

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Abderrahmane Mira



Faculté de la Technologie

Département d'Automatique, Télécommunications et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Thème

Etude et mise en place d'une infrastructure réseau sécurisée.

Préparé par :

- **BERKANI Djedjiga**
- **BOUZERIA Massylia**

Dirigé par :

Mr. Abdelhani Diboune

Examiné par :

Mr. Azni (président)

Mme. Mammeri (examinatrice)

Année universitaire : 2021/2022

Remercîment



*Tout d'abord, nos remerciements au bon dieu **ALLAH**, le grand et l'infini et le tout puissant de nous avoir illuminées et ouvert les portes du savoir et nous avoir données la volonté, la santé et le courage pour effectuer ce travail.*

*Nous remercions notre promoteur « **Mr Abdelhani DIBOUNE** » d'avoir accepté de nous encadrer et de nous orienter pour la réalisation de notre projet, ainsi que pour sa confiance, ses encouragements, ses corrections et pour les conseils qu'il nous a apporté. Nous tenons également à remercier l'ensemble des membres de jury « **Mr Azni (p) et Mme Marmmeri** » pour l'intérêt qu'ils ont portés à notre recherche en acceptant d'examiner notre travail et de l'enrichir par leurs propositions.*

*Et de manière spéciale, nous exprimons nos chaleureux remerciements pour notre encadreur de stage « **Mr Djebbari Yassine** » qui nous a donné l'opportunité de nous familiariser avec le milieu de travail.*

Nous tenons également à remercier toutes nos familles, nos amis(es), nos collègues étudiants et tous ceux qui ont participé de près ou de loin à la réalisation de ce travail.

Merci à tous.

Dédicaces



Je remercie Allah de m'avoir donné la force et le courage pour pouvoir réaliser ce modeste travail.

Avec un énorme plaisir, un cœur ouvert et une immense joie que je dédie ce modeste travail :

*À mes très chers parents « **Nouara et Loucif** que j'aime énormément », pour leur patience, leur amour, leur encouragement et leur sacrifice tout au long de mon parcours et que dieux vous garde en bonne santé pour nous ;*

*À ma cher et petite sœur « **Dihia** » ; que le bon dieu te garde pour nous, ma lumière ;*

*À mon seul et petit frère « **Lakhdar** » ; tu resteras mon petit pour toujours et je te souhaite réussir dans ton bac ;*

*À mes chers « **Dada Said, dada khaled et dada Nouredine** » ainsi que leurs familles ;*

*À ma grande sœur et ma meilleure amie « **Syrine** » ; merci pour ta présence et ton soutien ma belle ;*

*À mon meilleur ami « **karim** » ainsi que sa famille, merci pour tous les bons moments que nous avons passé durant cette période ;*

*À ma meilleure amie « **Dehia** », merci pour ta présence et ton soutien ma belle ;*

*Et surtout à Mes Grands-parents « **yemma Baya et yemma Tata** que le bon dieu l'accueille dans son vaste paradis » et « **Lakhdar et Ramtane** que le bon dieu les accueillent dans son vaste paradis »*

À toute ma famille;

*À mon cher binôme **Massylia** ainsi qu'à sa famille ;*

À tous mes amis(es) surtout;

Et à tous ceux qui m'ont aidé de près ou de loin à l'élaboration de ce travail.





Avec un énorme plaisir, un cœur ouvert et une immense joie que je dédie ce modeste travail :

À mes très chers parents pour leur patience, leur amour, leur encouragement et leur sacrifice durant mes études. Aucun hommage ne pourra être à la hauteur de l'amour dont ils ne cessent de me combler. Que dieu leurs procure bonne santé et longue vie ;

*À mes très chers frères « **Massi** et **Syphax** » ; pour leur amour et compréhension Et qui ont été toujours des très bons exemples pour moi ;*

*Au fils de ma tante « **AMAR** » à qui je souhaite un avenir radieux plein de réussites ; Et surtout à Mes Grands-parents, « **Aicha** à qui je souhaite une longue vie et une bonne santé et **Hamid, Djohra et Makhlouf** que le bon dieu les accueillent dans son vaste paradis » ;*

À toute ma famille pour leur soutien tout au long de mon parcours universitaire.

Merci d'être toujours là pour moi ;

*À mon cher binôme **Djedjiga** ainsi que sa famille ;*

À tous mes amis(es);

Et à tous ceux qui m'ont aidé de près ou de loin à l'élaboration de ce travail.



Table des matières

Remercîment.....	i
Table des figures.....	x
Liste des tableaux	xi
Liste des abréviations	xii
Introduction Générale.....	1
I Généralités sur les réseaux informatiques	2
I.1 Introduction	2
I.2 Définition	2
I.3 Classifications des réseaux	3
I.3.1 Classification selon la taille.....	4
I.3.2 Classification selon la topologie.....	5
I.3.3 Classification selon le mode de communication.....	7
I.4 Modelé hiérarchique.....	9
I.4.1 La couche cœur de réseau (Core layer).....	9
I.4.2 La couche distribution (Distribution layer).....	10
I.4.3 La couche d'accès (Access layer).....	10
I.5 Architecture des réseaux.....	10
I.6 Encapsulation des données	13

I.7	Conclusion Le protocole IP	14
I.7.1	L'adresse IP	15
I.8	Conclusion	16
II	Initiation à sécurité des réseaux informatique	17
II.1	Introduction	17
II.2	Sécurité des systèmes informatiques (SSI)	17
II.3	La terminologie de la sécurité	18
II.4	Principes de la sécurité informatique	18
II.5	Les attaques	20
II.5.1	Définition de l'attaque	20
II.5.2	Les types d'attaques informatiques	20
II.5.3	Exemples d'attaques informatiques	21
II.6	Mécanismes de défense	24
II.6.1	Antivirus	24
II.6.2	Chiffrement	25
II.6.3	Pare-feu	26
II.6.4	Proxy	26
II.6.5	Système de détection d'intrusion	27
II.6.6	Système de prévention d'intrusion	28
II.7	CONCLUSION	28
III	Présentations L'organisme d'accueil	29
III.1	INTRODUCTION	29
III.2	Partie 1 : Présentations de l'entreprise "CAMPUS NTS"	29
III.2.1	Création et évolution	29
III.2.2	La localisation de l'entreprise	30
III.2.3	Fiche technique	31
III.2.4	Objectifs, missions et activités de l'entreprise « N.T.S »	32
III.2.5	Organigramme général de l'organisme d'accueil	32
III.3	Partie 2 : Etat des lieux	38
III.3.1	Présentation du réseau campus NTS	38

III.4	Partie 3 : Problématiques et Solutions proposées	41
III.4.1	Problématiques	41
III.4.2	Solutions.....	42
III.5	CONCLUSION.....	42
IV	Réalisation.....	43
IV.1	Introduction	43
IV.2	Environnement de travail	43
IV.2.1	Présentation de logiciel de simulation.....	43
IV.2.2	Partie hardware.....	44
IV.2.3	Partie software.....	45
IV.2.4	Serveurs et Services.....	45
IV.3	La nouvelle architecture proposée.....	46
IV.3.1	Le plan d’adressage des sous réseaux « VLANs ».....	47
IV.3.2	Plan d’adressage des Privates VLANs et ports associés	47
IV.3.3	Plan d’adressage des équipements d’interconnexion	48
IV.3.4	Tableau du routage inter-vlan et du protocole HSRP.....	49
IV.4	Configuration de l’active Directory.....	49
IV.5	Configuration de relais DHCP	52
IV.6	Création d’un groupe et utilisateurs radius.....	53
IV.7	Configuration du Sophos UTM.....	60
IV.7.1	Création des interfaces « DMZ, LAN1, LAN2, Internet ».....	60
IV.7.2	Routage statique	61
IV.7.3	Filtrage sur pare-feu.....	62
IV.7.4	Le NAT.....	63
IV.7.5	VPN(Virtual Private Network)	64
IV.7.6	Configuration du VPN site à site IPSec.....	64
IV.7.7	Configuration du protocole IKE pour l’échange des clés	64
IV.7.8	Création de connexion IPSec.....	65
IV.7.9	Configuration du VPN client à site	66

IV.8	Configuration des équipements	70
IV.8.1	Configuration des commutateurs	70
IV.8.2	Configuration des interfaces trunk.....	70
IV.8.3	Configuration d'un domaine VTP	70
IV.8.4	Création des VLANs	71
IV.8.5	Configuration des interfaces au mode d'accès vlan.....	72
IV.8.6	Configuration VLAN natif.....	73
IV.8.7	Configuration du protocole LACP « l'agrégation des lien 802.3ad ».....	73
IV.8.8	Configuration du protocole SSH « Secure Shell »	74
IV.8.9	Vérification de la prise en compte du protocole ssh par l'IOS	74
IV.8.10	Configuration des VLANs privées pour notre réseau DMZ.....	77
IV.8.11	Configuration des routeurs.....	78
IV.8.12	Configuration du Routage Passerelle Par Défaut.....	79
IV.8.13	Configuration du protocole HSRP	80
IV.9	Tests.....	81
IV.9.1	Test DHCP et Active Directory.....	81
IV.9.2	Test SSH.....	85
IV.9.3	Test port Security	85
IV.9.4	Test Radius	86
IV.9.5	Test routage statique	87
IV.9.6	Test les pare-feu Bejaia et Alger	87
IV.9.7	Vérification du tunnel VPN	88
IV.9.8	Test de connexion RDP de puis Alger vers Bejaia.....	89
IV.9.9	Test DMZ.....	90
IV.10	Conclusion	90
	Conclusion générale.....	91
	ANNEXES.....	92
	Bibliographie	123

Table DES figures

I.1	Les composantes d'un réseau informatique	3
I.2	Classification d'un réseau informatique.	3
I.3	La taille des différentes catégories de réseaux informatiques	4
I.4	Les topologie physiques.	6
I.5	Fonctionnement d'un client /serveur.	8
I.6	Réseau poste à poste.	8
I.7	Modèle de conception hiérarchique à trois couches.	9
I.8	L'architecture des modèles OSI et TCP /IP	11
I.9	Principe d'encapsulation des données	14
I.10	Les trois caractéristiques de base de protocole IP	14
I.11	Exemple d'une l'adresse IPv4.	15
I.12	Masque de sous-réseau.	15
II.1	Les cinq dimensions de la sécurité informatique.	18
II.2	Attaque passive.	20
II.3	Attaque active	21
II.4	Attaque DOS et DDOS	24
II.5	Mécanismes de défense.	24
II.6	Le chiffrement symétrique.	25
II.7	Le chiffrement asymétrique.	25
II.8	Pare-feu	26
II.9	Proxy	27
III.1	Localisation de l'entreprise NTS.	30
III.2	Objectifs, Missions et Activités de l'NTS.	32
III.3	L'organigramme de campus NTS.	32
III.4	Organigramme de service d'accueil.	34

III.5 Architecture de réseau (NTS).....	38
IV.1 Logo de GNS3.....	44
IV.2 Logo de VMware Workstation 16.....	44
IV.3 Nouvelle architecture réseau de l'entreprise NTS.....	46
IV.4 Rôle AD DS et DNS	50
IV.5 Création des groupes, utilisateurs, ordinateurs	52
IV.6 Configuration de relais DHCP sur le router core1 pour le vlan 100.	52
IV.7 Création des utilisateurs et groupe radius.....	53
IV.8 Configuration d'une stratégie de connexion radius.	55
IV.9 Configuration de clients Radius.	56
IV.10 Stratégie radius configurée pour les utilisateurs.....	59
IV.11 Mise à jour des stratégies GPO.	59
IV.12 Les interfaces de Sophos UTM.	61
IV.13 Le routage statique.....	61
IV.14 Filtrage sur le pare-feu.	62
IV.15 Les règles de Nat sur Sophos Bejaia et Alger.	63
IV.16 Les passerelles distance de VPN.....	64
IV.17 La connexion IPSec « ESP ».....	65
IV.18 Connexion établie entre les deux sites bejaia et alger	66
IV.19 Configuration d'accès à distance SSL	67
IV.20 Configuration d'accès à distance SSL	69
IV.21 Configuration trunk sur le switch distribution DIS1.....	70
IV.22 Configuration trunk sur le switch d'accès S-access1.....	70
IV.23 Configuration VTP serveur sur le switch distribution DIS1	70
IV.24 Configuration VTP client sur le switch d'accès S-access1.....	71
IV.25 Création des VLANs sur le switch et vérification.....	72
IV.26 Configuration Access sur le switch Access et vérification.....	72
IV.27 Sécurisation du VLAN natif sur switch distributions et switch d'accès et vérification....	73
IV.28 Configuration du protocole LACP et vérification.....	74
IV.29 Vérification de la version system Ios Cisco.	74
IV.30 Configuration du protocole SSH sur le router core 2.....	75
IV.31 Configuration des ports security sur le switch access SWA1.....	76
IV.32 Configuration du client Radius sur le switch DIS2.....	76
IV.33 Configuration du mode VTP transparent sur le Switch DMZ et vérification.....	77
IV.34 Création des PVLANS Community sur le Switch DMZ.....	77
IV.35 Création des PVLANS Isolated sur le Switch DMZ.....	77
IV.36 Création des PVLANS primary sur le Switch DMZ.	78
IV.37 Affectation des ports aux PVLANS sur le Switch DMZ.....	78
IV.38 Configuration des interfaces sur le routeur1 et vérification.....	78

IV.39	Le routage sur le core 1.....	79
IV.40	Vérification de routage sur le core 1.....	79
IV.41	Configuration de HSRP sur le routeur1 et vérification.....	80
IV.42	Configuration de HSRP sur le routeur 2 et vérification.....	81
IV.43	Test dhcp réussi.....	82
IV.44	Test Active directory réussi.....	84
IV.45	Test SSH réussi.....	85
IV.46	Test réussi le port est down après la violation.....	85
IV.47	Test Radius réussi pour le client b.massyia.....	86
IV.48	Ping réussi vers le serveur google « internet ».....	87
IV.49	Ping réussi sur le pare-feu Bejaia.....	87
IV.50	Ping réussi sur le pare-feu Alger.....	88
IV.51	capture WireShark qui montre la négociation ISKAMP du tunnel vpn.....	88
IV.52	Ping réussi depuis le PCo1 Alger vers serveur Bejaia.....	88
IV.53	Accéder à distance en utilisant le VPN client to site.....	89
IV.54	Test DMZ.....	90
IV.55	Installation de GNS3.....	94
IV.56	l'interface GNS3.	94
IV.57	Installation de VMware Workstation version 16.1.2.	97
IV.58	Liaison GNS3 VM et GNS3 Client.	98
IV.59	Installation du Windows server 2022.....	103
IV.60	Installation du Windows 10 sous VMware Workstation.	107
IV.61	L'installation de l'Active Directory.	111
IV.62	Certificat de l'Active Directory.	113
IV.63	Installation de Dynamics Host Configuration Protocol.	116
IV.64	L'installation du rôle NPS	119
IV.65	Inscription radius avec active directory.	120
IV.66	Installation Firewall Sophos UTM.	121

LISTE DES TABLEAUX

I.1	Les classes d'adresse IP et Masque réseau.....	16
III.1	Identification sur campus NTS.....	31
III.2	L'environnement hardware et le software.....	39
III.3	Détails des ressources disponibles de l'entreprise.....	40
IV.1	Plan d'adressage des VLANs.....	47
IV.2	Plan d'adressage des sous(sous-réseaux) Private VLAN.....	47
IV.3	Plan d'adressage des équipements d'interconnexion.....	48
IV.4	Plan d'adressage des sous(sous-réseaux) Private VLAN.....	49

LISTE DES abREVIATIONS

A

AD : *Active Directory.*

AD CS : *Active Directory Certificat Services.*

AH : *Authentication Header.*

ARP : *Address Resolution Protocol.*

C

CDP : *Cisco Discovery Protocol.*

CSMA/CD : *Carrier Sense Multiple Access with Collision Detection.*

D

DDOS : *Distributed Denial of Service.*

DHCP : *Dynamics Host Configuration Protocol.*

DMZ : *Demilitarized Zone.*

DNS : *Domaine Name System.*

DOS : *Denial Of Service.*

E

EAP : *Extensible Authentication Protocol.*

ESP : *Encapsulating Security Payload.*

F

FAI : *Fournisseurs d'accès à Internet.*

FDDI : *Fibre Distributed data interface.*

G

Gns3 : *Graphical Network Emulator.*

H

HIDS : *Host Based Intrusion Detection System.*

HIPS : *Host based IPS.*

HSRP : *Hot Standby Routing Protocol.*

I

ICMP : *Internet Control Message Protocol.*

IDS : *Intrusion Detection System.*

IKE : *Internet Key Exchange.*

IOS : *International Organisation For Standardisation.*

IP : *Internet Protocol.*

IPS : *Intrusion Prévention System.*

ISAKMP : *Internet Security Association and Key Management Protocol.*

IPSec : *Internet Protocol Security.*

L

LACP : *Link Aggregation Control Protocol.*

LAN : *Local Area Network.*

LDAP: *Lighweight Directory Access Protocol.*

M

MAN : *Metropolitan Area Network.*

MAU : *Multistation Access Unit.*

N

NAT : *Network Adresse Translation.*

NBA : *Network behavior analysis.*

NBIDS : *Network-Based Intrusion Detection System. **

NIPS : *Network based IPS.*

NTS : *New Technology & Solutions.*

NPS: *Network Policy Server.*

O

OS : *Operating System.*

OSI : *Open Systems Interconnection.*

P

PAN : *Personal Area Network.*

R

RARP : *Reverse Address Resolution Protocol.*

RADIUS: *Remote Authentication Dial-In User Service.*

RDP: *Remote Desktop Protocol.*

S

SSH : *Secure Shell.*

T

TCP/IP : *Transmission Control Protocol/Internet Protocol.*

U

UDP : *User Datagram Protocol.*

V

Vlan : *Virtual Local Area Network.*

VPN : *Virtual Private Network.*

VTP : *VLAN Trunking Protocol.*

W

WAN : *Wide Area Network.*

WIPS : *Wireless based IPS.*

INTRODUCTION gÉNÉRALE

De nos jours, les réseaux informatiques occupent une place très importante au sein de chaque entreprise. Ces derniers permettent de connecter et d'assurer la communication entre les systèmes distribués d'infrastructures séparées. Néanmoins, ces réseaux deviennent également sujets à des attaques et des menaces de sécurité, ce qui présente une sensibilité accrue à leur bon fonctionnement. Pour cette raison, il est devenu incontestablement primordial d'anticiper ces attaques et d'établir une étude aussi exhaustive que possible de toutes les menaces afin d'aboutir à une politique de sécurité complète permettant de contourner ces failles de sécurité et prémunir contre toute sorte d'attaques sans pour autant trop altérer les performances du réseau et ses impacts sur le bon fonctionnement des systèmes d'information de l'entreprise. Dans ce contexte, la nécessité de mettre en place d'autres mécanismes de sécurité permettant protéger l'intégrité et la confidentialité des données sur les différents niveaux, tels que les PVLAV, VPN et les Pare-feux, etc.

Les travaux de notre projet de fin d'études s'inscrivent dans le cadre de projet de sécurisation des infrastructures réseau de l'entreprise N.T.S en utilisant un ensemble de technologies tels que les Pare-feux, les PVLAV, et les VPN, etc. Pour ce faire, nous avons structuré notre mémoire en quatre chapitres :

Le premier chapitre présente brièvement quelques généralités sur les réseaux informatiques. Il décrit les propriétés d'un réseau informatique et les modèles réseaux en couche. Ce chapitre termine par une description du protocole IPv4, un des principaux protocoles sur lequel repose le fonctionnement de certaines technologies de sécurité réseau utilisées dans le cadre de notre projet.

Dans le deuxième chapitre, nous abordons la sécurité informatique, nous commençons par présenter les différentes attaques réseau existantes ainsi que les différents mécanismes largement utilisés pour la sécurisation du réseau.

Le troisième chapitre a pour objectif d'expliquer l'organisme d'accueil N.T.S et sa structure organisationnelle hiérarchique. De plus, il évoque la problématique traitée dans le cadre de notre projet de fin d'études et les solutions adoptées.

Le dernier chapitre, est consacré à la réalisation d'une nouvelle architecture réseau sécurisée sur le simulateur réseaux « GNS3 ». Les tests et les résultats des différentes configurations y sont détaillés. Enfin, nous terminons le mémoire par une conclusion générale et quelques perspectives.

GénéRALITES SUR LES REseaux

INFORMATIQUES

I.1 Introduction

Les réseaux informatiques sont nés du besoin de communication des terminaux distants entre eux. Ils apportent beaucoup aux entreprises et à la société, ce qui les rend essentiels. Leur but est d'assurer l'interconnexion des ordinateurs afin qu'ils puissent communiquer entre eux et échanger des données.

Dans ce chapitre, nous allons définir quelques notions fondamentales sur les réseaux informatiques dans lesquels nous ferons référence à la classification des réseaux ainsi que son architecture (modèle OSI et modèle TCP) et, on va terminer par un aperçu sur le protocole IP qui est un protocole de base dans le réseau.

I.2 Définition

Un réseau informatique est un ensemble de dispositifs matériels et logiciels reliant les uns aux autres pour partager des ressources (données) selon des règles bien définies (également appelées protocoles) [1]. Il est composé d'un ensemble des nœuds (PC, Smartphone, Répéteur, Hub, Switch, Routeur, Firewall, etc.) et un ensemble des arcs (câble réseau, Wifi, fibre optique, Satellite), comme illustré dans la figure suivante :

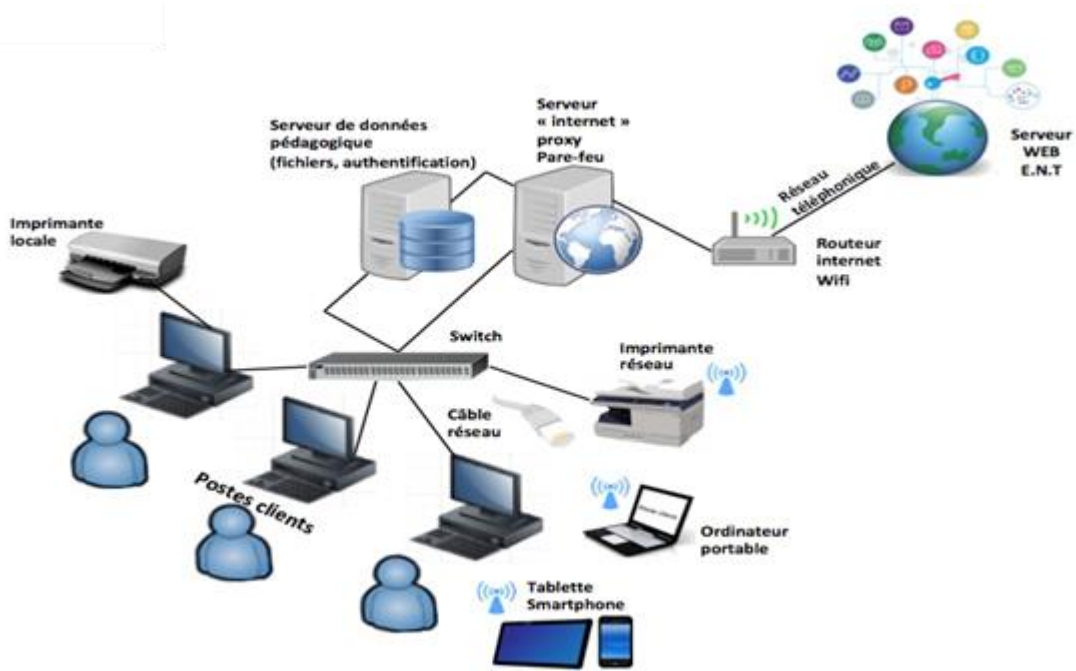


FIGURE I.1 – Les composantes d'un réseau informatique.

Les réseaux informatiques peuvent servir à plusieurs buts différents [2] :

- Réduire les coûts en partageant les données et les périphériques (fichiers, applications, etc.).
- Standardisation des applications.
- Accéder aux données en temps opportun.
- La communication et l'organisation sont plus efficaces et plus rapides.

I.3 Classifications des réseaux



FIGURE I.2 – Classification d'un réseau informatique.

I.3.1 Classification selon la taille

Est la classification la plus utilisée et la plus citée qui répertorie les réseaux selon la taille géographique. Généralement, elle est présentée sur quatre classes :

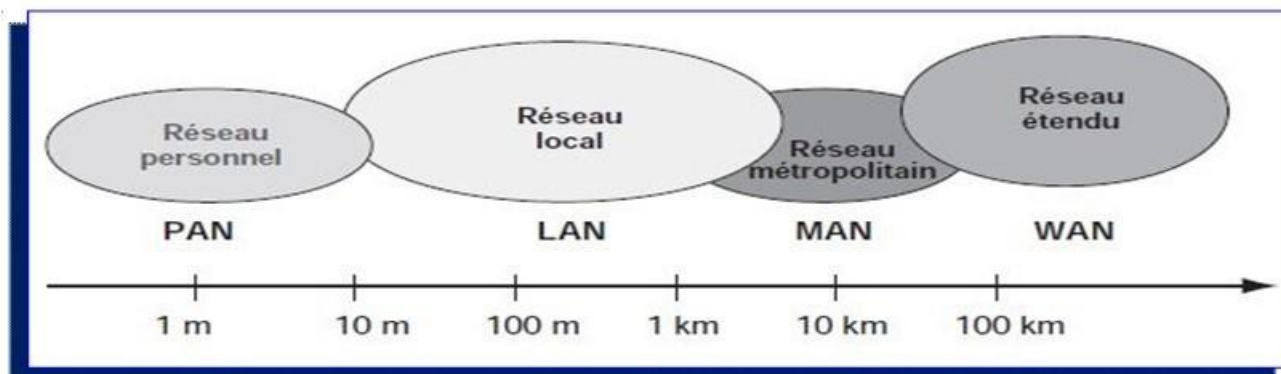


FIGURE I.3 – La taille des différentes catégories de réseaux informatiques [3]

I.3.1.1 Réseau personnel (PAN, pour Personal Area Network)

Un réseau PAN aussi appelé réseau domestique ou réseau individuel regroupe des équipements dans un rayon de 10 mètres [4]. Ces équipements appartiennent généralement à un même utilisateur comme : Un téléphone portable avec ses accessoires, un ordinateur avec ses périphériques et Bluetooth.

I.3.1.2 Réseau local (LAN, pour Local Area Network)

Un réseau LAN est un réseau qui géographiquement limité à moins de 10km avec un débit élevé de 10 à 100Mbit/s et fait partie des réseaux les plus répandus [4]. Il permet de relier des machines dans un bureau, dans un bâtiment, dans un campus- universitaire ou même dans une maison. Il est possible dans un réseau LAN d'utiliser un seul câble pour relier toutes les machines.

I.3.1.3 Réseau métropolitain (MAN, pour Metropolitan Area Network)

Un réseau MAN est également nommé réseau fédérateur. On rencontre ce type de réseau dans une ville ou dans les régions. Il assure des communications sur de plus longues distances et il est généralement utilisé pour relier plusieurs réseaux locaux par exemple les campus, les administrations.

Un MAN se compose de commutateurs ou de routeurs interconnectés par des liaisons à haut débit (généralement des fibres optiques).

I.3.1.4 Réseau étendu (WAN, pour Wide Area Network)

Un réseau WAN est un réseau à longue distance qui couvre une zone géographique importante telle qu'un pays, un continent ou même toute la terre. Ces réseaux sont généralement l'interconnexion de plusieurs réseaux LAN et MAN. Ils fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau. Le WAN le plus connu est l'internet public qui tire son nom de cette qualité : Inter Networking, ou interconnexion de réseaux.

I.3.2 Classification selon la topologie

La topologie d'un réseau est la représentation géométrique de tous les liens et dispositifs entre eux. Elle est aussi appelée le schéma de base, l'architecture ou le plan. Les topologies peuvent être classées en deux types de la manière la plus fondamentale :

I.3.2.1 Topologie physique

La topologie du réseau décrit comment les nœuds et les terminaux sont interconnectés entre utilisateurs. Il traite des bases de la mise en réseau, en ignorant de petits détails comme le transfert de données et le type d'appareil. On distingue principalement les types suivants :

❖ La topologie en bus :

Une topologie en bus, également appelée réseau en bus linéaire, est l'organisation de réseau la plus simple. Dans une topologie en bus, tous les ordinateurs sont reliés par des câbles à la même ligne de transmission, généralement coaxiale [5].

❖ La topologie en anneau :

Dans le cas où les extrémités d'un réseau de topologie en bus sont reliées entre elles, la topologie est dite topologie en anneau qui est une topologie de réseau fermé. Les ordinateurs communiquent chacun à leur tour. Ils sont en réalité reliés à un répartiteur (MAU, Multistation Access Unit) qui va gérer la communication entre eux en impartissant chacun un « temps de parole ».

❖ La topologie en étoile :

C'est la topologie la plus courante et plus coûteuse que les réseaux en bus et en anneau. Les ordinateurs du réseau sont reliés à un système matériel central appelé le point de concentration qui constitue le cœur du réseau. Les plus utilisés sont : le concentrateur (hub) (dans ce cas c'est une topologie en bus) et un commutateur (Switch).

❖ La topologie en maillée :

Une topologie maillée est une topologie hybride en étoile, mais avec des chemins d'accès différents d'un nœud à l'autre. C'est la méthode utilisée sur Internet : Pour les transmissions entre deux points, chaque nœud (routeur intelligent, techniquement appelé switch) choisira la route la plus rapide pour transmettre en temps réel.

❖ La topologie en arbre :

La topologie en arbre est aussi connue sous le nom topologie hiérarchique, est la plus utilisée dans les campus et les réseaux d'entreprises. Dans cette topologie, le réseau est divisé en niveaux.

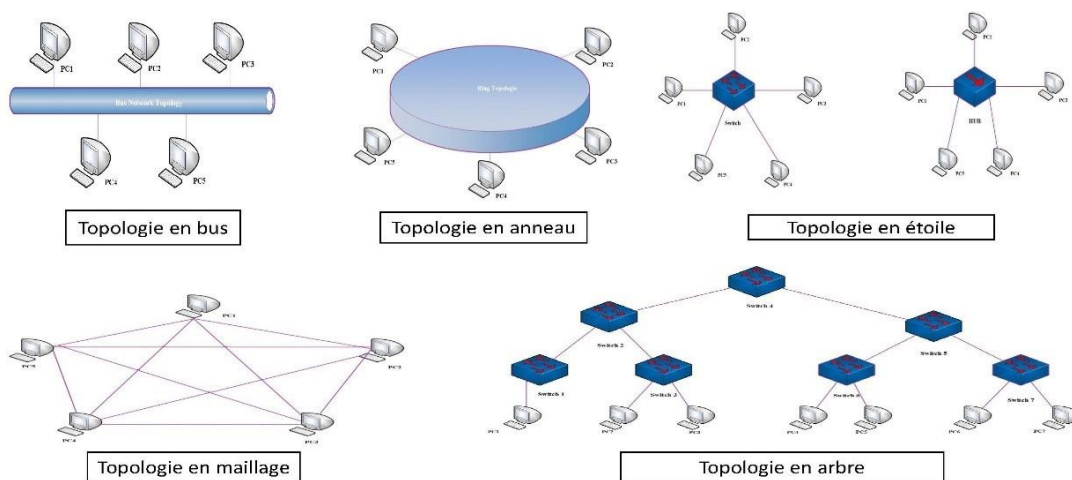


FIGURE I.4 – Les topologie physiques.

I.3.2.2 Topologie logique

Par opposition à la topologie physique, elle représente la façon selon laquelle les données transitent sur les lignes de communication. Elle gère :

- Discipline de ligne.
- Notifications d'erreur.
- Contrôle optimal du flux.

Les topologies logiques les plus courantes sont : Ethernet, Token Ring et FDDI (pour Fibre Distributed data interface).

❖ **Topologie Ethernet :**

Ethernet (aussi connu sous le nom de norme IEEE 802.3) est aujourd'hui l'un des réseaux les plus utilisés en local. Il est basé sur une topologie physique de type bus linéaire, c'est-à-dire que tous les ordinateurs sont connectés à un seul support de transmission et la communication se fait à l'aide d'un protocole appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detection) [1]. En utilisant ce protocole, n'importe quelle machine a le droit de transmettre en ligne à tout moment, et il n'y a pas de notion de priorité entre les machines.

❖ **Topologie Token Ring :**

La topologie Token Ring repose sur une topologie en anneau (ring). Elle utilise la méthode d'accès par jeton. Dans cette technologie, seule la station propriétaire du jeton a le droit de transmettre. Si une station veut émettre, elle doit attendre d'avoir le jeton.

❖ **Topologie FDDI :**

La topologie FDDI (Fibre Distributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibres optiques. Elle utilise Token Ring pour détecter et corriger les erreurs. Les jetons passent d'une machine à l'autre à une vitesse très élevée. S'il n'arrive pas après un certain temps, la machine pense qu'il y a une erreur dans le réseau.

I.3.3 Classification selon le mode de communication

On distingue généralement deux types de réseaux très différents en fonction de la nature des relations entre les sites, mais ils partagent des similitudes. Ils sont :

I.3.3.1 Réseau Client/serveur

Un client est un ordinateur qui accède aux ressources partagées fournies par un serveur de réseau. Le serveur est un ordinateur qui fournit des ressources partagées aux clients. Il est en général bien plus puissant et offre de multiples services tels que :

- Le partage de fichiers.
- Le partage d'imprimantes.
- Le stockage en base de données.
- L'accès aux informations du World Wide Web.

L'interaction entre client et serveur conduit à l'architecture client/serveur. En effet, l'architecture client/serveur spécifie un mode de communication entre plusieurs ordinateurs d'un réseau, qui distingue un ou plusieurs postes serveurs.

Un système client/serveur fonctionne selon le schéma suivant :

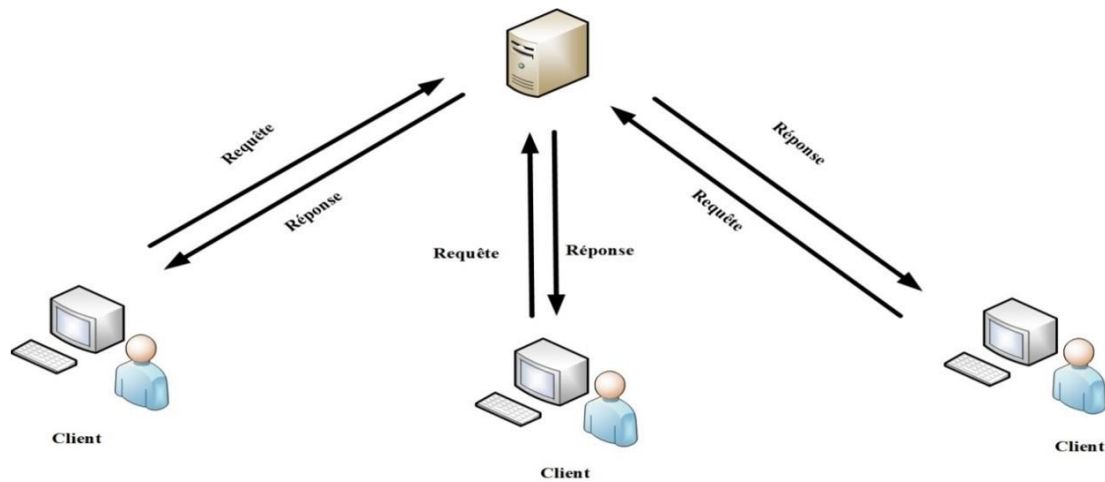


FIGURE I.5 – Fonctionnement d'un client /serveur.

Le client envoie une requête au serveur en utilisant son adresse et son port qui spécifient un service particulier au serveur lorsque ce dernier reçoit une demande et répond avec l'adresse de l'ordinateur client et son port.

I.3.3.2 Réseau poste à poste

Une autre architecture réseau est peer-to-peer ou P2P. Contrairement aux architectures réseaux de type client/serveur, il n'y a pas de serveurs dédiés [6]. Il est à la fois client/serveur. Cela signifie que chaque ordinateur du réseau peut librement partager ses ressources (données dans des répertoires partagés, imprimantes, cartes fax, etc.). Cette architecture n'est adaptée qu'aux petits réseaux.

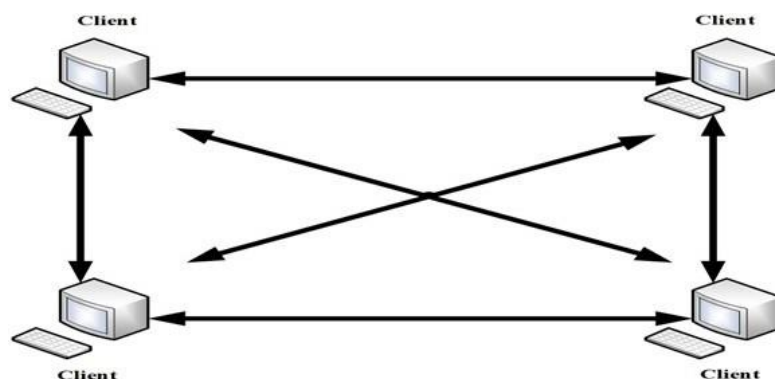


FIGURE I.6 – Réseau poste à poste.

Ce type de réseau est moins sécurisé qu'un réseau Client/serveur. Il ne nécessite cependant pas les services d'un administrateur réseau dédié.

On désigne par le terme "Administration" :

- Gestion des utilisateurs et de la sécurité.
- Mise à disposition des ressources.
- Maintenance des applications et des données.
- Installer et mettre à jour le logiciel utilisateur.

I.4 Modèle hiérarchique

Cisco a défini un modèle hiérarchique de réseaux. Ce modèle qui simplifie la tâche de construire un réseau d'interconnexion fiable, évolutif et moins coûteux. Comme le montre la figure ci-dessous, ce modèle est décomposé en trois couches distinctes qui sont en grande partie basées sur la répartition des rôles entre routage et commutation.

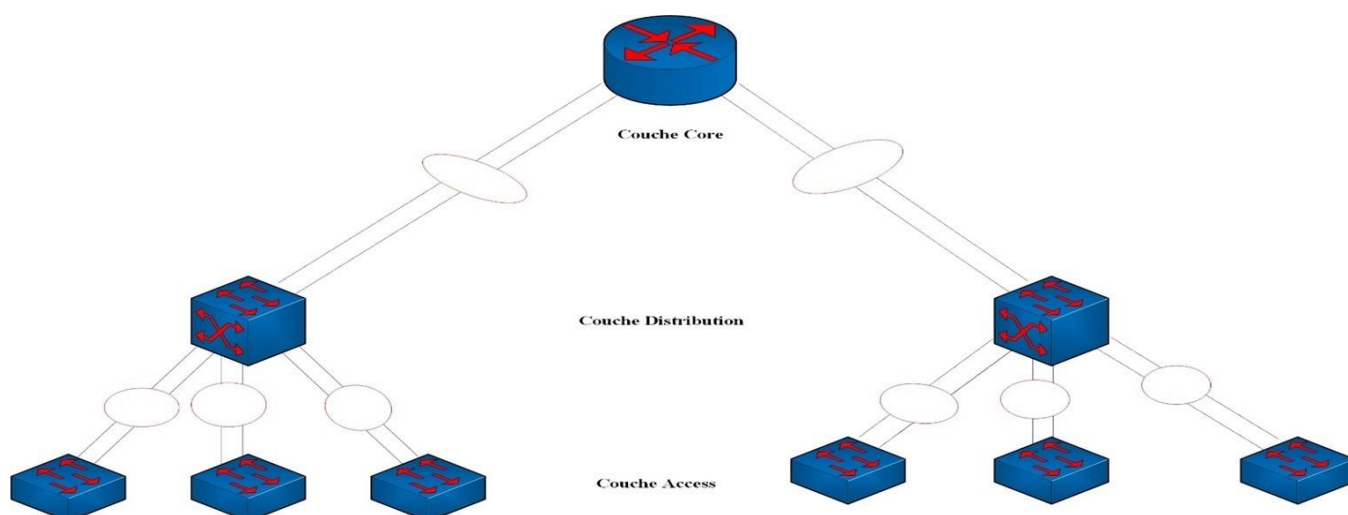


FIGURE I.7 – Modèle de conception hiérarchique à trois couches.

I.4.1 La couche cœur de réseau (Core layer)

On l'appelle aussi le Backbone est la couche supérieure. Cette couche est considérée comme l'épine dorsale du réseau et inclut les commutateurs haut de gamme et câbles à haute vitesse comme les câbles à fibres optiques dont le rôle principal consiste à relier entre eux les différents segments d'un réseau à savoir : les sites distants, les réseaux locaux (LANs) ou les étages de l'immeuble d'une société.

I.4.2 La couche distribution (Distribution layer)

On l'appelle la couche de groupe de travail. Cette couche se trouve entre la couche cœur et la couche d'accès c'est-à-dire entre la partie « liaison » et la partie « utilisateur ». A pour rôle d'assurer que les paquets sont correctement acheminés entre les sous-réseaux et VLAN dans votre entreprise.

Le commutateur de couche de distribution doit être capable de gérer la charge de traitement de tout le trafic provenant du périphérique d'accès. Ces commutateurs doivent avoir une haute densité de port haut débit pour fournir leurs services d'interconnexion. A partir de la couche d'accès. C'est au niveau de cette couche que la redondance de la passerelle par défaut de l'hôte est assurée.

I.4.3 La couche d'accès (Access layer)

Cette couche qui est la dernière du modèle hiérarchique permet de connecter les périphériques des utilisateurs finaux au réseau à l'aide du protocole IEEE 802.1X. A ce niveau, on utilise des switches de niveau 2. La configuration de ce type de switches pose moins de contraintes et aussi pour optimiser l'utilisation de la bande passante radio, les commutateurs intègrent de plus en plus des logiciels de contrôle radio qui permettent par exemple de réguler les puissances rayonnées par les antennes des points d'accès Wifi.

Cette couche est aussi appelée la couche bureau car elle se concentre sur des nœuds de connexion des clients tels que les postes de travail au réseau.

I.5 Architecture des réseaux

L'architecture des réseaux est l'implémentation des parties matérielles et logicielles pour réaliser un réseau. Une architecture de réseau est appelée aussi modèle de référence de réseau. Dans cette partie on va détailler deux modèles de référence, le modèle OSI (Open Systems Interconnection) qui est un modèle conceptuel de référence pour comprendre et concevoir une architecture de réseau flexible et robuste, Il se compose de sept couches. En revanche, le modèle TCP/IP (Transmission Control Protocol/Internet Protocol) est un modèle pratique utilisé par la plupart des spécialistes de la communauté réseau. Il est conçu autour de quatre couches ayant globalement les mêmes fonctionnalités que celles du modèle OSI.

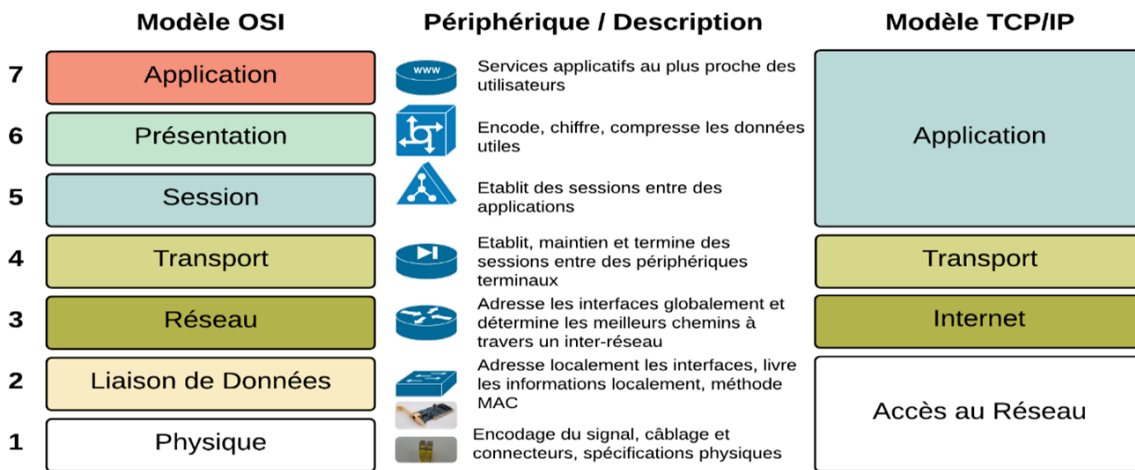


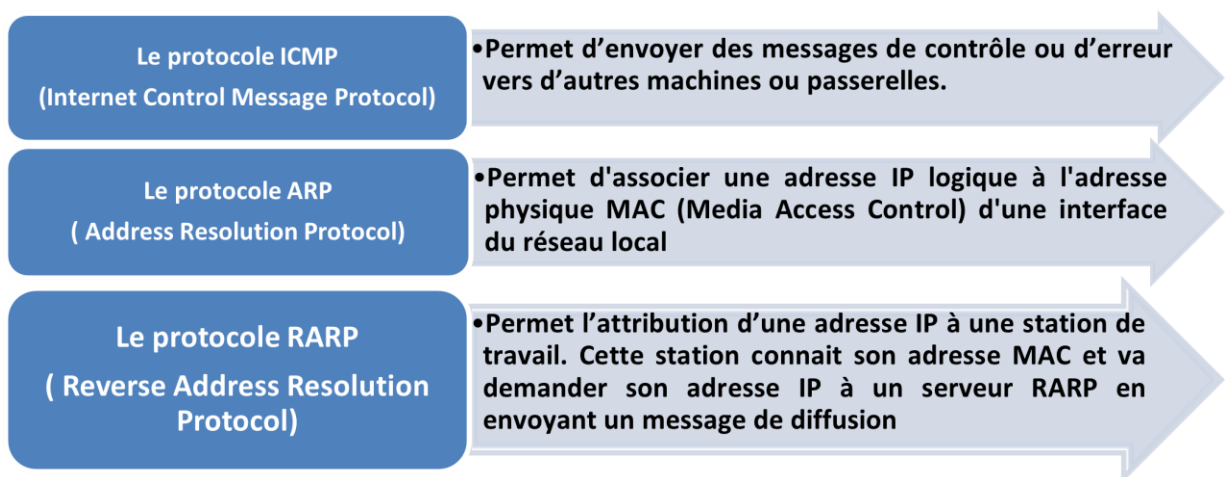
FIGURE I.8 – L'architecture des modèles OSI et TCP /IP [3].

Les rôles des différentes couches du modèle OSI et TCP /IP sont les suivants :

❖ **Couche physique et couche liaison de données :**

Ces deux couches du modèle OSI ont la même tâche de la couche accès réseau du modèle TCP /IP. Elles précisent la forme des données qui doivent être insérées au support de transmission indépendamment de la nature du support (fibre optique, sans fil, câbles réseau RJ45). Cette couche est constituée de la carte réseau et plusieurs normes existant au niveau de cette couche dont : Ethernet, Token Ring et FDDI.

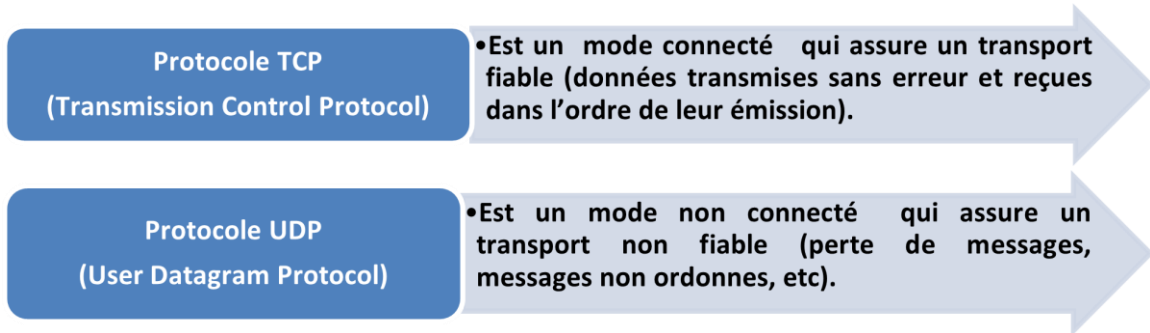
❖ **Couche réseau :** La Couche réseau du modèle OSI est similaire à la couche Internet du modèle TCP/IP. Elle s'occupe de l'adressage logique, de l'encapsulation des paquets de données et du routage. Le protocole central de cette couche est le Protocole IP mais, d'autres protocoles et services sont présents dans cette couche comme : les protocoles ICMP, ARP et RARP.



L'unité de données s'appelle en général un paquet.

❖ **Couche transport :**

La couche transport est le cœur du modèle OSI et TCP/IP. Cette couche s'occupe de réguler le flux de données et assure une communication de bout en bout [7]. Cette couche fonctionne en deux modes :



À noter que c'est cette couche qui affecte des numéros à des applications afin de pouvoir les identifier par les différents processus d'envoi et réception. Ces numéros sont appelés ports. L'adressage utilisé au niveau de cette couche est donc l'adressage applicatif (numéro de ports).

❖ **Couche session :**

La couche session gère les priorités d'accès et le dialogue et elle traite d'autres tâches telles que l'insertion des points de synchronisation dans les données à envoyer. Ce point de synchronisation représente des points de retour dans le cas de perte de données ou de données altérées.

❖ **Couche présentation :**

La couche présentation est la seule couche qui manipule la sémantique des données par contre les autres couches manipulent la syntaxe des données. Elle joue un rôle important dans un environnement hétérogène.

Les tâches principales de la couche présentation pour résoudre le problème de circulation des informations dans un réseau composé de machines hétérogènes :

- Le cryptage et la compression des informations à envoyer.
- L'utilisation d'un langage commun entre toutes les machines.

❖ **Couche application :**

La couche application a le même rôle que les couches application, présentation et session du modèle OSI et englobe les applications standards du réseau. Ci-dessous, les principaux protocoles faisant partie de la suite TCP/IP [4] :

SSH	• Connexion sécurisée à un ordinateur distant.
TELNET	• Connexion à un ordinateur distant.
FTP	• Téléchargement de fichiers.
SMTP	• Transfert de Messageries électroniques .
HTTP	• Transfert de documents Web.
SNMP	• Supervision réseau.
DNS	• Gestion des noms de domaine.
DHCP	• Gestion automatique des adresses IP.

Et beaucoup d'autres applications.



Remarque :

- Les couches : physique, liaison de données et réseau sont appelées couches basses. Ces dernières interviennent dans toutes les machines appartenant à un chemin pour acheminer les paquets.
- Les couches : transport, session, présentation et application sont appelées couches hautes. Celles-ci travaillent de bout en bout.

I.6 Encapsulation des données

Nous appelons "Encapsulation" le processus par lequel la couche N ajoute ses données de protocole à la séquence reçue de la couche [N+1] puis place le tout dans le champ de données de la couche [N-1].

Lors de la transmission, les données traversent chaque couche au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, qui est un en-tête (un ensemble d'informations dont la transmission est garantie).

À chaque couche, l'apparence du paquet change au fur et à mesure qu'il ajoute un en-tête donc, le nom change en fonction de la couche. Le principe d'encapsulation de données est représenté par le schéma suivant :

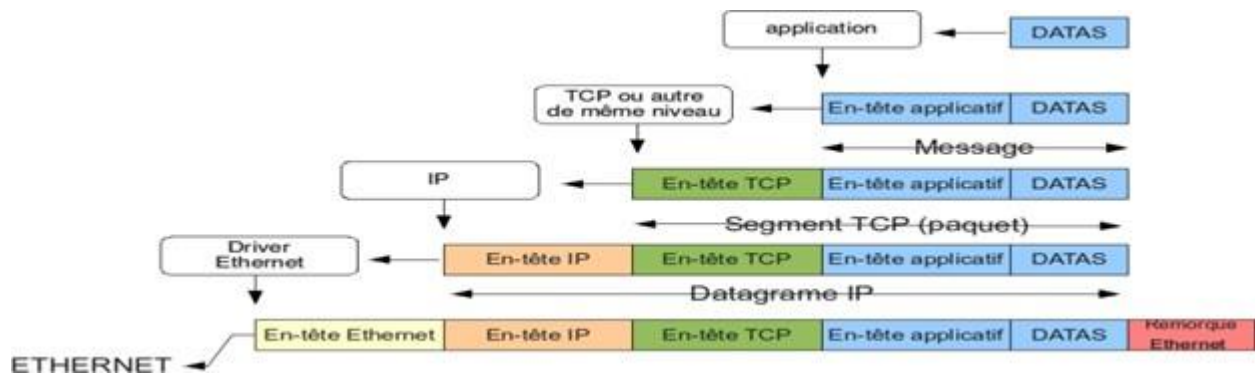


FIGURE I.9 – Principe d’encapsulation des données [3].

Sur la machine réceptrice, lors de son passage dans chaque couche, l’en-tête est lu puis supprimé. Ainsi, une fois le message reçu, le message est dans son état d’origine, il s’agit donc de décapsuler les données.

I.7 Le protocole IP

En télécommunication et informatique, le protocole IP (Internet Protocol) se trouve au cœur de l’architecture TCP/IP précisément dans la couche internet. Il gère l’acheminement des paquets de données (datagramme IP) d’une machine à une autre machine ainsi que l’adressage. En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.

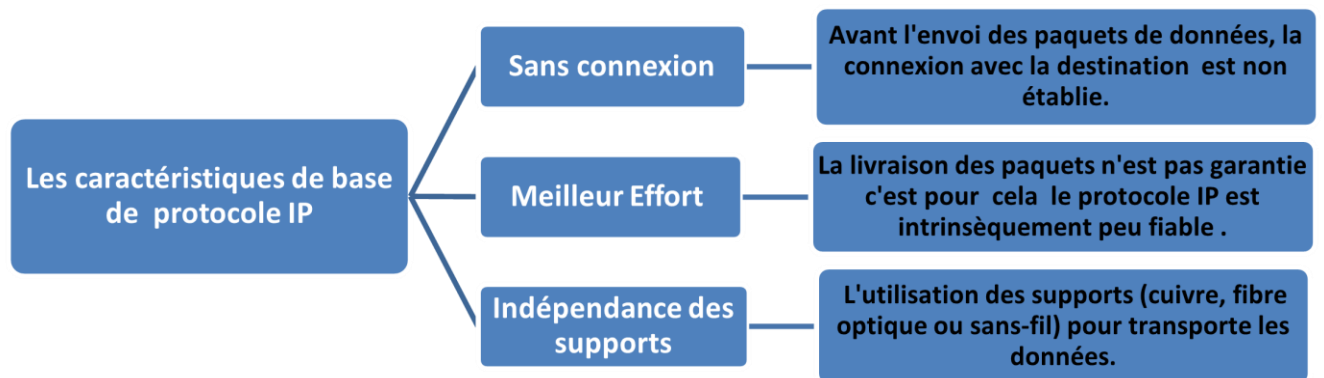


FIGURE I.10 – Les trois caractéristiques de base de protocole IP.

I.7.1 L'adresse IP

Le protocole IP permet d'établir une communication entre les ordinateurs grâce à des adresses numériques appelées aussi adresses IP. Alors pour communiquer entre deux machines se trouvant dans des réseaux différents, il faut passer par un relais (routeur).

- **L'adresse IPv4 :**

IPv4 (version 4 du protocole Internet) est une adresse hiérarchique la plus utilisée et représentée sous le format binaire (32 bits) ou sous le format décimal constitué de quatre nombres dont les valeurs sont entre 0 et 255 et séparés par des points [8] Exemple : 192.168.10.10.

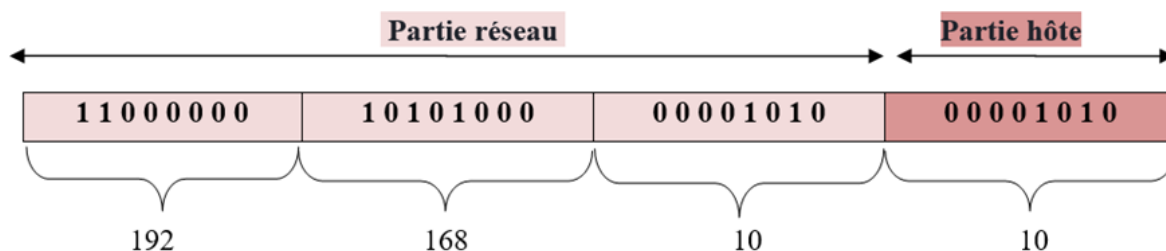


FIGURE I.11 – Exemple d'une l'adresse IPv4.

- **Masques de sous réseau :**

Une adresse IP est toujours associée à un masque de sous-réseau. Ce dernier est utilisé pour identifier la partie réseau et la partie hôte qui est une succession de bits à 1 suivie d'une séquence successive de bits à 0. Ces bits sont représentés aussi sous format 32 bits ou 4 octets séparés par des points. Les 0 indiquent la partie machine (hôte). Voir la figure ci-dessous :

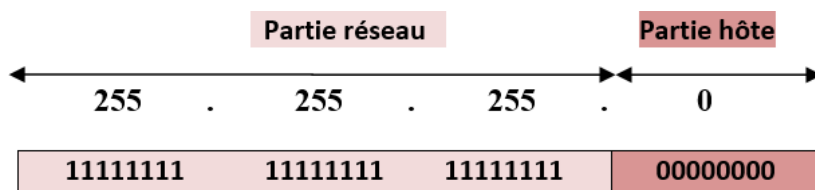


FIGURE I.12 – Masque de sous-réseau.

Les classe	Intervalle du premier octet en décimal	Masque de sous-réseau	Longueur de préfixe	Nombre de réseau	Nombre de machines (hôtes) par réseau
A	[0 à 127]	255.0.0.0	/8	$2^7 - 2 = 126$	$2^{24} - 2 = 16777214$
B	[128 à 191]	255.255.0.0	/16	$2^{14} = 16384$	$2^{16} - 2 = 65534$
C	[192 à 223]	255.255.255.0	/24	$2^{21} = 2097152$	$2^8 - 2 = 254$
D	[224 à 239]	Non défini	/4	Adresses uniques	Adresses uniques
E	[240 à 255]	Non défini	Non défini	Adresses uniques	Adresses uniques

Table I.1 – Les classes d’adresse IP et Masque réseau.

Il existe deux types d’adresse IPv4 permettant aux appareils de communiquer entre eux :

- **Les adresses IPv4 publiques (externes)** : sont des adresses uniques dans le monde qui sont attribuées à une seule entité pour établir la communication entre les hôtes et internet et qui sont acheminées de manière globale entre les routeurs des FAI (fournisseurs d’accès à Internet).
- **Les adresses IPv4 privées (internes)** : est une adresse unique dans un réseau local (LAN) cette adresse attribuée à plusieurs entités en même temps pour établir une connexion sécurisée a d’autre appareils du réseau.

I.8 Conclusion

À la fin de ce chapitre, nous avons une bonne compréhension des concepts de base des réseaux informatiques qui sont importants dans le domaine des télécommunications. Les réseaux informatiques continuent d’évoluer et occupent de plus en plus de place dans l’environnement des entreprises. Par conséquent, le risque augmente. C’est pourquoi dans le chapitre suivant, nous aborderons les préoccupations concernant la sécurité du transport des données.

INITIATION à sÉCURITE DES REseaUX

inFORMaTIQUE

II.1 Introduction

La sécurité des systèmes informatiques comprend la protection de l'accès et de la manipulation des données et des ressources du système par des mécanismes d'authentification. Cependant, l'émergence d'Internet a apporté de nombreux problèmes à la sécurité de l'information, que ce soit via un réseau privé ou un réseau public, des mécanismes et des stratégies de sécurité doivent être mis en place.

Ce chapitre introductif présente les concepts de base de la sécurité des systèmes informatiques et les différentes attaques qui peuvent survenir, ainsi que les mécanismes qui peuvent être utilisés pour assurer la sécurité.

II.2 Sécurité des systèmes informatiques (SSI)

Avec le développement de la technologie et l'avènement d'internet, le phénomène du vol d'informations numériques s'est beaucoup propagé. Nous avons donc eu recours à la sécurité des systèmes informatiques. La SSI également appelée cyber sécurité, est un ensemble de techniques impliquées sur les données de transmission afin de les protéger de tous les dangers qui peuvent détruire notre système quelque soient le danger accidentel ou intentionnel [9]

II.3 La terminologie de la sécurité

- ❖ **Une menace** : un danger qui existe dans un environnement indépendant des systèmes informatiques comme : criminel, pirate, employé mécontent, concurrent, agences gouvernementales.
- ❖ **Une vulnérabilité** : c'est une faiblesse ou une faille de sécurité dans un système informatique qui le rend vulnérable aux menaces aux niveaux suivants : système d'exploitation, applications, protocoles de communication, etc.
- ❖ **Un risque** : est la probabilité qu'une menace donnée puisse exploiter une vulnérabilité au système donné [10].

Un risque = Une menace + Une vulnérabilité

- ❖ **Contre-mesures** : ce sont les moyens de contrôle mis en place dans un système informatique pour réduire ou éliminer les risques. Il existe deux types : administratifs (règles), physiques (agent de sécurité).

II.4 Principes de la sécurité informatique

La sécurité informatique vise cinq principaux objectifs. Comme illustré la figure suivante :

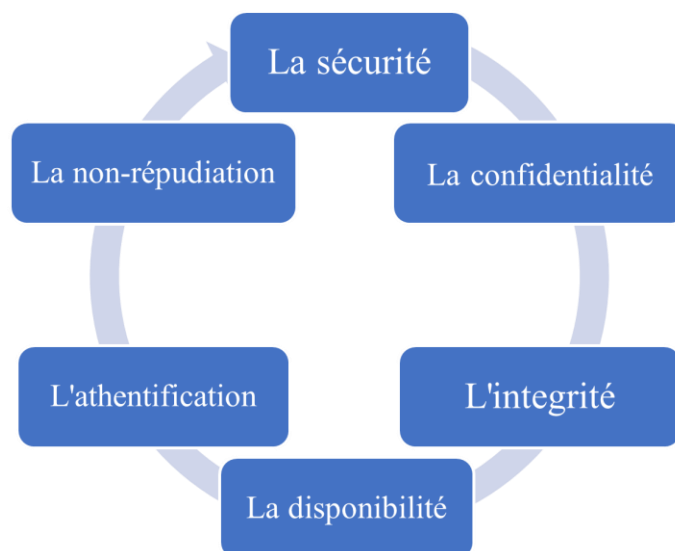


FIGURE II.1 – Les cinq dimensions de la sécurité informatique.

❖ **La confidentialité :**

Les mesures de confidentialité sont conçues pour interdire le dévoile d'informations [11]. Le but des principes de confidentialité est de garder les informations personnelles privées et de garantir qu'elles ne peuvent être vues et consultées que par ceux qui en sont propriétaires ou qui en ont besoin pour s'acquitter de leurs fonctions organisationnelles.

❖ **Intégrité :**

Visé pour maintenir et assurer la fiabilité des données. Les données reçues par le destinataire doivent être les mêmes que les données envoyées par l'expéditeur. L'intégrité garantit également l'authenticité des données [12].

❖ **La disponibilité :**

La disponibilité de l'information consiste à s'assurer qu'elle est toujours accessible pour les utilisateurs finaux et les applications, quels que soient les événements (forte charge du réseau, panne d'équipement, etc.). La disponibilité d'un équipement se mesure en divisant la durée à laquelle cet équipement est opérationnel par la durée pour laquelle il aurait dû être opérationnel.

❖ **L'authentification :**

Elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identification d'un individu, d'une entité mais également l'origine de l'information ou encore d'une opération effectuée sur celle-ci [13].

❖ **La non-répudiation :**

C'est la propriété qui détermine qu'une transaction ne peut pas être rejetée. La non-répudiation de l'origine et la réception des données prouvent que les données ont été reçues. Cela se fait au moyen d'un certificat numérique utilisant une clé privée. Il est couramment utilisé pour les contrats numériques, les signatures et les e-mails.

II.5 Les attaques

II.5.1 Définition de l'attaque

Une attaque, également connue sous le nom de « cyber attaque », est définie comme toute action ou ensemble d'actions susceptibles d'affecter la sécurité des informations d'un système ou d'un réseau informatique. L'agent qui effectue l'attaque est un cybercriminel ou un attaquant ou un agent de menace. Son objectif est d'accéder au réseau et de le bloquer ou de le perturber. Dans de nombreux cas, les attaquants peuvent également tenter d'obtenir un accès non autorisé aux périphériques réseaux en utilisant une ou plusieurs stratégies d'attaques (par exemple : déni de service, logiciel malveillant, etc.).

II.5.2 Les types d'attaques informatiques

II.5.2.1 Attaque passive

Est une tentative d'apprentissage ou d'utilisation des informations du système qui n'affecte pas les ressources du système. Son objectif principal est de fournir aux attaquants la possibilité de surveiller le trafic réseau et de découvrir potentiellement des données précieuses et d'autres informations confidentielles.

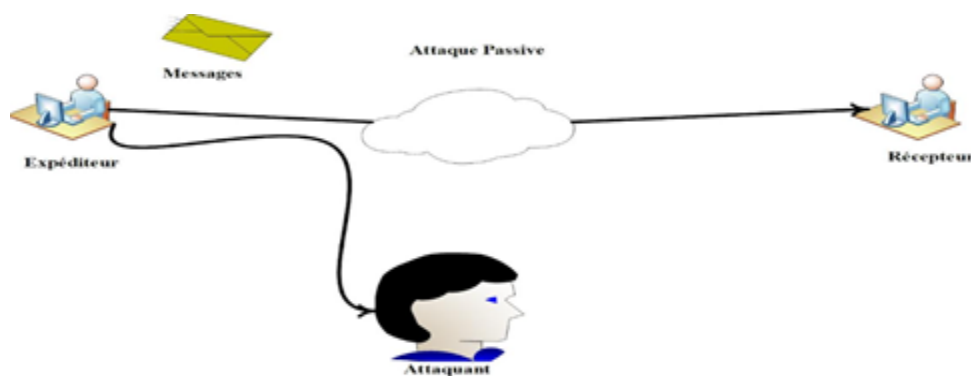


FIGURE II.2 – Attaque passive.

II.5.2.2 Attaque active

Est une tentative de modifier les ressources du système, d'affecter leur fonctionnement ou de créer de faux messages. L'attaque active se produit lorsque l'attaquant détourne une session sur le réseau.

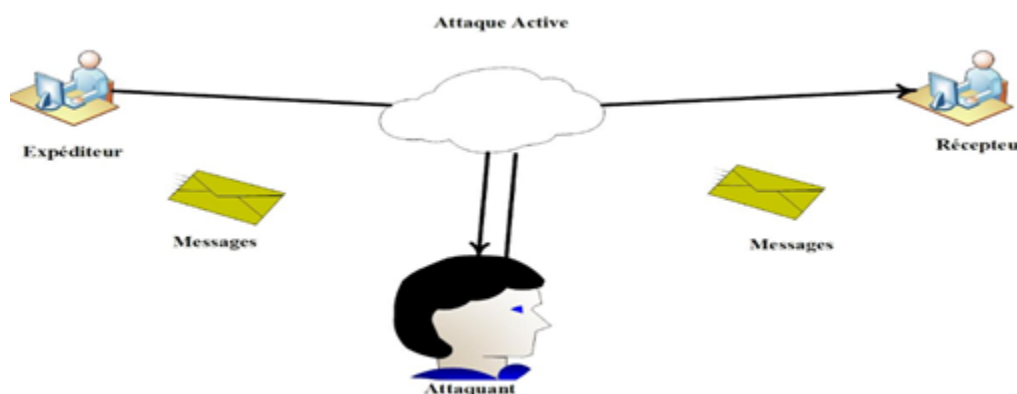


FIGURE II.3 – Attaque active.

II.5.3 Exemples d'attaques informatiques

Il existe de nombreuses attaques qui menacent les systèmes informatiques à travers le monde, les plus célèbres aujourd'hui sont :

II.5.3.1 Programme malveillant

Le programme malveillant « le malware » est un code ou un logiciel développé par les attaquants afin de perturber le fonctionnement normal d'un appareil informatique pour supprimer, modifier ou voler des données. Les types courants de code malveillant sont :

❖ Virus

Les virus informatiques sont les types les plus courants de logiciels malveillants qui se fixent sur des programmes ou des fichiers dans le but d'infecter d'autres programmes. Ils peuvent se répliquer et se propager sur les autres machines lorsque des fichiers infectés sont envoyés par email ou bien lorsque les utilisateurs transportent sur des supports physiques. Les virus sont dangereux et peuvent détruire des données, ralentir les ressources du système et d'enregistrer les frappes au clavier.

❖ **Vers**

Les vers « Worms » sont des programmes qui peuvent s'auto-reproduire et de se propager en utilisant les mécanismes réseaux [14]. Ils sont identiques aux virus mais contrairement à ces derniers, les worms sont capables d'utiliser des réseaux informatiques pour infecter les autres machines connectées sans l'aide des utilisateurs. Les vers ne sont pas toujours performants sur les ordinateurs, mais ils entraînent généralement des problèmes de performance et de stabilité de l'ordinateur et du réseau.

❖ **Un cheval de Troie**

Un cheval de Troie (Trojan horse en anglais) est un autre type de programme malveillant, nommé ainsi en raison du cheval de bois que les Grecs utilisèrent jadis pour s'introduire dans la ville de Troie. Le Trojan est un logiciel qui ouvre une porte dérobée dans un système pour introduire des pirates ou d'autres programmes indésirables. Il se compose de deux parties, une partie serveur (victime) et une partie client (hacker). Une fois le cheval est installé sur le serveur via un outil de communication (email, messagerie instantanée, etc.), le hacker envoie à la victime une demande de requête après cette dernière répond aux requêtes demandées.

Contrairement aux virus et vers informatiques, les chevaux de Troie ne se reproduisent pas. Ces opérations peuvent être :

- Supprimer les données.
- Blocage des données.
- Modifier les données.
- Réplication des données.
- Perturbation des performances de l'ordinateur ou du réseau informatique.

II.5.3.2 L'attaque de reconnaissance

Une attaque de reconnaissance (recon en anglais) est un type d'attaque sécurisée qu'un attaquant utilise pour rassembler un maximum d'informations sur l'infrastructure avant de lancer une attaque réelle. Il existe deux types d'attaques de reconnaissance :

- ❖ **Attaque de reconnaissance active** : l'attaquant interagit avec la victime pour obtenir des informations.
- ❖ **Attaque de reconnaissance passive** : l'attaquant peut obtenir des informations sur la victime sans la solliciter.

II.5.3.3 Attaque par accès

Une attaque d'accès permet à quelqu'un d'obtenir un accès non autorisé à des informations pour consultation. Ces attaques d'accès incluent :

- ❖ **Les attaques par mot de passe** : est le mécanisme le plus couramment utilisé, il consiste à faire de nombreux essais jusqu'à trouver le bon mot de passe d'un utilisateur. L'obtention de ce dernier permet à un attaquant d'accéder à un système ou à un réseau.
- ❖ **L'exploitation de la confiance** : un acteur de menaces utilise des privilèges non autorisés pour accéder à un système, ce qui peut compromettre la cible.
- ❖ **La redirection de port** : est un processus en coulisse consistant à intercepter le trafic de données se dirigeant vers la combinaison IP d'un ordinateur et à le rediriger vers une adresse IP différente.
- ❖ **Les attaques d'homme de milieu** : est une technique de piratage dans laquelle un pirate se place entre deux ordinateurs et se fait passer pour l'un pour obtenir le mot de passe de l'autre afin de modifier des données.

II.5.3.4 L'attaque par déni de service (DOS)

Le déni de service (DOS, Denial Of Service) est un type d'attaque très courant conçu pour rendre un service, un système ou un réseau indispensable, vise généralement des serveurs web [15]. Ceci peut s'effectuer en saturant le service ciblé en lui envoyant tellement d'information qu'il n'est plus capable de les gérer correctement. Par exemple : L'envoi massif de courrier électronique pour saturer une boîte aux lettres. En générale, on utilise le DOS pour extorquer de l'argent aux victimes. Pour la plupart, il s'agit d'entreprises prospères qui pourraient perdre beaucoup d'argent si leurs services en ligne ou leurs réseaux informatiques étaient bloqués.

- ❖ **DDOS (Distributed Denial of Service)** Une attaque par déni de service distribué est une attaque DOS lancée à partir de plusieurs sources différentes. DDOS est conçu pour saturer les connexions réseau avec des données illégales [16]. Ces données peuvent submerger une connexion Internet au point de bloquer le trafic légitime. Ce type d'attaque reste très difficile à contrer ou à éviter il s'agit donc d'une menace que beaucoup craignent.

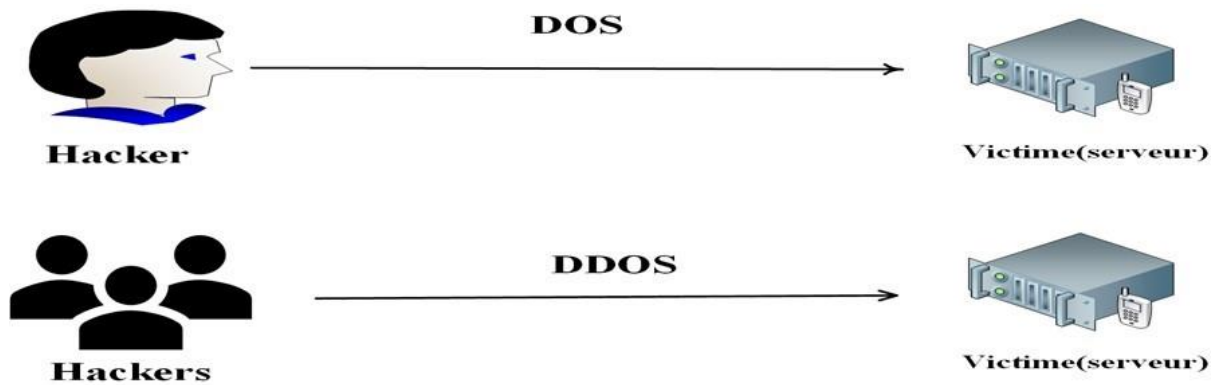


FIGURE II.4 – Attaque DOS et DDOS.

II.6 Mécanismes de défense



FIGURE II.5 – Mécanismes de défense.

II.6.1 Antivirus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des fichiers exécutables ou des logiciels malveillants, notamment les virus, les vers, les chevaux de Troie et parfois les logiciels espions qui peuvent infecter un ordinateur [17]. Un logiciel antivirus n'est efficace que lorsque sa base de données est mise à jour au cours desquelles il mémorise les nouvelles formes de virus de circulation. Il existe deux types de protections :

- Favorisant les logiciels antivirus sur toutes les machines, il est absolument nécessaire de prévoir des mises à jour automatiques pour tous les sites du réseau.
- Mettre en place un antivirus aux points d'entrée/sortie de données du réseau après que tous ces points de données soient parfaitement identifiés. Les exigences strictes du programme doivent être obtenues par tout le personnel.

II.6.2 Chiffrement

Le chiffrement des données est une méthode de conversion des données du texte en clair (non chiffré) en texte chiffré généralement à l'aide d'un algorithme basé sur une clé. Le cryptage est l'élément fondamental de la sécurité des données. C'est le moyen le plus simple et le plus efficace de s'assurer que les informations du système informatique ne peuvent être ni volées ni lues par quelqu'un qui souhaite les utiliser à des fins malveillantes. Les deux principaux types de chiffrement des données sont :

- ❖ **Le chiffrement symétrique (chiffrement à clé secrète) :** L'émetteur et le récepteur utilisent la même clé secrète qu'ils appliquent à un algorithme donné pour chiffrer ou déchiffrer un texte. Elle est la forme la plus ancienne de la cryptographie mais plus rapide que les autres types de chiffrements.

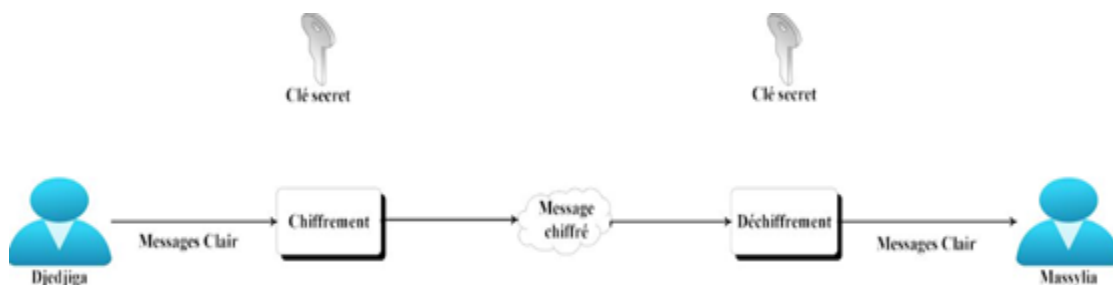


FIGURE II.6 – Le chiffrement symétrique.

- ❖ **Le chiffrement asymétrique (chiffrement à clé publique) :** Cette méthode est basée sur l'utilisation d'une paire de clés :

- La première clé, visible appelée clé publique est utilisée pour chiffrer un texte en clair.
- La deuxième clé, secrète appelée clé privée est connue uniquement par le destinataire, qui est utilisée pour décrypter un texte.

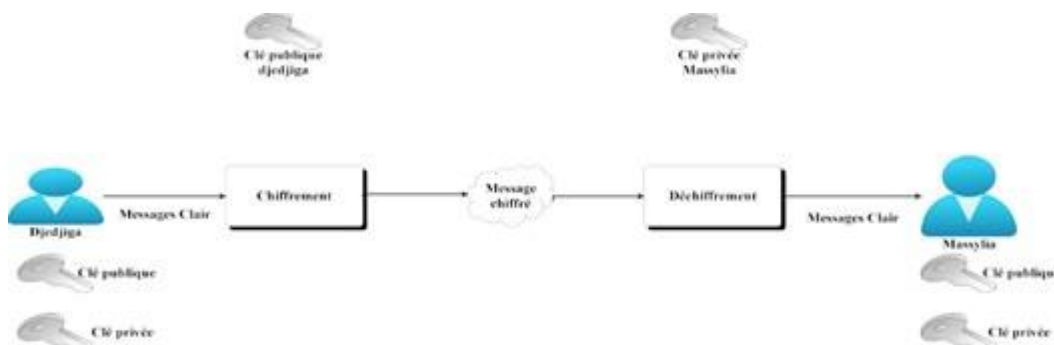


FIGURE II.7 – Le chiffrement asymétrique.

II.6.3 Pare-feu

Un pare-feu (également appelé Firewall en anglais) est un élément d'un réseau informatique matériel ou logiciel qui permet la protection d'un ordinateur ou d'un réseau informatique et sécurise les communications avec Internet en utilisant un système filtrage (filtrer les paquets de données échangés avec le réseau), il s'agit d'une passerelle de filtrage qui comprend au moins les interfaces réseau suivantes :

- L'interface réseau à protéger (réseau interne).
- Interfaces vers des réseaux externes.

Le système de pare-feu contient un ensemble de règles prédéfinies :

- Autoriser la connexion (allow).
- Bloquer la connexion (deny).
- Rejeter les demandes de connexion sans avertir l'expéditeur (Drop).

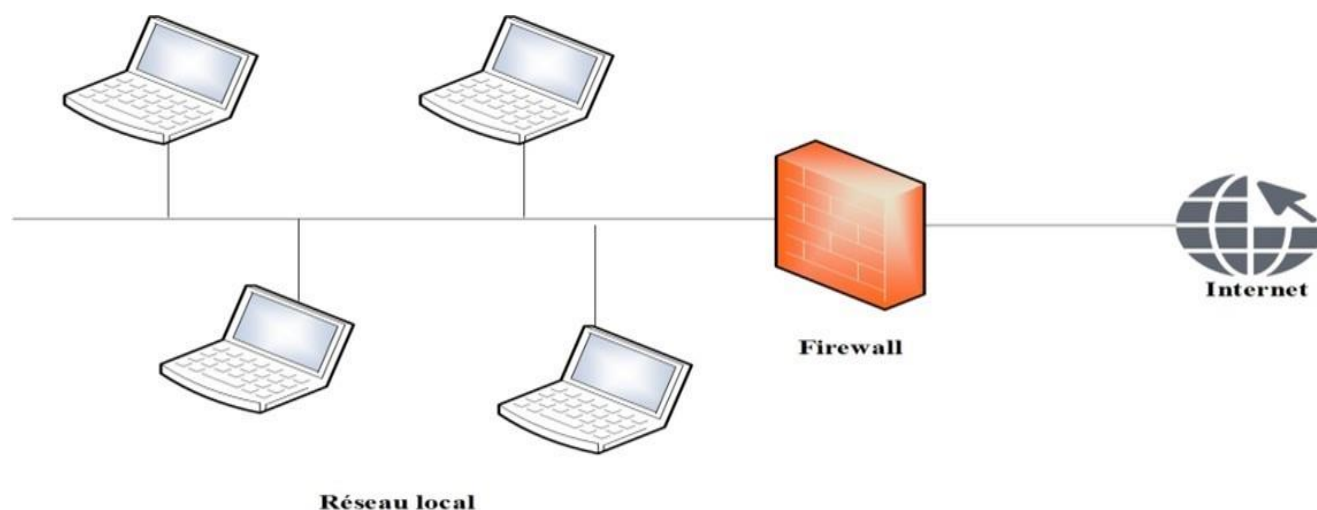


FIGURE II.8 – Pare-feu.

II.6.4 Proxy

Le proxy (ou serveur mandataire) est une machine qui agit comme l'intermédiaire entre un terminal (Ordinateur, Smartphone, Tablette, etc) et réseaux externes (Internet) comme dans la figure ci-dessous. Lorsqu'un utilisateur fait une requête sur Internet, il se connectera d'abord à un serveur proxy, qui enverra la requête au serveur de l'application que l'utilisateur essaie de rejoindre. Le serveur envoie sa réponse au proxy, qui à son tour la transmet à l'utilisateur. Un serveur mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (HTTP, FTP, SMTP, etc.) mais, la plupart du temps le serveur proxy est utilisé pour le Web. Il s'agit alors d'un proxy HTTP.

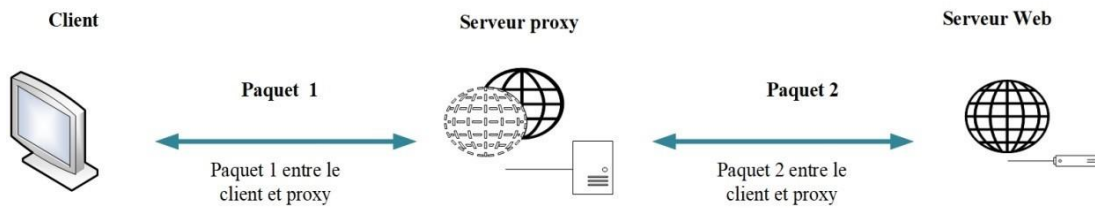


FIGURE II.9 – Proxy.

L'utilité des proxys est importante, notamment dans le cadre de la sécurisation des systèmes d'information. Il permet de sécuriser et d'améliorer l'accès à certaines pages web en stockant des copies, en filtrant certains contenus web et logiciels malveillants, et en renforçant l'anonymat de ses utilisateurs.

II.6.5 Système de détection d'intrusion

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un ensemble de composants logiciels et/ou matériels dont le but de détecter et d'analyser toute tentative d'effraction volontaire et les activités malveillantes. Ainsi il peut connaître les tentatives réussies comme échouées des intrusions. Selon différentes catégories, les IDS les plus connus sont [18]:

- Les NIDS (Network Based Intrusion Detection System), qui surveillent l'état de la sécurité au niveau du réseau sont le plus largement utilisés. Exemple : l'analyse de trafic réseau entrant.
- Les HIDS (Host Based Intrusion Detection System), qui surveillent l'état de la sécurité au niveau des hôtes. Exemple : la surveillance les fichiers importants du système d'exploitation.
- Les IDS hybrides, qui utilisent les NIDS et HIDS pour avoir des alertes plus pertinentes. De plus, ils permettent une meilleure détection d'attaques distribuée.

II.6.6 Système de prévention d'intrusion

Un système de prévention d'intrusion (ou IPS : Intrusion Prévention System), est un dispositif de sécurité réseau utilisé pour surveiller les activités du réseau ou du système pour détecter toute activité malveillante [19]. Il est capable de prévenir une attaque avant qu'elle atteigne sa destination. Contrairement aux IDS, les IPS sont des outils aux fonctions « actives », qui en plus de détecter une intrusion, tentent de la bloquer.

On distingue généralement quatre principaux types d'IPS :

- NIPS (Network based IPS) est un système de prévention des intrusions basé sur le réseau qui surveille l'ensemble du réseau à la recherche de trafic suspect en analysant l'activité du protocole.
- WIPS (Wireless based IPS) est un système de prévention des intrusions sans fil, qui surveille un réseau sans fil pour détecter et signaler les intrusions, les violations de la politique du réseau et les utilisations non autorisées en analysant les protocoles de réseau sans fil.
- HIPS (Host based IPS) est un système de prévention des intrusions hôtes intégré en tant que package logiciel secondaire qui surveille un seul hôte pour détecter toute activité suspecte en analysant les événements se produisant au sein de cet hôte.
- NBA (Network behavior analysis) est une analyse du comportement du réseau qui examine le trafic réseau pour identifier les menaces qui génèrent des flux de trafic inhabituels. Parmi ces menaces, on retrouvera le plus souvent les attaques par déni de service, différentes formes de logiciels malveillants et les violations des politiques de sécurité.

II.7 Conclusion

Ce chapitre présente une analyse des exigences de sécurité et étapes clés avant de mettre en œuvre des politiques de sécurité dans le réseau. Le prochain chapitre se concentrera sur le réseau existant au sein de l'entreprise et résumera ses faiblesses et leurs solutions.

PRESENTIONS de L'ORGANISME d'accUEIL

III.1 Introduction

Ce chapitre sera réservé à la présentation du campus NTS (New Technology & Solutions) où nous effectuons notre stage. Dans un premier temps, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Nous étudierons ensuite l'architecture réseau de cette entreprise et ses composantes afin de pouvoir suggérer d'éventuelles améliorations.

III.2 Partie 1 : Présentions de l'entreprise "Campus NTS"

III.2.1 Création et évolution

NTS est une jeune entreprise axée sur la recherche, la conception et la mise en œuvre de solutions, d'intégration de systèmes de sécurité, d'importation et de la distribution d'équipements et de matériels de sécurité des réseaux et des télécommunications, de la formation et du conseil. Elle a été créée en 2020 à Béjaïa par M. Djebbari Yassine, qui a de nombreuses d'années d'expérience et a réalisé d'importants projets dans différents secteurs et régions du pays, comme référence :

- Air Algérie.
- Retelem Alger.
- Poste d'Algérie.
- Adèle.
- RATP ALJAZAIR.
- La technologie.
- Géant de l'électronique BBR.
- Morsi.
- Université de Bejaïa.
- Cité universitaire à Bejaïa (targa ouzamour, 17 octobre, etc).
- SARL Alphas Bejaïa.
- Providentia Béjaïa.

III.2.2 La localisation de l'entreprise

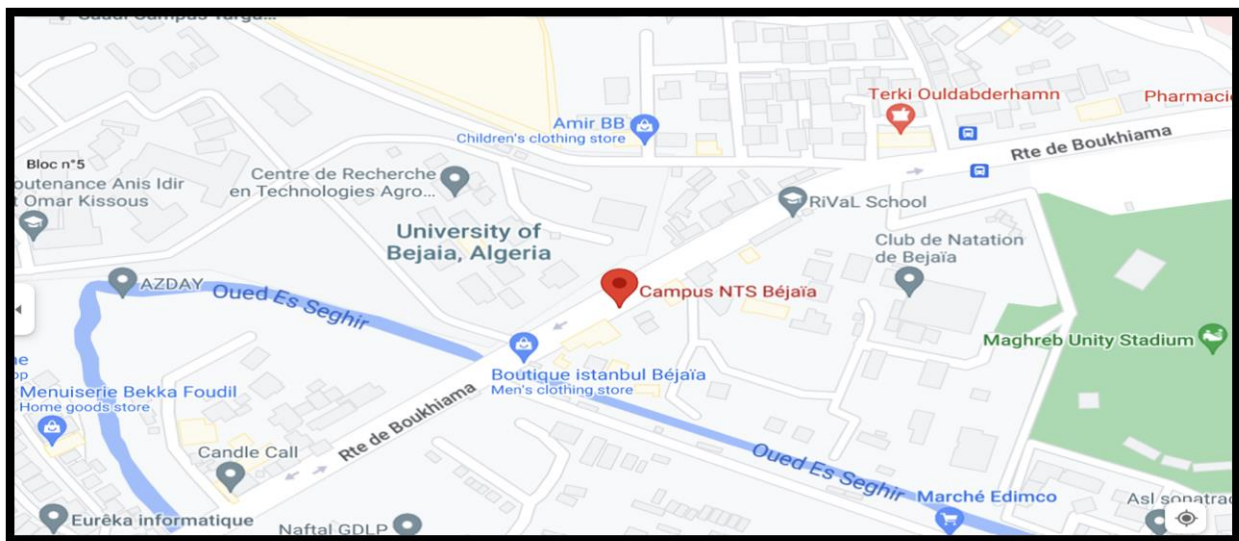


Figure III.1 – Localisation de l'entreprise NTS.

III.2.3 Fiche technique

Le tableau III.1 ci-dessous représente quelques informations relatives à l'entreprise dans laquelle nous avons effectué notre stage de projet de fin d'études.

Dénomination	Campus NTS
Logo	
Siège	Bâtiment A les beaux quartiers Targa Ouzemour, Béjaïa 06000
Secteurs d'activités	Informatique et télécommunication
Numéros de FAX	044 204 400
Numéros de Téléphone	0770 44 61 01
Email	contact@campus-nts.com
Site Internet	http ://www.campus-nts.com/

Table III.1 – Identification sur campus NTS.

III.2.4 Objectifs, missions et activités de l'entreprise « N.T.S »

Les objectifs, les missions et les activités sont représentés dans la figure III.2 :

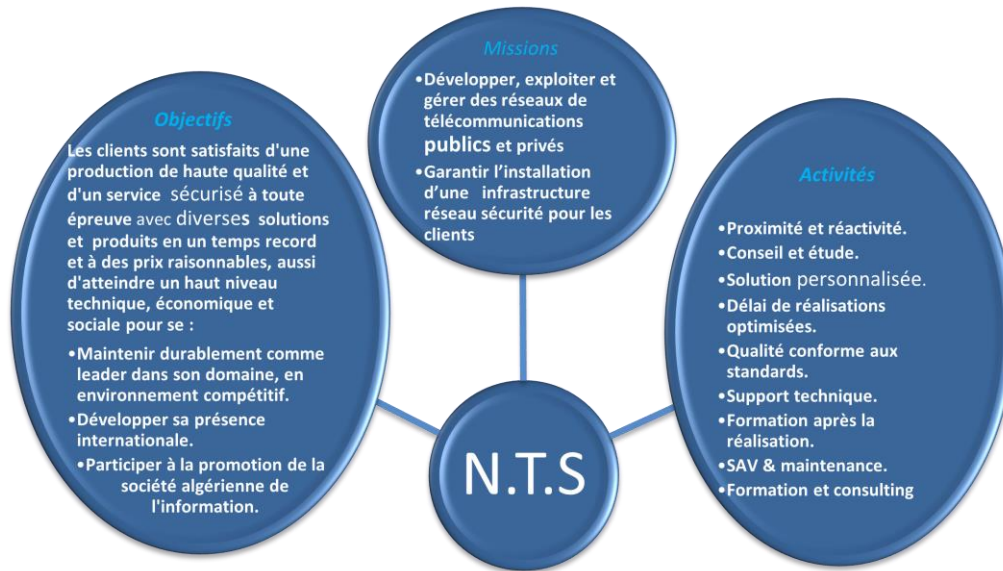


FIGURE III.2 – Objectifs, Missions et Activités de l'NTS.

III.2.5 Organigramme général de l'organisme d'accueil

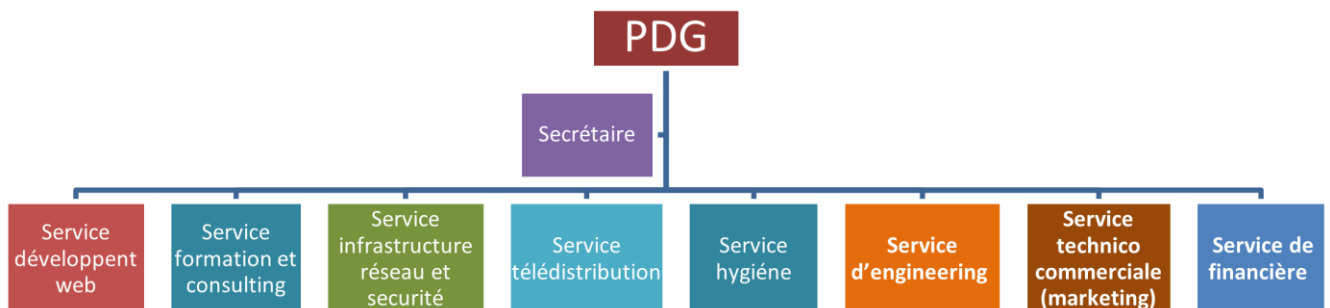


FIGURE III.3 – L'organigramme de campus NTS.

Nous allons nous contenter de présenter ci-dessous la description de l'organigramme du campus NTS (voir la figure III.3)

A. Service développement web

Il est responsable de la création des sites web, des applications pour internet, applications mobiles ou des solutions logicielles adaptées aux besoins des clients utilisant des langages de programmation informatique tels que : HTML5, CSS, JavaScript ou PHP. En général, il représente les tâches liées au développement du site Web en améliorant son positionnement sur les moteurs de recherche qui seront hébergés sur Internet.

B. Service formation et consulting

Ce secteur a été créé par le campus NTS pour offrir des stages et des formations professionnelles dans les domaines suivants :

- Installation et configuration des réseaux informatiques.
- Administration et sécurité des réseaux et système.
- Installation et configuration des firewalls (pfsense, Sophos, fortigate, palo alto, etc.).
- Installation et configuration des réseaux sans fil professionnel.
- Installation et configuration des caméras de surveillance analogique et numérique.
- Fibre optique les réseaux d'accès FTTH/FTTX.
- Création des sites web.
- Programmation (C, C++, C#, Java, Python, etc.).
- Electricités Bâtiments et industriels.
- Formation Cisco CCNA, CCNP S&R.
- Virtualisation.
- Microsoft server, SQL.
- Cyber sécurité.

Ces stages s'adressent aux étudiants, ouvriers, entreprises en fin de projet et à tous ceux qui apprécient le terrain pour développer leurs compétences en sécurité, acquérir des qualifications supérieures et leur expérience en entreprise. NTS repose sur la capacité des ressources et des structures à délivrer à ses clients et à ses partenaires (Alhua, Hikvision, Cisco, Legend, Mikrotik, Zkteco, Commax, D-link, Alcatel-Lucent, Synology, Microsoft, Apollo, Panasonic, Huawei).

C. Service d'accueil

- **Présentation de service infrastructure réseau et sécurité** : L'infrastructure réseau est au cœur des opérations commerciales dans la plupart des industries. Il peut être considéré comme le centre sensible de toute l'organisation informatique car il centralise les données, simplifie les échanges de données et facilite la communication entre les employés. A ce titre, il est un outil important pour le fonctionnement normal de l'entreprise et nécessite une attention constante en matière de sécurité. Ceci afin d'empêcher le nombre croissant et l'affectation des attaques externes et internes.

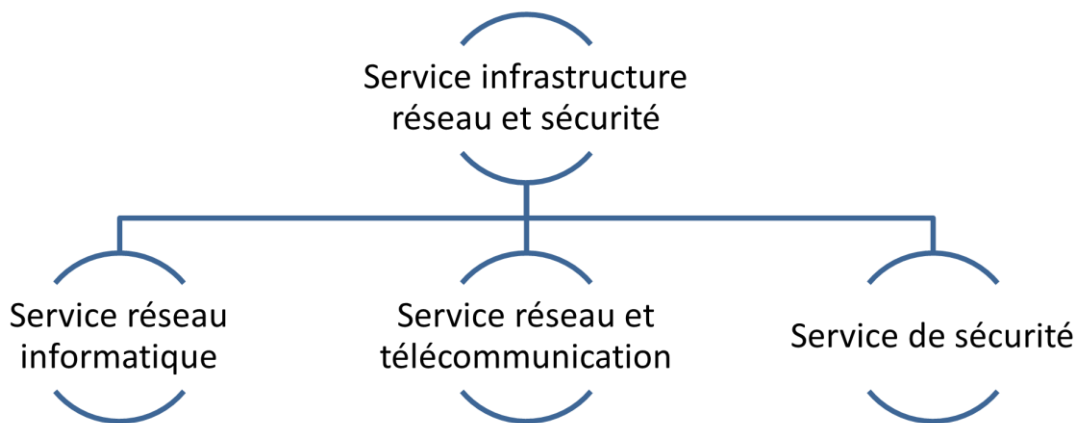


FIGURE III.4 – Organigramme de service d'accueil.

- **Service réseau informatique** : Ce service représente tous les appareils et périphériques au sein d'une entreprise qui sont physiquement ou virtuellement connectés les uns aux autres à partir d'un wifi professionnel ou d'autres méthodes afin de partager des ressources ou des informations. En fait, l'infrastructure réseau offre un large éventail de fonctionnalités pour les clients de services et les producteurs de services, telles que :
Limitation de débit, analyse, vérification, surveillance et enregistrement et sécurisation du réseau de cette entreprise.
- **Service réseau et Télécommunication** : Les services de télécommunications sont conçus pour transmettre des informations en un temps réel (synchronisation des informations) sous forme analogique ou numérique à l'exception de la radio et de la télévision. La plupart de ces services peuvent aider les clients à identifier leurs besoins en matière d'infrastructure de télécommunications.

Voici des exemples de services d'infrastructure de télécommunications :

- Pose de fibre optique.
 - Emplacement du site de la tour cellulaire.
 - Test d'antenne radio.
 - Installation d'équipements téléphoniques standards et réseau de données.
 - Téléphonie standard.
- **Service de sécurité** : Cette entreprise NTS accomplit à la fois le gardiennage et l'installation des systèmes de sécurité électroniques. Aussi elle fournit aux clients des solutions complètes et fiables pour protéger leurs ressources. Les services qu'elle réalise sont les suivants :
 - Caméras de surveillance.
 - Alarme anti- intrusion.
 - Détection incendie.
 - Pointeuse et Contrôles d'accès.
 - Vidéophonie.

D. Service télédistribution

Ce service est spécialisé dans la transmission de données par câble (fibre optique, paire torsadée et onde horizontale) ou autres systèmes de distribution (paraboles collectif, télévision numérique terrestre et audiovisuelle). Son objectif principal est de garantir l'installation de ces supports de transmission à haut débit. Enfin, les services de télédistribution ont été appelés à jouer un rôle majeur dans l'émergence des nouveaux médias tels que :

- Rediffusion de programmation par satellite.
- Transmission de chaînes de télévision par abonnement.
- Services interactifs.
- Programmation locale.

E. Service d'engineering

Il est constitué d'une équipe multidisciplinaire d'experts dont la mission est de rechercher et d'analyser les besoins des clients pour trouver la meilleure solution spécifique à leur projet. L'équipe de campus NTS n'hésite pas à se déplacer sur le terrain pour consulter l'état d'avancement du projet afin de faire face à d'éventuelles difficultés qui auraient pu survenir auparavant.

Cette équipe est composée :

- D'ingénieurs en télécommunications.
- D'informaticiens en gestion et sécurité des réseaux.
- D'administrateurs de systèmes d'information.
- D'informaticiens en programmation.
- De techniciens fibre.
- De techniciens supérieurs en informatique.

Leurs propositions sont en recherche informatique et sécurité et leurs cotations est dans la recherche sur les réseaux et les systèmes de télécommunication.

F. Service technico commerciale (marketing)

Leurs offres ne se limitent pas à de simples fournitures standards. Ils disposent d'une équipe qui s'assure de répondre aux besoins et au confort de ses précieux clients dans le but de développer les services de cette entreprise. Par ailleurs, ce service commercialise aussi les services proposés par campus NTS.

G. Service de financière

Le service financier situé au cœur de l'entreprise, représente l'ensemble des personnes chargées de la fonction comptable. Il intervient pour faire de bons investissements en prévenant d'éventuels risques de perte. Ce service contient un ensemble de tâches et rôles au sein de la société NTS :

Les tâches principales du Service des finances :

- Assurer une saine gestion des ressources financières de l'entreprise par la planification.
- La coordination et le contrôle de toutes les politiques et procédures requises pour la protection des actifs.
- La production des informations financières exactes et pertinentes afin que le gestionnaire puisse prendre la décision éclairée.

Le rôle du service financier :

- La préparation et du suivi des budgets de fonctionnement et d'investissement.
- La préparation des états financiers.
- La gestion de la trésorerie et des encaissements.
- La rémunération des employés, des comptes à payer.
- De l'acquisition des biens et services pour l'ensemble de l'entreprise, des projets de recherche.
- La réception des marchandises et du courrier.

H. Service hygiène

La sécurité et la santé occupent une place prépondérante dans les conditions de travail. L'employeur est en effet responsable de la santé et de la sécurité de ses salariés. Il coordonne ses différentes équipes et attribue les moyens nécessaires tels que :

- Des actions de prévention des risques professionnels et de la pénibilité au travail.
- La mise en place d'une organisation et de moyens adaptés.

III.3 Partie 2 : Etat des lieux

III.3.1 Présentation du réseau campus NTS

L'entreprise a une architecture en couches et, pour assurer la communication entre ses différents services, elle connecte son LAN à une connexion FTTH fournie par un fournisseur d'accès Internet. Le schéma ci-dessous nous montre l'infrastructure du réseau NTS :

A. Présentation de l'architecture réseau existant dans l'entreprise

NTS construit un réseau en choisissant une topologie arborescente pour connecter ses différents appareils, comme illustrée dans la figure suivante :

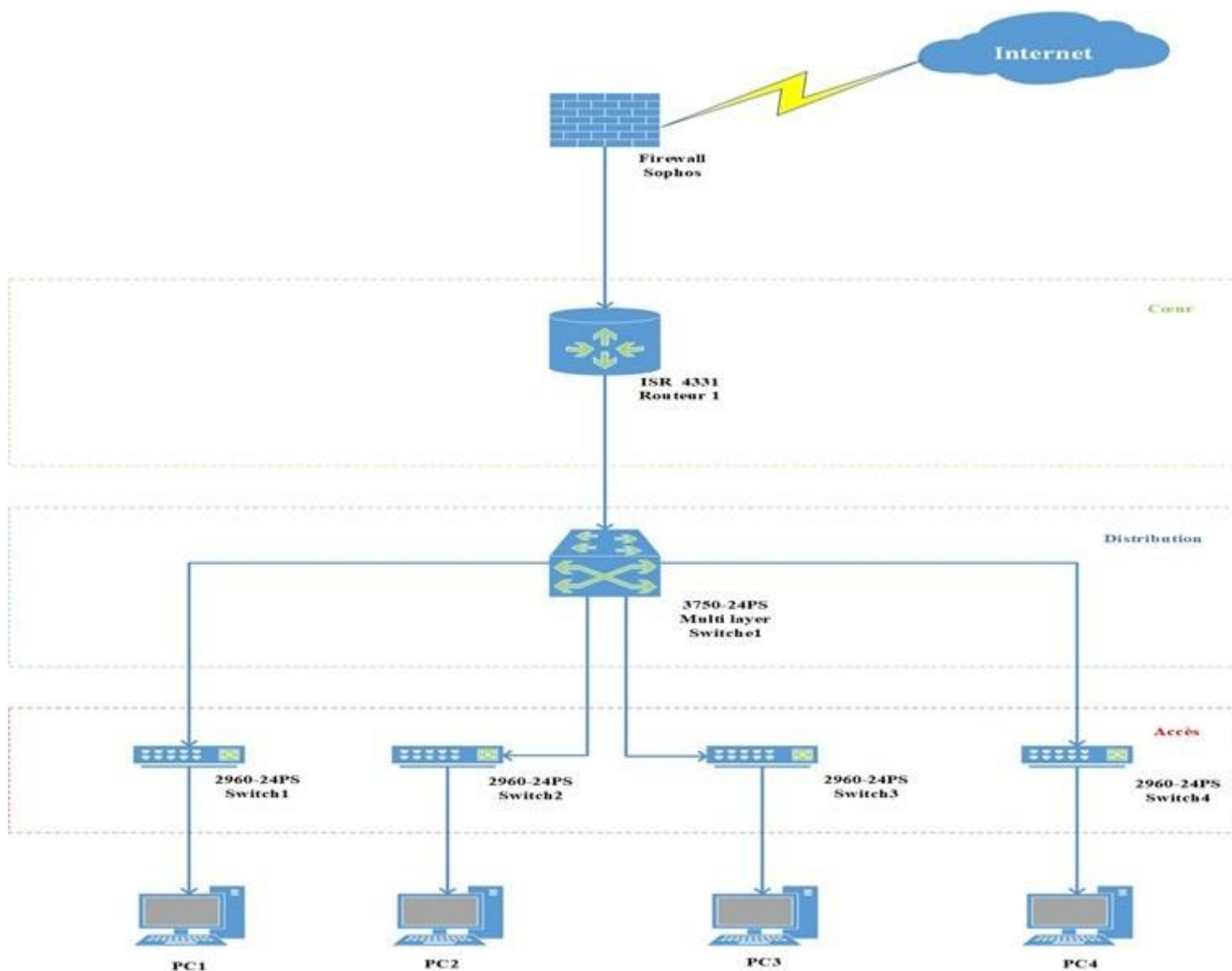


FIGURE III.5 – Architecture de réseau (NTS).

B. Analyse du parc informatique

❖ Présentation d'environnement hard et soft :

Nom de l'équipement	Le hardware (hard)	Software (soft)
Routeur	ISR 4331	IOS (International Organisation For Standardisation)
Pare-feu	SOPHOS XG	Linux
Switch	<ul style="list-style-type: none">• Cisco Catalyst 3750-24PS• Cisco Catalyst2960-24PS	IOS (International Organisation For Standardisation)
Server	HP Pro Liant DL380P génération 10	Windows server 2022
PC portable	Dell IAER 35 R	Windows 10

Table III.2 – L'environnement hardware et le software.

❖ Les caractéristiques des équipements par niveaux :

Nom de l'équipement	Modèle	Caractéristique
<p>Routeur</p> 	ISR 4331	<ul style="list-style-type: none"> • RAM : 4 Go (installé) /16 GO (maximum) • Mémoire Flash : 4000 MO • Débit : 100 Mb/s • Protocole de liaison de données : Ethernet, fast Ethernet et gigabit-ethernet
<p>Pare-feu</p> 	SOPHOS XG	<ul style="list-style-type: none"> • Débit : 4000 Mbit/s • Débit IPS : 2700Mbit/s • Débit VPN IP sec : 560 Mbit/s • @ IP/Numéro de port
<p>Switch</p> 	Cisco Catalyst 3750-24PS Switch	<ul style="list-style-type: none"> • Ports : 24 ports • Mémoire Flash : 16MO • Mémoire RAM : 128MO • Capacité de commutation : 32 Gbit/s
<p>Switch</p> 	Cisco Catalyst 2960-24PS Switch	<ul style="list-style-type: none"> • Ports : 24 ports • Mémoire Flash : 128MO • Mémoire RAM : 512MO • Capacité de commutation : 56 Gbit/s
<p>Server</p> 	HP ProLiant DL380P génération 10	<p>Processeur Intel Xeon Silver 4110 (Octo-Core 2.1 GHZ / 3.0 GHZ Turbo-16 Threads-cache 11Mo)16 Go DDR4 RDIMM (1x 16 GO -12 slots)</p>
<p>PC portable</p> 	Dell IAER 35 R	<ul style="list-style-type: none"> • AMD core : i5 8th génération • RAM : 8GO • Disque : 256GO • Ecran : UHD Graphics 620 (1920×1080×32b)

Table III.3 – Détails des ressources disponibles de l'entreprise.

III.4 Partie 3 : Problématiques et Solutions proposées

III.4.1 Problématiques

Lors de notre stage à Bejaia entreprise NTS, nous avons constaté qu'il dispose d'un réseau local de diverses plates-formes, de différents services, nous avons pu mettre en évidence des pannes de réseau, à savoir :

- La plupart des ports de commutateur se trouvent sur le VLAN natif, ce qui risque d'augmenter les domaines de diffusion et de compromettre la sécurité. Contredit, l'objectif de l'utilisation des VLAN, qui est de micro-segmenter le réseau en petits domaines de diffusion.
- Absence de contrôle d'accès pour certains sites Web gourmands en bande passante qui réduit la vitesse à laquelle les employés travaillent (YouTube, Face book, etc.).
- Les adresses IP changées entre les sites de l'entreprises ne sont pas masquées.
- La société s'étend à des sites distants et à plusieurs centres de distribution. Il dispose donc d'un réseau important et nécessite une interconnexion permanente fiable et privée entre ces différents sites.
- Leur réseau manque de plusieurs configurations et technologies :
 - Technologie d'agrégation de liens pour augmenter la bande passante.
 - Protocole de transfert de données.
 - L'authentification Radius 802 .1X.

III.4.2 Solutions

Le principal défi d'une architecture de réseau sécurisée est de pouvoir réguler l'accès aux ressources réseau à partir du réseau local et de l'extérieur, tout en limitant autant que possible les vulnérabilités aux éventuelles attaques ou vol d'informations afin d'améliorer la sécurité du réseau local. Pour cela, nous avons proposé différentes solutions pour les problèmes que nous avons déjà mentionnés :

- Les VLAN réduisent les domaines de diffusion et améliorent la sécurité du réseau.
- Le VLAN privé enregistre les adresses IP et améliore la sécurité des ports basculer sur le calque 2.
- Mettre en place une solution de pare-feu grâce à sa fonction de configuration, selon les besoins d'accès et de filtrage au réseau Internet, les utilisateurs sont répartis en groupes. Ports sécurisés, utilisés pour filtrer et limiter le nombre d'adresses MAC autorisées à se connecter aux ports des commutateurs Cisco. Établir un lien VPN entre les sites de Béjaïa et d'Alger.
- Placez une zone démilitarisée (DMZ) qui aidera les entreprises à détecter et à corriger les failles de sécurité avant qu'elles n'atteignent le réseau interne où sont stockées les ressources les plus précieuses.
- Le protocole HSRP intégré, fournit une redondance pour tous les périphériques réseau, c'est-à-dire que si le chemin actif rencontre une erreur, un autre chemin sera ouvert.
- Mise en œuvre de la technologie Ether channel conçue pour augmenter la vitesse et tolérance aux pannes entre les commutateurs, les routeurs et les serveurs.
- La définition de la zone démilitarisée peut désactiver les services de la zone démilitarisée utilisée pour empêcher les autres d'accéder aux appareils interconnectés au réseau.
- Ajouter une authentification pour les ports qui est Radius.

III.5 Conclusion

Dans ce chapitre, nous avons donné un aperçu général de l'entreprise du campus NTS, puis nous avons découvert un problème qui nous a amenés à rechercher et à mettre en œuvre une nouvelle architecture de réseau sécurisée. Enfin, l'application de la solution proposée fera l'objet du chapitre suivant.

Réalisation

IV.1 Introduction

Ce chapitre est dédié à l'amélioration de l'architecture réseau du campus NTS, nous définirons les différents outils que nous utiliserons et l'installation et la configuration requises, dans lequel nous ferons référence aux différentes étapes pour mettre en œuvre la solution proposée en Chapitre 3.

IV.2 Environnement de travail

IV.2.1 Présentation de logiciel de simulation

IV.2.1.1 GNS3

Gns3 (Graphical Network Emulator) est un émulateur de réseau graphique multiplateforme à savoir Windows, Linux et MacOS. L'un des avantages majeurs du logiciel est qu'il est open source et gratuit que vous pouvez télécharger sur <http://gns3.com>. Il est utilisé par les ingénieurs réseau du monde entier pour simuler, configurer, tester et dépanner des réseaux virtuels et réels cars il permet de connecter des hyper viseurs à partir de VMware ou Virtual Box.



FIGURE IV.1 – Logo de GNS3.

IV.2.1.2 VMware Workstation 16.1.2

VMware Workstation est un logiciel de machine virtuelle (VM) qui permet aux utilisateurs d'exécuter plusieurs machines virtuelles sur une seule machine physique. Elle se réalise sur son propre système d'exploitation (OS, Operating System), tel que : Linux, MacOS, Windows, et bénéficie des mêmes équipements qu'une machine physique : CPU, mémoire RAM, disque dur et carte réseau. VMware simplifie la gestion et offre un meilleur contrôle sur l'infrastructure informatique.



FIGURE IV.2 – Logo de VMware Workstation 16.

IV.2.2 Partie hardware

- **Une carte réseau** : est un élément matériel informatique de couche 1 du modèle OSI qui fournit l'interface entre le réseau et l'équipement.
- **Pont (Bridge)** : est un périphérique d'infrastructure réseau intelligent de couche 2 du modèle OSI qui utilise des adresses MAC pour échanger, envoyer et filtrer les trames Ethernet. Mais, il n'a que quelques ports et semble lent.
- **Commutateur (Switch)** : est un équipement d'interconnexion réseau de niveau 2 du modèle OSI. Il permet de rediriger les informations reçues seulement vers le port de la machine concernée.
- **Routeur (router)** : est un périphérique réseau informatique de couche 3 du modèle OSI qui assure le routage des paquets de données.

IV.2.3 Partie software

- **Système linux** : est un système d'exploitation open source qui représente l'interface entre l'application et le matériel.
- **IOS** : (abréviation de Internetwork Operating System, « système d'exploitation pour la connexion des réseaux »), anciennement IOS, est le système d'exploitation produit par Cisco Systèmes et qui équipe la plupart de ses équipements.
- **Windows 10** : est le successeur du système d'exploitation Windows 8 publié par Microsoft en 2015 pour gérer les ressources d'un ordinateur. Il est destiné aux particuliers et aux entreprises.
- **Windows Server 2022** : est le système d'exploitation orienté vers le serveur de Microsoft basé sur l'architecture Windows NT. Il connecte l'environnement sur site avec Azure la plateforme sur cloud de Microsoft. Il ajoute une nouvelle couche de sécurité tout en vous aidant à moderniser vos applications et infrastructures.
- **Putty** : est une application open source qui établit des sessions à distance sur des ordinateurs à l'aide des protocoles réseaux tels que SSH, Telnet et login.
- **Wireshark** : est un analyseur de paquets réseau gratuit et open source. Il peut être utilisé comme un simple outil de dépannage réseau ainsi que pour l'analyse de la sécurité et le développement de logiciels.

IV.2.4 Serveurs et Services

- **Serveur DHCP** : est un protocole réseau qui attribue dynamiquement des adresses IP aux machines connectées à un réseau. Il fournit également d'autres paramètres réseau : masque de sous-réseau, adresse IP de la passerelle et DNS.
- **Serveur DNS (Domaine Name System)** : est un protocole qui permet de convertir un nom de domaine en adresse IP pour simplifier la gestion de réseau.
- **Active Directory** : Est un service d'annuaire utilisé dans un environnement Windows server. Il s'agit d'une structure de base de données qui partage des informations d'infrastructure pour gérer l'authentification et l'autorisation des utilisateurs et des machines sur le réseau.
- **L'authentification Radius 802 .1X** : Norme IEEE 802.1X pour le contrôle d'accès au réseau basé sur les ports et la protection des réseaux locaux Ethernet contre les utilisateurs non autorisés. Il bloque tout le trafic entrant et sortant du demandeur (client) au niveau de l'interface jusqu'à ce que les informations d'identification du demandeur soient fournies et associées au serveur d'authentification (serveur RADIUS). Lorsque le demandeur est authentifié, le commutateur cesse de bloquer l'accès et ouvre l'interface du demandeur.

IV.3.1 Le plan d'adressage des sous réseaux « VLANs »

Nom du VLAN	ID du VLAN	Adresse du sous-réseau	Passerelle du sous-réseau
VLAN SC	100	10.0.100.0 /24	10.0.100.254
VLAN SCF	101	10.0.101.0 /24	10.0.101.254
VLAN FH	102	10.0.102.0 /24	10.0.102.254
VLAN SF	103	10.0.103.0 /24	10.0.103.254
VLAN SERP	104	10.0.104.0 /24	10.0.104.254
VLAN Management	105	10.0.105.0 /24	10.0.105.254
VLAN Voice	106	10.0.104.0 /24	10.0.106.254
VLAN NATIVE	999

Table IV.1 – Plan d'adressage des VLANs.

IV.3.2 Plan d'adressage des Privates VLANs et ports associés

Nom du VLAN	ID du VLAN	Ports hosts	Ports promiscuous mapping	Adresse Private VLAN
SECONDARY COMMUNITY	201	200 201	200 201,202	192.168.3.10/24 192.168.3.11/24
SECONDARY ISOLATED	202	200 202	200 201,202	192.168.3.12/24 192.168.3.13/24
PRIMARY	200	/	200 201,202	192.168.3.1/24

Table IV.2 – Plan d'adressage des sous(sous-réseaux) Private VLAN.

IV.3.3 Plan d'adressage des équipements d'interconnexion

Equipements	Interface réseau	Adresse IP
Pare feu bejaia	Internat 1 Internal 2 DMZ External(WAN)	192.168.100.1/24 192.168.200.1/24 192.168.3.1/24 192.168.111.133/24
Pare feu alger	Internal External(WAN)	192.168.2.1/24 192.168.111.134/24
Router Core 1	Ethernet 0/0 Ethernet 0/1	Utilisé pour le routage inter-vlan et HSRP 192.168.100.2/24
Router Core 2	Ethernet 0/0 Ethernet 0/1	Utilisé pour le routage inter-vlan et HSRP 192.168.200.2/24
Switch DIS1	Management vlan 105	10.0.105.3/24
Switch DIS2	Management vlan 105	10.0.105.4/24
Switch acces 1	Management vlan 105	10.0.105.5/24
Switch acces 2	Management vlan 105	10.0.105.6/24
Switch acces 3	Management vlan 105	10.0.105.7/24
Switch acces 4	Management vlan 105	10.0.105.8/24
Serveur	Ethernet $\frac{1}{2}$	10.0.105.100/24

Table IV.3 – Plan d'adressage des équipements d'interconnexion.

IV.3.4 Tableau du routage inter-vlan et du protocole HSRP

Equipement	Interface	Adresses IP	Passerelle virtuel
Core1	e0/0	/	/
	e0/0.100	10.0.100.1/24	10.0.100.254
	e0/0.101	10.0.101.1/24	10.0.101.254
	e0/0.102	10.0.102.1/24	10.0.102.254
	e0/0.103	10.0.103.1/24	10.0.103.254
	e0/0.104	10.0.104.1/24	10.0.104.254
	e0/0.105	10.0.105.1/24	10.0.105.254
	e0/0.106	10.0.106.1/24	10.0.106.254
Core2	e0/0.100	10.0.100.2/24	10.0.100.254
	e0/0.101	10.0.101.2/24	10.0.101.254
	e0/0.102	10.0.102.2/24	10.0.102.254
	e0/0.103	10.0.103.2/24	10.0.103.254
	e0/0.104	10.0.104.2/24	10.0.104.254
	e0/0.105	10.0.105.2/24	10.0.105.254
	e0/0.106	10.0.106.2/24	10.0.106.254

Table IV.4 – Plan d’adressage des sous(sous-réseaux) Private VLAN.

IV.4 Configuration de l’active Directory

Nous allons maintenant commencer à configurer notre Active Directory. La première étape consiste à créer une nouvelle forêt qu’on va renommer « **campusnts.local** ». Le nom attribué, Windows nous invite à sélectionner le niveau fonctionnel de la forêt Active Directory. Dans notre exemple, nous allons établir un niveau opérationnel pour Windows 2022 qui nous offre des options d’installations supplémentaires comme un serveur DNS compatible avec notre Active Directory. Le nom de domaine « **campusnts.local** » est notre premier contrôleur de domaine activé depuis le catalogue global. Après avoir installé et configuré ces services, cliquez sur FIN pour redémarrer le système. À la fin de l’installation, nous installerons deux rôles comme indiqué dans l’image suivante :

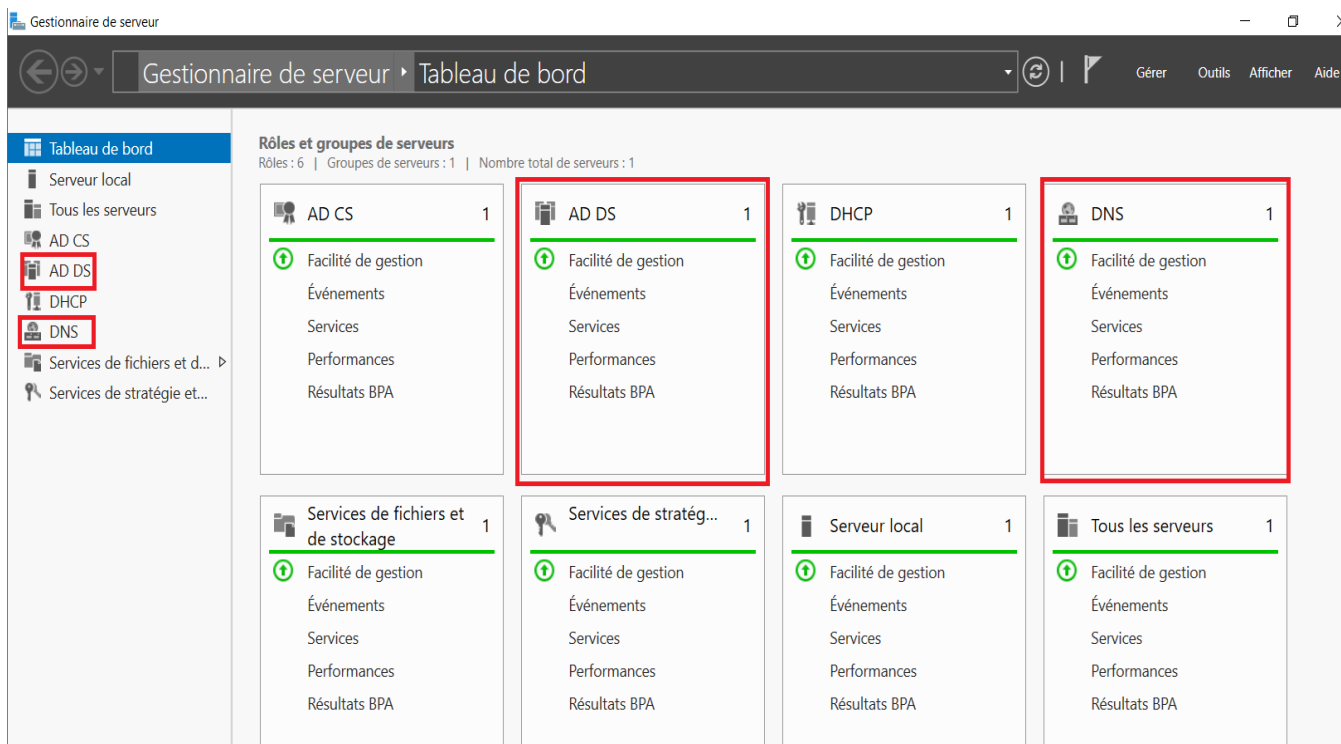


FIGURE IV.4 – Rôle AD DS et DNS.

On a commencé par créer une unité d'organisation, il suffit d'aller sur le nom de notre domaine campusnts.local → en cliquant sur le bouton droit, on sélectionne → nouveau Unité d'organisation puis on va entrer le nom de notre unité de l'organisation qui est SITE BEJAIA → SERVICE ETUDE pour créer des comptes pour les utilisateurs, il faut aller sur utilisateur → cliquer sur le bouton droit nouveau → utilisateur pour remplir les informations correspondantes à l'utilisateur ainsi que le mot de passe d'ouverture de sa session → valider.

Ensuite on passe à la création des groupes et des ordinateurs pour les utilisateurs déjà créés.

Utilisateurs et ordinateurs Active Directory

Nom	Type	Description
Builtin	builtinDomain	
Computers	Conteneur	Default container for up...
Domain Con...	Unité d'organis...	Default container for do...
Foreign Secur...	Conteneur	Default container for sec...
Managed Se...	Conteneur	Default container for ma...
Users	Conteneur	Default container for up...

Nouvel objet - Unité d'organisation

Créer dans : campusnts.local/

Nom : SITE BEJAIA

Protéger le conteneur contre une suppression accidentelle

OK Annuler Aide

1

Nouvel objet

Créer dans : campusnts.local/SITE BEJAIA

Nom : SERVICE ETUDE

Protéger le conteneur contre une suppression accidentelle

OK Annuler Aide

2

Nouvel objet - Groupe

Créer dans : campusnts.local/SITE BEJAIA/SERVICE ETUDE/Utilisateurs

Nom du groupe : groupe télécom et réseau

Nom de groupe (antérieur à Windows 2000) : groupe télécom et réseau

Étendue du groupe

- Domaine local
- Globale
- Universelle

Type de groupe

- Sécurité
- Distribution

OK Annuler

3

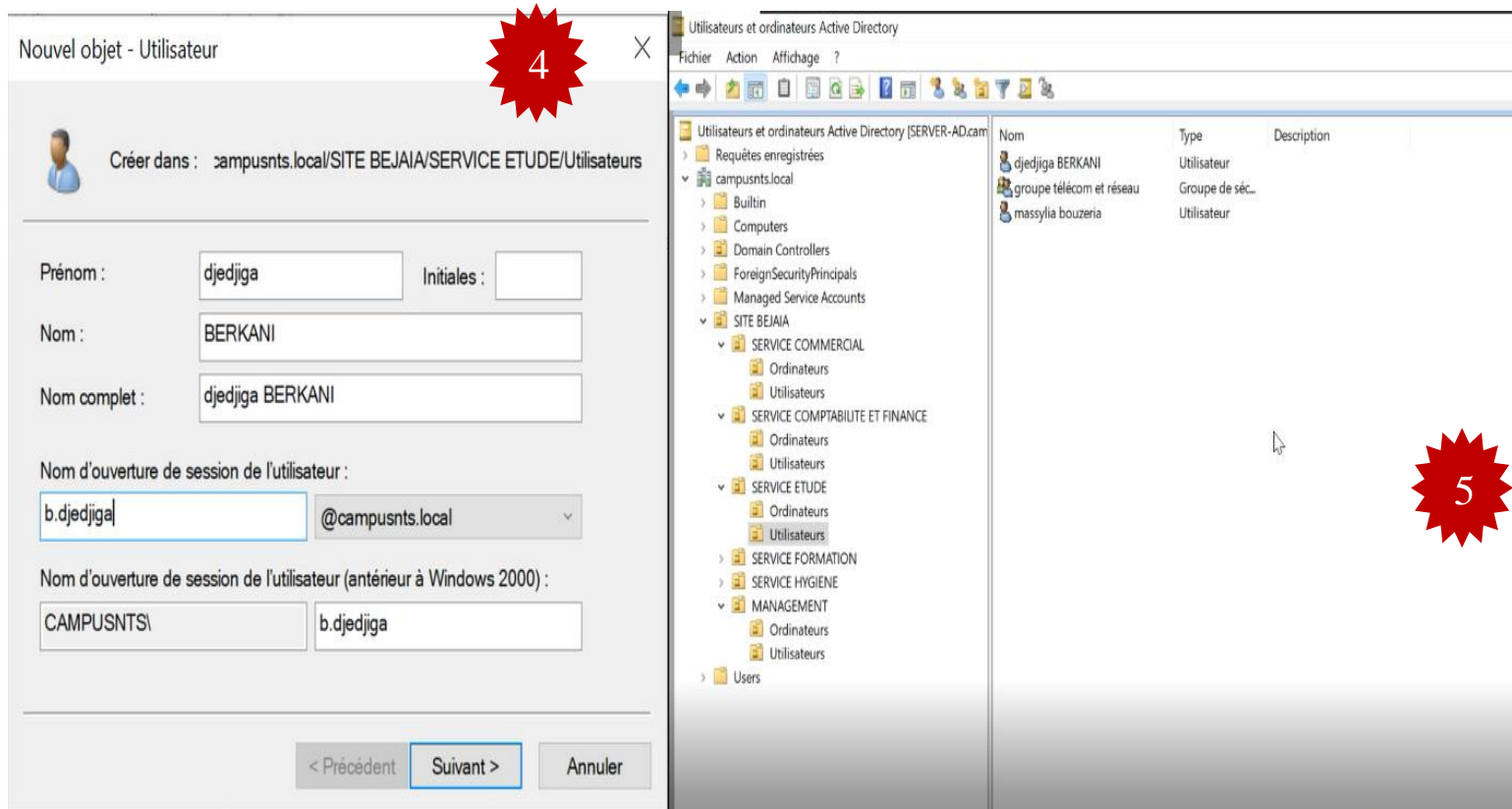


FIGURE IV.5 – Création des groupes, utilisateurs, ordinateurs.

IV.5 Configuration de relais DHCP

Le relais DHCP est une fonctionnalité utilisée par les routeurs (également appelés agents de relais) pour permettre le transfert des configurations DHCP entre les hôtes et les serveurs DHCP distants qui ne se trouvent pas sur le même réseau. La configuration du relais DHCP est illustrée dans la figure suivante :

```

core1(config)#interface Ethernet0/0.100
core1(config-subif)# encapsulation dot1Q 100
core1(config-subif)# ip address 10.0.100.1 255.255.255.0
core1(config-subif)# ip helper-address 10.0.105.100
    
```

FIGURE IV.6 – Configuration de relais DHCP sur le router core1 pour le vlan 100.

IV.6 Création d'un groupe et utilisateurs radius

Aller sur utilisateur Cliquer → sur le bouton droit « nouveau » pour Remplir les informations correspondantes à l'utilisateur Radius → Valider → Ensuite on passe à la création du groupe « télécoms et réseau » pour les utilisateurs : « berkani djedjiga et bouzeria massylia ».

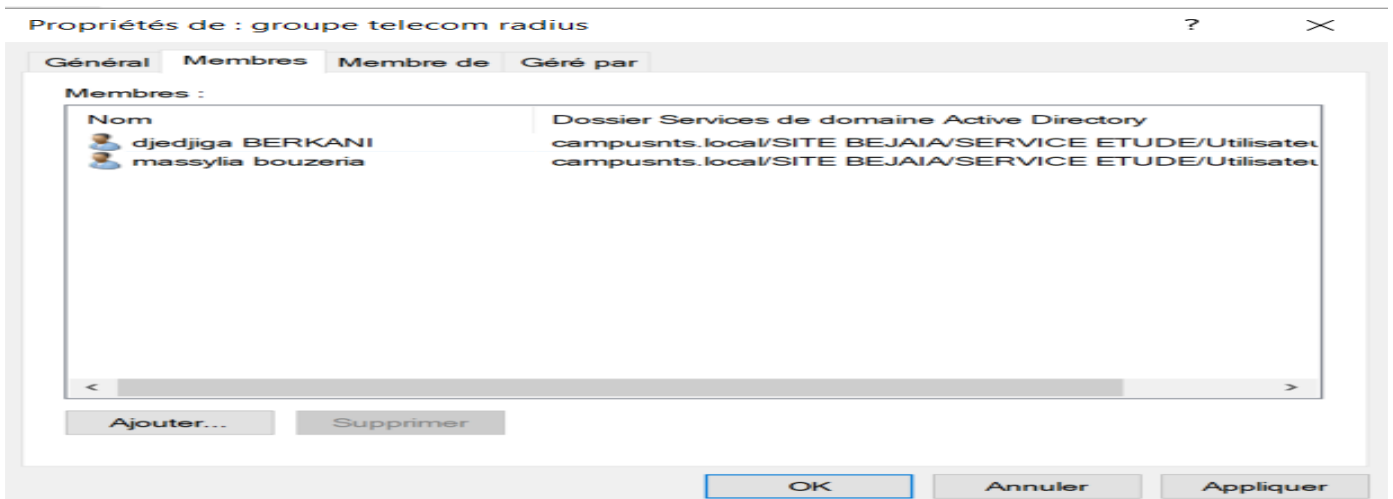
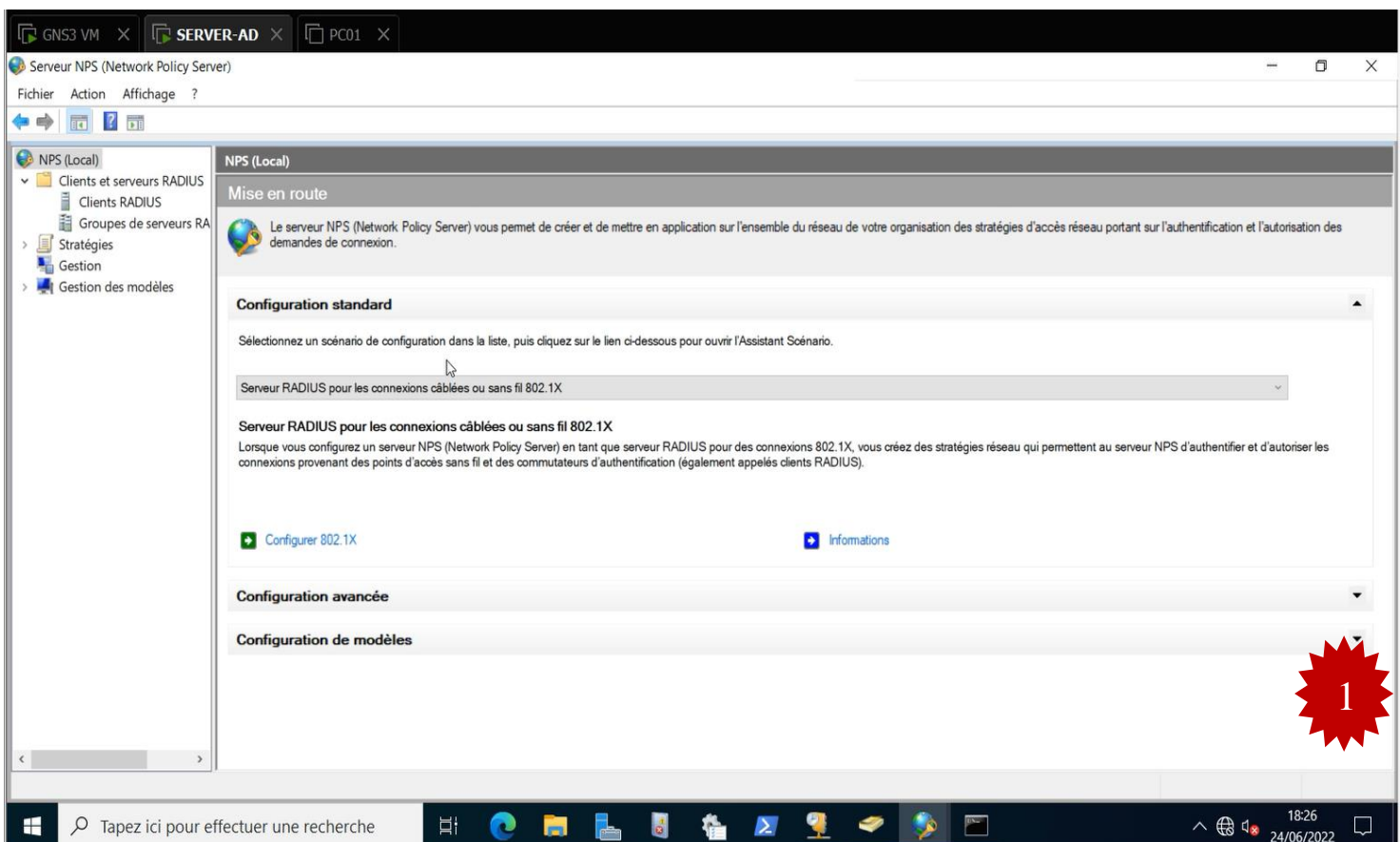


FIGURE IV.7 – Création des utilisateurs et groupe radius.

Par la suite on va créer une stratégie d'authentification et de la demande de connexion des clients radius pour le groupe vlan 104 que nous avons choisi pour cette dernière.



Configurer 802.1X

Sélectionner le type de connexions 802.1X

Type de connexions 802.1X :

Connexions sans fil sécurisées

Lorsque vous déployez des points d'accès sans fil 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients sans fil qui se connectent via ces points d'accès.


Connexions câblées (Ethernet) sécurisées

Lorsque vous déployez des commutateurs d'authentification 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients Ethernet qui se connectent via ces commutateurs.

Nom :
Ce texte par défaut est utilisé pour composer le nom de chacune des stratégies créées à l'aide de cet Assistant. Vous pouvez vous servir du texte par défaut ou le modifier.

Connexions câblées (Ethernet) sécurisées vlan 104

Précédent **Suivant** Terminer Annuler



Configurer 802.1X

Spécifier les commutateurs 802.1X

Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification. Les clients RADIUS ne sont pas des ordinateurs clients.


Pour spécifier un client RADIUS, cliquez sur Ajouter.

Clients RADIUS :

DIS1

Ajouter...
Modifier...
Supprimer

Précédent **Suivant** Terminer Annuler



Configurer 802.1X

Configurer une méthode d'authentification


Sélectionnez le type de protocole EAP pour cette stratégie.

Type (basé sur la méthode d'accès et la configuration réseau) :

Microsoft: PEAP (Protected EAP)

Configurer...

Précédent **Suivant** Terminer Annuler



Configurer 802.1X

Modifier les propriétés EAP Protégé

Sélectionnez le certificat que le serveur doit utiliser comme preuve de son identité auprès du client. Un certificat configuré pour EAP Protégé dans la stratégie de demande de connexion remplacera ce certificat.

Certificat délivré à : SERVER-AD.campusnts.local

Nom convivial : SERVER-AD.campusnts.local

Émetteur : campusnts-SERVER-AD-CA

Date d'expiration : 24/06/2023 18:22:56

Activer la reconnexion rapide
 Déconnecter les clients sans chiffrement forcé

Types EAP


Mot de passe sécurisé (EAP-MSCHAP version 2)

Monter
Descendre

Ajouter Modifier Supprimer **OK** Annuler

Configurer...

Précédent **Suivant** Terminer Annuler



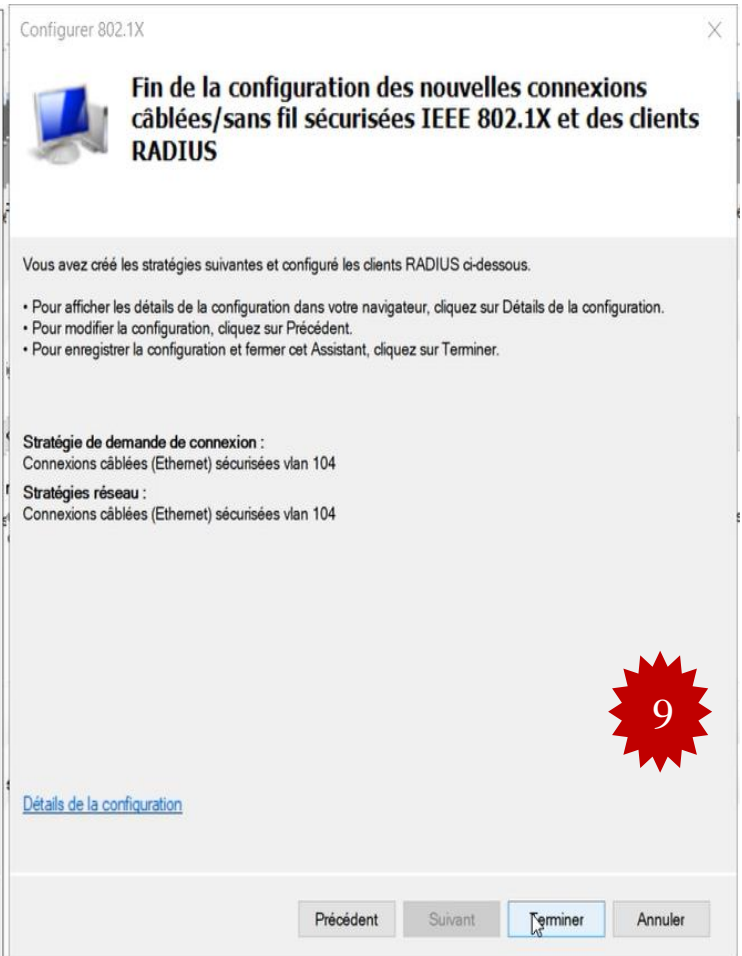
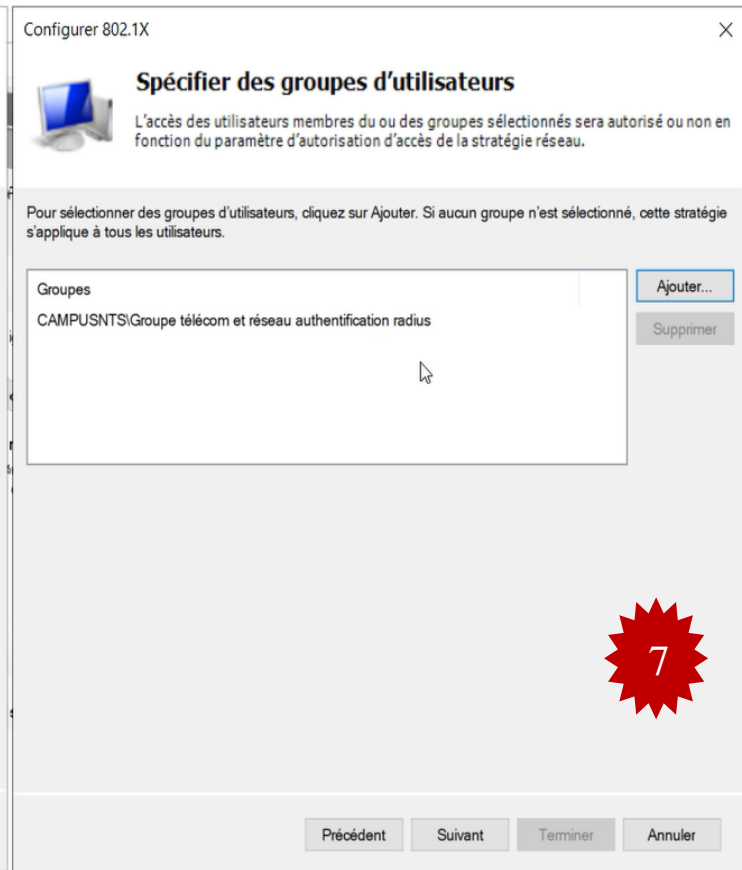
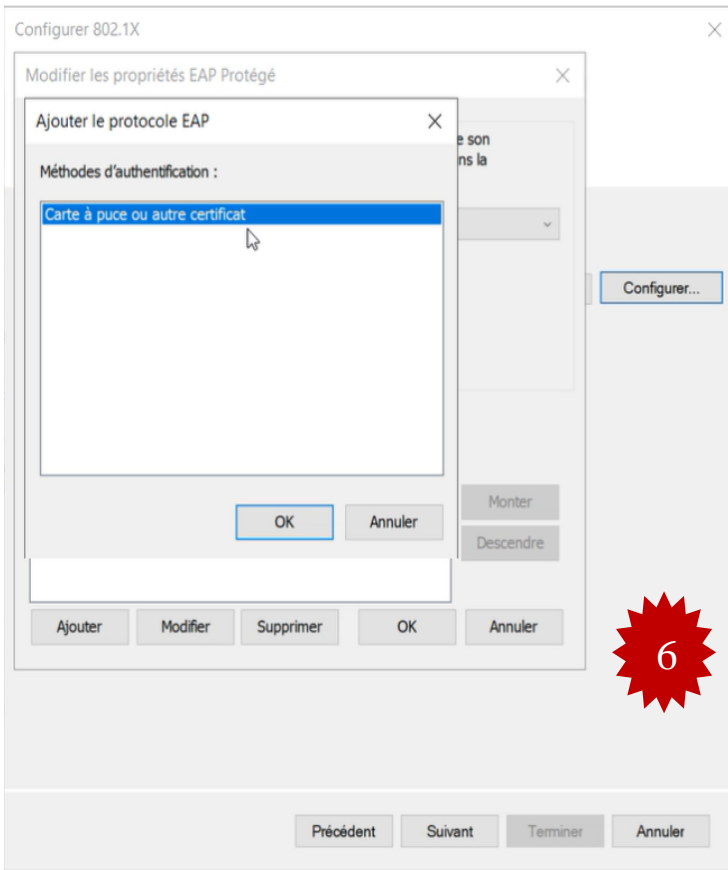


FIGURE IV.8 – Configuration d'une stratégie de connexion radius.

Maintenant, on va créer des connexions pour nos clients radius. Dans notre cas, nous avons choisi le Switch distributeur 2 qui est le plus près des clients Vlan 104.

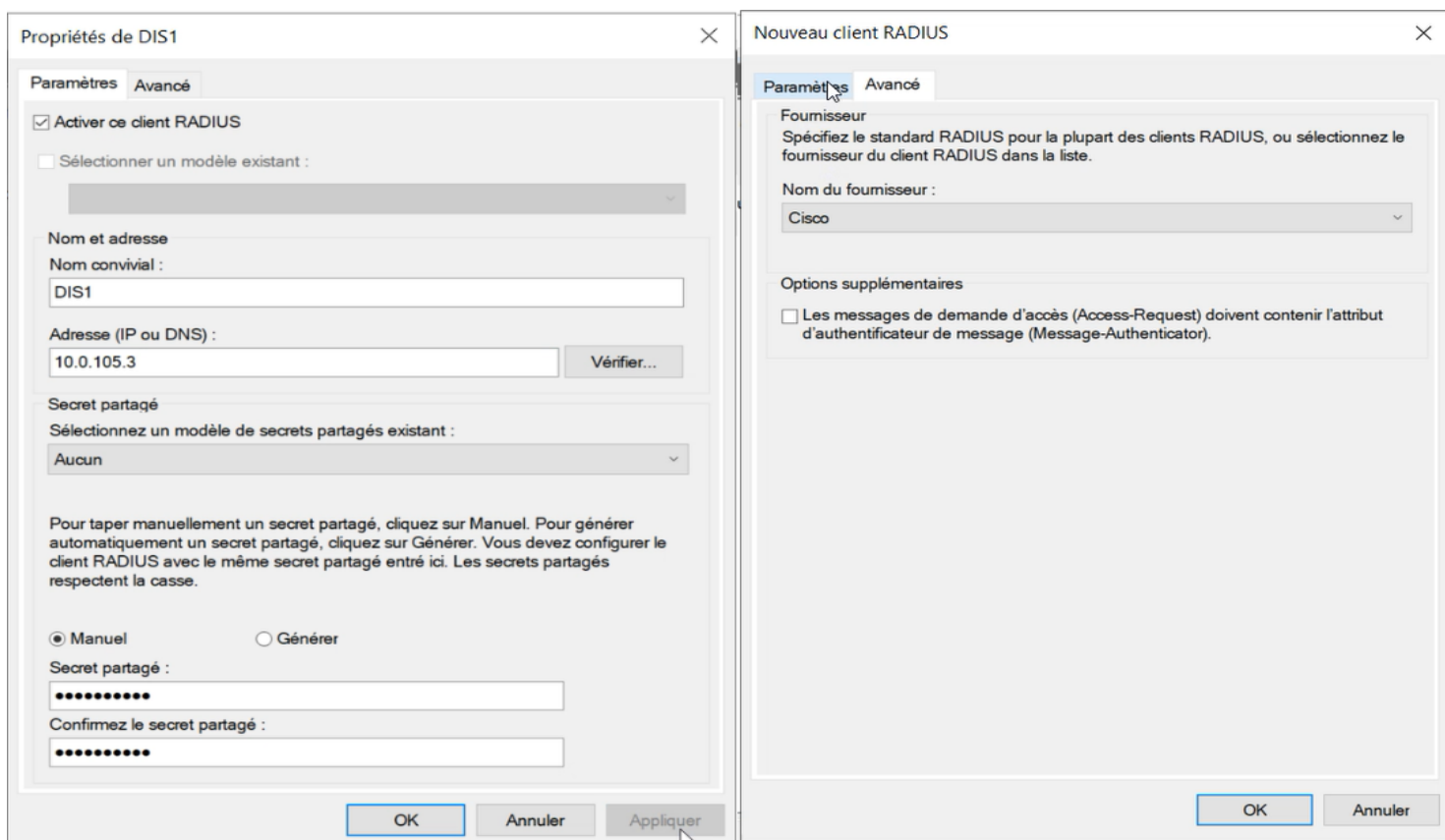
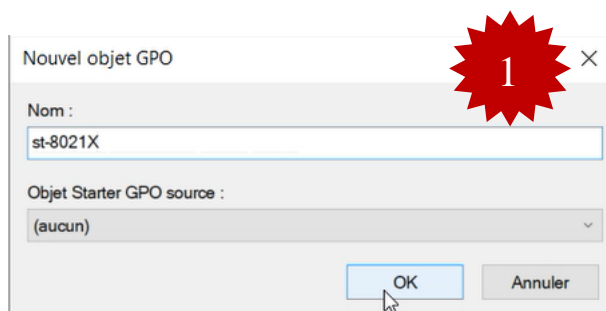


FIGURE IV.9 – Configuration de clients Radius.

Après la création des groupes et des utilisateurs radius, on va passer à la création de la stratégie du groupe radius qui est un ensemble d'outils intégrés à Windows Serveur afin de permettre aux services informatiques de gérer de manière centralisée les environnements utilisateurs et les configurations des machines en appliquant des stratégies.



Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Scripts (démarrage/arrêt)

- Paramètres de sécurité
 - Stratégies de comptes
 - Stratégies locales
 - Journal des événements
 - Groupes restreints
 - Services système
 - Registre
 - Système de fichiers
 - Stratégies de réseau filaire (IEEE 802.3)
 - Pare-feu Windows Defender avec fonctionnalités avancées
 - Stratégies du gestionnaire de listes de ressources
 - Stratégies de réseau sans fil (IEEE 802.11)
 - Stratégies de clé publique
 - Stratégies de restriction logicielle
 - Stratégies de contrôle de l'application
 - Stratégies de sécurité IP sur Active Directory
 - Configuration avancée de la stratégie d'application
 - QoS basée sur la stratégie
- Modèles d'administration : définitions de stratégie
 - Composants Windows
 - Imprimantes
 - Menu Démarrer et barre des tâches
 - Panneau de configuration
 - Réseau
 - Serveur
 - Système
 - Tous les paramètres
- Préférences

Nom du service	Démarrage	Autorisation
Accès aux données utilisateur_5f3cb	Non défini	Non défini
Acquisition d'image	Non défini	Non défini
Agent de stratégie IPS	Non défini	Non défini
Alimentation	Non défini	Non défini
Appel de procédure distante	Non défini	Non défini
Application d'assistance	Non défini	Non défini
Application système	Non défini	Non défini
Assistance IP	Non défini	Non défini
Assistance NetBIOS sur IP	Non défini	Non défini
Assistant Connectivité	Non défini	Non défini
Assistant Connexion à Internet	Non défini	Non défini
Audio Windows	Non défini	Non défini
CaptureService_5f3cb	Non défini	Non défini
Carte à puce	Non défini	Non défini
Carte de performance	Non défini	Non défini
Centre de distribution	Non défini	Non défini
Clichié instantané des applications	Non défini	Non défini
Client de stratégie de groupe	Non défini	Non défini
Client de suivi de lien	Non défini	Non défini
Client DHCP	Non défini	Non défini
Client DNS	Non défini	Non défini
Collecteur d'événements de Windows	Non défini	Non défini
Configuration automatique de réseau câblé	Non défini	Non défini
Configuration des services Bureau à distance	Non défini	Non défini
Connaissance des emplacements réseau	Non défini	Non défini
Connexions réseau	Non défini	Non défini
Conteneur Microsoft Passport	Non défini	Non défini

Propriétés de : Configuration automatique de réseau c...

Paramètre de stratégie de sécurité

Configuration automatique de réseau câblé

Définir ce paramètre de stratégie

Sélectionnez le mode de démarrage du service :

Automatique

Manuel


Désactivé

Modifier la sécurité...

OK Annuler Appliquer

Tapez ici pour effectuer une recherche

19:13 24/06/2022



SERVER-AD

Éditeur de gestion des stratégies de groupe

Fichier Action Affichage ?

Scripts (démarrage/arrêt)

- Paramètres de sécurité
 - Stratégies de comptes
 - Stratégies locales
 - Journal des événements
 - Groupes restreints
 - Services système
 - Registre
 - Système de fichiers
 - Stratégies de réseau filaire (IEEE 802.3)
 - Pare-feu Windows Defender avec fonctionnalités avancées
 - Stratégies du gestionnaire de listes de ressources
 - Stratégies de réseau sans fil (IEEE 802.11)
 - Stratégies de clé publique
 - Stratégies de restriction logicielle
 - Stratégies de contrôle de l'application
 - Stratégies de sécurité IP sur Active Directory
 - Configuration avancée de la stratégie d'application
 - QoS basée sur la stratégie
- Modèles d'administration : définitions de stratégie
 - Composants Windows
 - Imprimantes
 - Menu Démarrer et barre des tâches
 - Panneau de configuration
 - Réseau
 - Serveur
 - Système
 - Tous les paramètres
- Préférences

Nom	Description
Nouvelle stratégie d...	Exemple de description

Nouvelle stratégie de réseau câblé Properties

Général Sécurité

Permettre l'utilisation de l'authentification IEEE 802.1X pour l'accès au réseau

Sélectionner une méthode d'authentification réseau :

Microsoft: PEAP (Protected EAP) Propriétés...

Mode d'authentification :

Authentification utilisateur


Nbre max. d'échecs d'authentification : 2

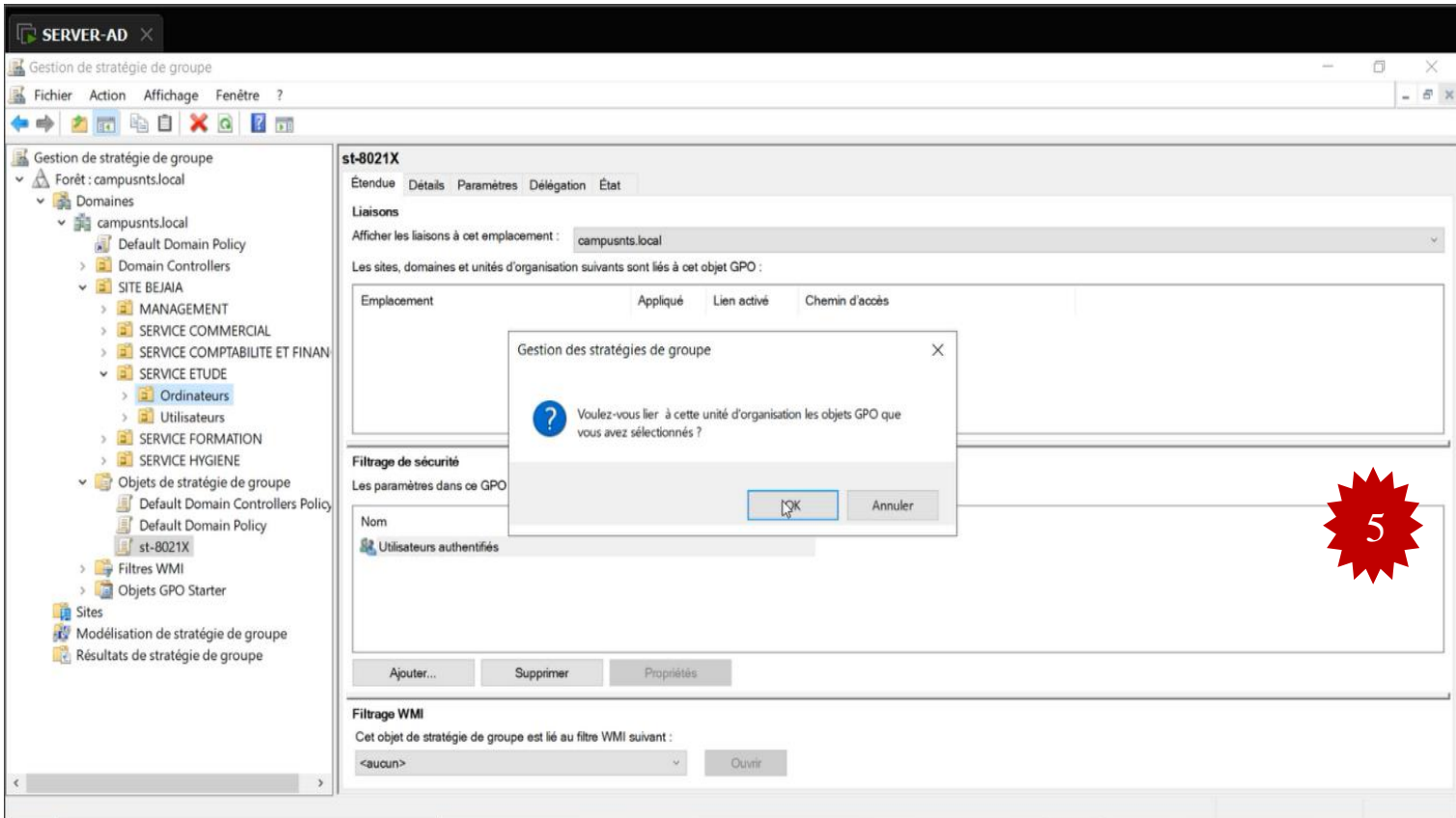
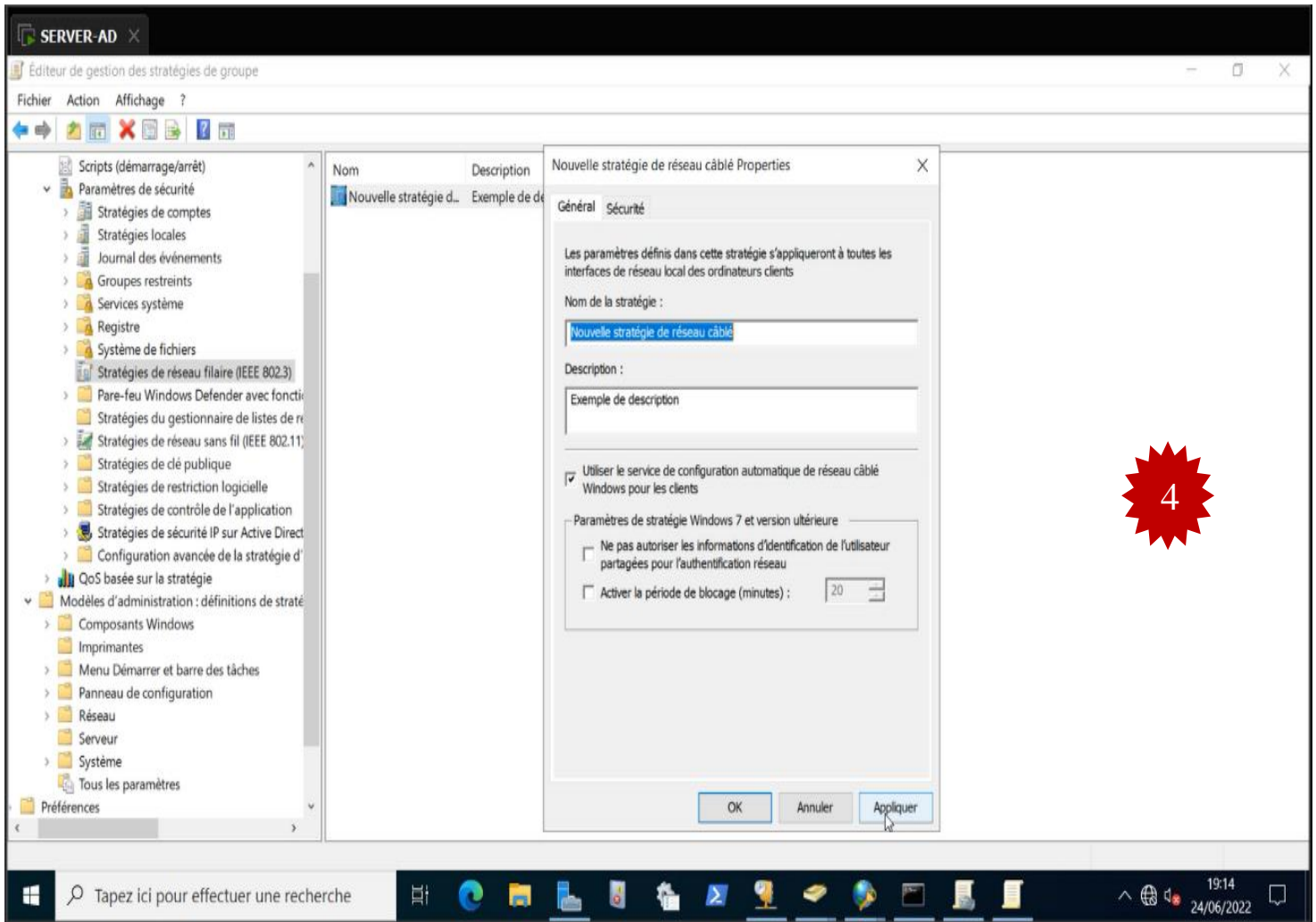
Mettre en mémoire cache les informations utilisateur pour les futures connexions à ce réseau

Avancé...

Tapez ici pour effectuer une recherche

19:14 24/06/2022





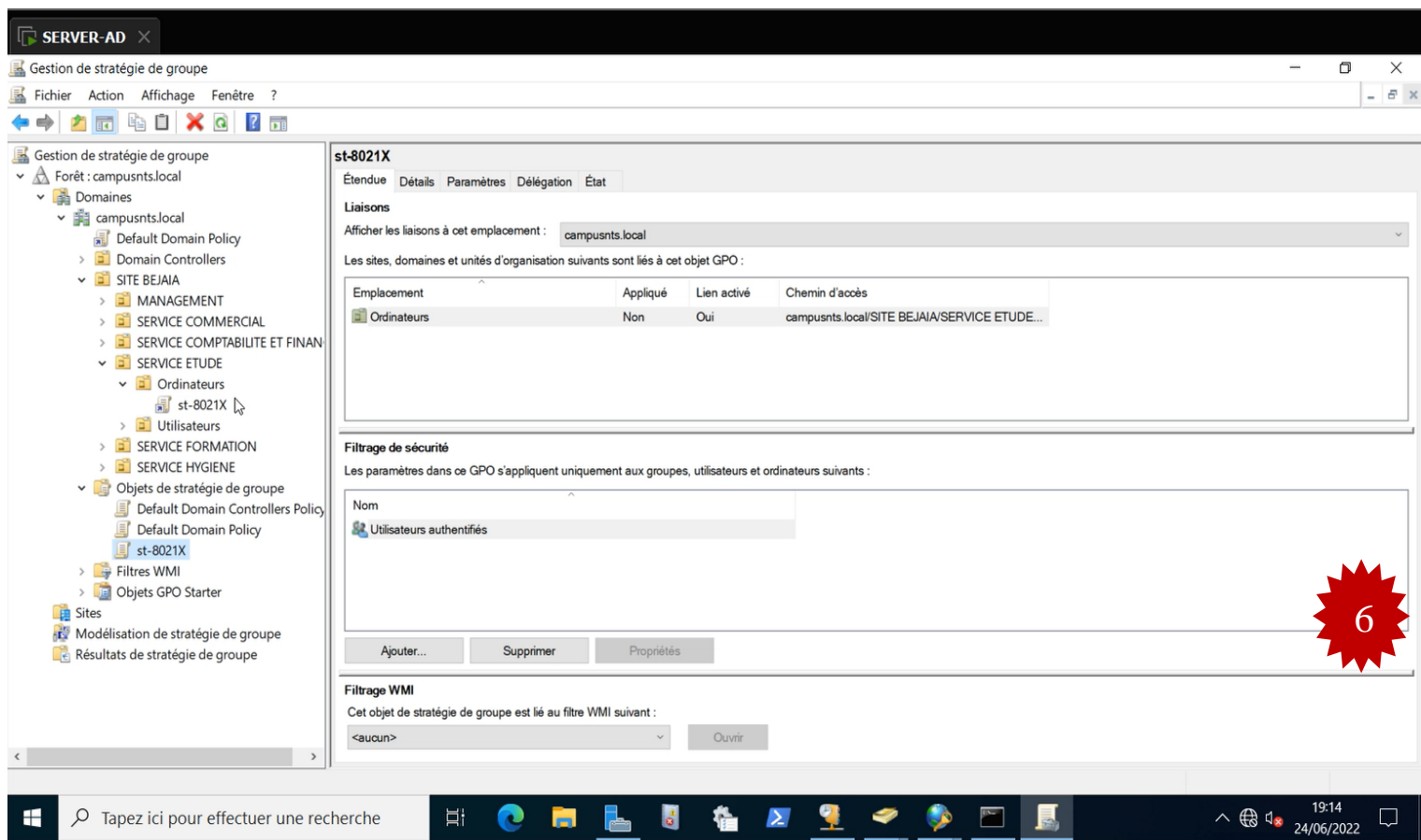


FIGURE IV.10 – Stratégie radius configurée pour les utilisateurs.

Pour forcer la mise à jour de la stratégie appliquée sur les utilisateurs, on doit saisir la commande **gpupdate** sur invité de commande coté serveur et redémarrer les stations de travail.



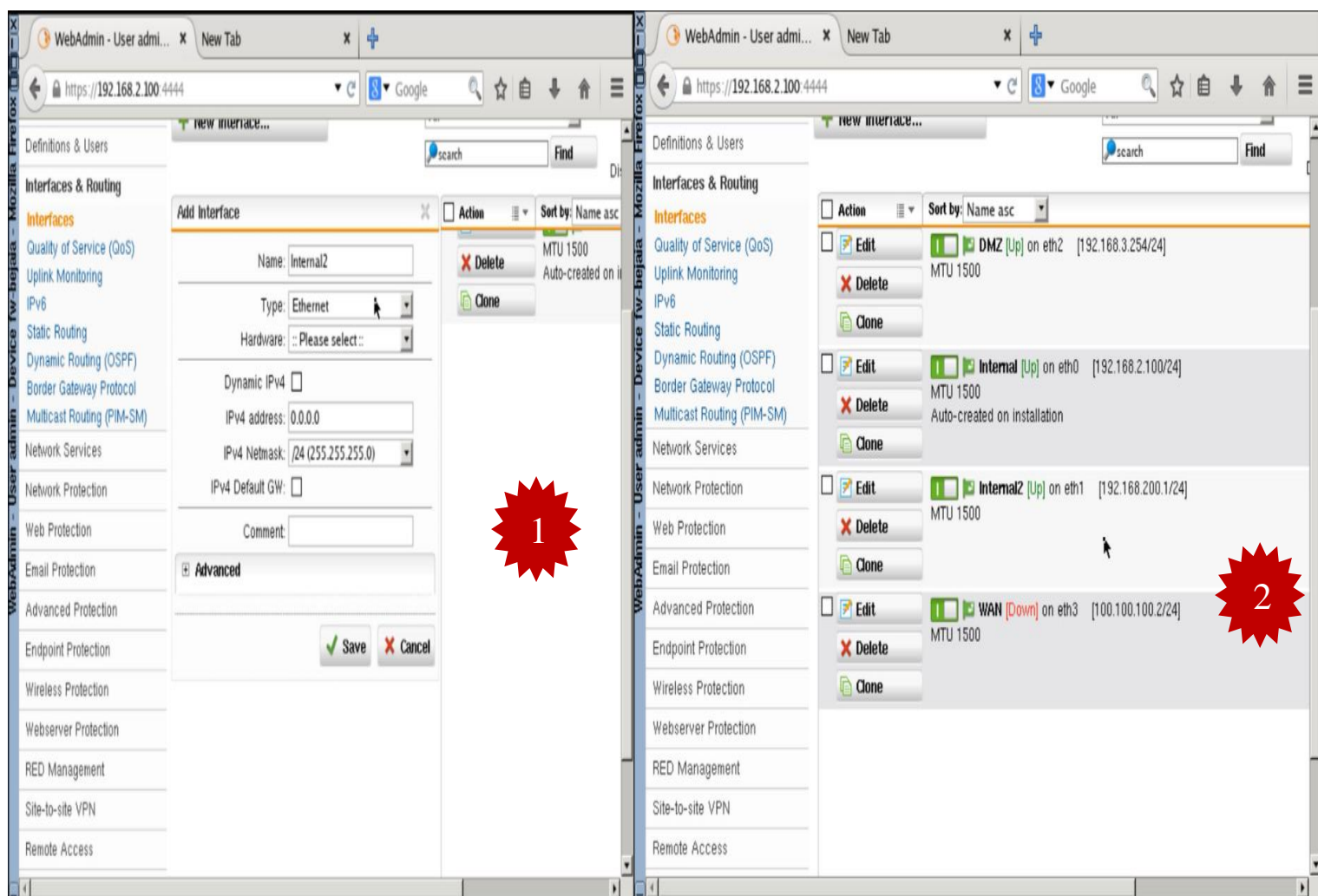
FIGURE IV.11 – Mise à jour des stratégies GPO.

IV.7 Configuration du Sophos UTM

IV.7.1 Création des interfaces « DMZ, LAN1, LAN2, Internet »

Afin que le site Bejaia puisse communiquer avec l'extérieur Alger, on doit créer quatre interfaces une externe et deux pour le réseau interne, la dernière pour la DMZ. et pour le pare-feu d'Alger, deux interfaces une pour le réseau interne et l'autre pour le réseau externe. Pour la communication réussie entre les deux sites, il faut suivre les étapes suivantes :

- Aller à interfaces and routages.
- Interfaces.
- Nouvelle interface.
- Entrer les informations correspondantes comme nom de l'interface, l'adresse IP ...



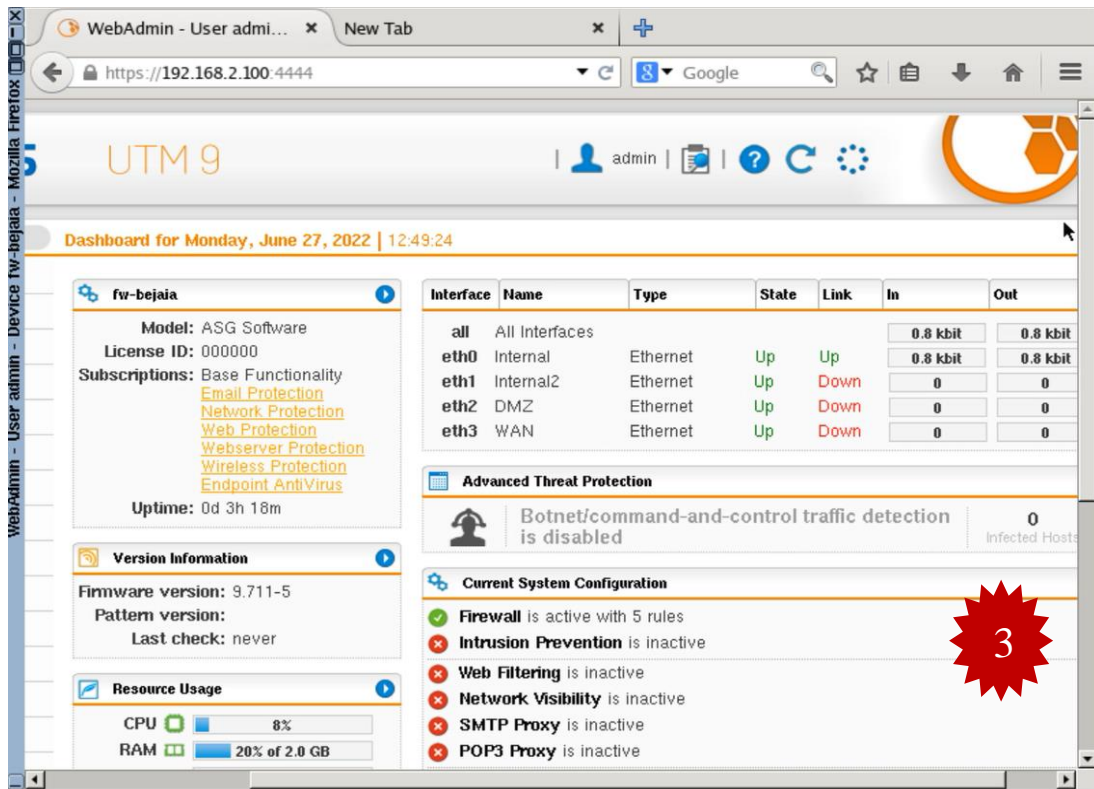


FIGURE IV.12 – Les interfaces de Sophos UTM.

IV.7.2 Routage statique

Le routage statique est une technologie de routage réseau. Il s'agit de la configuration manuelle et de la sélection des itinéraires réseaux, généralement gérés par l'administrateur réseau. Dans le cas suivant, on va router tout le trafic entrant venant de l'extérieur afin de les bénéficier d'une connexion internet et de les reconnaître par la suite à la création de notre tunnel VPN site to site.

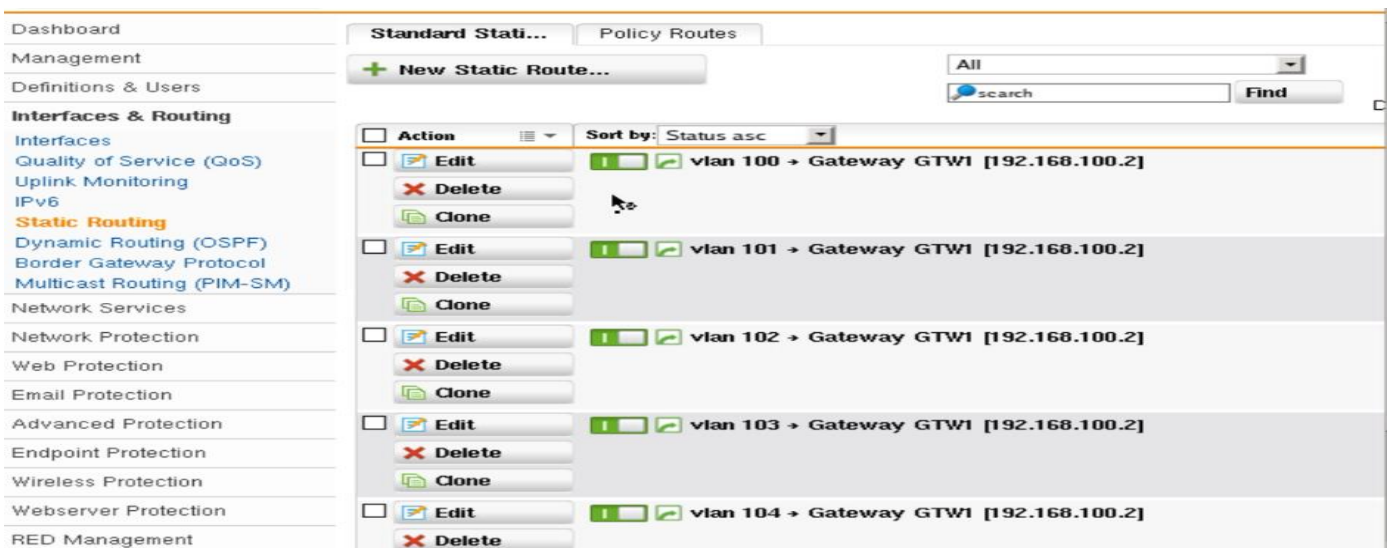


FIGURE IV.13 – Le routage statique.

IV.7.3 Filtrage sur pare-feu

Pour assurer la protection de notre entreprise, on définit les politiques de sécurité en filtrant les flux de données circulant entre les différentes zones.

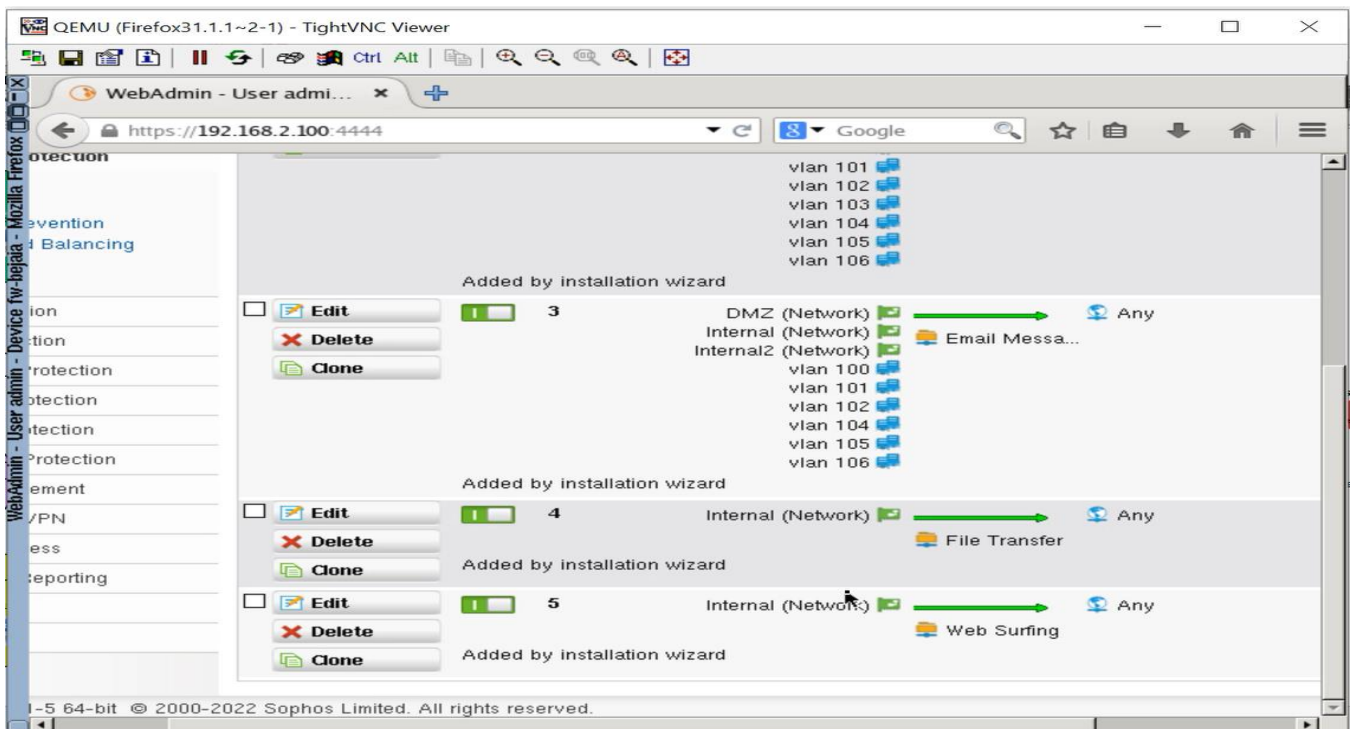
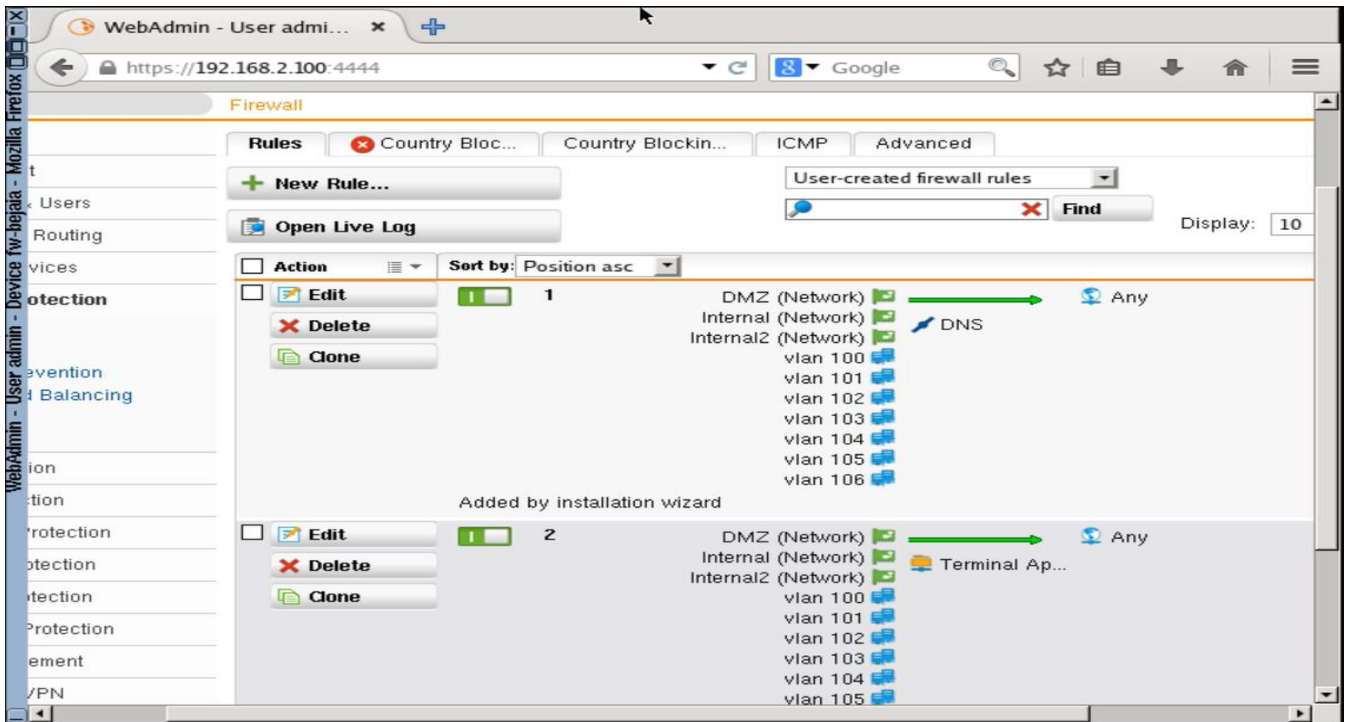


Figure IV.14 – filtrage sur le pare-feu.

IV.7.4 Le NAT

IV.7.4.1 Le NAT (Network Adresse Translation)

NAT est un processus de modification des adresses IP et des ports source et de destination. Généralement effectué par un routeur ou un pare-feu. Dans notre cas, on utilise le NAT pour les pare-feux Bejaïa, Alger :

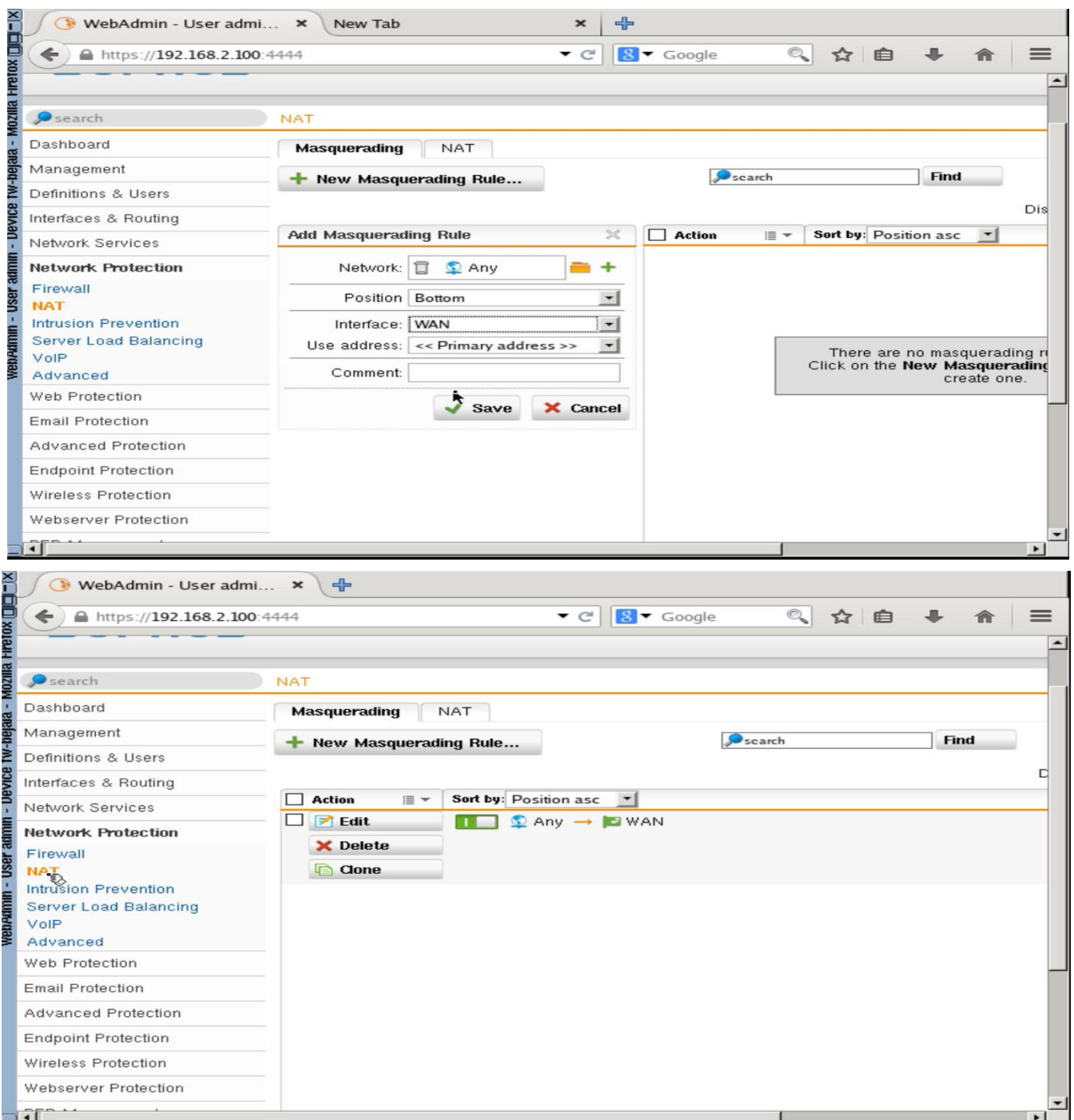


Figure IV.15 – Les règles de Nat sur Sophos Bejaia et Alger.

IV.7.5 VPN (Virtual Private Network)

Un réseau privé virtuel (VPN) est un réseau privé qui permet de créer un lien logique direct entre deux ou plusieurs machines distantes en utilisant un tunnel sécurisé à l'intérieur d'un réseau physique et public comme Internet.

IV.7.6 Configuration du VPN site à site IPSec

VPN site à site, c'est l'interconnexion de deux sites en utilisant un tunnel virtuelle chiffré qui se base sur les trois piliers de la sécurité confidentialité, intégrité et authentification en passant par une connexion internet. Pour ce faire, nous allons configurer deux phases, la phase une consiste à mettre l'échange des clés asymétrique par le protocole IKE, phase deux consiste à configurer la négociation du tunnel avec le protocole ESP qui utilise le protocole ISAKMP pour cette dernière.

IV.7.7 Configuration du protocole IKE pour l'échange des clés

Pour créer la passerelle distante sur laquelle le site d'Alger va demander la connexion auprès du site de Bejaia. D'abord, il faut aller au VPN site to site IPSec > Passerelles distantes > nouvelle passerelle VPN, ensuite on va remplir les informations nécessaires le nom de la passerelle et son type, la clé partagée sur le tunnel entre les deux sites, type id vpn et on sélectionne le réseau distant qu'on veut atteindre.

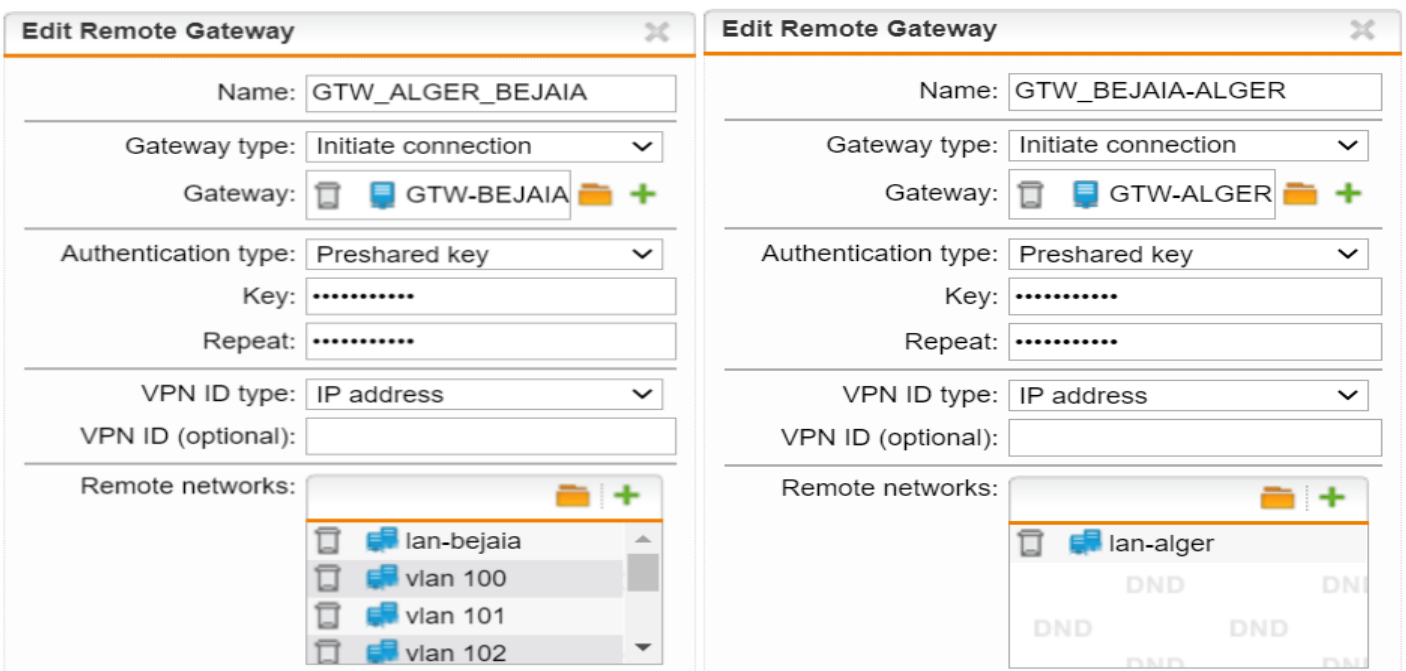


FIGURE IV.16 – Les passerelles distance de VPN.

IV.7.8 Création de connexion IPSec

Pour créer la connexion IPSec, on va aller au VPN site à site → IPSec → Connexions → Nouvelle connexion IPSec d'où on va sélectionner la passerelle distante qu'on vient de créer, l'interface local WAN dont laquelle on va sortir sur ce tunnel et on va sélectionner le réseau LAN local.

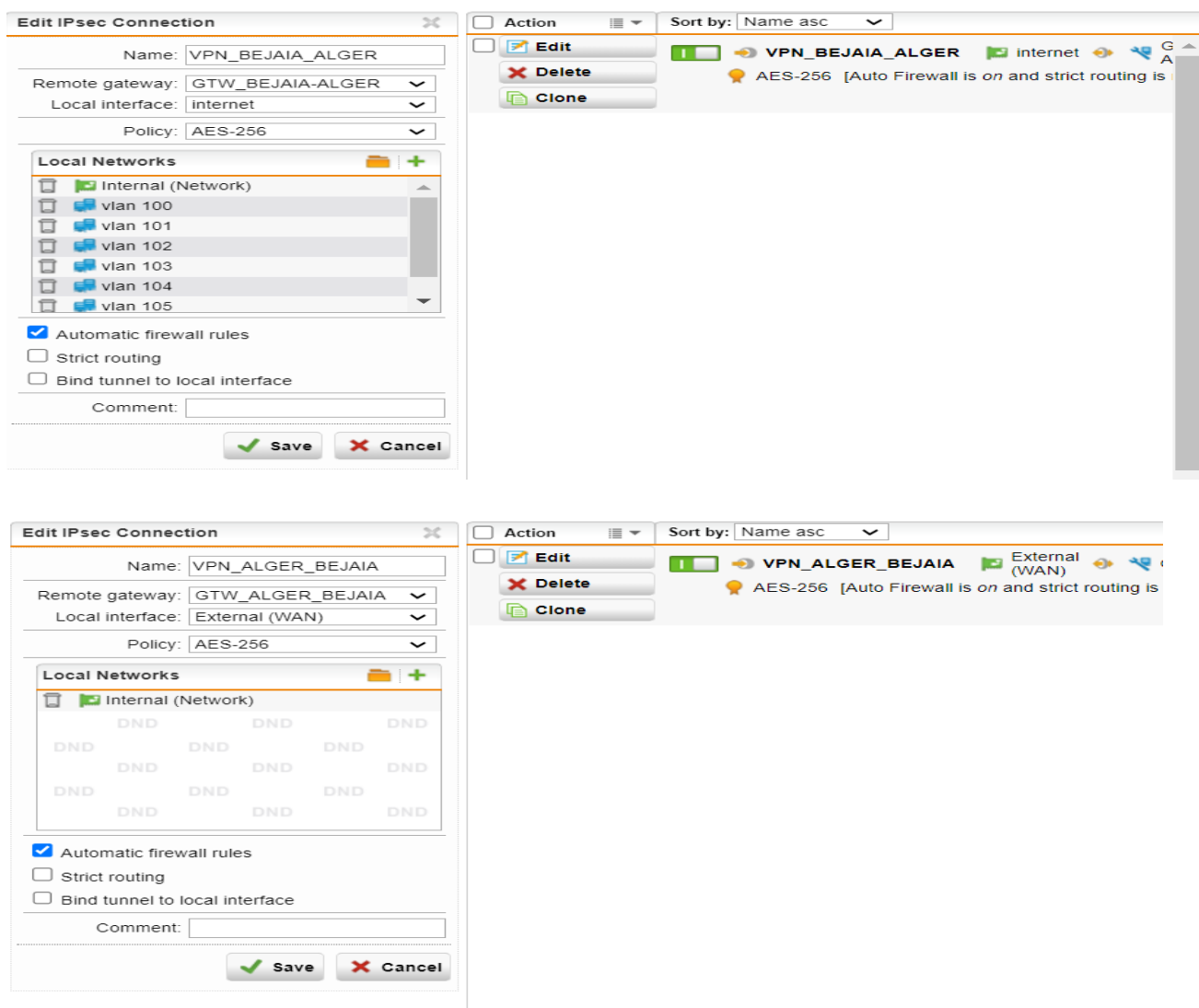


FIGURE IV.17 – La connexion IPSec « ESP ».

Pour la vérification aller à VPN site à site → État du tunnel. Il doit être on vert.

- Vert : le tunnel a été créé.
- Rouge : le tunnel n'a pas été créé.



FIGURE IV.18 – Connexion établi entre les deux sites bejaia et alger.

IV.7.9 Configuration du VPN client à site :

Le client d'accès VPN SSL est un logiciel qui permet aux utilisateurs ambulants aux ressources locales depuis n'importe où, Pour le configurer, on va aller à Accès à distance SSL → Profils → Nouveau → profil d'accès distant. On va entrer le nom du profil puis on va choisir les utilisateurs ou les groupes qui vont utiliser ce profil ensuite, on sélectionne le réseau que ce profil doit avoir accès.

Users/Groups (CTRL+V) Open Live Log Display: 10 1-1 of 1

All

- admin
- djedjiga
- massyllia
- SuperAdmins

Edit Remote Access Profile

Profile name: VPN_SERVEUR_BEJAIA

Users and Groups

- admin
- djedjiga
- massyllia

Local Networks

- Internal (Network)
- vlan 105

Automatic firewall rules

Comment:

Action

Sort by: Name asc

VPN_SERVEUR_BEJAIA Auto Firewall is on.

Networks (CTRL+Z) SSL

All

- internet (Address)
- internet (Broadcast)
- internet (Network)
- Internet IPv4
- Internet IPv6
- lan-alger
- massyllia (User Network)
- NTP Server Pool
- Sophos LiveConnect
- SuperAdmins (User Group)
- vlan 100
- vlan 101
- vlan 102
- vlan 103
- vlan 104
- vlan 105
- vlan 106
- VPN Pool (Cisco)
- VPN Pool (IPsec)
- VPN Pool (L2TP)
- VPN Pool (PPTP)
- VPN Pool (SSL)

Profiles Settings **Advanced**

Server Settings

Interface address: Any

Protocol: TCP

Port: 443

Override hostname: ssl.campusnts.com

Server settings saved successfully.

Virtual IP Pool

Pool network: VPN Pool (SSL)

Virtual IP addresses for peers are selected from this IP pool. It may be changed or replaced to resolve conflicts. For SSL site-to-site connections it is possible to assign a peer a static virtual IP address, which bypasses use of this pool.

Duplicate CN

Allow multiple concurrent connections per user

When enabled, duplicate common names are allowed in different SSL VPN sessions. This allows users to open multiple concurrent SSL VPN sessions from different hosts. Otherwise, only one SSL VPN session is allowed per user.

SOPHOS UTM 9 admin

Networks (CTRL+Z) SSL

All

- internet (Address)
- internet (Broadcast)
- internet (Network)
- Internet IPv4
- Internet IPv6
- lan-alger
- massyllia (User Network)
- NTP Server Pool
- Sophos LiveConnect
- SuperAdmins (User Group)
- vlan 100
- vlan 101
- vlan 102
- vlan 103
- vlan 104
- vlan 105
- vlan 106
- VPN Pool (Cisco)
- VPN Pool (IPsec)

Profiles Settings **Advanced**

Cryptographic Settings

Encryption algorithm: AES-128-CBC

Authentication algorithm: SHA1

Key size: 2048 bit

Server certificate: Local X509 Cert

Key lifetime: 28800 seconds

These setting control the cryptographic parameters for all SSL VPN connections.

Compression Settings

Compress SSL VPN traffic

When enabled, SSL VPN traffic will be transparently compressed and uncompressed.

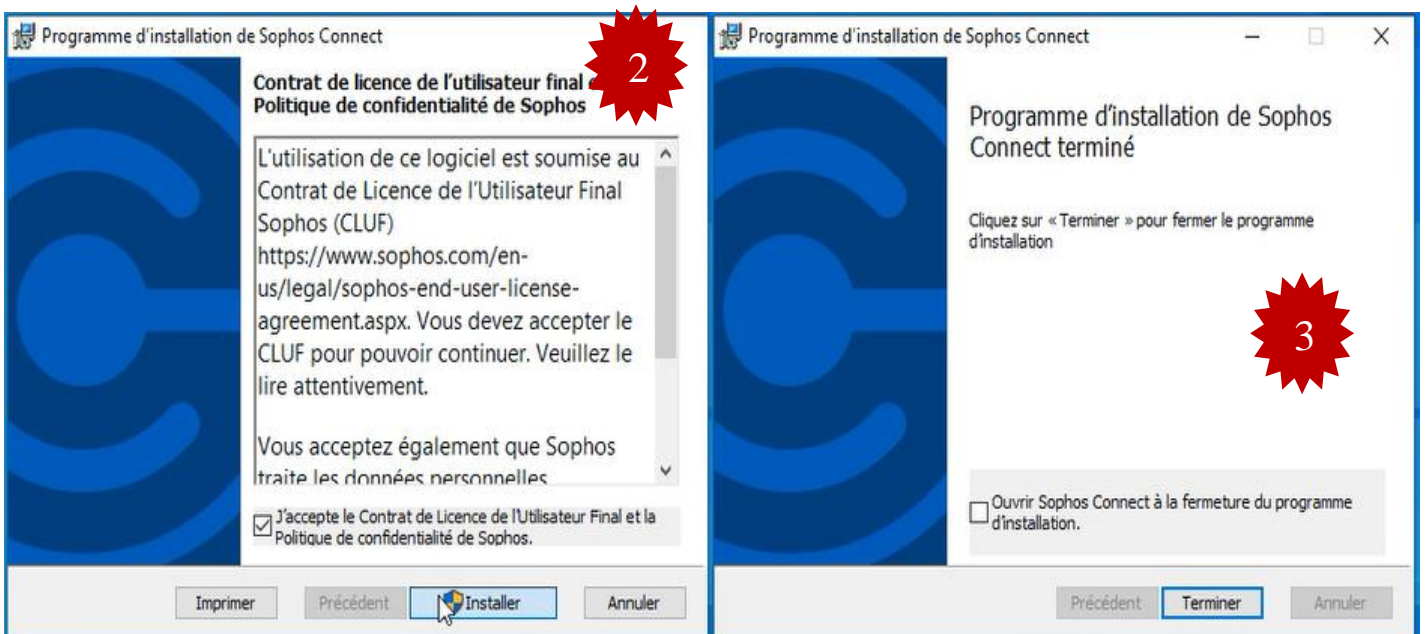
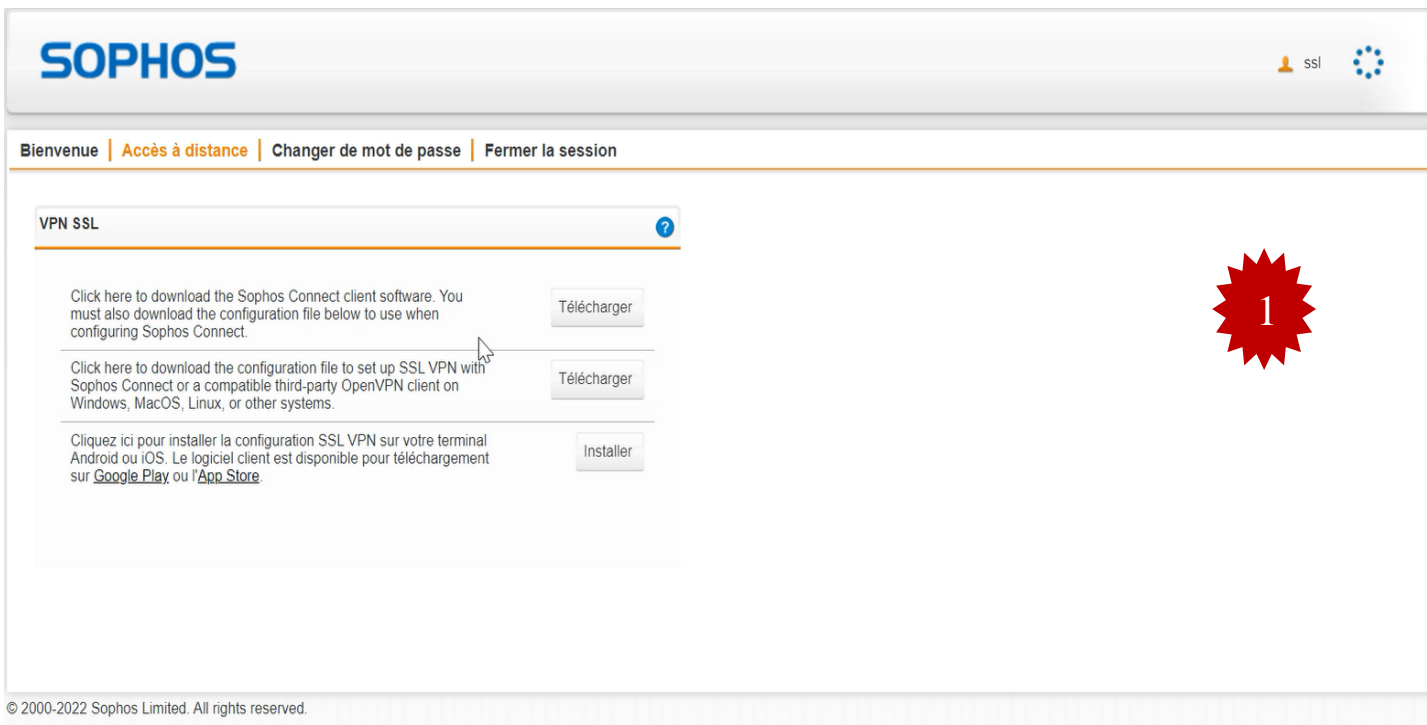
Debug Settings

Enable debug mode

When enabled, the SSL VPN log will contain additional debugging information.

FIGURE IV.19 – Configuration d'accès a distance SSL.

On va accéder au portail utilisateur, on clique sur onglet Accès à distance, un menu VPN SSL s'affiche puis on doit télécharger le package d'installation complet comprenant le logiciel client, les clés et la configuration automatique pour Windows 10. Une fois l'installation du package est faite on reçoit un message qui va nous permettre d'installer la carte réseau dédiée pour la convention vpn. Donc on va sur panneau de configuration → réseau et internet → Centre réseau et partage → Modifier les paramètres de la carte. On remarque la présence d'une seule carte réseau et un fois la configuration installée, on remarque qu'une nouvelle carte réseau virtuelle vient d'être créé.



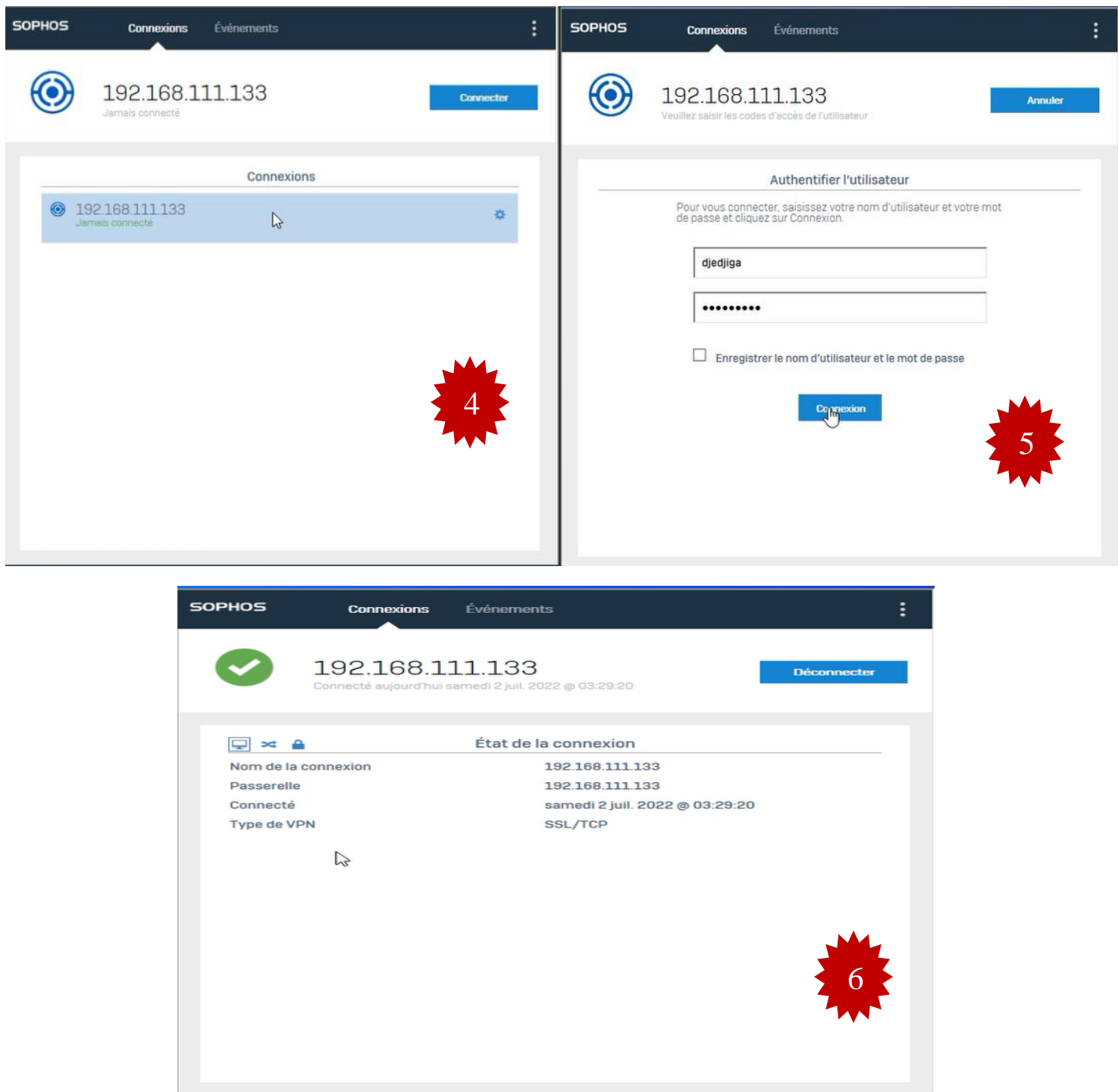


FIGURE IV.20 – Configuration d'accès à distance SSL.

IV.8 Configuration des équipements

Dans ce qui suit, nous allons présenter la configuration en générale des équipements qui vont nous permettre de mettre en place la nouvelle architecture proposée.

IV.8.1 Configuration des commutateurs

Nous commençons par la configuration des commutateurs qui permettent l'interconnexion des différents réseaux hétérogènes.

IV.8.2 Configuration des interfaces trunk

Un trunk est une liaison d'agrégation de VLANs. C'est une connexion physique sur lequel on transmet le trafic de plusieurs VLANs. Pour configurer les interfaces trunk entre deux switches, on suit les étapes suivantes.

Vu le nombre d'interface à configurer, on utilisera la même configuration.

```
DIS1(config)#interface Ethernet0/0
DIS1(config-if)# switchport trunk encapsulation dot1q
DIS1(config-if)# switchport mode trunk
DIS1(config-if)#exit
```

FIGURE IV.21 – Configuration trunk sur le switch distribution DIS1.

```
S-acces1(config)#interface Ethernet0/1
S-acces1(config-if)# switchport mode trunk
S-acces1(config-if)#exit
```

FIGURE IV.22 – Configuration trunk sur le switch d'accès S-acces1.

IV.8.3 Configuration d'un domaine VTP

VTP permet d'ajouter, de renommer ou de supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau. On a configuré le VTP server sur les switches distribution et le VTP client sur les switches Access.

```
DIS1(config)#vtp password campus1234
DIS1(config)#vtp mode server
Device mode already VTP Server for VLANs.
DIS1(config)#vtp domain campus.vtp
Domain name already set to campus.vtp.
DIS1(config)#vtp password campus1234
Password already set to campus1234
DIS1(config)#vtp version 2
VTP version is already in V2.
DIS1(config)#vtp pruning
Pruning already switched on
```

FIGURE IV.23 – Configuration VTP serveur sur le switch distribution DIS1.

```
S-acces1(config)#vtp mode client
Device mode already VTP Client for VLANS.
S-acces1(config)#vtp password campus1234
Password already set to campus1234
S-acces1(config)#vtp domain campus.vtp
Domain name already set to campus.vtp.
S-acces1(config)#vtp version 2
```

FIGURE IV.24 – Configuration VTP client sur le switch d'accès S-acces1.

IV.8.4 Création des VLANs

La création des VLANs permet de regrouper d'une part les périphériques et d'autre part les utilisateurs et de gérer individuellement les droites et priorités d'accès des utilisateurs. Dans notre cas, on a créé huit VLANs, chacun est associé à son service de plus on a créé le VLAN voice, le VLAN native et VLAN management.

```
DIS1(config-vlan)#vlan 100
DIS1(config-vlan)#name SC
DIS1(config-vlan)#vlan 101
DIS1(config-vlan)#name SCF
DIS1(config-vlan)#vlan 102
DIS1(config-vlan)#name FH
DIS1(config-vlan)#vlan 103
DIS1(config-vlan)#name SF
DIS1(config-vlan)#vlan 104
DIS1(config-vlan)#name SERP
DIS1(config-vlan)#vlan 105
DIS1(config-vlan)#name management
DIS1(config-vlan)#
DIS1(config-vlan)#vlan 106
DIS1(config-vlan)#
DIS1(config-vlan)#name voice
DIS1(config-vlan)#vlan 999
DIS1(config-vlan)#name native
DIS1(config-vlan)#
```

```
S-acces1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et1/1, Et1/2, Et1/3, Et2/0 Et2/1, Et2/2, Et2/3, Et3/0 Et3/1, Et3/2, Et3/3
100	SC	active	Et0/0, Et0/3, Et1/0
101	SCF	active	
102	FH	active	
103	SF	active	
104	SERP	active	
105	management	active	
106	voice	active	Et0/0, Et0/3, Et1/0
999	native	active	
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

FIGURE IV.25 – Création des VLANs sur le switch et vérification.

IV.8.5 Configuration des interfaces au mode d'accès vlan

Passons maintenant à la configuration des interfaces Access qui veut dire qu'elle recevra que les paquets qui lui sont destinés. On utilisera la même configuration pour les autres interfaces Access.

```
S-access3(config)#interface Ethernet1/0
S-access3(config-if)# switchport access vlan 102
S-access3(config-if)# switchport mode access
S-access3(config-if)# switchport voice vlan 106
S-access3(config-if)#exit
S-acces1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et1/1, Et1/2, Et1/3, Et2/0 Et2/1, Et2/2, Et2/3, Et3/0 Et3/1, Et3/2, Et3/3
100	SC	active	Et0/0, Et0/3, Et1/0
101	SCF	active	
102	FH	active	
103	SF	active	
104	SERP	active	
105	management	active	
106	voice	active	Et0/0, Et0/3, Et1/0
999	native	active	
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

FIGURE IV.26 – Configuration Access sur le switch Accesset vérification.

IV.8.6 Configuration VLAN natif

Toutes les trames passant par un “Trunks” sont ainsi étiquetées sauf les trames appartenant au VLAN natif. Donc, les trames du VLAN natif, par défaut le VLAN 1, ne sont pas étiquetées. Donc on a changé la valeur du VLAN natif de 1 à 999 et on a forcé le tagging sucre VLAN. Pour ne pas véhiculer des trames de protocoles comme CDP, DTP dans le même VLAN et d’éviter qu’un utilisateur ne puisse capturer ce trafic ou de gérer des faux messages CDP, DTP afin de détourner le fonctionnement du réseau, on a fait la même configuration pour tous les switches.

```
DIS2(config)#interface Ethernet0/0
DIS2(config-if)# switchport trunk allowed vlan 100-102,104-106,203,999
DIS2(config-if)# switchport trunk native vlan 999
S-access2(config)#interface Ethernet0/0
S-access2(config-if)# switchport trunk native vlan 999
S-access2(config-if)# switchport trunk allowed vlan 100-106,999
S-access2(config-if)#exit
DIS2#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/0	on	802.1q	trunking	999
Et0/1	on	802.1q	trunking	999
Et0/2	on	802.1q	trunking	999

FIGURE IV.27 – Sécurisation du VLAN natif sur switch distributions et switch d’accès et vérification.

IV.8.7 Configuration du protocole LACP « l’agrégation des lien 802.3ad

»

Pour configurer un port channel sur notre switch nous devons assigner toutes les interfaces qui vont composer notre lien logique dans le même channel-group. On a créé quatre liens logiques entre les deux switches de distribution et on a configuré EtherChannel en mode active sur le switch distribution 1 et en mode passive sur le switch distribution 2.

```
DIS2(config)#interface range ethernet 3/0-3
DIS2(config-if-range)#channel-group 1 mode active
DIS2(config-if-range)#exit
```



```

DIS2#show etherchannel summary
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       N - not in use, no aggregation
       f - failed to allocate aggregator

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

       A - formed by Auto LAG

```

```

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

```

Group	Port-channel	Protocol	Ports
1	Po1(SU)	LACP	Et3/0(P) Et3/1(P) Et3/2(P) Et3/3(P)

FIGURE IV.28– Configuration du protocole LACP et vérification.

IV.8.8 Configuration du protocole SSH « Secure Shell »

En général, il y a le choix entre l'administration web sécurisée ou pas (protocole http ou https) et/ou l'administration en ligne de commande sécurisée ou pas (telnet ou ssh). L'administration du switch en utilisant une interface web peut être pratique. Mais nous choisirons en priorité l'administration du switch en utilisant la ligne de commande pour les raisons suivantes :

- En cas de coupure réseau, il nous faudra intervenir directement sur le switch, donc autant être habitué à travailler en ligne de commande,
- L'interface web peut être moins stable que l'interface en ligne de commande (CLI),
- Les configurations avancées sont souvent disponibles uniquement au travers de la ligne de commande.

IV.8.9 Vérification de la prise en compte du protocole ssh par l'IOS

Tout d'abord, il faut vérifier que l'IOS du switch supporte ssh. La mention k9 (crypto) doit figurer dans le nom de l'IOS. La commande pour vérifier la version de l'IOS est :

```

core2#show version
Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.5(2)T, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 26-Mar-15 07:36 by prod_rel_team

```

FIGURE IV.29 – Vérification de la version system Ios cisco.

Après avoir assuré qu'on peut configurer ssh sur notre équipement on passe maintenant aux étapes de configuration :

- Configuration du nom d'hôte et du nom de domaine.
- Création de la clé.
 - Les évènements associés aux connexions ssh sont enregistrés dans les logs.
 - Un timeout de 60 secondes est ajouté en cas d'inactivité durant l'authentification.
 - Nous laissons trois essais pour la connexion au switch. Suite à ces essais, la connexion est fermée.
- Création d'un utilisateur local pour l'authentification.

```
core2(config)#ip domain-name campus.ssh
core2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: core2.campus.ssh

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

core2(config)#
*Jul  4 02:41:19.962: %SSH-5-ENABLED: SSH 1.99 has been enabled
core2(config)#ip ssh version 2
core2(config)#ip ssh logging events
core2(config)#ip ssh time-out 60
core2(config)#ip ssh authentication-retries 3
core2(config)#line vty 0 4
core2(config-line)#login local
core2(config-line)#transport input ssh
core2(config-line)#exit
core2(config)#username massylia.djedjiga password campus1234 privilege 15
```

FIGURE IV.30 – Configuration du protocole SSH sur le router core 2.

IV.8.9.1 Port Security

On a sécurisé tous les ports access car la sécurité se fait sur les ports qui font face à des clients et afin de limiter le nombre d'adresse MAC derrière un port et de se protéger du MAC Address Flooding qui consiste à envoyer des milliers de messages en indiquant à chaque fois une adresse MAC source différente. Tout d'abord, le port doit être en mode Access ensuite, activer la sécurité de port et limiter le nombre d'adresse MAC par port. Pour la gestion d'adresse mac, on a appliqué le mode sticky pour que le switch apprend automatiquement les adresses et les enregistrer. En cas ou il y a une violation sur le port, on a appliqué le mode shutdown pour que le port se désactivé automatiquement. On utilisera la même configuration pour les autres ports Access.

```

S-acces1(config)#interface ethernet 0/3
S-acces1(config-if)#switchport port-security mac-address sticky
S-acces1(config-if)#switchport port-security maximum 1
S-acces1(config-if)#switchport port-security violation shutdown
S-acces1(config-if)#exit

```

FIGURE IV.31 – Configuration des port security sur le switch access SWA1.

IV.8.9.2 Configuration du client Radius

On a configuré radius sur le client switch DIS2 afin d'authentifier les utilisateurs sur ce switch. D'abord, on a créé un nouveau model AAA après, on a créé l'ensemble AAA authentication et l'ensemble AAA authorization. A la fin, on a utilisé une clé partagée telecom1234 avec le serveur. Pour ce faire nous avons suivi les étapes suivantes :

- Activation du AAA sur les switches.
- Configuration de la communication entre le Switch Cisco et le serveur RADIUS.
- Activation du protocole 802.1X sur le switch.
- Configuration du 802.1x sur les interfaces des clients.

```

DIS2(config)#aaa new-model
DIS2(config)#aaa authentication dot1x default group radius
DIS2(config)#aaa authorization network default group radius
DIS2(config)#Radius server WIN2022
DIS2(config-radius-server)#address ipv4 10.0.105.100
DIS2(config-radius-server)#key telecom1234
DIS2(config-radius-server)#exit
DIS2(config)#aaa new-model
DIS2(config)#aaa authentication dot1x default group radius
DIS2(config)#aaa authorization network default group radius
DIS2(config)#Radius server WIN2022
DIS2(config-radius-server)#address ipv4 10.0.105.100
DIS2(config-radius-server)#key telecom1234
DIS2(config-radius-server)#exit
DIS2(config)#dot1x system-auth-control
DIS2(config)#in
DIS2(config)#interface eth
DIS2(config)#interface ethernet 0/2
DIS2(config-if)#authentication port-control auto
DIS2(config-if)#authentication open
DIS2(config-if)#dot1x pae authenticator
DIS2(config-if)#authentication host-mode multi-domain
DIS2(config-if)#EXIT

```

FIGURE IV.32 – Configuration du client Radius sur le switch DIS2.

IV.8.10 Configuration des VLANs privées pour notre réseau DMZ

Les VLANs privés est une technologie de segmentation de réseau pour les réseaux de couche 2 qui permet l'isolation des ports ou la segmentation du trafic sous le même segment IP. Un Vlan consiste en une association de VLAN :

1. Vlan primaire : fait référence au VLAN d'origine qui est utilisé pour envoyer des trames de liaison descendante à tous les sous-VLAN (VLAN secondaire).

2. Vlan secondaire :

- **Isolé :** les ports d'un même VLAN isolé ne peuvent pas communiquer entre eux.
- **Communauté :** les ports du même VLAN de communauté peuvent communiquer entre eux et avec le VLAN principal. Ils ne peuvent pas communiquer avec d'autres VLAN secondaires.
- Pour configurer ses derniers on suit les étapes suivantes :

Etape 1 : Configuration VTP mode transparent

```
SW-DMZ(config)#vtp mode transparent
Device mode already VTP Transparent for VLANs.
```

FIGURE IV.33 – Configuration du mode VTP transparent sur le Switch DMZ et vérification.

Etape 2 : Création des PVLANS Community

```
SW-DMZ(config)#vlan 201
SW-DMZ(config-vlan)#pri
SW-DMZ(config-vlan)#private-vlan co
SW-DMZ(config-vlan)#private-vlan community
SW-DMZ(config-vlan)#exit
```

FIGURE IV.34 – Création des PVLANS Community sur le Switch DMZ.

Etape 3 : Création des PVLANS Isolated

```
SW-DMZ(config)#vlan 202
SW-DMZ(config-vlan)#pri
SW-DMZ(config-vlan)#private-vlan i
SW-DMZ(config-vlan)#private-vlan isolated
SW-DMZ(config-vlan)#exit
SW-DMZ(config)#
```

FIGURE IV.35 – Création des PVLANS Isolated sur le Switch DMZ.

Etape 4 : Création des PVLANS Primary

```
SW-DMZ(config)#vlan 200
SW-DMZ(config-vlan)#private-vlan primary
SW-DMZ(config-vlan)#private-vlan association 201,202
SW-DMZ(config-vlan)#exit
```

FIGURE IV.36 – Création des PVLANS primary sur le Switch DMZ.

Etape 5 : Affectation des ports aux PVLANS sur le Switch DMZ

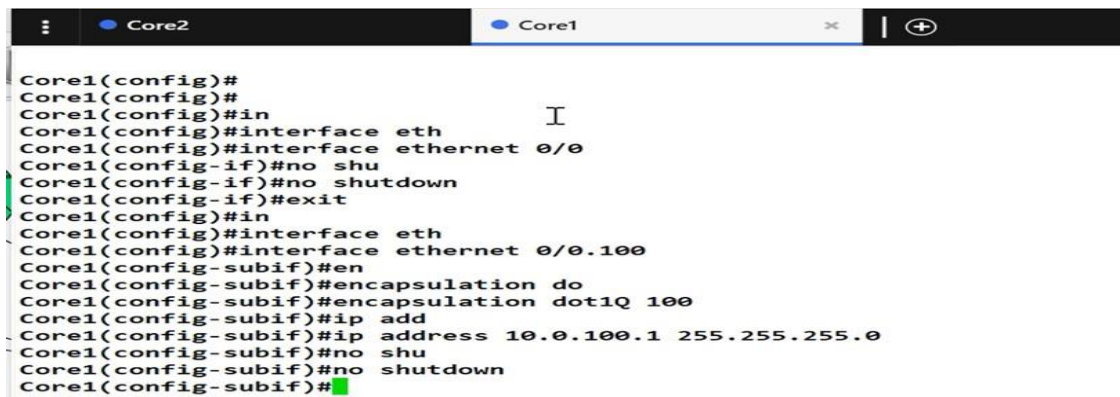
```
SW-DMZ(config)#interface range ethernet 0/2-3
SW-DMZ(config-if-range)#switchport mode private-vlan host
SW-DMZ(config-if-range)#switchport private-vlan host-association 200 201
SW-DMZ(config-if-range)#interface range ethernet 0/0-1
SW-DMZ(config-if-range)#switchport mode private-vlan host
SW-DMZ(config-if-range)#switchport private-vlan host-association 200 202
SW-DMZ(config)#interface ethernet 1/0
SW-DMZ(config-if)#switchport mode private-vlan promiscuous
SW-DMZ(config-if)#switchport private-vlan mapping 200 201,202
```

FIGURE IV.37 – Affectation des ports aux PVLANS sur le Switch DMZ.

IV.8.11 Configuration des routeurs

IV.8.11.1 Routage inter VLANs

Le routage inter VLAN permet le transfert du trafic réseau d'un vlan à l'autre à l'aide d'un périphérique de couche 3 comme le routeur. Nous allons configurer une des interfaces réseaux du routeur. Le principe est toujours le même pour chacune des interfaces réseau.



```
Core1(config)#
Core1(config)#
Core1(config)#in
Core1(config)#interface eth
Core1(config)#interface ethernet 0/0
Core1(config-if)#no shu
Core1(config-if)#no shutdown
Core1(config-if)#exit
Core1(config)#in
Core1(config)#interface eth
Core1(config)#interface ethernet 0/0.100
Core1(config-subif)#en
Core1(config-subif)#encapsulation do
Core1(config-subif)#encapsulation dot1Q 100
Core1(config-subif)#ip add
Core1(config-subif)#ip address 10.0.100.1 255.255.255.0
Core1(config-subif)#no shu
Core1(config-subif)#no shutdown
Core1(config-subif)#
```

FIGURE IV.38 – Configuration des interfaces sur le routeur1 et vérification.

IV.8.12 Configuration du Routage Passerelle Par Défaut

On a routé du réseau 0.0.0.0 vers n'importe quelle réseau 0.0.0.0 par la passerelle de sortie du routeur.

```
ip route 0.0.0.0 0.0.0.0 192.168.100.1
!
```

FIGURE IV.39 – Le routage sur le core 1.

```
core1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.100.1 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 192.168.100.1
     10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
C     10.0.100.0/24 is directly connected, Ethernet0/0.100
L     10.0.100.1/32 is directly connected, Ethernet0/0.100
C     10.0.101.0/24 is directly connected, Ethernet0/0.101
L     10.0.101.1/32 is directly connected, Ethernet0/0.101
C     10.0.102.0/24 is directly connected, Ethernet0/0.102
L     10.0.102.1/32 is directly connected, Ethernet0/0.102
C     10.0.103.0/24 is directly connected, Ethernet0/0.103
L     10.0.103.1/32 is directly connected, Ethernet0/0.103
C     10.0.104.0/24 is directly connected, Ethernet0/0.104
L     10.0.104.1/32 is directly connected, Ethernet0/0.104
C     10.0.105.0/24 is directly connected, Ethernet0/0.105
L     10.0.105.1/32 is directly connected, Ethernet0/0.105
C     10.0.106.0/24 is directly connected, Ethernet0/0.106
L     10.0.106.1/32 is directly connected, Ethernet0/0.106
     192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.100.0/24 is directly connected, Ethernet0/1
L     192.168.100.2/32 is directly connected, Ethernet0/1
```

FIGURE IV.40– Vérification de routage sur le core 1.

IV.8.13 Configuration du protocole HSRP

IV.8.13.1 Le Protocol HSRP (Hot Standby Routing Protocol)

HSRP est un protocole mis en œuvre dans les routeurs et les commutateurs pour garantir la disponibilité des passerelles par défaut dans un sous-réseau malgré les pannes de routeur.

```
core1(config)#interface Ethernet0/0.100
core1(config-subif)# encapsulation dot1Q 100
core1(config-subif)# ip address 10.0.100.1 255.255.255.0
core1(config-subif)# ip helper-address 10.0.105.100
core1(config-subif)# standby version 2
core1(config-subif)# standby 100 ip 10.0.100.254
core1(config-subif)# standby 100 priority 110
core1(config-subif)# standby 100 preempt
core1(config-subif)#interface Ethernet0/0.101
core1(config-subif)# encapsulation dot1Q 101
core1(config-subif)# ip address 10.0.101.1 255.255.255.0
core1(config-subif)# ip helper-address 10.0.105.100
core1(config-subif)# standby version 2
core1(config-subif)# standby 101 ip 10.0.101.254
core1(config-subif)# standby 101 priority 110
core1(config-subif)# standby 101 preempt
core1(config-subif)#interface Ethernet0/0.102
core1(config-subif)# encapsulation dot1Q 102
core1(config-subif)# ip address 10.0.102.1 255.255.255.0
core1(config-subif)# ip helper-address 10.0.105.100
core1(config-subif)# standby version 2
core1(config-subif)# standby 102 ip 10.0.102.254
core1(config-subif)# standby 102 priority 110
core1(config-subif)# standby 102 preempt

core1#show standby brief
                P indicates configured to preempt.
                |
Interface   Grp  Pri  P State   Active        Standby        Virtual IP
Et0/0.100   100  110  P Active local        10.0.100.2     10.0.100.254
Et0/0.101   101  110  P Active local        10.0.101.2     10.0.101.254
Et0/0.102   102  110  P Active local        10.0.102.2     10.0.102.254
Et0/0.103   103  110  P Active local        10.0.103.2     10.0.103.254
Et0/0.104   104  110  P Active local        10.0.104.2     10.0.104.254
Et0/0.105   105  110  P Active local        10.0.105.2     10.0.105.254
Et0/0.106   106  110  P Active local        10.0.106.2     10.0.106.254
```

FIGURE IV.41 – Configuration de HSRP sur le routeur1 et vérification.

```

core2(config-subif)#interface Ethernet0/0.100
core2(config-subif)# encapsulation dot1Q 100
core2(config-subif)# ip address 10.0.100.2 255.255.255.0
core2(config-subif)# ip helper-address 10.0.105.100
core2(config-subif)# standby version 2
core2(config-subif)# standby 100 ip 10.0.100.254
core2(config-subif)#interface Ethernet0/0.101
core2(config-subif)# encapsulation dot1Q 101
core2(config-subif)# ip address 10.0.101.2 255.255.255.0
core2(config-subif)# ip helper-address 10.0.105.100
core2(config-subif)# standby version 2
core2(config-subif)# standby 101 ip 10.0.101.254
core2(config-subif)#interface Ethernet0/0.102
core2(config-subif)# encapsulation dot1Q 102
core2(config-subif)# ip address 10.0.102.2 255.255.255.0
core2(config-subif)# ip helper-address 10.0.105.100
core2(config-subif)# standby version 2
core2(config-subif)# standby 102 ip 10.0.102.254
core2(config-subif)#do show standby brief
                P indicates configured to preempt.
                |
Interface      Grp  Pri P State   Active        Standby        Virtual IP
Et0/0.100     100 100   | Standby 10.0.100.1    local          10.0.100.254
Et0/0.101     101 100   | Standby 10.0.101.1    local          10.0.101.254
Et0/0.102     102 100   | Standby 10.0.102.1    local          10.0.102.254
Et0/0.103     103 100   | Standby 10.0.103.1    local          10.0.103.254
Et0/0.104     104 100   | Standby 10.0.104.1    local          10.0.104.254
Et0/0.105     105 100   | Standby 10.0.105.1    local          10.0.105.254
Et0/0.106     106 100   | Standby 10.0.106.1    local          10.0.106.254

```

FIGURE IV.42– Configuration de HSRP sur le routeur 2 et vérification.

IV.9 Tests

Nous allons finaliser notre travail par des tests aux configurations déjà faites et qui sont présentées dans la partie configuration pour s’assurer que le réseau est bien sécurisé.

IV.9.1 Test DHCP et Active Directory

IV.9.1.1 Test DHCP

On va tester notre client dhcpn et nous allons sur la carte réseau d’un client vlan 104 en tapons la commande `nca.cpl` et la commande `ipconfig` pour afficher l’adresse ip de notre carte sur l’invité de commande comme suit :


```
DIS1 DIS2 PC1 PC9
Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

PC9> ip dhcp
DORA IP 10.0.100.12/24 GW 10.0.100.254

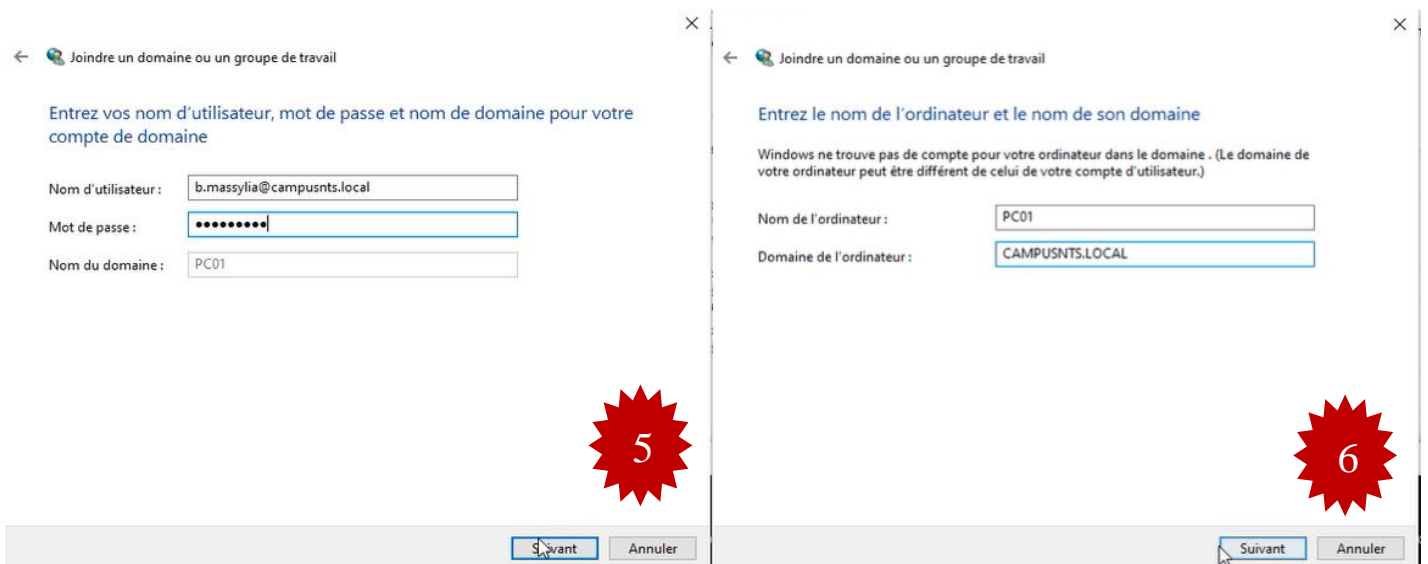
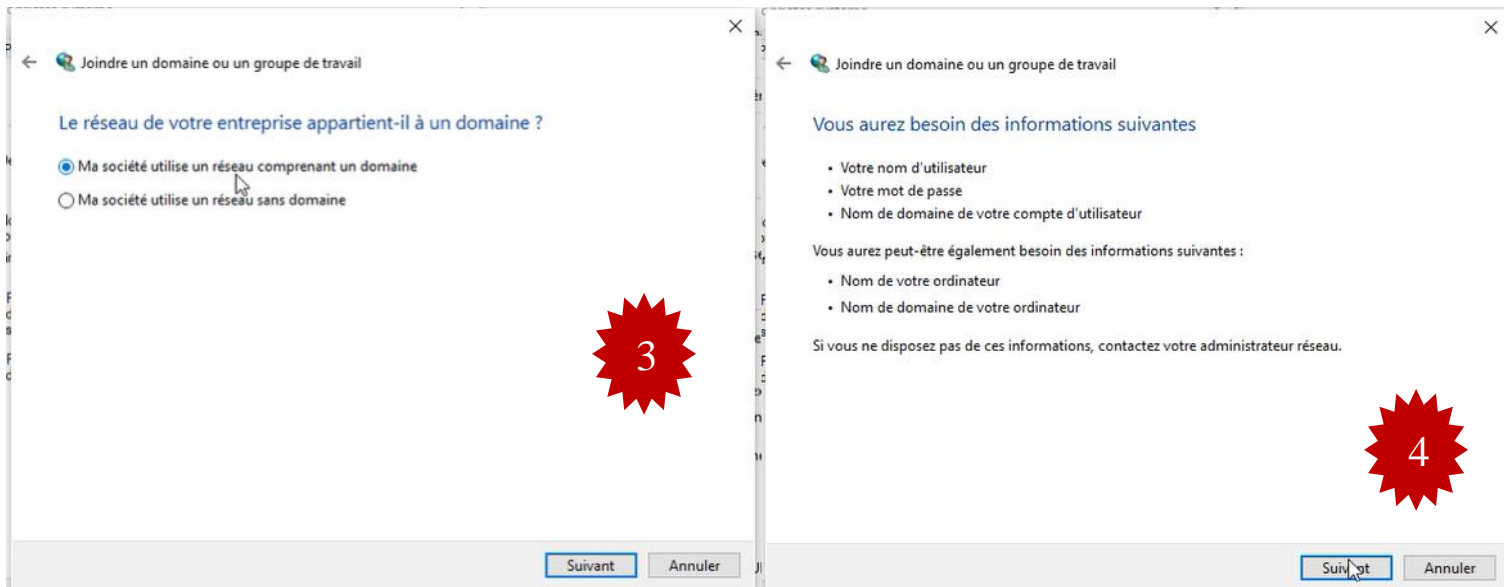
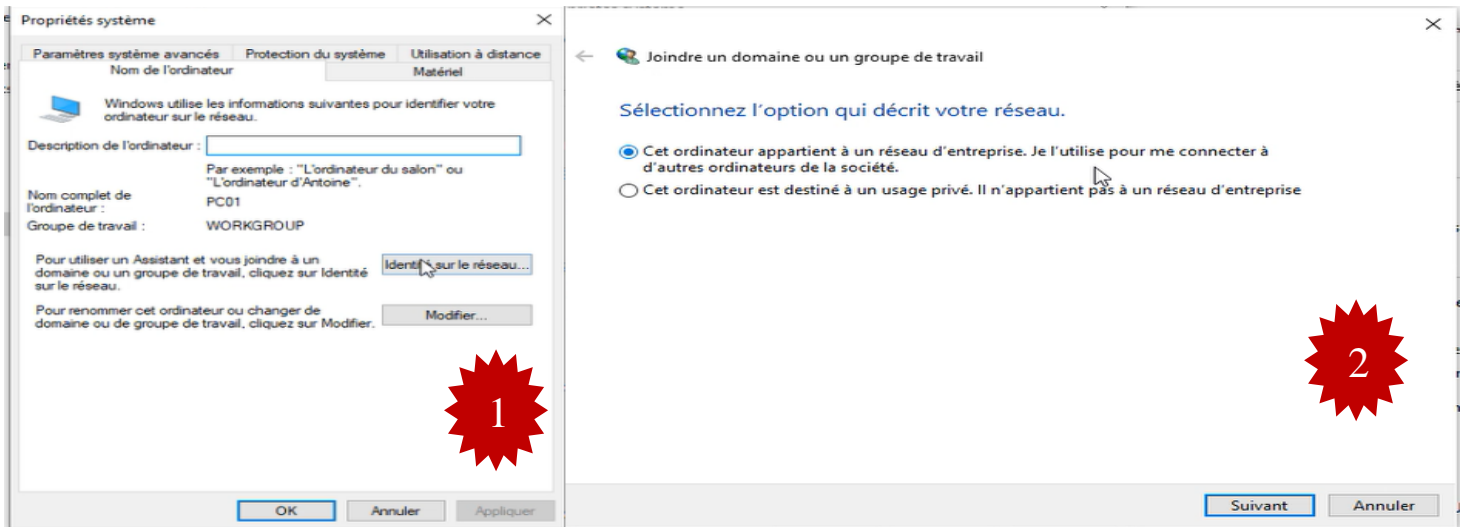
PC9>
```

Adresse IP du client	Nom	Expiration du bail	Type	ID unique	Description	Protection d'accès réseau	Actions
10.0.100.11	PC11.campusnts.local	24/06/2022 16:41:32	DHCP	005079666...		Accès complet	Baux d'adresses
10.0.100.12	PC91.campusnts.local	24/06/2022 16:42:14	DHCP	005079666...		Accès complet	Autres actions
10.0.100.13	PC71.campusnts.local	24/06/2022 16:42:29	DHCP	005079666...		Accès complet	

FIGURE IV.43 – Test dhcp réussi.

IV.9.1.2 Test Active directory

On va essayer de joindre notre domaine à partir de notre machine client et voir le résultat :



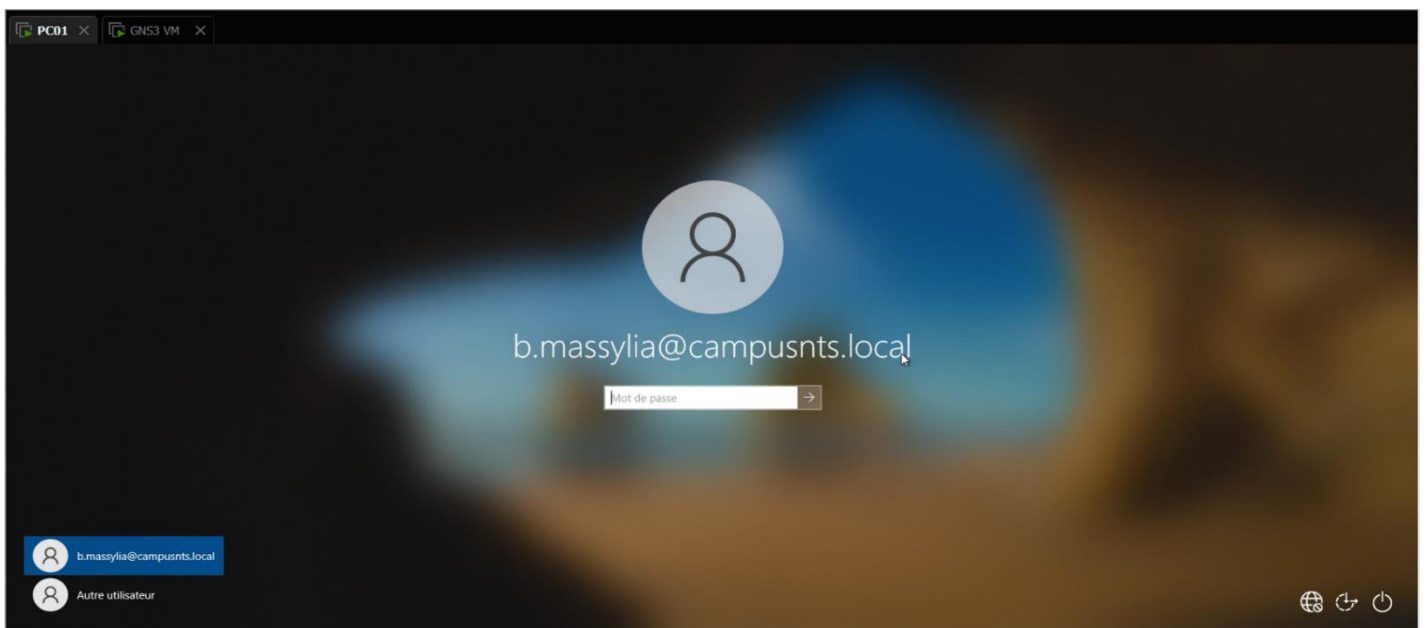
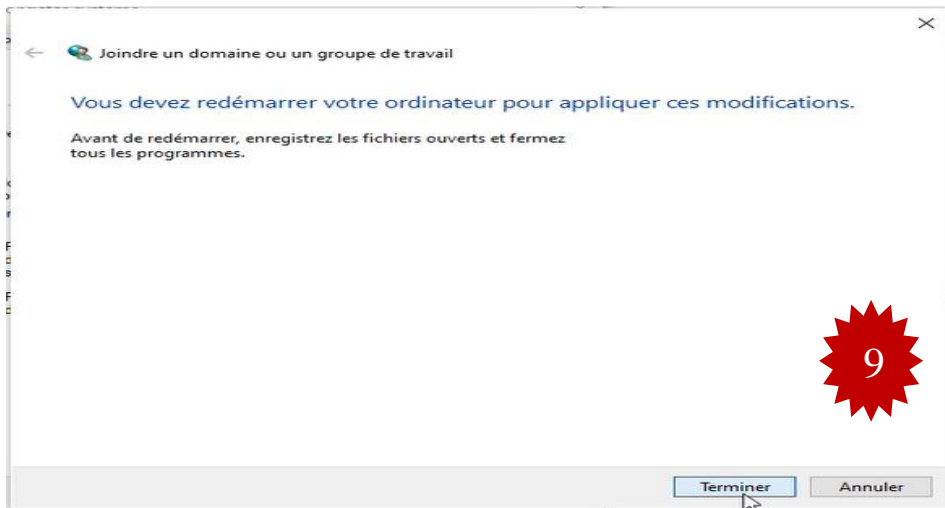
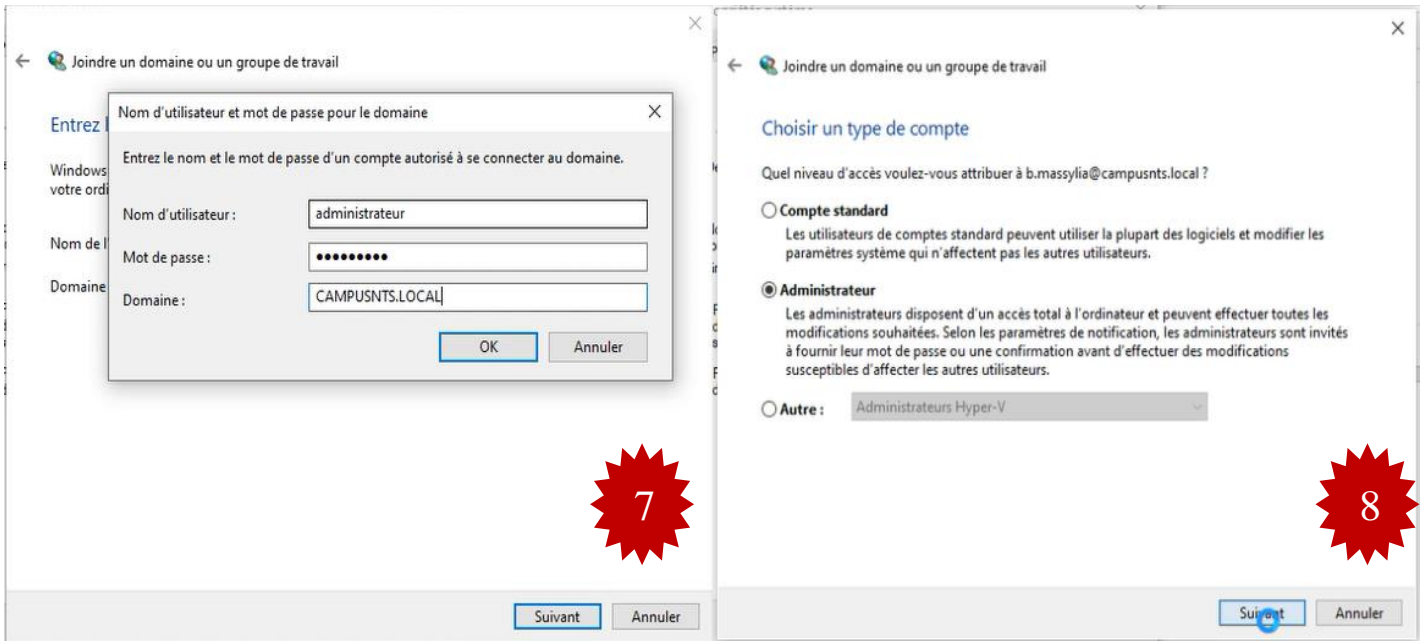


FIGURE IV.44 – Test Active directory réussi.

IV.9.2 Test SSH

SSH est maintenant activé. Nous pouvons accéder au routeur à l'aide d'un client SSH dans notre cas via l'outil Windows PuTTY.

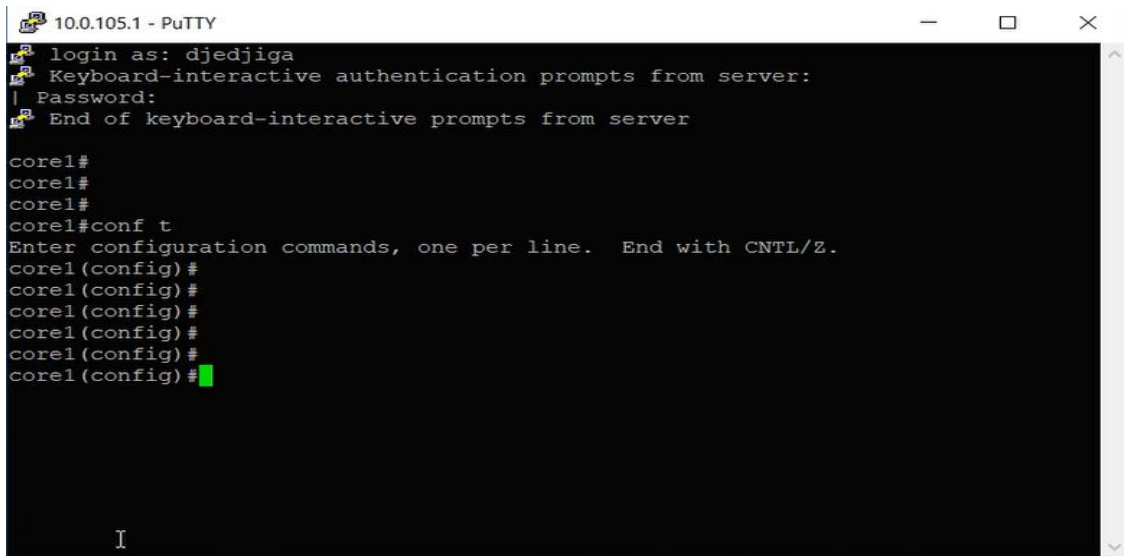


FIGURE IV.45 – Test SSH réussi.

IV.9.3 Test port Security

On va tester la fonction de ports Security. On a mis le mode shutdown en cas de violation, après avoir fixé une adresse mac sur notre port au mode static. On va essayer de mettre un autre ordinateur pour tester le résultat des ports qui sont fermés après la violation d'adresse MAC

```
S-access4#
*Jul 6 14:29:09.055: %PM-4-ERR_DISABLE: psecure-violation error detected on Et1/0, putting Et1/0 in err-disable state
S-access4#
*Jul 6 14:29:09.055: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0050.7966.6814 on port Ethernet1/0.
*Jul 6 14:29:10.064: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
S-access4#
*Jul 6 14:29:11.062: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to down
```

```
S-access4#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	unassigned	YES	unset	up	up
Ethernet0/1	unassigned	YES	unset	up	up
Ethernet0/2	unassigned	YES	unset	up	up
Ethernet0/3	unassigned	YES	unset	up	up
Ethernet1/0	unassigned	YES	unset	down	down
Ethernet1/1	unassigned	YES	unset	up	up
Ethernet1/2	unassigned	YES	unset	up	up
Ethernet1/3	unassigned	YES	unset	up	up
Ethernet2/0	unassigned	YES	unset	up	up
Ethernet2/1	unassigned	YES	unset	up	up
Ethernet2/2	unassigned	YES	unset	up	up
Ethernet2/3	unassigned	YES	unset	up	up
Ethernet3/0	unassigned	YES	unset	up	up
Ethernet3/1	unassigned	YES	unset	up	up
Ethernet3/2	unassigned	YES	unset	up	up
Ethernet3/3	unassigned	YES	unset	up	up
Vlan1	unassigned	YES	unset	administratively down	down

FIGURE IV.46 – Test réussi le port est down après la violation.

IV.9.4 Test Radius

On va tester l'authentification RADIUS sur le switch client

```

Server Policies:
  Vlan Group:  Vlan: 104

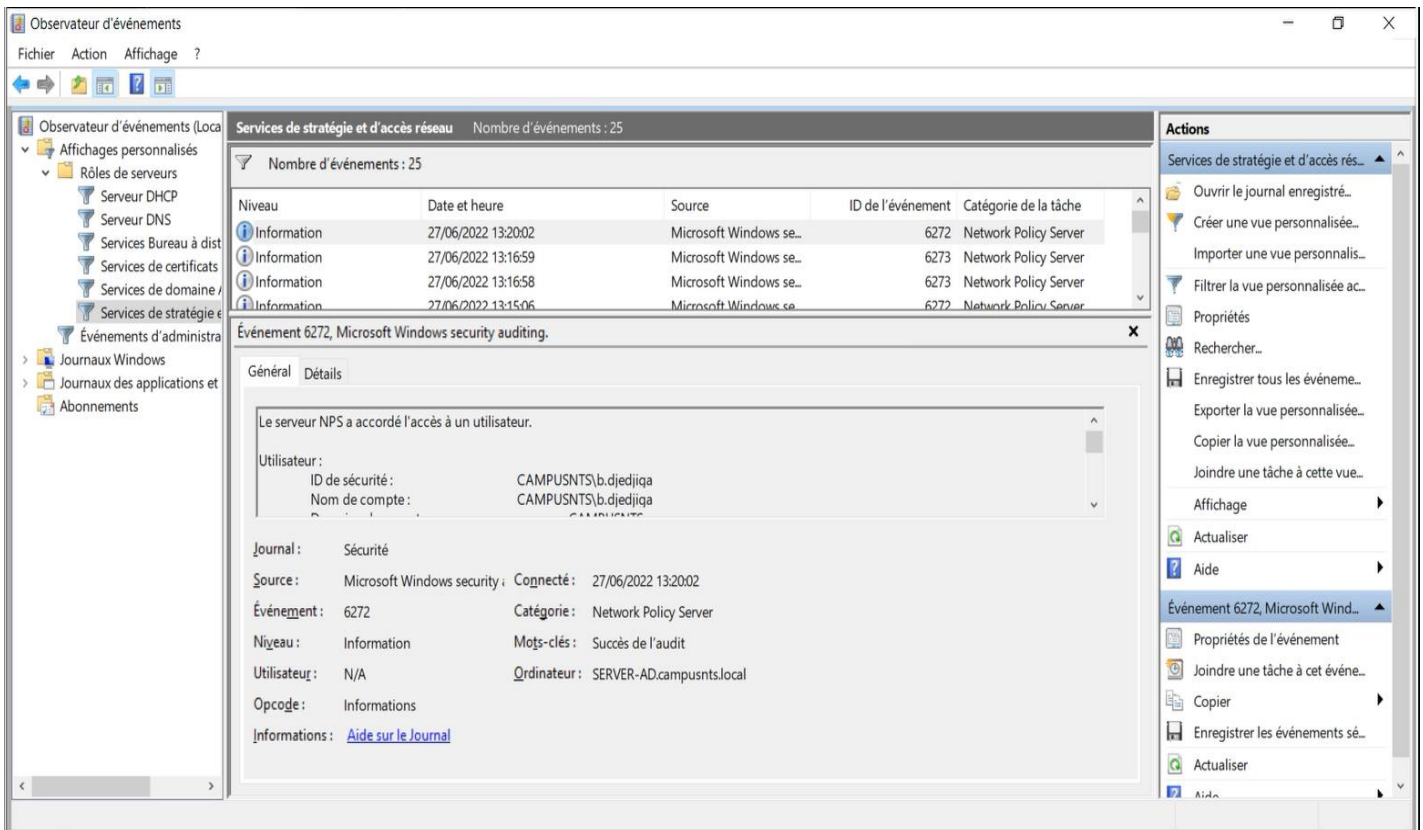
Method status list:
  Method      State

SWD2#Show authentication sessions interface eth 2/1 details
  Interface:  Ethernet2/1
  MAC Address: 000c.29b0.0d2c
  IPv6 Address: Unknown
  IPv4 Address: 10.0.104.11
  User-Name:  CAMPUSNTS\b.djedjiga
  Status:    Authorized
  Domain:    DATA
  Oper host mode: multi-domain
  Oper control dir: both
  Session timeout: N/A
  Common Session ID: 0A0069030000000C0030887E
  Acct Session ID: Unknown
  Handle:     0x71000001
  Current Policy: POLICY_Et2/1

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
  Security Policy:  Should Secure
  Security Status:  Link Unsecure

Server Policies:
  Vlan Group:  Vlan: 104

Method status list:
  Method      State
  dot1x      Authc Success
  
```

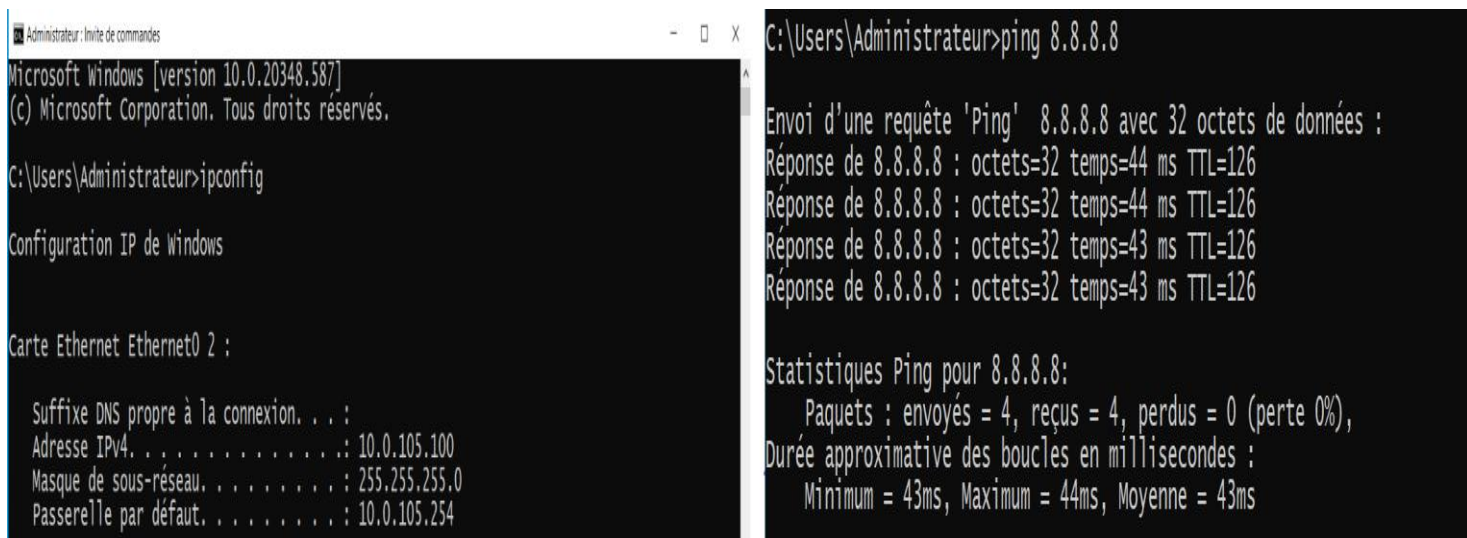


No.	Time	Source	Destination	Protocol	Length	Info
11570	5470.504009	10.0.105.100	10.0.105.3	RADIUS	162	Access-Challenge id=41
11571	5470.509085	10.0.105.3	10.0.105.100	RADIUS	403	Access-Request id=42
11572	5470.510753	10.0.105.100	10.0.105.3	RADIUS	177	Access-Challenge id=42
11573	5470.520172	10.0.105.3	10.0.105.100	RADIUS	398	Access-Request id=43
11574	5470.524814	10.0.105.100	10.0.105.3	RADIUS	192	Access-Challenge id=43
11575	5470.551649	10.0.105.3	10.0.105.100	RADIUS	457	Access-Request id=44

FIGURE IV.47 – Test Radius réussi pour le client b. massylia.

IV.9.5 Test routage statique

Maintenant, on va pinger vers internet depuis notre serveur ad « vlan 105 »



```
Administrateur: invite de commandes
Microsoft Windows [version 10.0.20348.587]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet0 2 :

Suffixe DNS propre à la connexion. . . . :
Adresse IPv4. . . . . : 10.0.105.100
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . : 10.0.105.254

C:\Users\Administrateur>ping 8.8.8.8

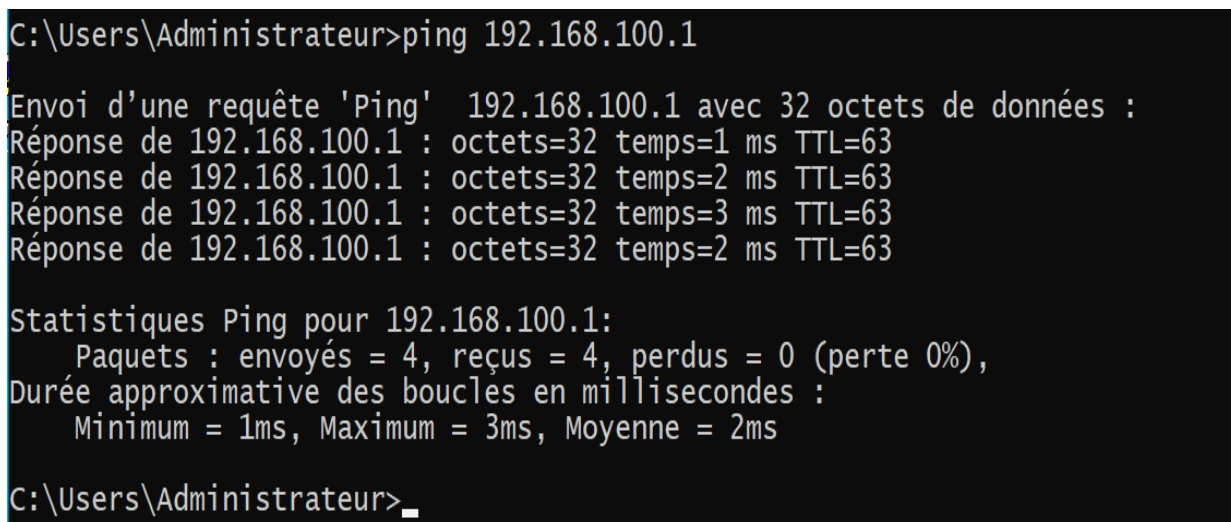
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=44 ms TTL=126
Réponse de 8.8.8.8 : octets=32 temps=44 ms TTL=126
Réponse de 8.8.8.8 : octets=32 temps=43 ms TTL=126
Réponse de 8.8.8.8 : octets=32 temps=43 ms TTL=126

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 43ms, Maximum = 44ms, Moyenne = 43ms

C:\Users\Administrateur>
```

FIGURE IV.48 – Ping réussi vers le serveur google « internet ».

IV.9.6 Test les pare-feu Bejaia et Alger



```
C:\Users\Administrateur>ping 192.168.100.1

Envoi d'une requête 'Ping' 192.168.100.1 avec 32 octets de données :
Réponse de 192.168.100.1 : octets=32 temps=1 ms TTL=63
Réponse de 192.168.100.1 : octets=32 temps=2 ms TTL=63
Réponse de 192.168.100.1 : octets=32 temps=3 ms TTL=63
Réponse de 192.168.100.1 : octets=32 temps=2 ms TTL=63

Statistiques Ping pour 192.168.100.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 3ms, Moyenne = 2ms

C:\Users\Administrateur>
```

FIGURE IV.49 – Ping réussi sur le pare-feu Bejaia.

```
C:\Users\Administrateur>ping 192.168.2.1

Envoi d'une requête 'Ping' 192.168.2.1 avec 32 octets de données :
Réponse de 192.168.2.1 : octets=32 temps=3 ms TTL=62
Réponse de 192.168.2.1 : octets=32 temps=5 ms TTL=62
Réponse de 192.168.2.1 : octets=32 temps=4 ms TTL=62
Réponse de 192.168.2.1 : octets=32 temps=3 ms TTL=62

Statistiques Ping pour 192.168.2.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 5ms, Moyenne = 3ms
```

FIGURE IV.50 – Ping réussi sur le pare-feu Alger.

IV.9.7 Vérification du tunnel VPN

La négociation dans le tunnel VPN, ça se passe bien donc il est bien réussi. Et elle se fait en deux phases :

Phase 1 : Dans cette phase, on fait les échanges des clés sécurisées avec IKE afin que les utilisateurs puissent négocier dans le tunnel secrètement et c'est la deuxième phase.

Phase 2 : C'est là où on fait la négociation avec les deux protocoles suivants :

- **Le protocole ESP (Encapsulating Security Payload)** Fournit des services d'authentifications optionnels pour garantir l'intégrité des paquets protégés.
- **Le protocole AH (Authentication Header)** Garantit l'authenticité des paquets échangés en saisissant une somme de contrôle chiffrée (de l'en-tête IP jusqu'à la fin du paquet).

No.	Time	Source	Destination	Protocol	Length	Info
11570	5470.504009	10.0.105.100	10.0.105.3	RADIUS	162	Access-Challenge id=41
11571	5470.509085	10.0.105.3	10.0.105.100	RADIUS	403	Access-Request id=42
11572	5470.510753	10.0.105.100	10.0.105.3	RADIUS	177	Access-Challenge id=42
11573	5470.520172	10.0.105.3	10.0.105.100	RADIUS	398	Access-Request id=43
11574	5470.524814	10.0.105.100	10.0.105.3	RADIUS	192	Access-Challenge id=43
11575	5470.551649	10.0.105.3	10.0.105.100	RADIUS	457	Access-Request id=44

FIGURE IV.51 – capture WireShark qui montre la négociation ISKAMP du tunnel vpn.

```
C:\Users\PC01>ping 10.0.105.100

Envoi d'une requête 'Ping' 10.0.105.100 avec 32 octets de données :
Réponse de 10.0.105.100 : octets=32 temps=55 ms TTL=126
Réponse de 10.0.105.100 : octets=32 temps=3 ms TTL=126
Réponse de 10.0.105.100 : octets=32 temps=3 ms TTL=126
Réponse de 10.0.105.100 : octets=32 temps=3 ms TTL=126

Statistiques Ping pour 10.0.105.100:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 55ms, Moyenne = 16ms
```

FIGURE IV.52 – Ping réussi depuis le PC01 Alger vers serveur Bejaia.

IV.9.8 Test de connexion RDP de puis Alger vers Bejaia

Le test est réussi, on peut accéder à distance en utilisant le VPN client to site.

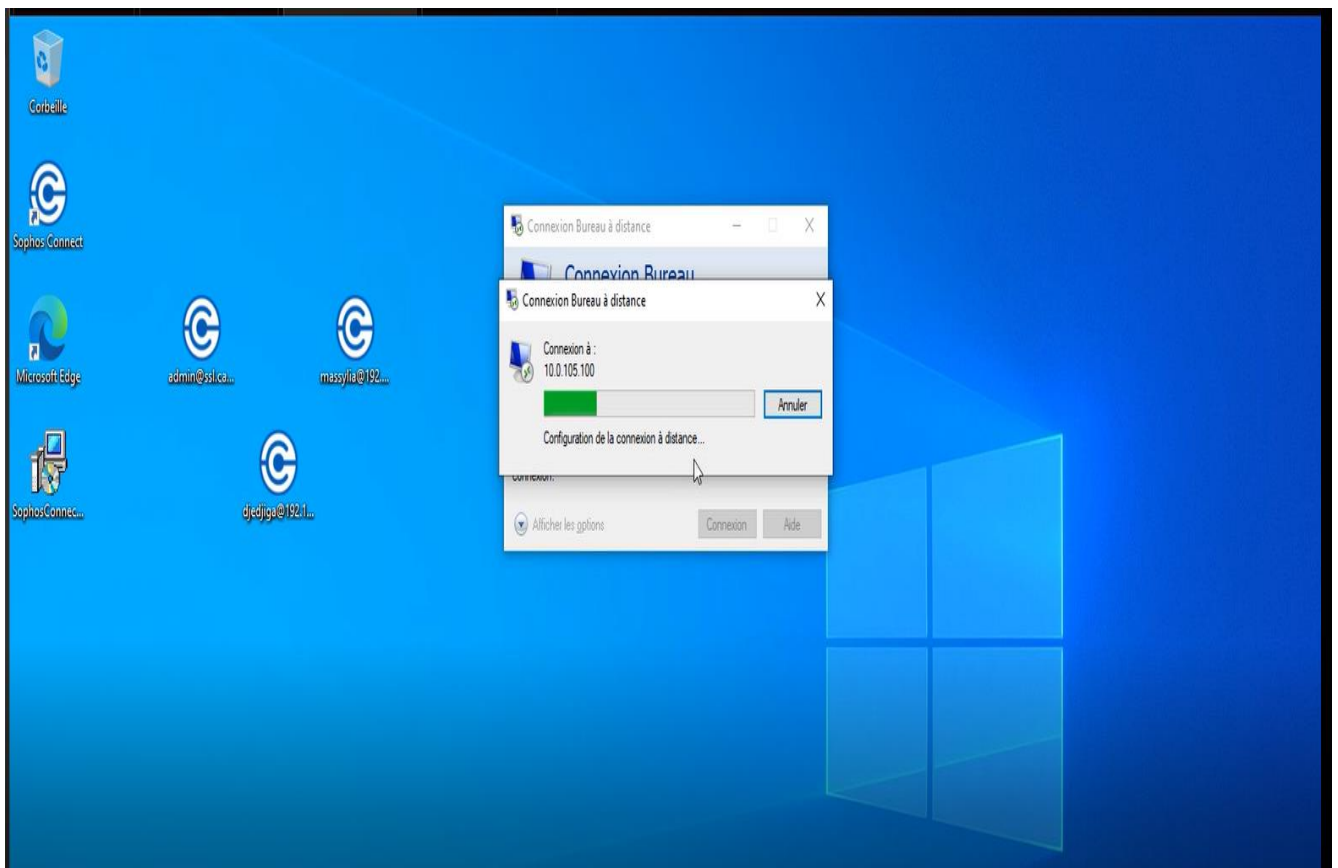
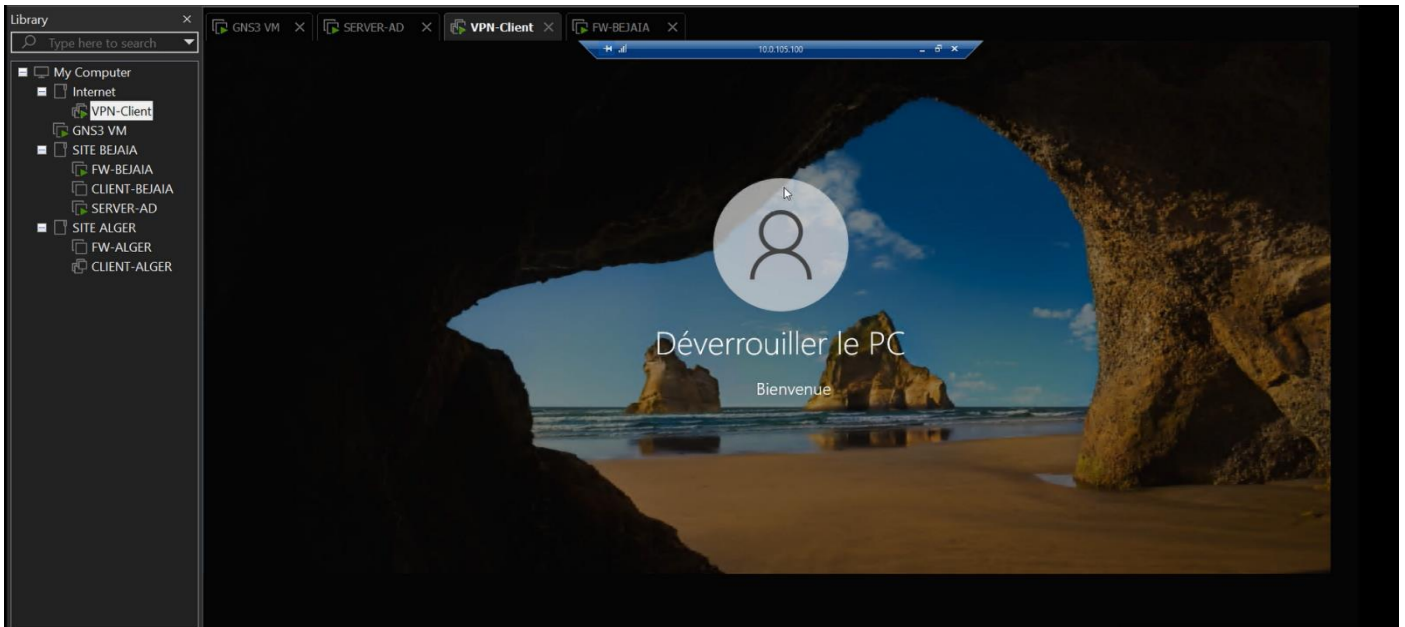


FIGURE IV.53 – Accéder à distance en utilisant le VPN client to site.

IV.9.9 Test DMZ

IV.9.9.1 DMZ

Une zone démilitarisée (DMZ) est un sous-réseau qui héberge des services exposés et accessibles depuis l'extérieur de l'entreprise. Il agit comme un tampon pour les réseaux non sécurisés tel qu'Internet. Son objectif est de renforcer le niveau de sécurité du réseau local de l'entreprise. Et pour vérifier si notre DMZ marche bien, on Ping les serveurs community entre eux puis les serveurs isoleted entre eux. Enfin les serveurs community (serveur BDD, web) et isoleted (serveur POP, FTP) entre eux.

```
SER-WEB> ping 192.168.3.2
84 bytes from 192.168.3.2 icmp_seq=1 ttl=64 time=1.631 ms
84 bytes from 192.168.3.2 icmp_seq=2 ttl=64 time=1.711 ms
84 bytes from 192.168.3.2 icmp_seq=3 ttl=64 time=1.863 ms
84 bytes from 192.168.3.2 icmp_seq=4 ttl=64 time=2.196 ms
84 bytes from 192.168.3.2 icmp_seq=5 ttl=64 time=2.259 ms

SER-WEB> ping 192.168.3.4
host (192.168.3.4) not reachable

SER-WEB> ping 192.168.3.3
host (192.168.3.3) not reachable

SER-FTP> ping 192.168.3.1
host (192.168.3.1) not reachable

SER-FTP> ping 192.168.3.2
host (192.168.3.2) not reachable

SER-ASTERISK> ping 192.168.3.1
host (192.168.3.1) not reachable

SER-ASTERISK> ping 192.168.3.2
host (192.168.3.2) not reachable

SER-ASTERISK> ping 192.168.3.3
host (192.168.3.3) not reachable
```

Figure IV.54 – Test DMZ.

IV.10 Conclusion

Ce chapitre est consacré à la pratique et, plus particulièrement à la mise en œuvre et à la sécurité de l'architecture réseau que nous avons présenté précédemment. Les détails de configuration pour chaque appareil et serveur dans l'architecture réseau, nous l'avons simulé avec GNS3. De plus, grâce à la capture ci-dessus, nous pouvons voir que nous avons atteint la cible.

CONCLUSION gÉNÉRALE

La sécurité du système d'information d'entreprise est une exigence importante des entreprises pour suivre ses activités. Qu'il s'agisse de voler ses secrets de fabrication ou de perdre ses données clients, cela nous ramène à la nécessité de garantir certains besoins de sécurité : intégrité et confidentialité des données transmises, authentification des utilisateurs, et non répudiation de leurs actions.

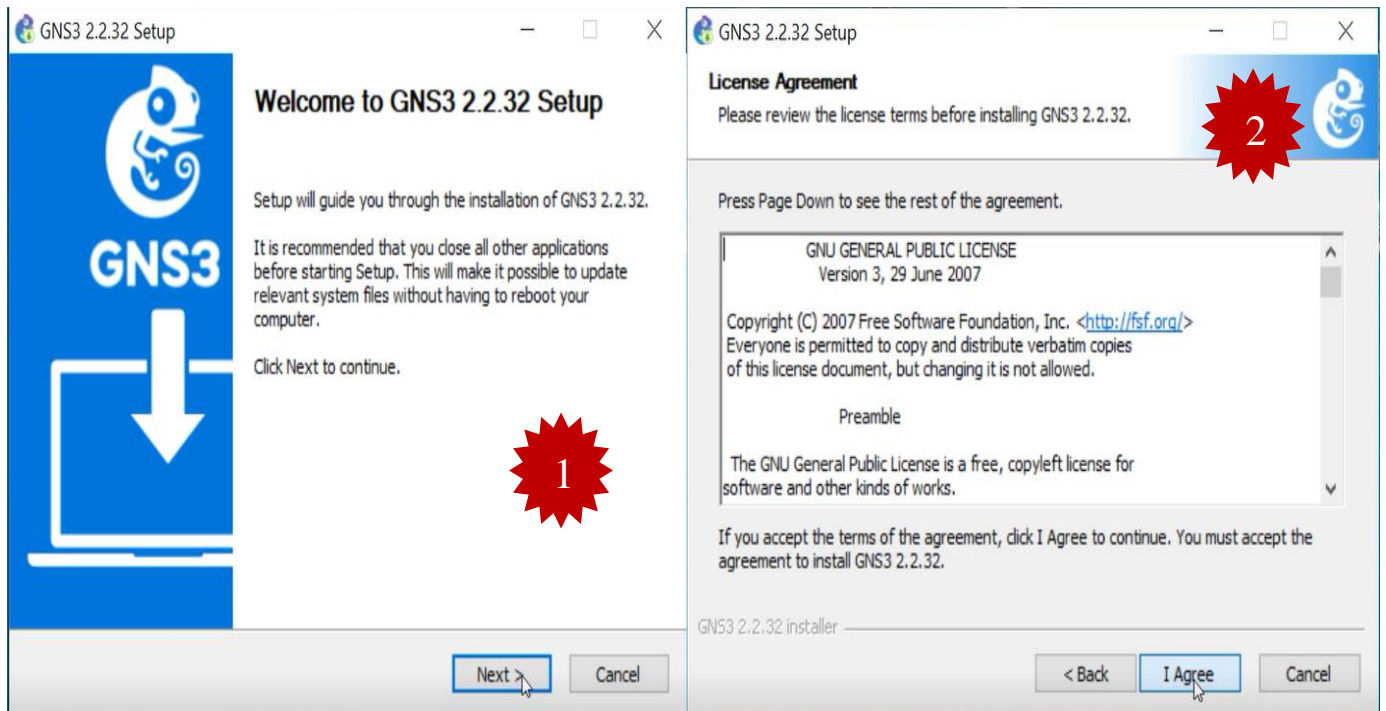
Dans notre mémoire, nous nous intéressons à un ensemble de techniques (méthodes) afin d'aider à construire et à faire fonctionner une infrastructure réseau protégée par : Radius, Firewalls, VPN et VLAN, Active Directory, Port Security contre ces différentes menaces et attaques. Notre proposition de politique de sécurité nécessite la configuration de plusieurs éléments du réseau (routeurs, radius, HSRP, etc.) pour une plus grande sécurité au sein de notre entreprise campus NTS.

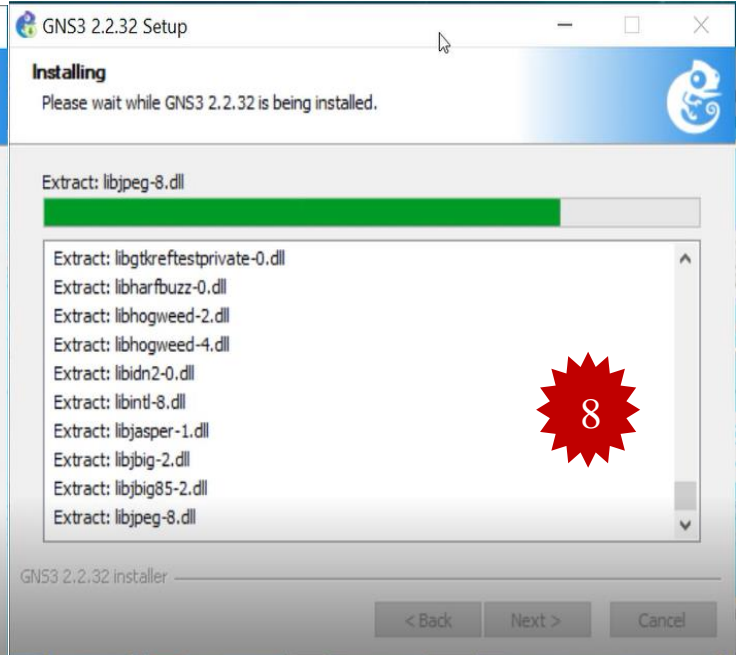
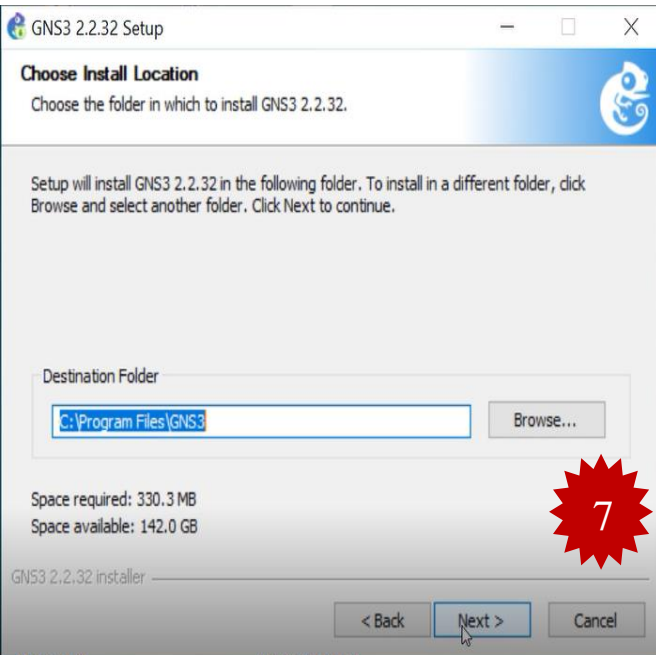
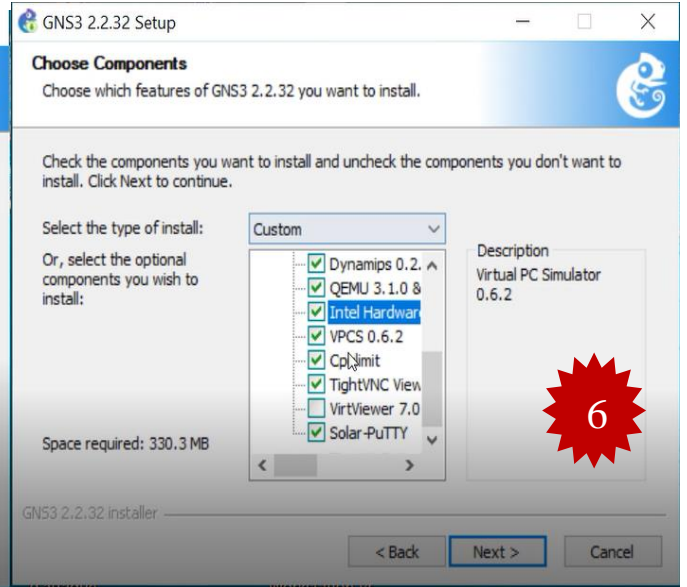
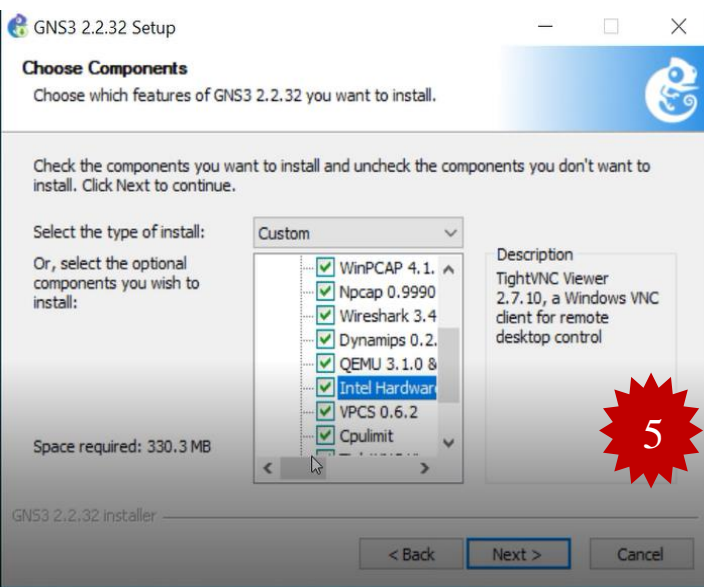
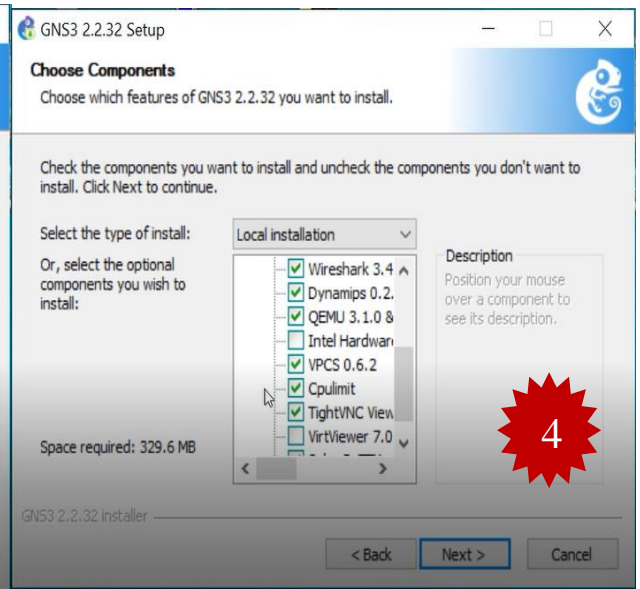
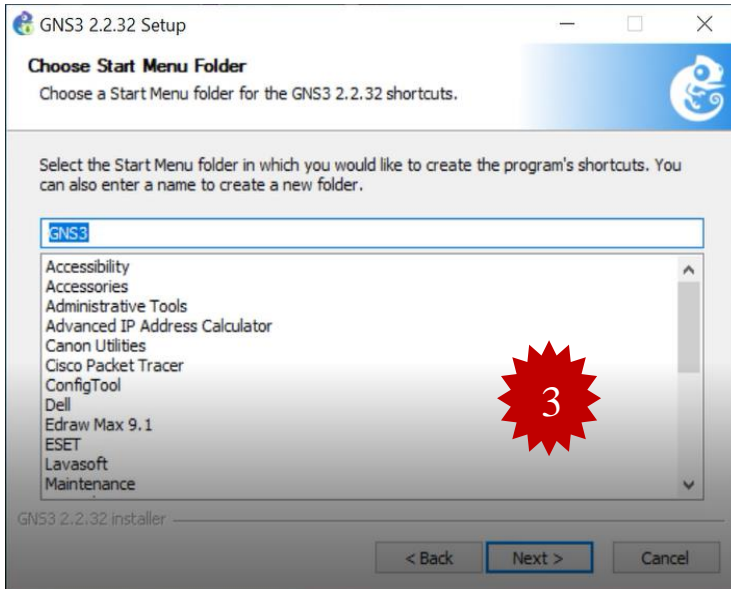
ANNEXES

Annexe 1

Installation de GNS3

Sous Windows, l'installation est assez classique. Après avoir lancé l'installation, la fenêtre de configuration apparaît et nous suivons les instructions ci-dessous :





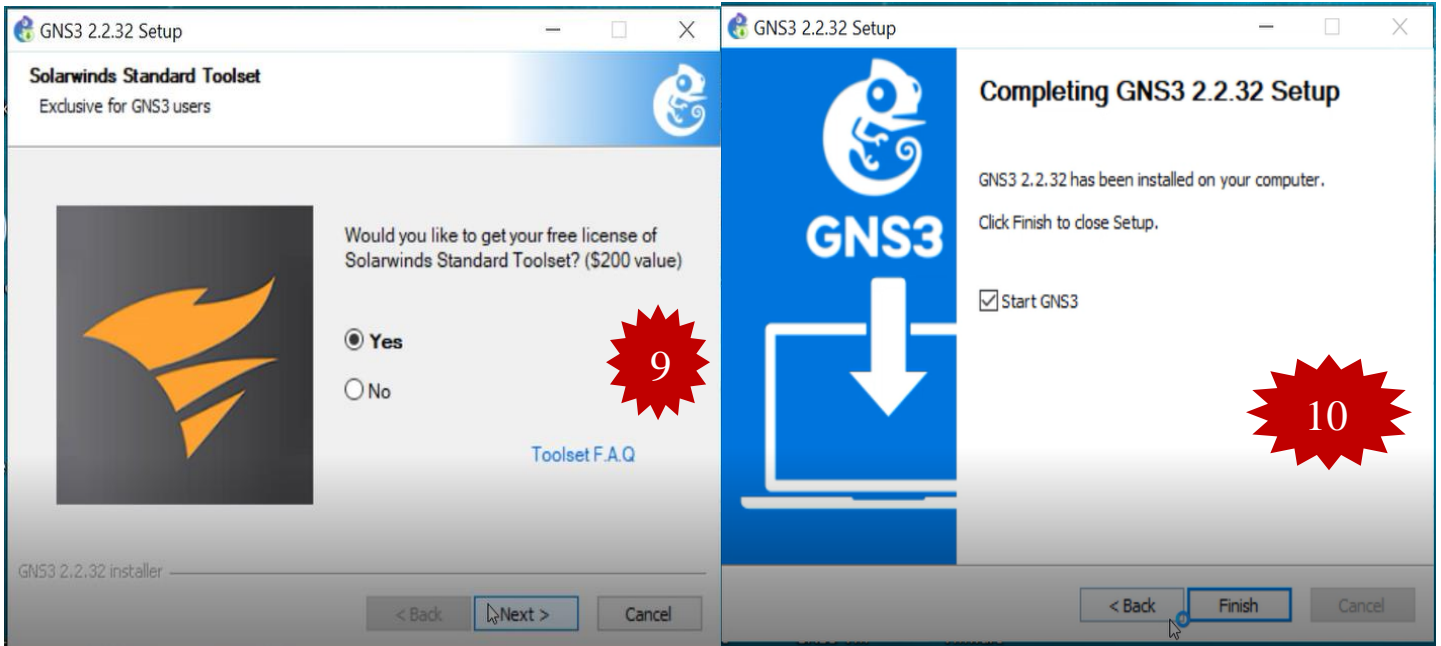


FIGURE IV.55 – Installation de GNS3.

Une fois l'installation terminée, nous aurons l'interface GNS3 suivante :

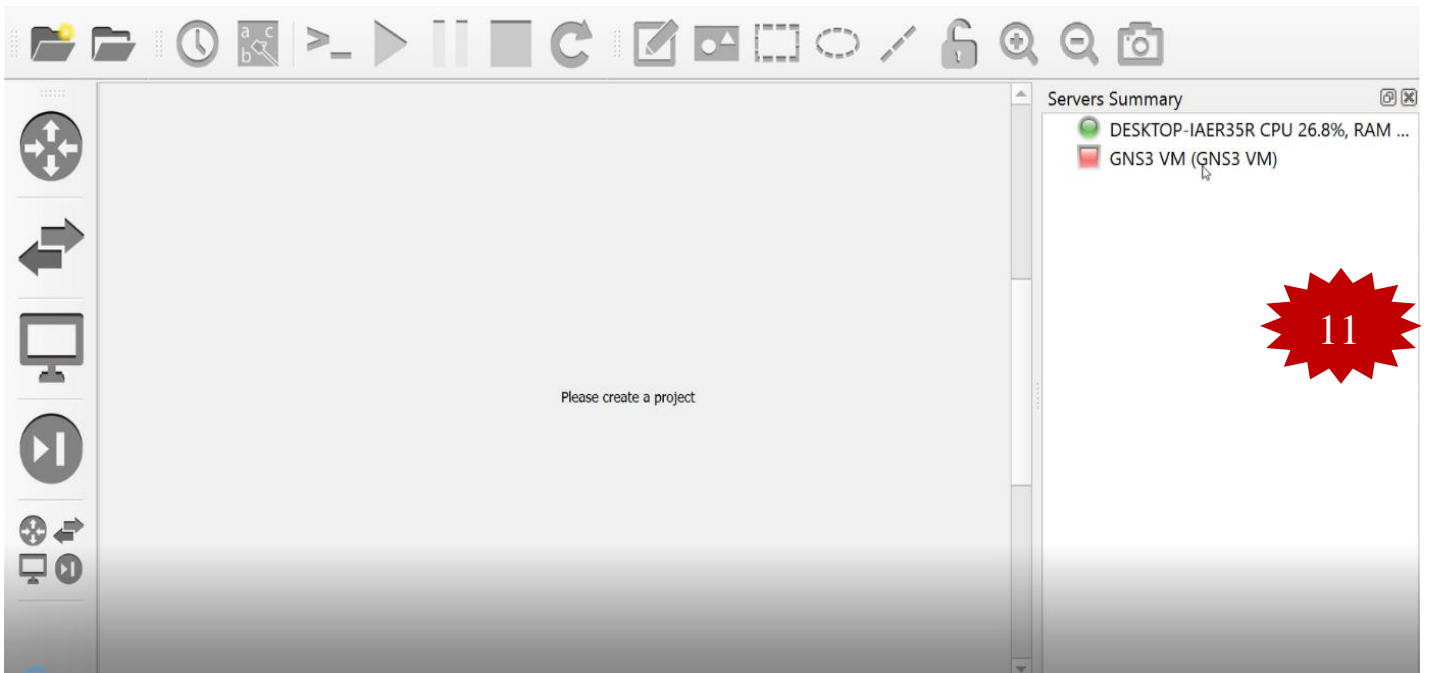
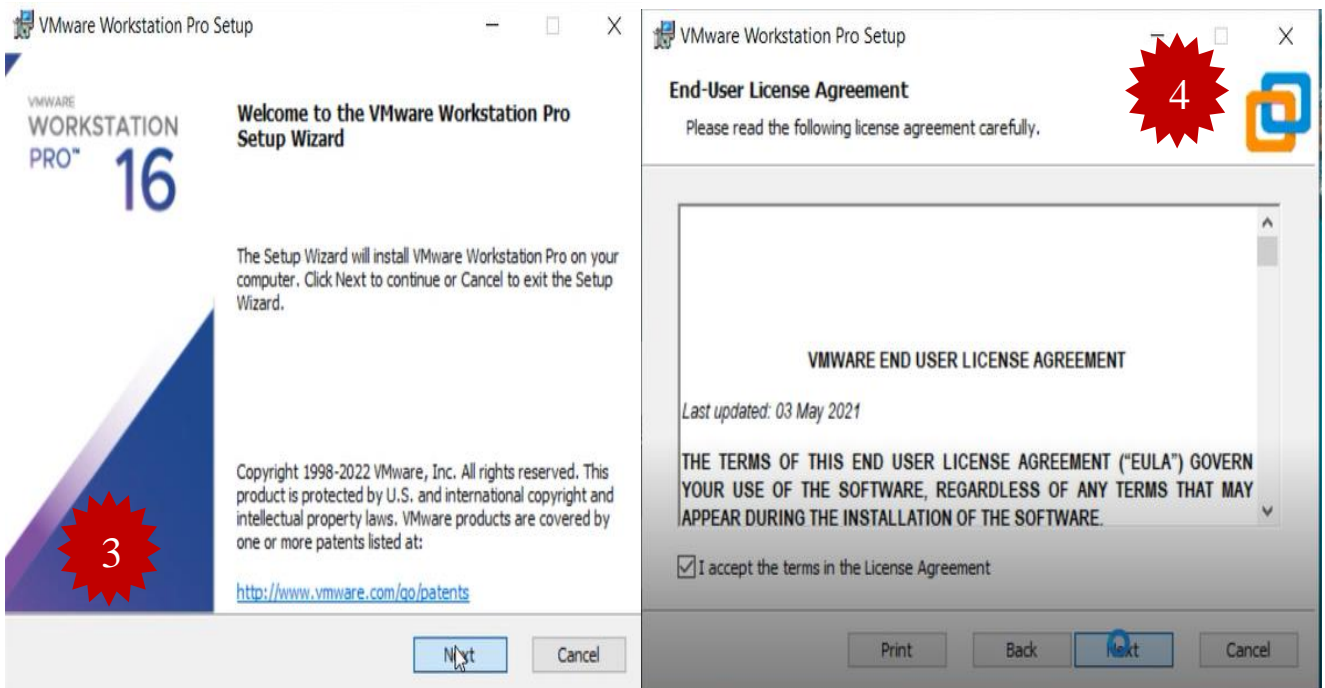


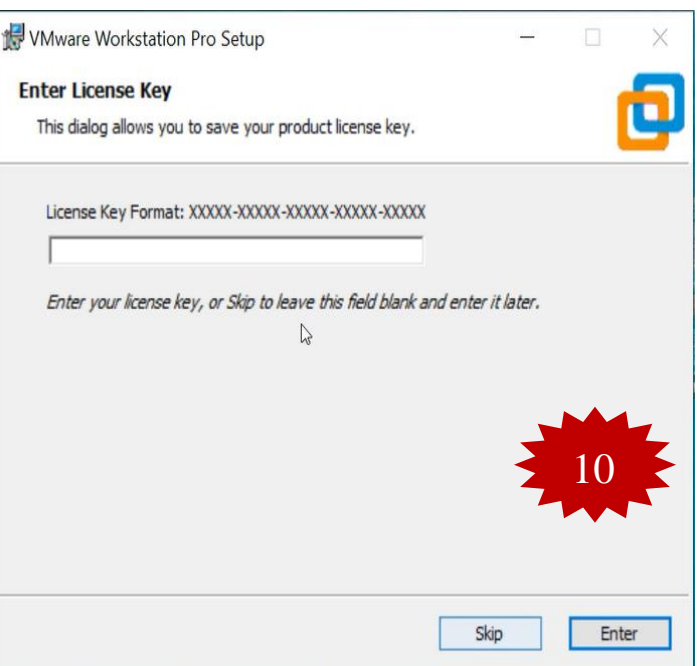
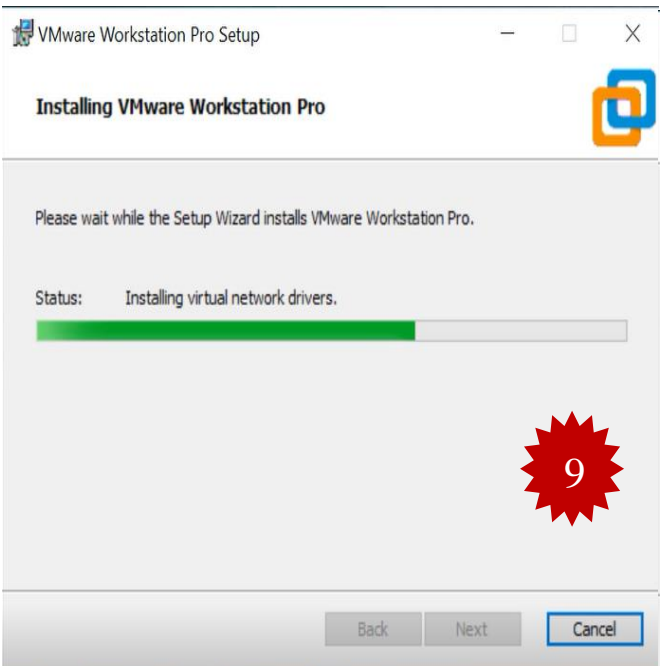
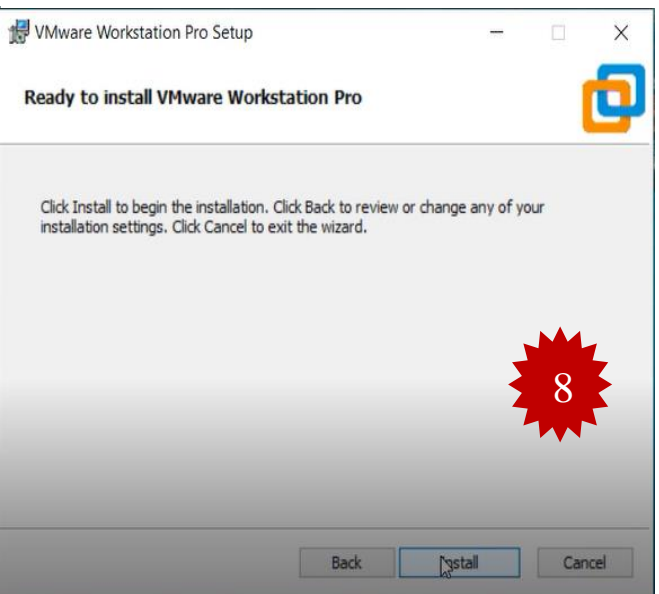
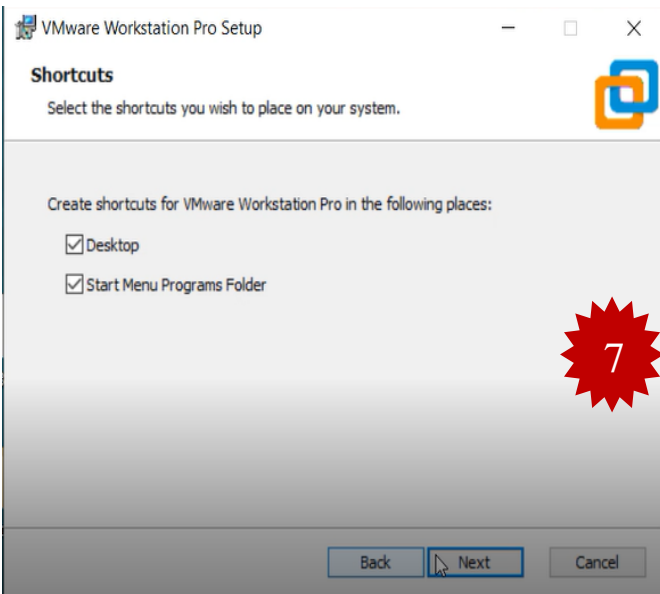
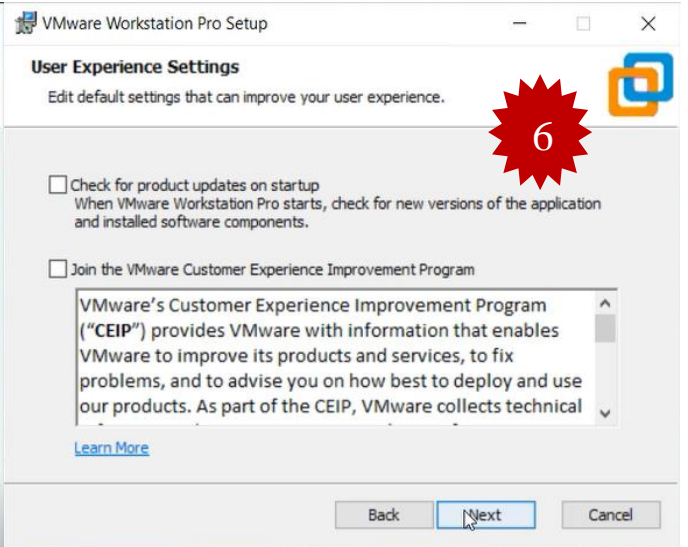
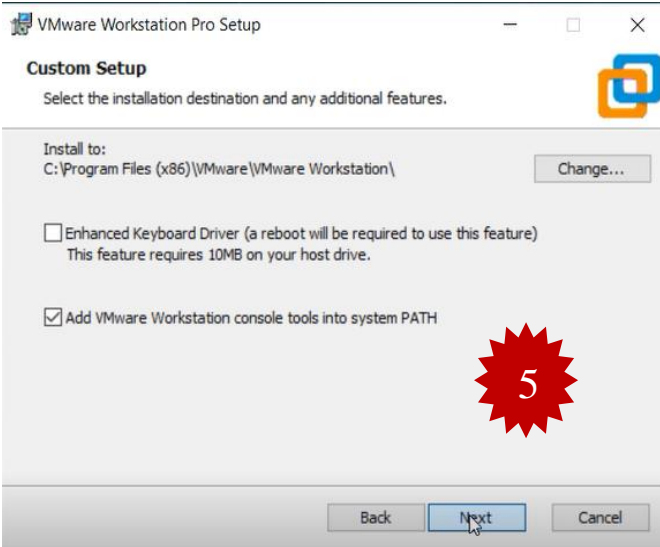
FIGURE IV.56 –l'interface GNS3.

Annexe 2

A. Installation de VMware Workstation version 16.1.2

Afin de créer une machine utilisateur virtuelle sur le même ordinateur, nous devons suivre les étapes ci-dessous pour installer VMware Workstation





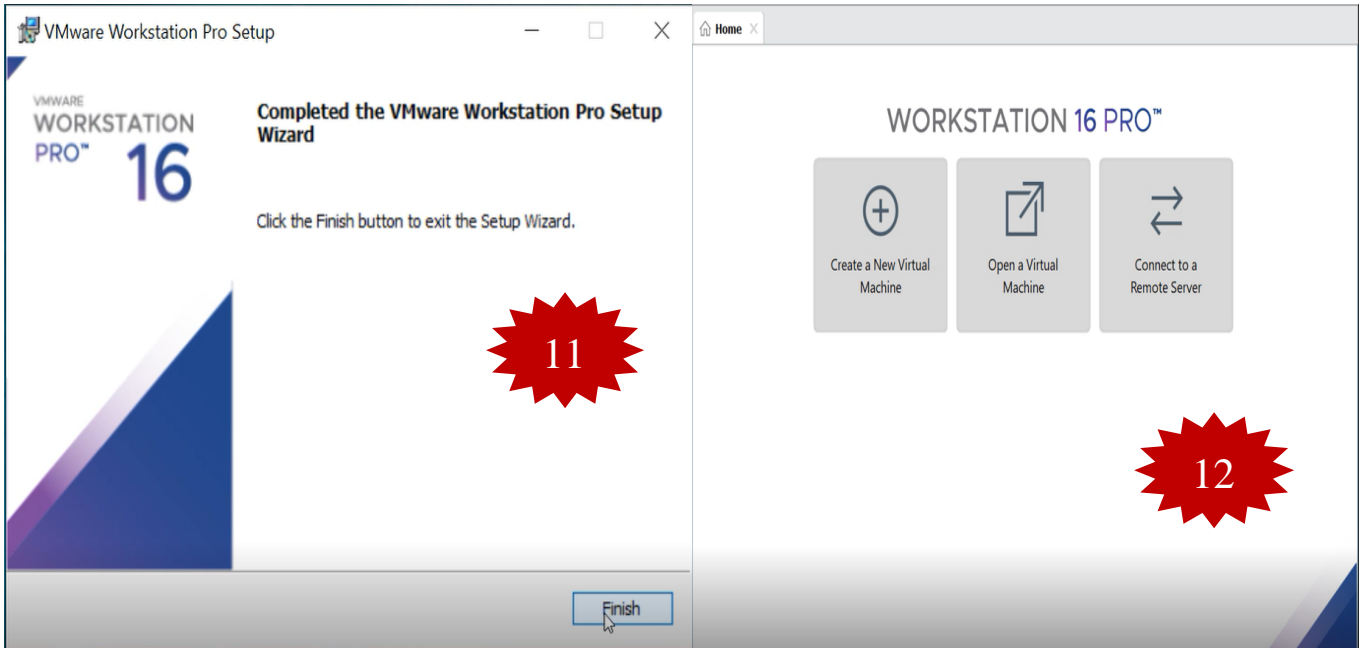
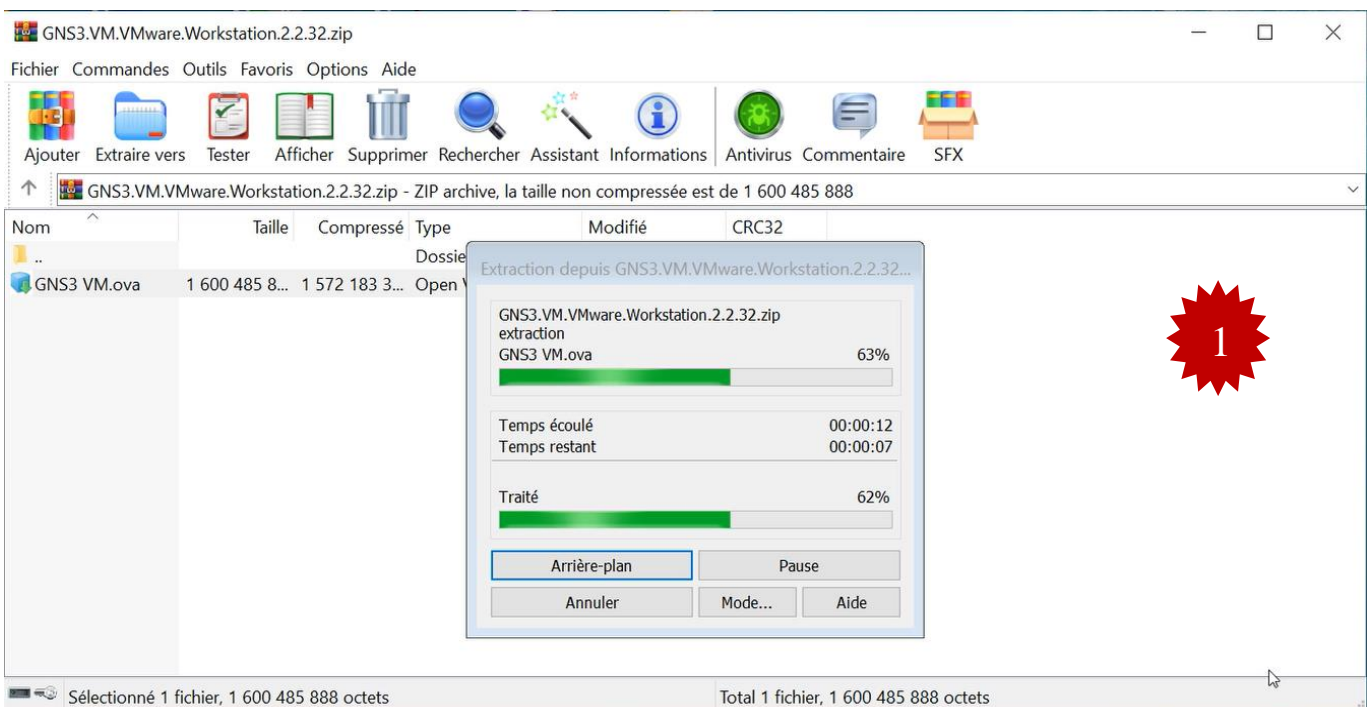


FIGURE IV.57 – Installation de VMware Workstation version 16.1.2.

B. Liaison GNS3 VM et GNS3 Client

Après avoir téléchargé le fichier "GNS3 VM", on va faire une liaison entre GNS3 VM et GNS3 Client. Pour cela il faut suivre les étapes suivant :



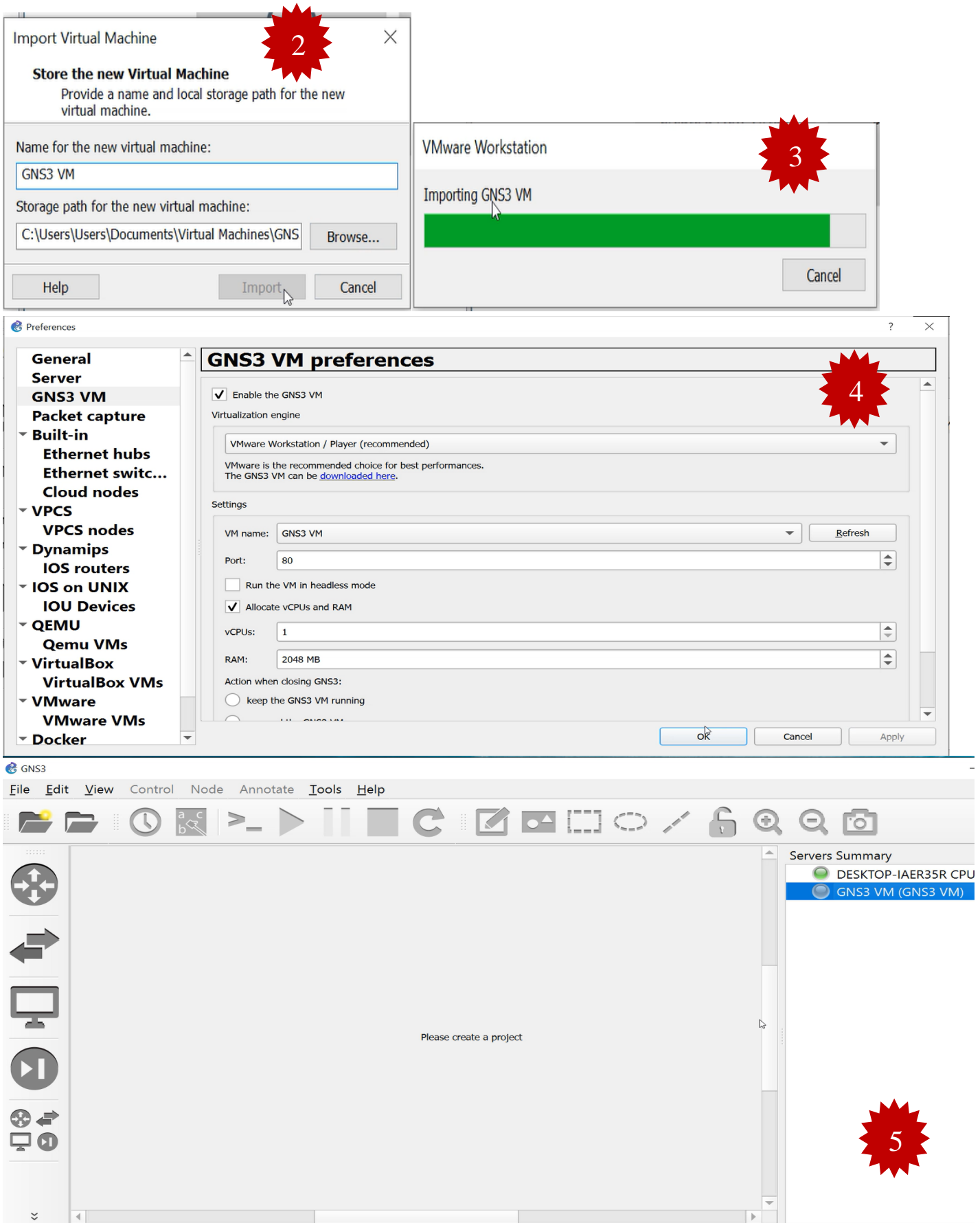


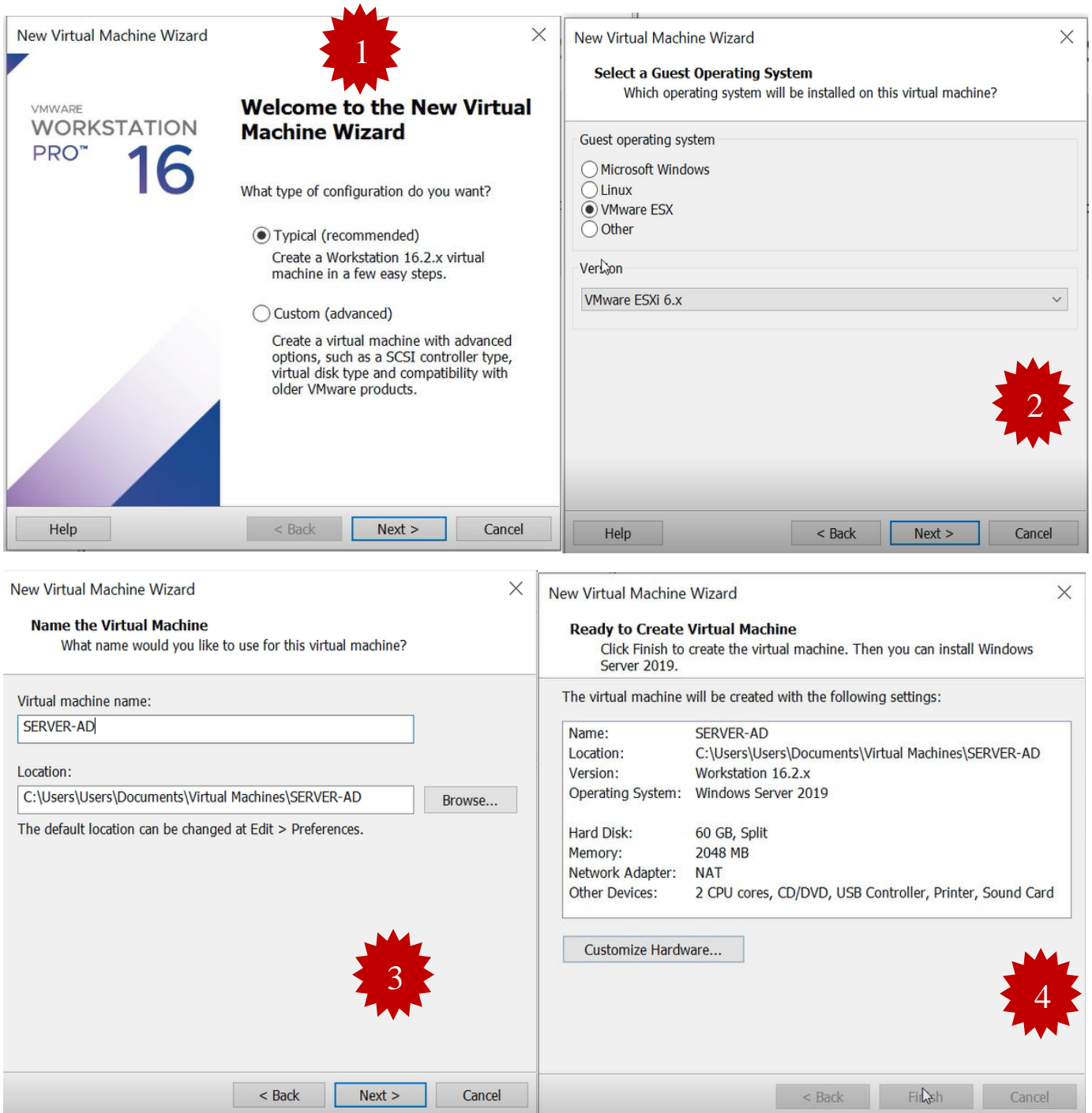
FIGURE IV.58 – Liaison GNS3 VM et GNS3 Client.

Annexe 3

Création des machines virtuelles

A. Installation du Windows server 2022

Dans la présente section, nous examinerons les diverses étapes de l'installation de Windows Server 2022.



Hardware

Device	Summary
Memory	2 GB
Processors	2
New CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

Connected
 Connect at power on

Network connection

Bridged: Connected directly to the physical network
 Replicate physical network connection state

NAT: Used to share the host's IP address
 Host-only: A private network shared with the host
 Custom: Specific virtual network

VMnet0

LAN segment:

LAN Segments... Advanced...

Add... Remove

Close Help



Virtual Machine Settings

Hardware Options

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

Connected
 Connect at power on

Connection

Use physical drive:
Auto detect

Use ISO image file:
P:\SERVER_EVAL_x64FRE_fr-fr.iso Browse... Advanced...

Add... Remove

OK Cancel Help



Library

Type here to search

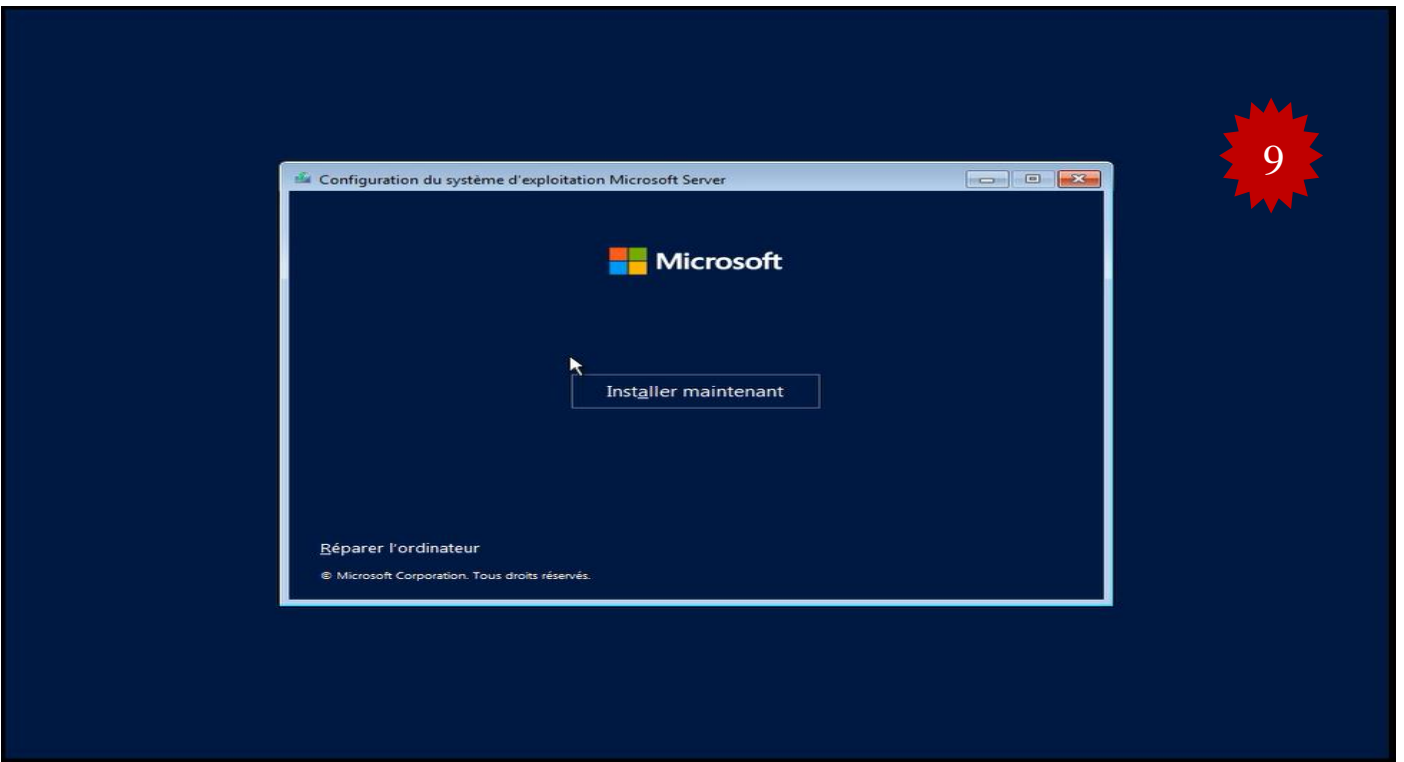
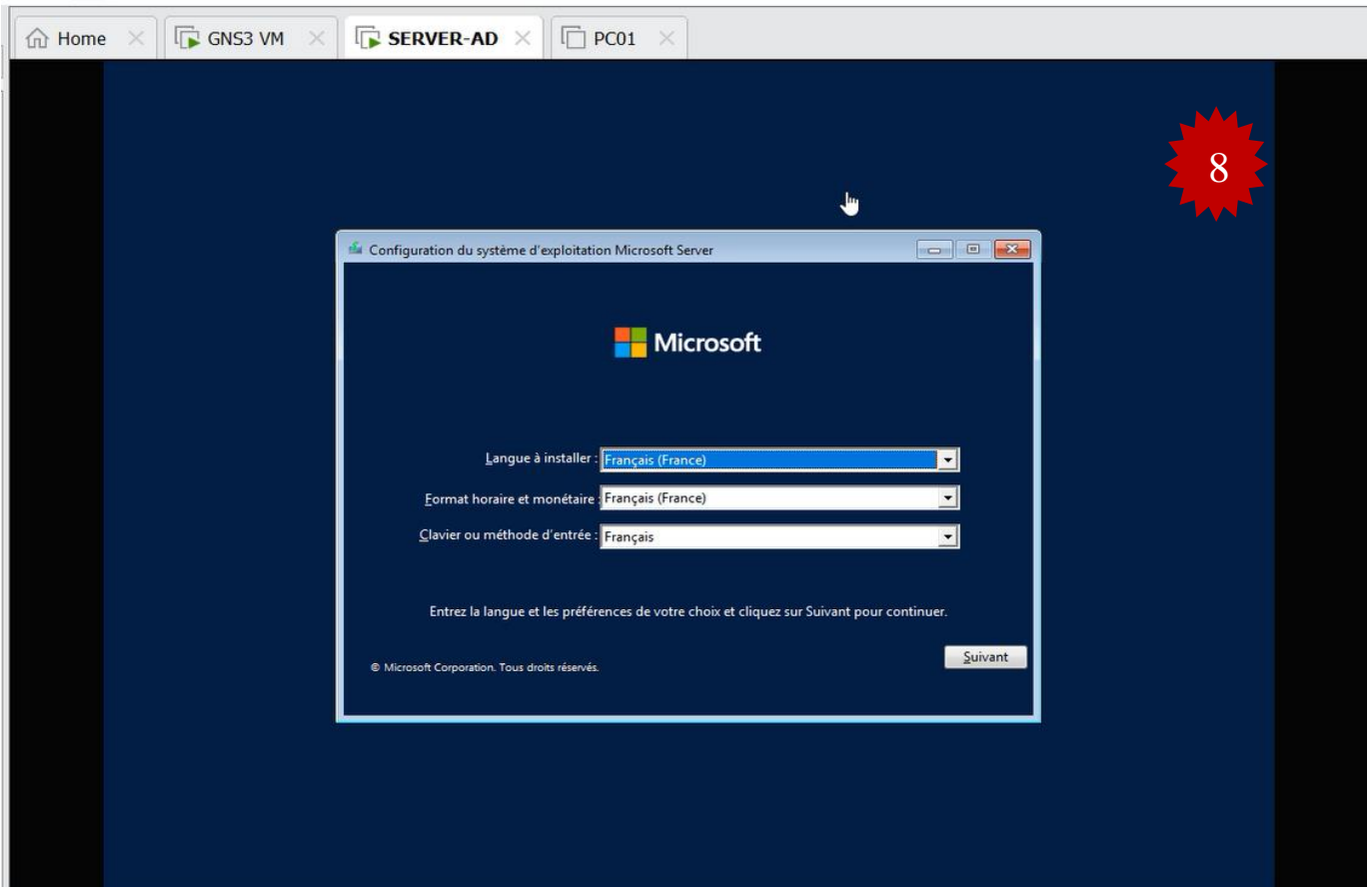
- My Computer
 - GNS3 VM
 - SERVER-AD
 - PC01

Home GNS3 VM SERVER-AD

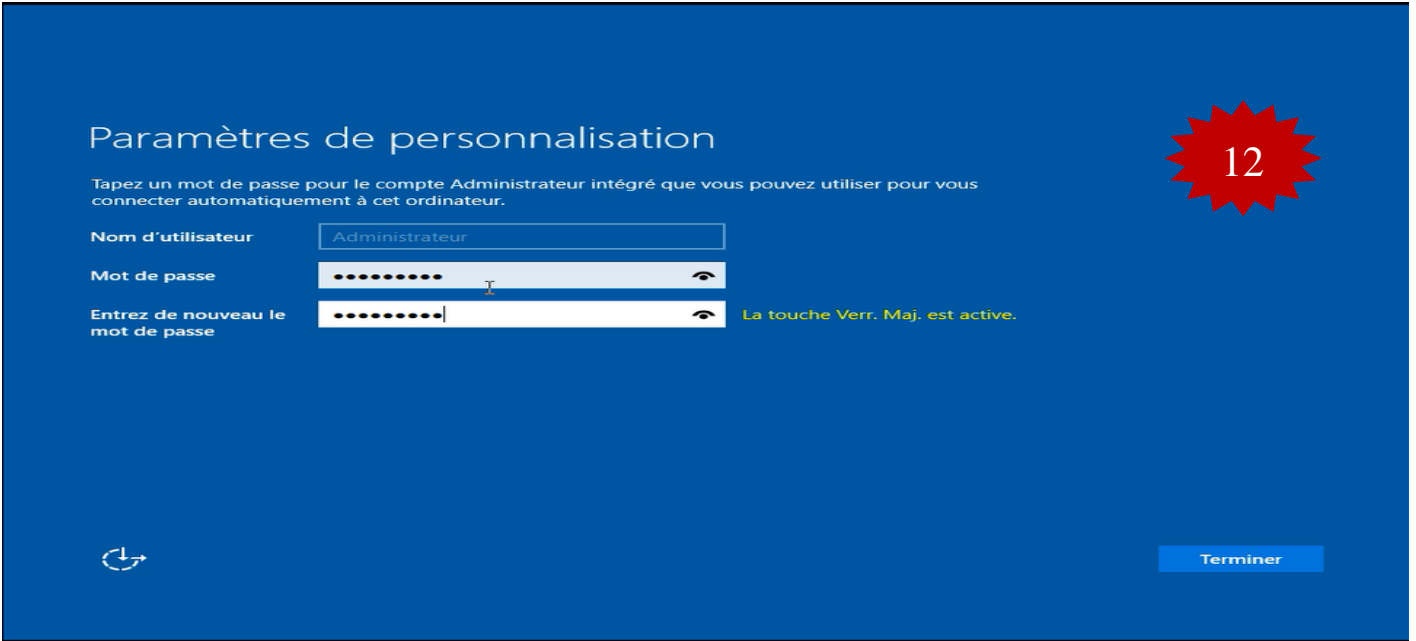
Loading files...

The virtual printing feature is globally disabled on this system, and will not be enabled for t... Virtual device 'serial0' will start disconnected.

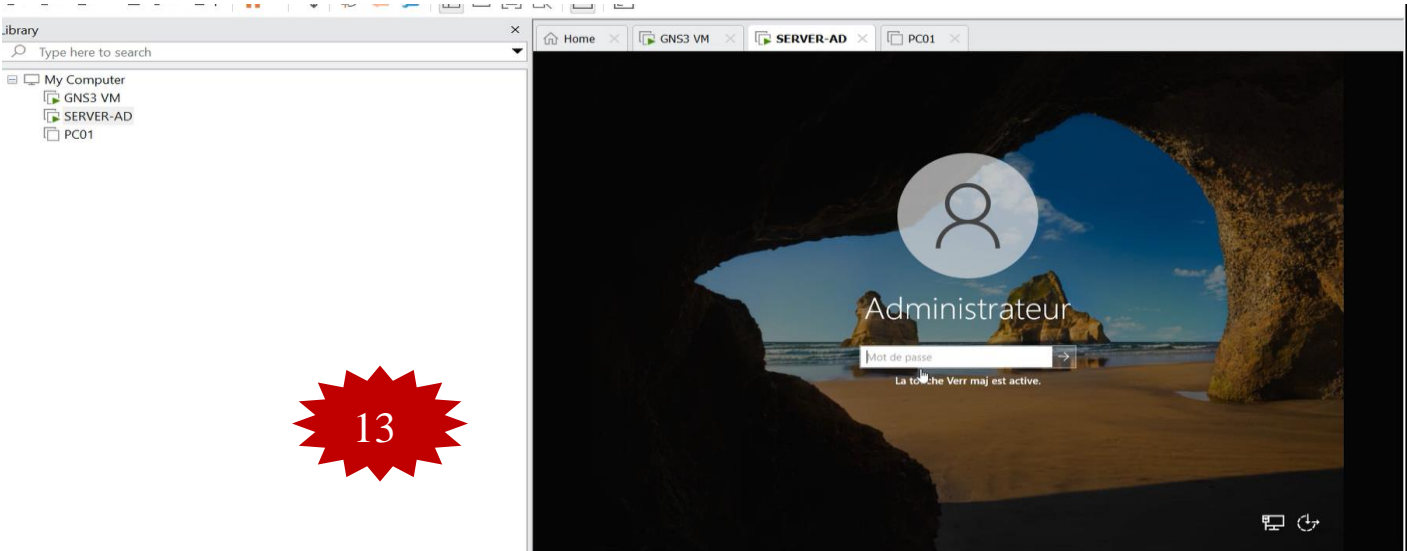








12



13



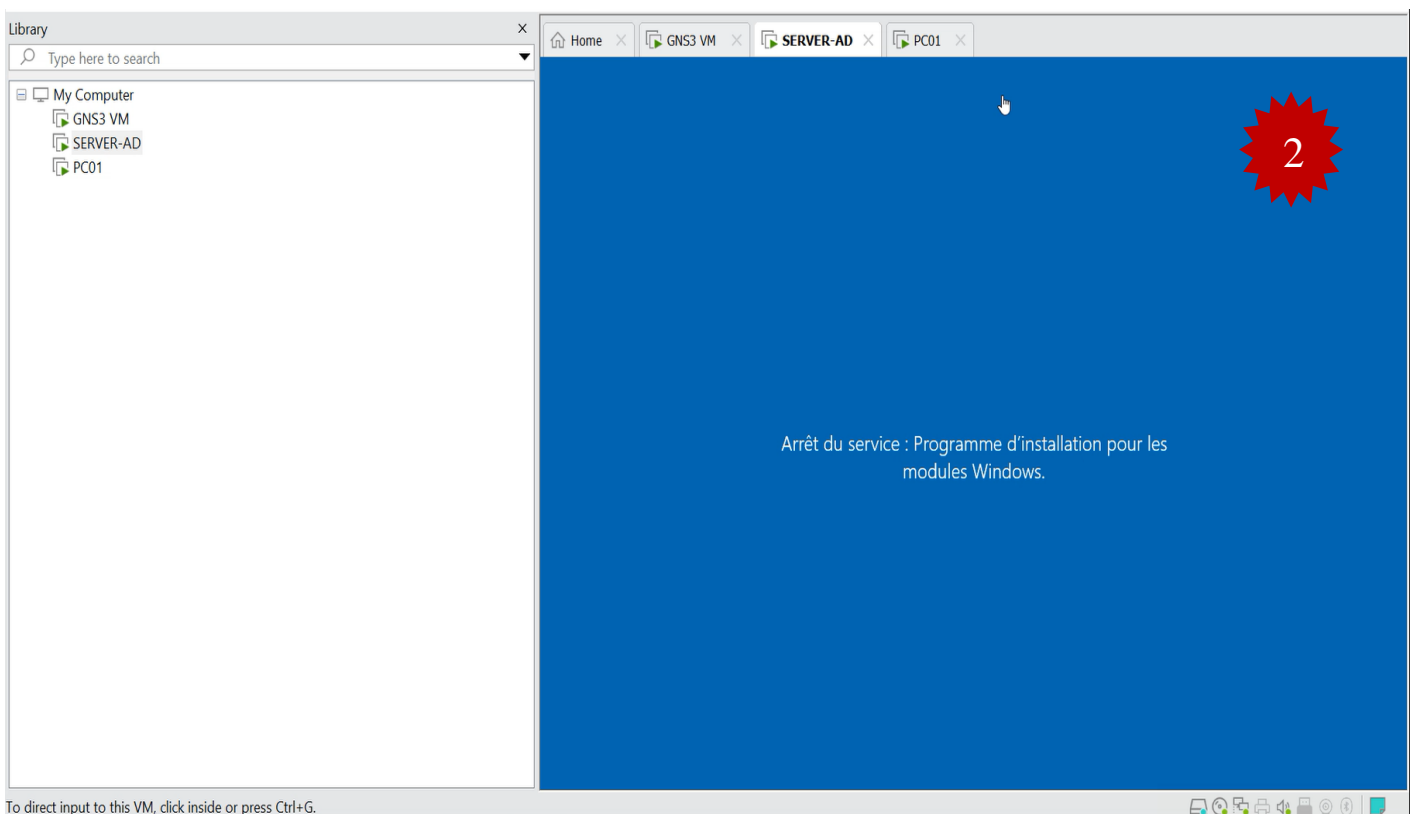
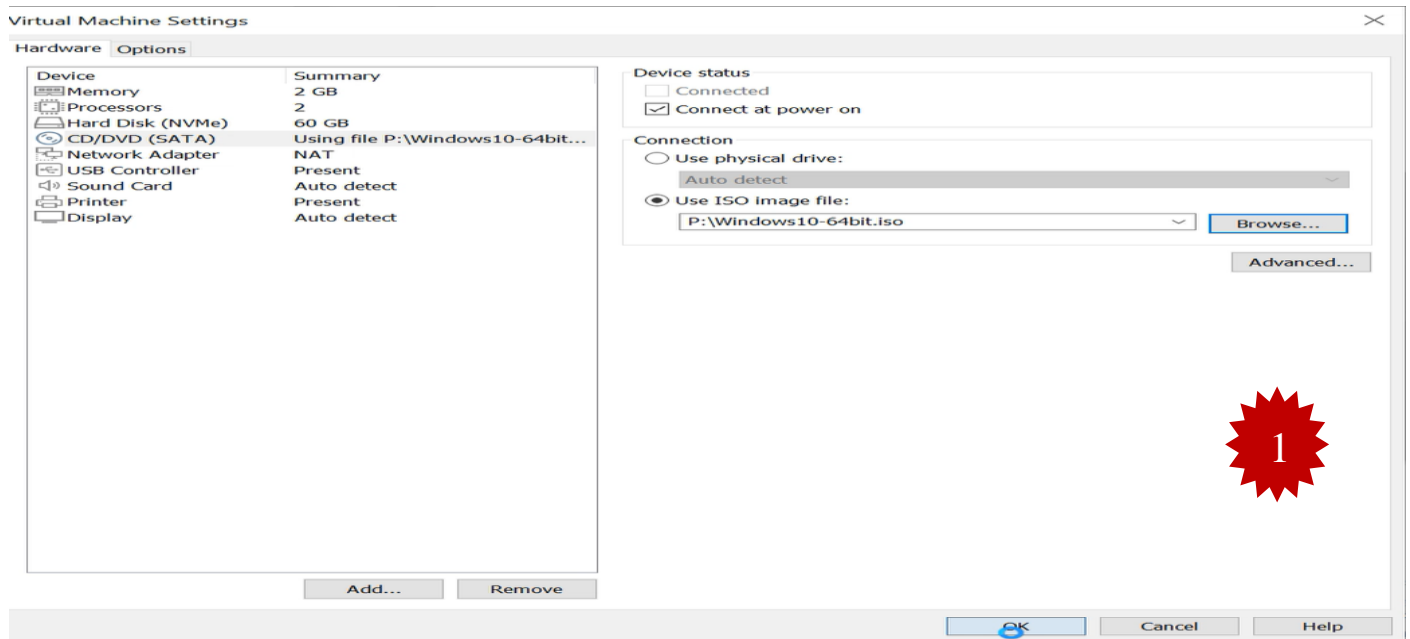
14

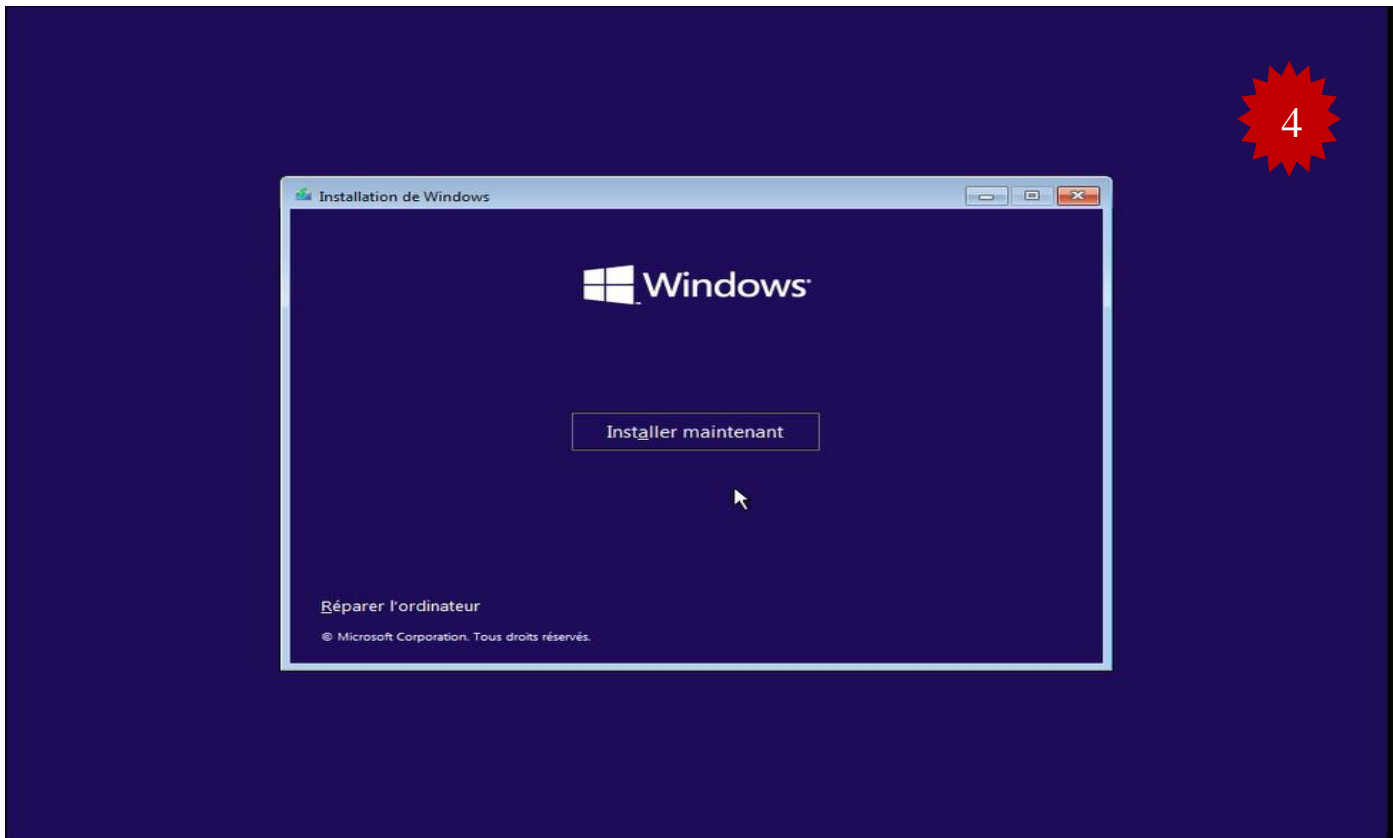
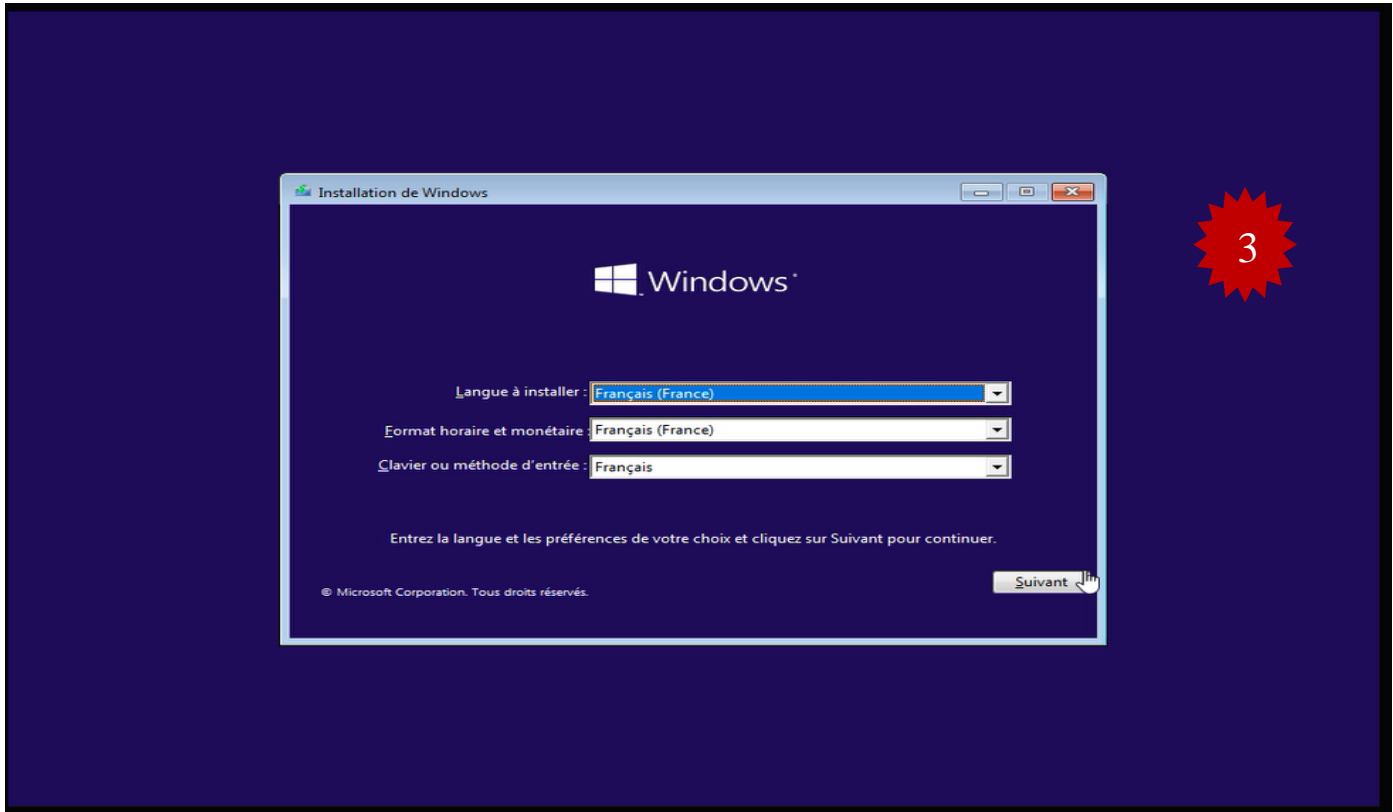
FIGURE IV.59 – Installation du Windows server 2022.

B. Installation du Windows 10 sous VMware Workstation

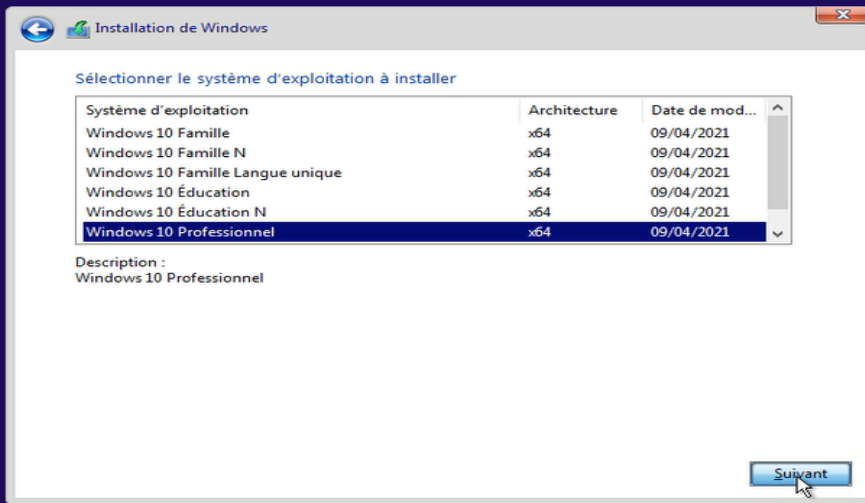
Après avoir ajouté l'image Windows 10 sur VMware, nous avons créé une machine. Les fonctionnalités suivantes sont attribuées :

- L'allocation de mémoire de la machine est fixée à 2 Go,
- Deux processeurs,
- Un disque dur de 60 Go.





5



1 Collecte des informations 2 Installation de Windows

6



1 Collecte des informations 2 Installation de Windows

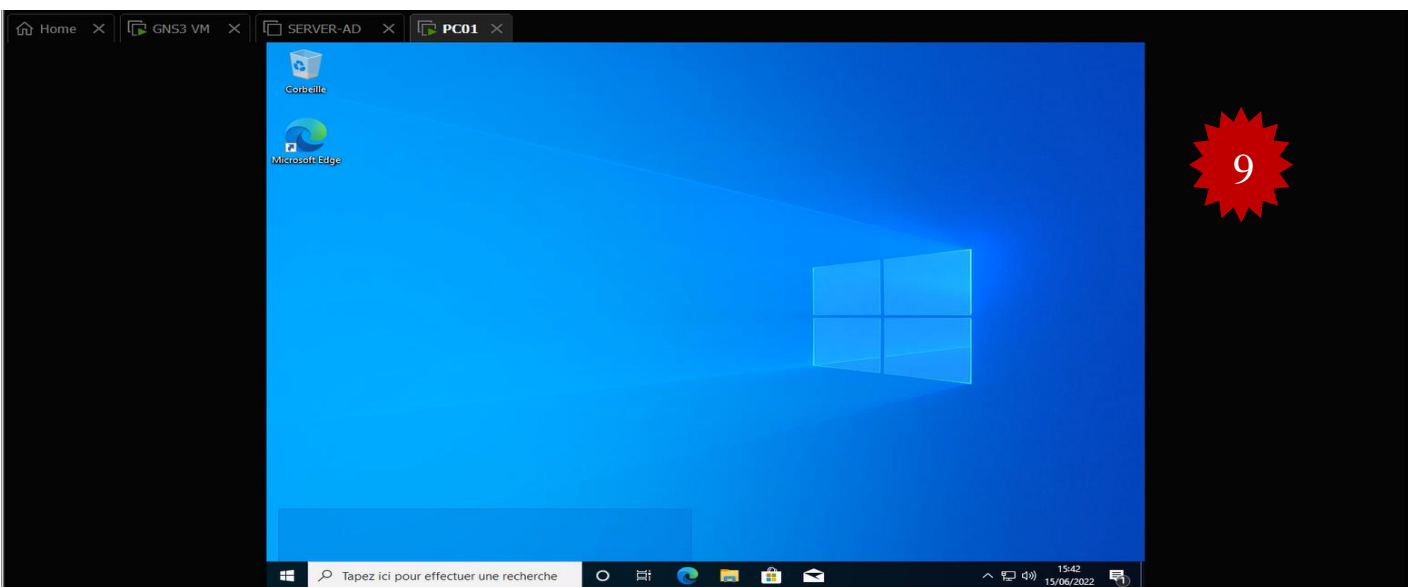
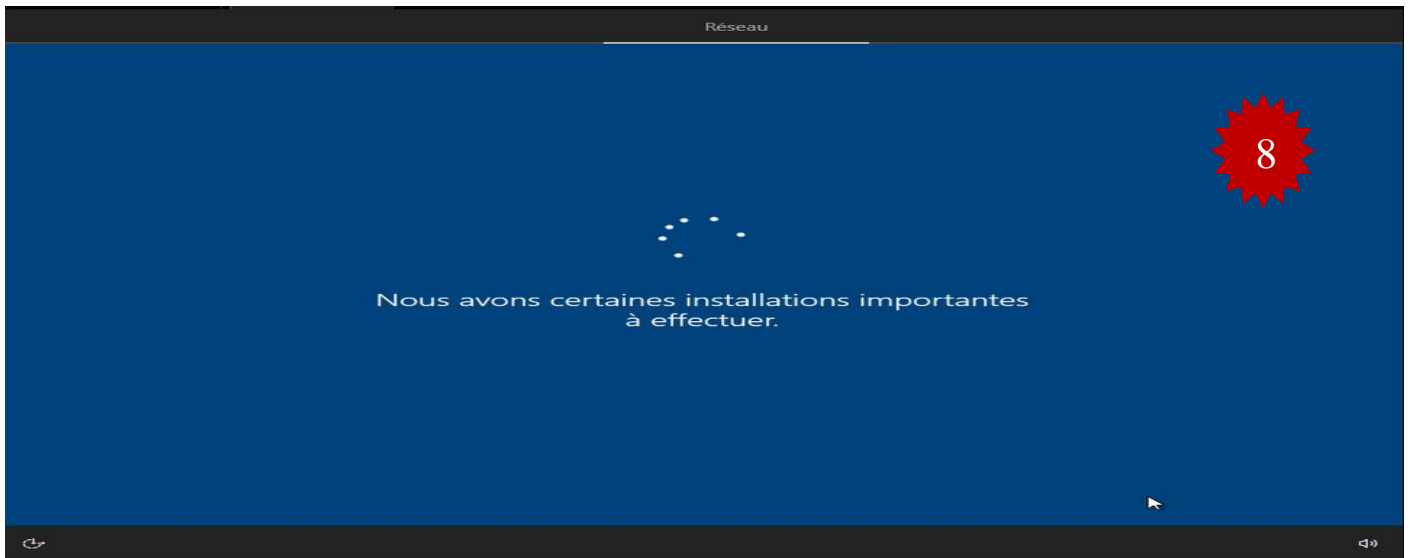
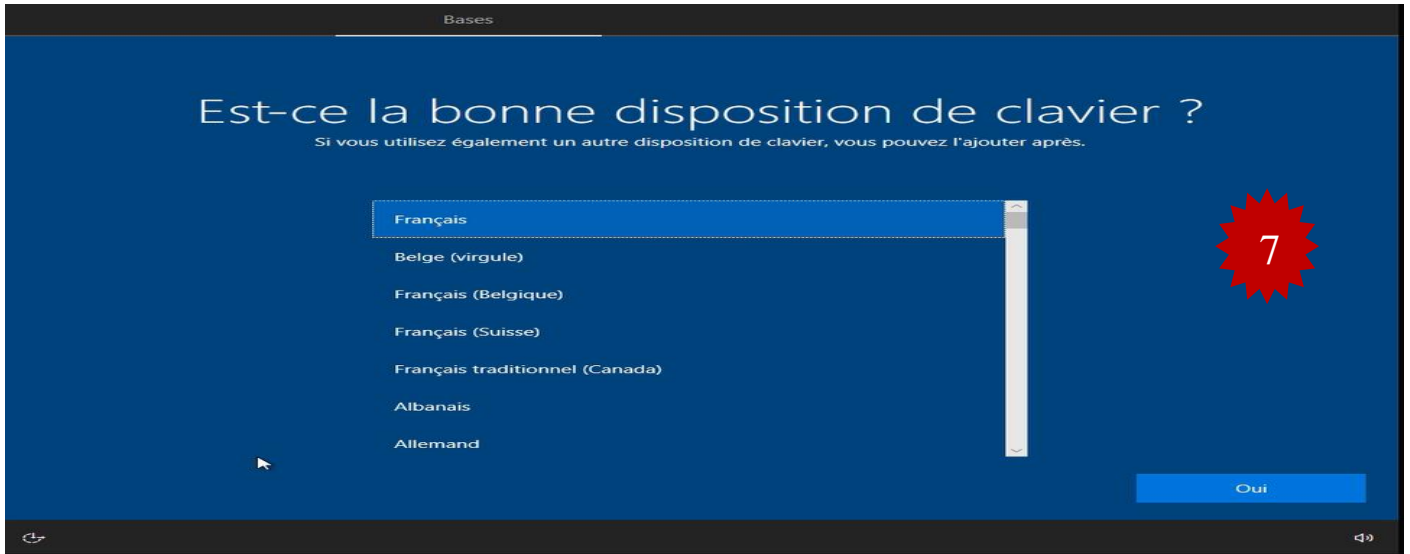
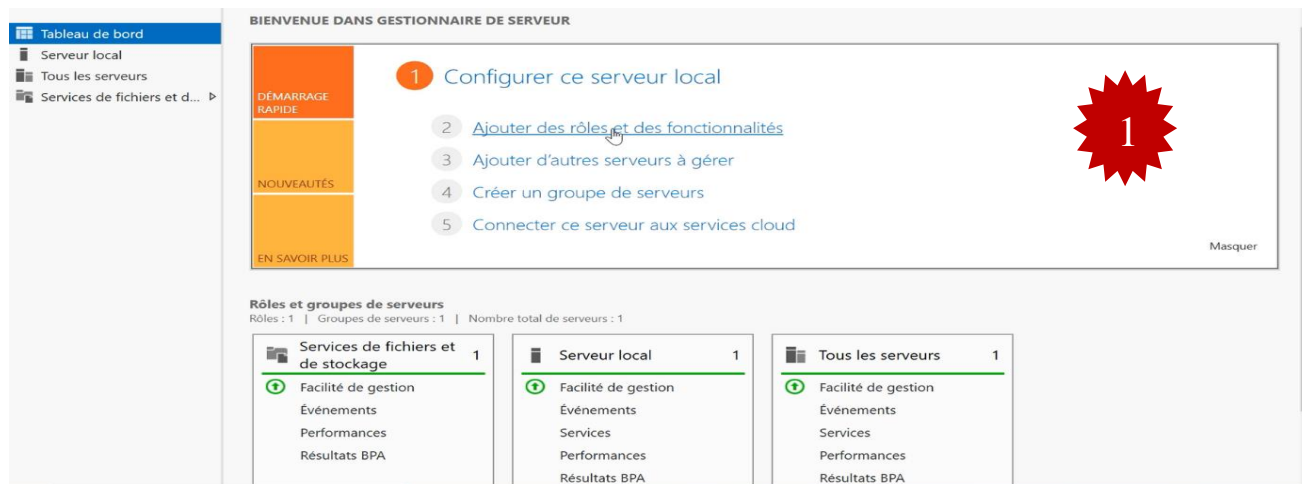


FIGURE IV.60 – Installation du Windows 10 sous VMware Workstation.

Annexe 4

A. Installation de l'Active Directory (AD)

Sur la machine Windows serveur 2016 nous avons installé un contrôleur de domaine dont le nom de domaine est campusnts.local. Pour commencer l'installation, il va falloir ajouter le Service de Role Active Directory. Lancer l'installation et ajouter les fonctionnalités qui nous manquent.



Sélectionner des fonctionnalités

Assistant Ajout de rôles et de fonctionnalités

SERVEREUR DE DESTINATION
SERVER-AD

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD DS

Confirmation

Résultats

Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

Fonctionnalités	Description
<input type="checkbox"/> Serveur de gestion des adresses IP (IPAM)	
<input type="checkbox"/> Serveur SMTP	
<input type="checkbox"/> Serveur WINS	
<input type="checkbox"/> Service d'activation des processus Windows	
<input type="checkbox"/> Service de migration du stockage	
<input type="checkbox"/> Service de recherche Windows	
<input type="checkbox"/> Service de réseau local sans fil	
<input type="checkbox"/> Service de transfert intelligent en arrière-plan (BITS)	
<input type="checkbox"/> Service SNMP	
<input type="checkbox"/> Services TCP/IP simples	
<input type="checkbox"/> Support de partage de fichiers SMB 1.0/CIFS	
<input type="checkbox"/> Support Hyper-V pour Host Guardian	
<input type="checkbox"/> Virtualisation de réseau	
<input type="checkbox"/> Windows Biometric Framework	
<input type="checkbox"/> Windows Identity Foundation 3.5	
<input checked="" type="checkbox"/> Windows PowerShell (1 sur 4 installé(s))	.NET Framework 4.8 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.
<input type="checkbox"/> Windows Server Migration Tools	
<input type="checkbox"/> Windows Subsystem for Linux	
<input checked="" type="checkbox"/> XPS Viewer (Installé)	

< Précédent Suivant > Installer Annuler

Confirmer les sélections d'installation

Assistant Ajout de rôles et de fonctionnalités

SERVEREUR DE DESTINATION
SERVER-AD

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD DS

Confirmation

Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Gestion de stratégie de groupe

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils AD DS et AD LDS

Module Active Directory pour Windows PowerShell

Outils AD DS

Centre d'administration Active Directory

Composants logiciels enfichables et outils en ligne de commande AD DS

Services AD DS

Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source

< Précédent Suivant > **Installer** Annuler

Progression de l'installation

Assistant Ajout de rôles et de fonctionnalités

SERVEREUR DE DESTINATION
SERVER-AD

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

AD DS

Confirmation

Résultats

Afficher la progression de l'installation

Installation de fonctionnalité

Configuration en cours. Installation réussie sur SERVER-AD.

Services AD DS

Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.

Promouvoir ce serveur en contrôleur de domaine

Gestion de stratégie de groupe

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils AD DS et AD LDS

Module Active Directory pour Windows PowerShell

Outils AD DS

Centre d'administration Active Directory

Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

< Précédent Suivant > **Fermer** Annuler

Configuration de déploiement

Assistant Configuration des services de domaine Active Directory

SERVEREUR CIBLE
SERVER-AD

Configuration de déploie...

Options du contrôleur de...

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner l'opération de déploiement

Ajouter un contrôleur de domaine à un domaine existant

Ajouter un nouveau domaine à une forêt existante

Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

En savoir plus sur les configurations de déploiement

< Précédent Suivant > Installer Annuler

Options du contrôleur de domaine

8

Configuration de déploiement...
Options du contrôleur de...
 Options DNS
 Options supplémentaires
 Chemins d'accès
 Examiner les options
 Vérification de la configur...
 Installation
 Résultats

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt : Windows Server 2016
 Niveau fonctionnel du domaine : Windows Server 2016

Spécifier les fonctionnalités de contrôleur de domaine

Serveur DNS (Domain Name System)
 Catalogue global (GC)
 Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :
 Confirmer le mot de passe :

En savoir plus sur les options pour le contrôleur de domaine

< Précédent **Suivant >** Installer Annuler

Options DNS

9

Configuration de déploiement...
 Options du contrôleur de...
Options DNS
 Options supplémentaires
 Chemins d'accès
 Examiner les options
 Vérification de la configur...
 Installation
 Résultats

Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable. Afficher plus

Spécifier les options de délégation DNS

Créer une délégation DNS

En savoir plus sur la délégation DNS

< Précédent **Suivant >** Installer Annuler

Options supplémentaires

10

Configuration de déploiement...
 Options du contrôleur de...
 Options DNS
Options supplémentaires
 Chemins d'accès
 Examiner les options
 Vérification de la configur...
 Installation
 Résultats

Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire.

Le nom de domaine NetBIOS : CAMPUSNTS

En savoir plus sur d'autres options

< Précédent **Suivant >** Installer Annuler

Vérification de la configuration requise

11

Configuration de déploiement...
 Options du contrôleur de...
 Options DNS
 Options supplémentaires
 Chemins d'accès
 Examiner les options
Vérification de la configur...
 Installation
 Résultats

Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer. Afficher plus

La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur

Réexécuter la vérification de la configuration requise

⬆ Voir les résultats

⚠ Les contrôleurs de domaine Windows Server 2022 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.

Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (http://go.microsoft.com/fwlink/?LinkId=104751).

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est introuvable ou elle n'exécute pas le serveur DNS Windows. Si vous procédez à l'intégration avec une infrastructure DNS existante, vous devez

⚠ Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.

En savoir plus sur les conditions préalables

< Précédent **Suivant >** Installer Annuler

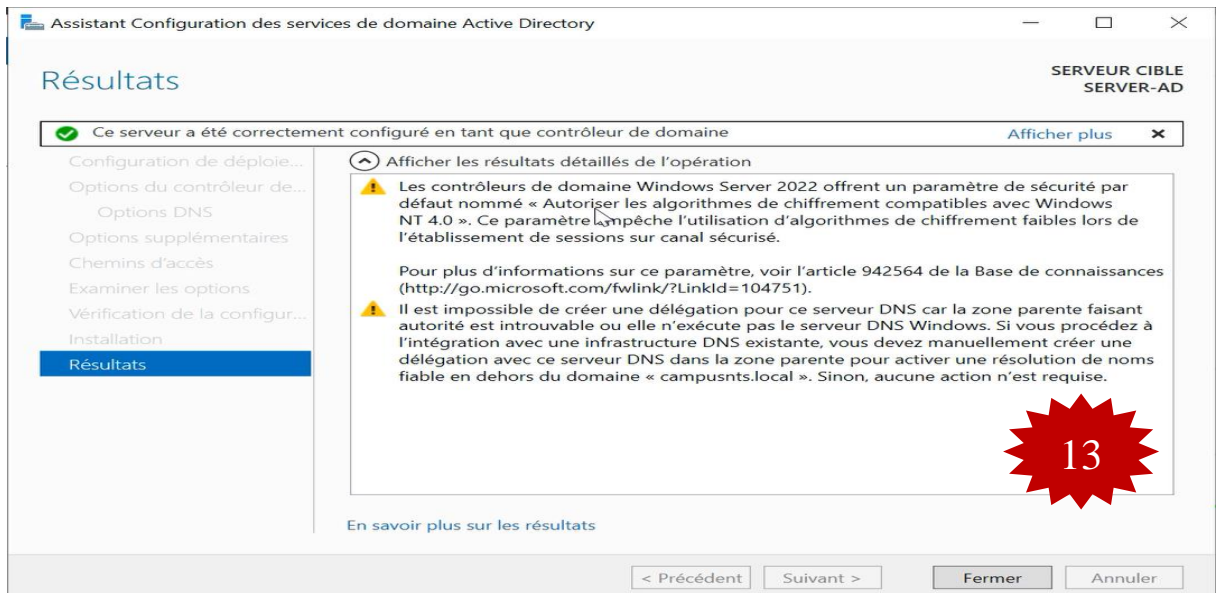
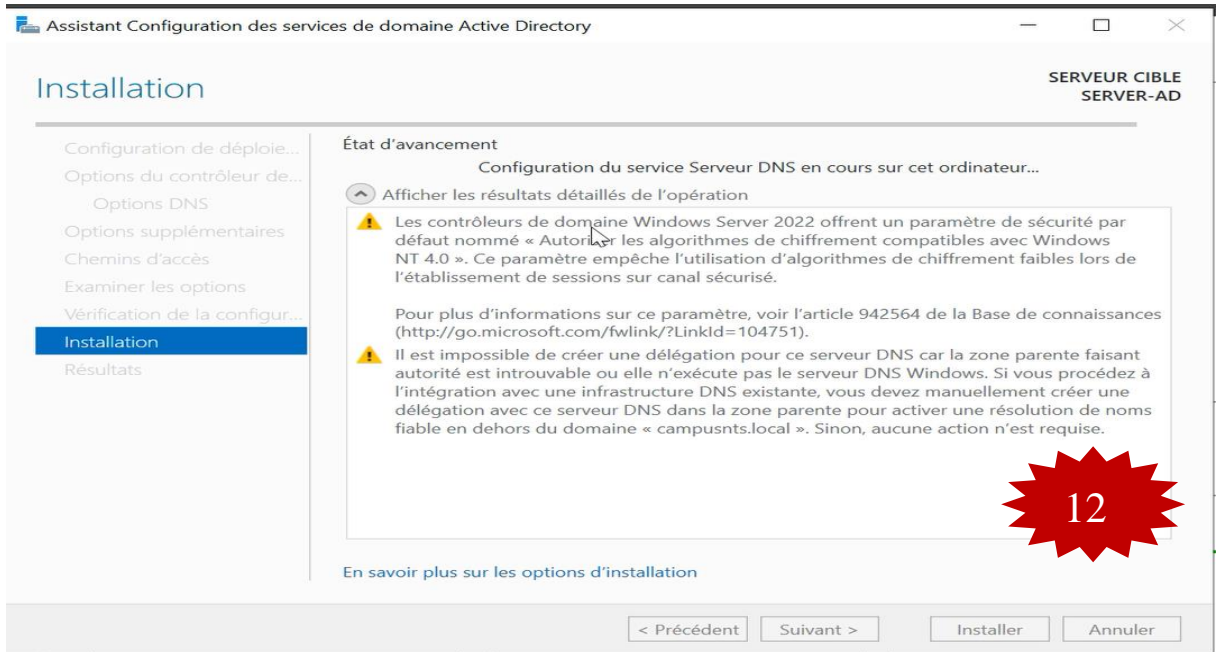
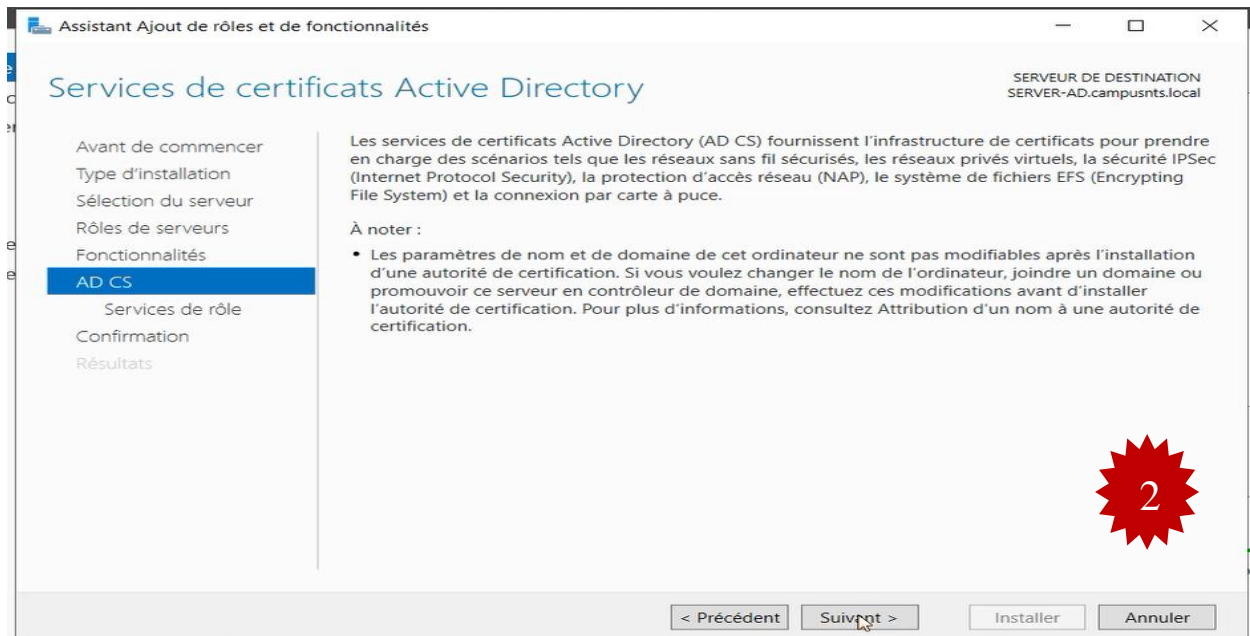
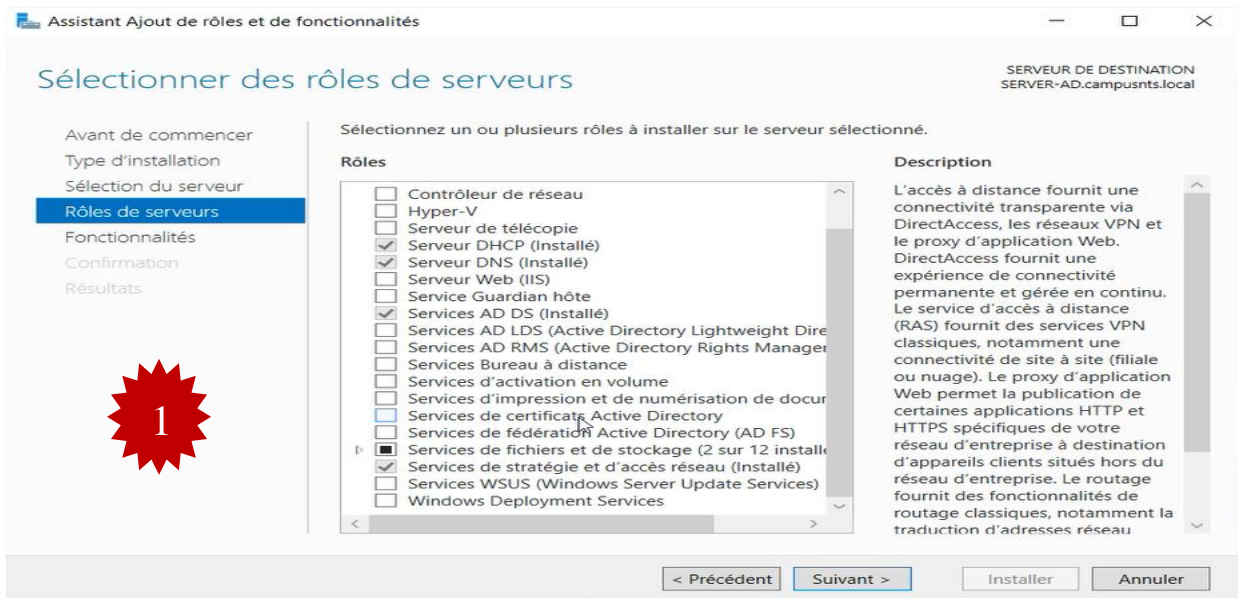


FIGURE IV.61 – L'installation de l'Active Directory.

B. Certificat de l'Active Directory

Le déploiement d'une autorité de certification en installant le rôle « Active Directory Certificate Services (AD CS) » nous a permis de protéger de nombreux services qui ne sont librement accessibles que depuis les ordinateurs de l'entreprise. La procédure à suivre est la suivante :



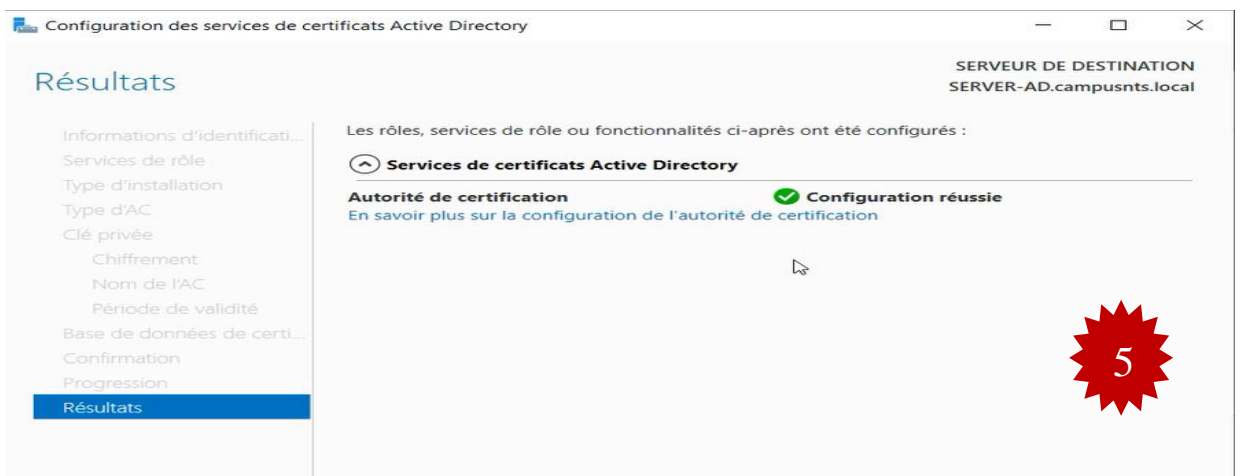
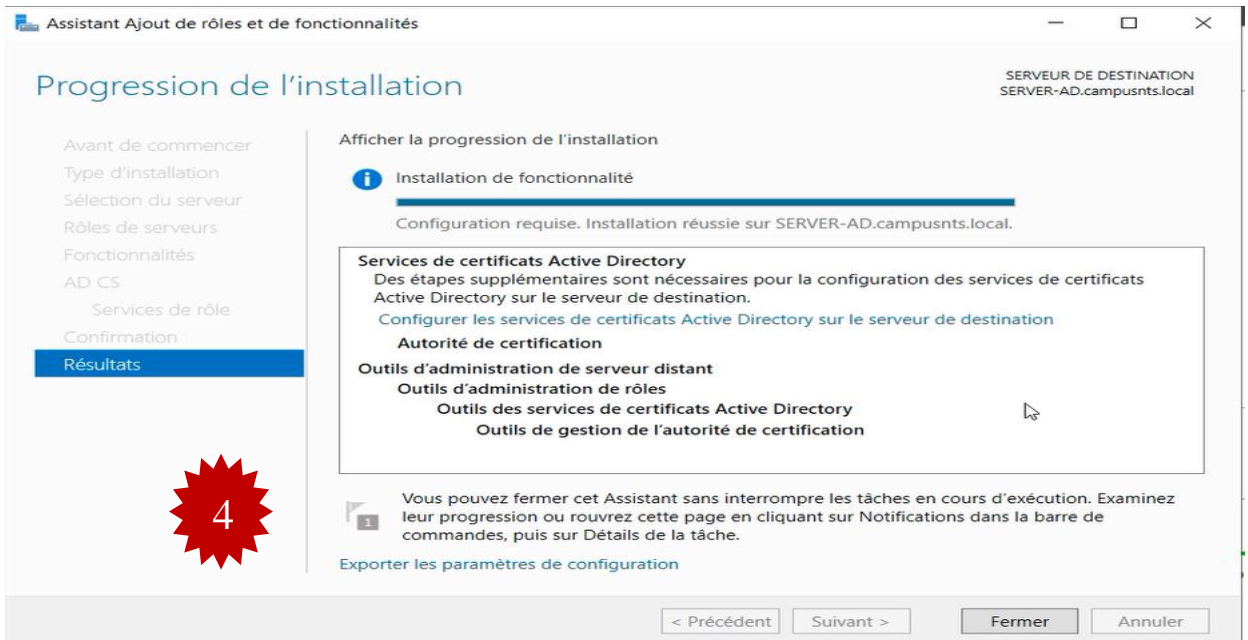
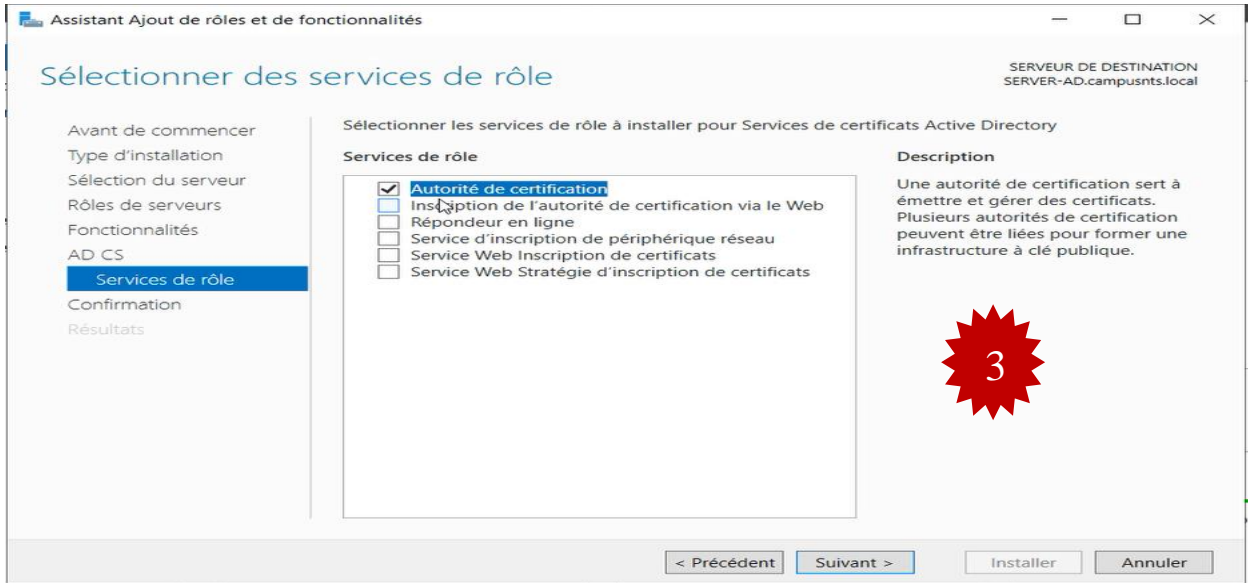


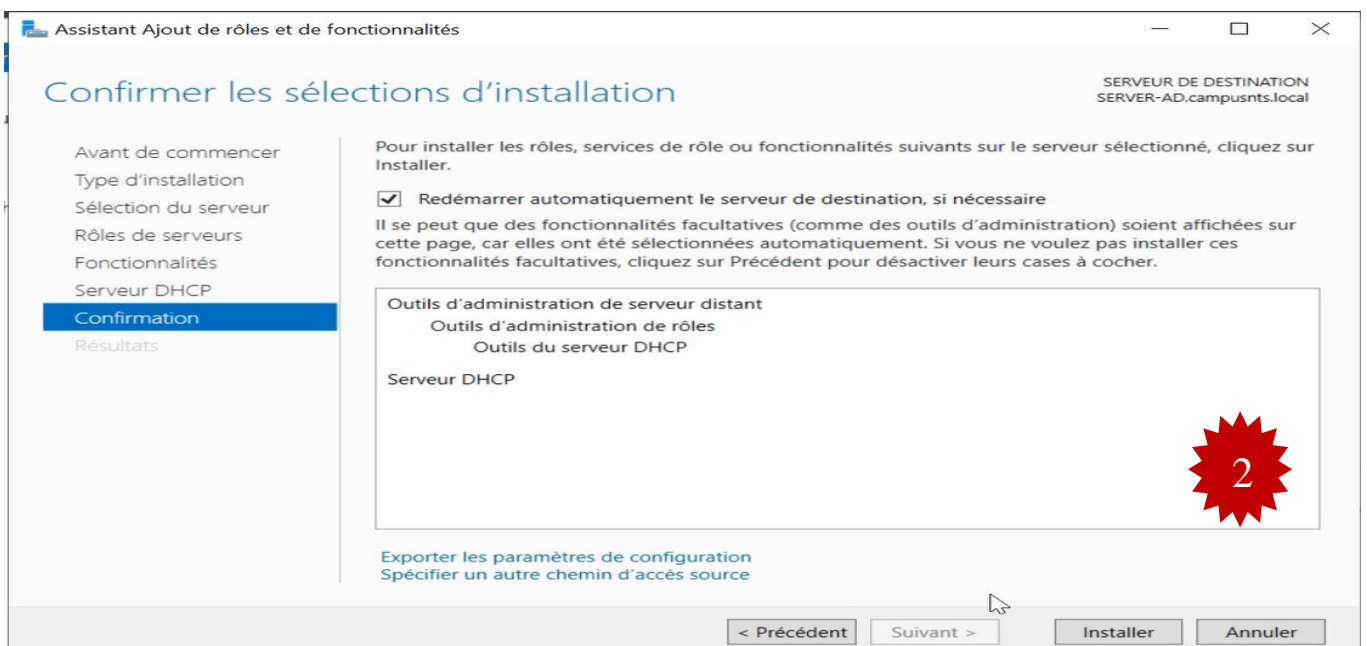
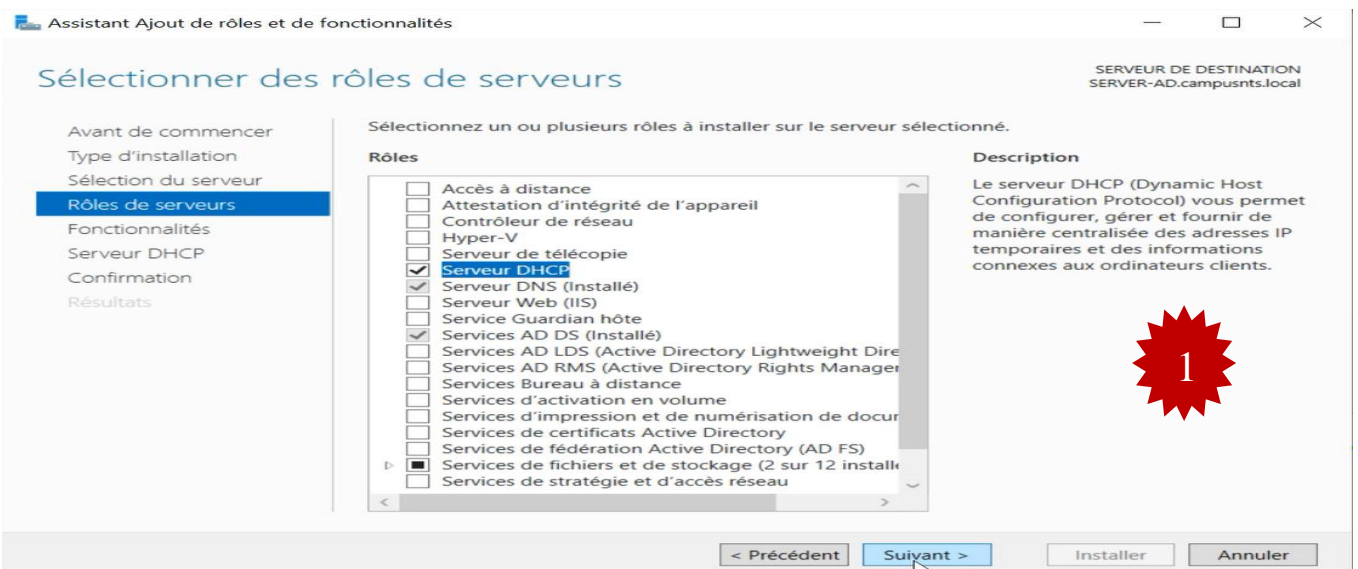
FIGURE IV.62 – Certificat de l'Active Directory.

Annexe 5

Installation de Dynamics Host Configuration Protocol (DHCP)

Dans cette partie nous allons installer DHCP serveur et nous ajoutons ses fonctionnalités par la suite nous allons dans :

- Serveur dhcp campusnts.local.
- IPV4.
- Création de Nouvelle étendu.
- La figure ci-dessous montre les étendus des vlans créés.



Assistant Ajout de rôles et de fonctionnalités

Progression de l'installation

SEVEUR DE DESTINATION
SERVER-AD.campusnts.local

3

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DHCP
Confirmation
Résultats

Afficher la progression de l'installation

Installation de fonctionnalité

Configuration requise. Installation réussie sur SERVER-AD.campusnts.local.

Serveur DHCP
Lancer l'Assistant Post-installation DHCP
Terminer la configuration DHCP

Outils d'administration de serveur distant
Outils d'administration de rôles
Outils du serveur DHCP

Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

< Précédent Suivant > Fermer Annuler

Assistant Configuration post-installation DHCP

Autorisation

4

Description

Autorisation

Résumé

Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.

Utiliser les informations d'identification de l'utilisateur suivant

Nom d'utilisateur : CAMPUSNTS\Administrateur

Utiliser d'autres informations d'identification

Nom d'utilisateur : Spécifier...

Ignorer l'autorisation AD

< Précédent Suivant > Valider Annuler

Assistant Configuration post-installation DHCP

Résumé

5

Description

Autorisation

Résumé

L'état des étapes de configuration post-installation est indiqué ci-dessous :

Création des groupes de sécurité Terminé

Redémarrez le service Serveur DHCP sur l'ordinateur cible pour que les groupes de sécurité soient effectifs.

Autorisation du serveur DHCP Terminé

< Précédent Suivant > Fermer Annuler

Gestionnaire de serveur

Tableau de bord

1 Configurer ce serveur local

2 Ajouter des rôles et des fonctionnalités

3 Ajouter d'autres serveurs à gérer

4 Créer un groupe de serveurs

5 Connecter ce serveur aux services cloud

Rôles et groupes de serveurs

Rôles : 4 | Groupes de serveurs : 1 | Nombre total de serveurs : 1

AD DS 1	DHCP 1	DNS 1
Facilité de gestion	Facilité de gestion	Facilité de gestion
Événements	Événements	Événements
Services	Services	Services
Performances	Performances	Performances
Résultats BPA	Résultats BPA	Résultats BPA

6

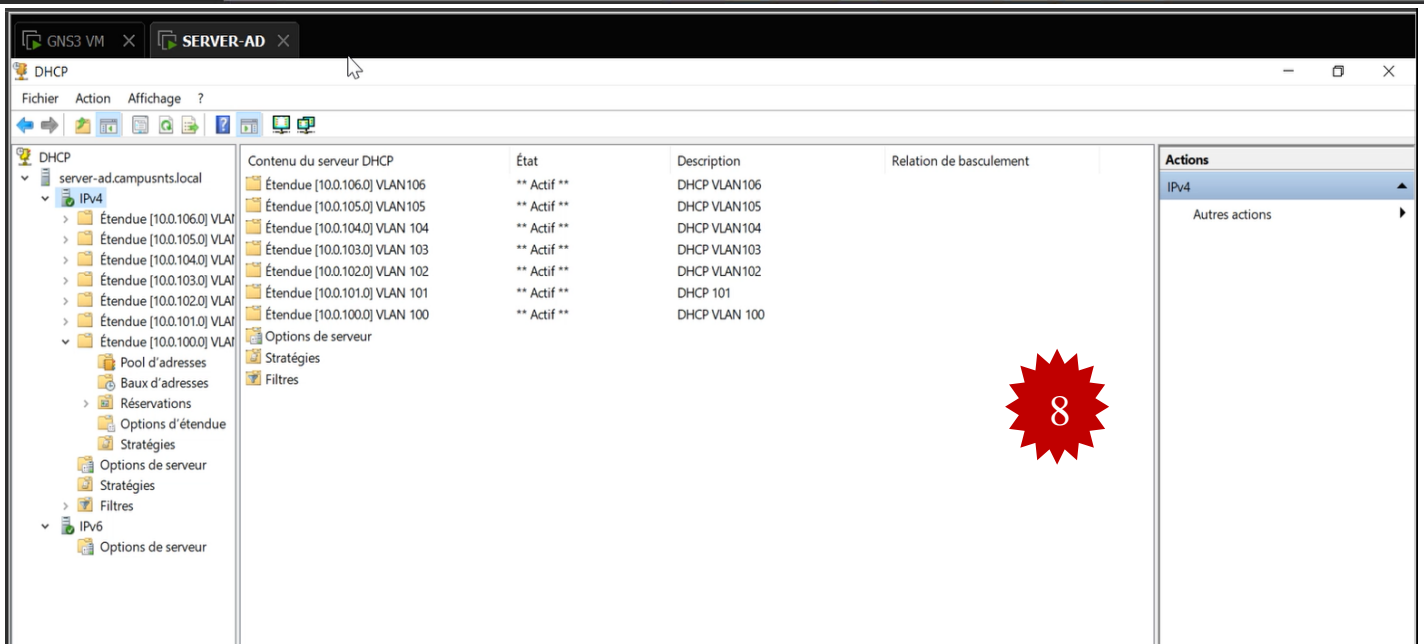
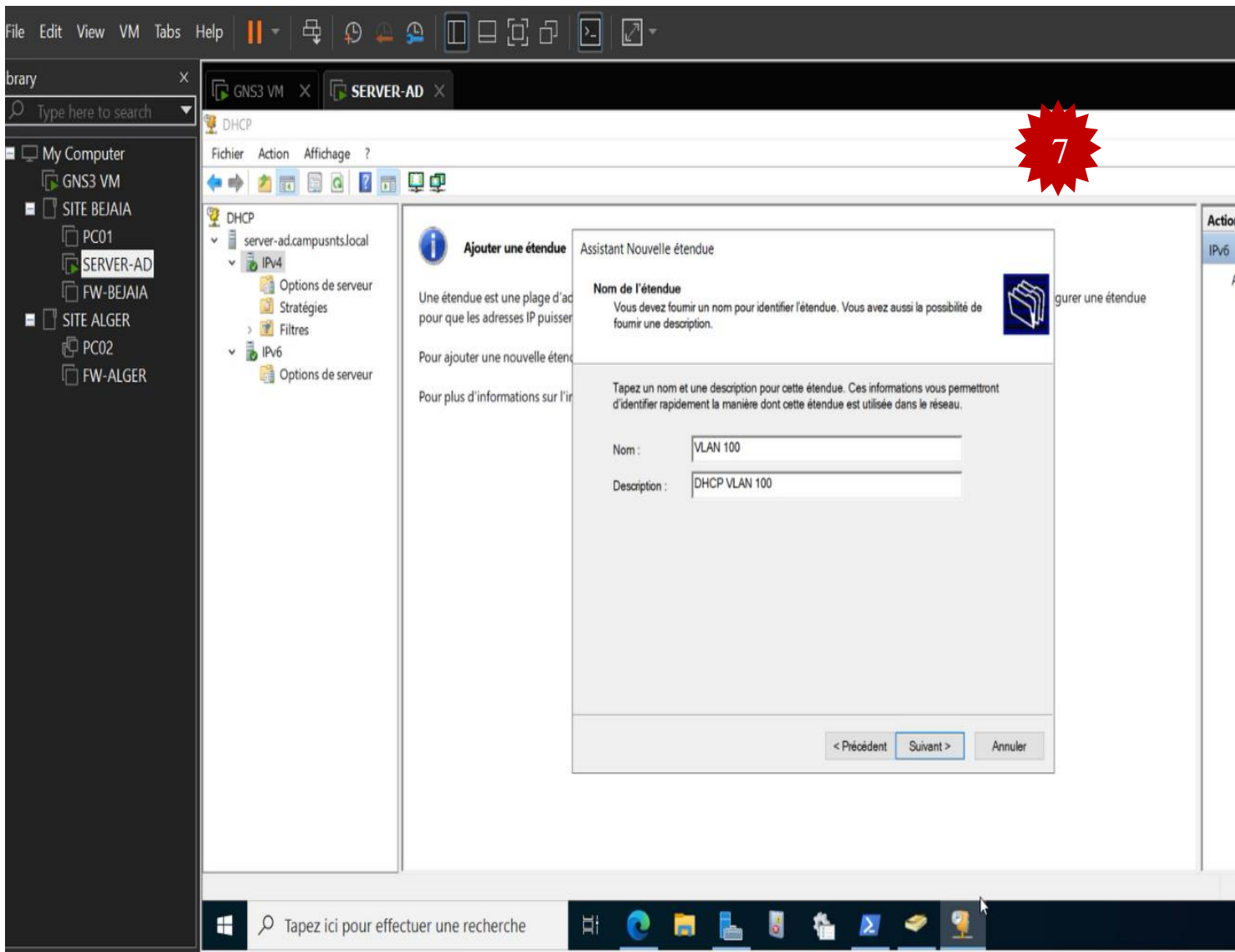
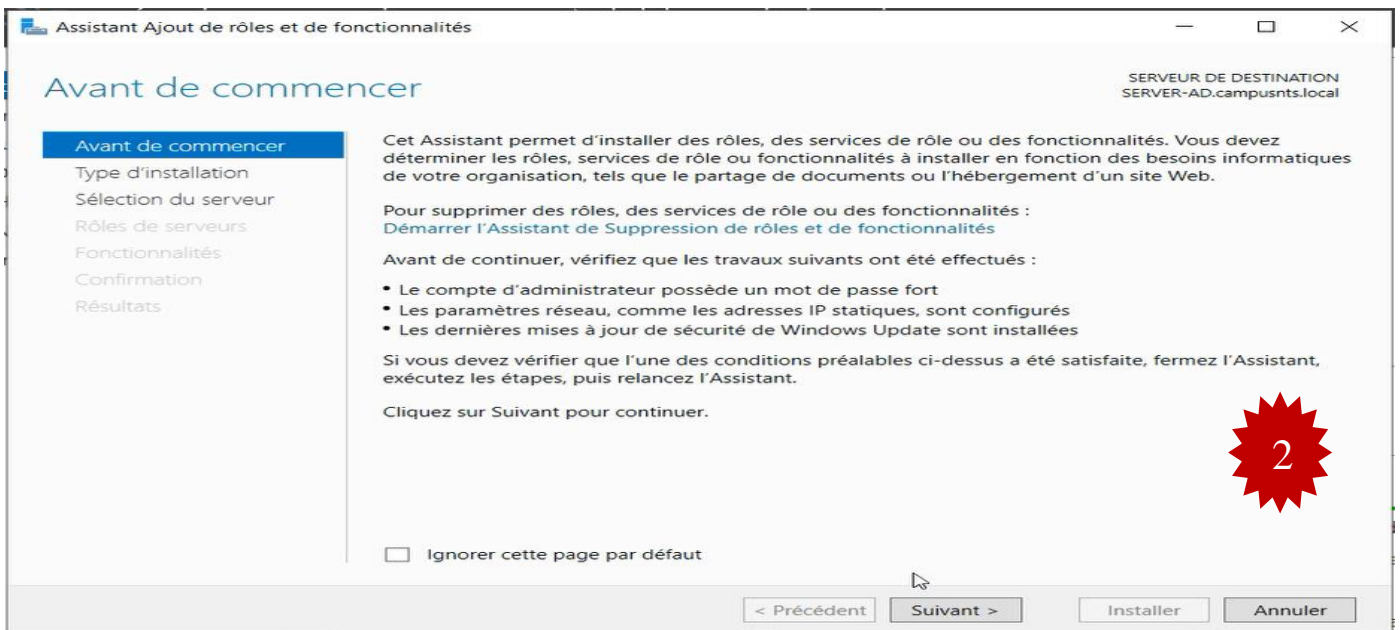
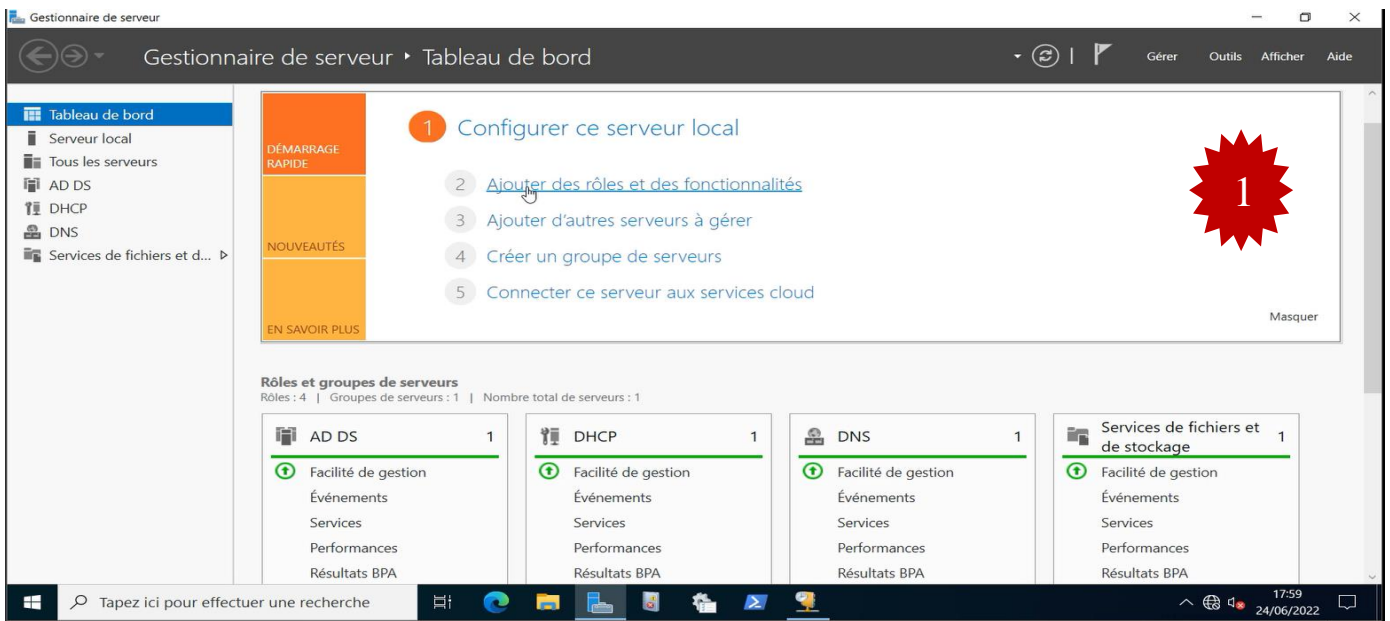


FIGURE IV.63 – Installation de Dynamics Host Configuration Protocol.

Annexe 6

Installation du rôle NPS « Serveur radius »

On installe le serveur radius sur le même serveur Windows2022 comme la montre la figure qui suit :



Sélectionner le type d'installation

SERVEREUR DE DESTINATION
SERVER-AD.campusnts.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

Installation basée sur un rôle ou une fonctionnalité
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

Installation des services Bureau à distance
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

3

< Précédent Suivant > Installer Annuler

Sélectionner des rôles de serveurs

SERVEREUR DE DESTINATION
SERVER-AD.campusnts.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles	Description
<input type="checkbox"/> Contrôleur de réseau	Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Serveur de télécopie	
<input checked="" type="checkbox"/> Serveur DHCP (Installé)	
<input checked="" type="checkbox"/> Serveur DNS (Installé)	
<input type="checkbox"/> Serveur Web (IIS)	
<input type="checkbox"/> Service Guardian hôte	
<input checked="" type="checkbox"/> Services AD DS (Installé)	
<input type="checkbox"/> Services AD LDS (Active Directory Lightweight Directory Services)	
<input type="checkbox"/> Services AD RMS (Active Directory Rights Management Services)	
<input type="checkbox"/> Services Bureau à distance	
<input type="checkbox"/> Services d'activation en volume	
<input type="checkbox"/> Services d'impression et de numérisation de documents	
<input type="checkbox"/> Services de certificats Active Directory	
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input checked="" type="checkbox"/> Services de fichiers et de stockage (2 sur 12 installés)	
<input checked="" type="checkbox"/> Services de stratégie et d'accès réseau	
<input type="checkbox"/> Services WSUS (Windows Server Update Services)	
<input type="checkbox"/> Windows Deployment Services	

4

< Précédent Suivant > Installer Annuler

Confirmer les sélections d'installation

SERVEREUR DE DESTINATION
SERVER-AD.campusnts.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Services de stratégie et d'

Confirmation

Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Cliquez sur les boutons de sélection pour sélectionner ou désélectionner ces fonctionnalités facultatives.

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils de la stratégie réseau et des services d'accès

Services de stratégie et d'accès réseau

! Si un redémarrage est nécessaire, ce serveur redémarrera automatiquement sans notification supplémentaire. Voulez-vous autoriser les redémarrages automatiques ?

Oui Non

Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source

5

< Précédent Suivant > Installer Annuler

Progression de l'installation

SERVEREUR DE DESTINATION
SERVER-AD.campusnts.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Services de stratégie et d'

Résultats

Afficher la progression de l'installation

1 Installation de fonctionnalité

Installation démarrée sur SERVER-AD.campusnts.local

Outils d'administration de serveur distant

Outils d'administration de rôles

Outils de la stratégie réseau et des services d'accès

Services de stratégie et d'accès réseau

Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou ouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

Exporter les paramètres de configuration

6

< Précédent Suivant > Fermer Annuler

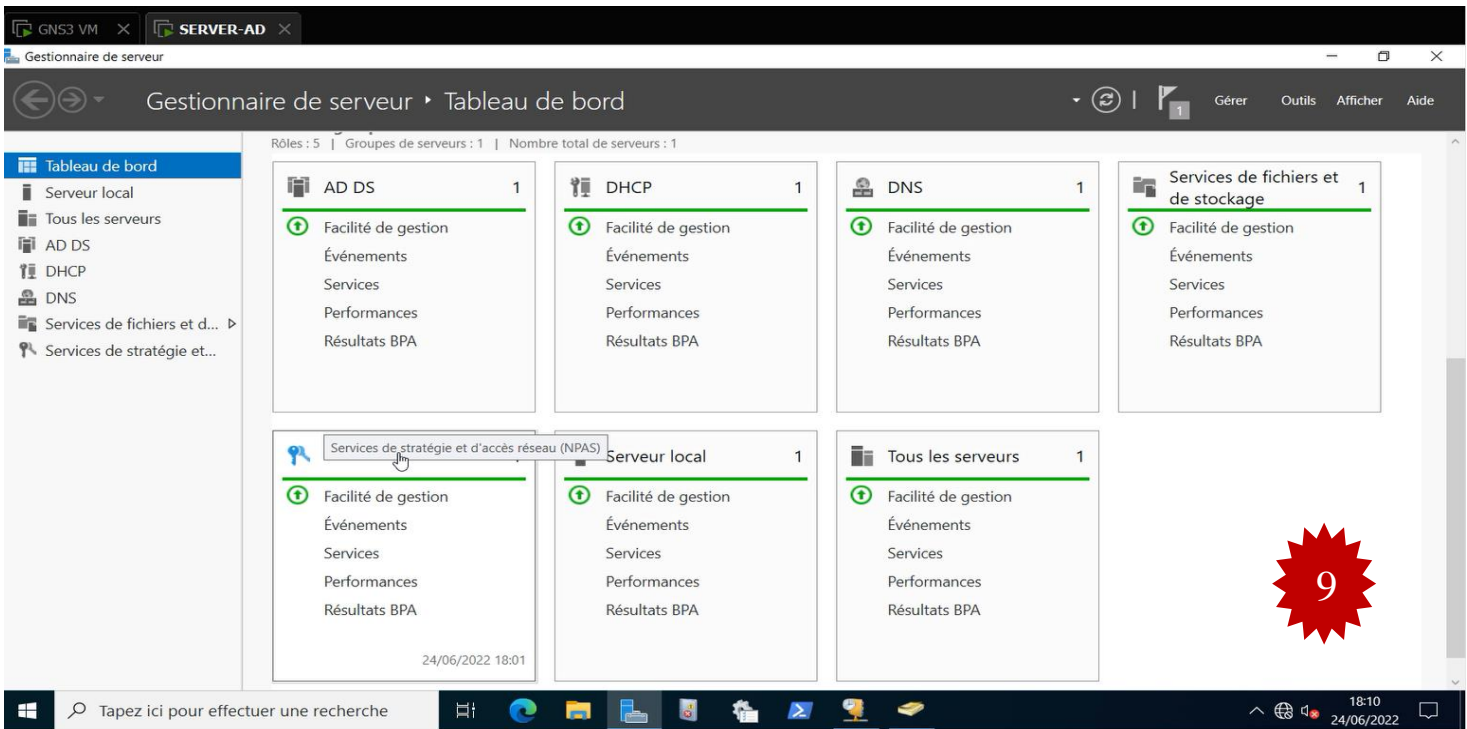
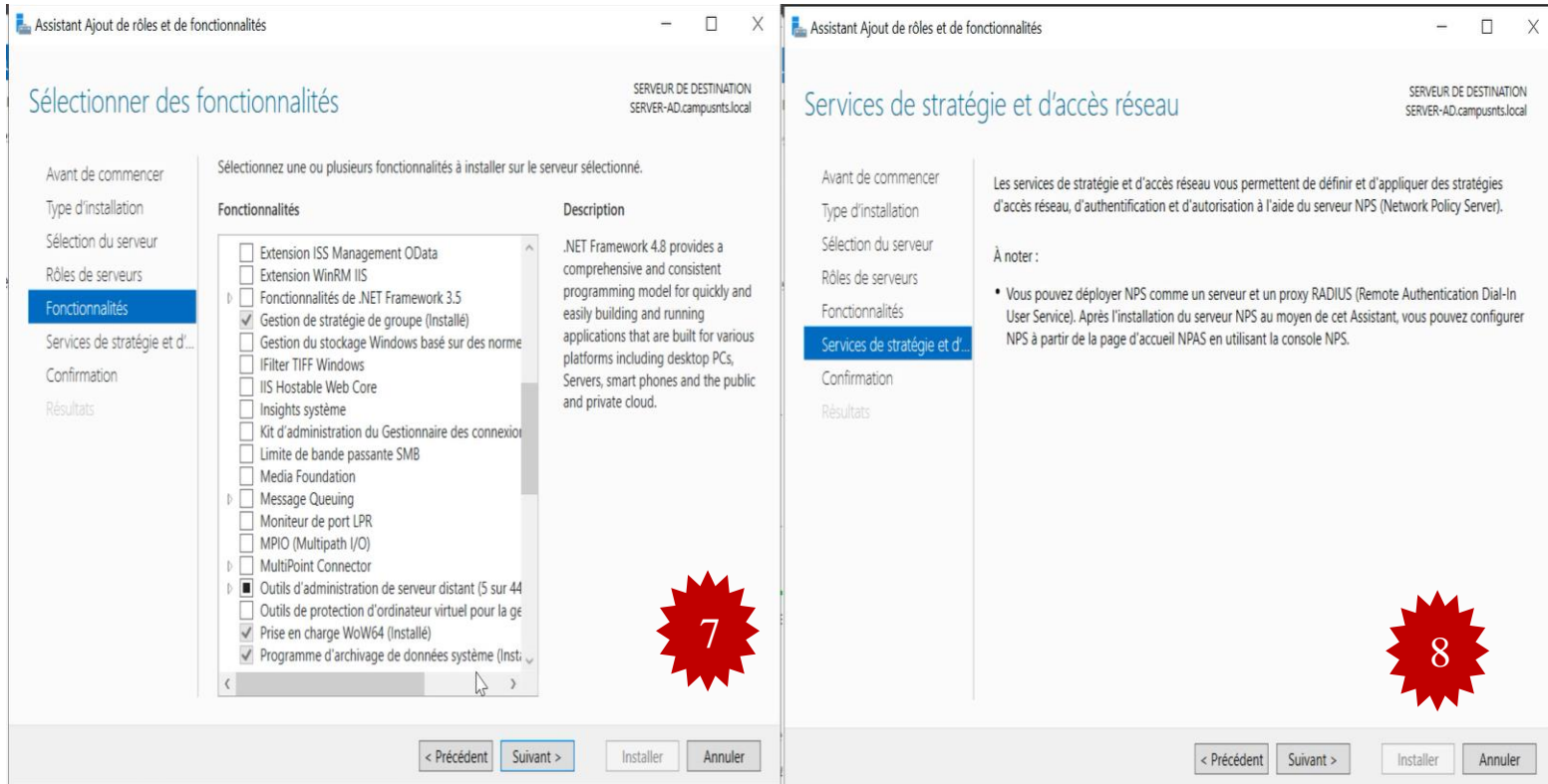


FIGURE IV.64 – L'installation du rôle NPS.

Après, on va inscrire notre serveur NPS « serveur radius » avec notre base de données L.D.A.Pde notre active directory afin d'authentifier les ports avec ce dernier.

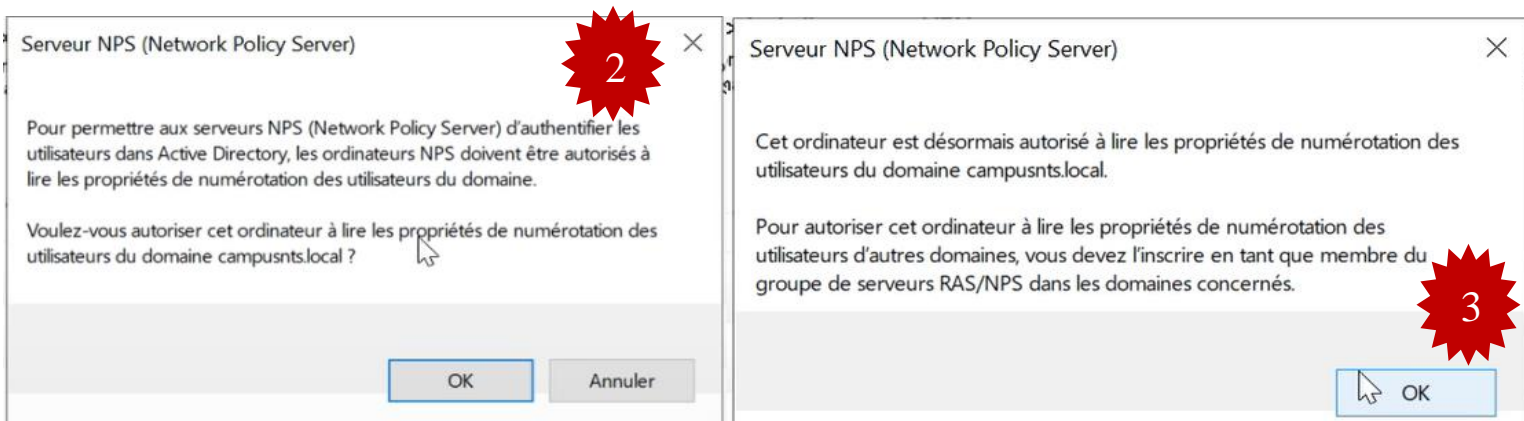
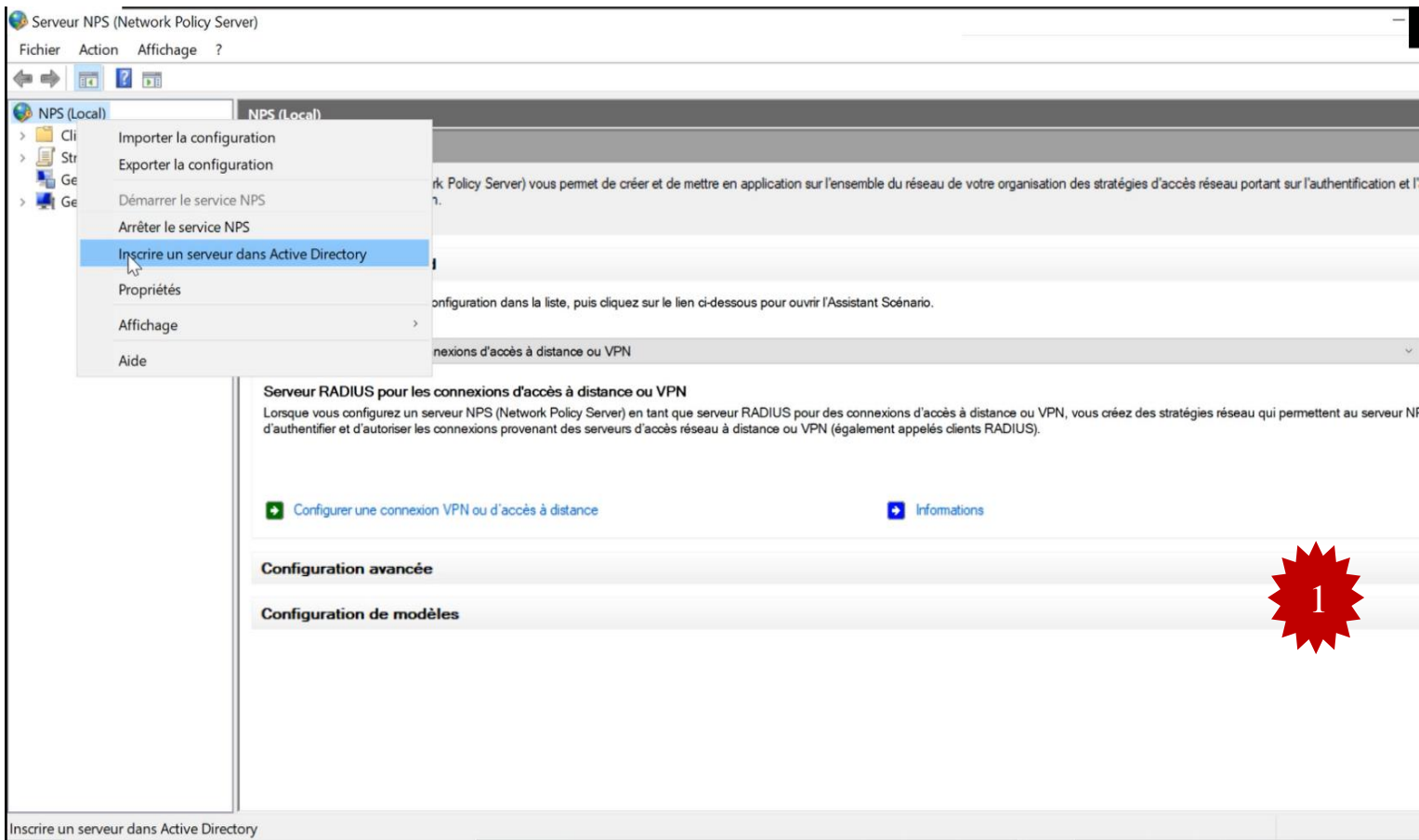


FIGURE IV.65 – Inscription radius avec active directory.

Annexe 7

Installation Firewall Sophos UTM

Pour les deux sites Alger et Béjaïa, on installe les deux machines virtuelles Sophos UTMversion18.



FIGURE IV.66 – Installation Firewall Sophos UTM.

BIBLIOGRAPHIE

- [1] *M^{elle} R. Tinhinan , M^{elle} S Fadhila , Mémoire de fin d'études en master 2 réseaux et télécommunications : «Etude et Mise en place d'un réseau VPN », UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU,2017.*
- [2] *M^r R. Mohammed, Réseaux Informatiques,2010-2011.*
- [3] *M^r O. Salvatori, Initiation aux réseaux, Éditions Eyrolles 2001, p 448.*
- [4] *M^r A. Moussaoui, Réseau de communication, Page Bleus internationale, Novembre2017, p 298.*
- [5] *M^r R. Manandrify, Mémoire de fin d'études en licenceès sciences techniques en télécommunication : « Sécurisation des réseaux informatiques sous linux », UNIVERSITE D'ANTANANARIVO, 2009.*
- [6] *M^r B. Said, Support de cours réseaux de communication Pour 2ème Année Licence informatique, UNIVERSITE 8 mai 1945- Guelma, p68.*
- [7] *M^r R. Mohamed Amine, Notions de Base en réseaux et systèmes de télécommunication, 2021 , UNIVERSITE MHAMED BOUGARA (BOUMERDES) , p 94.*
- [8] *M^{elle} M. Miharimanana ,Mémoire de fin d'études en télécommunications : « Sécurisation des reseaux vpn avec ipsec et Radius, UNIVERSITE D'ANTANANARIVO, 2013.*
- [9] *M^{elle} S.Mbacké DIENE, Mémoire de fin d'études en génie logiciel : «Conception et Implémentation d'une architecturesécurisée d'un réseau d'entreprise sur plusieurs sites » , UNIVERSITE assane seck de ziguinchor, 2021.*
- [10] *M^r A Sadiqui, Sécurités des réseaux informatiques , collection informatique, ltd 2019 , p 265.*
- [11] *M^{elle} C. Sarra ,Mémoire de Master 2 en Réseaux et Sécurité : La protection des réseaux contre les attaques DOS, Université Mohamed Seddiki Ben Yahia de Jijel,2020,*
- [12] *M^r B.Benmammar, Gestion et Contrôle intelligents des réseaux, éditions ltd 2020 , p295.*

- [13] M^r d. Godard, sécurité informatique 2^e édition, 2005. P 469.
- [14] M^{elle} S. lalia, *Mémoire de master 2 en réseaux : « Attaques informatique »*, UNIVERSITE DE M'SILA , 2015,
- [15] M^r C. Liorens , M^r L. Levier , M^r D. Valois, *Tableaux de bord de la sécurité réseau* , Eyrolles 2003 ,2e édition, p559.
- [16] M^r _S. Idir, *MEMOIRE de Master 2 en informatique 2: « Les attaques par déni de service distribué dans les systèmes informatiques*, Université Abderrahmane Mira de Bejai,2017.
- [17] M^r R. Yende , *SUPPORT DE COURS DE SÉCURITÉ INFORMATIQUE ET CRYPTO*, Congo-Kinshasa. 2018. ffccl-01965300, p139.
- [18] *La sécurité informatique* , Edition Livres pour tous (www.livrespourtous.com).
- [19] M^r D. Fernandes, M^r P. Amadou Sarr, *La protection des réseaux contre les attaques DOS*, Mai 2010, p32.