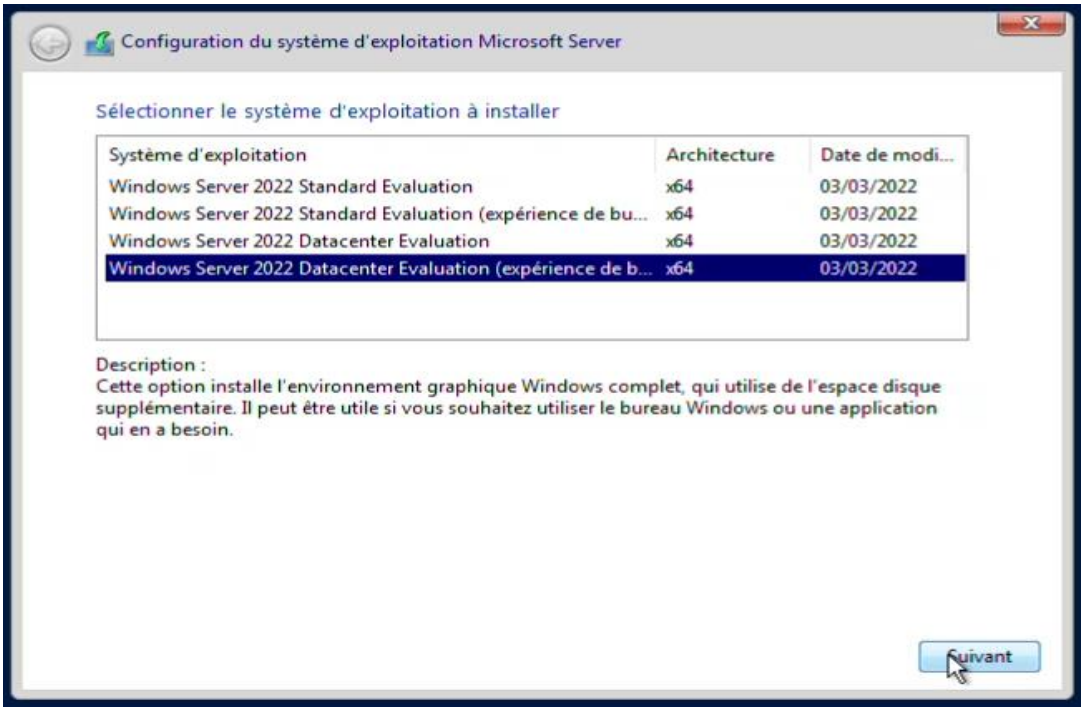
Annexe 4 : installation de Windows 10 pro sur la VM

Installation de Windows 10 professionnelle

Dans cette annexe nous avons donné un exemple sur l'installation d'un système d'exploitation qui est Windows 10 pro sur une VM. Tout d'abord nous avons besoin de l'image ISO du système d'exploitation en question. Ensuite pour compléter l'installation nous suivons les étapes clé illustré dans la figure précédente en passant par : la spécification de langue et région, choisir le type de système d'exploitation et partitionner le disque afin de choisir l'emplacement du système.

Annexe 5 : Installation de Windows serveur 2022

L'installation de Windows serveur 2022 est similaire a celle de window 10 la seule différence est dans l'étape, oú il faut choisir le système d'exploitation a installé dans le cas présent : Windows Server 2022 Datacenter Evaluation x64.

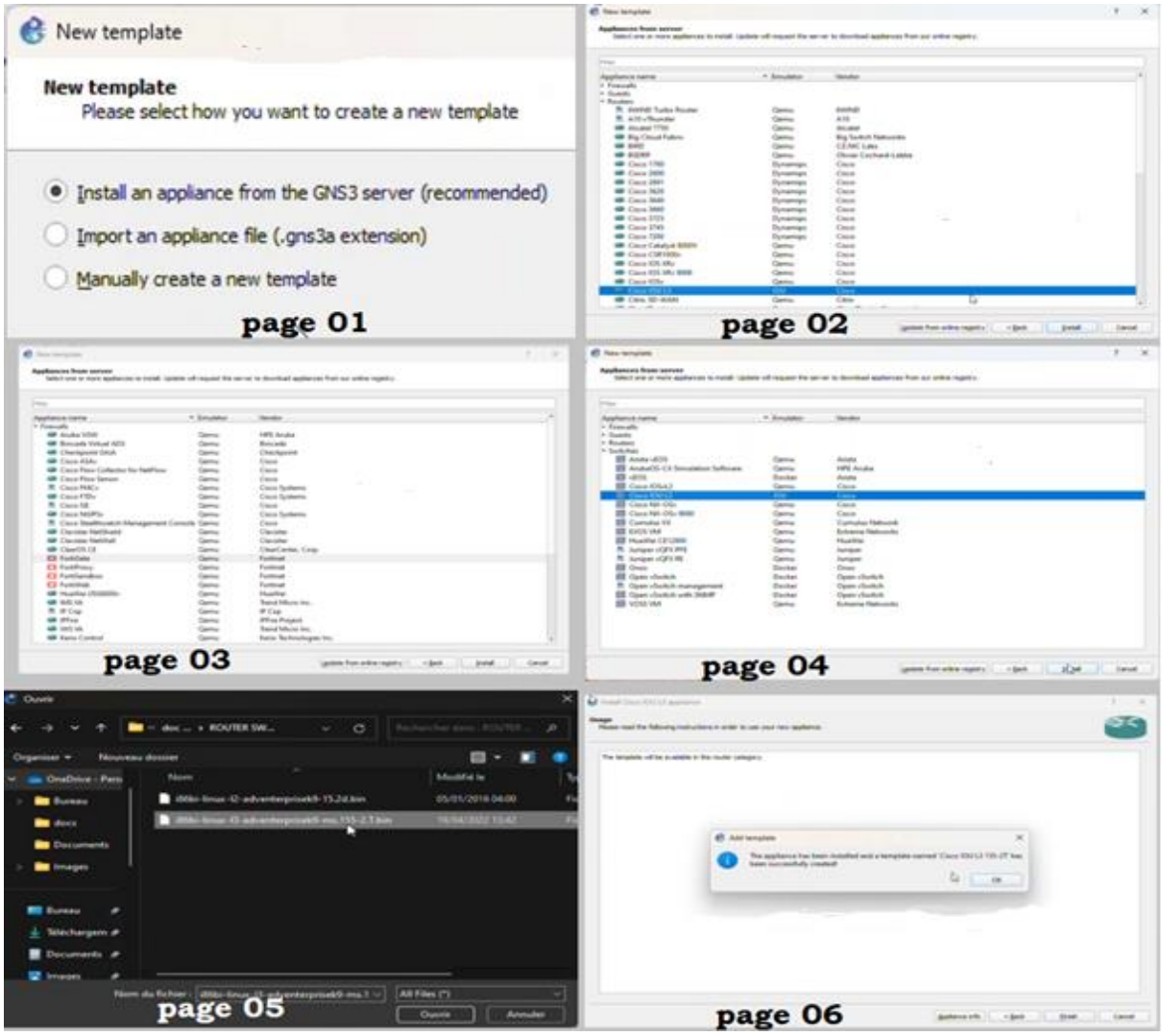


Installation Windows Serveur 22

Annexe 6 : L'ajout de Router, pare-feu et switch sur gns3

Pour installer un nouvel équipement qui ne figure pas déjà sur gns3, il faut suivre les étapes ci-dessous. Les trois installation (router, pare-feu et switch) sont similaire, la seule différence est dans la deuxième étape.

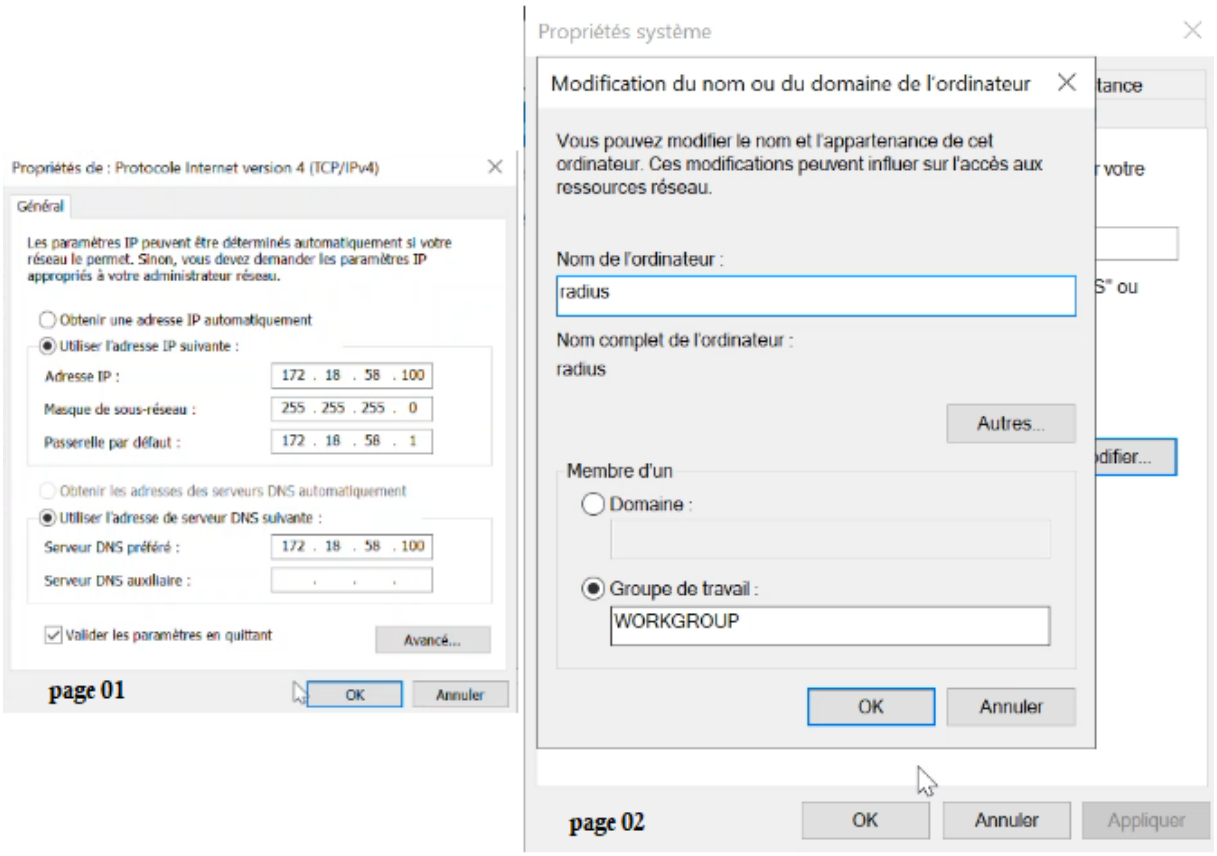
- Tout d'abord faut ouvrir gns3 ensuite cliquer sur « New Template » qui se trouve tout en bas à gauche dans la barre des Template déjà existante, ce qui nous mène à la page 01 dans la figure suivante pour choisir une procédure d'installation
- Dans la deuxième étape, il faut choisir le nouvel équipement à installer router, pare-feu et switch, comme nous l'avons montré respectivement pour chaque cas dans les pages 02, 03, et 04.
- Pour chaque nouvel équipement il nous faut télécharger puis importer l'image ISO qui va avec sur gns3, comme illustré dans la page 05.



Ajout des Templates

Annexe 7 : Configuration de base du serveur

La figure suivante montre quelques configurations de base pour notre serveur, nous avons configuré des adresses statiques comme nous l'avons montré sur la page 01 ensuite Dans la page 02 nous avons nommé le serveur puis le redémarrer afin d'appliquer les changements.



Configuration de base

Annexe 8 : Configuration de base des équipements de raccordements

Dans ce qui suit nous allons donner les configurations de base pour quelques équipements :

- Routeur

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#hostname Core1
Core1(config)#do wr                    page 01
```

```
Core1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core1(config)#interface ethernet 0/0
Core1(config-if)#no shutdown
Core1(config-if)#exit
Core1(config)#interface ethernet 0/1
Core1(config-if)#no shutdown
Core1(config-if)#ip address 10.0.1.2 255.255.255.252
Core1(config-if)#end                   page 02
```

Configuration de base pour routeur

La figure précédente nous montre les commandes qui nous ont permet de faire les configurations de base sur le routeur Core1 à savoir la nomination de l'équipement comme nous l'avons montré sur la page 01 ensuite la configuration des interface (l'activation et l'adressage) sur la page 02

- Firewall

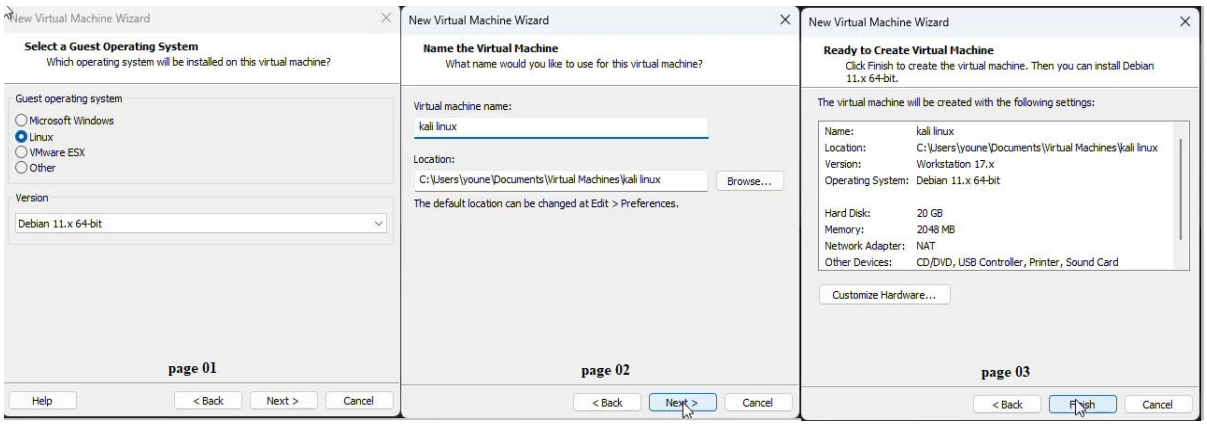
```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FG-LS
FortiGate-VM64-KVM (global) # end
FG-LS # config system interface
FG-LS (interface) # edit port1
FG-LS (port1) # set mode static
FG-LS (port1) # set ip 10.0.0.1/30
FG-LS (port1) # set allowaccess ping https http
```

Configuration de base pour le firewall

Nous avons commencé la configuration de notre pare-feu (Fortigate)par lui donner un nom (FG-LS) ensuite nous avons configurer le mode statique sur le port1 afin de porter quelques modifications (adressage et l'autorisation du ping, https et http). Port 1 sera associé au WAN, les mêmes commandes seront utilisées pour le port 2 qui sera associer au LAN et le port 3 de FG-LS pour la DMZ.

Annexe 9 : kali linux

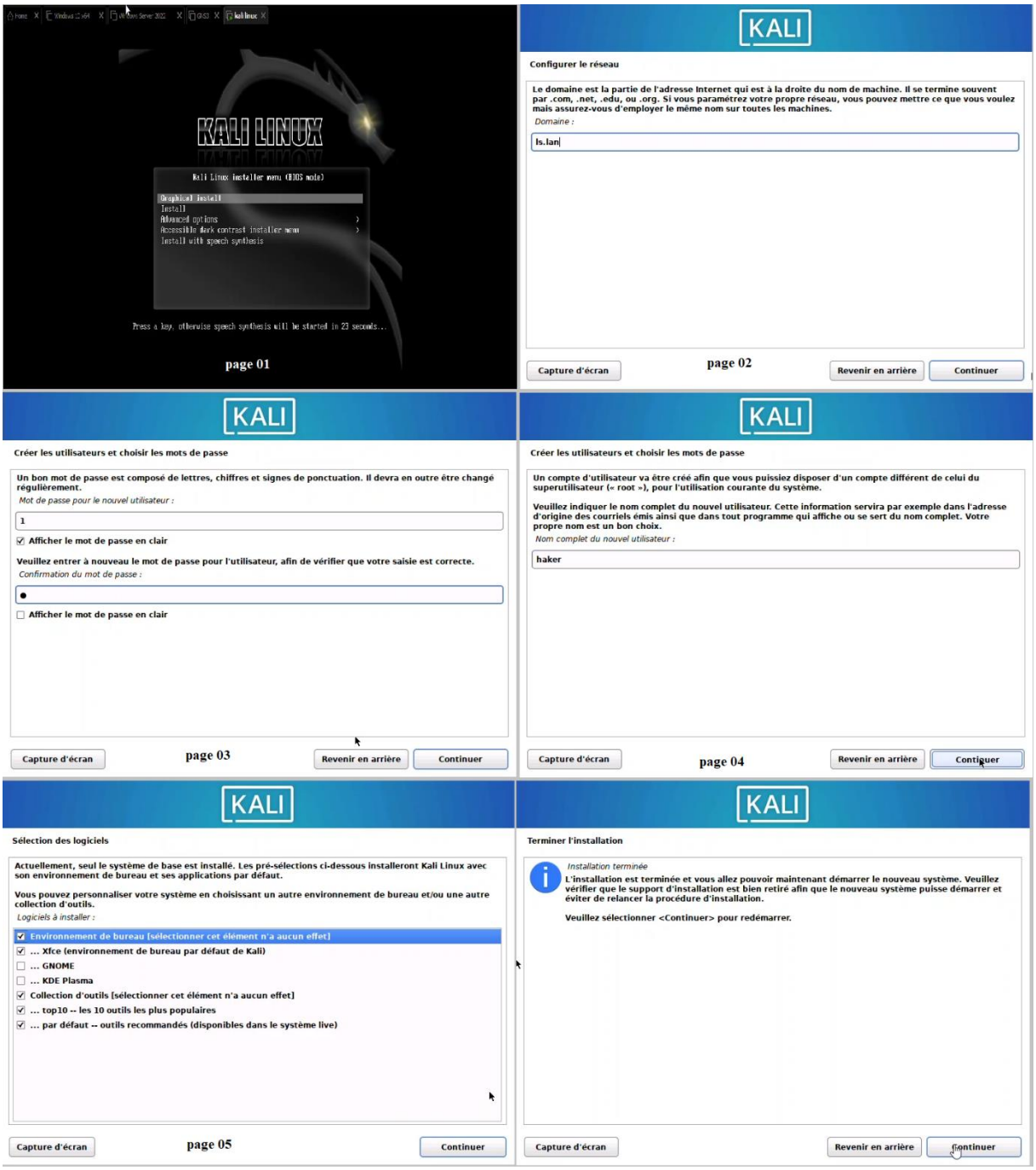
- **Création de la VM :**



Création de la VM

Les captures précédentes nous montrent quelques étapes lors de la création de notre VM pour contenir le système d'exploitation Kali Linux, dans la page 01 nous avons choisi le système d'exploitation, sur la deuxième page nous avons nommé « kali linux » pour notre VM, la dernière page est récapitulative des informations sur la VM.

- **Installation de kali linux sur la VM**



Installation de kali linux

La figure précédente nous montre quelques captures prise lors de l'installation de kali linux. L'installation commence sur la page 01 où nous avons choisi le type de système d'exploitation « Graphical Install », sur les pages 02,03 et 04 nous avons spécifier le domaine, le nom d'utilisateur et le mot de passe. Sur la page 05 nous avons choisi les logiciels à installer et enfin la dernière page nous montre la fin de l'installation.

Interface d'accueil sur kali linux

- **Explication des commandes lors des attaques effectués sur kali linux**

- **La commande HPING3 [26]**

HPING3 est un utilitaire réseau qui vous permet d'envoyer des paquets TCP/IP personnalisés et d'afficher les réponses cibles comme le fait la commande ping avec les réponses ICMP.

Voici quelques exemples des opérations effectuées par HPING3 :

- Tester les règles de pare-feu.
- Découvrez le chemin MTU.
- Traçage sous différents protocoles.
- Audit de la pile TCP/IP.

Dans ce qui suit nous allons présent la syntaxe pour utiliser la commande HPING3 et décrire quelques options :

$ sudo hping3 -S 192.168.5.10 -a 192.168.50.129 --flood

- -c, --count : spécifie le nombre de paquets à envoyer
- -a, --spoof : adresse source de l'usurpation
- -S, --syn : envoyer des paquets synchrones
- --flood : permet d'effectuer d'inondation du réseau par des paquets.