

Département : Informatique

Filière : Administration des Réseaux Informatiques

RAPPORT DE PROJET DE FIN D'ETUDES

Mise en place d'un réseau sécurisé au sein d'une entreprise

Soutenance : 13/04/2023 à partir de 10H30

Réalisé par :

- **EL OTMANI Hiba**
- **MOUNOUAR Abderrahim**
- **SOTIH Mohammed Amine**

Encadré par : Mr. BADAoui

Jury :

- Pr. AMRAOUI
Pr. BADAoui
Pr. BOUHADDOUR
Pr. ELHAZITI

Résumé

Nous avons réalisé un projet de fin d'études qui consistait à mettre en place un réseau informatique sécurisé dans une entreprise et à le superviser.

Notre projet incluait plusieurs aspects tels que la conception de l'architecture du réseau informatique, la virtualisation des serveurs, la mise en place d'un portail captif pour l'authentification des utilisateurs internes (admins, employés), l'installation d'un VPN pour la zone dématérialisée DMZ et la mise en place de services offrant un accès aux utilisateurs externes, tels que le service web. Nous avons également effectué une étude comparative des différentes solutions de supervision informatique disponibles et avons choisi l'outil de supervision qui répondait le mieux à nos besoins.

Abstract

We completed a final year project which involved setting up a secure computer network in a company and supervising it. Our project covered several aspects such as designing the computer network architecture, server virtualization, implementing a captive portal for internal user authentication (admins, employees), installing a VPN for the demilitarized zone (DMZ), and setting up services that provide external users access, such as web services. We also conducted a comparative study of different available IT supervision solutions and selected the supervision tool that best met our needs.

Remerciements

Il nous est agréable de saisir l'occasion pour présenter nos remerciements à tous ceux qui ont contribué de près ou de loin à l'aboutissement de notre PFE.

Nous tenons à exprimer notre gratitude la plus sincère à **Mr BADAOUI**, pour son soutien, pour sa guidance et ses conseils avisés tout au long de notre PFE. Votre remarquable talent pédagogique qui vous permet d'expliquer les concepts les plus complexes de manière claire et concise a été une source d'inspiration pour nous. Votre patience et votre empathie inconditionnel ont été des qualités qui nous ont aidé à surmonter les difficultés rencontrées au cours de l'année.

Encore une fois, merci pour tout ce que vous avez fait pour nous. Nous vous sommes profondément reconnaissants.

Nous voulons témoigner, au même titre, de notre reconnaissance sincère à **Mr AMRAOUI** pour son accompagnement précieux, son soutien indéfectible et ses conseils éclairés tout au long de notre projet.

Nous souhaitons également témoigner de notre appréciation envers **Mme BOUHADDOUR** pour son engagement envers notre réussite. Elle nous a prodigué de précieux conseils et nous a guidés tout au long de ce semestre. De même, nous tenons à remercier **Mr ELHAZITI** qui, grâce à ses conseils éclairés, nous a aidés à élaborer notre rapport de PFE avec rigueur et efficacité.

Nous tenons également à remercier chaleureusement tous les enseignants de notre école pour leurs encouragements, leurs gentillesses et leur passion pour l'enseignement qui ont fait de notre parcours académique une expérience enrichissante.

Nous voulons également exprimer notre profonde reconnaissance envers nos parents, qui ont été nos soutiens les plus inconditionnels tout au long de notre parcours académique. Leur amour, leur soutien indéfectible et leur dévouement sans faille ont été des piliers essentiels pour nous permettre de mener à bien ce projet. Leur confiance en nous et leur encouragement constant ont été une source d'inspiration et de motivation. Nous leur dédions ce rapport de PFE en signe d'appréciation et de reconnaissance pour tout ce qu'ils ont fait pour nous.

Enfin, nos remerciements vont aussi aux membres de jurys, nous sommes conscients de l'importance de votre temps et de l'expertise que vous allez apporter à notre travail. Nous vous sommes profondément reconnaissants pour votre engagement, votre soutien et vos contributions à notre projet. Nous espérons que vous continuerez à inspirer et à guider de nombreux autres étudiants dans leurs futurs projets.

Liste des abréviations

WAP : Wireless Acces Point (point d'accès sans fil)

WLAN: Wireless Local Area Network

HDMI: High-Definition Multimedia Interface

DHCP: Dynamic Host Configuration Protocol

IP: Internet Protocol address

HTTP: HyperText Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

DNS: Domain Name System

OSI: Open Systems Interconnection

PoE: Power over Ethernet

LDAP: Lightweight Directory Access Protocol

TLD: top-level domain

AD: Active Directory

AD DS: Active Directory Domain Services

NPS: Network Policy Server

RADIUS: Remote Authentication Dial-In User Service

IMAP : Internet Messaging Access Protocol

SMTP : Simple Mail Transfer Protocol

VoIP : Voice over Internet Protocol

SQL : Structured query language

LAN : Local area network

WAN: Wide area network

Liste des figures

Figure 1 : tableau des tâches	3
Figure 2 : diagramme de GANT	3
Figure 3 : Switch Cisco	5
Figure 4 : Switch Cisco Catalyst 3790	6
Figure 5 : switch administrable	7
Figure 6 : Routeur de cœur de réseau	8
Figure 7 : Routeur de périphérie	8
Figure 8 : Routeur sans fil	9
Figure 9 : Routeur virtuel	9
Figure 10 : l'architecture de réseau	15
Figure 11 : Cisco Catalyst 3750	17
Figure 12 : Routeur Cisco 1800	18
Figure 13 : DELL POWEREDGE R730 SERVEUR	19
Figure 14 : Linksys WRT54GL	20
Figure 15 : Fortigate 100A	21
Figure 16 : Virtualisation de serveur	26
Figure 17 : Hyperviseur type 1	27
Figure 18 : Hyperviseur type 2	27
Figure 19 : Couches composants VMware vSphere	28
Figure 20 : Logo du VMware vSphere	29
Figure 21 : démarrage de programme d'installation	29
Figure 22 : le chargement des fichiers d'installation	30
Figure 23 : Le message de bienvenu de serveur	30
Figure 24 : Validation de l'End User License Agreement	31
Figure 25 : La sélection du disque dur	31
Figure 26 : La sélection de la langue de serveur	32
Figure 27 : La saisie de mot de passe	32
Figure 28 : La confirmation de l'installation	33
Figure 29 : Le succès de l'installation	33
Figure 30 : Le redémarrage du serveur	34
Figure 31 : Affectation de l'adresse IP	34
Figure 32 : Authentification au serveur	35
Figure 33 : sélection de l'option de configuration VLAN	36
Figure 34 : Le choix de la carte réseau	36
Figure 35 : La saisie de l'adresse IP souhaitée	37
Figure 36 : Page d'authentification VMware ESXI	37
Figure 37 : L'ajout d'un commutateur virtuel standard	38
Figure 38 : Page d'accueil de VMware ESXI	38
Figure 39 : L'ajout d'un switch virtuel	39
Figure 40 : La page "Mise en réseau"	39
Figure 41 : La création de VLAN des administrateurs	40
Figure 42 : La création de VLAN des employés	40
Figure 43 : La création de VLAN des invités	41
Figure 44 : L'ajout d'une machine virtuelle	41
Figure 45 : La saisie du nom et le système de la machine virtuelle	42
Figure 46 : La sélection de stockage	43
Figure 47 : Configuration matérielle de la machine virtuelle	43
Figure 48 : La finalisation de l'installation	44
Figure 49 : L'ajout de la machine virtuelle	44
Figure 50 : Fonctionnement du DNS	46
Figure 51 : Hiérarchie d'un DNS	47

Figure 52 : Le diagramme séquence DHCP	49
Figure 53 : L'authentification de LDAP.....	51
Figure 54 : Active Directory (AD)	52
Figure 55 : Active Directory Domain Services (AD DS).....	53
Figure 56 : Schéma RADIUS	56
Figure 57 : Installation de Windows Server 2012 R2.....	57
Figure 58 : le début de l'installation de Windows Server	58
Figure 59 : La sélection de système d'exploitation à installer	58
Figure 60 : Le choix de type d'installation de Windows Server	59
Figure 61 : La création d'un compte administrateur	60
Figure 62 : configuration des paramètres réseaux de serveur.....	60
Figure 63 : Gestionnaire de serveur.....	61
Figure 64 : Installation basée sur un rôle ou une fonctionnalité.....	62
Figure 65 : La sélection du serveur de destination	63
Figure 66 : La sélection des rôles de serveurs	63
Figure 67 : La sélection des fonctionnalités	64
Figure 68 : La confirmation des sélections d'installation	65
Figure 69 : Le redémarrage du serveur.....	66
Figure 70 : La configuration de déploiement	67
Figure 71 : L'ajout d'une nouvelle forêt.....	68
Figure 72 : La vérification de la configuration requise	69
Figure 73 : La création du groupe	70
Figure 74 : La création de l'utilisateur	70
Figure 75 : La saisie du mot de passe	71
Figure 76 : L'ajout de l'utilisateur au groupe	72
Figure 77 : L'ajout d'un utilisateur à un groupe.....	73
Figure 78 : La sélection de groupe	73
Figure 79 : L'ajout d'une nouvelle zone.....	75
Figure 80 : L'ajout d'une nouvelle étendue	76
Figure 81 : L'ajout de l'étendue "Employés"	76
Figure 82 : La saisie de la plage d'adresses IP	77
Figure 83 : Fixation de la durée du bail.....	77
Figure 84 : La finalisation de la création d'étendue	78
Figure 85 : Installation du serveur RADIUS	79
Figure 86 : La sélection du serveur NPS	79
Figure 87 : Configuration des clients RADIUS.....	80
Figure 88 : Le choix de serveur RADIUS	81
Figure 89 : La sélection du type de connexion	81
Figure 90 : Authentification en tant qu'un nouveau client RADIUS.....	82
Figure 91 : La méthode d'authentification RADIUS	82
Figure 92 : Le client RADIUS.....	83
Figure 93 : Le choix d'un groupe autorisé à se connecter au point d'accès	83
Figure 94 : La finalisation de configuration RADIUS	84
Figure 95 : Configuration du point d'accès pour activer RADIUS	84
Figure 96 : Network Setup du point d'accès	85
Figure 97 : L'authentification d'un employé	86
Figure 98 : L'affichage du point d'accès	86
Figure 99 : La connexion RADIUS réalisé	86
Figure 100 : Schéma expliquant le portail captif.....	89
Figure 101 : Logo du Pfsense	90
Figure 102 : L'installation du PfSense	92
Figure 103 : Page d'accueil de l'installation du Pfsense	92
Figure 104 : Configuration des interfaces réseau	93
Figure 105 : Configuration des interfaces LAN et WAN.....	94
Figure 106 : Interface Web du Pfsense.....	95

Figure 107 : Page d'accueil Pfsense	95
Figure 108 : Configuration DHCP sur Pfsense.....	96
Figure 109 : Configuration DNS sur Pfsense	97
Figure 110 : Pfsense	97
Figure 111 : Zone portail captif.....	98
Figure 112 : Configuration portail captif.....	98
Figure 113 : Suite de configuration portail captif.....	99
Figure 114 : Serveurs d'authentification LDAP	99
Figure 115 : La création d'un groupe	100
Figure 116 : Les droits du portail captif	100
Figure 117 : Page d'authentification	101
Figure 118 : L'authentification a réussi	101
Figure 119 : Architecture DMZ.....	104
Figure 120 : Pare-feu	105
Figure 121 : Filtrage des paquets avec états	108
Figure 122 : Firewall applicatif	109
Figure 123 : L'interface de configuration DMZ	113
Figure 124 : Page d'accueil du pare-feu Fortigate 100A.....	113
Figure 125 : La configuration de l'interface "Vlan invites"	114
Figure 126 : La configuration de l'interface « DMZ »	115
Figure 127 : Validation de la configuration.....	115
Figure 128 : Les interfaces configurées.....	116
Figure 129 : le routage du Firewall	117
Figure 130 : Le routage statique et dynamique du Firewall	117
Figure 131 : Policy des VLAN des invités et les administrateurs	118
Figure 132 : Les politiques d'accès configurées	118
Figure 133 : Logo de Apache	119
Figure 134 : L'installation du "apache2"	121
Figure 135 : La création du répertoire « grp4site.ma »	121
Figure 136 : La copie de dossier de configuration	122
Figure 137 : La création d'un « Vhost ».....	123
Figure 138 : Le fichier "index.html"	123
Figure 139 : Redémarrage du service Web	124
Figure 140 : La page d'accueil du site Web.....	124
Figure 141 : Schéma serveur messagerie	125
Figure 142 : Le fonctionnement du serveur SMTP	127
Figure 143 : Logo de Postfix	127
Figure 144 : Logo de Dovecot.....	128
Figure 145 : Evolution logo.....	128
Figure 146 : L'installation du Postfix	128
Figure 147 : Configuration du Postfix	129
Figure 148 : Configuration des paquets.....	129
Figure 149 : La configuration de Postix	130
Figure 150 : La modification du fichier "grp4.pfe"	130
Figure 151 : La modification du fichier « main.cf ».....	131
Figure 152 : L'installation d'Evolution	131
Figure 153 : La page d'accueil Evolution	132
Figure 154 : Les informations du serveur messagerie	132
Figure 155 : La configuration de la réception du courriel	133
Figure 156 : La configuration de l'envoi du courriel	133
Figure 157 : La finalisation de la configuration "Evolution"	134
Figure 158 : L'installation du serveur de messagerie « Dovecot »	134
Figure 159 : Test de l'envoi du courriel.....	135
Figure 160 : La réception du courriel	135
Figure 161 : La VoIP	139

Figure 162 : Elastix logo	139
Figure 163 : Installation de Elastix.....	140
Figure 164 : Le type de partitionnement	140
Figure 165 : La liste des partitions présentes	141
Figure 166 : Le mot de passe du compte administrateur	141
Figure 167 : Début de l'installation de Elastix	142
Figure 168 : Le mot de passe du compte root de la base de données MySQL	142
Figure 169 : Authentification en tant qu'administrateur	143
Figure 170 : Configuration du réseau	143
Figure 171 : La saisie de l'adresse IP.....	144
Figure 172 : L'interface Web Elastix	144
Figure 173 : Le tableau de bord Elastix.....	145
Figure 174 : L'ajout d'une extension.....	145
Figure 175 : Les comptes SIP.....	146
Figure 176 : Configuration d'un client.....	146
Figure 177 : Téléphone 3cx	146
Figure 178 : L'ajout de client "abdo"	147
Figure 179 : Les comptes SIP sur X-Lite	147
Figure 180 : Téléphone X-Lite	148
Figure 181 : Configuration du client 2	148
Figure 182 : Vérification des deux clients.....	148
Figure 183 : Réception de l'appel de "abdo"	149
Figure 184 : Protocole SNMP	152
Figure 185 : Installation de Nagios XI	155
Figure 186 : Modification de la connexion	155
Figure 187 : Modification de l'adresse IP	156
Figure 188 : Activation de la connexion	156
Figure 189 : La page d'accueil du configurateur Web	156
Figure 190 : La finalisation de l'installation Nagios	157
Figure 191 : La page d'authentification de Nagios XI.....	157
Figure 192 : Le tableau de bord de Nagios.....	158
Figure 193 : La fenêtre "Options de configuration"	158
Figure 194 : La sélection de l'assistant de supervision.....	159
Figure 195 : Le démarrage du service SNMP	159
Figure 196 : Configuration du Switch	159
Figure 197 : La saisie de l'adresse IP- Supervision du Switch	160
Figure 198 : Détection des ports du Switch.....	160
Figure 199 : L'état des services du Switch	161
Figure 200 : L'activation de service SNMP dans le routeur	161
Figure 201 : Le service SNMP est activé dans le routeur.....	161
Figure 202 : Configuration du routeur.....	161
Figure 203 : : La saisie de l'adresse IP- Supervision du routeur.....	162
Figure 204 : Détection des ports du routeur	162
Figure 205 : L'état des services du routeur	163
Figure 206 : La saisie de l'adresse IP- Supervision du Firewall	163
Figure 207 : Détection des ports du Firewall 1.....	164
Figure 208 : Détection des ports du Firewall 2.....	164
Figure 209 : L'état des services du Firewall	165
Figure 210 : L'activation de "services Bureau à distance".....	165
Figure 211 : L'activation du "Fournisseur WMI SNMP"	166
Figure 212 : Confirmation des sélection d'installation	166
Figure 213 : Propriétaires de service SNMP	167
Figure 214 : La saisie de l'adresse IP- Supervision de Windows Server.....	167
Figure 215 : Authentification NCPA.....	168
Figure 216 : Les services qu'on va superviser	168

Figure 217 : L'état des services du Windows Server	169
Figure 218 : L'activation de protocole SNMP	169
Figure 219 : La saisie de l'adresse IP de la machine Pfsense.....	170
Figure 220 : Détection des ports et des services de Pfsense.....	170
Figure 221 : L'état des services du Pfsense.....	171
Figure 222 : Supervision de Linux Server.....	171
Figure 223 : Supervision du Web Server.....	172
Figure 224 : Les services qu'on va superviser.....	172
Figure 225 : Les services du Web Server	173
Figure 226 : L'état des services du Web Server	173
Figure 227 : Supervision du Mail Server.....	174
Figure 228 : L'état des services du Mail Server	174
Figure 229 : Architecture VPN.....	176
Figure 230 : L'intranet VPN	180
Figure 231 : L'extranet VPN.....	180
Figure 232 : Le protocole PPTP	182
Figure 233 : Le protocole L2TP	182
Figure 234 : Le protocole SSTP	183
Figure 235 : La mise en place du VPN.....	184
Figure 236 : L'installation du VPN.....	185
Figure 237 : L'ajout des fonctionnalités du VPN	185
Figure 238 : L'activation de l'accès à distance.....	186
Figure 239 : La confirmation des sélections d'installation VPN	186
Figure 240 : La création d'une unité d'organisation.....	187
Figure 241 : L'unité d'organisation "VPN_USERS"	187
Figure 242 : La création d'un groupe VPN.....	188
Figure 243 : La création d'un utilisateur dans le groupe "VPN_USERS"	188
Figure 244 : Le mot de passe de l'utilisateur VPN	189
Figure 245 : La configuration du VPN	190
Figure 246 : La configuration du routage et l'accès à distance	190
Figure 247 : L'assistant d'installation	191
Figure 248 : La configuration personnalisée	191
Figure 249 : L'activation de l'accès VPN	192
Figure 250 : La finalisation de l'installation d'accès à distance	192
Figure 251 : Stratégie accès réseau VPN.....	193
Figure 252 : L'ajout d'une nouvelle stratégie.....	193
Figure 253 : La saisie du nom de la stratégie	194
Figure 254 : Spécification des conditions.....	195
Figure 255 : La sélection du groupe VPN	195
Figure 256 : La condition du VPN est ajoutée	196
Figure 257 : Type de tunnel.....	196
Figure 258 : La configuration de la méthode d'authentification	197
Figure 259 : La finalisation de la configuration de la stratégie	198
Figure 260 . La configuration du point d'accès sur le VPN	198
Figure 261 : La finalisation de la configuration VPN dans le point d'accès	199
Figure 262 : Centre Réseau et partage.....	199
Figure 263 : Connexion à votre espace de travail.....	200
Figure 264 : Utiliser ma connexion Internet « VPN ».....	200
Figure 265 : La saisie de l'adresse Internet.....	201
Figure 266 : L'authentification VPN	202
Figure 267 : Connexion VPN	202

Liste des tableaux

Tableau 1 : Répartition des services réseau	14
Tableau 2 : Plan d'adressage de réseau	15
Tableau 3 : Plan d'adressage des machines virtuelles	16
Tableau 4 : Caractéristiques du switch Cisco Catalyst 3750	17
Tableau 5 : Caractéristiques du routeur Cisco 1800	18
Tableau 6 : Caractéristiques du DELL POWEREDGE R730 SERVEUR	19
Tableau 7 : Caractéristiques de Linksys WRT54GL	20
Tableau 8 : Caractéristiques de Fortigate 100A	21
Tableau 9 : Configuration du Switch	22
Tableau 10 : Configuration de routeur	23

Sommaire

Résumé	III
Abstract	III
Remerciements	IV
Liste des abréviations	V
Liste des figures.....	VI
Liste des tableaux	XI
Sommaire.....	XII
Introduction	1
Présentation du projet.....	2
Gestion du projet	3
Chapitre I : Étude des matériaux	4
I. Un switch :.....	5
II. Un routeur :.....	7
III. Un serveur :	10
IV. Un point d'accès :	11
V. Un pare-feu :.....	12
Chapitre II : Infrastructure du réseau.....	13
I. Infrastructure du réseau :.....	14
II. Schéma de l'architecture de réseau :	15
III. Les matériaux utilisés :	16
IV. Configuration des éléments d'interconnexion :	22
Chapitre III : La virtualisation	24
I. Contexte de virtualisation :.....	25
II. Virtualisation des serveurs :	28
III. Configuration de VMware vSphere ESXi 6.7.0 :	34
Chapitre IV : Mise en œuvre du réseau des employés.....	45
I. Services réseaux :	46
II. Politique de sécurité :	54
III. Serveur RADIUS :	55
IV. La phase de l'installation :.....	57
Chapitre V : Mise en œuvre du réseau des invités.....	87
I. Portail Captif :	88
II. Pfsense :	89
III. Configuration du PfSense :	94
Chapitre VI : Firewall & DMZ.....	102
I. DMZ :	103

II.	Firewall :	104
III.	Mise en place d'une DMZ avec FortiGate 100A :	112
IV.	Les serveurs implémentés dans la DMZ :	119
V.	Le serveur de messagerie :	125
	Chapitre VII : La VoIP	136
I.	Etude théorique de la VoIP :	137
II.	Elastix :	139
	Chapitre VIII : Mise en place d'un serveur de supervision	150
I.	La supervision informatique :	151
II.	Supervision des matériaux :	159
III.	Supervision des machines :	165
	Chapitre IX : VPN	175
I.	La partie théorique du VPN :	176
	Conclusion générale	203
	Table de matière	204
	Webographie	209

Introduction

La performance du système d'information d'un établissement est d'une immense importance pour son efficacité et son bon fonctionnement.

La recherche de cette performance entraîne de plus en plus l'utilisation d'un système informatique sécurisé pour la gestion quotidienne des informations. Ainsi, l'apparition de ces environnements informatiques imposants et cruciaux rend la surveillance des éléments clefs de réseau essentielle. Ces éléments doivent fonctionner pleinement et en permanence pour garantir la fiabilité et l'efficacité exigées, ainsi que la réduction des défaillances, pannes et des différents problèmes techniques qui peuvent subvenir. Cela est rendu possible grâce aux méthodes de supervision informatique.

En outre, le développement d'utilisation d'internet a mené beaucoup d'établissements de nos jours à ouvrir leurs systèmes d'information à leur public, leurs partenaires, utilisateurs ou visiteurs. Il s'avère donc essentiel de connaître les ressources de l'établissement à protéger et ainsi maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Et donc, à partir de n'importe quel endroit les utilisateurs se connectent au système d'information, ils transportent une partie du système d'information hors de l'infrastructure sécurisée de l'établissement. Or, la sécurité des systèmes informatiques se contente généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et/ou d'identifications et de contrôle permettant d'assurer que les utilisateurs possèdent uniquement les droits qui leurs ont été accordés.

C'est dans cette vision-là qu'il nous a été proposé par Ecole Supérieure de Technologie de Salé (ESTS), dans le cadre de notre projet de fin d'études, de mettre en place dans une entreprise, un réseau informatique sécurisé et de le superviser.

Présentation du projet

Cahier de charge :

Notre projet de fin d'études consiste à mettre en place un réseau informatique fonctionnel pour exploiter les connaissances que nous avons acquises au cours de notre parcours universitaire.

Le réseau sera configuré pour différents types d'utilisateurs, chacun soumis à des politiques d'accès spécifiques pour les connexions filaires et sans fil.

Les employés et les admins seront séparés sur le réseau, chacun ayant accès aux services indispensables pour assurer un fonctionnement optimal. De plus, le réseau sera supervisé par une solution de gestion pour garantir une disponibilité maximale.

En outre, l'ESTS souhaite exposer certains de ses services au grand public via une zone DMZ, tandis que le réseau interne ne sera pas accessible depuis l'extérieur, nécessitant l'utilisation d'un pare-feu.

Un administrateur réseau sera chargé de gérer cette architecture complexe, y compris l'utilisation d'un VPN sécurisé pour les accès à distance en cas de déplacement ou d'urgence depuis son domicile.

Objectifs :

- La mise en place d'un réseau sans fil sécurisé destiné aux admins, employés et aux invités.
- Les services réseau indispensables au bon fonctionnement du réseau.
- La supervision du réseau
- Assurer la sécurité de l'accès à internet et intranet
- L'accès à distance

Gestion du projet

La gestion de projet implique l'organisation et la coordination d'activités pour garantir la réussite d'un projet dans les délais impartis et conformément aux objectifs établis. Notre sujet complexe nécessite une quantité considérable de travail, car il englobe la plupart des services de base que l'on peut trouver dans une école ou une entreprise. Ainsi, il est essentiel de définir les tâches, de les répartir en fonction des échéances fixées et de les assigner aux membres du groupe afin d'accomplir le projet.

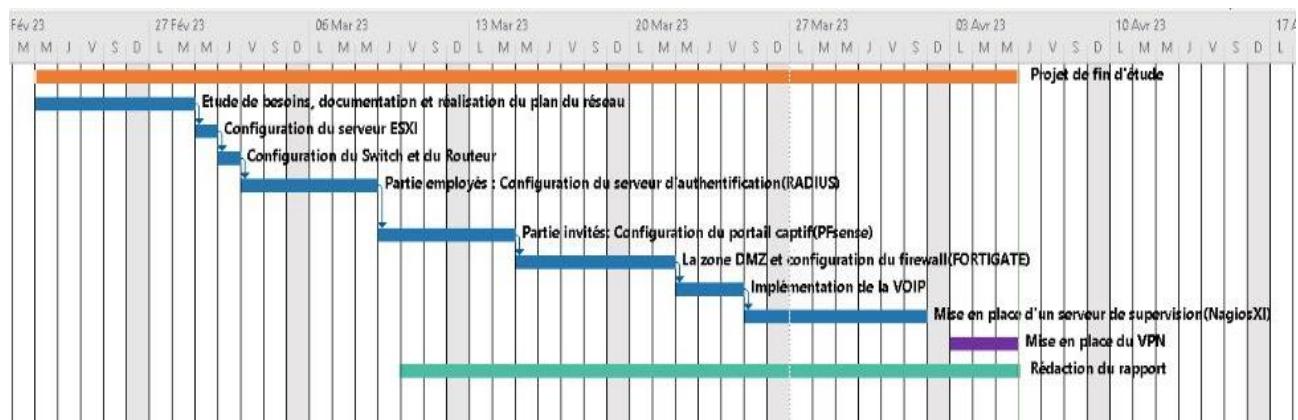
Le tableau des tâches :

N°	Nom de la tâche	Durée	Début	Fin	Prédécesseurs
1	Projet de fin d'étude	34 jours	Mer 22/02/23	Mer 05/04/23	
2	Etude de besoins, documentation et réalisation du plan du réseau	5 jours	Mer 22/02/23	Mar 28/02/23	
3	Configuration du serveur ESXI	1 jour	Mer 01/03/23	Mer 01/03/23	2
4	Configuration du Switch et du Routeur	1 jour	Jeu 02/03/23	Jeu 02/03/23	3
5	Partie employés : Configuration du serveur d'authentification(RADIUS)	4 jours	Ven 03/03/23	Mer 08/03/23	4
6	Partie invités: Configuration du portail captif(PFSense)	4 jours	Jeu 09/03/23	Mar 14/03/23	5
7	La zone DMZ et configuration du firewall(FORTIGATE)	5 jours	Mer 15/03/23	Mar 21/03/23	6
8	Implémentation de la VOIP	3 jours	Mer 22/03/23	Ven 24/03/23	7
9	Mise en place d'un serveur de supervision(NagiosXI)	7 jours	Sam 25/03/23	Sam 01/04/23	8
10	Mise en place du VPN	3 jours	Lun 03/04/23	Mer 05/04/23	
11	Rédaction du rapport	22 jours	Ven 10/03/23	Mer 05/04/23	

Figure 1 : tableau des tâches

Gant :

Afin de conduire ce projet avec succès, nous avons créé un diagramme de Gantt, un outil de planification et de gestion de projet qui permet de représenter graphiquement dans le temps les différentes étapes qui le composent.



Chapitre I : Étude des matériaux

Dans ce chapitre, nous aborderons les matériaux de réseau que nous utiliserons dans notre projet : la mise en place d'un réseau informatique au sein d'une entreprise.

I.Un switch :

1. Définition :

Qu'est-ce qu'un switch, ou commutateur réseau ?

Un **switch**, commutateur ou commutateur réseau, est un boîtier doté de quatre à plusieurs centaines de **ports Ethernet**, qui fonctionne comme un pont multiport et qui permet de relier plusieurs segments d'un réseau informatique entre eux. Le switch présente plusieurs avantages dans la gestion de votre parc informatique. Il contribue à la sécurité du réseau et à **la protection des données échangées via le réseau**. Il permet notamment de créer différents circuits au sein d'un même réseau, de recevoir des informations et d'envoyer des données vers un destinataire précis en les transportant via le port adéquat.

Il est également chargé d'analyser les trames qui arrivent sur les ports d'entrée, il opère une filtration des données afin de les orienter vers le bon port. Le **switch** a donc une double fonction de filtrage et de connectivité. Il sert de véhicule au transport de trame, comme peut également le faire le routage. Il crée aussi des circuits virtuels.



Figure 3 : Switch Cisco

Le switch permet avant tout de répartir l'information de manière « intelligente » au sein de l'entreprise. Il contrôle et sécurise au maximum votre réseau pour vous éviter les intrusions. Une fois paramétré par un technicien informatique, le switch distribue l'information seulement aux utilisateurs prédéfinis en fonction de la typologie de collaborateurs ou de certaines restrictions, améliorant ainsi **la confidentialité des données d'entreprise**.

Ainsi, ce commutateur réseau **assure la communication, la réception et la redistribution de messages**, entre les différents ordinateurs et serveurs d'un même réseau.

2. Les différents types de switches :

Il existe une multitude de types de switches qui fonctionnent de manière différente selon les usages au sein de votre entreprise. *On cite notamment le switch Ethernet, le switch HDMI, etc.* Tous sont proposés par des entreprises spécialisées comme **Cisco**, l'entreprise HP où encore Netgear, auprès desquels nous sommes partenaire privilégié.



Figure 4 : Switch Cisco Catalyst 3790

Chacun des switches informatiques peut employer un mode de transmission particulier selon la méthode :

- Mode direct : sans détection d'erreur
- Mode différé : avec une opération de contrôle sur chaque trame
- Mode fragment free : un mix entre le mode direct et le mode différé
- Mode de commutation automatique : un choix automatique entre les trois modes précédents (Configuration préalable pour la mise en route de chaque mode)

Le modèle standard de switch fonctionne en mode « différé », également appelé « **store and forward** » : c'est à dire qu'il stocke les données réseau pour les analyser afin de détecter d'éventuelles erreurs avant de les envoyer sur les différents équipements.

3. Un switch manageable (administrable) :

Qu'est-ce qu'un switch administrable ?

Les Switches Administrables offrent des possibilités de configuration qui vous permettent de modifier et de gérer leur fonctionnement. Cela s'avère particulièrement utile pour identifier les problèmes, en cas de trafic multicast sur le réseau et si les temps d'arrêt coûtent cher. D'où l'importance d'opter pour des switches administrables. Le switch administrable constitue une solution abordable & plug-and-play, mais ils n'offrent pas d'avantages liés à un système d'administration de l'appareil. Ils sont logiquement dépourvus d'interface et d'options permettant d'en modifier les paramètres.



Figure 5 : switch administrable

II. Un routeur :

1. Définition :

Le routeur est un périphérique intermédiaire de réseau informatique qui connecte les réseaux locaux au plus grand des réseaux informatiques : l'internet, il est la première ligne de sécurité contre l'intrusion dans un réseau. Les routeurs font souvent office de serveurs DHCP dans les petits réseaux d'entreprise ; en émettant des adresses IP uniques.

C'est une technologie dont tout le monde entend parler sans pour autant la connaître.

2. Les différents types de routeurs :

a) Routeur de cœur de réseau :

Les routeurs de cœur de réseau sont généralement utilisés par les opérateurs télécom (comme AT&T, Verizon, Vodafone) ou les fournisseurs cloud (comme Google, Amazon, Microsoft). Ils fournissent une bande passante maximale pour connecter des routeurs ou des commutateurs supplémentaires. La plupart des PME n'ont pas besoin de routeurs de cœur de réseau. Mais les très grandes entreprises dont les nombreux collaborateurs travaillent dans différents bâtiments ou lieux intègrent souvent ce type de routeur au sein de leur architecture réseau.



Figure 6 : Routeur de cœur de réseau

b) Routeur de périphérie :

Un routeur de périphérie, également appelé routeur passerelle ou simplement « passerelle », est le dernier point de connexion d'un réseau avec les réseaux externes, y compris Internet.

Les routeurs de périphérie sont optimisés pour la bande passante et conçus pour se connecter à d'autres routeurs afin de distribuer les données aux utilisateurs. Les routeurs de périphérie n'offrent généralement pas de connectivité Wi-Fi ou la possibilité de gérer entièrement des réseaux locaux. Ils sont uniquement dotés de ports Ethernet, avec une entrée pour la connexion Internet et plusieurs sorties pour la connexion de routeurs supplémentaires.



Figure 7 : Routeur de périphérie

c) Routeur de distribution

Un routeur de distribution, ou routeur intérieur, reçoit les données du routeur de périphérie (également appelé « passerelle ») via une connexion filaire et les transmet aux utilisateurs, généralement via une connexion Wi-Fi, bien que le routeur fournit généralement aussi des connexions physiques (Ethernet) pour connecter des utilisateurs ou des routeurs supplémentaires.

d) Routeur sans fil :

Les routeurs sans fils, ou passerelles résidentielles, combinent les fonctions des routeurs de périphérie et des routeurs de distribution. Ces routeurs sont très utilisés pour les réseaux domestiques et l'accès Internet.

La plupart des opérateurs télécom fournissent des routeurs sans fil multifonctions comme équipement standard. Mais même si vous avez la possibilité d'utiliser un routeur sans fil de FAI dans votre PME, vous voudrez peut-être profiter des performances sans fil d'exception, des contrôles de connectivité supplémentaires et de la sécurité accrue d'un routeur professionnel.



Figure 8 : Routeur sans fil

e) Routeur virtuel :

Les routeurs virtuels sont des composants logiciels qui permettent de virtualiser certaines fonctions du routeur dans le cloud et de les mettre à disposition en tant que service. Ces routeurs sont parfaits pour les grandes entreprises dont les besoins en réseau sont complexes. Ils offrent une grande flexibilité, une évolutivité simple et un coût initial réduit. L'autre avantage des routeurs virtuels est la gestion réduite du matériel réseau local.



Figure 9 : Routeur virtuel

III.Un serveur :

1. Définition :

C'est un **système qui fournit des données, des services ou des programmes informatiques** accessibles sur un réseau internet ou intranet, un serveur informatique qui offre des services accessibles via un réseau. Il peut être matériel ou logiciel, c'est un ordinateur qui exécute des opérations suivant les requêtes effectuées par un autre ordinateur appelé « client », il traite les requêtes effectuées à partir d'un PC personnel, d'un smartphone ou d'une tablette : on parle alors de relation « client/serveur ».

Par exemple, un utilisateur (côté client) va rechercher un site internet en utilisant un navigateur web, pour que ce dernier puisse l'afficher il va effectuer une requête au serveur HTTP qui est un serveur web.

2. Les différents types de serveurs :

Compte tenu de la multitude de services qu'il propose, le serveur informatique se décline en plusieurs catégories.

- **Serveurs web**

Les **serveurs web** proposent des services d'hébergement et de gestion de sites. Ce sont eux qui affichent les pages web sollicitées par les utilisateurs sur internet ou sur intranet par le biais d'un navigateur. Les serveurs web les plus connus sur le marché sont *Microsoft Internet Information Services* (IIS), Nginx et Apache.

- **Serveurs de fichiers**

Les **serveurs de fichiers** servent à stocker et diffuser des documents afin de les rendre accessibles aux utilisateurs à partir de n'importe quel ordinateur du réseau. Le stockage de fichiers permet ainsi d'effectuer des sauvegardes, mais aussi de recourir à des solutions de tolérance aux pannes. Afin d'optimiser les performances, la partie matérielle des serveurs de fichiers peut être conçue pour augmenter les vitesses de lecture et d'écriture.

- **Serveurs de bases de données**

Les **serveurs de bases de données** sont des outils informatiques utilisés pour héberger et traiter d'indénombrables informations afin de les rendre accessibles. Intégrés à d'autres applications et systèmes, ils démultiplient la diffusion la plus pointue possible afin de répondre de manière exhaustive à la requête.

- **Serveurs de messagerie**

Les **serveurs de messagerie** offrent des services dédiés au courrier électronique. Ils donnent aux internautes la possibilité d'envoyer, de recevoir et de consulter des e-mails. Ils gèrent la distribution des courriels puisqu'ils transmettent les messages d'un utilisateur à un autre via un réseau.

- **Serveurs DNS**

Les **serveurs DNS** sont utilisés pour traduire les noms de domaines des ordinateurs clients en adresses IP exploitables par une machine. Sorte de base de données géante contenant tous les noms de domaines et d'autres serveurs DNS identifiés, ils associent un ordinateur avec un domaine.

- **Serveurs PROXY**

Les **serveurs PROXY** jouent un rôle de passerelle entre le réseau et l'internaute. Il sert d'intermédiaire entre les utilisateurs privés et les sites web et fait office de pare-feu pour limiter les accès et faciliter les connexions autorisées.

IV.Un point d'accès :

1. Définition :

Un point d'accès est un appareil qui crée un réseau local sans fil (WLAN) et le connecte à un réseau câblé. Il agit comme un pont entre les deux réseaux, permettant aux utilisateurs d'accéder à Internet ou à d'autres appareils sur le réseau câblé. Il se connecte à un routeur câblé, un commutateur ou un concentrateur par câble Ethernet ; il retransmet le signal Wi-Fi vers une zone désignée. Si vous souhaitez activer l'accès Wi-Fi dans la zone de réception de votre entreprise par exemple, mais ne disposez pas d'un routeur à portée, vous pouvez installer un point d'accès près de la réception et acheminer un câble Ethernet à travers le plafond vers à la salle des serveurs.

Pourquoi utiliser un WAP pour configurer un réseau sans fil ?

Le WAP vous permet de créer un réseau sans fil sur votre réseau filaire existant afin de prendre en charge les dispositifs sans fil.

Vous pouvez également utiliser un WAP ou des modules d'extension maillés pour étendre la portée du signal et la puissance du réseau sans fil pour fournir une couverture sans fil complète et éviter les « zones mortes », en particulier dans les espaces de travail ou les bâtiments plus grands. En plus, vous pouvez configurer les paramètres des WAP à l'aide d'un seul appareil.

Principaux avantages de la mise à niveau vers les WAP

Les WAP constituent une alternative plus pratique, plus sécurisée et plus économique par rapport aux câbles et aux fils pour connecter chaque ordinateur ou appareil sur votre réseau. Utiliser des WAP pour configurer un réseau sans fil peut également fournir de nombreux avantages et bénéfices pour votre petite entreprise.

Premièrement, l'accès au réseau sans fil est plus pratique. L'ajout d'utilisateurs est également moins complexe. Puis, vous pouvez facilement fournir un accès Internet aux utilisateurs invités en leur donnant un mot de passe pour accéder à votre réseau sans fil en toute sécurité.

Vous pouvez également facilement segmenter les utilisateurs, y compris les invités pour mieux protéger les ressources et les actifs de votre réseau.

V.Un pare-feu :

1. Définition :

Un pare-feu constitue la première ligne de défense des réseaux depuis plus de 25 ans. C'est un appareil de protection du réseau qui surveille le trafic entrant et sortant en établissant une barrière entre les réseaux internes sécurisés et contrôlés qui sont dignes de confiance et les réseaux externes non fiables tels qu'Internet, ensuite il décidera d'autoriser ou de bloquer une partie de ce trafic en fonction d'un ensemble de règles de sécurité prédéfinies.

Un pare-feu peut être un équipement physique, un logiciel ou une combinaison des deux.

2. Types de pare-feu :

Les différents types de pare-feu intègrent des méthodes de filtrage variées. Bien que chaque type ait été développé pour dépasser les générations précédentes de pare-feu, une grande part de la technologie de base a été transmise de génération en génération.

Les types de pare-feu se distinguent par leur approche des éléments suivants :

- Suivi des connexions
- Règles de filtrage
- Journaux d'audit.

Chaque type fonctionne à un niveau différent du modèle de communication normalisé, le modèle d'interconnexion des systèmes ouverts (OSI). Ce modèle permet de mieux visualiser la manière dont chaque pare-feu interagit avec les connexions.

Chapitre II : Infrastructure du réseau

Suite à l'analyse du cahier des charges du projet, ce chapitre sera consacré aux services installés, à l'architecture du réseau, au plan d'adressage et au plan d'adressage des machines virtuelles.

I. Infrastructure du réseau :

1. Les services installés :

Nous avons alors convenu ces services à mettre en place pour notre réseau :

→ Réseau des employés :

- DNS, DHCP, RADIUS (NPS), AD DS, AD CS, (Windows server 2012 R2).

→ Réseau des administrateurs :

- Nagios XI (CentOS 7).

→ Réseau des invités :

- DNS, DHCP, Captive portal (Pfsense),

En plus d'un service Web, VOIP, et un service messagerie.

Tableau 1 : Répartition des services réseau

Réseaux	Services	
Invités	Portail captif	Serveur d'authentification(pfSense)
	Messagerie	Postfix
Employés	Radius	Serveur d'authentification (Radius)
	VOIP	Elastix
	Messagerie	SMTP
Administrateur	Supervision	Nagios
	Serveur web(apache)	Https
	VOIP	Elastix
	Messagerie	Postfix

2. Plan d'adressage de réseau :

Notre réseau est divisé en trois sous-réseaux distincts -Admins, Employés et Invités- au sein de notre intranet. Le plan d'adressage du réseau peut être présenté sous la forme suivante :

Tableau 2 : Plan d'adressage de réseau

Réseaux	VLAN	Adresse IP
Invités	10	192.168.10.0/24
Employés	20	192.168.20.0/24
Administrateur	30	192.168.30.0/24
Serveur (vSphere ESXI)	(Trunk avec switch)	10.10.10.254/24
DMZ		172.120.1.0/24

II.Schéma de l'architecture de réseau :

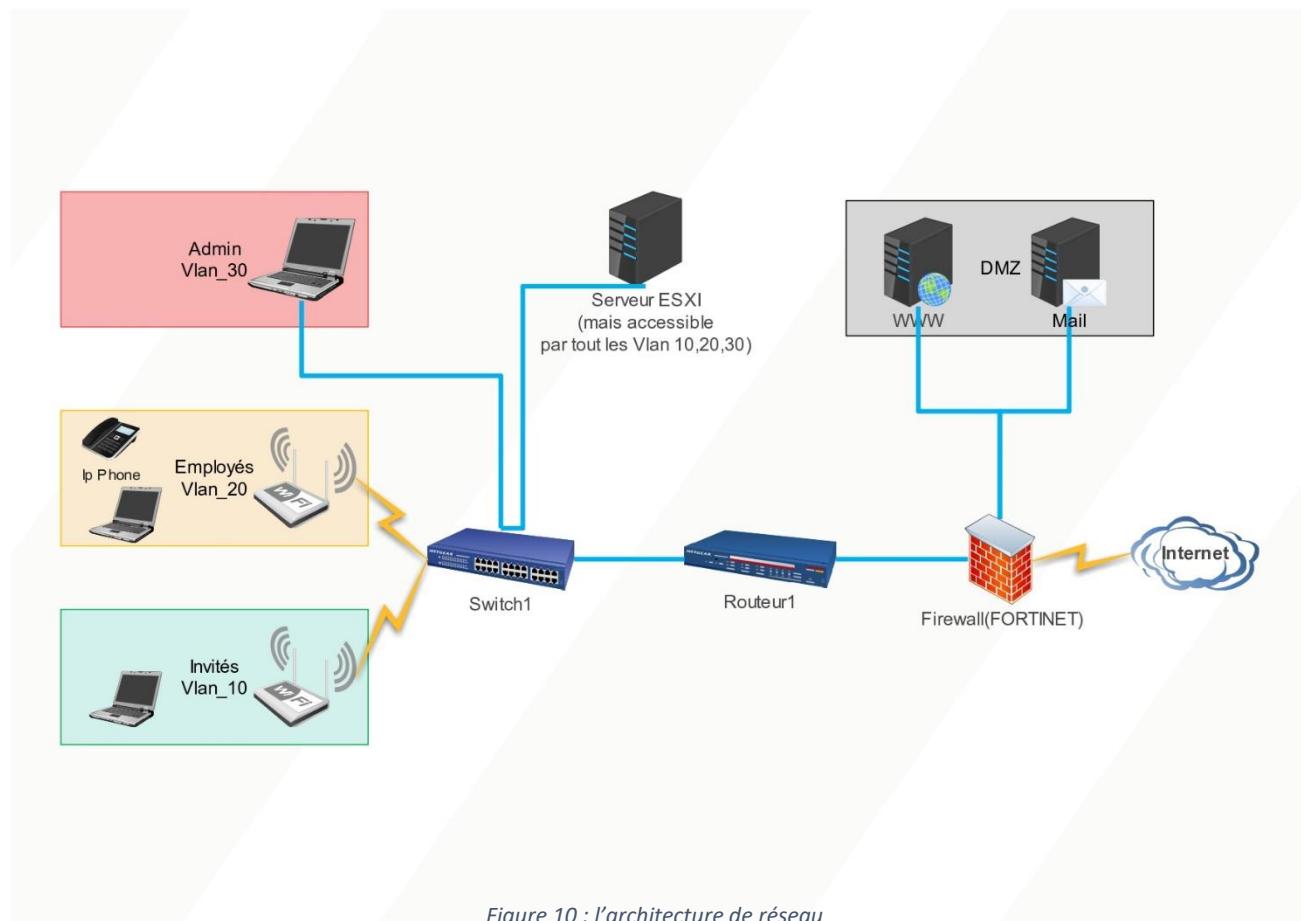


Figure 10 : l'architecture de réseau

1. Plan d'adressage des machines virtuelles :

Tableau 3 : Plan d'adressage des machines virtuelles

Réseaux	VLAN	Adresse IP
Serveur ESXI	---	10.10.10.254/24
Les machines virtuelles de ESXI		
Nagios	30	192.168.30.252/24
Pfsense	10	192.168.10.253/24
Windows Server 2012(Radius)	20	192.168.20.253/24
Elastix	20	192.168.20.250
Linux Server	---	172.120.1.101

III.Les matériaux utilisés :

Au cours de cette section du deuxième chapitre, nous examinerons les matériaux que nous avons employés pour concrétiser notre projet.

1. Un switch :

La gamme Cisco® Catalyst® 3750 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWise™, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de construire un système unique de commutation à haute disponibilité, vu comme un simple commutateur virtuel.

Tableau 4 : Caractéristiques du switch Cisco Catalyst 3750



Figure 11 : Cisco Catalyst 3750

Nom	Cisco Catalyst 3750
Type de périphérique	Commutateur - 24 ports - C3 - Géré - empilable
Ports	24 x 10/100/1000 (PoE) + 4 x SFP
Taux de transfert des données	100 Mbit/s
Protocole de routage	RIP-1, RIP-2, EIGP, routage IP statique, RIPng
Taille de la table d'adresses MAC	12 000 entrées
Ram	128 Mo
Mémoire flash	32 Mo flash

2. Un routeur

Le routeur Cisco 1800 est un équipement de réseau professionnel conçu pour les entreprises de taille moyenne à grande. Il offre des fonctionnalités avancées pour aider les entreprises à gérer leurs réseaux de manière efficace et sécurisée.

Tableau 5 : Caractéristiques du routeur Cisco 1800



Figure 12 : Routeur Cisco 1800

Nom	Routeur Cisco 1800
Interfaces	2 x 10Base-T/100Base-TX/1000Base-T - RJ-45 Série : 1 x console Gestion : 1 x console - mini-USB Type B Série : 1 x auxiliaire USB 2.0 : 1 x USB 4 broches Type A
Protocole de routage	OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, routage IP statique, IGMPv3, GRE, PIM-SSM, routage IPv4 statique, routage IPv6 statique, routage basé sur des politiques (PBR), MPLS
RAM	512 Mo (installé) / 512 Mo (max)
Mémoire flash	256 Mo (installé) / 256 Mo (max)
Protocole de liaison de données	Ethernet, Fast Ethernet, Gigabit Ethernet

3. Un serveur :

Tableau 6 : Caractéristiques du DELL POWEREDGE R730 SERVEUR



Figure 13 : DELL POWEREDGE R730 SERVEUR

Nom	DELL POWEREDGE R730 SERVEUR
Processeur	Gamme de processeurs Intel® Xeon E5-2600 v4
Sockets de processeur	2
Système d'exploitation	<p>Microsoft® Windows Server® 2008 R2</p> <p>Microsoft Windows Server 2012</p> <p>Microsoft Windows Server 2012 R2</p> <p>Microsoft® Windows Server® 2016</p> <p>Novell® SUSE® Linux Enterprise Server</p> <p>Red Hat® Enterprise Linux</p> <p>Hyperviseurs intégrés en option :</p> <p>Citrix® XenServer®</p> <p>VMware vSphere® ESXi™</p> <p>Microsoft Windows Server 2012 (Hyper-V inclus)</p>
Mémoire	Jusqu'à 1,5 To de mémoire DDR4 (24 emplacements DIMM) : 4, 8, 16, 32 ou 64 Go et jusqu'à 2 400 MT/s
Mémoire RAM	De 8 Go et plus
Format du boîtier	Rack

4. Un point d'accès :

Le **Linksys WRT54GL** est un routeur sans fil de la marque Linksys, connue pour ses produits de qualité en matière de réseaux domestiques. Le WRT54GL est un modèle de routeur populaire qui a été introduit pour la première fois en 2005 et qui est toujours apprécié des utilisateurs pour sa fiabilité et sa performance.

Tableau 7 : Caractéristiques de Linksys WRT54GL



Figure 14 : Linksys WRT54GL

Nom	Linksys WRT54GL
Type de produit	Routeurs sans fil / Commutateur
Ports	4 ports LAN et 1 WAN
Protocole de liaison de données	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g
Débit de transfert de données	54 Mbits/s
Connectivité	Sans fil, câble
Algorithme de chiffrement	WEP 128 bits, WEP 64 bits, WPA, WPA2

5. Un pare-feu :

Fortigate 100A est un pare-feu de sécurité réseau de la série Fortigate de Fortinet, conçu pour les petites et moyennes entreprises. Il offre une protection avancée contre les menaces en ligne, ainsi qu'un large éventail de fonctionnalités de sécurité, telles que la détection d'intrusion, la prévention des virus, le filtrage du contenu et la protection contre les attaques de déni de service (DDoS).

Tableau 8 : Caractéristiques de Fortigate 100A

	
<i>Figure 15 : Fortigate 100A</i>	
Nom	Fortigate 100A
Facteur de forme	Externe
Méthode d'authentification	LDAP, RADIUS, Secure Shell (SSH)
Taux de transfert des données	100 Mbit/s
Protocole de gestion à distance	HTTPS, SNMP
Réseau / Protocole de transport	IPSec, L2TP, PPPoE, PPTP
Performance	<p>➔ Débit du pare-feu : 100 Mbps</p> <p>➔ Débit 3DES : 40 Mbps</p>

IV. Configuration des éléments d'interconnexion :

1. Configuration du switch :

Tableau 9 : Configuration du Switch

La configuration	Les commandes
La création des VLANs	<pre>Switch_GRP4(config)#vlan 10 Switch_GRP4(config-vlan)#name Invites Switch_GRP4(config-vlan)#ex Switch_GRP4(config)#vlan 20 Switch_GRP4(config-vlan)#name Employes Switch_GRP4(config-vlan)#ex Switch_GRP4(config)#vlan 30 Switch_GRP4(config-vlan)#name Admin Switch_GRP4(config-vlan)#ex Switch_GRP4(config)#vlan 40</pre>
Affectation des ports aux VLANs	<pre>Switch_GRP4(config)#interface range Gi2/0/1-4 Switch_GRP4(config-if)#switchport mode access Switch_GRP4(config-if)#switchport access vlan 10 Switch_GRP4(config-if)#ex Switch_GRP4(config)#interface range Gi2/0/5-8 Switch_GRP4(config-if)#switchport mode access Switch_GRP4(config-if)#switchport access vlan 20 Switch_GRP4(config-if)#ex Switch_GRP4(config)#interface range Gi2/0/9-12 Switch_GRP4(config-if)#switchport mode access Switch_GRP4(config-if)#switchport access vlan 30 Switch_GRP4(config-if)#ex</pre>
Configuration des ports trunk	<pre>Switch_GRP4(config)# interface range Gi1/0/22-24 Switch_GRP4(config)#switchport trunk encapsulation dot1q Switch_GRP4(config-if)#switchport mode trunk Switch_GRP4(config-if)#ex</pre>

Affectations des adresses aux VLANs	<pre> Switch_GRP4(config)#interface vlan 10 Switch_GRP4(config-if)#ip address 192.168.10.253 255.255.255.0 Switch_GRP4(config-if)#ex Switch_GRP4(config)#interface vlan 20 Switch_GRP4(config-if)#ip address 192.168.20.253 255.255.255.0 Switch_GRP4(config-if)#ex Switch_GRP4(config)#interface vlan 30 Switch_GRP4(config-if)#ip address 192.168.30.253 255.255.255.0 Switch_GRP4(config-if)#ex </pre>
-------------------------------------	---

2. Configuration de routeur :

En se basant sur le schéma mentionné, il est nécessaire de configurer deux sous-interfaces dans l'interface réseau interne du routeur car nous avons trois VLAN.

Tableau 10 : Configuration de routeur

La configuration	Les commandes
La création des sous-interfaces	<pre> Router_GRP4(config)#interface FastEthernet0.10 Router_GRP4 (config-if)# encapsulation dot1Q 10 Router_GRP4 (config-if)#ip address 192.168.10.254 255.255.255.0 Router_GRP4 (config-if)#no sh Router_GRP4 (config-if)#ex Router_GRP4(config)#interface FastEthernet0.20 Router_GRP4 (config-if)# encapsulation dot1Q 20 Router_GRP4 (config-if)#ip address 192.168.10.254 255.255.255.0 Router_GRP4 (config-if)#no sh Router_GRP4 (config-if)#ex Router_GRP4(config)#interface FastEthernet0.30 Router_GRP4 (config-if)# encapsulation dot1Q 30 Router_GRP4 (config-if)#ip address 192.168.30.254 255.255.255.0 Router_GRP4 (config-if)#no sh Router_GRP4 (config-if)#ex Router_GRP4(config)#interface FastEthernet1 Router_GRP4 (config-if)#ip address 192.168.40.254 255.255.255.0 Router_GRP4 (config-if)#no sh </pre>

Chapitre III : La virtualisation

La virtualisation est un domaine crucial pour les professionnels de l'industrie des systèmes d'information, qui implique l'utilisation de techniques matérielles et logicielles permettant de fournir des ressources informatiques indépendamment de la plateforme matérielle. Acquérir des compétences dans ce domaine peut être un atout considérable pour notre formation et notre future carrière. Dans cette optique, nous allons commencer par explorer les concepts clés de la virtualisation, en examinant les avantages et les différentes techniques disponibles. Nous allons également approfondir la notion d'hyperviseur, avant de nous concentrer sur l'installation et la configuration d'ESXI pour répondre à nos besoins spécifiques.

I.Contexte de virtualisation :

1. Définition :

La virtualisation de serveurs englobe un ensemble de techniques et d'outils qui permettent de faire fonctionner plusieurs systèmes d'exploitation sur un seul serveur physique. Ce principe de virtualisation repose sur un partage des ressources du serveur entre les différents systèmes d'exploitation. Pour être opérationnelle, la virtualisation doit respecter deux principes fondamentaux :

- Le premier principe fondamental de la virtualisation **le cloisonnement** complet entre chaque système d'exploitation, assurant ainsi leur fonctionnement indépendant et empêchant toute interférence entre eux.
- Le deuxième principe fondamental de la virtualisation est **la transparence** : cela signifie que l'exécution en mode virtualisé ne doit pas avoir d'impact sur le fonctionnement du système d'exploitation et en particulier sur les applications qui y sont exécutées.

Néanmoins, avec l'utilisation d'un hyperviseur (une plateforme qui permet de virtualiser les systèmes d'exploitation pour qu'ils fonctionnent sur la même machine physique), les ressources de la machine physique sont gérées et partagées entre les machines virtuelles.

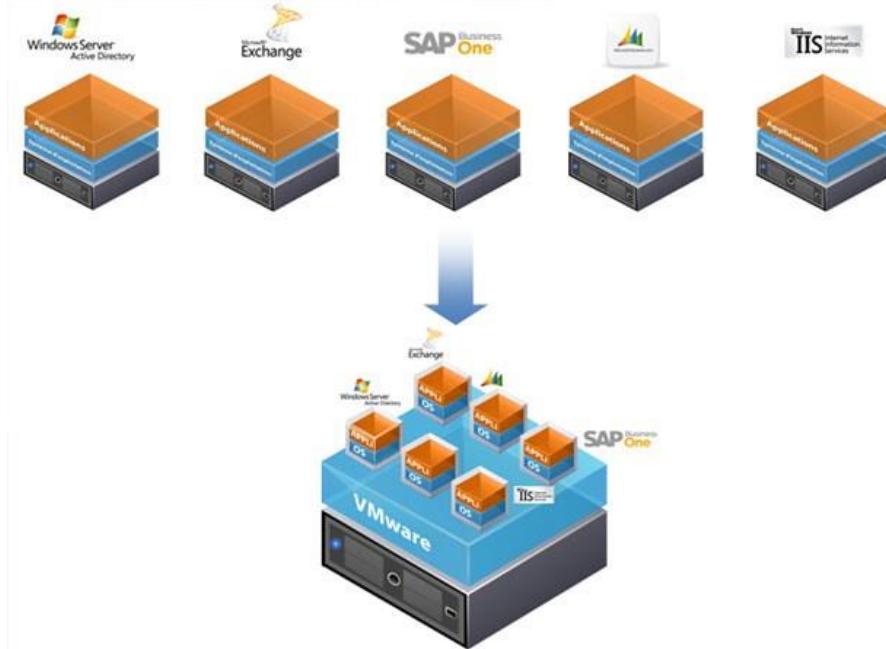


Figure 16 : Virtualisation de serveur

2. Historique :

Dans les années 80-90, des technologies de virtualisation ont vu le jour sur les ordinateurs personnels. Ces solutions étaient principalement logicielles, mais pouvaient également être associées à du matériel supplémentaire tel que des processeurs ou des cartes réseau. Il était alors possible d'utiliser des ordinateurs Amiga dotés de processeurs hétérogènes tels que le 80386 et 80486, 68xxx et PPC pour exécuter d'autres systèmes d'exploitation tels que Windows, Mac OS ou des distributions Linux, le tout en multitâche sous AmigaOS. Des émulateurs tels que le SideCar et PC Task étaient également disponibles pour les PC, tandis qu'Emplant et ShapeShifter étaient utilisés sur Macintosh.

Vers la fin des années 90 et le début des années 2000, les émulateurs de machines anciennes telles que les ordinateurs Atari, Amiga, Amstrad et les consoles NES, SNES et Neo-GEO AES ont connu un grand succès sur les architectures x86. C'est à cette époque que VMware a développé et popularisé un système propriétaire de virtualisation logicielle pour les architectures x86, suivi par des logiciels libres tels que Xen, KVM, QEMU, Bochs, Linux-VServer et Virtual Box, ainsi que des logiciels propriétaires gratuits tels que VirtualPC, Virtual Server et VMware Server, qui ont permis la démocratisation de la virtualisation sur les architectures x86.

3. Pourquoi virtualiser ?

- Diminution du nombre de serveurs
- Réduction de la surface utilisée dans les datacenters
- Baisse de la consommation d'énergie des datacenters
- Réduction des frais d'administration

4. Hyperviseur :

Un hyperviseur est une plateforme de virtualisation qui permet à plusieurs systèmes d'exploitation de s'exécuter simultanément sur une seule machine physique.

On distingue généralement deux types d'hyperviseurs :

a) Hyperviseur type 1 :

Un hyperviseur de type 1 est un logiciel qui fonctionne directement sur une plateforme matérielle. Cette plateforme est alors utilisée comme outil de contrôle pour le système d'exploitation, ce qui permet à un système d'exploitation secondaire d'être exécuté au-dessus du matériel.

L'hyperviseur de type 1 est un noyau hôte léger et optimisé qui est conçu pour exécuter des noyaux de systèmes d'exploitation invités adaptés et optimisés pour cette architecture spécifique.

Ces systèmes invités sont "conscients" d'être virtualisés. Sur des processeurs dotés des instructions de virtualisation matérielle (AMD-V et Intel VT), le système d'exploitation créé n'a plus besoin d'être modifié pour pouvoir fonctionner dans un hyperviseur de type 1.

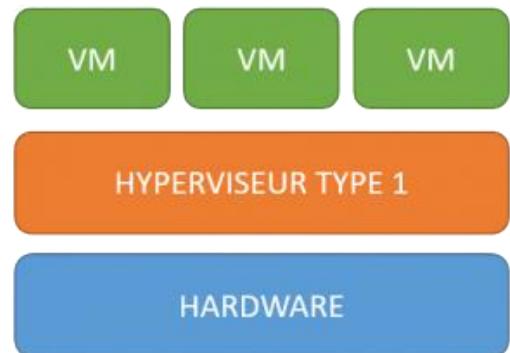


Figure 17 : Hyperviseur type 1

b) Hyperviseur type 2 :

Un hyperviseur de Type 2 est un logiciel qui s'exécute à l'intérieur d'un autre système d'exploitation, permettant ainsi à un système d'exploitation invité de s'exécuter en troisième niveau au-dessus du matériel. Contrairement à l'hyperviseur de Type 1, les systèmes d'exploitation invités exécutés sous un hyperviseur de Type 2 n'ont pas conscience d'être virtualisés, et par conséquent, ils n'ont pas besoin d'être adaptés à nouveau pour fonctionner correctement.

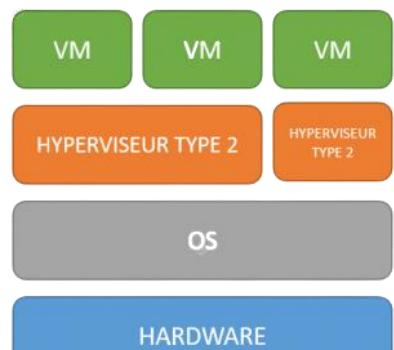


Figure 18 : Hyperviseur type 2

II. Virtualisation des serveurs :

La virtualisation des serveurs est un processus qui permet de faire fonctionner plusieurs serveurs virtuels sur un même serveur physique. Chaque serveur virtuel est capable de faire tourner son propre système d'exploitation de manière indépendante. L'objectif de cette méthode est de mutualiser les ressources de chaque serveur, afin d'optimiser leur utilisation et de maximiser leur efficacité.

1. VMware vSphere :

VMware vSphere est une solution de virtualisation qui permet de simplifier les infrastructures informatiques et de fournir des services informatiques hautement fiables. Cette solution permet de virtualiser les ressources matérielles sous-jacentes et de les combiner pour créer des pools de ressources virtuelles dans le centre de données. En tant que système d'exploitation infonuagique, VMware vSphere gère de grandes quantités d'infrastructure, telles que le CPU, le stockage et la gestion de réseau, pour créer un environnement opérationnel continu et dynamique. Il permet également de gérer la complexité du centre de données en utilisant les couches de composants suivantes.

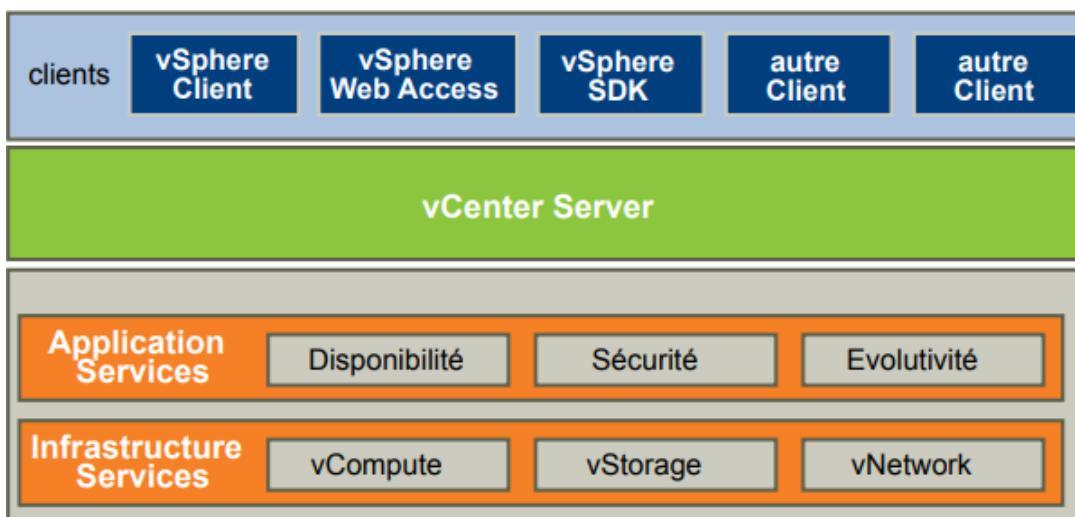


Figure 19 : Couches composants VMware vSphere

2. VMware ESX et ESXi :

Les composants VMware ESX et ESXi peuvent être mis en place comme des éléments de la plateforme VMware vSphere ou de la suite de produits VMware View pour permettre la gestion centralisée des applications du datacenter et des postes de travail de l'entreprise, ainsi qu'une amélioration de la qualité de service. Ces composants présentent des avantages tels que la consolidation des serveurs de production et une protection avancée à moindre coût grâce à la continuité d'activité.

Nous avons également la possibilité de télécharger VMware ESXi pour créer et gérer des machines virtuelles sous forme de solution de virtualisation sur un serveur autonome.

3. VMware vSphere 6.7 :

Le vSphere 6.7.0 offre des services cruciaux pour les environnements de cloud hybride contemporains, permettant d'alimenter les applications modernes, l'IA/ML et les applications d'entreprise critiques. Les utilisateurs peuvent déployer leurs applications en utilisant une combinaison de machines virtuelles, de conteneurs et de Kubernetes. En outre, vSphere 6.7.0 avec Kubernetes, accessible via VMware Cloud Foundation, propose des services de gestion axés sur les applications ainsi que des fonctionnalités de VMware Cloud Foundation pour simplifier le développement, améliorer les opérations et stimuler l'innovation.



Figure 20 : Logo du VMware vSphere

4. Installation de VMware vSphere ESXi 6.7 :

Pour utiliser **VMware vSphere ESXi 6.7.0** en toute simplicité, il est crucial de l'installer sur un serveur équipé d'un processeur qui supporte la technologie Intel-VT ou AMD-V. Ces technologies permettent l'exécution simultanée de plusieurs systèmes d'exploitation sur une même puce.

Après avoir démarré le serveur à partir de l'ISO, deux options s'offrent à nous : démarrer le serveur à partir du programme d'installation ou du disque local. Puisque le disque local ne contient aucun système d'exploitation installé, nous allons sélectionner la première option, c'est-à-dire démarrer à partir du programme d'installation.

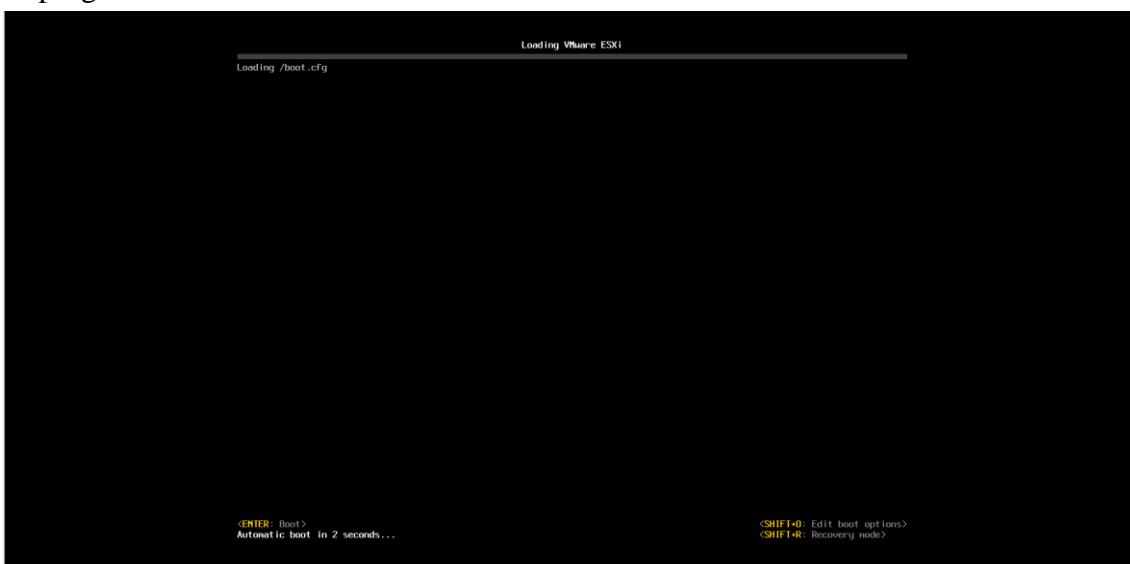


Figure 21 : démarrage de programme d'installation.

- Le processus de sélection du programme d'installation standard consiste à démarrer le serveur et à charger le fichier d'installation d'ESXi, puis attendre le chargement des fichiers d'installation.



Figure 22 : le chargement des fichiers d'installation.

- Une fois que le programme d'installation aura chargé tous les éléments, un message de bienvenu apparaît, vous invitant à vérifier si votre serveur est compatible avec VMware vSphere ESXi 7.8

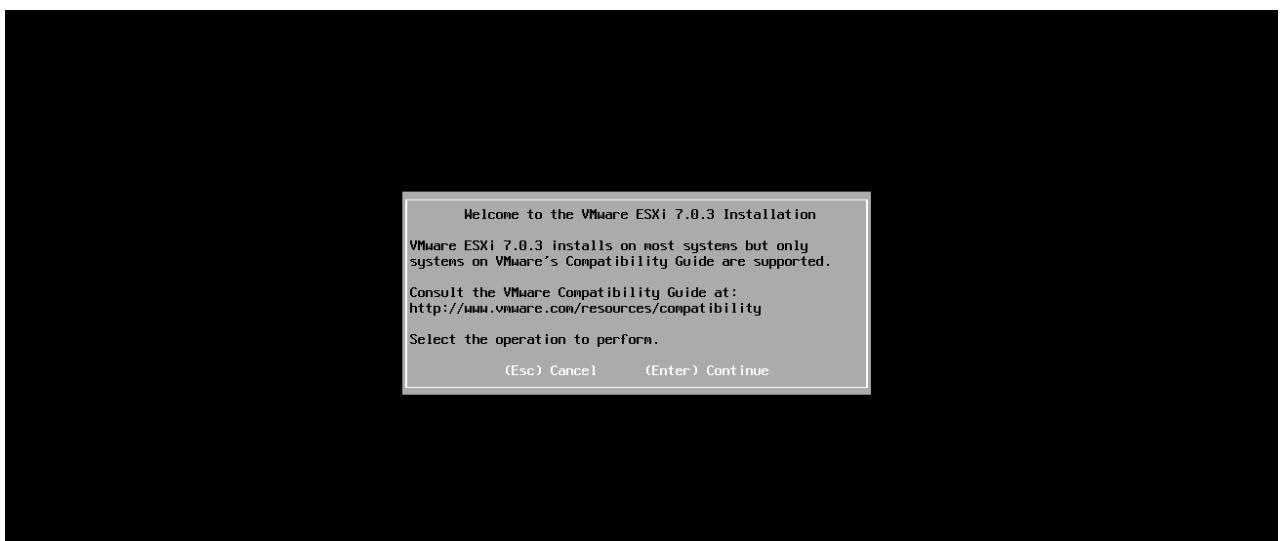


Figure 23 : Le message de bienvenu de serveur

- Si ce dernier est compatible, pressez la touche "F11" pour Validez l'End User License Agreement.

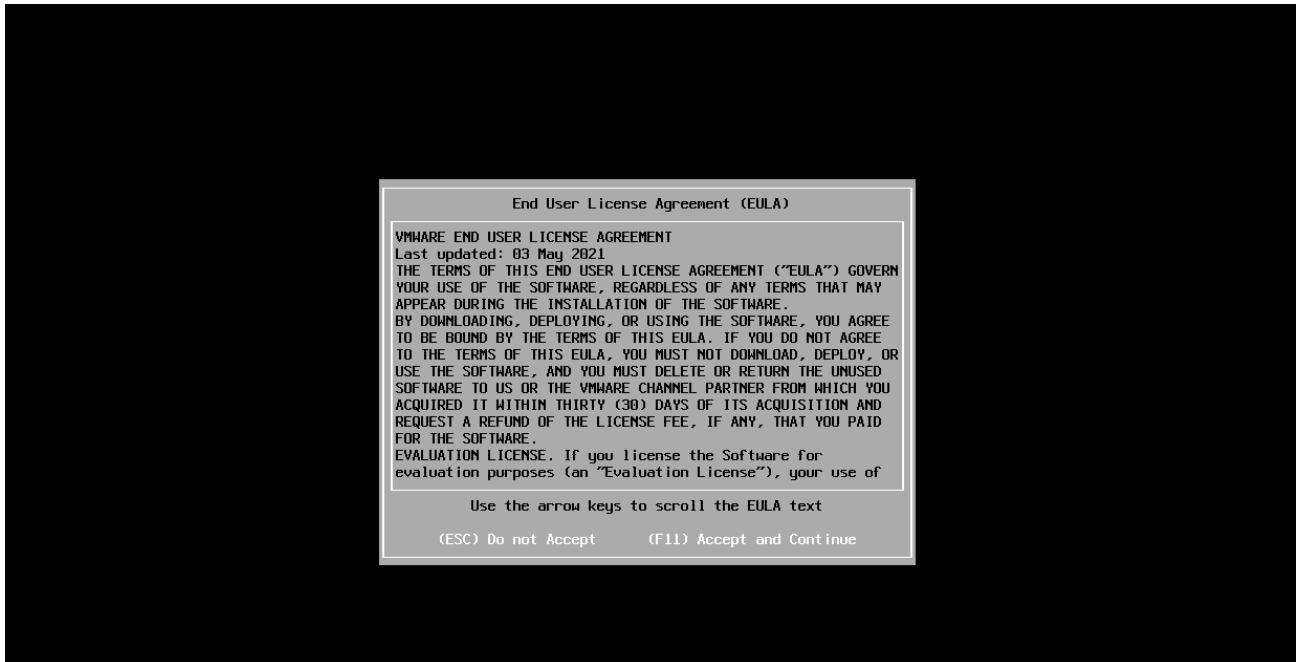


Figure 24 : Validation de l'End User License Agreement.

- Lorsque vous accédez à la fenêtre « Sélectionner un disque à installer ou à mettre à niveau », vous pouvez visualiser l'ensemble des disques locaux connectés au serveur. Dans ce cas précis, un seul disque est présent sur le serveur. Pour poursuivre l'installation, appuyez sur la touche Entrée.

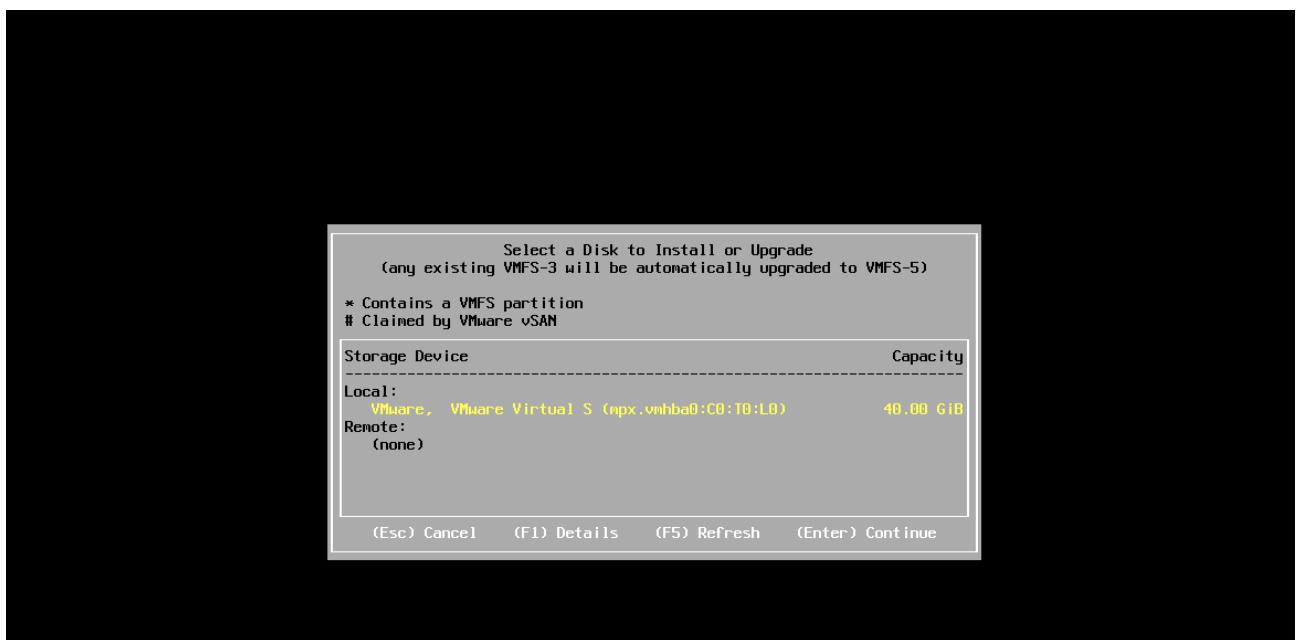


Figure 25 : La sélection du disque dur

- Sélectionnez la langue du clavier et appuyez sur Entrée pour continuer



Figure 26 : La sélection de la langue de serveur

- Root est le super-utilisateur prédéfini de VMWare ESXi 6.7.0, attribuez le mot de passe root et appuyez sur Entrée pour continuer :

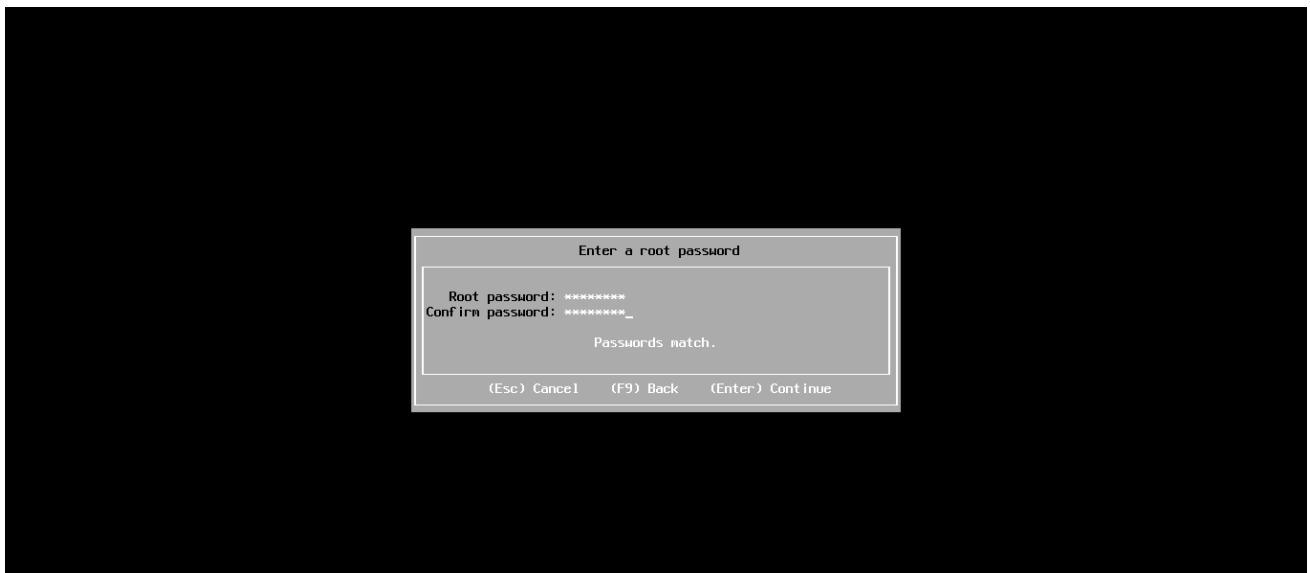


Figure 27 : La saisie de mot de passe

- Après un scan rapide du matériel, un message de vérification va s'afficher vous demandant de confirmer l'installation sur le disque précédemment choisi, Pressez F11 pour lancer l'installation.

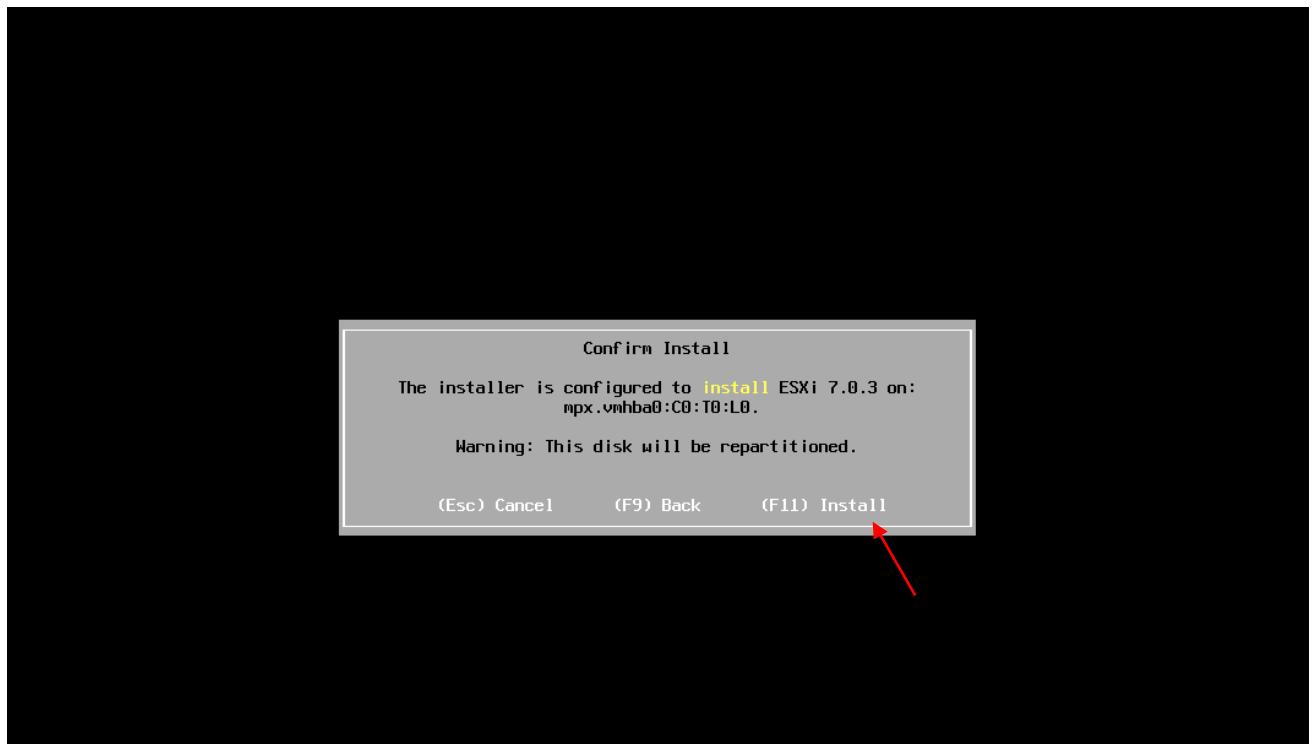


Figure 28 : La confirmation de l'installation

- L'installation de vSphere peut prendre plusieurs minutes. Une fois l'installation terminée, vous devriez avoir un message confirmant le succès de l'installation de cette dernière.

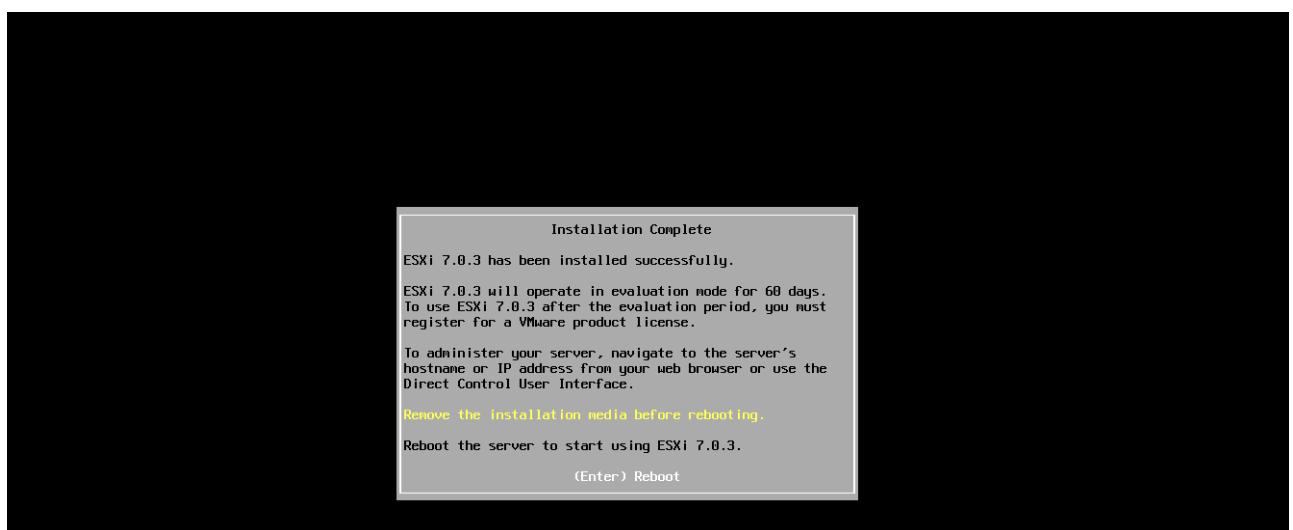


Figure 29 : Le succès de l'installation

- Votre serveur a besoin de redémarrer pour continuer. Appuyez sur "Entrer" pour lancer le redémarrage.



Figure 30 : Le redémarrage du serveur

III. Configuration de VMware vSphere ESXi 6.7.0 :

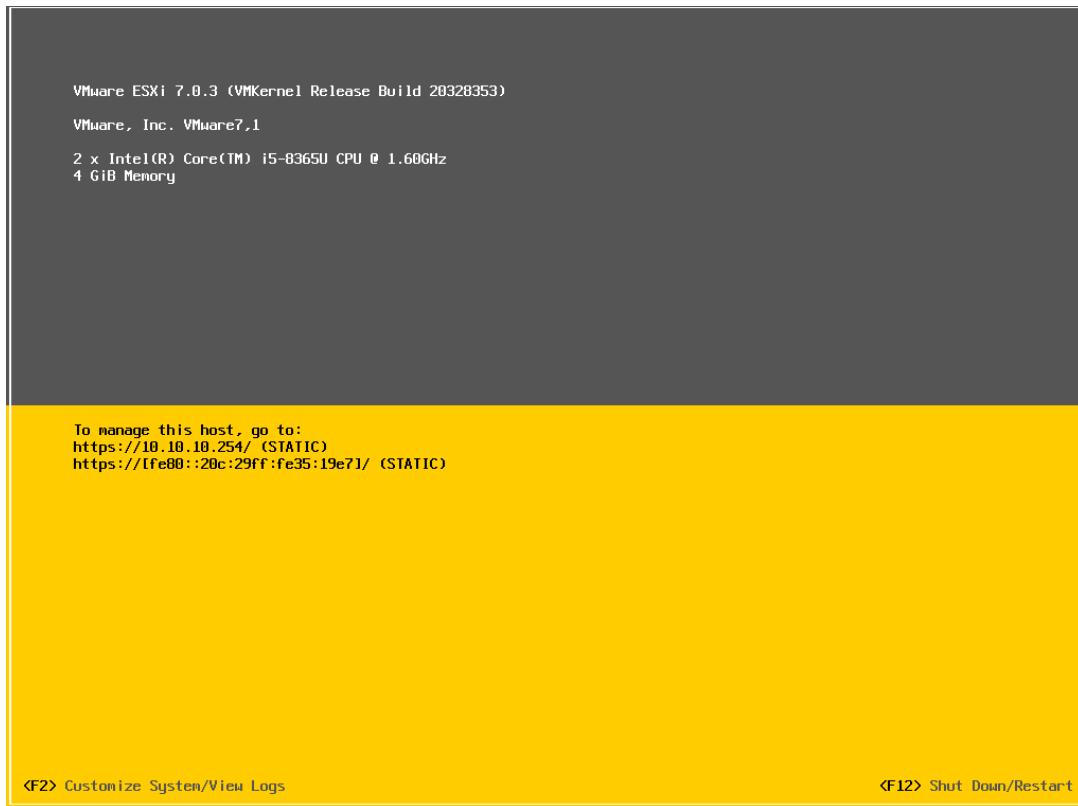


Figure 31 : Affectation de l'adresse IP

- Afin de gérer VMware vSphere ESXi 6.7.0, nous allons passer l'adresse IP de notre serveur en Statique. En effet, par défaut, l'adresse est distribuée par DHCP. Pour renseigner une IP fixe à notre serveur, appuyez sur la touche F2.
- Elle donnera accès au panneau d'administration du serveur. Cependant, vous devrez renseigner le login et le mot de passe que vous avez dû mettre lors de l'installation du serveur.

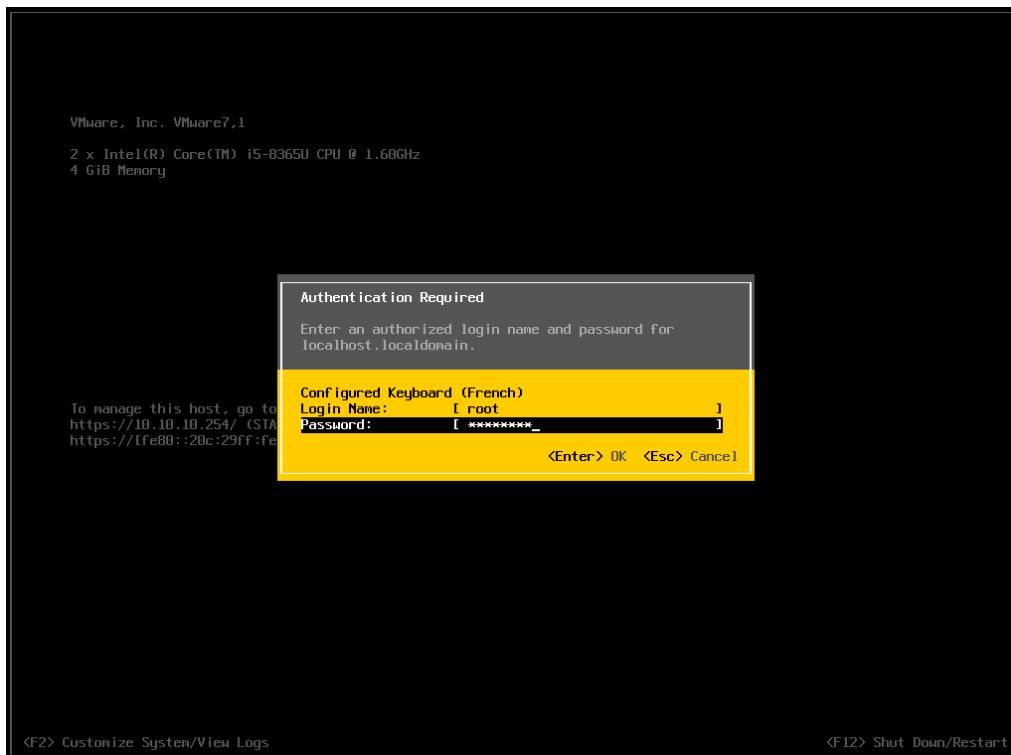


Figure 32 : Authentification au serveur

- Dans la fenêtre de personnalisation du système, sélectionnez l'option « Configure Management Network » et appuyez sur le bouton « Entrée ».
- Et pour les besoins de notre projet, nous allons préciser le VLAN, Sur le « Configure Management Network », sélectionnez une option de configuration VLAN, nous allons entrer l'adresse IP appartient au VLAN des administrateurs :

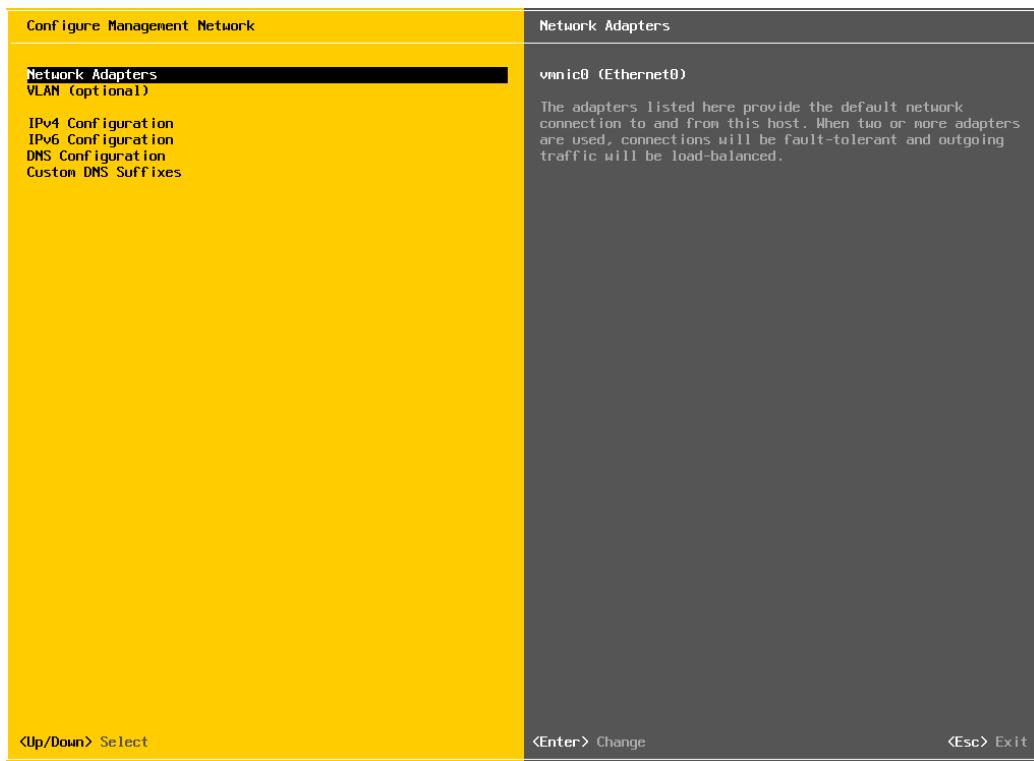


Figure 33 : sélection de l'option de configuration VLAN

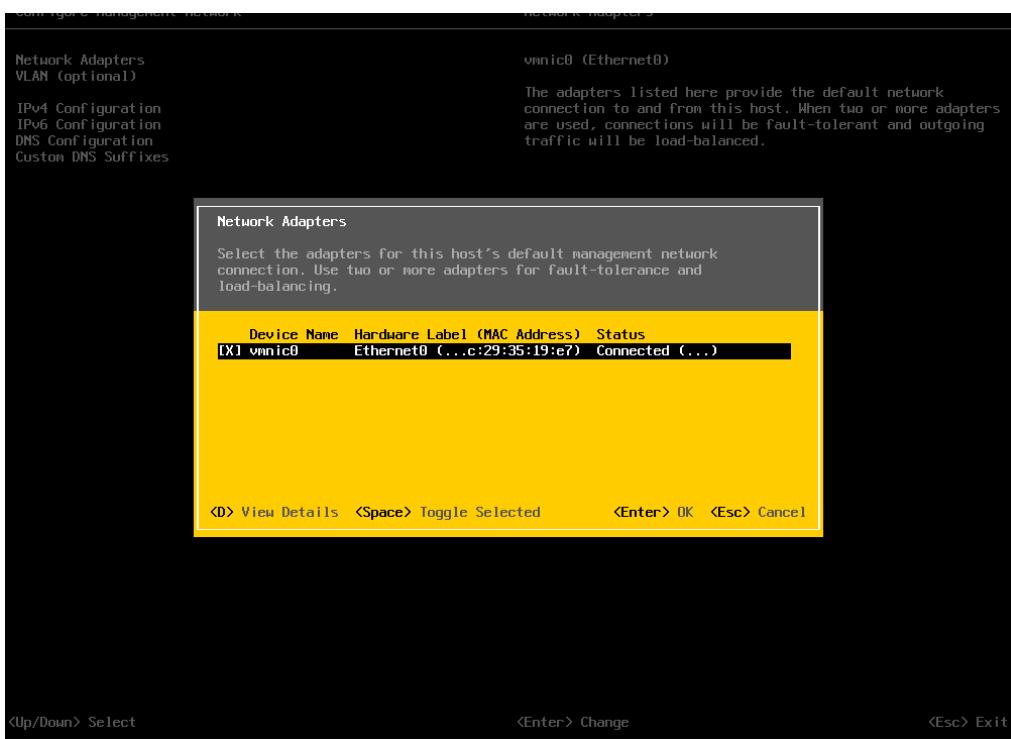


Figure 34 : Le choix de la carte réseau

- Changez votre configuration IP en sélectionnant, avec la barre Espace : "Set static IP addresses and Network Configuration" Puis renseigner l'IP de votre choix.

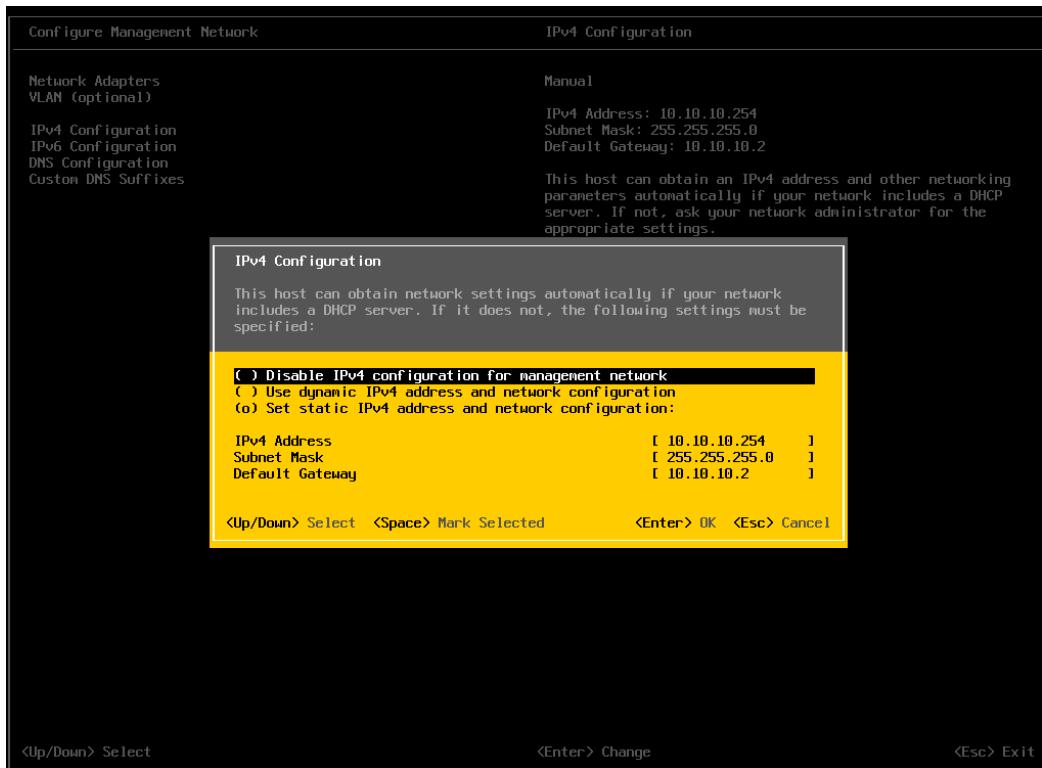


Figure 35 : La saisie de l'adresse IP souhaitée

1. La configuration des VLAN :

Selon notre plan, nous allons utiliser le serveur que nous avons exploité pour la virtualisation dans les trois VLAN que nous avons créé. Afin de le faire, nous devons configurer ces VLAN dans le switch de l'ESXI en allant dans la fenêtre de mise en réseau et en sélectionnant le groupe de port approprié.

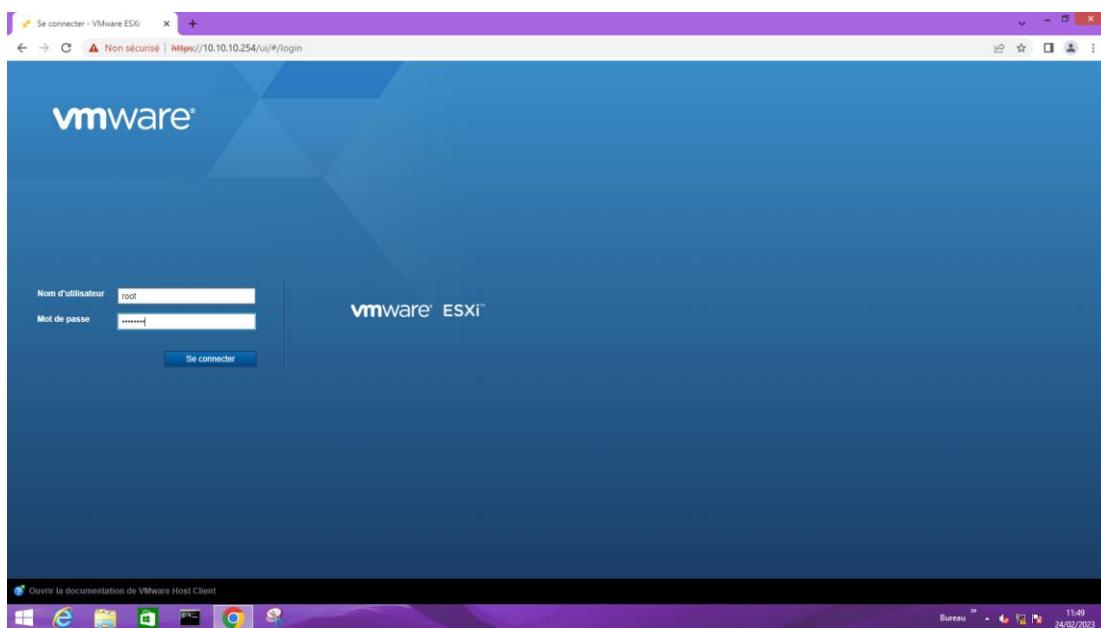


Figure 36 : Page d'authentification VMware ESXi

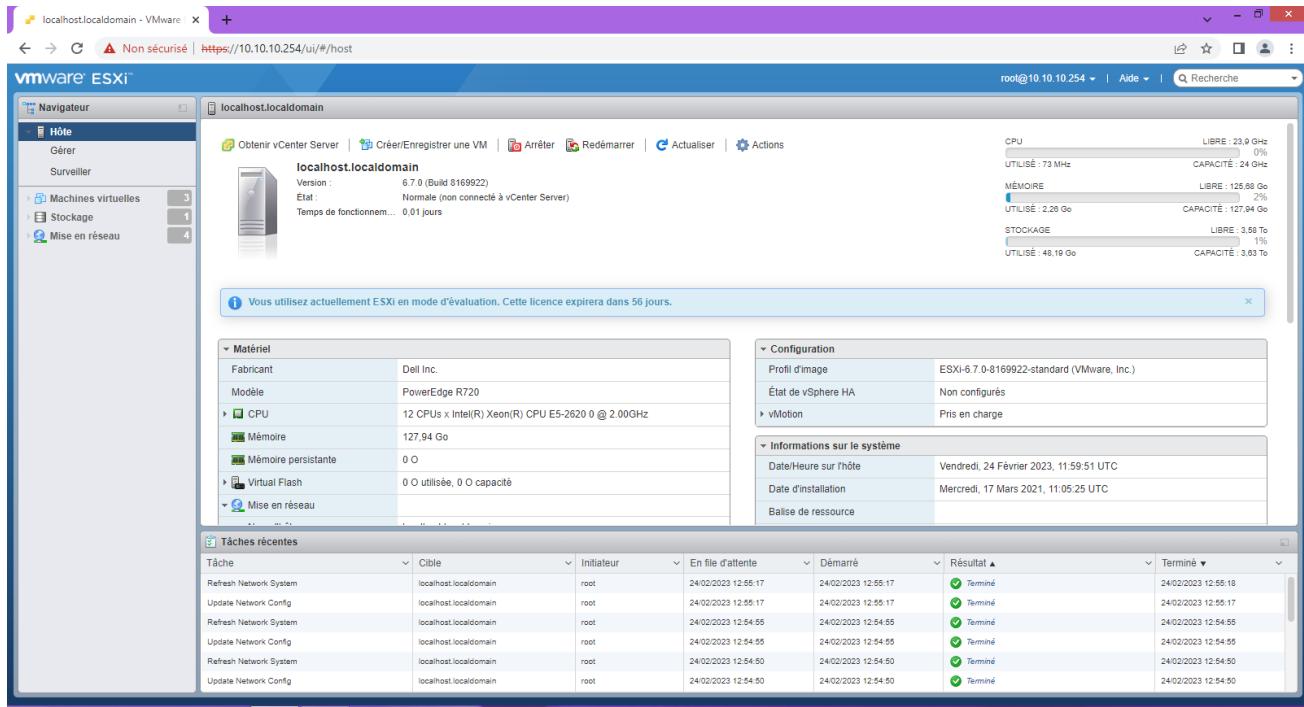


Figure 38 : Page d'accueil de VMware ESXi

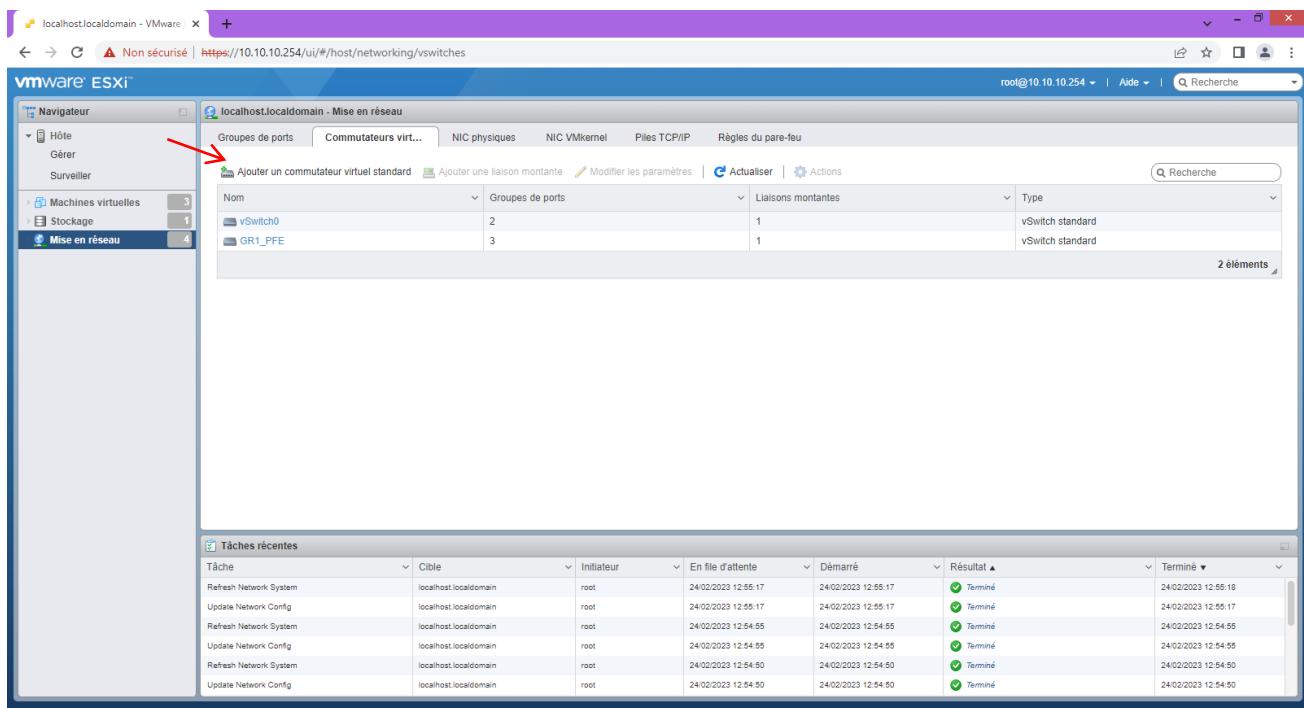


Figure 37 : L'ajout d'un commutateur virtuel standard

- On va ajouter un switch virtuel et l'associer à un port physique du serveur en cliquant sur « Ajouter un commutateur virtuel standard »

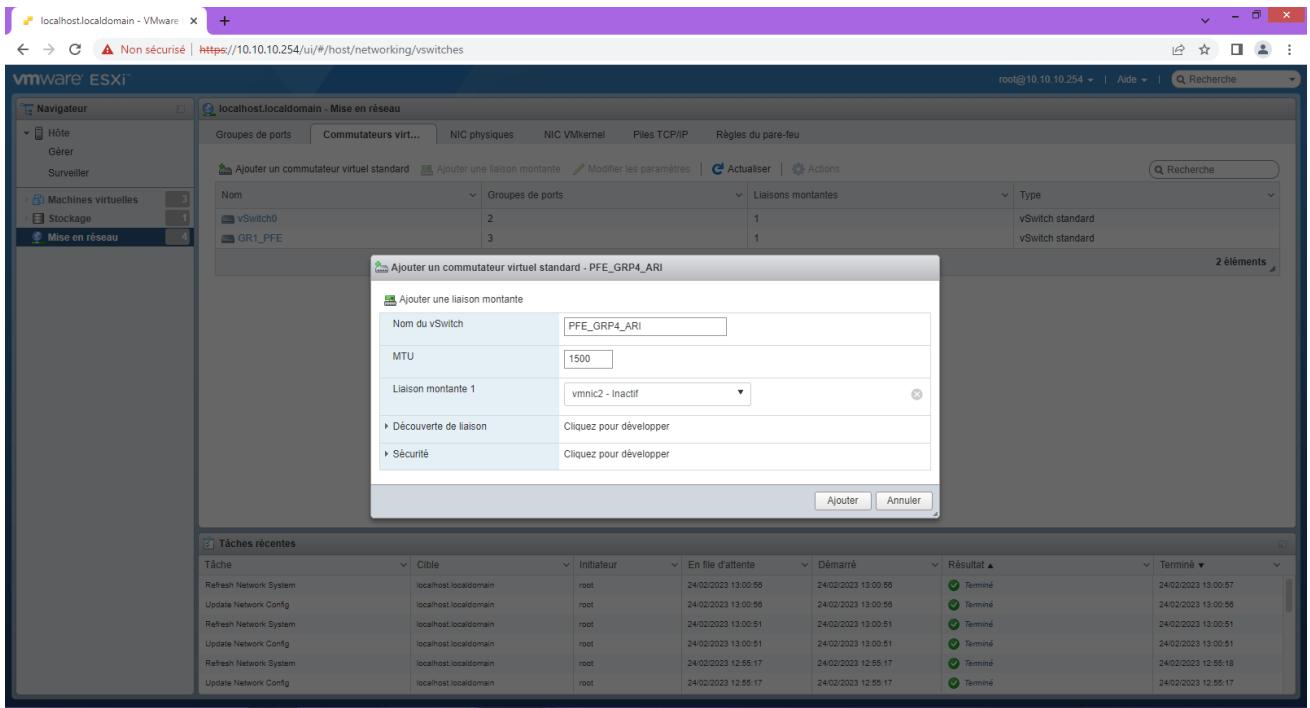


Figure 39 : L'ajout d'un switch virtuel

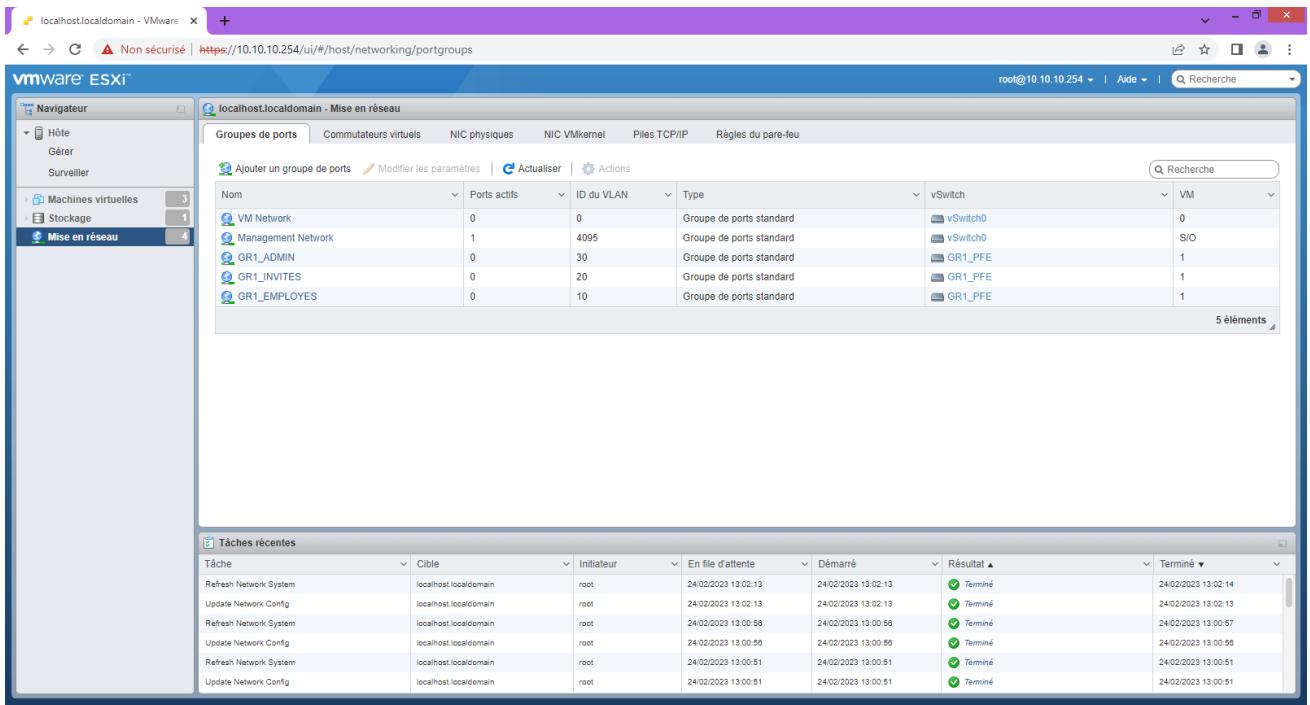


Figure 40 : La page "Mise en réseau"

- On clique sur « Ajouter un groupe de ports », ensuite on donne le nom du vlan, l'ID et le commutateur virtuel.

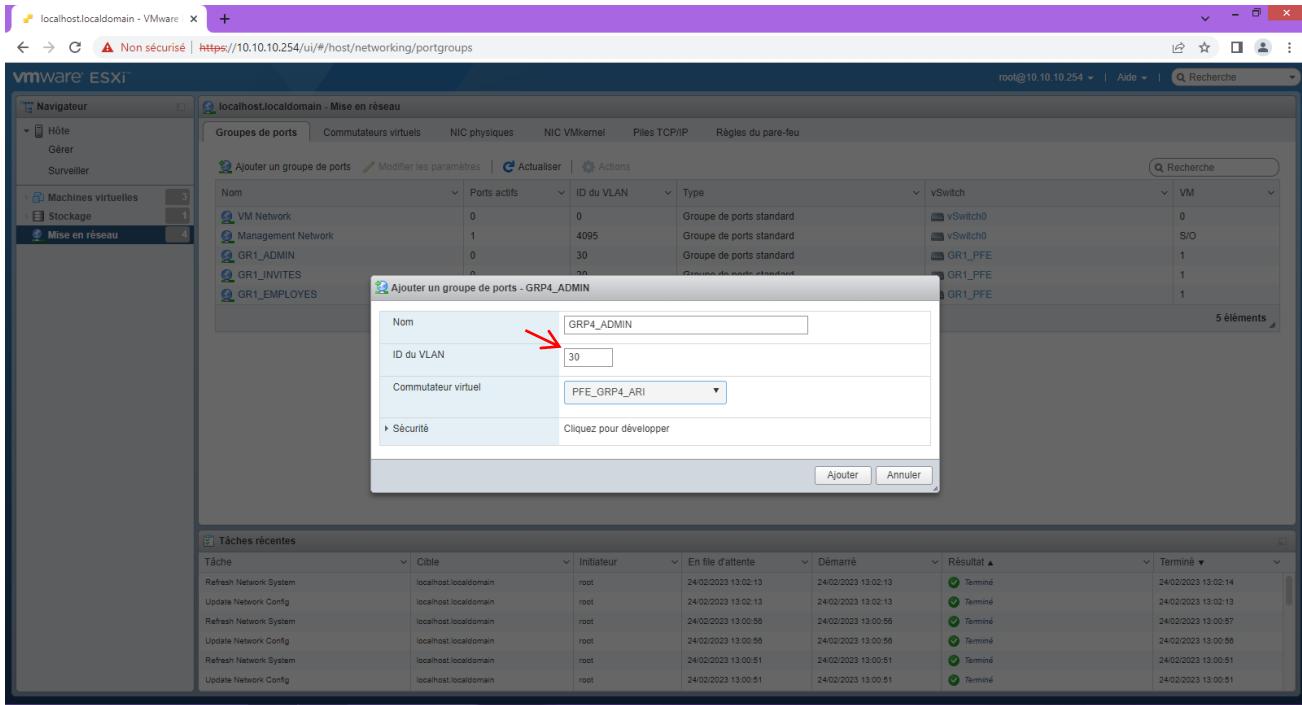


Figure 41 : La création de VLAN des administrateurs

- On commence par la création des VLAN.

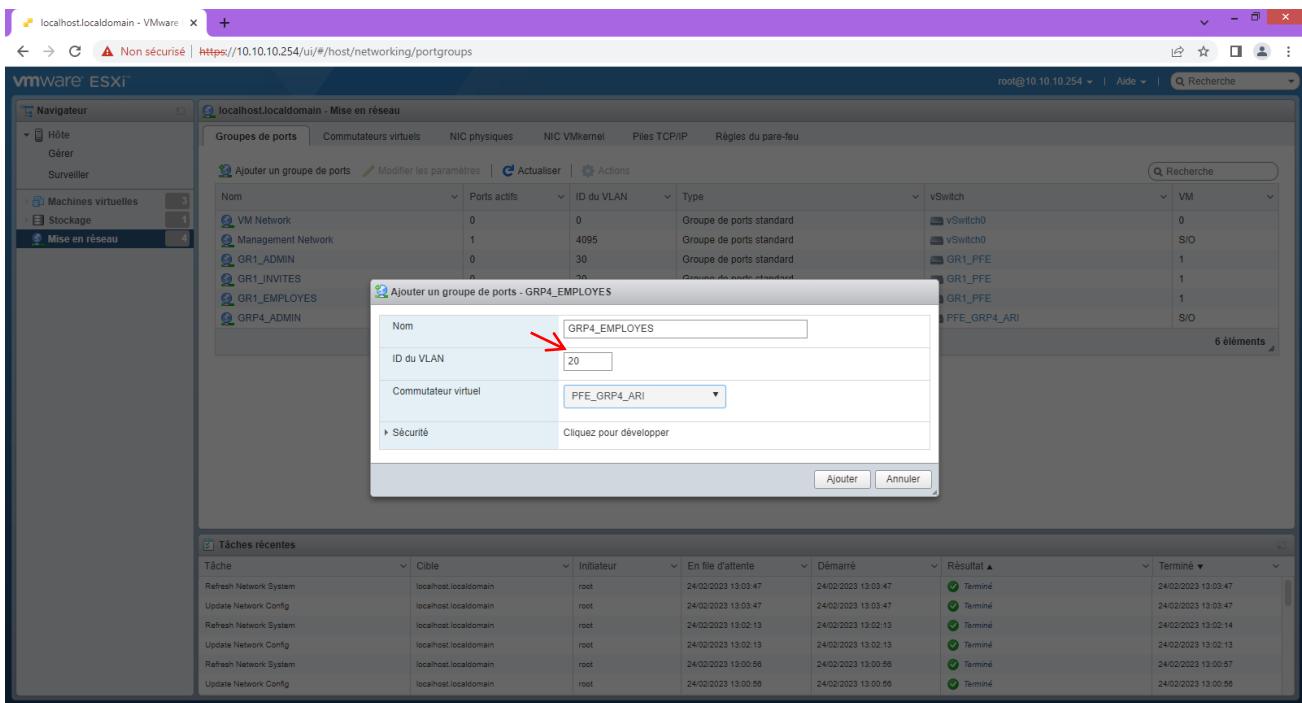


Figure 42 : La création de VLAN des employés

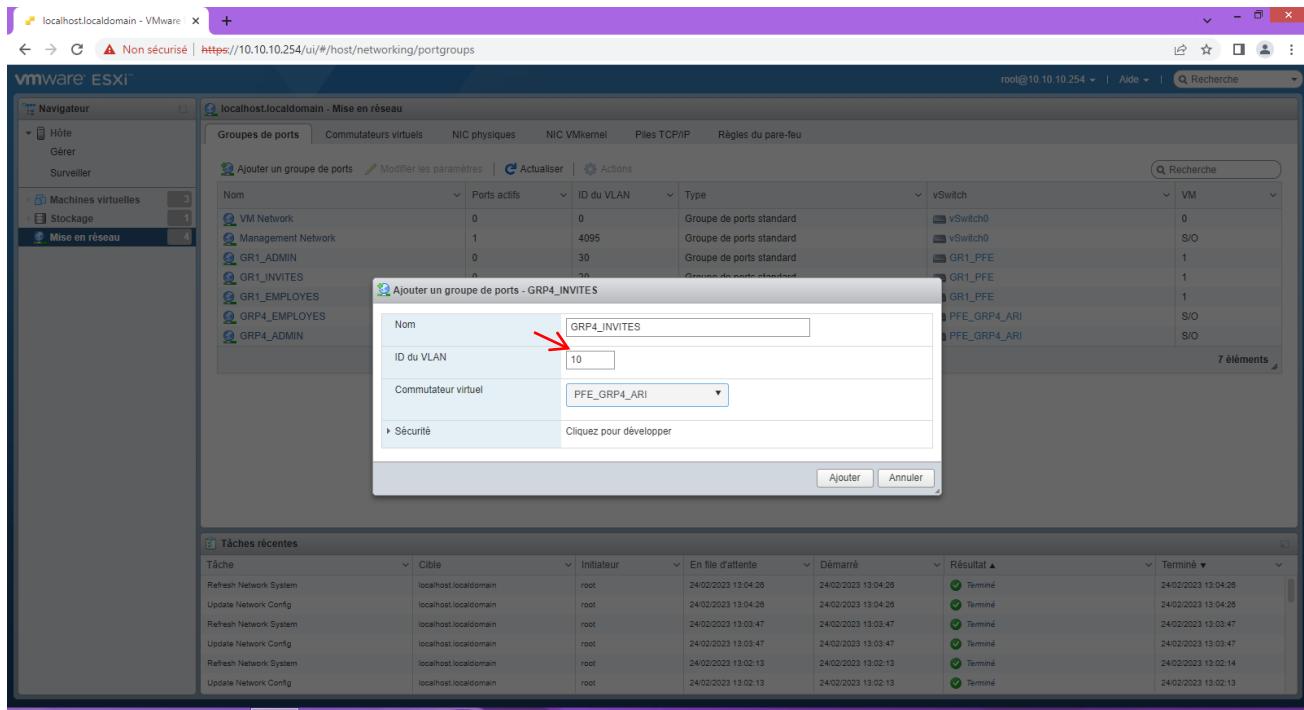


Figure 43 : La création de VLAN des invités

- Et voilà on a créé les trois VLAN : le premier est pour les administrateurs, le deuxième est pour les employés et le dernier est pour les invités.
- Ensuite, on clique sur « Machine virtuelle » et sélectionnez « Créer / Enregistrer une machine virtuelle ». Cela ouvrira un assistant et vous guidera tout au long du processus de création de la configuration de la machine virtuelle.

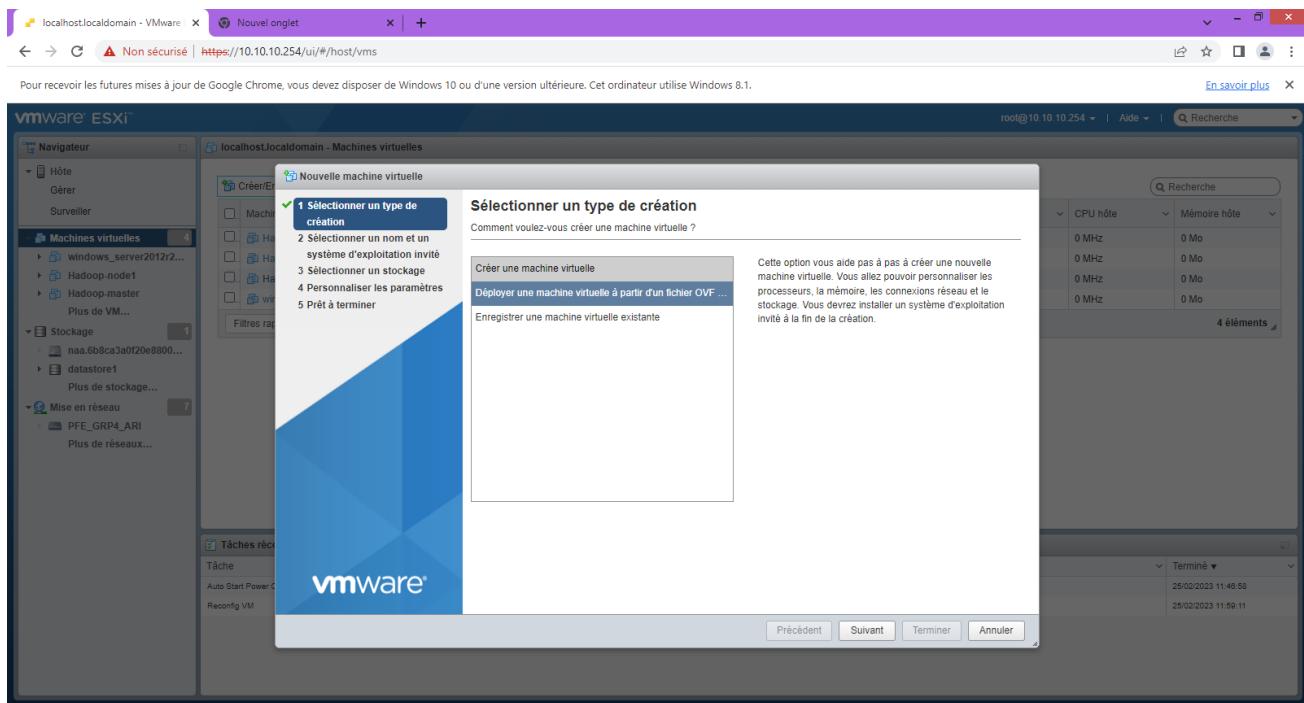


Figure 44 : L'ajout d'une machine virtuelle

- Après avoir sélectionné « Créer un nouvel ordinateur virtuel », la boîte de dialogue et l'assistant « Créer un nouvel ordinateur virtuel » seront affichés. Cela vous permet de spécifier vos exigences pour la machine virtuelle : le nombre de processeurs, la quantité de mémoire, le stockage requis et la carte réseau. Il s'agit des exigences de base nécessaires à la création d'une machine virtuelle.
- L'assistant de création de machine virtuelle crée la configuration ou le modèle pour que nous puissions installer notre système d'exploitation ultérieurement. Il inclut des modèles de spécification, basés sur les exigences minimales du fournisseur pour le système d'exploitation. On sélectionne « Créer une machine virtuelle ».

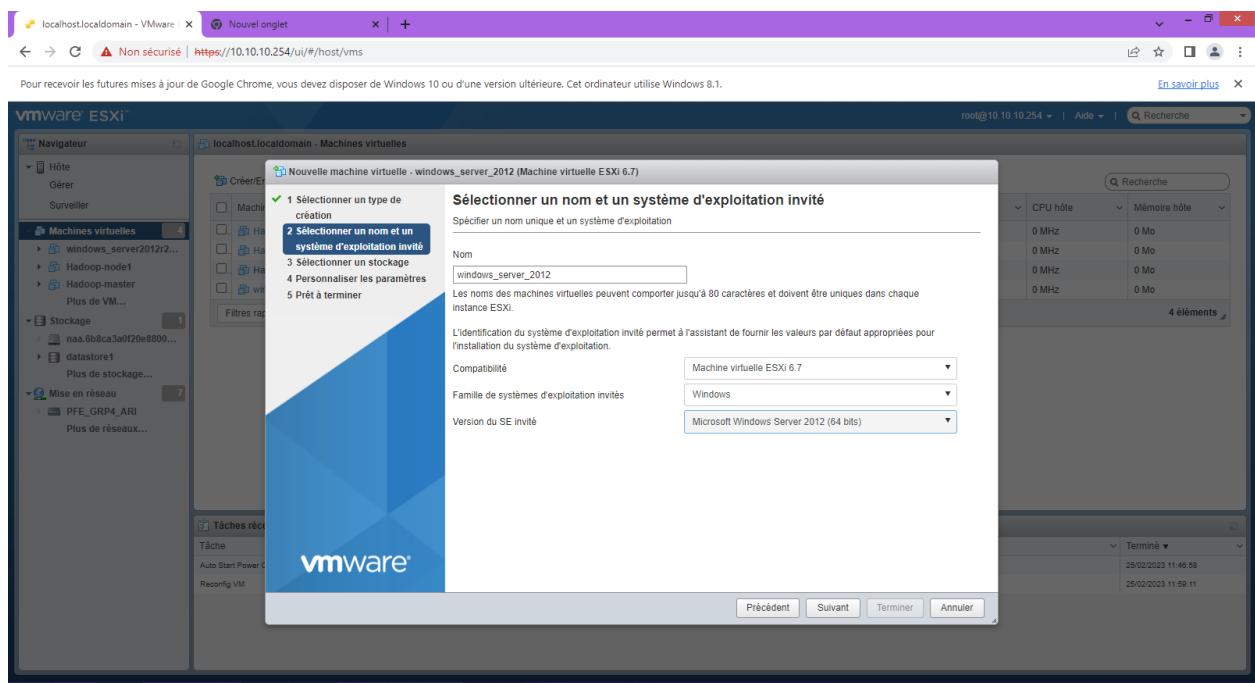


Figure 45 : La saisie du nom et le système de la machine virtuelle

- On entre un nom pour la machine virtuelle et cliquez sur « Suivant ». C'est le nom qui apparaîtra dans l'inventaire, il ne faut pas le confondre avec le nom d'hôte du système d'exploitation, qui sera défini lors de l'installation du OS.

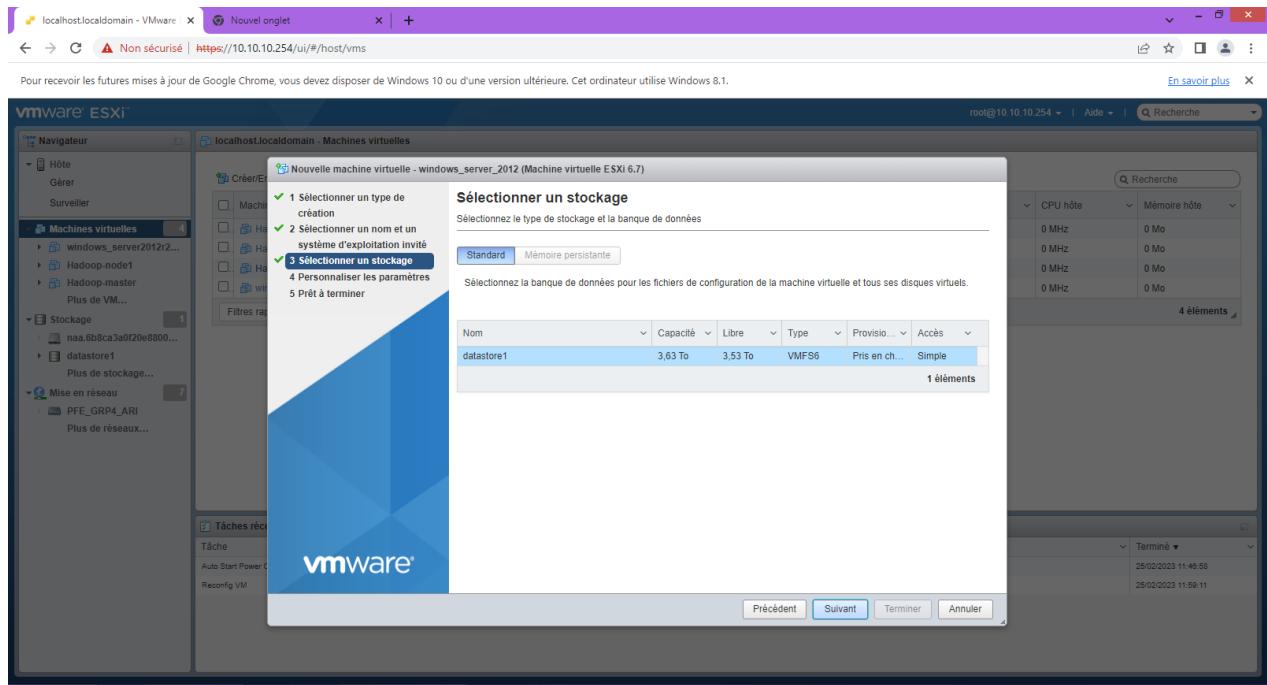


Figure 46 : La sélection de stockage

- Sélectionnez la banque de données de stockage à utiliser pour stocker la machine virtuelle

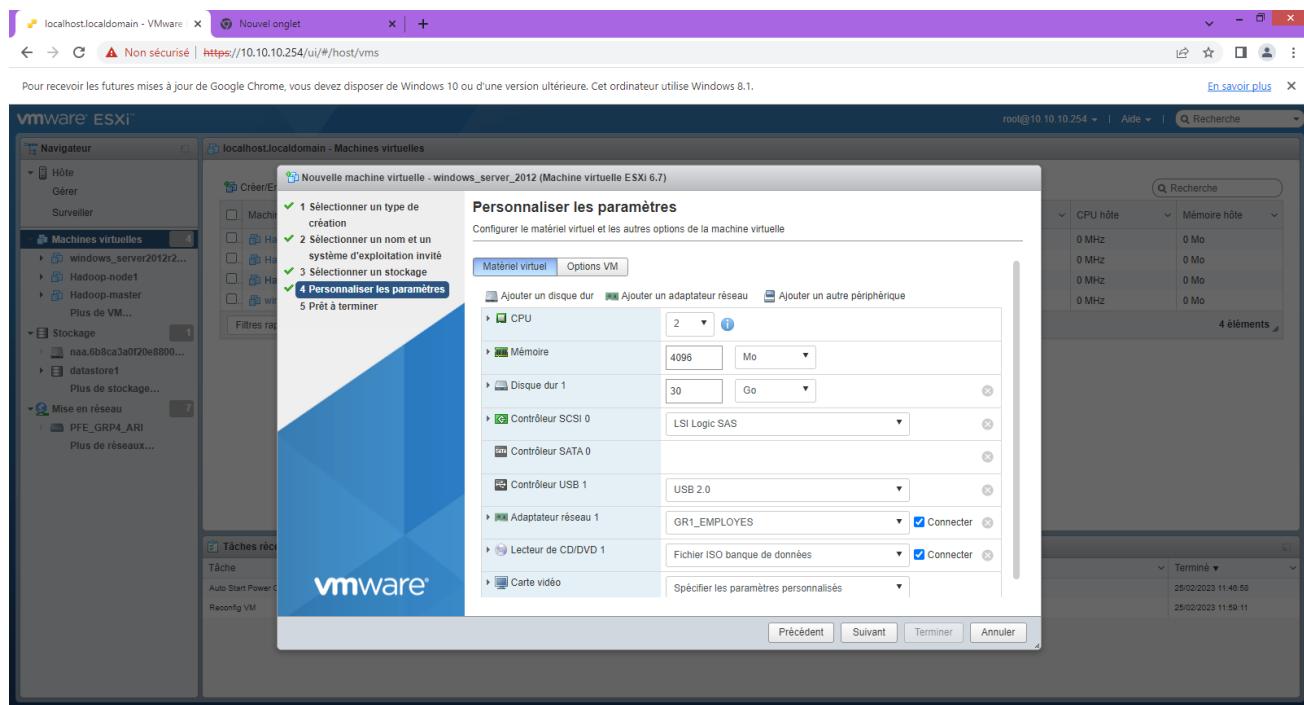


Figure 47 : Configuration matérielle de la machine virtuelle

- On configure les options supplémentaires relatives au matériel et à la machine virtuelle, puis clique sur Suivant pour continuer.

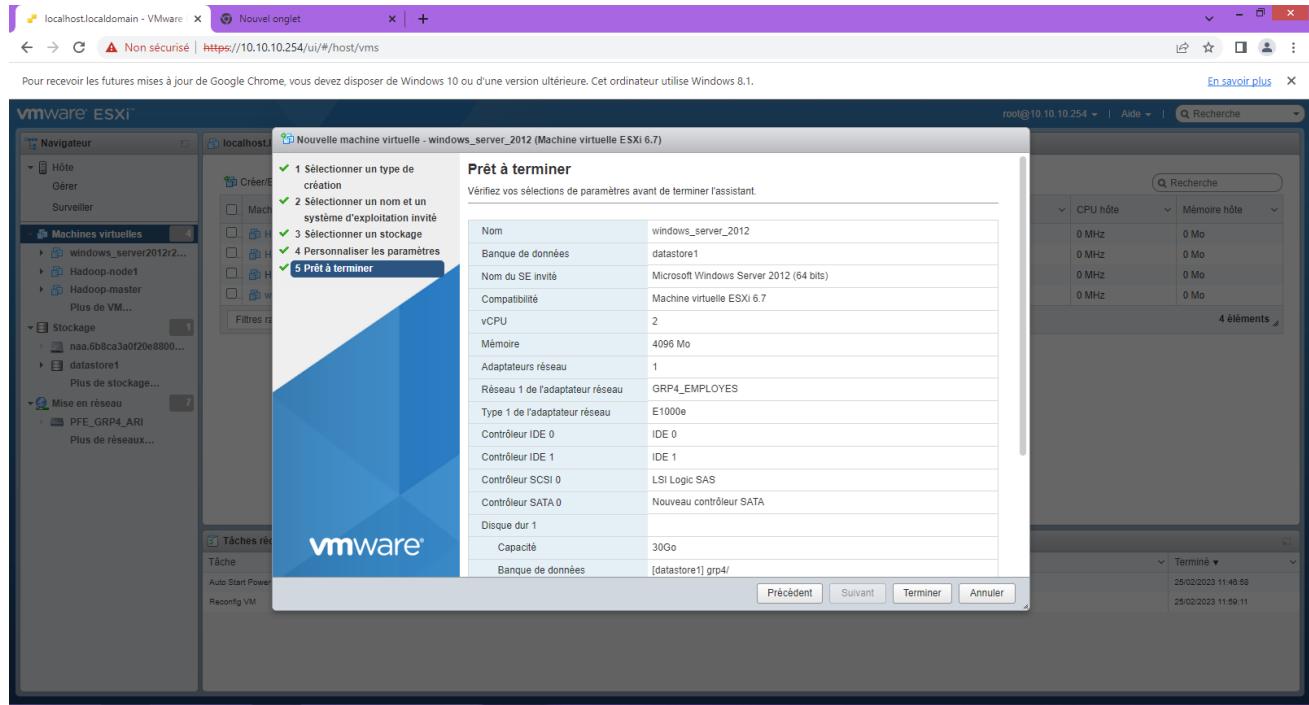


Figure 48 : La finalisation de l'installation

- Cliquez sur « Terminer » pour créer la configuration de la machine virtuelle. La machine virtuelle sera créée. On vérifie l'inventaire des hôtes, notre machine virtuelle apparaîtra - "windows_server2012r2_grp4" dans l'inventaire :

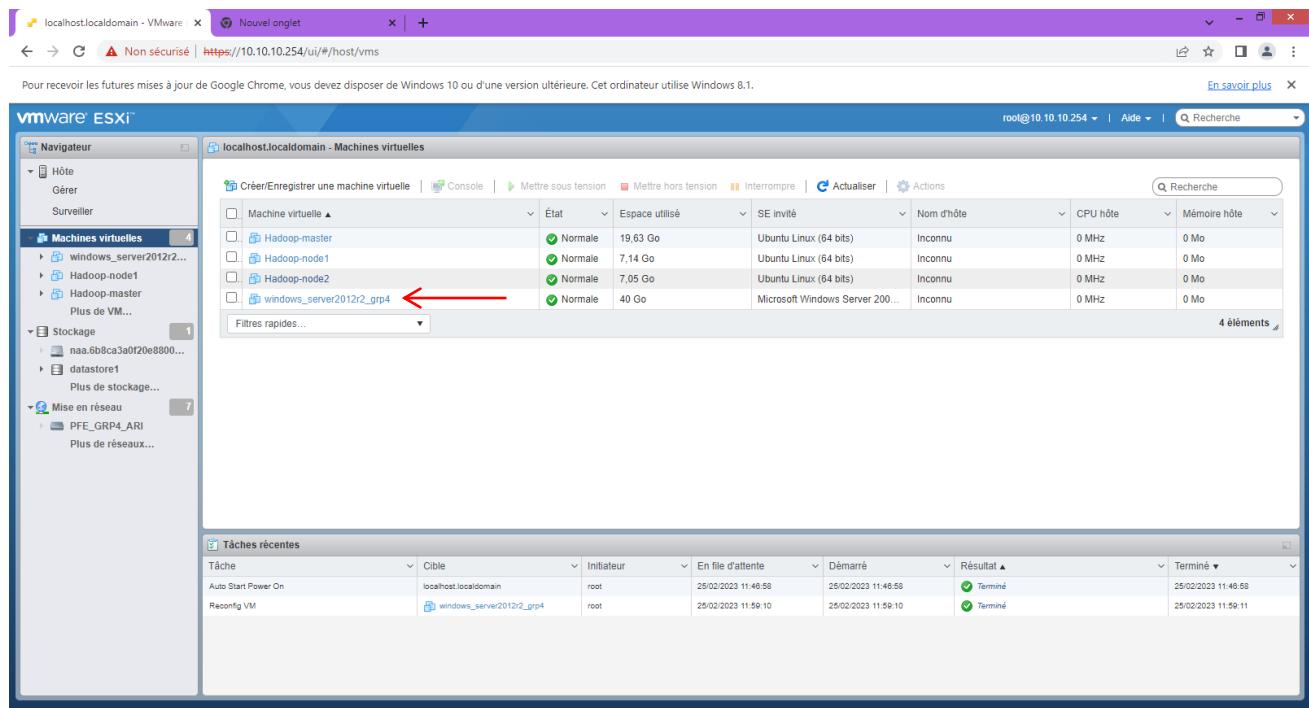


Figure 49 : L'ajout de la machine virtuelle

Chapitre IV : Mise en œuvre du réseau des employés

I.Services réseaux :

1. Système des noms de domaine DNS :

a) Définition :

Le **DNS** (Domain Name System) ou système de noms de domaine, permet de traduire les requêtes de noms en adresses IP. Les serveurs DNS permettent aux utilisateurs d'Internet de ne pas avoir à se souvenir des adresses IP, mais seulement des noms de domaine.

Le fonctionnement d'un serveur DNS est similaire à celui d'un annuaire pour ordinateur. Lorsque vous souhaitez accéder à un ordinateur sur le réseau, votre ordinateur interroge le serveur DNS pour obtenir l'adresse de l'ordinateur que vous voulez contacter. Après avoir récupéré cette adresse, votre ordinateur peut directement communiquer avec le destinataire en utilisant son adresse IP.

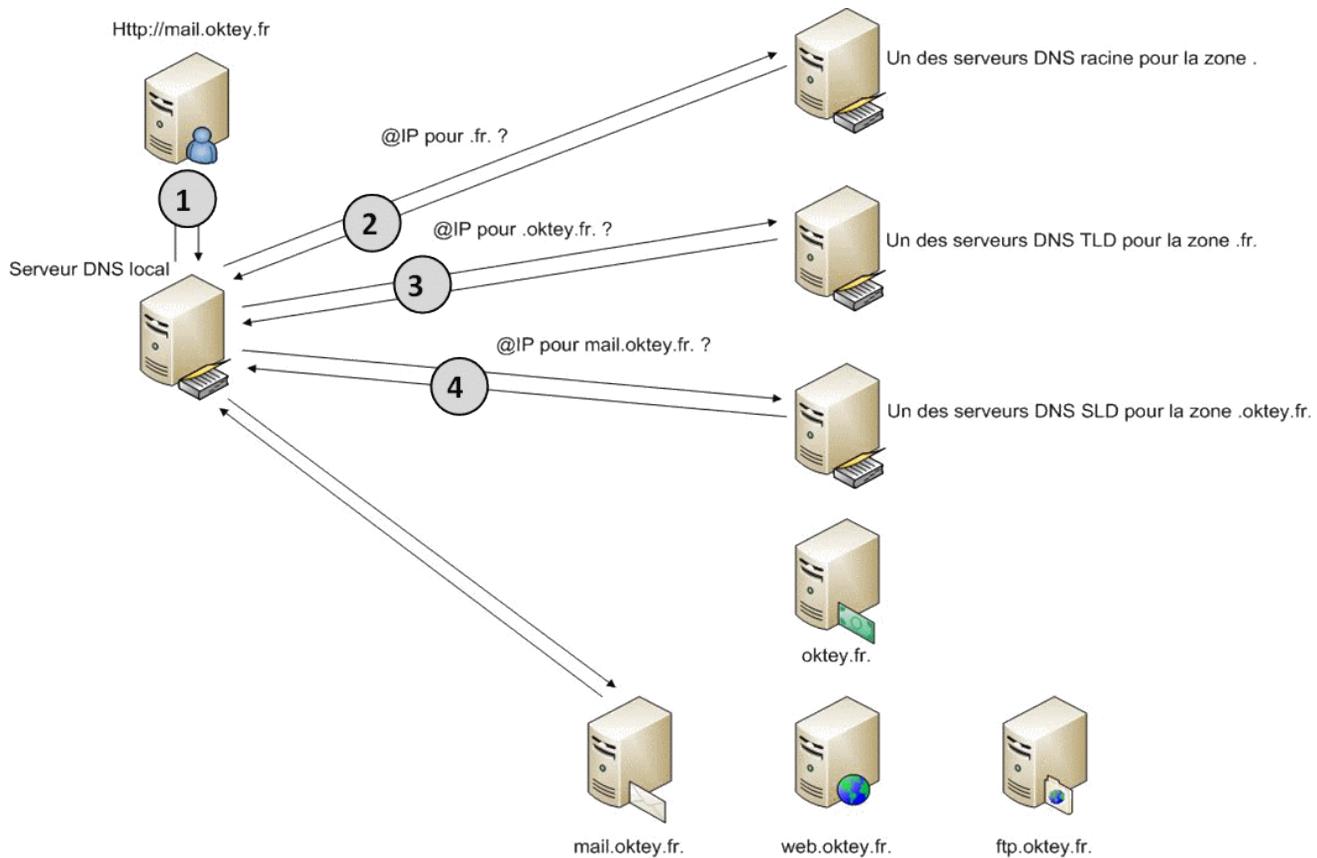


Figure 50 : Fonctionnement du DNS

b) Fonctionnement d'un DNS :

Le processus de résolution DNS consiste à transformer un nom d'hôte (par exemple www.est.s.com) en une adresse IP (telle que 192.168.10.2).

Le serveur de noms faisant autorité est celui où les administrateurs gèrent les noms de serveur et les adresses IP de leurs domaines. Lorsqu'un administrateur de DNS souhaite modifier, ajouter ou supprimer un nom de serveur ou une adresse IP, il effectue une mise à jour sur son serveur DNS faisant autorité (parfois appelé "serveur DNS maître").

Il existe également des serveurs DNS "esclaves" qui possèdent des copies des enregistrements DNS pour leurs zones et leurs domaines.

c) Types de DNS :

Il existe deux types de services DNS sur Internet, chacun traitant les requêtes DNS différemment en fonction de leur fonctionnalité :

- **Le résolveur DNS récursif** répond à la requête en cherchant soit le serveur de noms faisant autorité, soit un cache DNS contenant le résultat de la requête.
- **Le serveur DNS faisant autorité** contient le résultat de la requête DNS et n'a donc pas besoin d'interroger un autre serveur.

d) Hiérarchie d'un DNS :

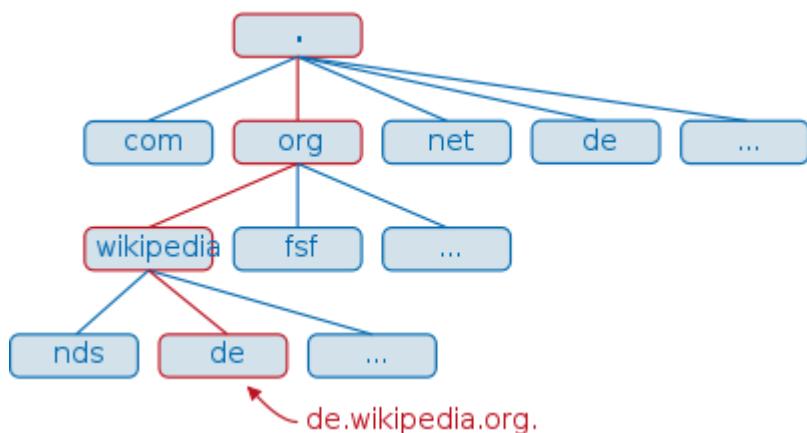


Figure 51 : Hiérarchie d'un DNS

Le système des noms de domaine fonctionne selon une hiérarchie où la racine est au sommet. On peut créer des sous-domaines et des délégations pour ces derniers, qui peuvent eux-mêmes déléguer à d'autres serveurs. Les délégations créent des zones, des ensembles de domaines et de sous-domaines configurés sur un serveur donné. Les domaines de premier niveau sont les domaines immédiatement sous la racine, appelés TLD, et les noms de domaines sont résolus en parcourant la hiérarchie de droite à gauche en suivant les délégations successives. Un nom de domaine doit être correctement délégué dans le domaine de niveau supérieur pour fonctionner correctement.

e) Résolution du nom par un hôte :

Lorsqu'un hôte doit résoudre un nom de domaine, il fait appel à un serveur DNS récursif qui parcourt la hiérarchie DNS pour fournir une réponse. Les adresses IP de ces serveurs récursifs sont souvent obtenues via DHCP ou configurées en dur sur la machine hôte. Les fournisseurs d'accès à Internet mettent également à disposition de leurs clients ces serveurs récursifs. Le processus itératif de recherche de l'adresse IP commence avec les serveurs racine et se poursuit avec les serveurs DNS pour la zone appropriée jusqu'à ce que l'adresse IP soit trouvée. Les serveurs DNS récursifs font également office de cache pour optimiser les requêtes ultérieures. Les noms de domaine peuvent utiliser plusieurs serveurs DNS primaires et secondaires pour garantir une continuité dans la résolution des noms en cas de panne d'un serveur DNS.

f) Résolution inverse :

Les recherches DNS inversées pour les adresses IPv4 utilisent le domaine spécial in-addr.arpa. Pour représenter une adresse IPv4, une séquence de quatre nombres décimaux est concaténée, séparée par des points, avec le suffixe de domaine de second niveau .in-addr.arpa. Les quatre nombres décimaux sont obtenus en scindant l'adresse IPv4 32 bits en quatre octets et en les convertissant en nombres décimaux, puis en les concaténant dans l'ordre inverse de la convention décimale par points. Ainsi, pour rechercher l'adresse IP 8.8.4.4, l'enregistrement PTR pour le nom de domaine 4.4.8.8.in-addr.arpa serait recherché et trouvé pour pointer vers google-public-dns-b.google.com. Si l'enregistrement A pour google-public-dns-b.google.com pointait à son tour vers 8.8.4.4, cela confirmerait l'adresse IP précédemment recherchée.

2. Protocole de configuration dynamique des hôtes (DHCP) :

a) Définition :

DHCP (Dynamic Host Configuration Protocol) est un protocole de gestion de réseau qui automatise et gère de manière centralisée l'attribution dynamique d'une adresse IP (Internet Protocol) à chaque périphérique ou nœud d'un réseau afin qu'ils puissent communiquer via IP. DHCP permet d'éviter la tâche fastidieuse d'attribuer manuellement des adresses IP à tous les périphériques d'un réseau, et est utilisé sur des réseaux locaux de petite taille ainsi que sur des réseaux d'entreprise de grande taille.

Le DHCP attribue automatiquement de nouvelles adresses IP lorsque les périphériques sont déplacés d'un endroit à l'autre, évitant ainsi aux administrateurs réseau la tâche de configurer manuellement chaque périphérique avec une adresse IP valide ou de reconfigurer le périphérique avec une nouvelle adresse IP s'il est déplacé vers un nouvel emplacement sur le réseau. DHCP est disponible pour une utilisation dans les protocoles Internet version 4 (IPv4) et Internet version 6 (IPv6).

Le fonctionnement du protocole DHCP :

Le protocole DHCP (Dynamic Host Configuration Protocol), qui permet à une machine de se connecter à un réseau et d'obtenir une adresse IP sans intervention manuelle de l'utilisateur. Pour cela, il faut qu'il y ait un serveur DHCP sur le réseau qui distribue les adresses IP et toutes les autres informations de configuration nécessaires. Lorsqu'une machine démarre, elle envoie une requête de type DHCPDISCOVER en broadcast sur le réseau pour trouver un serveur DHCP disponible. Le serveur DHCP répond ensuite avec un paquet de type DHCPOFFER, contenant les premiers paramètres et une adresse IP proposée pour la machine. Si la machine accepte cette adresse, elle envoie une requête DHCPREQUEST pour valider son adresse IP, puis le serveur répond avec un paquet de type DHCPACK, qui contient l'adresse IP confirmée pour la machine. Il existe également d'autres types de paquets DHCP qui peuvent être utilisés dans certaines situations, comme DHCPNAK pour signaler une mauvaise configuration réseau ou DHCPRELEASE pour libérer une adresse IP.

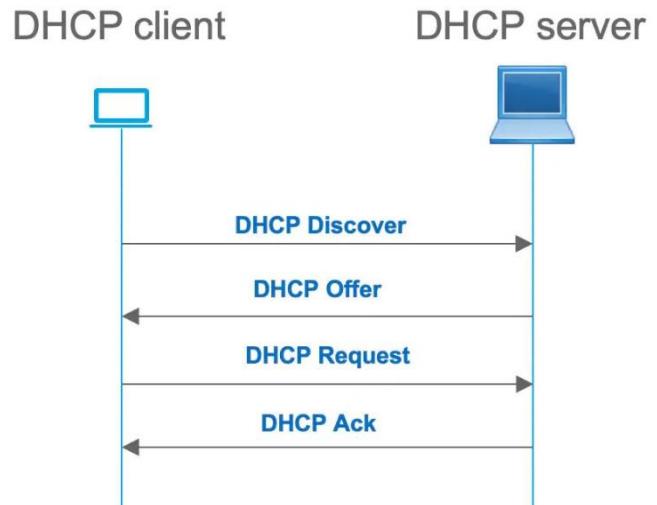


Figure 52 : Le diagramme séquence DHCP

3. Les services d'annuaire LDAP :

LDAP (Lightweight Directory Access Protocol) est un protocole logiciel qui permet de localiser des organisations, des individus et d'autres ressources dans un réseau, que ce soit sur Internet ou sur un intranet d'entreprise. Il est plus léger que DAP (Directory Access Protocol) car il ne contient pas de fonctionnalités de sécurité. LDAP a été approuvé par au moins 40 entreprises et est inclus dans des produits tels que Communicator de Netscape et Active Directory de Microsoft. Il permet de rechercher une personne sans savoir où elle se trouve, ce qui peut faciliter la recherche d'informations dans un réseau.

La hiérarchie "arborescente" d'un annuaire LDAP comprend plusieurs niveaux :

- Commençant par le répertoire racine,
- Suivi par les pays,
- Les organisations,
- Les unités organisationnelles,
- Et enfin les particuliers qui représentent les personnes, fichiers et ressources partagées telles que les imprimantes.

Chaque niveau se branche sur le niveau supérieur.

Il est possible de distribuer un annuaire LDAP sur plusieurs serveurs, chacun ayant une copie synchronisée régulièrement. Chaque serveur LDAP est appelé un agent de système de répertoire (DSA). Lorsqu'un utilisateur envoie une requête à un serveur LDAP, celui-ci prend en charge la demande et la transmet à d'autres DSA si nécessaire, en garantissant une réponse coordonnée et unique pour l'utilisateur.

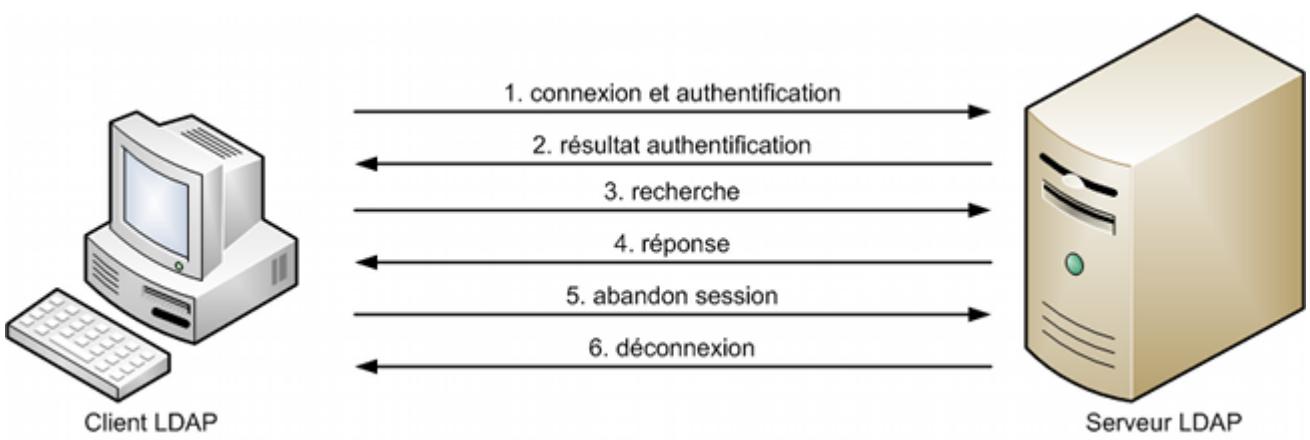


Figure 53 : L'authentification de LDAP

4. Active Directory (AD) :

Active Directory (AD) est un ensemble de services Microsoft qui s'exécutent sur Windows Server et permettent de gérer les autorisations et l'accès aux ressources en réseau. Les données sont stockées sous forme d'objets, qui peuvent être des utilisateurs, des groupes, des applications ou des périphériques. Ces objets sont classés en fonction de leur nom et de leurs attributs, tels que des mots de passe et des clés Secure Shell (SSH).

Le service principal dans Active Directory est AD DS, qui stocke les informations de l'annuaire et gère l'interaction de l'utilisateur avec le domaine. AD DS contrôle l'accès des utilisateurs aux ressources en vérifiant les informations d'identification lorsqu'un utilisateur se connecte à un périphérique ou tente de se connecter à un serveur via un réseau. Les autres produits Microsoft, tels que Exchange Server et SharePoint Server, utilisent AD DS pour fournir un accès aux ressources.

Le serveur qui héberge AD DS est appelé contrôleur de domaine. Les administrateurs ont généralement un niveau d'accès différent de celui des utilisateurs finaux, ce qui permet à AD DS de contrôler les utilisateurs qui ont accès à chaque ressource.

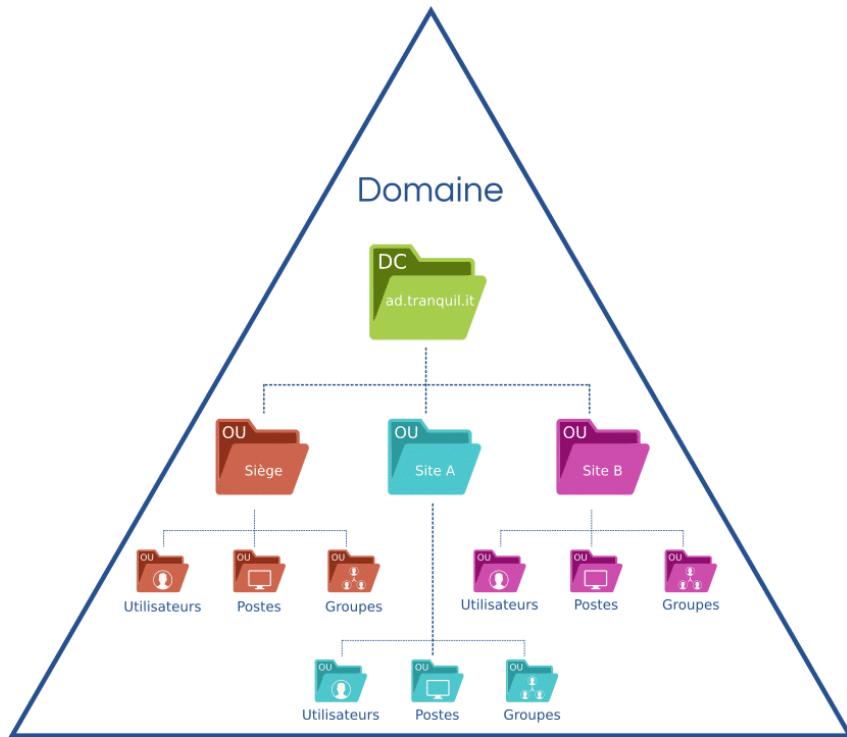


Figure 54 : Active Directory (AD)

5. Active Directory Domain Services (AD DS):

Les AD DS (Active Directory Domain Services) constituent les fonctions essentielles d'Active Directory pour gérer les utilisateurs et les ordinateurs et pour permettre aux administrateurs système d'organiser les données en hiérarchies logiques.

AD DS fournit des certificats de sécurité, l'authentification unique (SSO), LDAP, et la gestion des droits.

La compréhension d'AD DS est une priorité absolue pour les professionnels de la réponse aux incidents et de la cybersécurité. En effet, toutes les cyberattaques affecteront AD et, lorsqu'elles se produisent, vous devez savoir ce qu'il faut rechercher et comment y répondre.

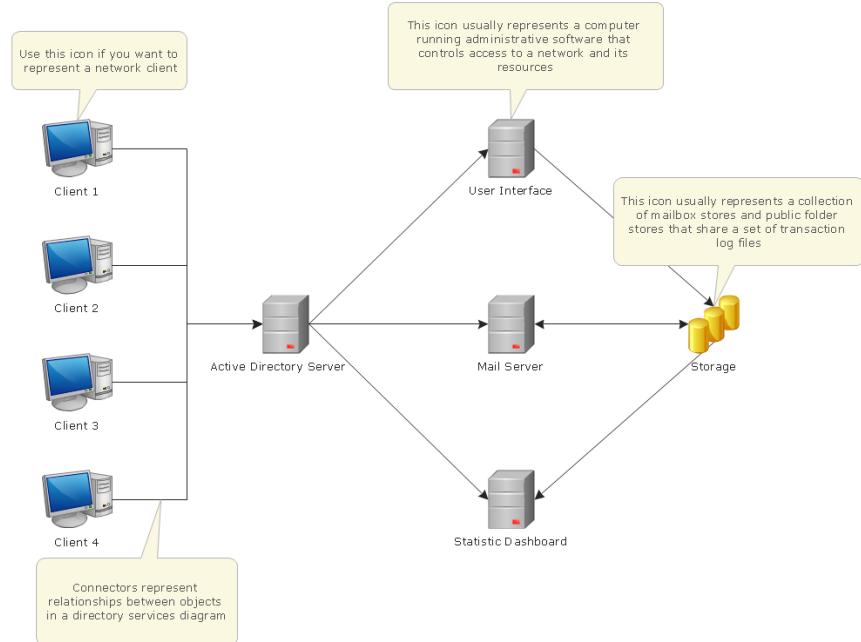


Figure 55 : Active Directory Domain Services (AD DS)

a) Les avantages d'AD DS :

Pour l'administration de base de vos utilisateurs et ordinateurs réseau, l'utilisation d'AD DS présente plusieurs avantages :

- Vous pouvez personnaliser la façon dont vos données sont organisées de façon à répondre aux besoins de votre entreprise
- Si cela s'avère nécessaire, vous pouvez gérer AD DS à partir de n'importe quel ordinateur du réseau
- AD DS fournit une fonction intégrée de réplication et de redondance : si un contrôleur de domaine tombe en panne, un autre contrôleur de domaine prend la charge à son compte
- Tout accès aux ressources réseau passe par AD DS, ce qui assure une gestion centralisée des droits d'accès au réseau

b) Les services fournis par AD DS :

Voici les services fournis par AD DS, qui constituent les fonctionnalités de base d'un système de gestion centralisée des utilisateurs :

- **Services de domaines** : stocke les données et gère les communications entre les utilisateurs et le contrôleur de domaine. Il s'agit de la principale fonctionnalité d'AD DS.
- **Services de certificat** : permet à votre contrôleur de domaine de servir des certificats et des signatures numériques, ainsi qu'un chiffrement à clé publique.
- **Lightweight Directory Services** : prend en charge LDAP pour des services de domaine multiplateformes, par exemple l'ensemble des ordinateurs Linux présents sur votre réseau.
- **Services de fédération d'annuaire** : dans la même session, fournit une authentification SSO pour plusieurs applications. Ainsi, les utilisateurs ne sont pas obligés de ressaisir les mêmes identifiants.
- **Gestion des droits** : contrôle les politiques en matière de droits à l'information et d'accès aux données. Par exemple, la gestion des droits détermine si vous pouvez accéder à un dossier ou envoyer un e-mail.

II. Politique de sécurité :

1. Généralité :

Le principal objectif d'un système d'information est de stocker et faciliter l'échange de données. Assurer la sécurité d'un tel système implique de minimiser les risques de compromission des données ou d'interruption des échanges. Dans le cas où le système informatique contrôle des équipements industriels ou le trafic aérien, les conséquences d'une faille de sécurité pourraient être catastrophiques. Par conséquent, la sécurisation d'un réseau implique la prise en compte de tous les risques possibles, y compris les attaques malveillantes, les accidents, les erreurs de logiciel ou de matériel, ainsi que les erreurs humaines, afin de les minimiser autant que possible.

2. Vulnérabilité :

Dans un contexte où les informations circulent librement et où de nombreuses ressources sont hautement disponibles, les responsables doivent être conscients de toutes les menaces potentielles qui peuvent compromettre la sécurité de leur réseau, étant donné la vulnérabilité de ce dernier.

Une vulnérabilité dans un système d'information (SI) désigne toute faille permettant à un attaquant d'altérer le fonctionnement normal du SI, ainsi que la confidentialité et l'intégrité des données qu'il contient.

Au fil des années, la sécurité des SI est devenue un besoin crucial, car leur complexité croissante les rend plus vulnérables aux menaces. Toutefois, les organisations sont souvent mal protégées contre les attaques de réseau. Les raisons de cette vulnérabilité des systèmes sont multiples : la sécurité est souvent considérée comme coûteuse, et les entreprises ou les écoles n'ont souvent pas de budget alloué à ce domaine. De plus, la sécurité ne peut jamais être fiable à 100 % en raison de la présence de bugs dans les applications, que les attaquants peuvent exploiter. Les organisations accordent également une faible priorité à la sécurité, voire aucune.

Enfin, même la cryptographie, qui est censée offrir une protection supplémentaire, peut être vulnérable, car les mots de passe peuvent être cassés.

Solution pour la sécurité :

III. Serveur RADIUS :

1. Définition :

Le **service RADIUS** (Remote Authentication Dial-In User Service) est un protocole de sécurité informatique utilisé pour l'authentification, l'autorisation et la comptabilité des utilisateurs qui accèdent à un réseau informatique à distance. Il permet de centraliser l'authentification des utilisateurs, ce qui signifie que les utilisateurs doivent se connecter avec un nom d'utilisateur et un mot de passe valides pour accéder au réseau.

Le **protocole RADIUS** utilise un serveur central pour authentifier les utilisateurs qui tentent d'accéder au réseau. Lorsqu'un utilisateur essaie de se connecter, le serveur RADIUS vérifie les informations d'identification de l'utilisateur dans une base de données centralisée. Si les informations d'identification sont valides, l'utilisateur est autorisé à accéder au réseau. Le protocole RADIUS prend également en charge la comptabilisation des utilisateurs, ce qui permet de suivre l'utilisation du réseau par les utilisateurs et de générer des rapports d'utilisation.

Le protocole RADIUS est largement utilisé dans les réseaux d'entreprise et les réseaux sans fil (Wi-Fi) pour garantir un accès sécurisé au réseau et pour contrôler l'utilisation du réseau par les utilisateurs.

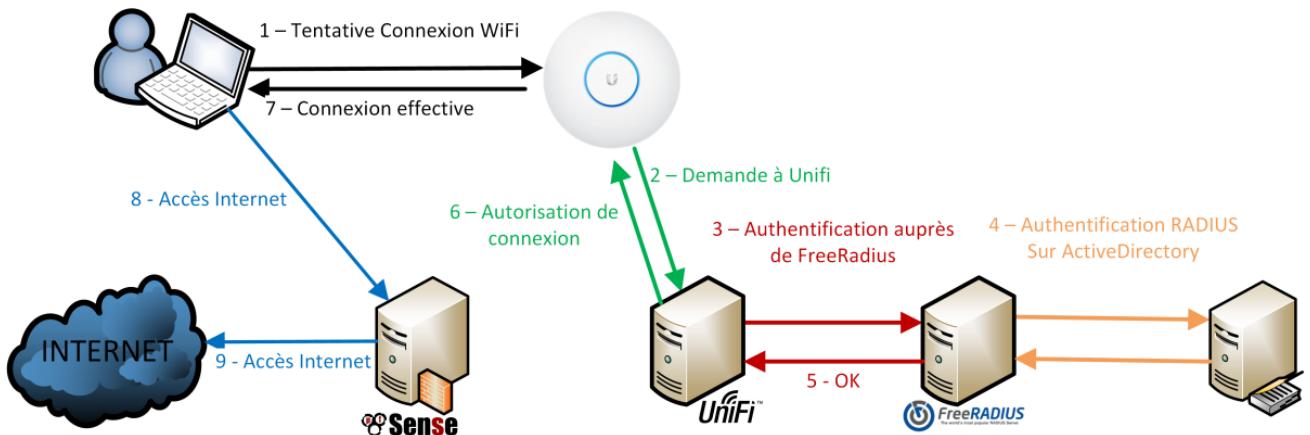


Figure 56 : Schéma RADIUS

2. Scénario d'utilisation du serveur RADIUS :

Un utilisateur tente de se connecter à un réseau en utilisant un appareil, tel qu'un ordinateur portable ou un téléphone mobile. Lorsqu'il tente de se connecter, son appareil envoie une demande de connexion au point d'accès, également appelé NAS (Network Access Server), qui est généralement un routeur ou un commutateur.

Le point d'accès NAS transmet alors la demande d'authentification à un serveur Radius, qui est responsable de la gestion des identités et des autorisations pour le réseau. Le serveur Radius demande ensuite à l'utilisateur de fournir des informations d'identification, telles qu'un nom d'utilisateur et un mot de passe.

Une fois que l'utilisateur a fourni les informations d'identification, le serveur Radius vérifie si les informations sont correctes en les comparant avec les informations d'identification stockées dans une base de données d'utilisateurs autorisés. Si les informations d'identification sont correctes, le serveur Radius envoie une réponse positive (appelée « Access-Accept ») au point d'accès NAS, qui permet à l'utilisateur de se connecter au réseau.

Si les informations d'identification ne sont pas correctes, le serveur Radius envoie une réponse négative (appelée « Access-Reject ») au point d'accès NAS, qui empêche l'utilisateur de se connecter au réseau. Cela garantit que seuls les utilisateurs autorisés peuvent accéder au réseau et que le réseau est sécurisé.

IV.La phase de l'installation :

1. Installation de Windows Server :

Le Windows server est une plateforme de cloud et de centre de données professionnelles capable d'évoluer pour exécuter les plus grandes charges de travail, tout en permettant des options de récupération robustes afin de se protéger contre les pannes de service. Il permet d'accélérer l'efficacité en simplifiant notre infrastructure sous-jacente et en nous permettant de réduire les coûts en exploitant le matériel standard.

Voici les étapes de l'installation :

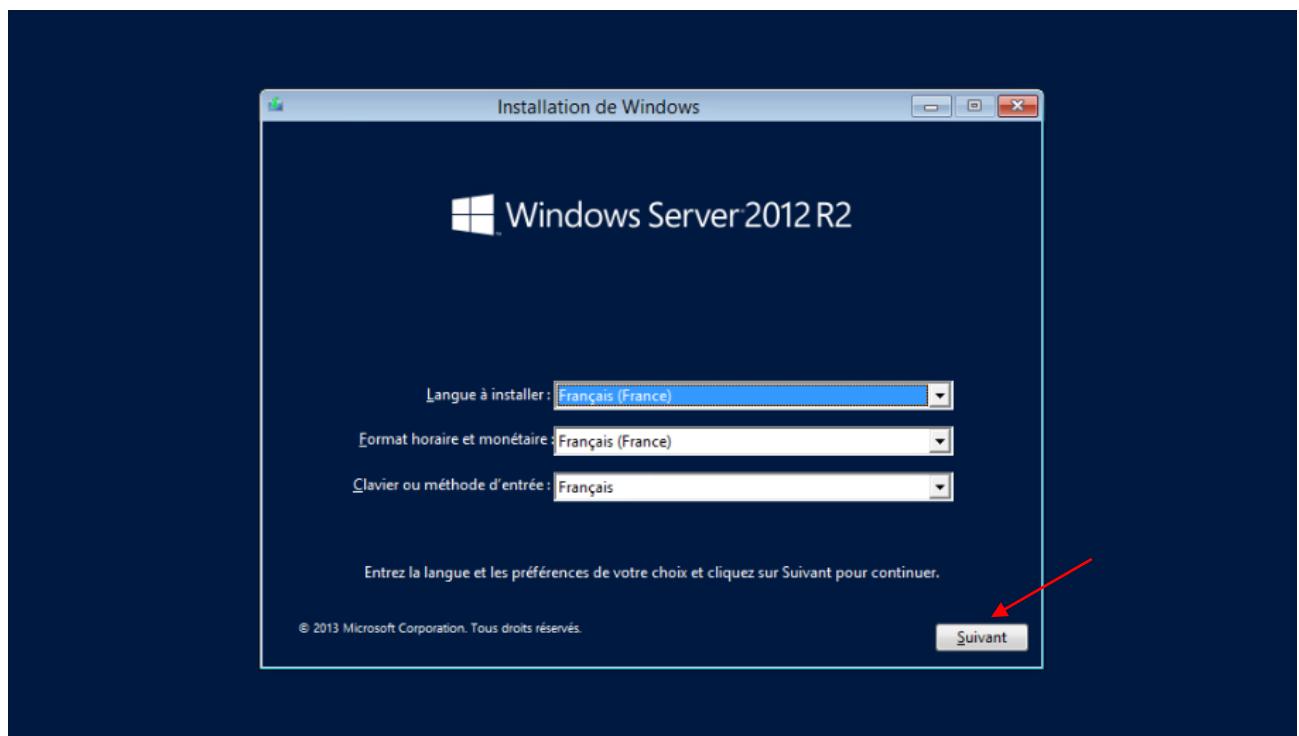


Figure 57 : Installation de Windows Server 2012 R2

- On clique sur « Suivant »

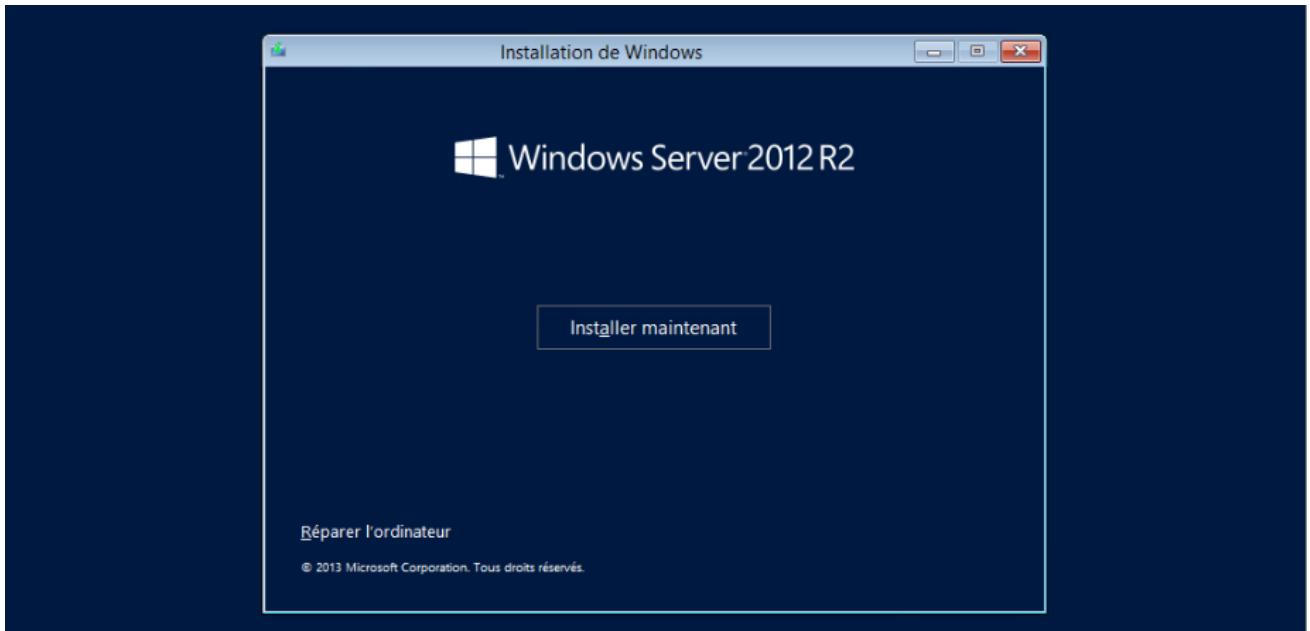


Figure 58 : le début de l'installation de Windows Server

- Lors de l'installation du programme, vous serez invité à choisir un système d'exploitation.
- Veuillez choisir « Windows Server 2012 Standard avec une Interface graphique utilisateur » et cliquer sur le bouton "suivant" :

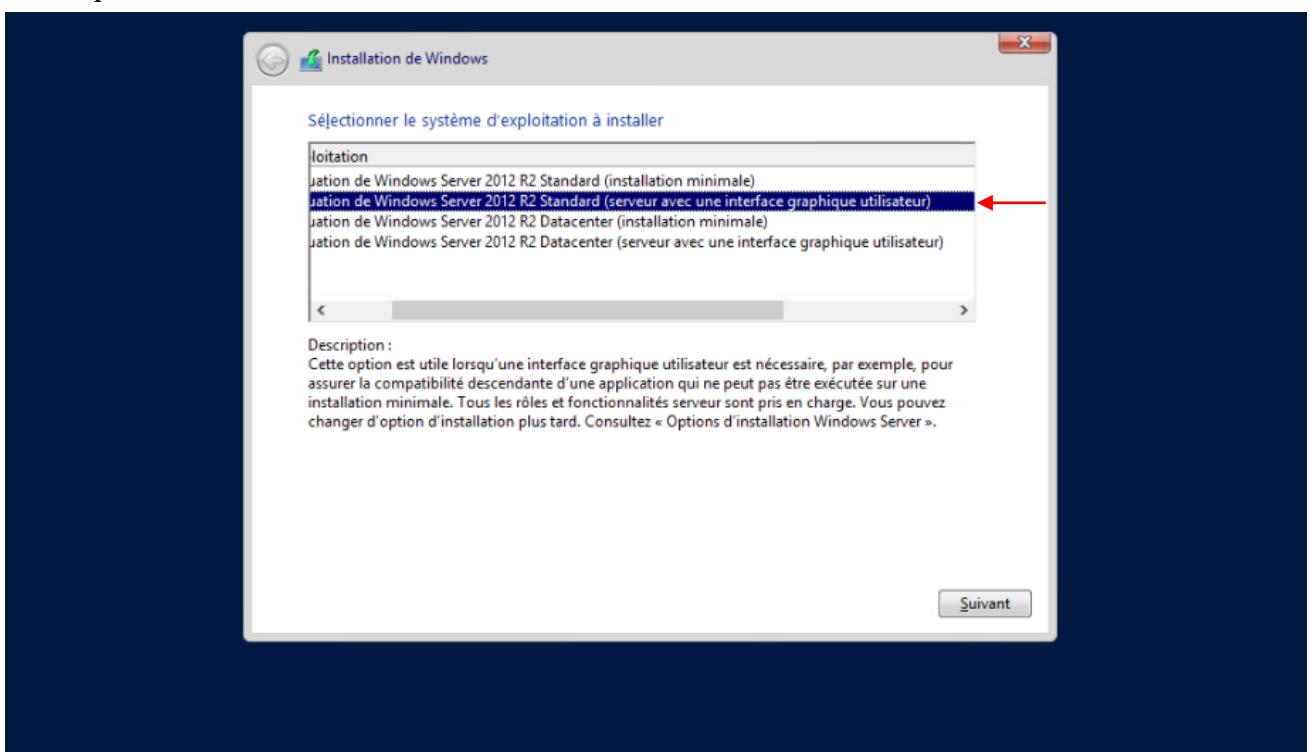


Figure 59 : La sélection de système d'exploitation à installer

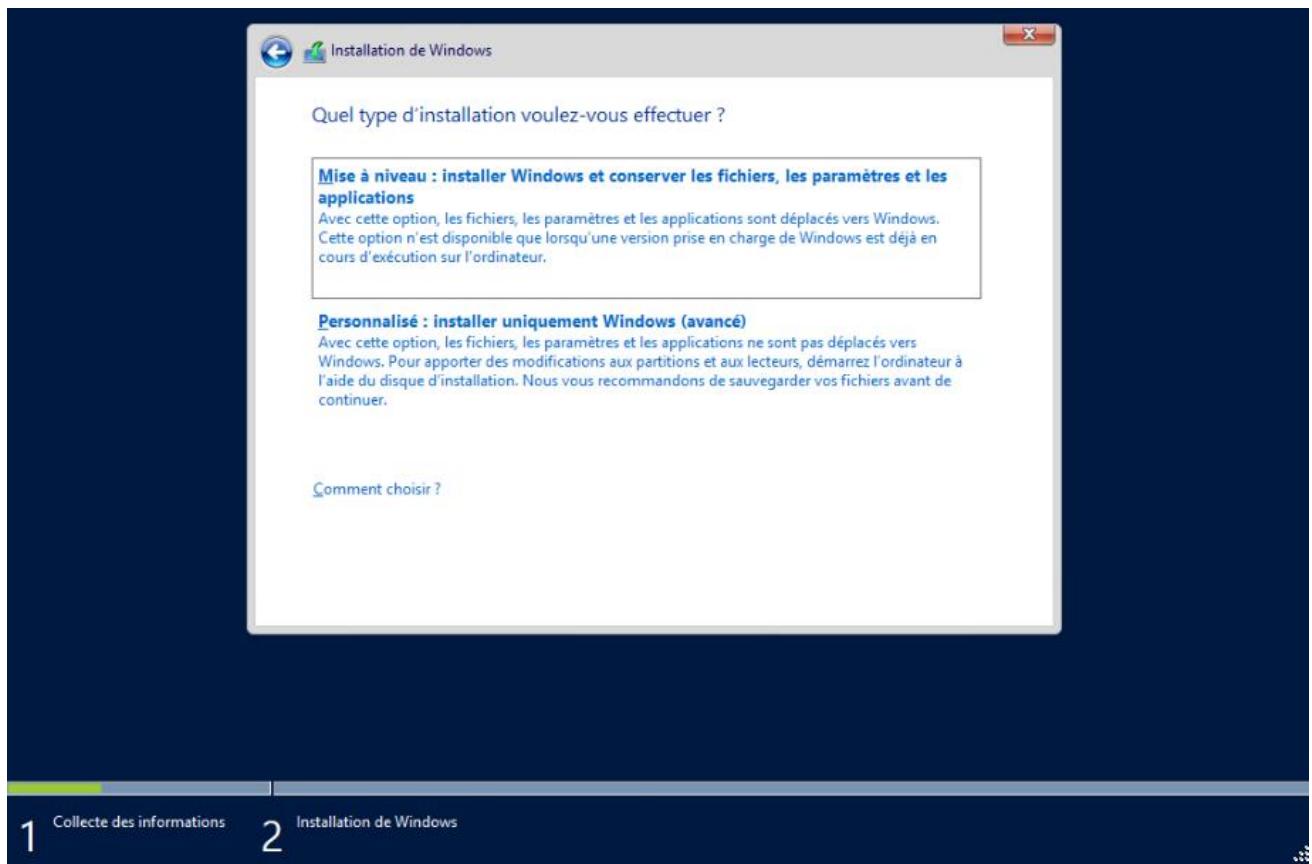


Figure 60 : Le choix de type d'installation de Windows Server

- Lors du processus d'installation du programme, vous serez invité à choisir le type d'installation. Pour une nouvelle installation, sélectionnez « Installer uniquement ». Une fois l'installation terminée, vous devrez définir le mot de passe du compte Administrateur :

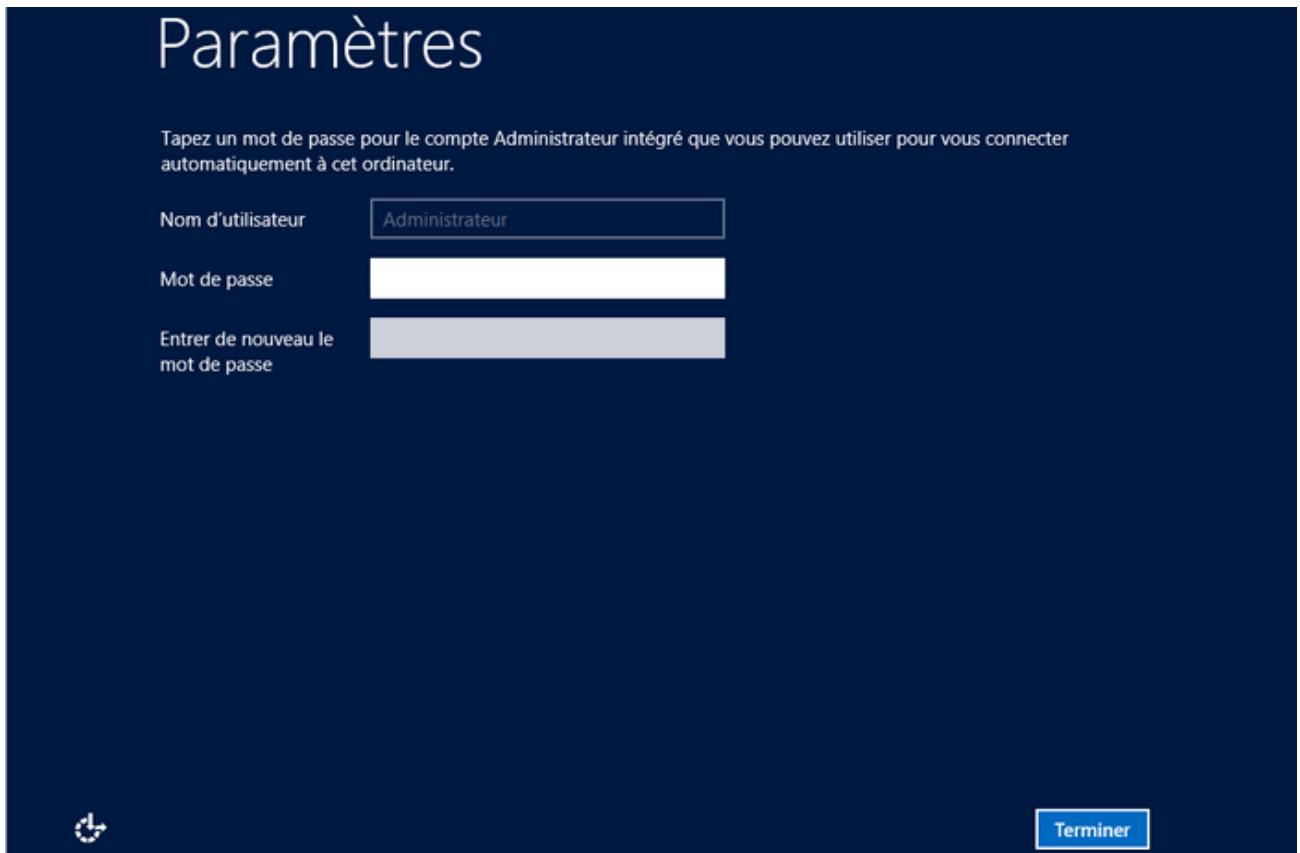


Figure 61 : La création d'un compte administrateur

- Ensuite, on va configurer les paramètres réseaux de notre serveur :
- Et donner une adresse IP statique au serveur (192.168.20.253)

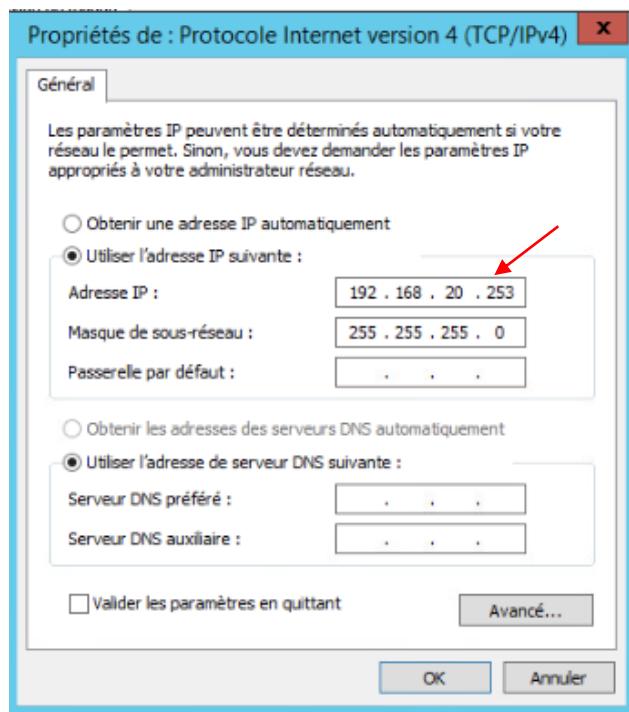


Figure 62 : configuration des paramètres réseaux de serveur

a) L'installation et la configuration de l'Active Directory :

Pour installer Active Directory sur votre serveur, suivez les étapes ci-dessous :

- À partir de la barre des tâches, ouvrez le Gestionnaire de serveur.
- Dans le tableau de bord du « Gestionnaire de serveur », sélectionnez l'option "Ajouter des rôles et des fonctionnalités" pour démarrer l'assistant rôles et fonctionnalités. Celui-ci vous permettra de configurer votre instance de Windows Server 2012 en fonction de vos besoins.

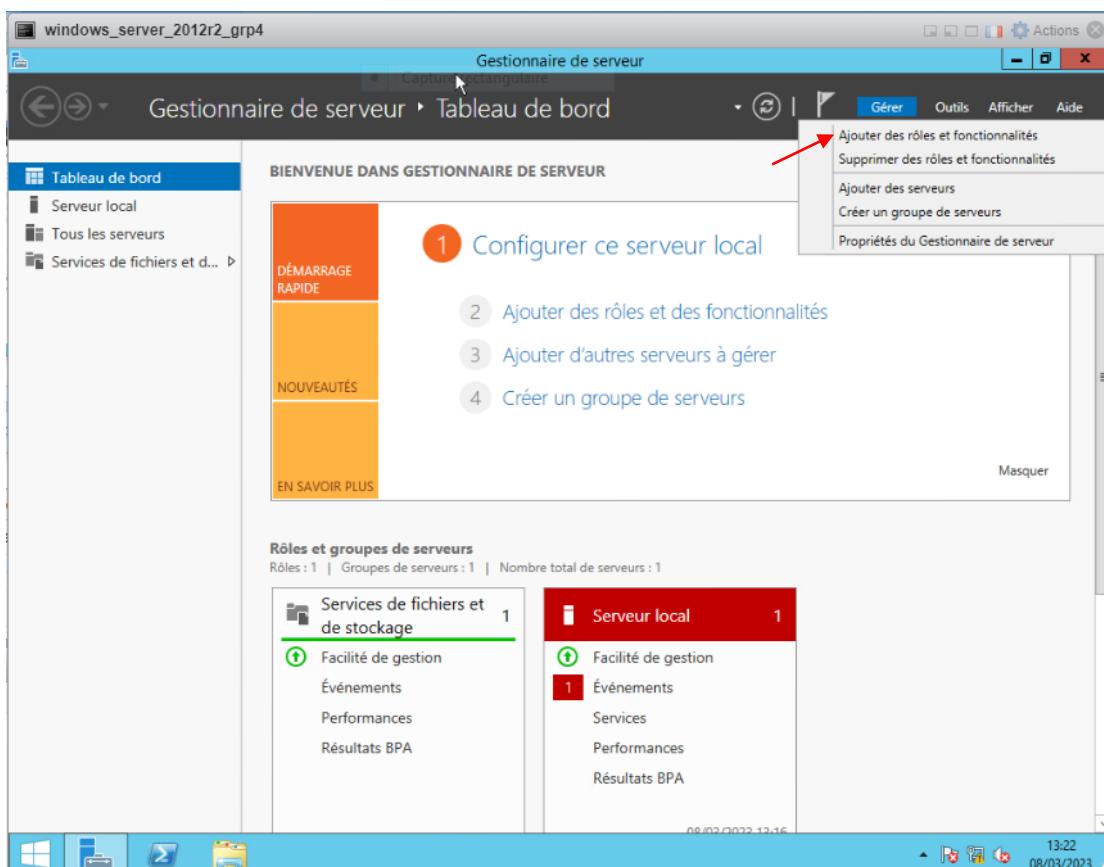


Figure 63 : Gestionnaire de serveur

- Dans la fenêtre « Sélectionner le type d'installation », choisissez l'option « Installation basé sur un rôle sur une fonctionnalité », puis appuyez sur le bouton « Suivant ».

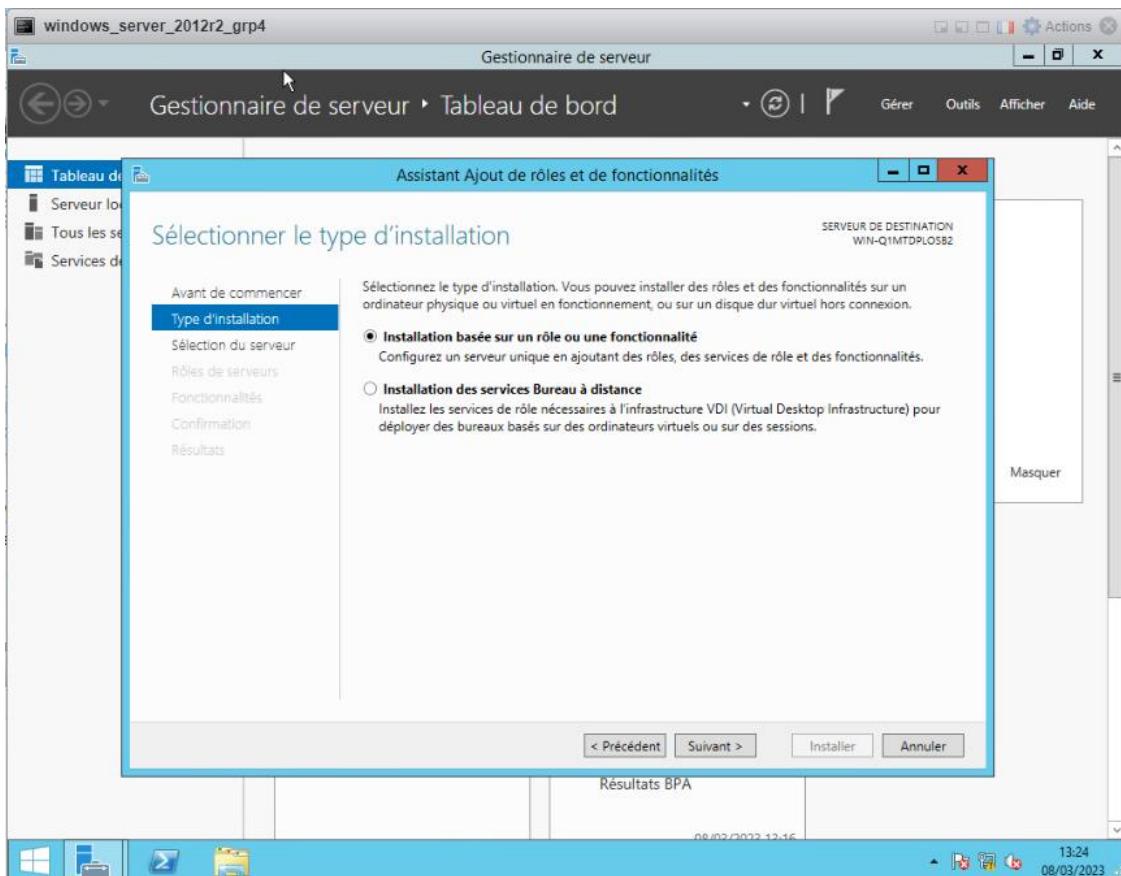


Figure 64 : Installation basée sur un rôle ou une fonctionnalité

- Le serveur actuel est sélectionné par défaut. Cliquez sur le bouton « Suivant ».

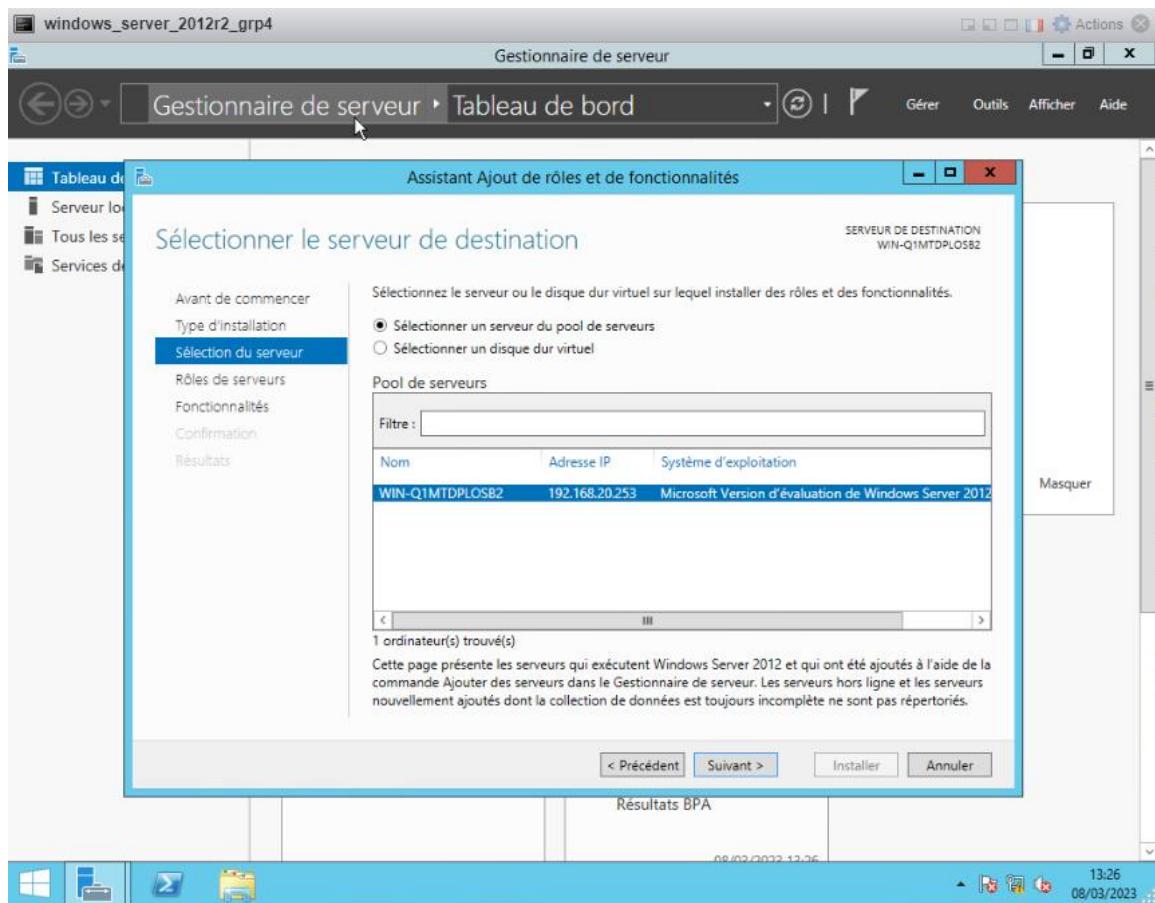


Figure 65 : La sélection du serveur de destination

- Dans la fenêtre « Rôles du serveurs », cochez la case correspondant à « Services de stratégie et d'accès réseau ».

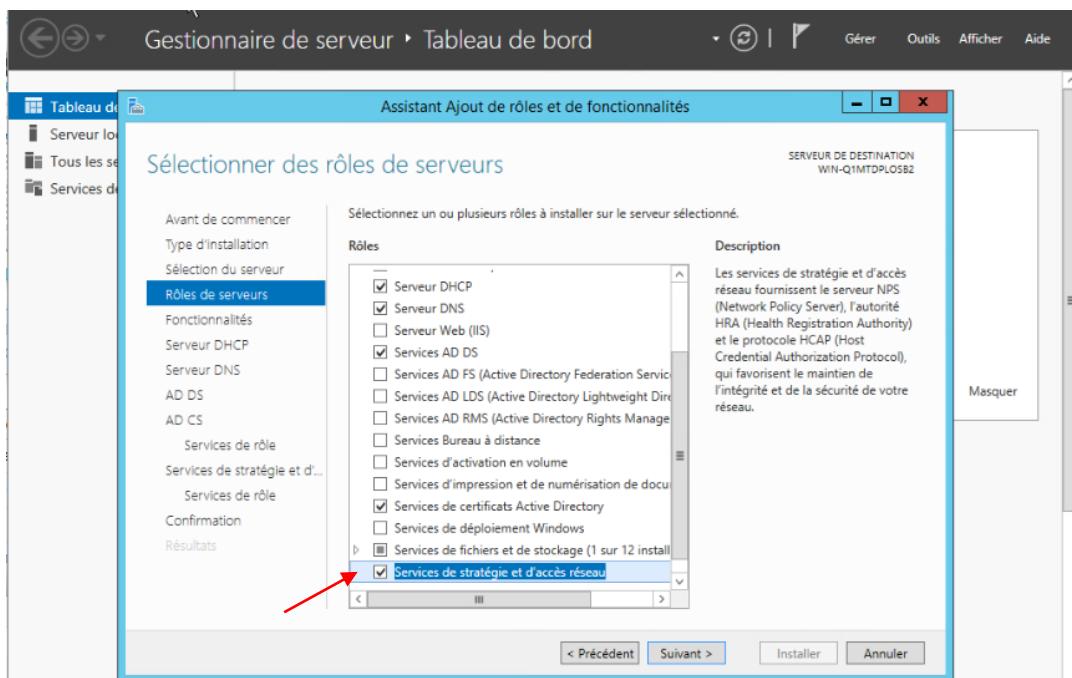


Figure 66 : La sélection des rôles de serveurs

- Une notification s'affichera pour vous informer que l'installation des services de domaine nécessite également l'installation de certains rôles, services ou fonctionnalités supplémentaires. Parmi ces fonctionnalités supplémentaires, on peut citer les services de certificat, les services de fédération, les services d'annuaire légers et la gestion des droits.
- Dans la fenêtre « Sélectionner des fonctionnalités », cochez les cases en regard des fonctionnalités que vous souhaitez installer pendant le processus d'installation des Services de domaine Active Directory (AD DS), puis appuyez sur le bouton "Suivant".

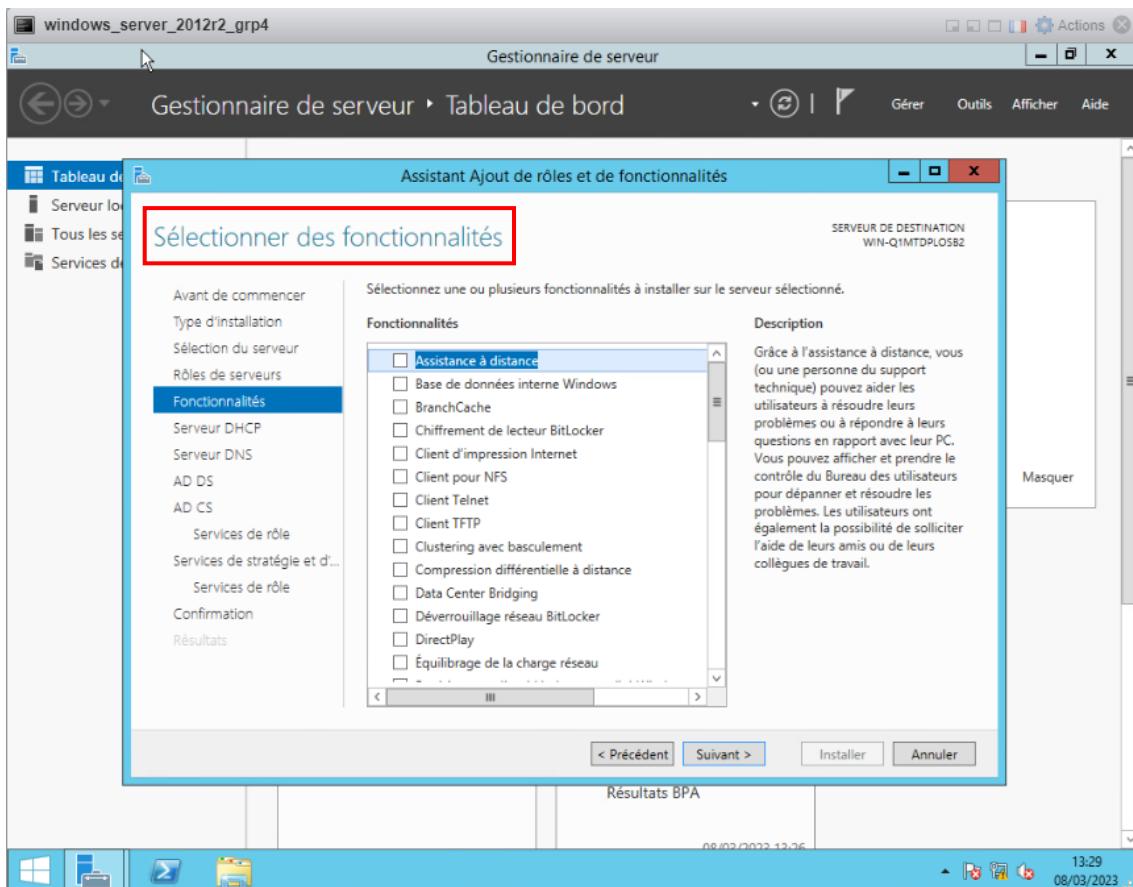


Figure 67 : La sélection des fonctionnalités

- Vérifiez les informations présentées dans l'onglet AD DS, puis appuyez sur « Suivant ».
- Examinez les informations affichées dans l'écran « Confirmer les sélections d'installation », puis cliquez sur le bouton « Installer » :

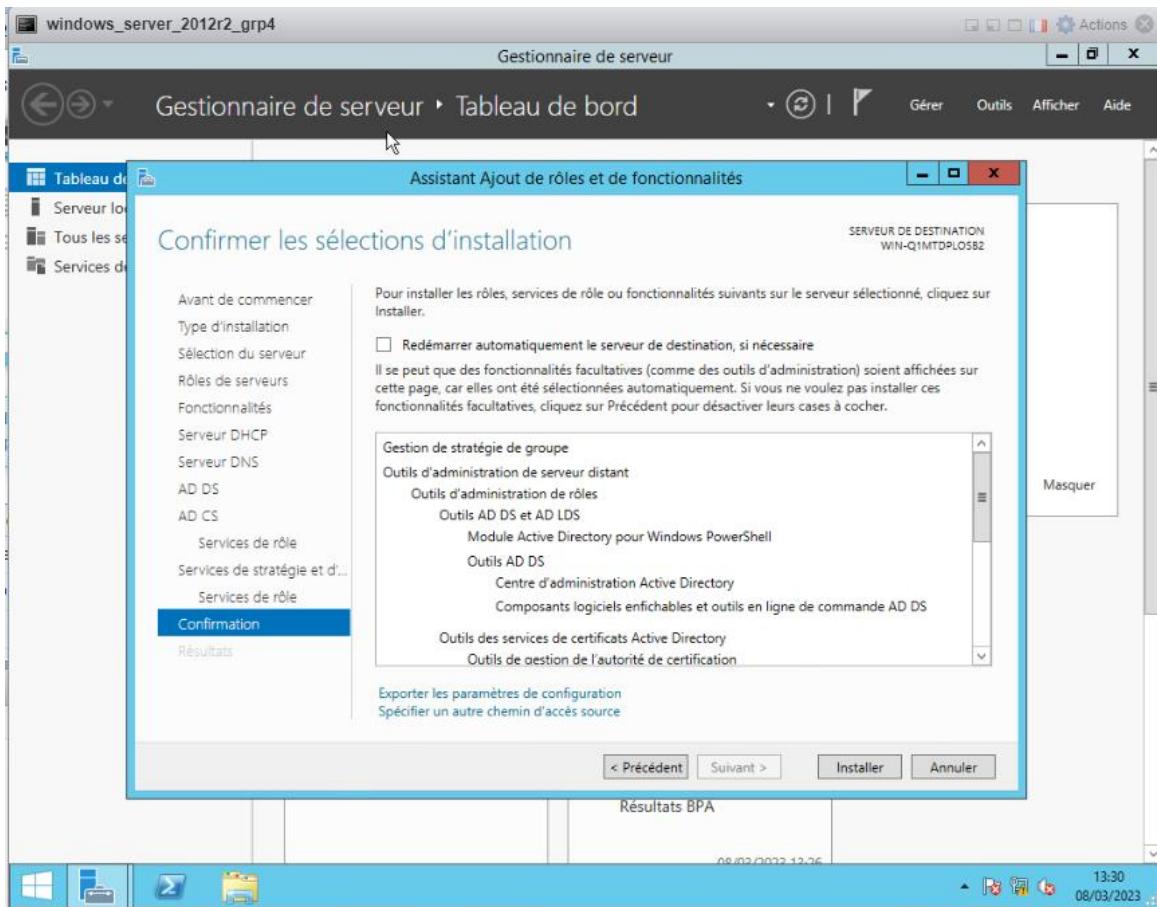


Figure 68 : La confirmation des sélections d'installation

NB : Le redémarrage du serveur prendra plus de temps que d'habitude, en raison de la mise en place des nouveaux services qui ont été installés.

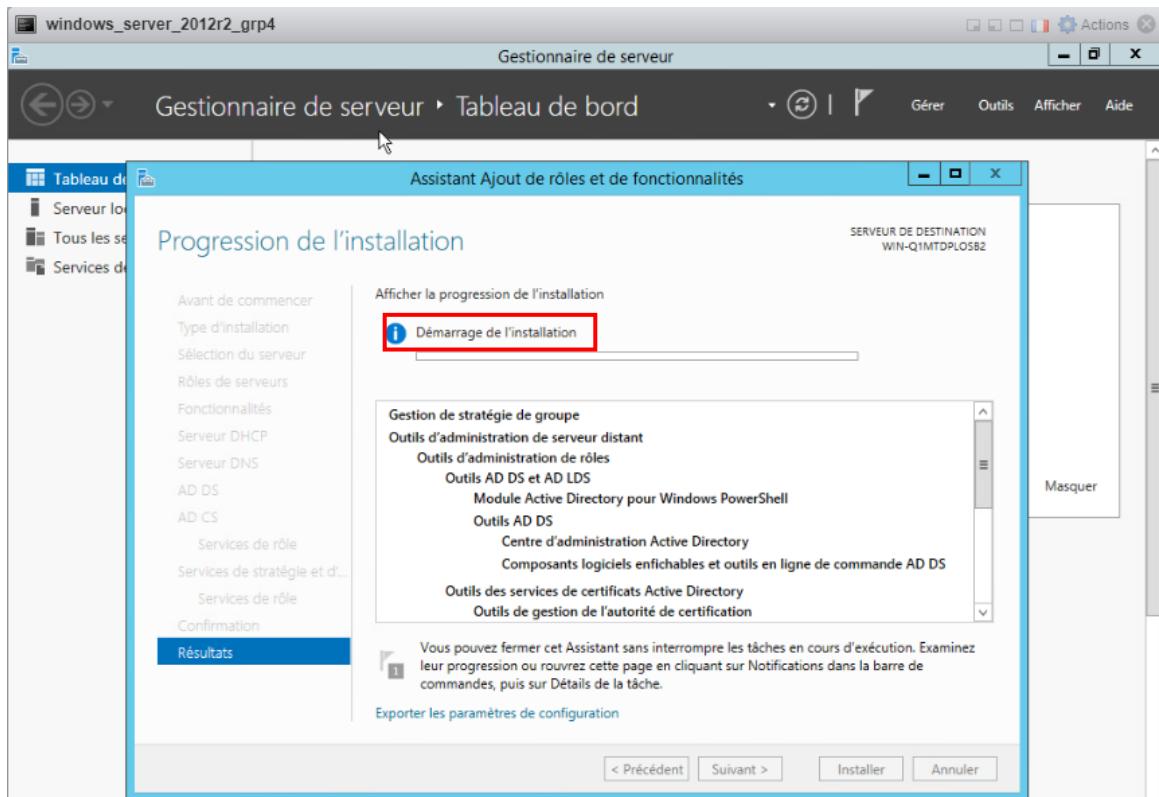


Figure 69 : Le redémarrage du serveur

2. Configuration de l'Active Directory pour un nouveau domaine :

Pour accéder à la notification de configuration post-déploiement, il faut cliquer sur l'icône de notification jaune dans la barre de navigation supérieure de la fenêtre du gestionnaire de serveur. En cliquant sur ce bouton, le volet « Notifications » s'affiche, et la notification de configuration post-déploiement apparaît. Pour promouvoir ce serveur en contrôleur de domaine, il suffit de cliquer sur le lien correspondant qui s'affiche dans la notification.

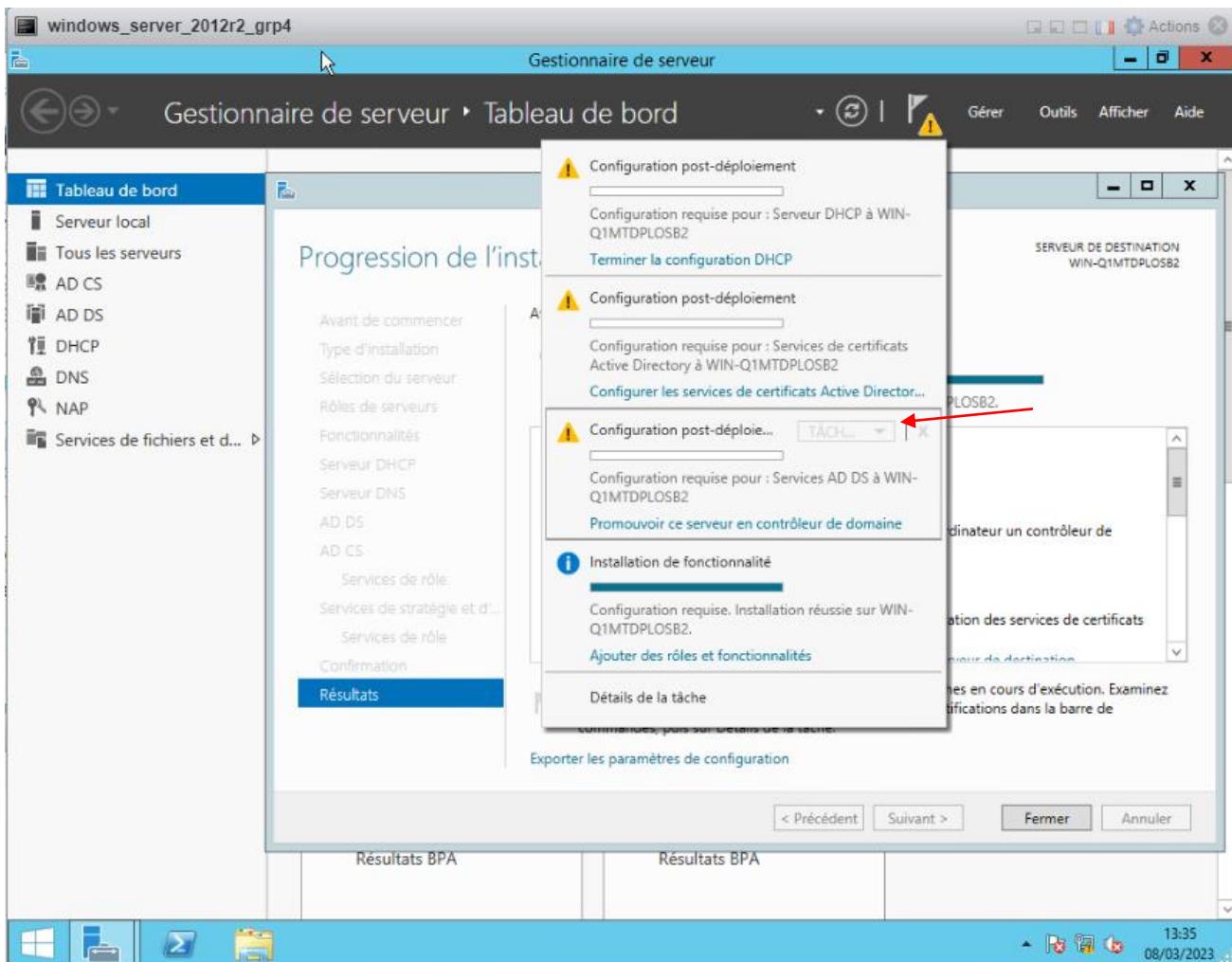


Figure 70 : La configuration de déploiement

- Dans la fenêtre « Configuration de déploiement », sélectionnez l'option « Ajouter une nouvelle forêt ». Entrez votre nom de domaine racine dans le champ « Nom du domaine racine », pour notre cas on a choisi comme nom : « **grp4.pfe** »
- Ensuite, cliquez sur le bouton « Suivant ».

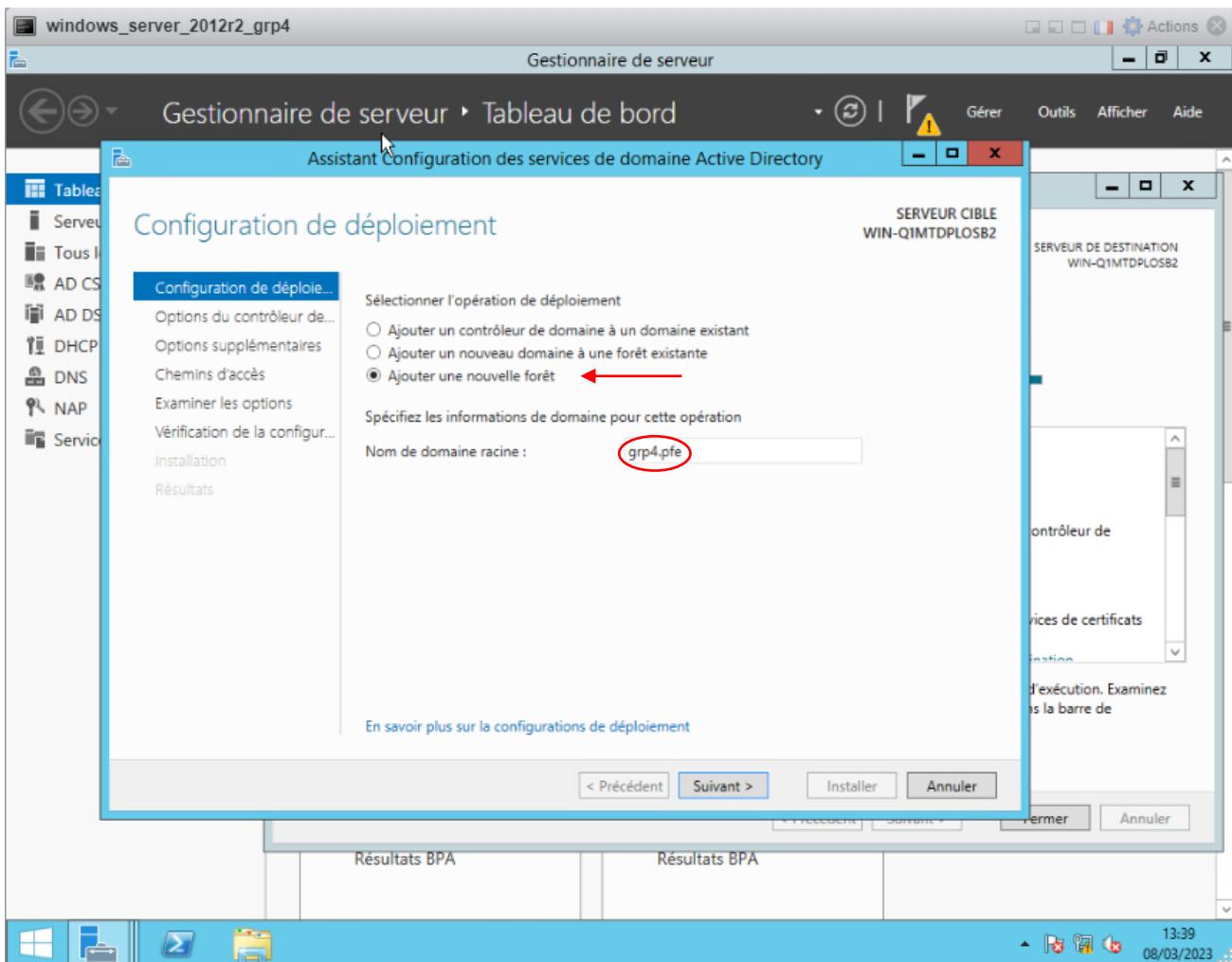


Figure 71 : L'ajout d'une nouvelle forêt

- Entrez un mot de passe pour le mode de restauration des services d'annuaire (DSRM) dans le champ « Mot de passe ».
- Dans l'onglet "Options DNS", prenez connaissance de l'avertissement affiché, puis cliquez sur « Suivant ».
- Confirmez ou entrez un nom NetBIOS, puis appuyez sur « Suivant ».
- Précisez les chemins d'accès aux dossiers Base de données, Fichiers journaux et SYSVOL, et cliquez sur « Suivant ».
- Examinez les options de configuration proposées, puis appuyez sur « Suivant ».
- Le système procède à une vérification des conditions préalables requises pour l'installation. Si toutes les vérifications sont concluantes, appuyez sur « Installer ».

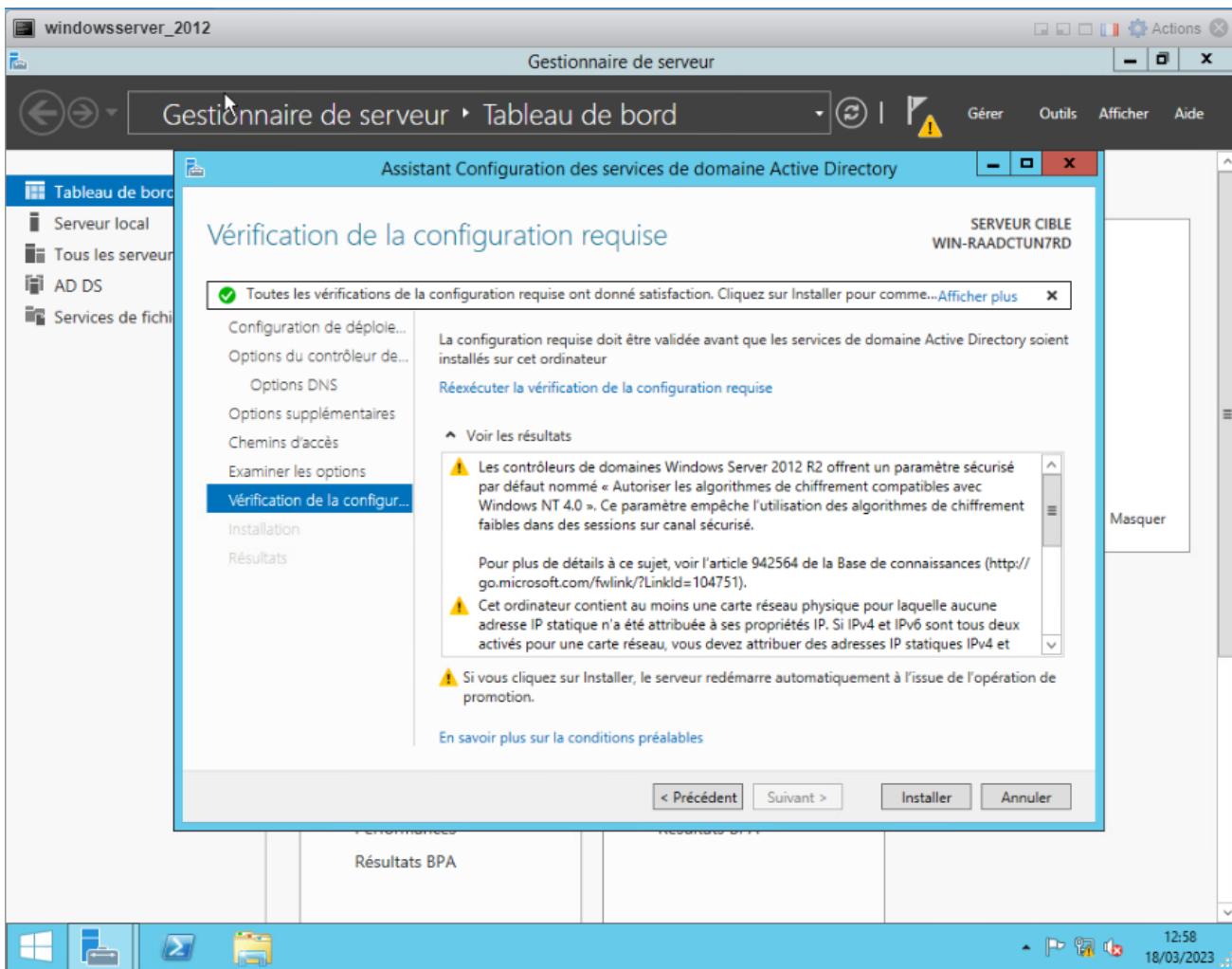


Figure 72 : La vérification de la configuration requise

NB : Une fois que tous les paramètres préliminaires auront été configurés, un redémarrage du serveur sera obligatoire.

La création du groupe et des utilisateurs :

Une fois l'installation d'AD terminée, nous avons créé des utilisateurs et les avons ajoutés à un groupe appelé « PFE ».

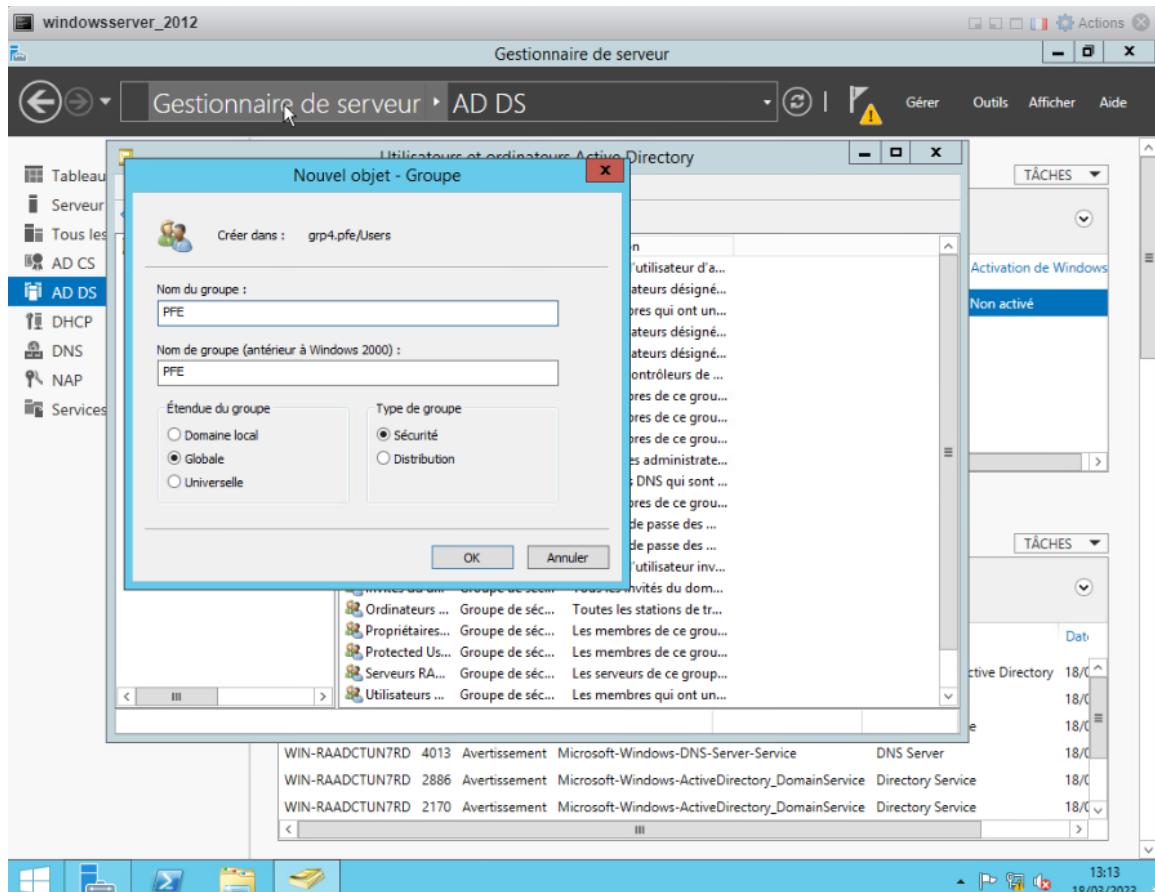


Figure 73 : La création du groupe

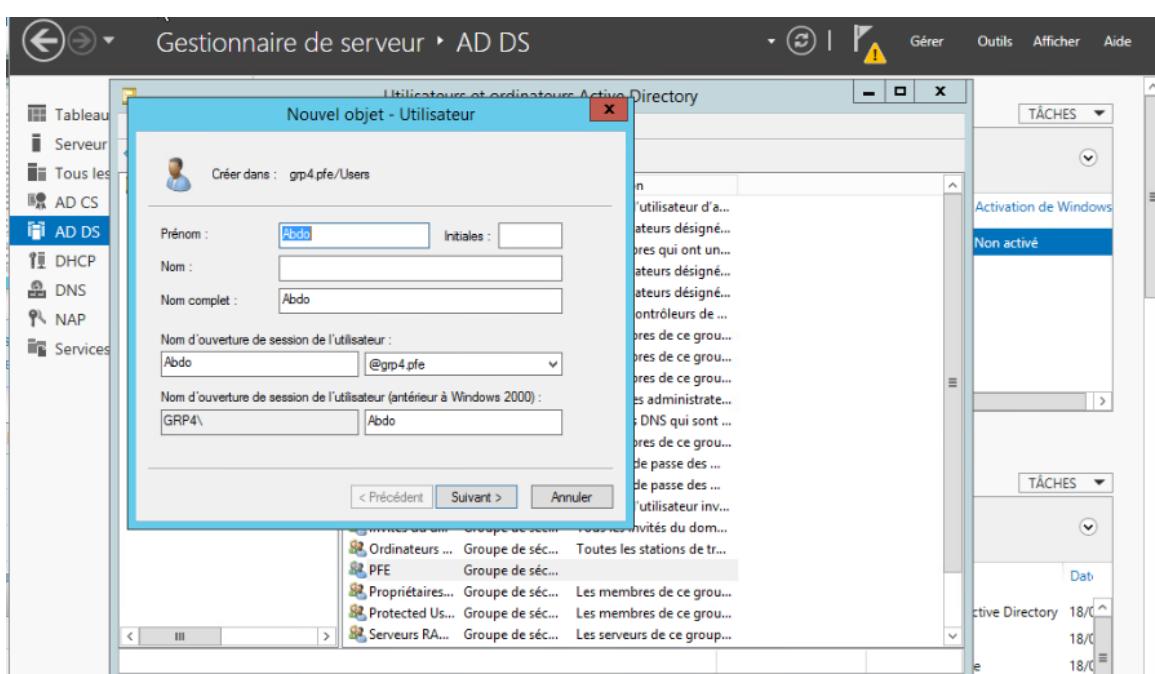


Figure 74 : La création de l'utilisateur

- Saisissez les informations d'utilisateur tel que son nom, prénom et son nom d'ouverture de session de l'utilisateur, puis appuyer sur le bouton « Suivant ».
- Ensuite, saisissez un mot de passe fort et cliquez sur « Suivant ».

Qu'appelle-t-on un mot de passe fort ?

On dit d'un mot de passe qu'il est fort s'il répond à certaines exigences :

- **Son nombre de caractères.** Il doit comporter plus de 8 caractères, 12 dans l'idéal
- **Le type de caractère utilisé.** Il doit contenir plusieurs types de caractères différents : majuscules, minuscules, nombres, ponctuation, caractères spéciaux tels que @, [...]
- **Les informations qu'il pourrait contenir.** Évitez d'y mettre des informations personnelles faciles à deviner, comme le nom d'un animal de compagnie, votre date ou lieu de naissance, etc.

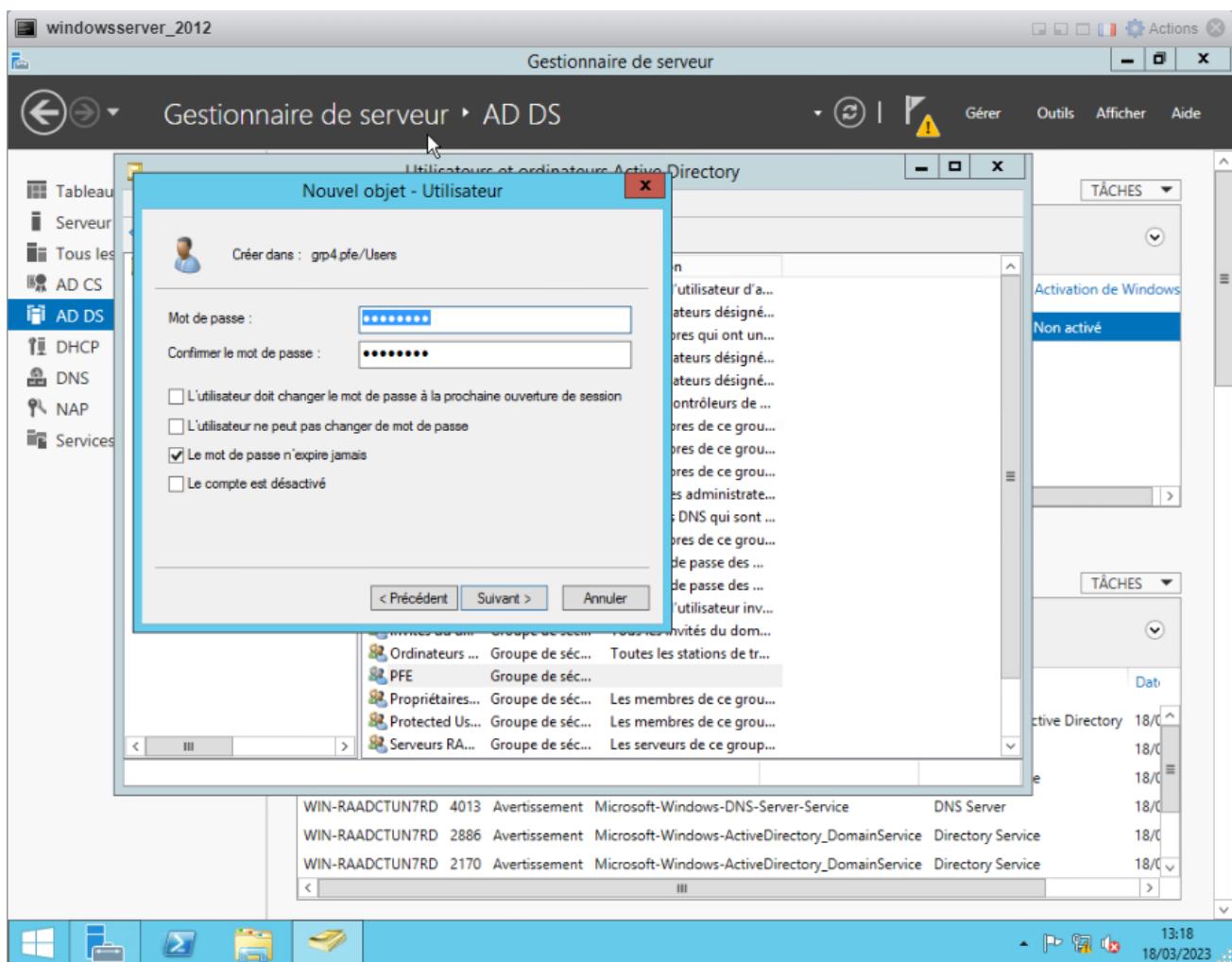


Figure 75 : La saisie du mot de passe

Pour finaliser l'opération, appuyez sur « Termier » :

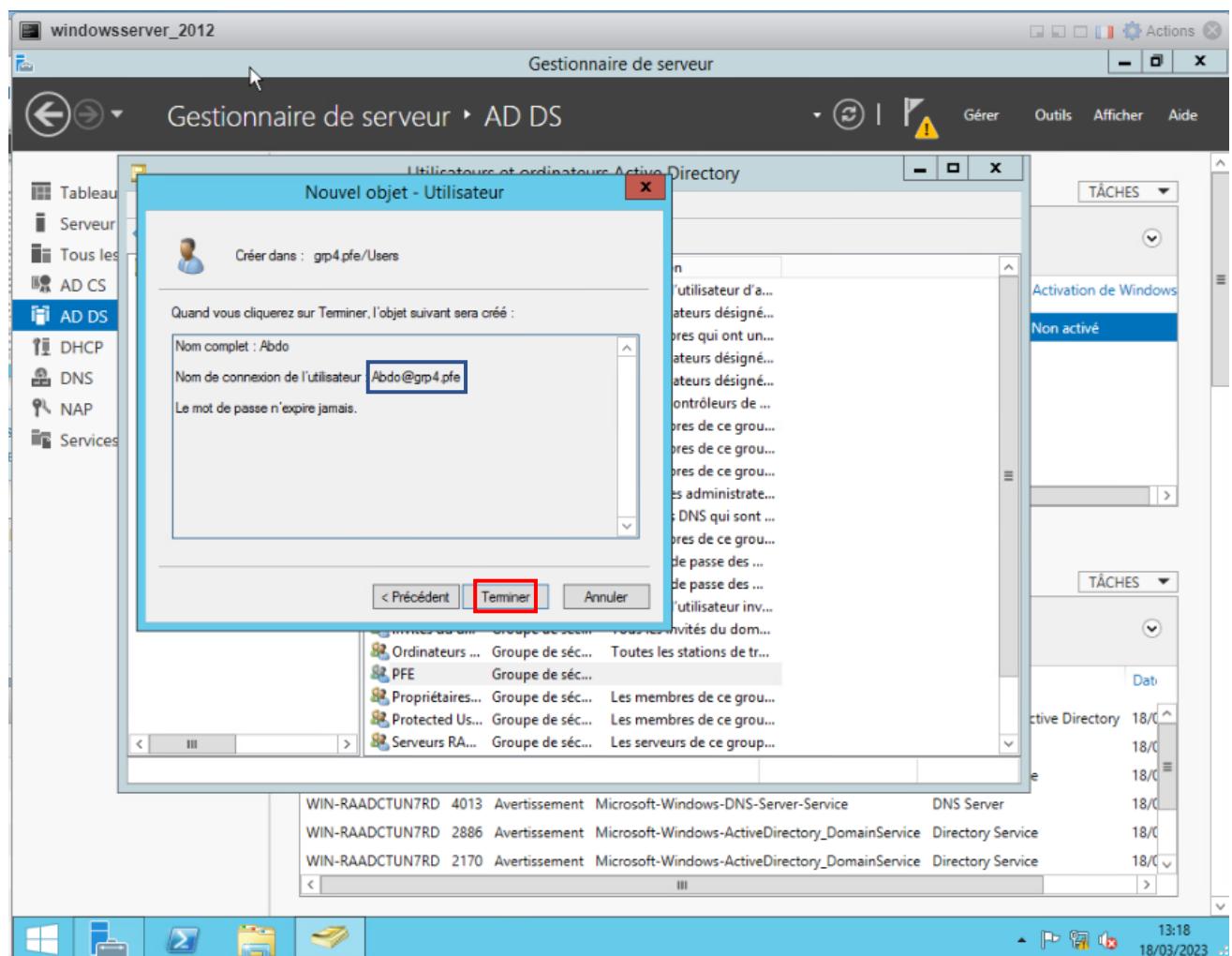


Figure 76 : L'ajout de l'utilisateur au groupe

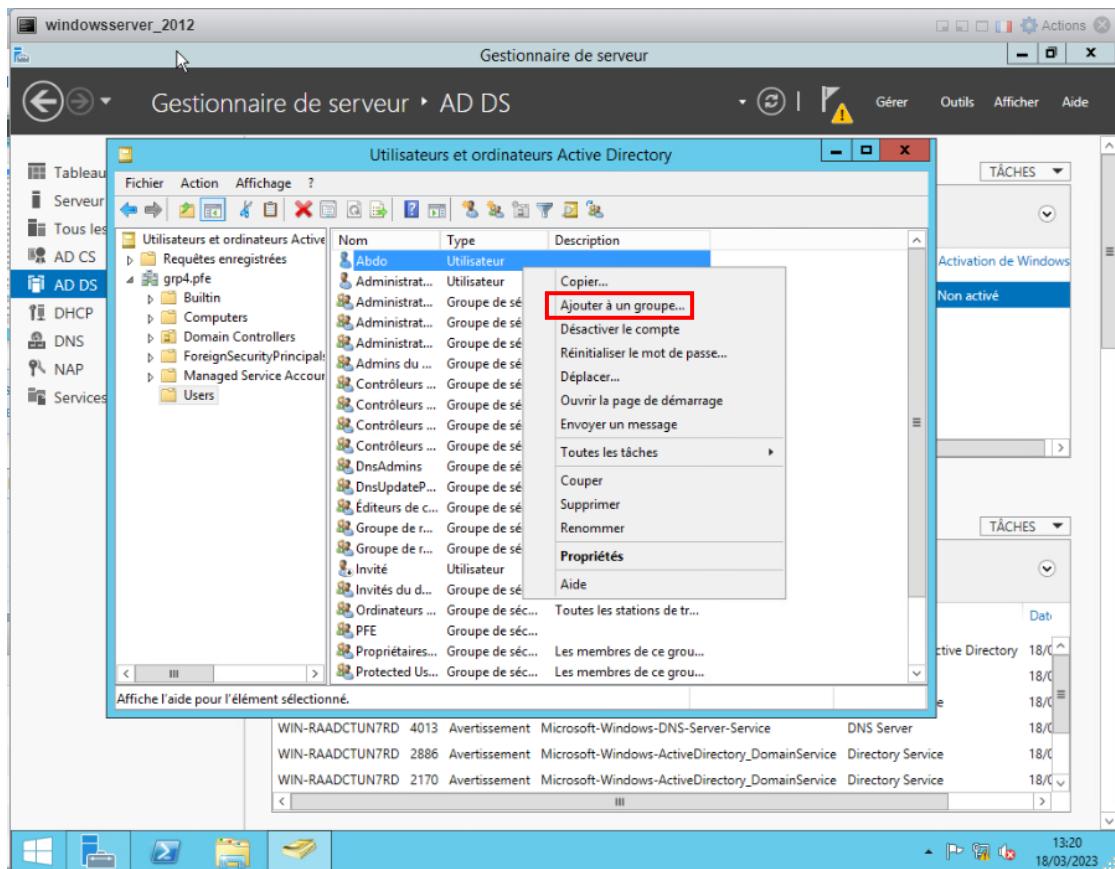


Figure 77 : L'ajout d'un utilisateur à un groupe

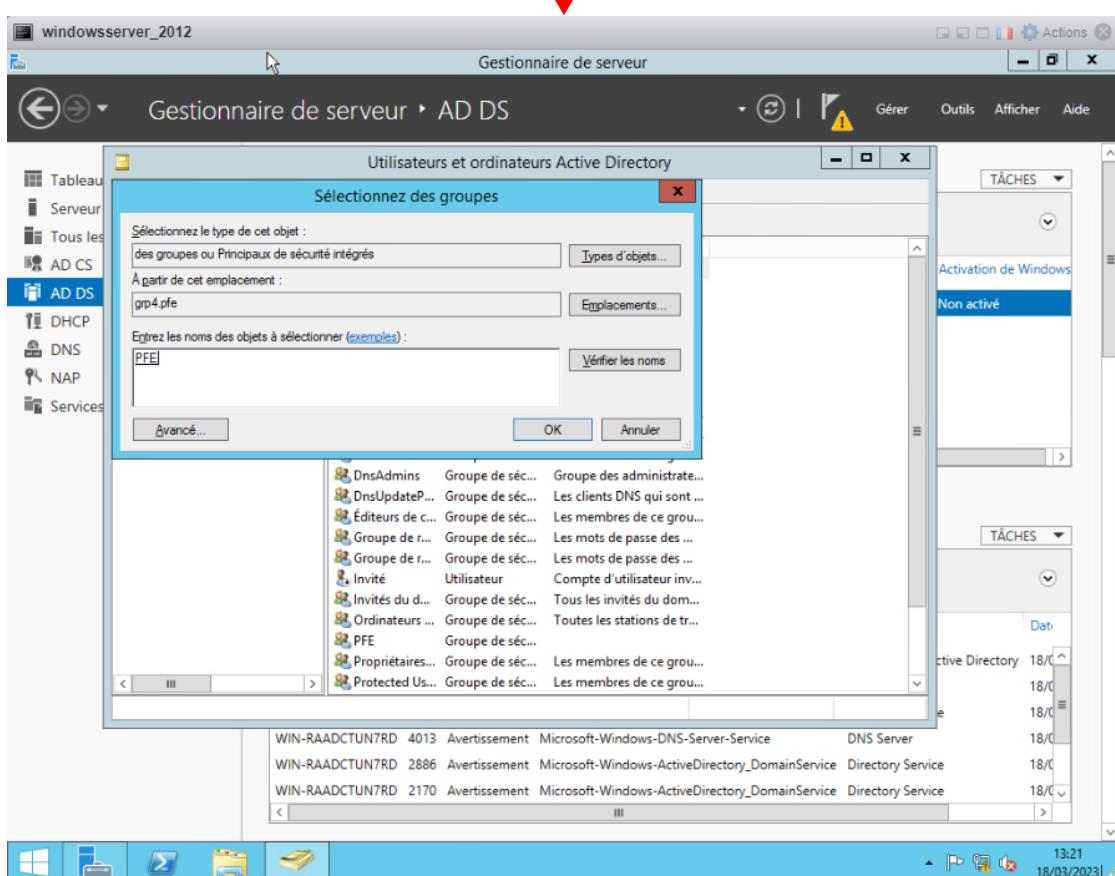


Figure 78 : La sélection de groupe

a) Etendue du groupe :

Domaine Local : Les groupes de domaines locaux rassemblent des comptes et des groupes provenant de différents domaines Windows tels que Windows Server 2003, Windows 2000, Windows NT, Windows Server 2008 et Windows Server 2008 R2. Cependant, les autorisations accordées aux membres de ces groupes ne s'appliquent qu'au sein d'un seul domaine. Les groupes avec une étendue de domaine local sont donc utiles pour définir et gérer l'accès aux ressources dans un domaine spécifique.

Pour simplifier la gestion des autorisations, il est recommandé de créer un groupe avec une étendue de domaine local et de lui attribuer l'autorisation d'accès à l'imprimante. Ensuite, il suffit de placer les cinq comptes d'utilisateurs dans un groupe avec une étendue globale et d'ajouter ce groupe au groupe avec une étendue de domaine local. Ainsi, en cas d'ajout d'une nouvelle imprimante, il suffit d'octroyer au groupe une autorisation d'étendue de domaine local pour accéder à cette nouvelle ressource.

L'accès à la nouvelle imprimante est automatiquement accordé à tous les membres du groupe ayant une étendue globale.

Globale : Les membres des groupes à étendue globale sont limités aux groupes et comptes du domaine où le groupe est créé. Cependant, ces membres peuvent recevoir des autorisations dans n'importe quel domaine de la forêt. Les groupes à étendue globale sont particulièrement utiles pour gérer des objets d'annuaire tels que les comptes d'utilisateurs et d'ordinateurs qui nécessitent une maintenance quotidienne. De plus, les groupes à étendue globale ne sont pas répliqués en dehors de leur propre domaine, ce qui permet de modifier fréquemment les comptes dans le groupe sans provoquer de trafic de réPLICATION vers le catalogue global.

Universelle : Les membres des groupes universels peuvent inclure des groupes et des comptes provenant de tous les domaines de la forêt ou de l'arborescence de domaine. Les membres de ces groupes peuvent recevoir des autorisations dans n'importe quel domaine de la forêt ou de l'arborescence de domaine. Les groupes à étendue universelle sont particulièrement utiles pour regrouper des groupes qui s'étendent sur plusieurs domaines. Pour ce faire, il suffit d'ajouter des comptes aux groupes à étendue globale et de les insérer dans des groupes à étendue universelle. Lorsque cette stratégie est utilisée, les changements d'appartenance dans les groupes à étendue globale n'affectent pas les groupes à étendue universelle.

3. L'installation et la configuration du DNS :

Maintenant que notre contrôleur de domaine est opérationnel, nous devons effectuer une étape supplémentaire sur notre serveur DNS. Lors de l'installation du rôle AD DS, un avertissement nous a informé que si le serveur DNS était accessible, une configuration automatique serait effectuée, sinon nous devrions la configurer manuellement. Dans ce cas, le DNS a été partiellement configuré et une zone de recherche inversée doit être créée.

Pour ce faire, il faut ouvrir le « Gestionnaire DNS » et naviguer dans l'arborescence du serveur DNS.

Ensuite, un clic droit sur le dossier « Zones de recherche inversée » et sélectionner « Nouvelle zone ». Étant donné que ce serveur DNS est le principal, l'option « Zone principale » doit être cochée et l'option « Enregistrer la zone dans un AD » doit également être sélectionnée pour que l'AD sache vers quel serveur DNS effectuer ses demandes de résolutions de noms.

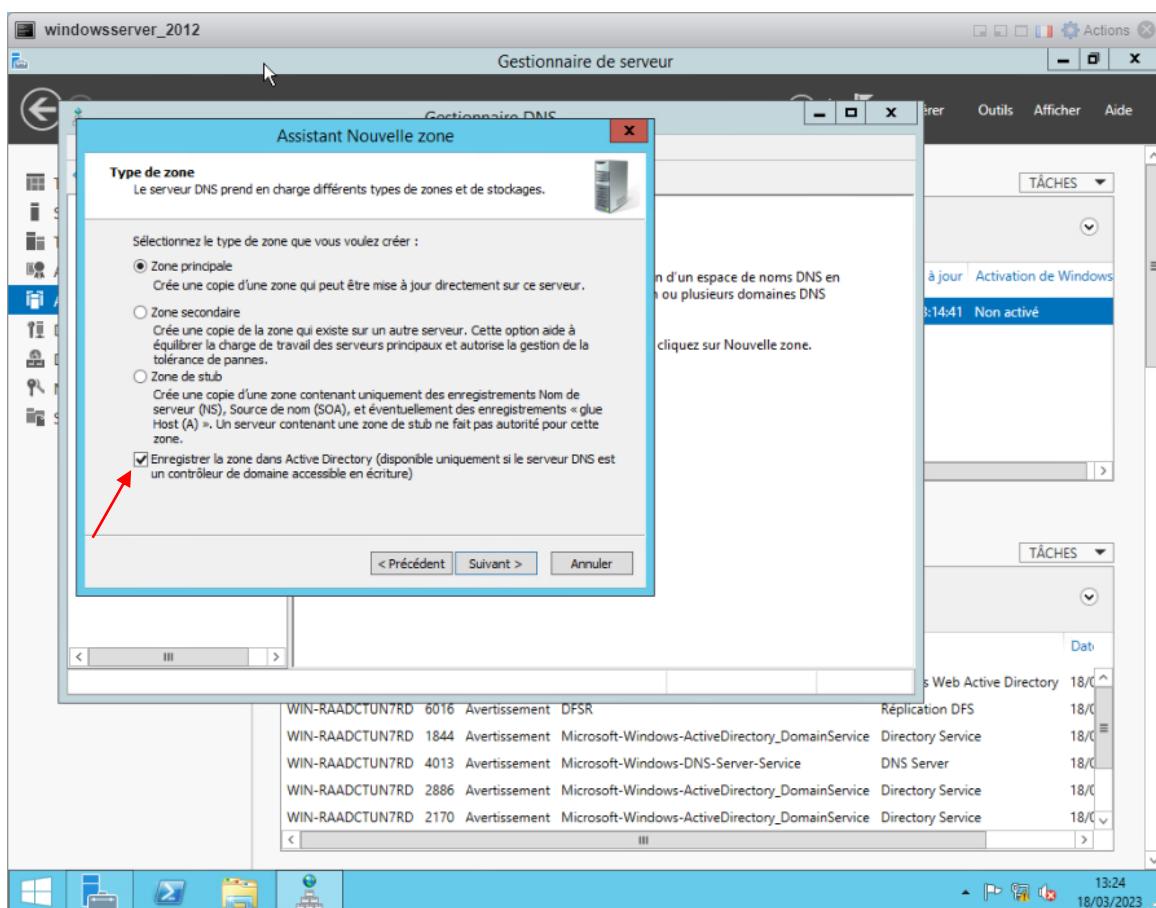


Figure 79 : L'ajout d'une nouvelle zone

- Dans la fenêtre « Gestionnaire de serveur DHCP » :
- Pour créer une nouvelle étendue, accédez à la console de gestion, faites un clic droit sur IPv4, faites défiler jusqu'à l'option « Nouvelle étendue... » puis cliquez dessus.

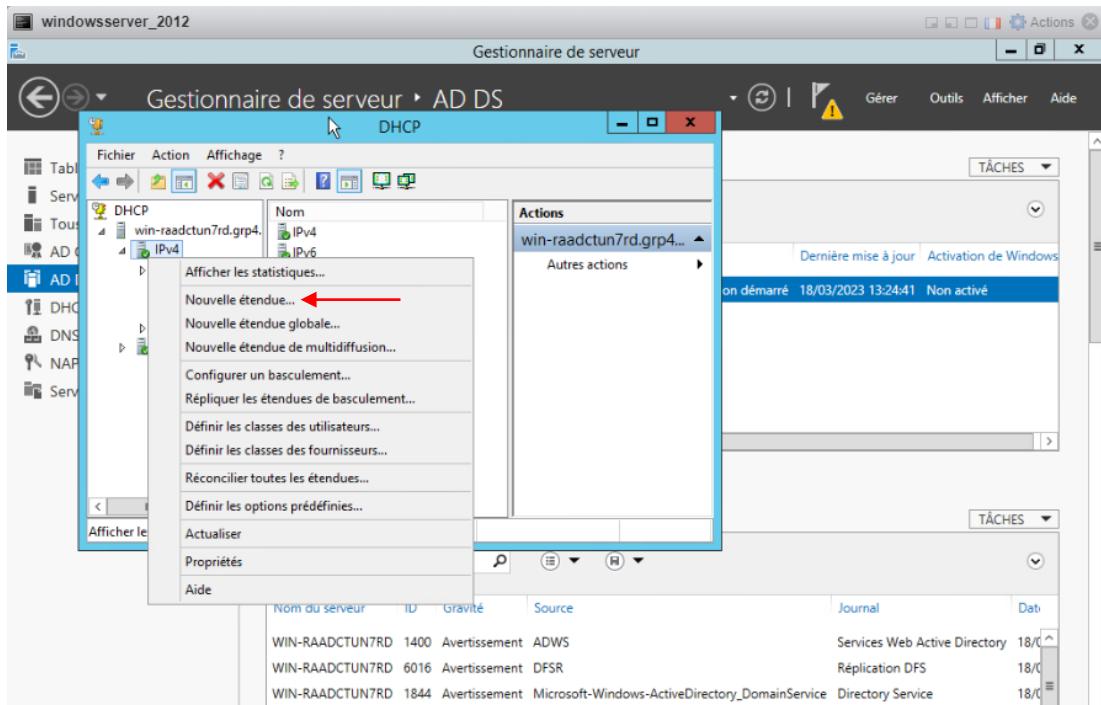


Figure 80 : L'ajout d'une nouvelle étendue

- Donnez un nom et une description à cette étendue, puis appuyez sur le bouton « Suivant ».

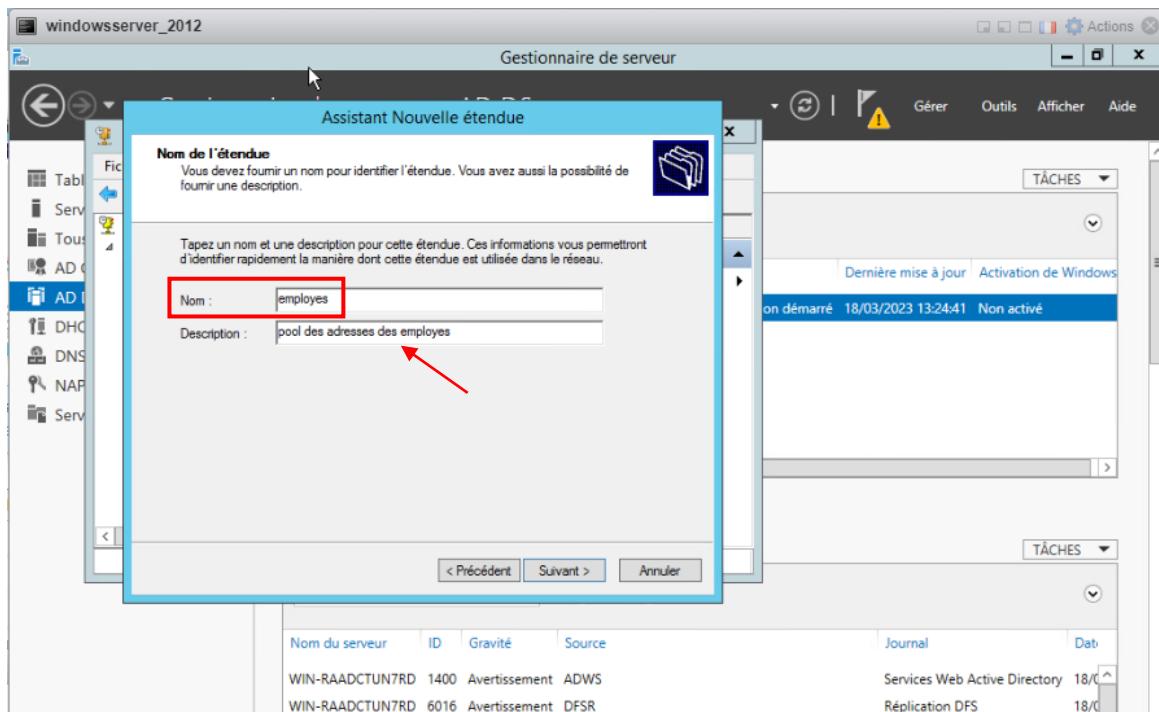


Figure 81 : L'ajout de l'étendue "Employés"

- Indiquez la plage d'adresses IP avec le sous-réseau que vous devez distribuer aux ordinateurs clients, puis cliquez sur le bouton « Suivant ».

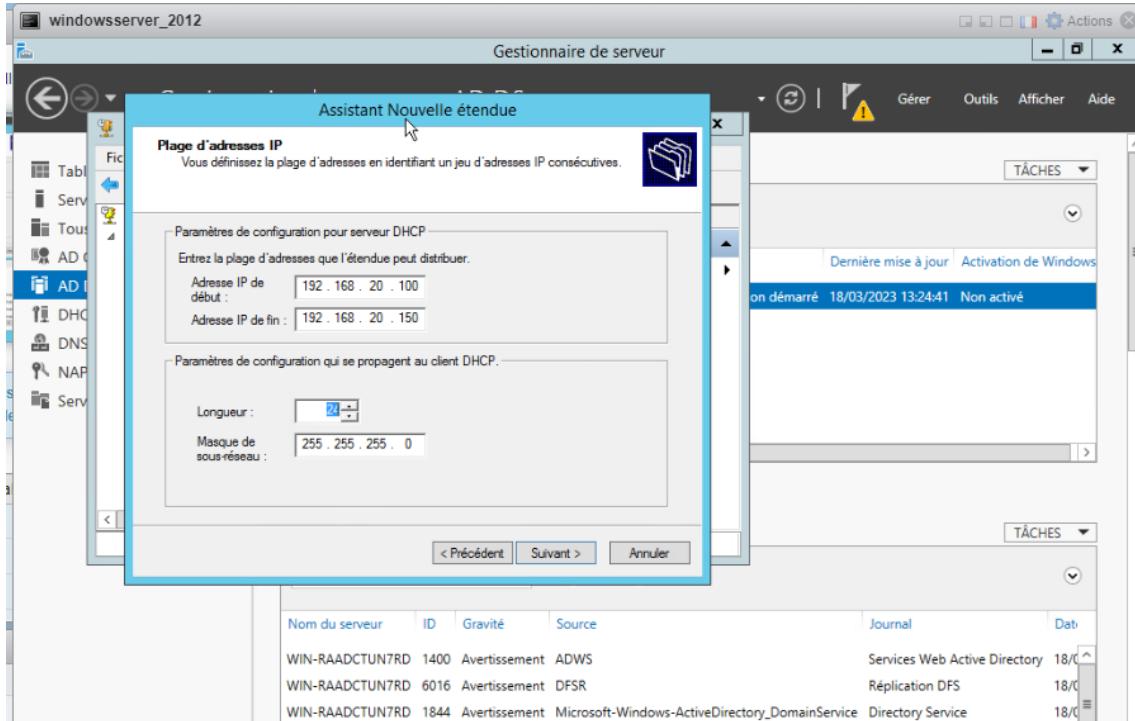


Figure 82 : La saisie de la plage d'adresses IP

- Fixez la durée du bail à 8 jours et appuyez sur le bouton « Suivant ».

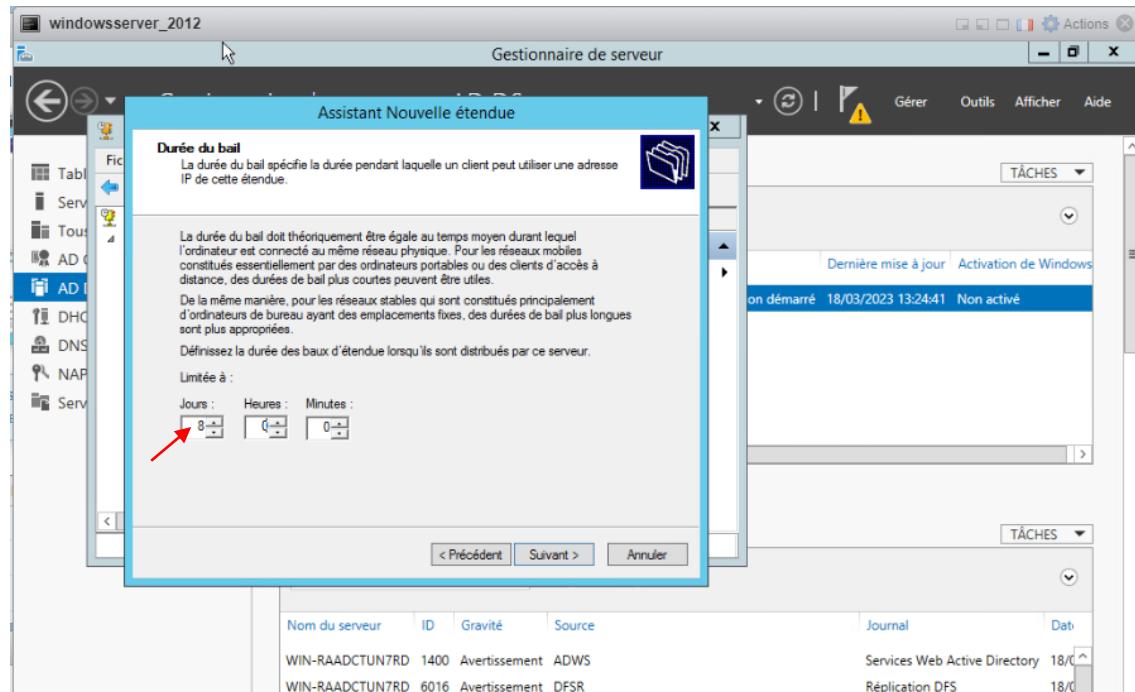


Figure 83 : Fixation de la durée du bail

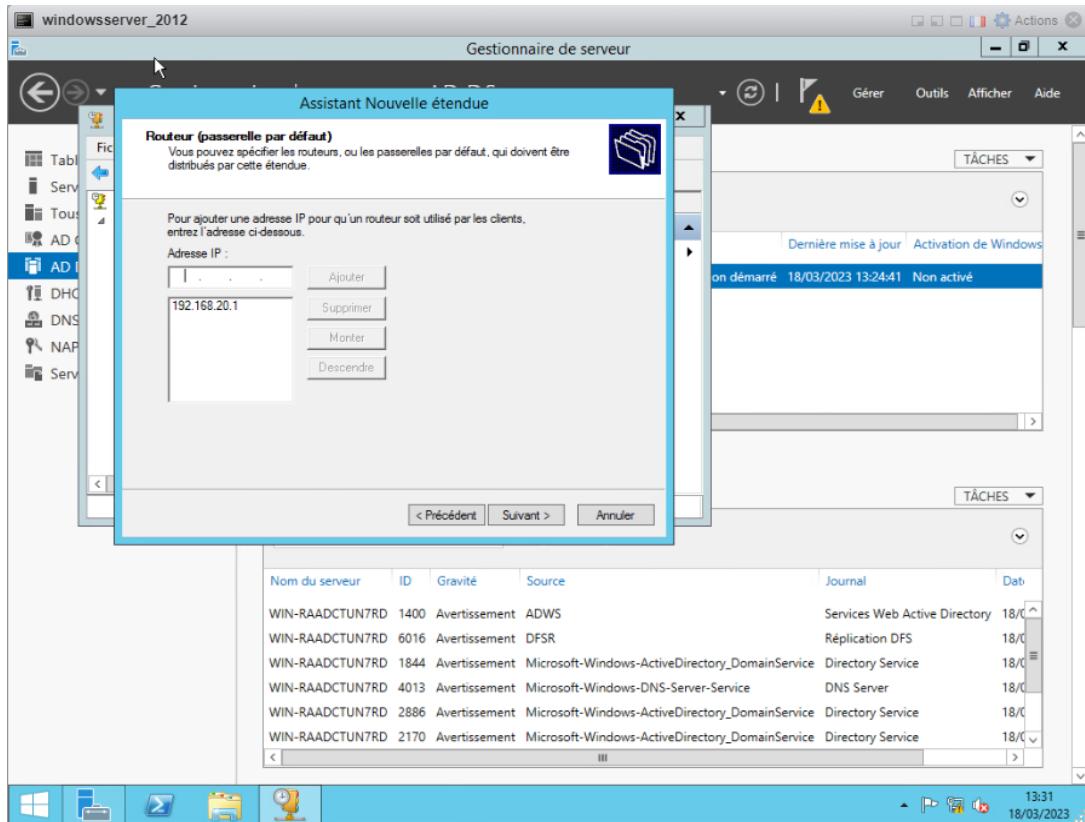


Figure 84 : La finalisation de la création d'étendue

- Enfin, cliquez sur « Terminer » pour mettre fin à l'assistant de création d'étendue.

4. L'installation et la configuration du serveur RADIUS :

a) Installation du Serveur RADIUS (NPS) :

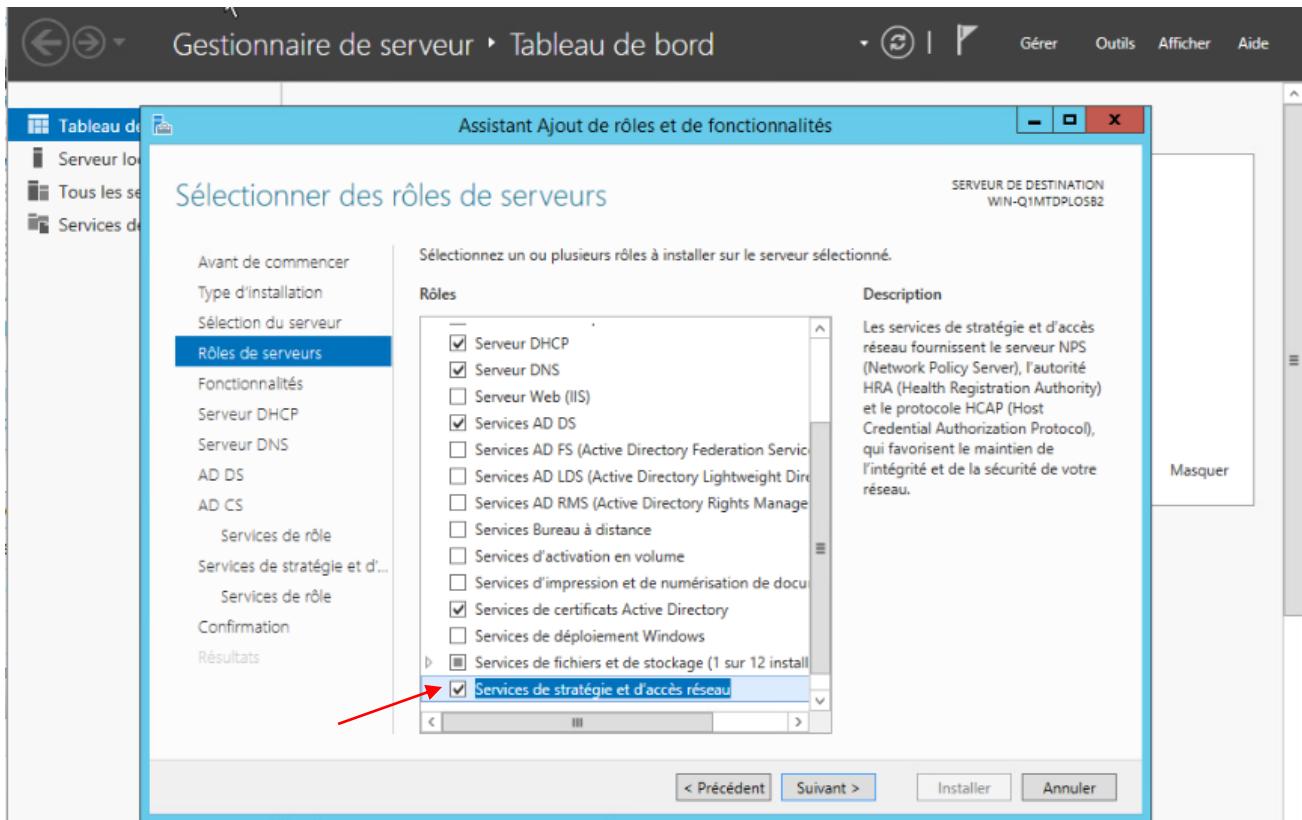


Figure 85 : Installation du serveur RADIUS

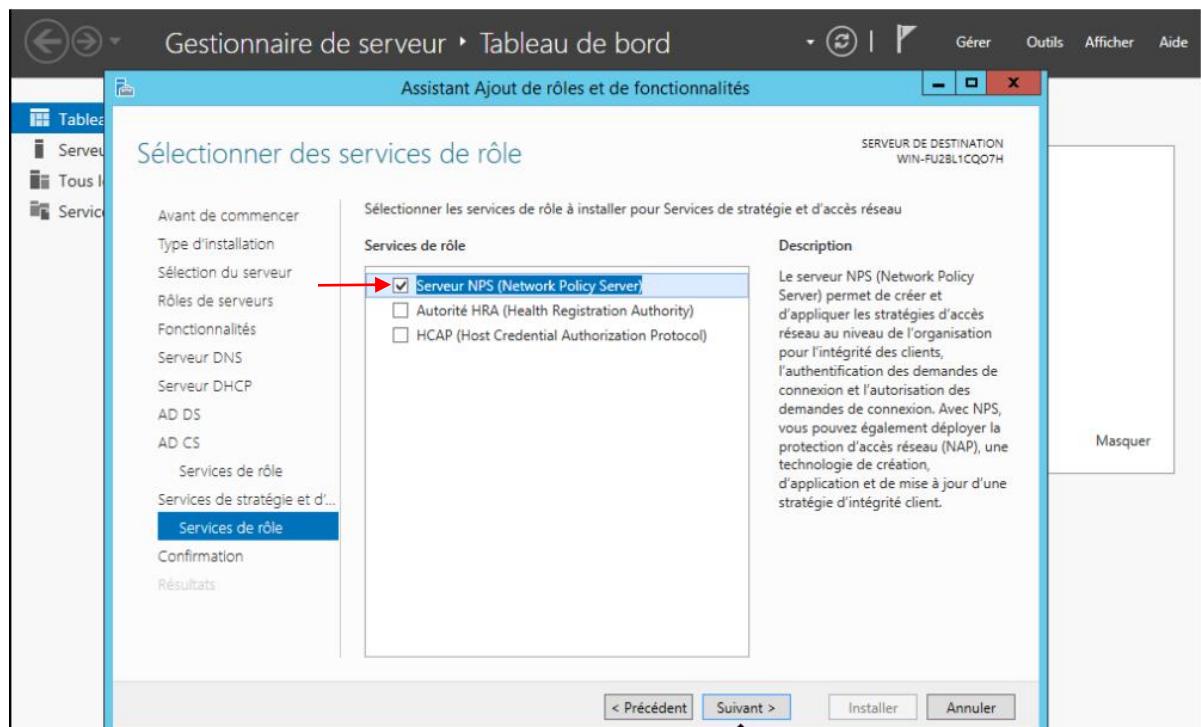


Figure 86 : La sélection du serveur NPS

b) Configuration du NPS :

Lors de la configuration de NPS en tant que serveur RADIUS, vous avez paramétré les clients RADIUS, la stratégie réseau ainsi que la gestion des comptes RADIUS.

i. Configuration des clients RADIUS :

Pour configurer les clients RADIUS, il y a deux étapes à suivre :

- Pour configurer le client RADIUS physique, tel qu'un point d'accès sans fil ou un commutateur d'authentification, vous devez fournir des informations permettant au serveur d'accès réseau de communiquer avec les serveurs NPS. Cela implique de configurer l'adresse IP du serveur NPS et le secret partagé via l'interface utilisateur du point d'accès ou du commutateur.
- Pour ajouter un nouveau client RADIUS dans NPS, il faut ajouter chaque point d'accès ou commutateur d'authentification en tant que client RADIUS sur le serveur NPS. Avec NPS, il est possible de donner un nom convivial pour chaque client RADIUS et de spécifier l'adresse IP du client RADIUS ainsi que le secret partagé.

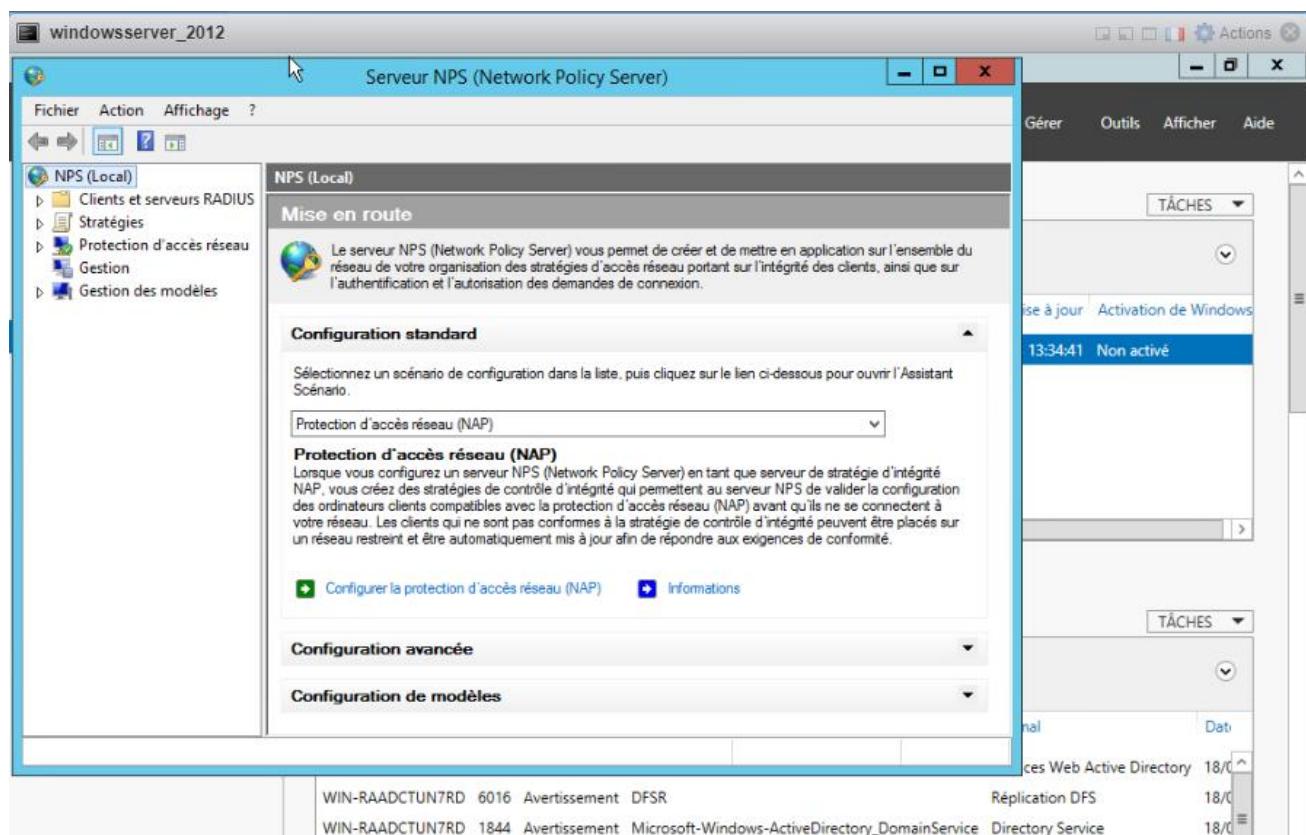


Figure 87 : Configuration des clients RADIUS

- Veuillez sélectionner « Serveur RADIUS » pour les connections câblées ou sans fils 802.1X

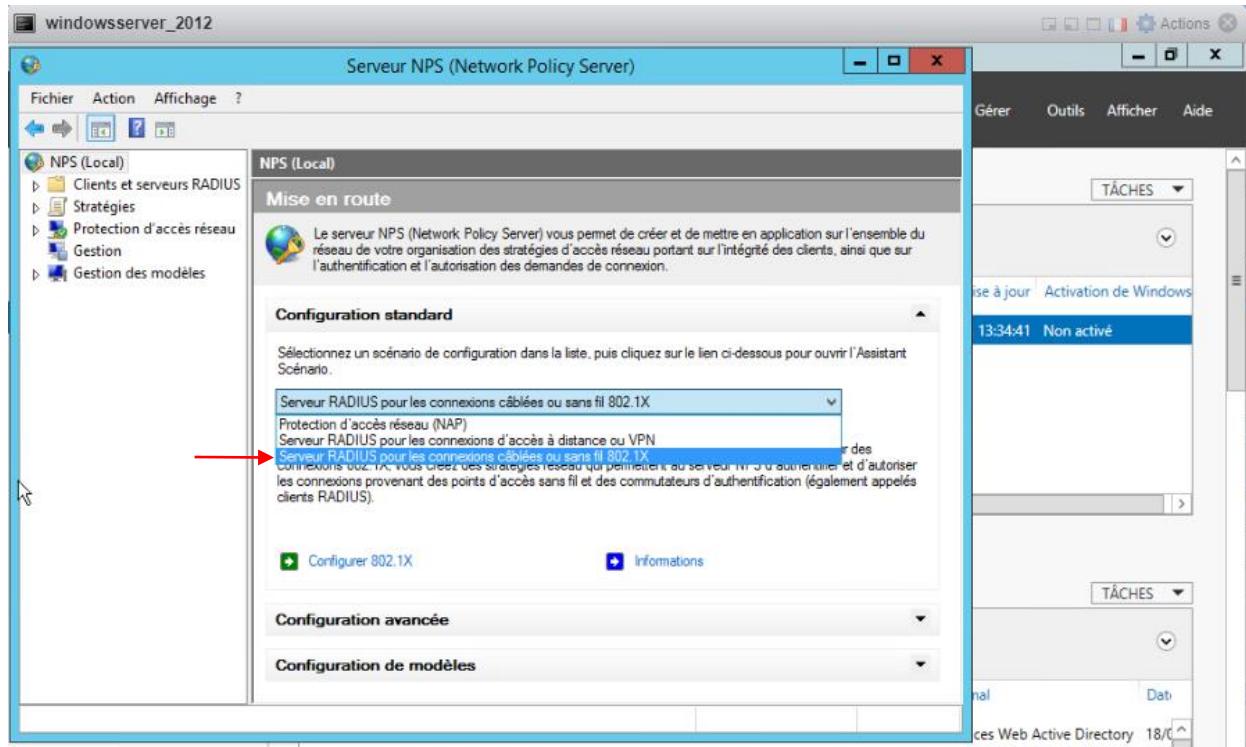


Figure 88 : Le choix de serveur RADIUS

- Ensuite, sélectionner le type de connexion (optionnel)

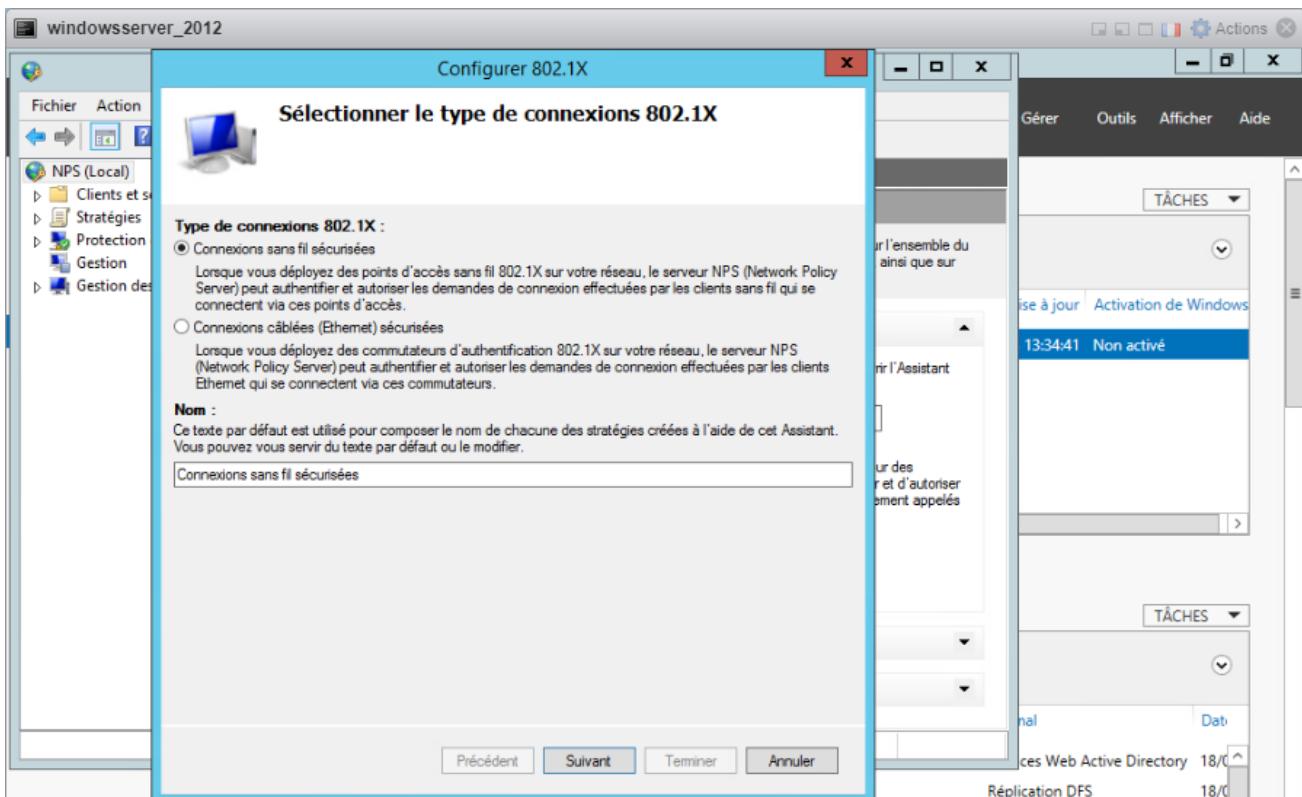


Figure 89 : La sélection du type de connexion

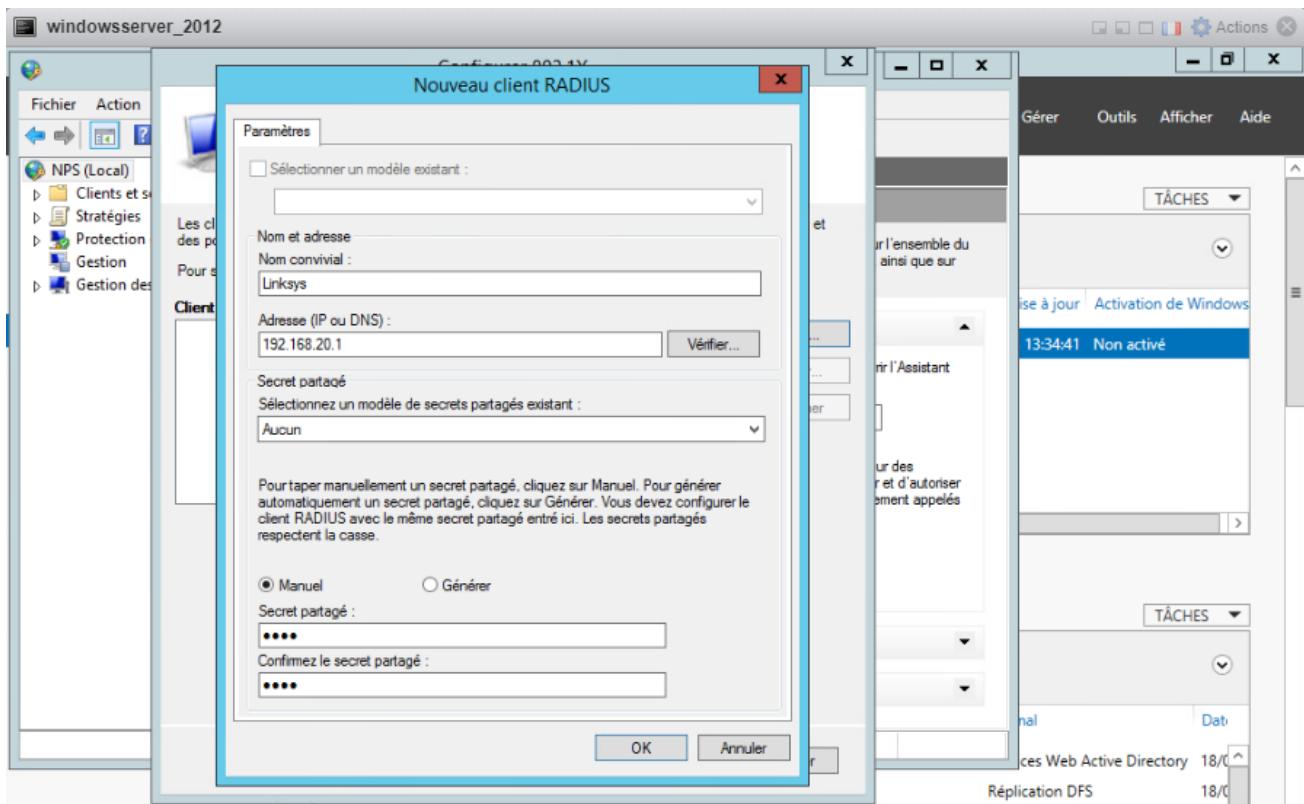


Figure 90 : Authentification en tant qu'un nouveau client RADIUS

- Sélectionner le client que vous avez ajouté et votre méthode d'authentification.

La méthode d'authentification :

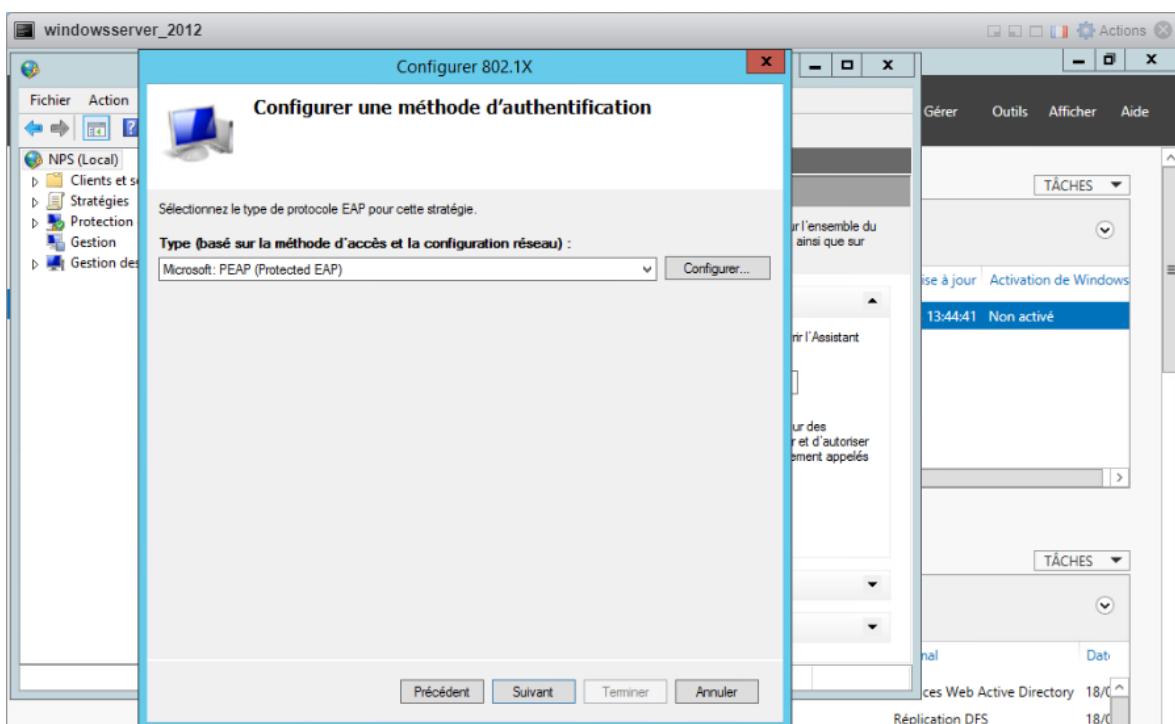


Figure 91 : La méthode d'authentification RADIUS

- Le client :

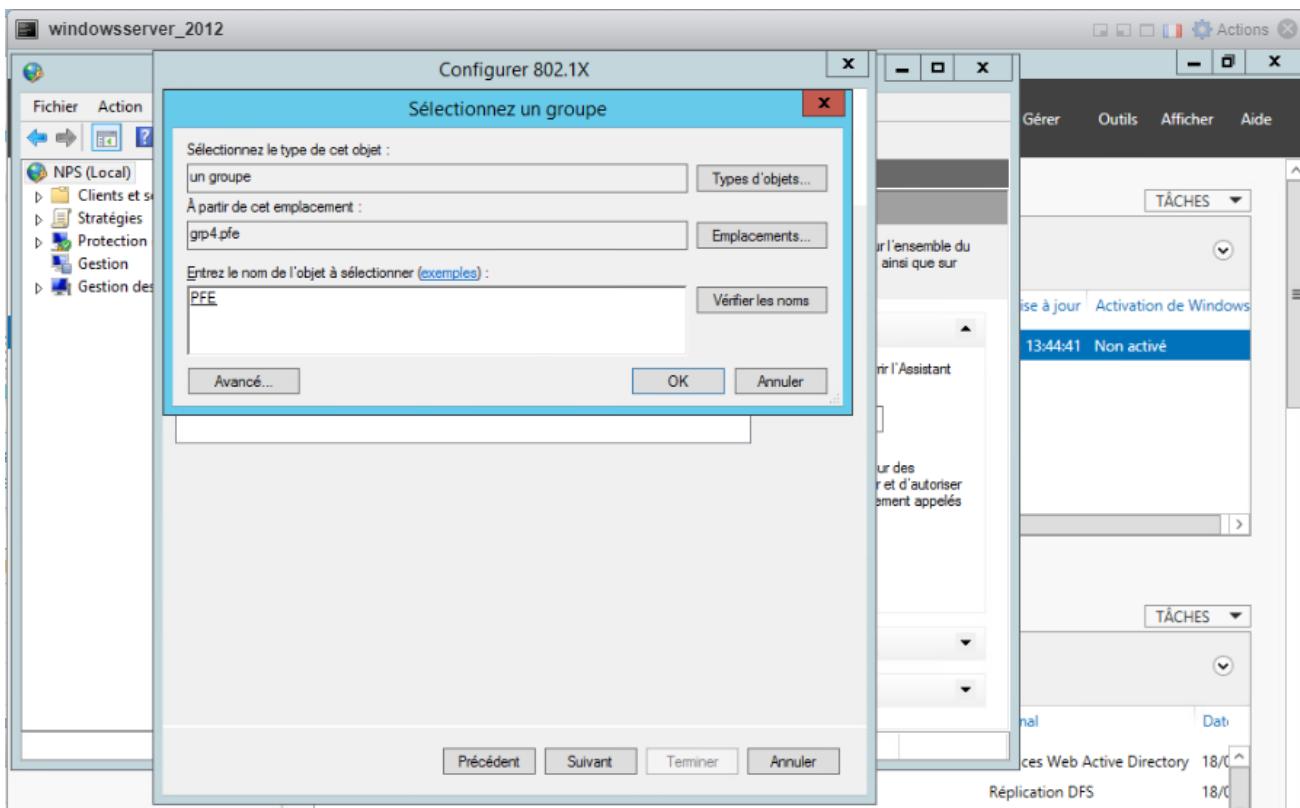


Figure 92 : Le client RADIUS

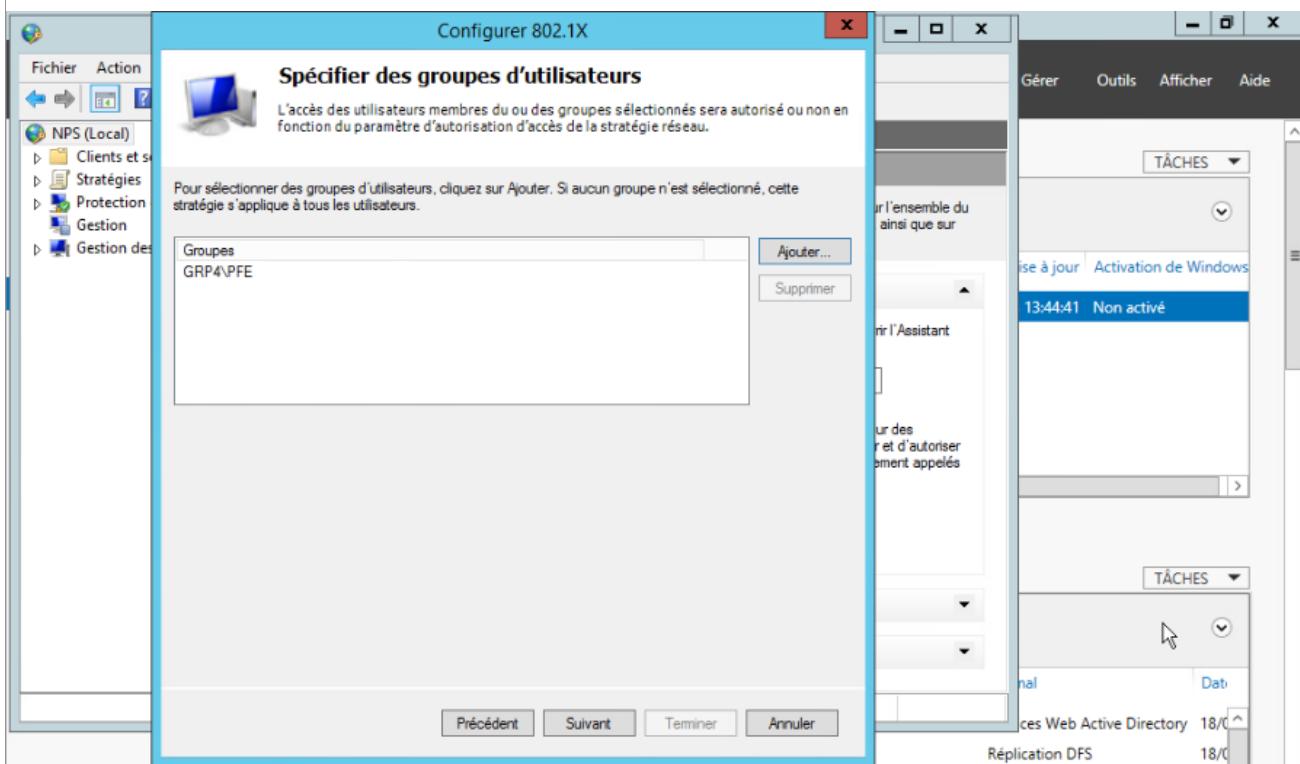


Figure 93 : Le choix d'un groupe autorisé à se connecter au point d'accès

- Nous avons choisi les groupes d'utilisateurs PFE, c'est-à-dire ceux qui sont autorisés à se connecter au point d'accès après l'authentification. Nous poursuivons jusqu'à la fin.

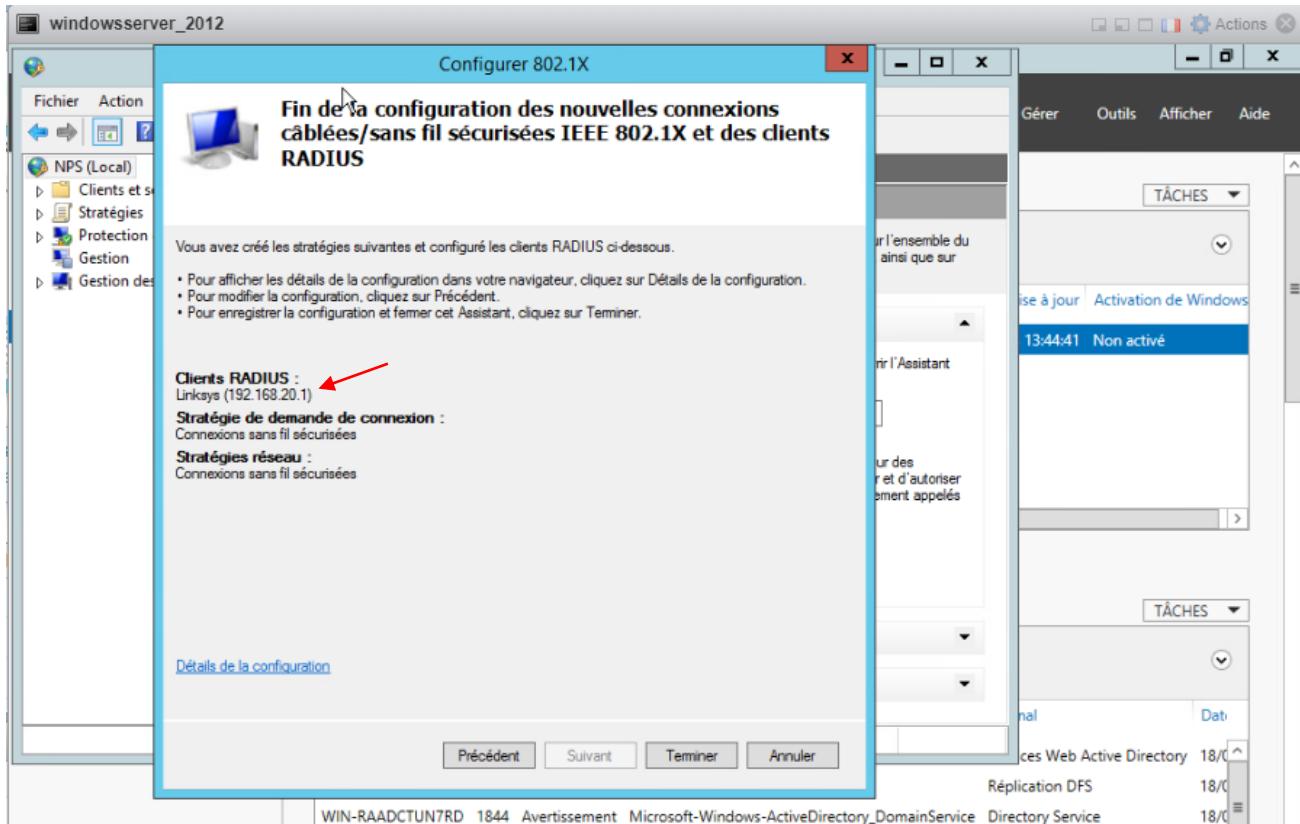


Figure 94 : La finalisation de configuration RADIUS

c) Test de fonctionnement :

Configuration du point d'accès pour activer RADIUS :

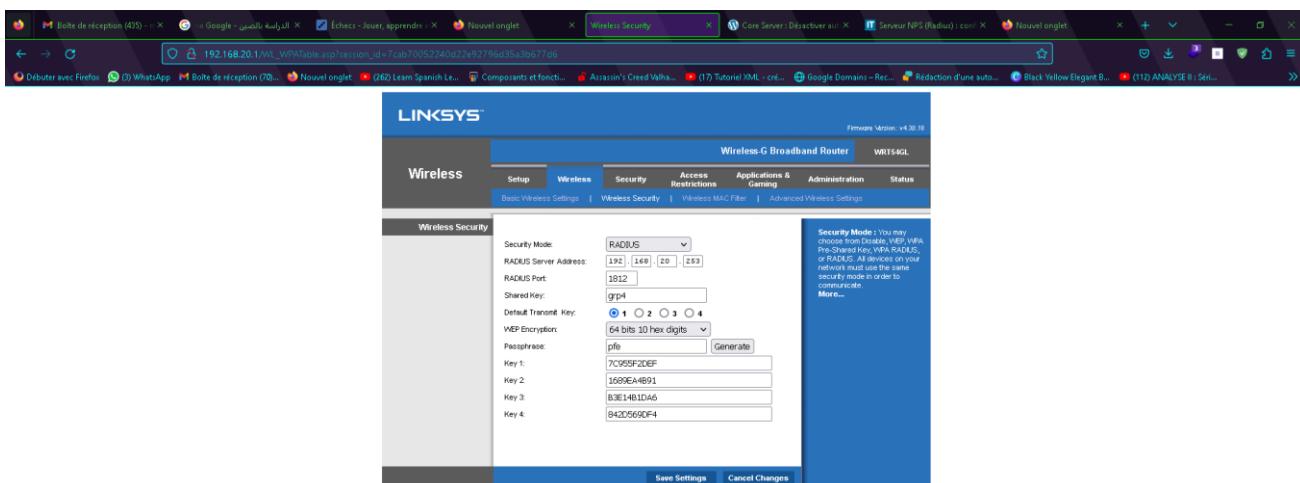


Figure 95 : Configuration du point d'accès pour activer RADIUS

LINKSYS™

Firmware Version: v4.30.18

Wireless-G Broadband Router WRT54GL

Setup

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Language
Select your language
English ▾

Internet Setup
Internet Connection Type
Optional Settings (required by some ISPs)

Automatic Configuration - DHCP ▾

Router Name: Linksys
Host Name:
Domain Name: gpr4.pfe
MTU: Auto ▾
Size: 1500

Network Setup
Router IP

Local IP Address: 192 . 168 . 20 . 1
Subnet Mask: 255.255.255.0 ▾

DHCP Server: Enable Disable
Starting IP Address: 192.168.20.100
Maximum Number of DHCP Users: 50
IP Address Range: 192.168.20.100 to 149
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 192 . 168 . 20 . 253
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0

Time Setting
Time Zone: (GMT) Gambia, Liberia, Morocco ▾
 Automatically adjust clock for daylight saving changes

Save Settings **Cancel Changes**

Automatic Configuration - DHCP: This setting is most commonly used by Cable operators.

Host Name: Enter the host name provided by your ISP.

Domain Name: Enter the domain name provided by your ISP.
[More...](#)

Local IP Address: This is the address of the router.

Subnet Mask: This is the subnet mask of the router.

DHCP Server: Allows the router to manage your IP addresses.

Starting IP Address: The address you would like to start with.

Maximum number of DHCP Users: You may limit the number of addresses your router hands out.
[More...](#)

Time Setting: Choose the time zone you are in. The router can also adjust automatically for daylight savings time.

Figure 96 : Network Setup du point d'accès

La connexion au point d'accès réseau.



Figure 98 : L'affichage du point d'accès

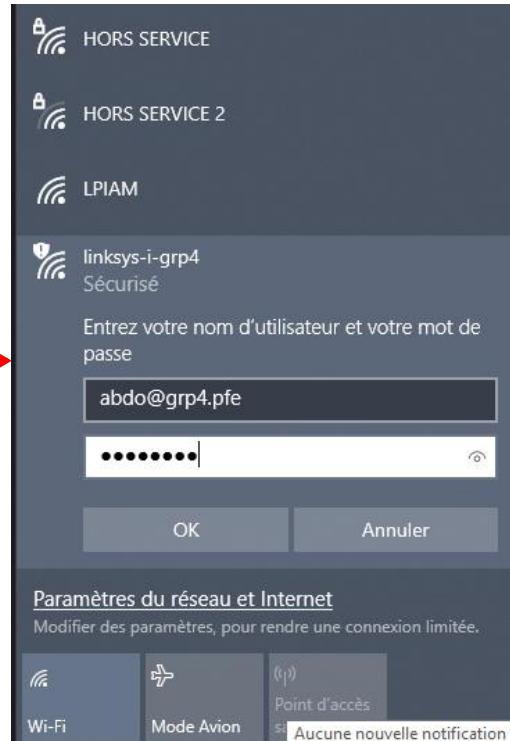


Figure 97 : L'authentification d'un employé

Connexion RADIUS établie :



Figure 99 : La connexion RADIUS réalisé

Chapitre V : Mise en œuvre du réseau des invités

Notre entreprise est axée sur les invités et cherche à leur offrir des services dédiés. Ainsi, nous souhaitons leur permettre d'accéder en toute sécurité à Internet et aux services proposés en mettant en place une solution technique facile à utiliser qui permettra l'authentification des invités pour se connecter au réseau.

I. Portail Captif :

1. Définition :

Le portail captif est une technique utilisée pour contrôler l'accès à un réseau Wi-Fi ou filaire. Lorsqu'un utilisateur se connecte à un réseau équipé d'un portail captif, son accès à Internet est bloqué et il est automatiquement redirigé vers une page web spécifique (le portail captif) où il doit entrer des informations d'identification ou accepter les conditions d'utilisation du réseau pour obtenir l'accès complet à Internet.

Le portail captif est souvent utilisé dans les lieux publics tels que les aéroports, les cafés, les hôtels ou les centres commerciaux, où il est nécessaire de contrôler l'accès à Internet pour des raisons de sécurité ou de respect des lois et réglementations en vigueur.

2. Fonctionnement :

Le portail captif fonctionne en interceptant tous les paquets liés aux protocoles HTTP/HTTPS (protocoles de communication pour le web) des utilisateurs qui tentent de se connecter à Internet via le réseau Wi-Fi ou filaire.

Lorsqu'un utilisateur tente d'accéder à une page web, sa demande est redirigée automatiquement vers la page du portail captif. Cette page peut demander à l'utilisateur de s'authentifier en entrant des informations d'identification ou en acceptant les conditions d'utilisation du réseau.

Si l'utilisateur, qui représente l'employé sans notre cas, entre les informations d'identification correctes ou accepte les conditions d'utilisation, il est autorisé à accéder à Internet. Si les informations d'identification sont incorrectes ou si les conditions d'utilisation ne sont pas acceptées, l'accès à Internet est bloqué.

Le portail captif peut également être utilisé pour afficher des publicités ou des informations importantes pour les utilisateurs avant de leur permettre l'accès complet à Internet.

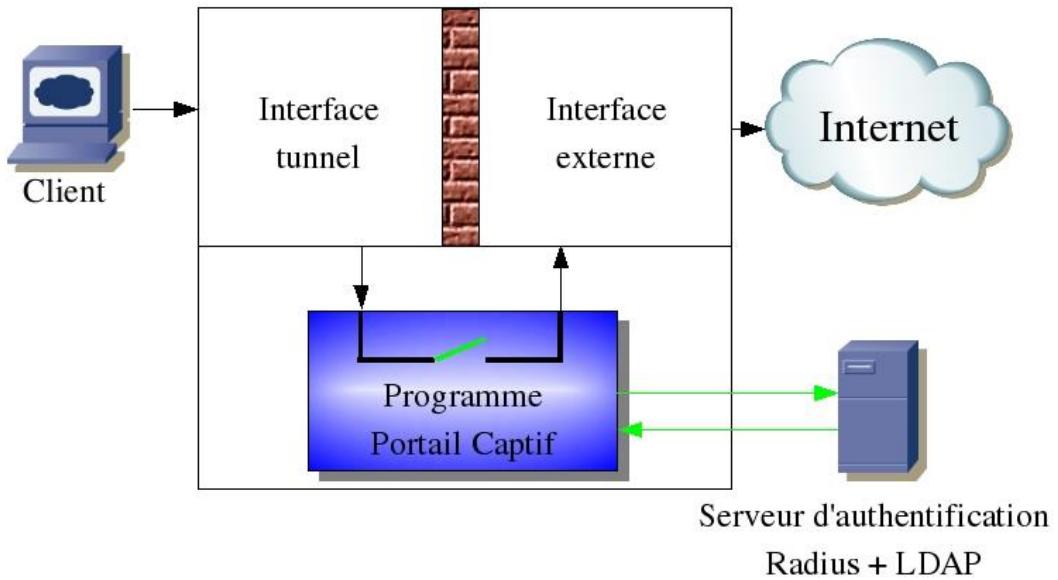


Figure 100 : Schéma expliquant le portail captif

Au cours de la première étape, l'employé se connecte au point d'accès en utilisant son SSID. Lorsqu'il souhaite accéder à une URL sur Internet, un formulaire d'authentification est envoyé par le portail captif. Ce formulaire, contenant les champs d'authentification, est transmis au portail captif.

Si les informations d'authentification fournies sont correctes, l'accès à Internet est autorisé par le portail.

II.Pfsense :

1. Définition :

Pfsense est une distribution gratuite et open source de pare-feu et de routeur basée sur le système d'exploitation FreeBSD. Il est conçu pour être facile à installer et à utiliser, et offre une interface web graphique pour la configuration et la gestion.

Pfsense est utilisé par de nombreux professionnels de la sécurité et des réseaux pour créer des réseaux sécurisés et fiables. Il offre une variété de fonctionnalités de sécurité, notamment des pare-feux, des VPN, des proxys, des antivirus et des filtrages de contenu web.

Pfsense est également connu pour sa flexibilité, car il peut être utilisé sur du matériel personnalisé, ou installé sur des machines virtuelles. Cela permet aux utilisateurs de choisir le matériel qui convient le mieux à leurs besoins et de personnaliser la configuration du système en fonction de leurs besoins spécifiques.

2. Les services du Pfsense :

Pfsense offre une large gamme de services pour la sécurité, la gestion des réseaux et la connectivité. Voici quelques-uns des services offerts par Pfsense :

- Pare-feu : Pfsense est équipé d'un puissant pare-feu qui permet de filtrer le trafic réseau entrant et sortant. Il offre des règles de pare-feu personnalisables pour bloquer ou autoriser le trafic selon les besoins de l'utilisateur.
- VPN : pfsense prend en charge les connexions VPN pour permettre un accès sécurisé aux réseaux distants. Il offre des protocoles VPN tels que OpenVPN et IPSec.
- Proxy : pfSense prend en charge les serveurs proxy, ce qui permet de filtrer et de bloquer le trafic Web indésirable. Il peut également accélérer les connexions Web en mettant en cache les pages Web populaires.
- DNS : pfSense prend en charge les serveurs DNS et peut être utilisé pour gérer les domaines et les résolutions de noms.
- Filtrage de contenu : pfSense offre un filtrage de contenu Web pour bloquer les sites Web malveillants ou inappropriés. Il peut également être utilisé pour bloquer les publicités en ligne.



Figure 101 : Logo du Pfsense

3. Le cycle de vie de l'authentification :

Lorsque l'invité se connecte à un réseau Wi-Fi via un point d'accès sans fil, le service DHCP installé sur le serveur Windows lui attribue une adresse IP et configure les paramètres réseau à l'aide de la fonction DHCP Relay de Pfsense. Cependant, le client n'a initialement accès qu'au réseau entre lui et la passerelle Pfsense, étant donné que la passerelle lui interdit l'accès au reste du réseau.

Lorsque l'invité effectue sa première requête Web en HTTP ou HTTPS, la passerelle redirige la requête DNS vers le serveur DNS de Windows, qui répond ou interroge son propre serveur DNS. Après l'obtention de la réponse DNS, la passerelle redirige l'invité vers une page Web d'authentification qui requiert un login et un mot de passe cryptés à l'aide du protocole SSL pour sécuriser la transmission. Le système d'authentification contacte ensuite une base de données contenant la liste des utilisateurs autorisés à accéder au réseau.

Une fois que l'invité est authentifié, le système d'authentification indique à la passerelle que le couple MAC/IP de l'invité est autorisé à accéder au réseau. L'invité est alors redirigé vers la page Web qu'il avait demandée initialement et a désormais accès à l'ensemble du réseau derrière la passerelle. Le portail captif surveille l'activité de l'utilisateur en utilisant divers mécanismes tels qu'une fenêtre pop-up rafraîchie à intervalles réguliers ou des requêtes Ping vers le client. Si l'invité est absent du réseau pendant un certain temps, le portail captif coupera son accès.

4. L'installation du PfSense :

Nous avons décrit les étapes pratiques pour mettre en œuvre le logiciel, que ce soit en l'installant directement sur le disque dur ou en utilisant un live CD. Bien que la seconde option soit rapide et efficace, elle présente des inconvénients tels qu'un chargement long, une fiabilité réduite et l'impossibilité d'ajouter des logiciels supplémentaires en raison de la structure du CD. Ainsi, pour plus de sécurité, nous avons choisi d'installer le logiciel sur le disque dur pour l'implémenter dans le réseau. De plus, il est également possible de l'installer sur un ESXI en utilisant une image ISO, un CD ou une clé bootable.

Dans notre cas, nous avons opté pour l'installation via une image ISO, ce qui implique de copier cette image sur le disque dur du serveur à l'aide de SSH et de créer une nouvelle machine virtuelle pour PfSense dans l'ESXI.

Après avoir configuré les paramètres tels que la carte réseau, le disque dur et la RAM, nous pouvons alors allumer la machine virtuelle.

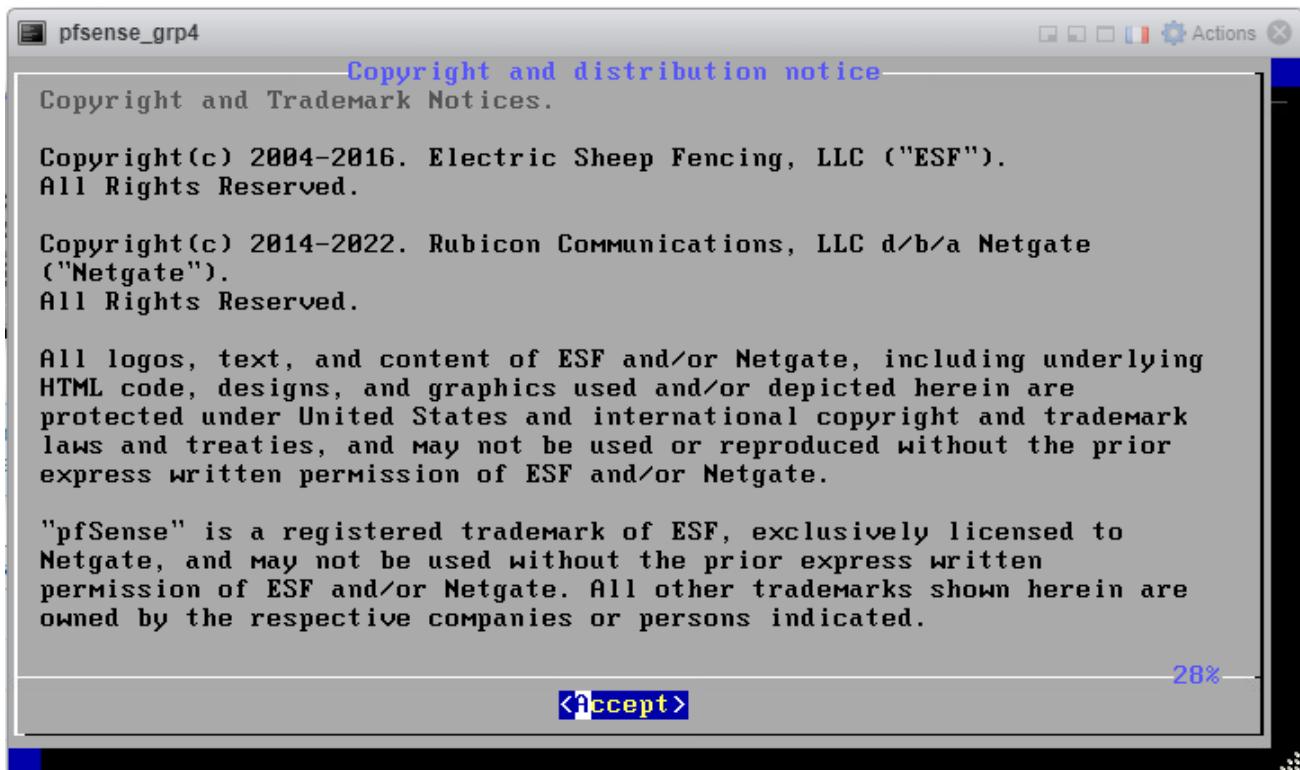


Figure 102 : L'installation du PfSense

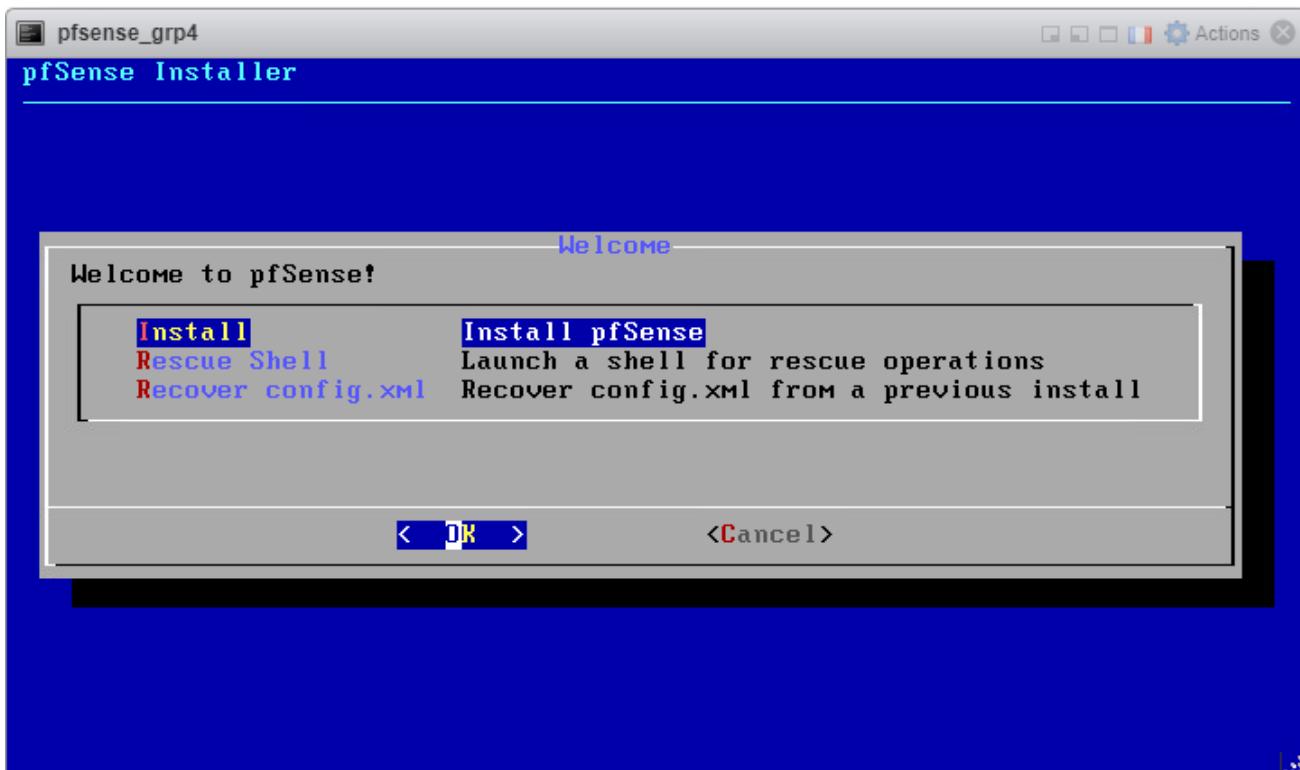


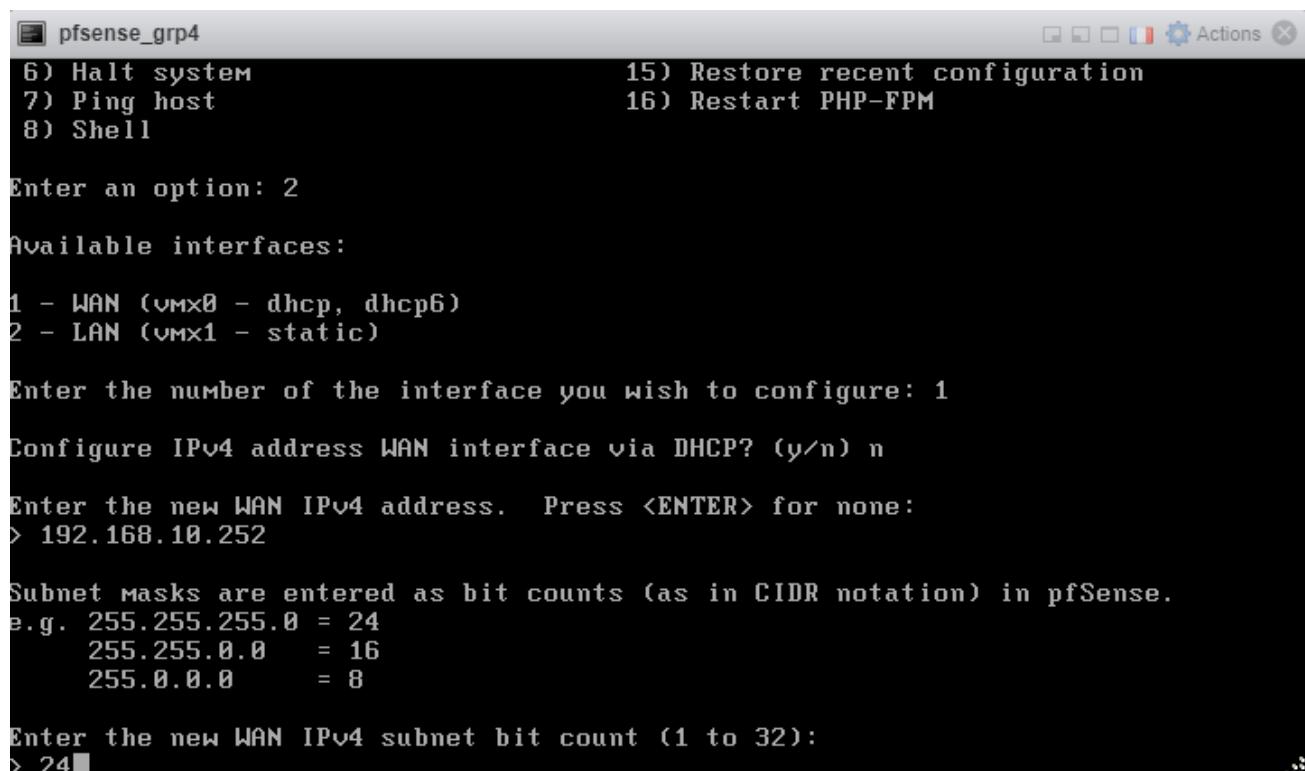
Figure 103 : Page d'accueil de l'installation du PfSense

Une fois l'installation et le lancement de Pfsense terminés, la première étape consiste à configurer les interfaces réseau. Pour cela, nous allons utiliser la console de Pfsense et sélectionner l'option numéro 2 (Set interfaces IP address) pour configurer l'interface réseau numéro 1 (vmx0) et l'interface réseau numéro 2 (vmx1).

Nous avons attribué des adresses d'une manière statique :

WAN → vmx0 : 192.168.10.252/24

LAN → vmx1 : 192.168.1.254/24



```
pfSense_grp4 Actions
6) Halt system 15) Restore recent configuration
7) Ping host 16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (vmx0 - dhcp, dhcp6)
2 - LAN (vmx1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.10.252

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0    = 16
      255.0.0.0      = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24
```

Figure 104 : Configuration des interfaces réseau

The screenshot shows a terminal window titled "pfSense_grp4". The boot process is displayed:

```
Starting syslog...done.  
Starting CRON... done.  
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022  
Bootup complete
```

System information follows:

```
FreeBSD/amd64 (invites.lan) (ttyv0)  
VMware Virtual Machine - Netgate Device ID: f8e7395ea48a2c931e89
```

A welcome message for pfSense 2.6.0-RELEASE (amd64) on invites is shown:

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on invites ***
```

Network interfaces are listed:

```
WAN (wan)      -> vmx0      -> v4: 192.168.10.252/24  
LAN (lan)      -> vmx1      -> v4: 192.168.1.254/24
```

A menu of 16 options is provided:

0) Logout (SSH only)	9) pfTop
1) Assign Interfaces	10) Filter Logs
2) Set interface(s) IP address	11) Restart webConfigurator
3) Reset webConfigurator password	12) PHP shell + pfSense tools
4) Reset to factory defaults	13) Update from console
5) Reboot system	14) Enable Secure Shell (sshd)
6) Halt system	15) Restore recent configuration
7) Ping host	16) Restart PHP-FPM
8) Shell	

The prompt "Enter an option: " is visible at the bottom.

Figure 105 : Configuration des interfaces LAN et WAN

Maintenant l'interface LAN et WAN sont configurés alors on peut accéder à l'interface web pour continuer la configuration restante.

III. Configuration du PfSense :

1. L'interface Web PfSense :

Pour accéder à l'interface de configuration via le navigateur web, il est nécessaire de connecter un PC à l'interface LAN de PFSense. Il suffit ensuite d'ouvrir un navigateur web et d'entrer l'adresse IP LAN de la machine dans la barre d'adresse, en l'occurrence <http://192.168.1.254> dans notre cas. Une fois la page de connexion affichée, il faut entrer un nom d'utilisateur et un mot de passe pour accéder à l'interface. Le nom d'utilisateur par défaut est "admin" et le mot de passe est "pfsense". Ces informations permettent de se connecter en tant qu'administrateur.

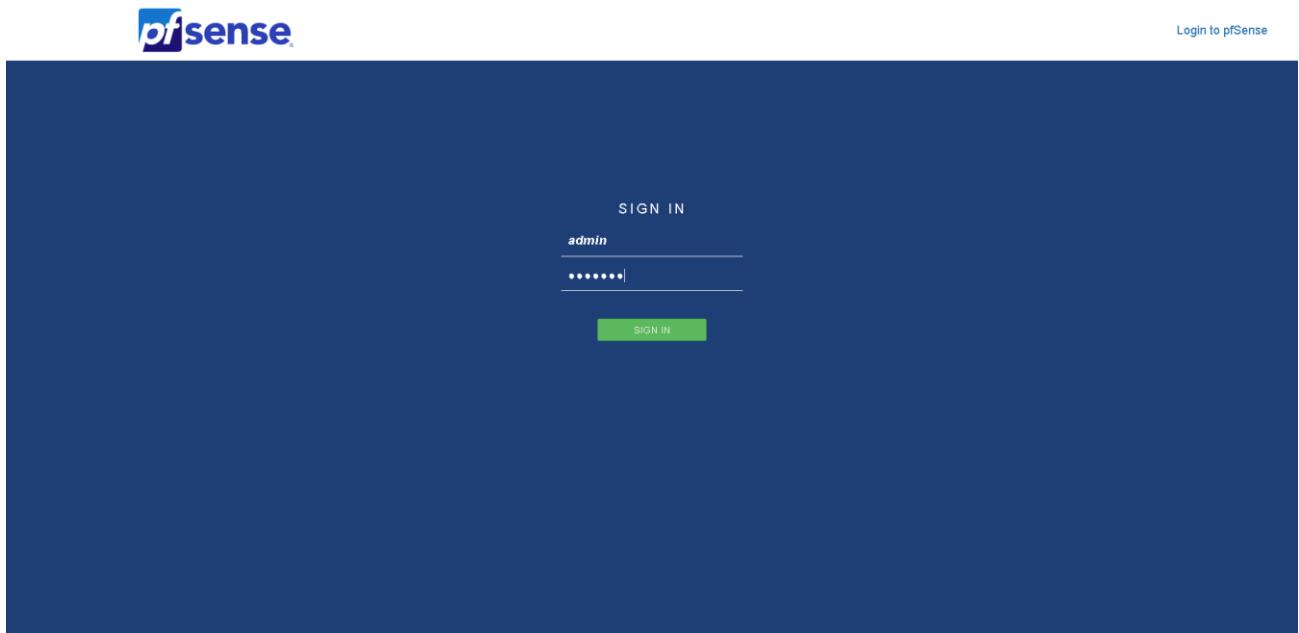


Figure 106 : Interface Web du Pfsense

Nous accédons maintenant au tableau de bord de notre Pfsense. Dans cette fenêtre, nous pouvons trouver diverses informations telles que l'utilisation des ressources de la machine, ses adresses IP, sa version et les mises à jour disponibles...

A screenshot of the pfSense dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red warning message says: 'WARNING: The "admin" account password is set to the default value. Change the password in the User Manager.' The main dashboard is divided into several sections: 'System Information' (including Name, User, System, BIOS, Version, CPU Type, Hardware crypto, Kernel PTI, MDS Mitigation, Uptime, Current date/time, DNS server(s), Last config change, State table size, and MBUF Usage); 'Netgate Services And Support' (showing 'Retrieving support information'); and 'Interfaces' (listing WAN and LAN ports with their respective IP addresses: 192.168.10.252 and 192.168.1.254).

Figure 107 : Page d'accueil Pfsense

a) DHCP et DNS :

On vérifie maintenant la plage d'adresse du DHCP que nous avons configuré :

192.168.1.1 – 192.168.1.254

The screenshot shows the Pfsense web interface under the 'Services / DHCP Server / LAN' section. The 'LAN' tab is selected. In the 'General Options' section, the 'Enable' checkbox is checked, and the 'Subnet' is set to 192.168.1.0 with a 'Subnet mask' of 255.255.255.0. The 'Available range' is specified as 192.168.1.1-192.168.1.254. Below this, there are sections for 'Deny unknown clients' (set to 'Allow all clients'), 'Ignore denied clients' (unchecked), and 'Ignore client identifiers' (unchecked). An 'Additional Pools' section at the bottom contains an 'Add' button and a note about specifying additional address pools outside the main range.

Figure 108 : Configuration DHCP sur Pfsense

Ensuite, dans le menu « System », on clique sur « General setup ». Il faut indiquer le nom que l'on donne à la machine, et le domaine sur lequel elle se trouve. On indique ensuite le serveur DNS

- Domaine : invites.lan
- Dns Serveur : 192.168.1.3

The screenshot shows the 'System / General Setup' section of the Pfsense web interface. Under 'System', the 'Hostname' is set to 'invites' and the 'Domain' is set to 'lan'. In the 'DNS Server Settings' section, there is one entry for 'DNS Servers' with the address '192.168.1.3'. There is also a 'DNS Hostname' field. Below this, there is a 'DNS Server Override' section with a checked checkbox for 'Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server'. At the bottom, under 'DNS Resolution Behavior', it says 'Use local DNS (127.0.0.1), fall back to remote DNS Servers (Default)'. A note states that by default, the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise.

Figure 109 : Configuration DNS sur Pfsense

b) Pare-feu :

The screenshot shows the 'Firewall / Rules / LAN' section of the Pfsense web interface. It displays a table of 'Rules (Drag to Change Order)' with the following data:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 1.49 MB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	WAN net	*	*	none			
<input type="checkbox"/>	0 / 1003 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom of the table, there are buttons for 'Add', 'Delete', 'Save', and 'Separator'.

Figure 110 : Pfsense

- Par défaut lors de son installation, tout le trafic est ouvert. On peut voir ceci dans le menu «Firewall», sous-menu « Rules » et partie « LAN ».
- Les règles présentes ici définissent que tout le trafic Ipv4 et Ipv6, tout protocole confondu, venant sur réseau local (LAN Net) sur n'importe quel port et vers n'importe quelle destination est autorisé.

c) Portail captif :

La configuration de ce portail captif s'effectue en plusieurs étapes. Tout d'abord, il est nécessaire de créer une zone dédiée à l'activation du portail captif, puis de procéder à sa configuration.

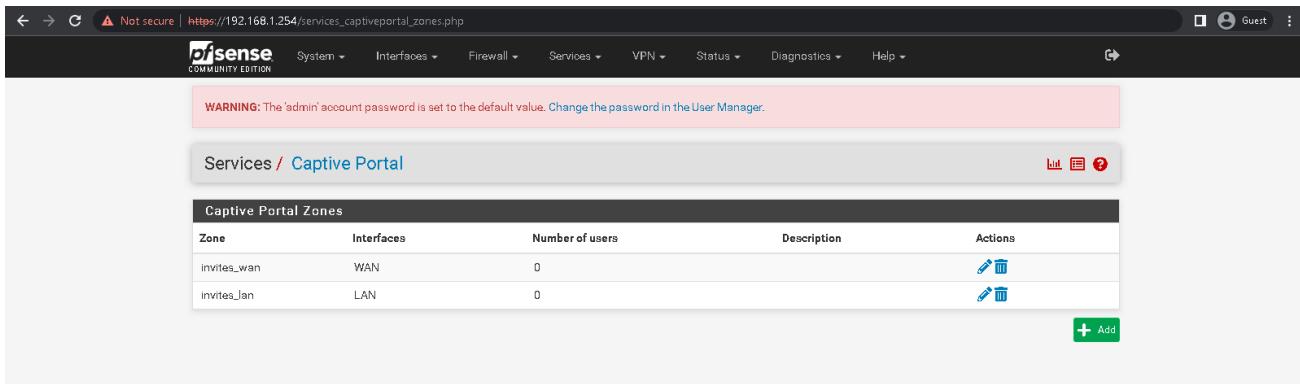


Figure 111 : Zone portail captif

- Pour activer le portail captif, il faut cocher l’option « Enable Captive Portal ». Ensuite, il faut sélectionner l’interface « LAN » sur laquelle le portail sera déployé. Enfin, pour permettre aux utilisateurs de se déconnecter, il convient d’activer l’option « Enable logout popup window », qui affiche une fenêtre contextuelle.

Setting	Value
Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Interfaces	WAN LAN
Maximum concurrent connections	[Input field]
Idle timeout (Minutes)	[Input field]
Hard timeout (Minutes)	[Input field]
Traffic quota (Megabytes)	[Input field]
Pass-through credits per MAC address	[Input field]

Figure 112 : Configuration portail captif

This screenshot shows the configuration page for a captive portal zone named 'portal'. It includes sections for 'Reset waiting period', 'Logout popup window', 'Pre-authentication redirect URL', 'After authentication Redirection URL', 'Blocked MAC address redirect URL', 'Preserve users database', 'Concurrent user logins' (set to 'Multiple'), 'MAC filtering' (disabled), and 'Pass-through MAC Auto Entry' (disabled). The page uses a light blue header and white background with black text.

Figure 113 : Suite de configuration portail captif

This screenshot shows the configuration page for a captive portal zone named 'invites_jan'. It includes sections for 'Authentication Method' (set to 'Use an Authentication backend'), 'Authentication Server' (set to 'Local Database'), 'Secondary authentication Server' (set to 'Local Database'), 'Reauthenticate Users' (unchecked), and 'Local Authentication Privileges' (checkbox checked). It also includes an 'HTTPS Options' section with a 'Login' checkbox (unchecked) and a 'Save' button at the bottom. The page has a dark header and a light blue background with black text.

Figure 114 : Serveurs d'authentification LDAP

- Le premier serveur d'authentification sélectionné est la base de données locale, suivi de la base LDAP en tant que second choix.

2. Cr ation d'un groupe et des utilisateurs :

On proc e    l'ajout du groupe « ari2 » dans la section « User Manager » du syst me. Ce groupe se voit attribuer les privil ges de connexion au portail captif.

The screenshot shows the 'User Manager / Groups / Edit' interface. The 'Groups' tab is selected. A warning message at the top states: 'WARNING: The admin account password is set to the default value. Change the password in the User Manager.' The 'Group Properties' section contains fields for 'Group name' (set to 'ari2'), 'Scope' (set to 'Local'), and 'Description' (empty). The 'Group membership' section shows 'admin' in the 'Not members' dropdown and 'user' in the 'Members' dropdown. Below these are two buttons: 'Move to "Members"' and 'Move to "Not members"'. A note says 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.' The 'Assigned Privileges' section is empty, with a '+ Add' button. At the bottom is a 'Save' button.

Figure 115 : La cr ation d'un groupe

The screenshot shows the 'User Manager / Groups / Edit' interface. The 'Groups' tab is selected. The 'Group Privileges' section shows the 'Group' as 'ari2'. The 'Assigned privileges' dropdown is open, displaying a list of options such as 'User - Services: Captive Portal login', 'User - System: Copy files (scp)', 'User - System: Shell account access', etc. The 'User - Services: Captive Portal login' option is highlighted. Below the dropdown is a 'Filter' input field with the placeholder 'Show only the choices containing this term'. The 'Privilege information' section at the bottom states: 'The following privileges effectively give administrator-level access to users in the group because the user gains access to execute general commands, edit system files, modify users, change passwords or similar.' It lists several privileges including 'User - System: Copy files (scp)', 'User - System: Shell account access', 'System - HA node sync', etc.

Figure 116 : Les droits du portail captif

Après la création du groupe, la dernière étape consiste à créer un compte utilisateur qui sera membre du groupe ari2.

a) Test d'authentification :

Lorsque les invités tenteront d'accéder à Internet, ils devront d'abord s'authentifier avant de pouvoir accéder au réseau.

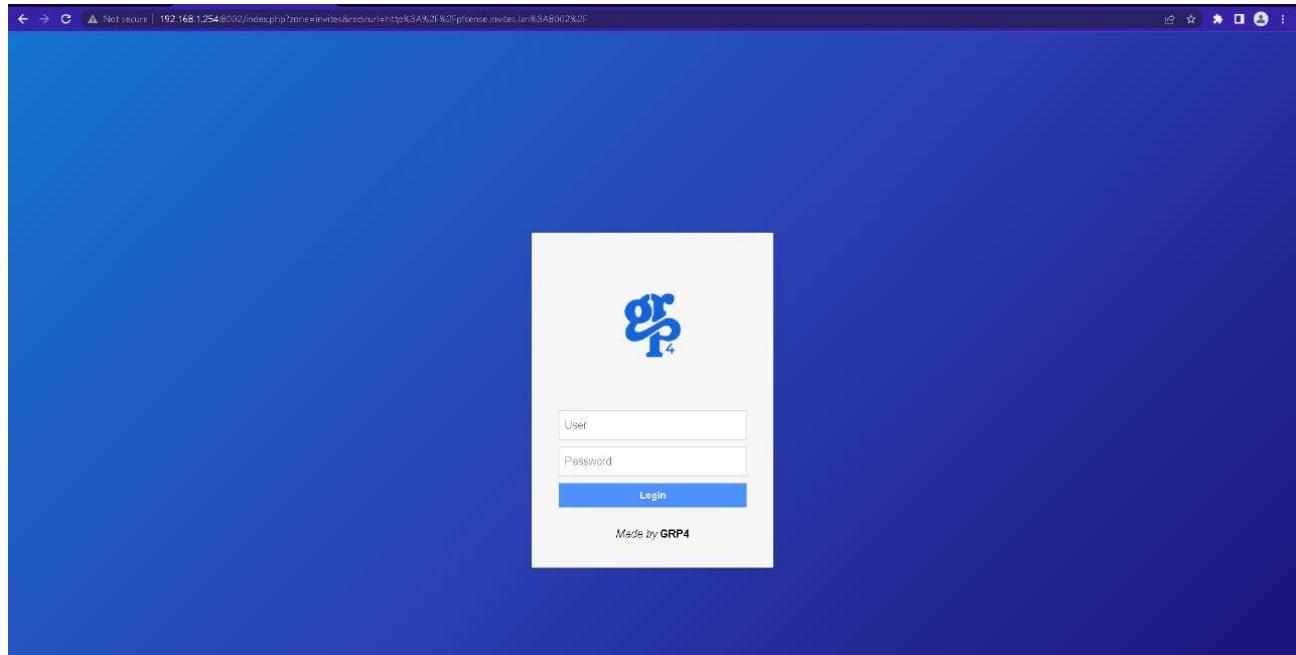


Figure 117 : Page d'authentification

- Après l'authentification :



Figure 118 : L'authentification a réussi

Chapitre VI : Firewall & DMZ

Aujourd’hui, pour assurer une sécurité maximale de l’information, il est important d’utiliser toutes les options de sécurité disponibles, comme **la DMZ**.

La DMZ est un segment de réseau qui héberge toutes les ressources accessibles et offre une sécurité partielle. Nous allons aborder l’objet de la DMZ, ses avantages et les différents types et niveaux de sécurité qu’elle propose.

I.DMZ :

1. Définition :

DMZ est l’abréviation de « zone démilitarisée » en anglais, qui est une zone tampon située entre deux réseaux informatiques différents, généralement entre un réseau privé (par exemple, le réseau interne d’une entreprise) et un réseau public (par exemple, l’Internet).

La DMZ est conçue pour fournir une couche de sécurité supplémentaire en empêchant les accès non autorisés à un réseau privé, tout en permettant une communication limitée avec le réseau public. Les serveurs hébergés dans la DMZ sont généralement accessibles depuis Internet, mais ils sont configurés pour limiter l’accès aux seuls services nécessaires pour répondre aux besoins de l’entreprise.

En d’autres termes, la DMZ est un sous-réseau intermédiaire qui offre une protection supplémentaire contre les attaques provenant de l’Internet, tout en permettant aux utilisateurs externes d'accéder aux ressources nécessaires de l’entreprise.

2. L’architecture DMZ :

L’architecture DMZ (zone démilitarisée) peut varier en fonction des besoins spécifiques d’une entreprise, mais elle suit généralement les principes de base suivants :

1. La DMZ est une zone tampon située entre un réseau privé (interne) et un réseau public (externe).
2. La DMZ contient des serveurs hébergés, tels que des serveurs web, des serveurs de messagerie électronique ou des serveurs de fichiers.
3. Les serveurs hébergés dans la DMZ sont configurés pour limiter l’accès uniquement aux services nécessaires, ce qui minimise les risques de compromission de la sécurité.
4. Les pare-feux sont utilisés pour contrôler le trafic réseau entrant et sortant de la DMZ, en filtrant le trafic non autorisé et en permettant uniquement le trafic nécessaire.
5. Les serveurs de la DMZ sont configurés pour limiter leur communication avec le réseau privé de l’entreprise, afin de minimiser les risques de propagation de logiciels malveillants.

En résumé, l'architecture DMZ est conçue pour offrir une couche de sécurité supplémentaire en empêchant les accès non autorisés à un réseau privé, tout en permettant une communication limitée avec le réseau public. Elle permet de protéger les serveurs hébergés dans la DMZ contre les attaques provenant de l'Internet, tout en permettant aux utilisateurs externes d'accéder aux ressources nécessaires de l'entreprise.

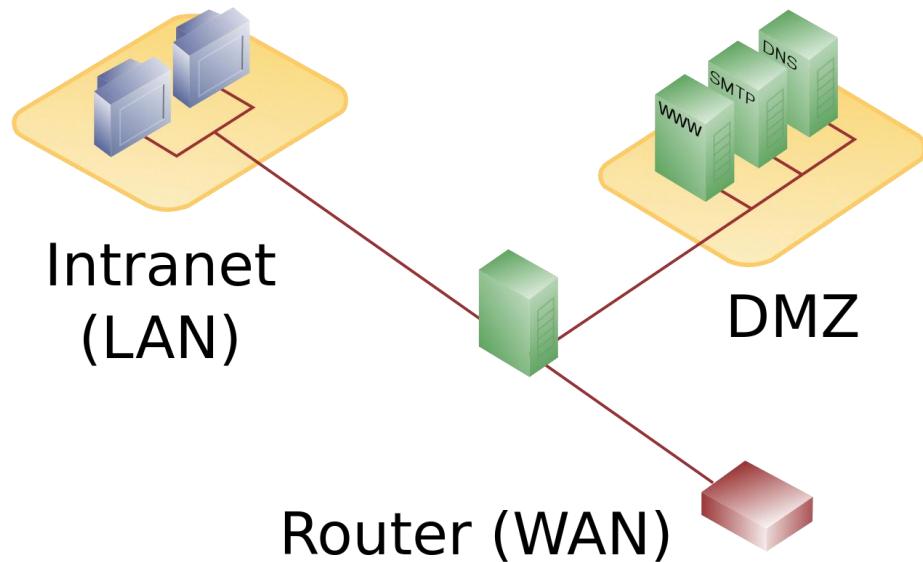


Figure 119 : Architecture DMZ

II.Firewall :

1. Définition :

Un pare-feu (en anglais, « firewall ») est un système de sécurité informatique qui sert à protéger un réseau informatique contre les attaques malveillantes provenant d'Internet ou d'autres réseaux. Le pare-feu permet de contrôler les connexions entrantes et sortantes en appliquant des règles de sécurité prédéfinies.

Le pare-feu peut être configuré pour bloquer les accès non autorisés à des ports spécifiques, pour filtrer le trafic en fonction des protocoles utilisés ou pour bloquer des adresses IP spécifiques. Il peut également être utilisé pour contrôler l'accès des utilisateurs à des ressources spécifiques sur le réseau.

Donc, nous pouvons dire qu'un pare-feu est un élément clé de la sécurité informatique, qui permet de protéger un réseau contre les intrusions et les attaques malveillantes.

2. Le but d'un pare-feu :

Le but principal d'un pare-feu est de protéger un réseau informatique en empêchant les accès non autorisés et les attaques malveillantes. Voici quelques-uns des objectifs clés d'un pare-feu :

- Bloquer les connexions entrantes non autorisées : Le pare-feu est configuré pour bloquer les connexions provenant de sources inconnues ou non autorisées. Cela aide à empêcher les attaques de type « intrusion » où un utilisateur malveillant tente de pénétrer dans un système ou un réseau.
- Contrôler l'accès aux ressources : Le pare-feu peut être utilisé pour contrôler l'accès des utilisateurs à certaines ressources sur le réseau, telles que les fichiers partagés, les imprimantes, etc. Cela peut aider à protéger les données sensibles contre les utilisateurs non autorisés.
- Filtre les paquets réseau : Le pare-feu peut filtrer le trafic réseau en fonction des protocoles utilisés, des adresses IP, des ports et d'autres critères. Cela peut aider à bloquer les attaques par déni de service, les attaques de type phishing et autres menaces en ligne.
- Gérer les politiques de sécurité : Les pare-feux peuvent être utilisés pour appliquer des politiques de sécurité cohérentes sur un réseau. Cela peut inclure des politiques telles que l'utilisation de mots de passe forts, la limitation de l'accès aux réseaux sociaux, etc.

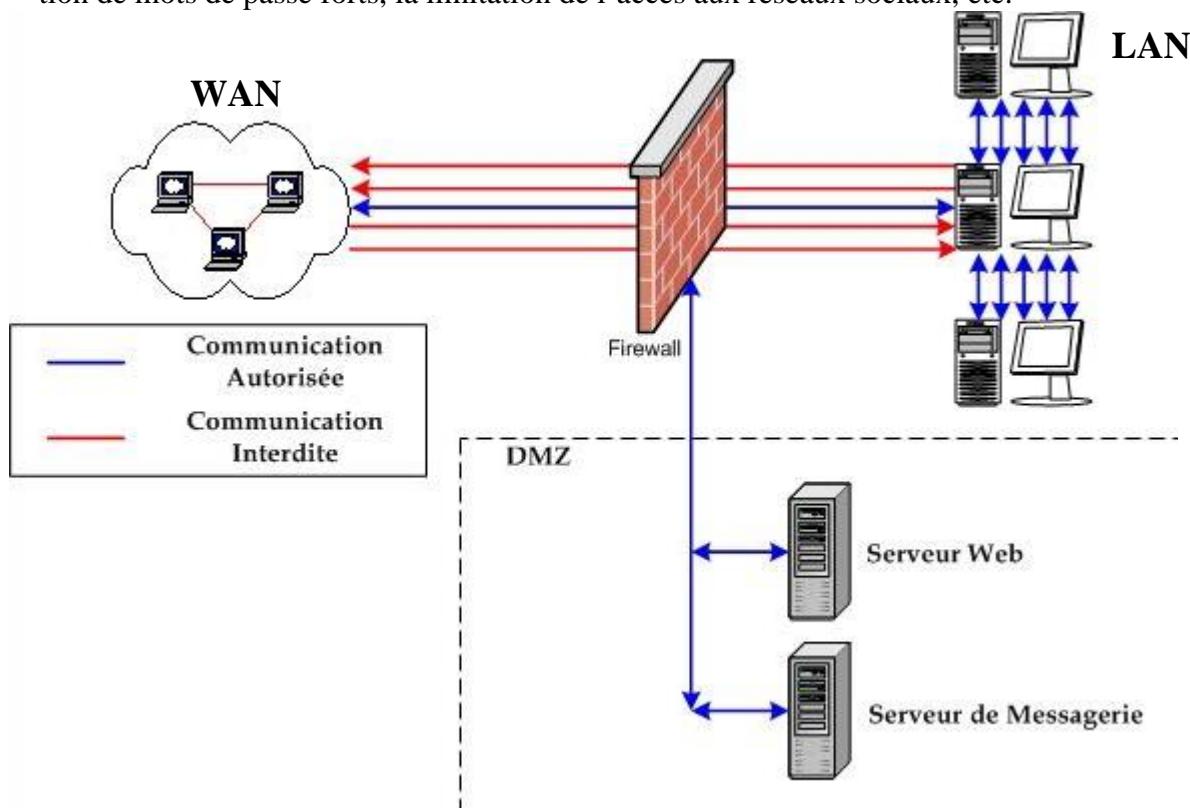


Figure 120 : Pare-feu

3. Filtrage de contenu :

Le filtrage de contenu par firewall est une méthode de sécurité informatique qui permet de contrôler le trafic réseau en fonction de règles de sécurité prédefinies pour protéger les réseaux contre les attaques malveillantes. Les firewalls peuvent être configurés pour bloquer l'accès à des sites web dangereux, limiter l'accès à certains types de fichiers ou de protocoles réseau, et empêcher les connexions non autorisées à des applications ou des services en ligne. Cependant, les firewalls ne sont pas une solution de sécurité complète en soi et doivent être utilisés en combinaison avec d'autres mesures de sécurité pour garantir une protection complète contre les menaces de sécurité.

4. Filtrage des paquets :

Le filtrage des paquets est une méthode de contrôle du trafic réseau qui permet de décider si un paquet de données doit être transmis ou non en fonction de critères prédefinis. Il est souvent utilisé pour protéger les réseaux contre les attaques malveillantes, bloquer l'accès à certains types de contenu ou limiter l'utilisation de la bande passante réseau. Cependant, l'utilisation du filtrage des paquets doit être équilibrée avec les préoccupations concernant la censure et la violation de la vie privée.

5. Types de filtrage :

a) Filtrage simple des paquets (Stateless) :

Le filtrage simple des paquets est une méthode de filtrage de contenu par firewall qui utilise l'adresse IP source et de destination pour décider si un paquet doit être transmis ou non. Cette méthode est simple mais moins sécurisée car elle ne prend pas en compte d'autres informations de l'en-tête du paquet. Elle est souvent utilisée pour bloquer l'accès à certains sites web ou limiter l'accès à des applications ou des services en ligne, mais doit être utilisée avec d'autres méthodes de filtrage pour garantir une sécurité adéquate du réseau.

i.Son principe :

Le principe du filtrage simple des paquets par firewall est de vérifier l'adresse IP source et de destination d'un paquet de données pour décider s'il doit être autorisé ou bloqué. Le firewall compare l'adresse IP source et de destination du paquet avec les règles de filtrage pour déterminer s'il doit être transmis ou non.

Les règles de filtrage peuvent être définies pour bloquer l'accès à certains sites web, limiter l'accès à des applications ou des services en ligne spécifiques, ou pour empêcher les connexions non autorisées à des ports spécifiques.

Cependant, le filtrage simple des paquets peut être contourné par des techniques telles que le spoofing d'adresse IP, qui implique de modifier l'adresse IP source d'un paquet pour masquer son origine réelle.

De plus, le filtrage simple des paquets ne prend pas en compte d'autres informations de l'en-tête du paquet, telles que le port source et de destination ou le protocole utilisé.

Par conséquent, il est important d'utiliser le filtrage simple des paquets en combinaison avec d'autres méthodes de filtrage, telles que le filtrage d'état ou le filtrage d'application, pour garantir une sécurité adéquate du réseau.

ii.Ses limites :

Le filtrage simple des paquets par firewall est une méthode de filtrage de contenu qui consiste à vérifier l'adresse IP source et de destination d'un paquet de données pour décider s'il doit être autorisé ou bloqué. Cependant, cette méthode présente des limites, notamment sa vulnérabilité aux attaques de spoofing d'adresse IP, son incapacité à prendre en compte les informations du paquet au-delà des adresses IP, son incapacité à fournir une protection contre les menaces de niveau applicatif, et son potentiel de causer des faux positifs. Par conséquent, le filtrage simple des paquets doit être utilisé en combinaison avec d'autres méthodes de filtrage pour garantir une sécurité adéquate du réseau.

b) Filtrage des paquets avec état (stateful) :

Le filtrage de paquet avec état est une méthode de filtrage de contenu par firewall qui utilise des informations sur l'état de la connexion pour déterminer si un paquet doit être autorisé ou bloqué. Contrairement au filtrage simple des paquets, qui ne prend en compte que les adresses IP source et de destination, le filtrage de paquet avec état est plus sécurisé car il peut bloquer les tentatives d'attaques en cours de connexion. Cependant, il peut également être vulnérable aux attaques par injection de code et nécessite une surveillance régulière pour détecter les éventuelles anomalies.

i.Son principe :

Le filtrage de paquet avec état est une méthode de filtrage de contenu par firewall qui se base sur l'état de la connexion pour déterminer si un paquet doit être autorisé ou bloqué. Pour chaque paquet entrant, le firewall examine l'en-tête de la connexion pour vérifier si elle correspond à une connexion active. L'en-tête de la connexion contient des informations telles que l'adresse IP source et de destination, le numéro de séquence, le numéro d'identification, le numéro de port et le type de protocole.

Le firewall examine ces informations pour déterminer si le paquet appartient à une connexion active en cours. Si c'est le cas, le paquet est autorisé à passer. Sinon, le paquet est bloqué car il ne correspond pas à une connexion établie. Cette méthode permet de bloquer les tentatives d'attaques en cours de connexion, telles que les attaques par déni de service distribué (DDoS) ou les tentatives de connexion frauduleuses.

Le filtrage de paquet avec état permet également de configurer des règles de filtrage de contenu pour des connexions spécifiques en fonction de leur état. Par exemple, il est possible d'autoriser le trafic entrant sur des ports spécifiques pour les connexions établies, tout en bloquant le trafic entrant sur ces mêmes ports pour les connexions non établies.

Le firewall enregistre également les paquets autorisés dans une table de suivi de connexion pour permettre une gestion optimale des flux de données. Cette table de suivi de connexion contient des informations sur les connexions actives, telles que les adresses IP source et de destination, les ports, les numéros de séquence et les numéros d'identification. Cette table est utilisée pour vérifier l'état de la connexion lors de la réception des paquets suivants.

Cependant, le filtrage de paquet avec état peut également être vulnérable aux attaques par injection de code, telles que les attaques de type « man in the middle », qui peuvent tromper le firewall en manipulant l'état de la connexion. Pour éviter ces problèmes, il est important de maintenir le firewall à jour avec les dernières mises à jour de sécurité et de surveiller régulièrement son fonctionnement pour détecter les éventuelles anomalies.

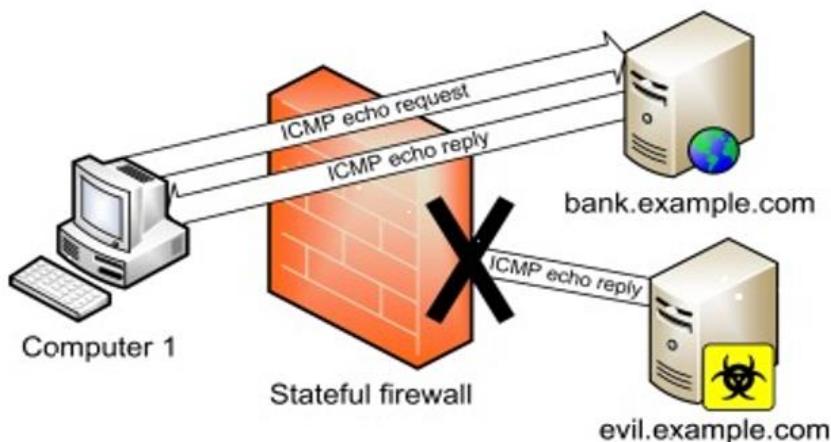


Figure 121 : Filtrage des paquets avec états

ii.Ses limites :

Le filtrage des paquets avec état est une méthode de filtrage de contenu utilisée par les firewalls pour améliorer la sécurité des réseaux. Cependant, cette technique présente également des limites importantes. Tout d'abord, le filtrage des paquets avec état peut être coûteux en termes de matériel et de logiciels nécessaires pour suivre l'état des connexions. De plus, les attaquants peuvent exploiter les vulnérabilités du filtrage des paquets avec état pour lancer des attaques de type « spoofing » ou « man in the middle ». En outre, le filtrage des paquets avec état peut avoir des difficultés à reconnaître certains types de protocoles, en particulier les protocoles personnalisés ou ceux qui n'ont pas encore

été identifiés. Par conséquent, il peut être plus difficile à mettre en place pour les connexions asymétriques, telles que celles qui utilisent des protocoles de tunnelling. Enfin, le filtrage des paquets avec état peut avoir des limites dans l'identification des applications spécifiques qui sont utilisées dans les connexions, ce qui peut entraîner des limitations dans les politiques de sécurité qui peuvent être mises en place. En résumé, bien que le filtrage des paquets avec état soit une méthode de sécurité avancée, il est important de comprendre ses limites et de mettre en place des mesures de sécurité complémentaires pour protéger les réseaux contre les attaques potentielles.

c) Firewall applicatif :

Un firewall applicatif est un type de solution de sécurité qui protège les applications en inspectant le trafic réseau au niveau de la couche applicative. Il peut bloquer les requêtes malveillantes et détecter les attaques « zero-day ». Cependant, il peut être complexe à mettre en place et avoir un impact sur les performances des applications.

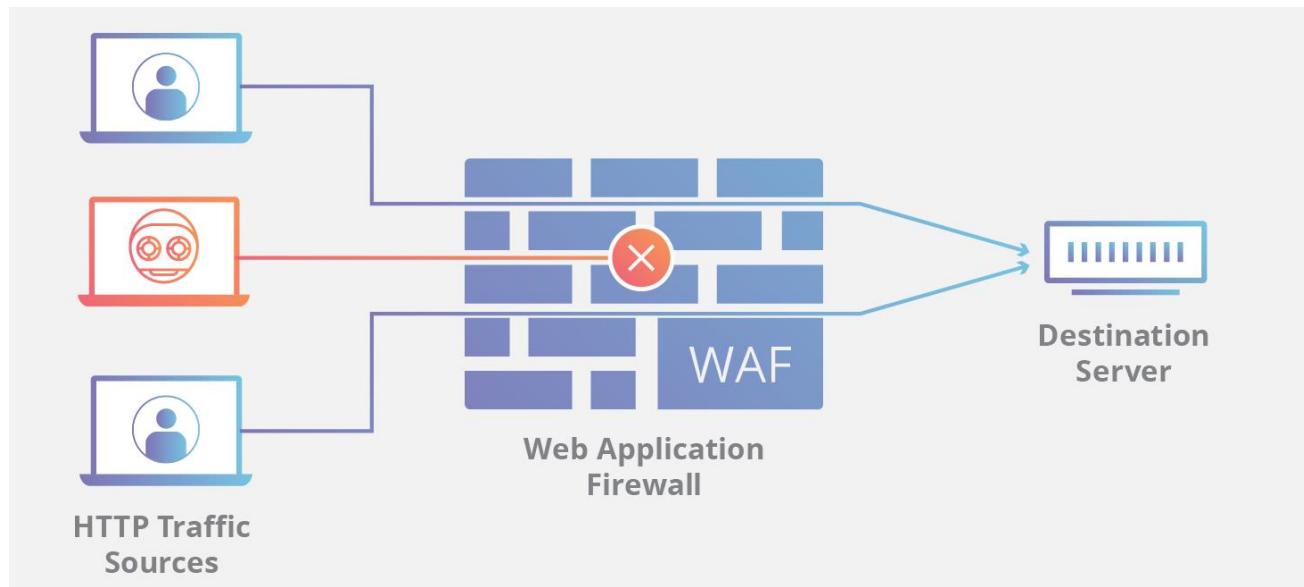


Figure 122 : Firewall applicatif

i.Son principe :

Le firewall applicatif opère au niveau de la couche applicative du modèle OSI, ce qui lui permet d'inspecter le contenu des requêtes et des réponses des applications pour détecter les tentatives d'attaques. Il utilise des règles de sécurité spécifiques pour chaque application, basées sur les caractéristiques des protocoles utilisés, les types de données transmises et les adresses IP sources et destinations.

Le firewall applicatif est capable de bloquer les requêtes malveillantes qui tentent d'exploiter des vulnérabilités connues dans les applications. Par exemple, il peut bloquer les requêtes SQL injectées dans une application web pour empêcher une attaque de type injection SQL. Il peut également détecter

les attaques de type « zero-day » en utilisant l’analyse comportementale pour identifier les comportements suspects des requêtes et des réponses.

En plus de la protection contre les attaques, le firewall applicatif peut fournir des fonctionnalités de chiffrement pour protéger les données sensibles en transit. Il peut également offrir des fonctionnalités de contrôle d'accès pour limiter l'accès aux ressources applicatives en fonction des droits d'accès des utilisateurs.

Cependant, la mise en place d'un firewall applicatif peut être complexe car elle nécessite une bonne connaissance des applications et des protocoles utilisés. De plus, l'inspection approfondie du trafic réseau peut avoir un impact sur les performances des applications. Il est donc important de bien planifier et de tester la mise en place d'un firewall applicatif pour minimiser les risques d'indisponibilité et de dégradation des performances des applications.

ii.Ses limites :

Les firewalls applicatifs sont une méthode de sécurité avancée pour surveiller le trafic des applications et protéger les réseaux contre les attaques potentielles. Cependant, ils ont également des limites importantes qui doivent être prises en compte. Les coûts élevés, la complexité de configuration et les difficultés de reconnaissance des applications peuvent constituer des défis importants. De plus, les firewalls applicatifs peuvent être vulnérables aux attaques avancées et avoir un impact sur les performances des applications. Par conséquent, il est important de comprendre ces limites et de mettre en place des mesures de sécurité complémentaires pour renforcer la sécurité des réseaux.

6. Les types de pares-feux :

Il existe plusieurs types de pare-feu, chacun ayant ses avantages et ses inconvénients. Voici quelques exemples :

a) Firewall bridge :

Un firewall bridge, également appelé pare-feu transparent, est un dispositif de sécurité réseau qui fonctionne au niveau de la couche de liaison de données (couche 2) du modèle OSI.

Un pare-feu bridge est conçu pour filtrer le trafic réseau en fonction des adresses MAC et d'autres informations contenues dans la couche de liaison de données du protocole réseau. Il fonctionne de manière transparente, ce qui signifie qu'il ne modifie ni n'altère le trafic réseau qui le traverse.

Contrairement à un pare-feu classique qui fonctionne à la couche réseau (couche 3) du modèle OSI, un pare-feu bridge peut filtrer le trafic sans avoir à modifier les adresses IP de la source ou de la destination. Cela peut être utile dans certaines situations, comme lorsque vous avez besoin de filtrer le trafic entre deux segments de réseau sans changer les adresses IP de ces segments.

b) Firewall logiciel :

Un firewall logiciel, également appelé pare-feu logiciel, est un programme informatique qui est utilisé pour protéger un ordinateur ou un réseau contre les menaces provenant d'Internet ou d'autres réseaux.

Un firewall logiciel analyse le trafic réseau entrant et sortant de l'ordinateur ou du réseau, et il filtre le trafic en fonction des règles de sécurité spécifiées par l'utilisateur. Les règles peuvent inclure des restrictions sur les types de connexions entrantes autorisées, les adresses IP autorisées à se connecter à l'ordinateur ou au réseau, et les types de protocoles réseau autorisés.

Le firewall logiciel est installé sur l'ordinateur ou le serveur, et peut être configuré pour permettre ou bloquer l'accès à des ports spécifiques ou à des services réseau. Il peut également être configuré pour envoyer des alertes lorsqu'une activité suspecte est détectée.

c) Firewall matériel :

Le firewall matériel est un équipement de sécurité réseau essentiel pour protéger les réseaux d'entreprise, les centres de données, les succursales et les filiales contre les attaques de cybercriminels. Il offre une protection robuste et fiable contre les menaces potentielles et aide les entreprises à assurer la sécurité de leurs données et de leur infrastructure réseau.

Il est important de noter que ces types de pare-feu peuvent se chevaucher et être utilisés conjointement pour fournir une protection plus complète.

Le firewall matériel est un dispositif dédié qui dispose de son propre processeur, de sa propre mémoire et de son propre système d'exploitation. Il offre une protection plus robuste que les firewalls logiciels car il est conçu pour gérer des volumes de trafic réseau plus importants, et est plus difficile à compromettre car il est distinct de l'ordinateur ou du serveur qu'il protège.

Le firewall matériel utilise plusieurs techniques pour protéger le réseau, telles que l'inspection des paquets de données en profondeur, le filtrage basé sur les adresses IP, les ports et les protocoles, et la mise en place de VPN (Virtual Private Network). Il peut également être configuré pour offrir des fonctions de détection et de prévention d'intrusion, ainsi que des systèmes de protection contre les virus et les logiciels malveillants.

d) FortiGate 100A :

FortiGate 100A est un type pare-feu de réseau d'entreprise de la société Fortinet. Il a été introduit en 2005 et depuis lors, il a été remplacé par des modèles plus récents et plus avancés. Cependant, le FortiGate 100A était un modèle populaire pour les petites et moyennes entreprises, offrant des fonctionnalités de sécurité avancées à un prix abordable.

Le FortiGate 100A est conçu pour offrir une protection de réseau de niveau entreprise contre les menaces en ligne telles que les virus, les attaques par déni de service, les tentatives d'intrusion et les logiciels malveillants. Il dispose de fonctionnalités de pare-feu de réseau, de VPN, d'IPS, d'antivirus, de filtrage web et d'autres fonctionnalités de sécurité.

Le FortiGate 100A est équipé de deux interfaces WAN et huit interfaces LAN, ce qui permet aux entreprises de connecter plusieurs réseaux et de gérer efficacement la circulation du trafic. Il dispose également de fonctionnalités de gestion centralisée pour faciliter la configuration, la surveillance et la maintenance du système.

Le FortiGate 100A est un produit ancien et il est peu probable qu'il soit utilisé dans les nouvelles installations de sécurité réseau. Cependant, il peut encore être utilisé dans des environnements existants pour fournir une protection de base contre les menaces en ligne.

III. Mise en place d'une DMZ avec FortiGate 100A :

Afin de mettre en place un réseau DMZ, nous avons opté pour l'utilisation d'un pare-feu matériel qui offre deux interfaces spécifiquement dédiées à l'implémentation d'une DMZ. Nous avons choisi le FortiGate 100A pour cette tâche.

Pour commencer la mise en place de la DMZ avec le FortiGate 100A, la première étape consiste à accéder à l'interface de configuration, comme illustré dans l'image suivante :

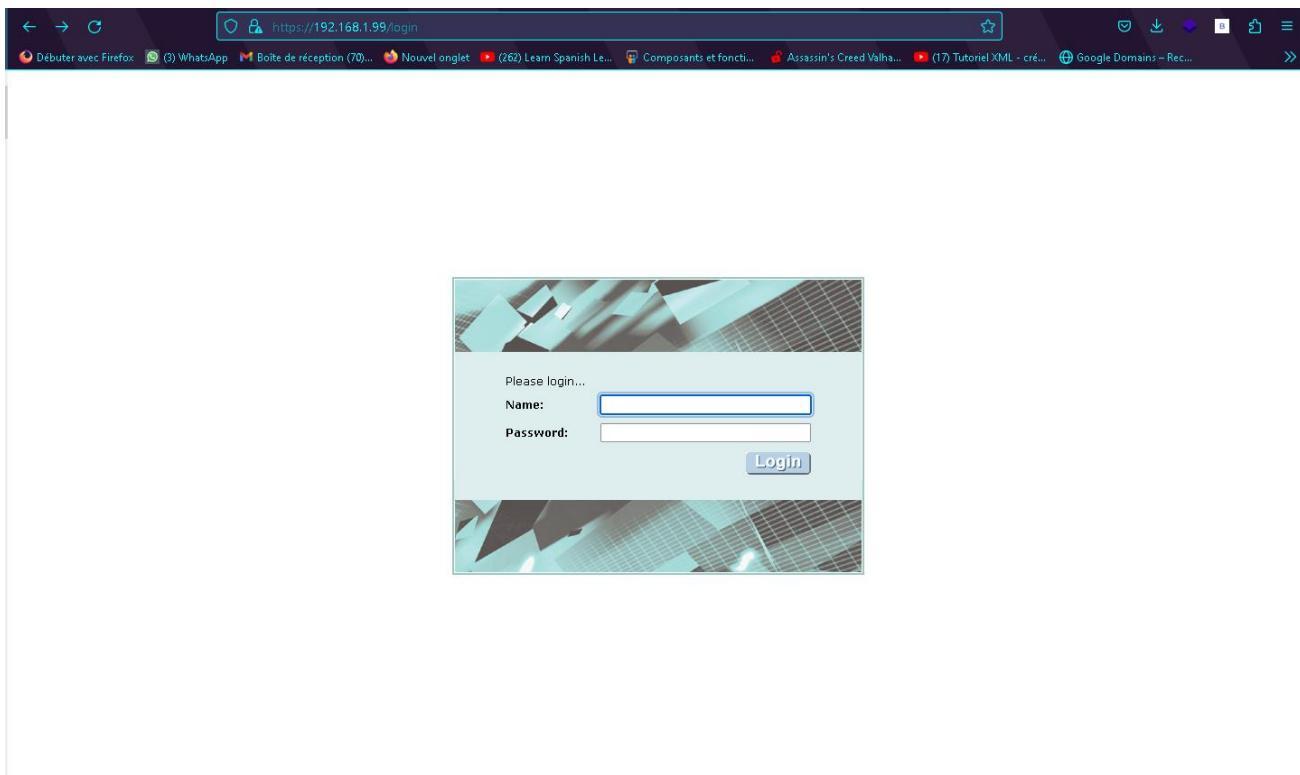


Figure 123 : L'interface de configuration DMZ

Une fois que vous avez effectué la connexion, une nouvelle fenêtre s'ouvrira :

System Information	
Serial Number	FG100A3907509949
Uptime	0 day(s) 3 hour(s) 23 min(s)
System Time	Wed Mar 29 13:18:19 2023 [Change]
HA Status	Standalone [Configure]
Host Name	FG100A3907509949 [change]
Firmware Version	Fortigate-100A 3.00-b0750(MR7 Patch 7) [Update]
Operation Mode	NAT [Change]
Virtual Domain	Disabled [Enable]
Current Administrators	2 [Details]

FortGuard Subscriptions	
Antivirus	Unreachable [Configure]
AV Definitions	26-02-2023 (Updated 2015-12-18) [Update]
Intrusion Protection	Unreachable [Configure]
IPS Definitions	2.0096 (Updated 2011-05-12) [Update]
Web Filtering	Unreachable [Configure]
AntiSpam	Unreachable [Configure]
Analysis & Management Service	Unreachable
Services Account ID	[Change]

Virtual Domain	
VDOMs Allowed	10

CLI Console (not connected)	
Click here to connect...	

System Resources	
------------------	--

Figure 124 : Page d'accueil du pare-feu Fortigate 100A

Dans cette fenêtre, vous pouvez accéder au tableau de bord (Dashboard) qui affiche plusieurs informations relatives à l'état de votre machine. Pour accéder aux paramètres du réseau, vous pouvez cliquer sur « Network » puis sur « Interface ».

Puis, vous cliquez sur « Create New » pour créer une nouvelle interface, cela ouvrira la fenêtre ci-dessous :

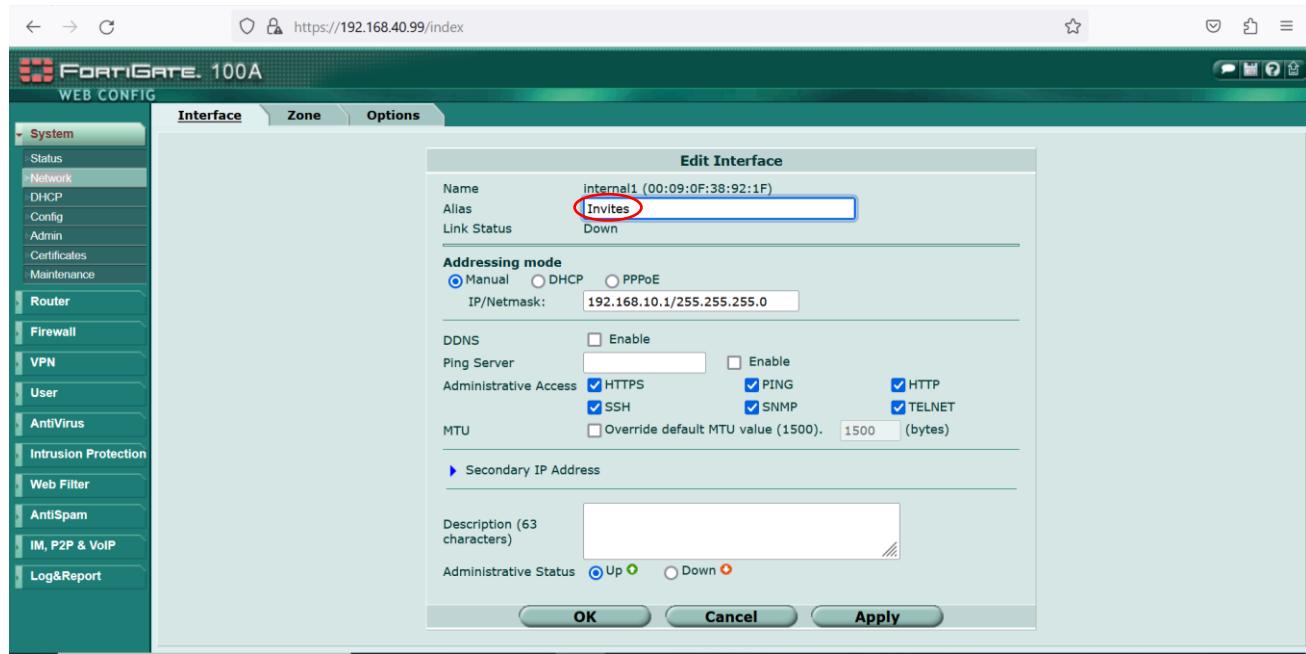


Figure 125 : La configuration de l'interface "Vlan invites"

- Une fois on clique sur « Create New », nous allons procéder à la configuration de l'interface « Vlan invites ».
- Ensuite, on va affecter l'adresse IP : 192.168.10.1 et définir le masque : 255.255.255.0.
- Par la suite, on va activer le statut administratif « Administrative Access » en sélectionnant les services souhaités : HTTPS / PING / http / SSH / SNMP / TELNET.
- Enfin, il suffit de cliquer sur « Apply » suivi de « Ok » pour valider les changements.

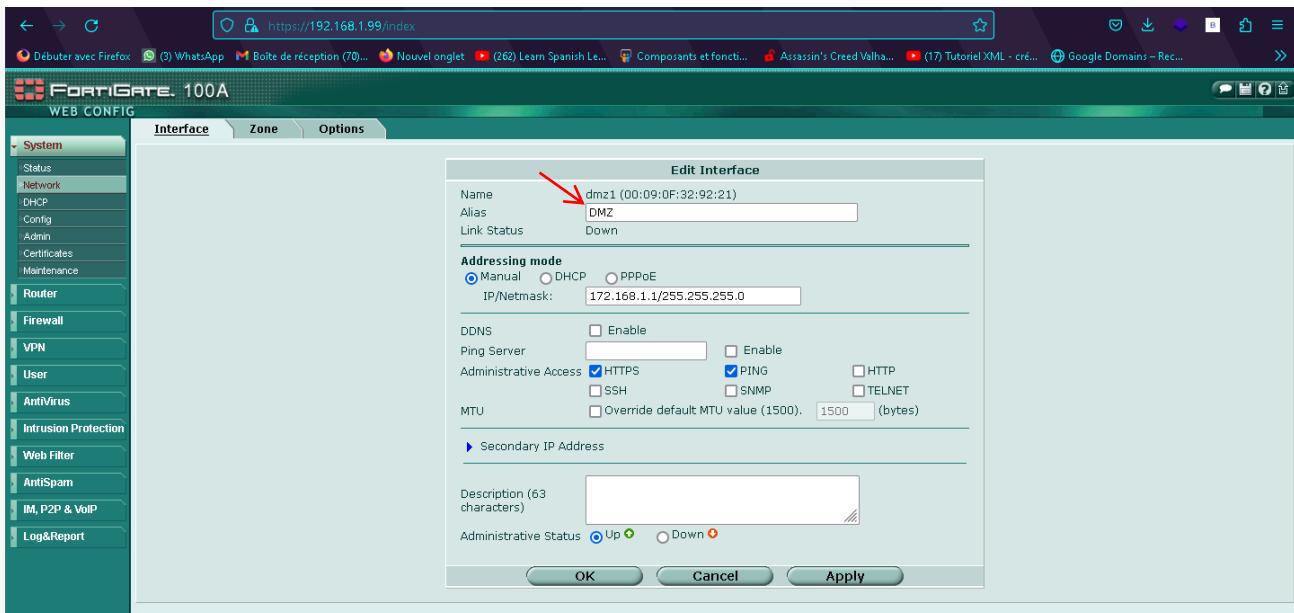


Figure 126 : La configuration de l'interface « DMZ »

- Nous allons de nouveau accéder à la fenêtre Interfaces pour procéder à la configuration de l'interface « DMZ ».
- Ensuite, on va affecter l'adresse IP : 172.168.1.1 et définir le masque : 255.255.255.0.
- Par la suite, on va activer le statut administratif « Administrative Access » en sélectionnant les services souhaités : HTTPS / PING.
- Enfin, il suffit de cliquer sur « Apply » suivi de « Ok » pour valider les changements

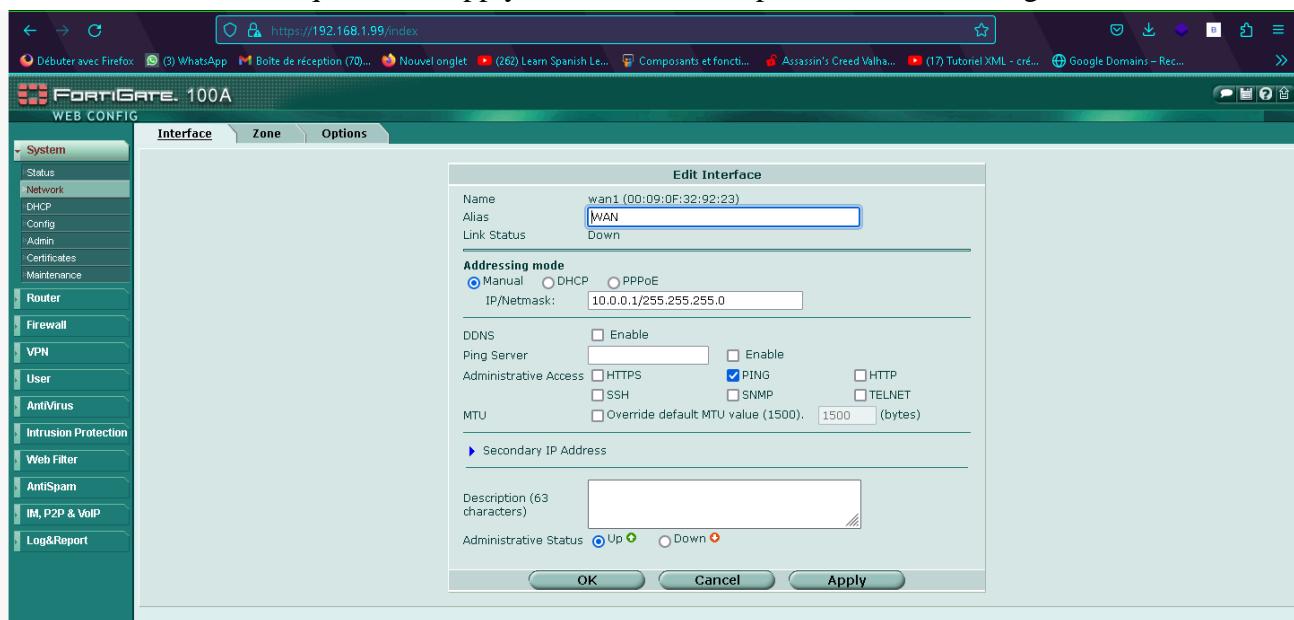


Figure 127 : Validation de la configuration

- Nous allons de nouveau accéder à la fenêtre Interfaces pour procéder à la configuration de l'interface « WAN ».
- Ensuite, on va affecter l'adresse IP : 10.0.0.1 et définir le masque : 255.255.255.0.
- Par la suite, on va activer le statut administratif « Administrative Access » en sélectionnant les services souhaités : PING.
- Enfin, il suffit de cliquer sur « Apply » suivi de « Ok » pour valider les changements.

Sur cette page, nous avons une vue d'ensemble de toutes les interfaces configurées.

The screenshot shows the FortiGate 100A Web Config interface. The left sidebar contains a navigation menu with options like System, Network, Router, Firewall, and others. The main area has tabs for Interface, Zone, and Options, with 'Interface' selected. Below these tabs are buttons for 'Create New' and 'Switch Mode'. A table lists the configured interfaces:

Name	IP/Netmask	Access	Administrative Status	Link Status	[Column Settings]
dmz1 (DMZ)	172.120.1.1 / 255.255.255.0	HTTP,PING,SNMP PING	○	○	✓
dmz2	0.0.0 / 0.0.0	HTTP,PING,SNMP	○	○	✓
internal	192.168.40.99 / 255.255.255.0	HTTP,PING,SNMP	○	○	✓
vlan employees	192.168.20.1 / 255.255.255.0	HTTP,HTTPS,PING,PING,SSH,TELNET,SNMP	○	○	✓
Vlan admin	192.168.30.1 / 255.255.255.0	HTTP,HTTPS,PING,PING,SSH,TELNET,SNMP	○	○	✓
Vlan invites	192.168.10.1 / 255.255.255.0	HTTP,HTTPS,PING,PING,SSH,TELNET,SNMP	○	○	✓
wan1 (WAN)	10.0.0.1 / 255.255.255.0	PING,SNMP	○	○	✓
wan2	0.0.0 / 0.0.0	PING	○	○	✓

Figure 128 : Les interfaces configurées

Il est temps de configurer les politiques d'accès à la DMZ, au LAN ou au WAN. Pour cela, nous devons accéder à l'option « Policy » et sélectionner « Create New ». Ensuite, nous pouvons ajouter les politiques d'accès selon nos besoins.

- Puis, on règle le routage statique et dynamique du Firewall.

WEB CONFIG

Static Route **Policy Route**

Create New

IP/Mask	Gateway	Device	Distance	
192.168.30.0/255.255.255.0	192.168.30.1	internal3	10	
172.120.1.0/255.255.255.0	172.120.1.1	dmz1	10	
192.168.20.0/255.255.255.0	192.168.20.1	internal2	10	
192.168.10.0/255.255.255.0	192.168.10.1	internal1	10	
10.10.10.0/255.255.255.0	10.10.10.99	wan1	10	
192.168.40.0/255.255.255.0	192.168.40.1	internal4	10	
10.10.11.0/255.255.255.0	10.10.10.254	wan1	10	

Figure 130 : Le routage statique et dynamique du Firewall

WEB CONFIG

RIP **OSPF** **BGP** **Multicast**

RIP Version 1 2
Advanced Options(Defaults, Timers, Route Redistribution)

Networks **IP/Netmask:** **Add**

IP/Netmask	
192.168.30.0/255.255.255.0	
192.168.20.0/255.255.255.0	
192.168.10.0/255.255.255.0	
192.168.40.0/255.255.255.0	
172.120.1.0/255.255.255.0	
10.10.11.0/255.255.255.0	
10.10.10.0/255.255.255.0	

Interfaces **Create New**

Interface	Send	Receive	Version	Authentication	Passive
dmz1	Both	Both	None		
internal1	Both	Both	None		
internal2	Both	Both	None		
internal3	Both	Both	None		
internal4	Both	Both	None		
wan1	Both	Both	None		

Figure 129 : le routage du Firewall

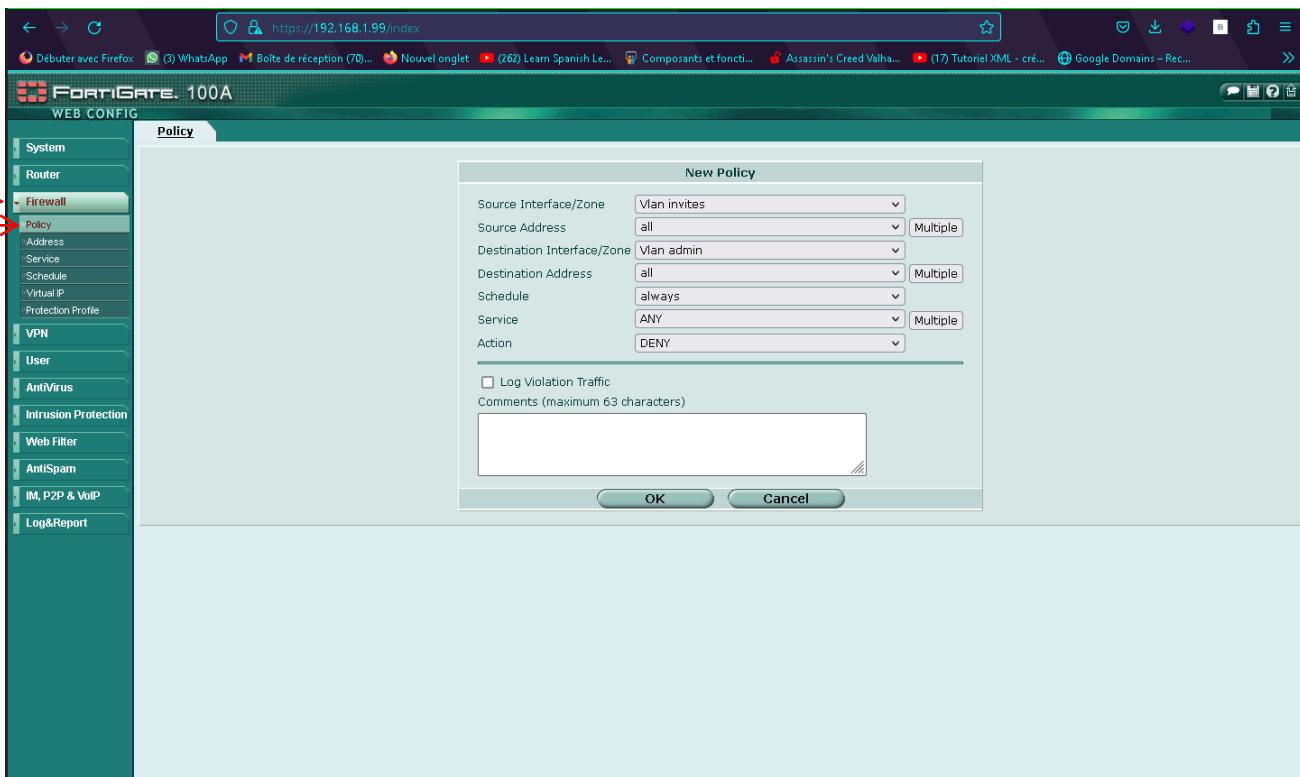


Figure 131 : Policy des VLAN des invités et les administrateurs

- Une règle de pare-feu a été créée pour interdire toute communication réseau entre les invités et les administrateurs.

Policy								
Create New								
Status	ID	Source	Destination	Schedule	Service	Profile	Action	[Column Settings]
✓	4	● all	● all	always	● ANY		ACCEPT	
✓	5	● all	● all	always	● ANY		ACCEPT	
✓	2	● all	● all	always	● ANY		DENY	
✓	7	● all	● all	always	● HTTP ● HTTPS ● PING		ACCEPT	
✓	1	● all	● all	always	● ANY		ACCEPT	
✓	3	● all	● all	always	● ANY		DENY	
✓	6	● all	● all	always	● ANY		DENY	

Figure 132 : Les politiques d'accès configurées

- Dans la fenêtre mentionnée précédemment, nous pouvons voir l'ensemble des politiques d'accès configurées.
- Une fois cette étape terminée, la configuration et la mise en place de notre DMZ sont finalisées.

Un serveur Web est un logiciel qui fonctionne en respectant le protocole de communication client-serveur http (HyperText Transfer Protocol), développé pour le World Wide Web. L'ordinateur sur lequel il s'exécute est également appelé serveur Web. Le terme « serveur Web » peut également faire référence au logiciel serveur http lui-même, car le protocole http est principalement utilisé pour servir des pages Web. Bien que d'autres protocoles soient fréquemment utilisés pour d'autres ressources du Web telles que les fichiers à télécharger ou les flux audios et vidéo.

IV.Les serveurs implémentés dans la DMZ :

Un serveur Web est un logiciel qui fonctionne en respectant le protocole de communication client-serveur http (HyperText Transfer Protocol), développé pour le World Wide Web. L'ordinateur sur lequel il s'exécute est également appelé serveur Web. Le terme « serveur Web » peut également faire référence au logiciel serveur http lui-même, car le protocole http est principalement utilisé pour servir des pages Web. Bien que d'autres protocoles soient fréquemment utilisés pour d'autres ressources du Web telles que les fichiers à télécharger ou les flux audios et vidéo.

1. Apache http Server :

a) Définition :

Le serveur http Apache, également connu sous le nom d'Apache http Server, est un logiciel serveur Web open source développé par la Apache Software Foundation. Il est l'un des serveurs Web les plus populaires et les plus utilisés sur Internet, offrant une grande flexibilité et de nombreuses fonctionnalités avancées telles que la prise en charge de SSL/TLS, la compression de données, la gestion de contenu dynamique, la mise en cache, la réécriture d'URL et bien plus encore. Le serveur http Apache peut être utilisé sur divers systèmes d'exploitation, y compris Linux, Unix, Windows, MacOs, etc.



Figure 133 : Logo de Apache

b) Fonctionnalités :

Le serveur http Apache est doté d'un large éventail de fonctionnalités, notamment :

- Prise en charge de SSL/TLS : permet de sécuriser les connexions avec des certificats SSL/TLS.
- Compression de données : permet de compresser les fichiers envoyés au client, réduisant ainsi la taille des données transférées et améliorant les performances.
- Gestion de contenu dynamique : permet de générer des pages Web dynamiques à partir de scripts et de bases de données.
- Mise en cache : permet de stocker en cache les pages Web pour améliorer les performances et réduire la charge sur le serveur.
- Réécriture d'URL : permet de modifier les URL des pages Web pour des raisons de sécurité, de convivialité ou d'optimisation pour les moteurs de recherche.
- Contrôle d'accès : permet de limiter l'accès aux ressources du serveur en fonction de l'adresse IP, de l'utilisateur, du mot de passe, etc.
- Journalisation : permet de suivre les activités du serveur et de collecter des données pour l'analyse.
- Support multiplateforme : le serveur http Apache peut être utilisé sur divers systèmes d'exploitation, y compris Linux, Unix, Windows, macOS, etc.
- Extensibilité : Apache dispose d'un large éventail de modules tiers disponibles pour étendre ses fonctionnalités, tels que les modules de sécurité, les modules de gestion de contenu, etc.

c) Modes de fonctionnement :

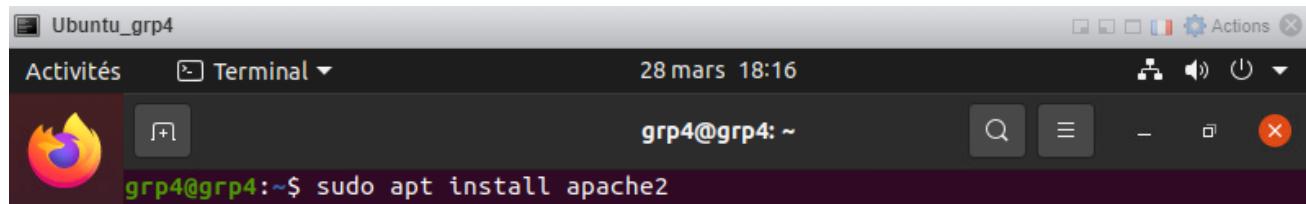
Le serveur http Apache propose deux modes de fonctionnement :

- **Mode préfabriqué (prefork)** : ce mode de fonctionnement crée des processus distincts pour chaque demande de connexion entrante. Chaque processus est isolé des autres, ce qui garantit la stabilité et la sécurité du serveur. Cependant, ce mode est relativement gourmand en ressources, car il nécessite un grand nombre de processus pour gérer de nombreuses connexions simultanées.
- **Mode multithread (worker)** : ce mode de fonctionnement utilise un seul processus principal, qui crée des threads pour chaque demande de connexion entrante. Chaque thread gère une seule connexion, ce qui permet de gérer un grand nombre de connexions simultanées avec moins de ressources système que le mode préfabriqué. Cependant, ce mode de fonctionnement peut être

moins stable que le mode préfabriqué, car les threads partagent les mêmes ressources système, ce qui peut causer des conflits et des problèmes de sécurité en cas d'erreur dans l'un des threads.

d) Configuration de Apache2 sur Ubuntu :

- Premièrement, on va exécuter la commande « **sudo apt-get update** » pour faire une mise à jour des paquets.
- Ensuite, il suffit de lancer la commande mentionnée ci-dessus pour installer le paquet « **apache2** »

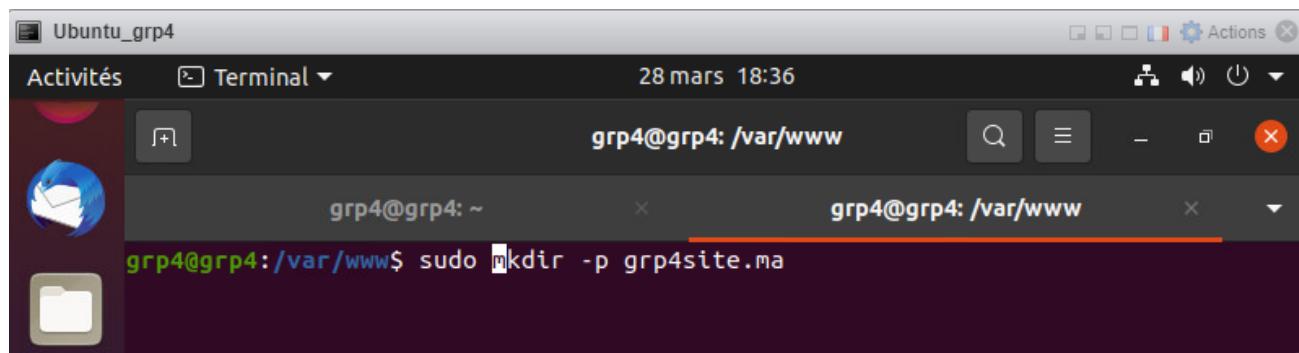


```
Ubuntu_grp4
Activités Terminal 28 mars 18:16
grp4@grp4:~$ sudo apt install apache2
```

Figure 134 : L'installation du "apache2"

Puis, on va créer un répertoire nommé « grp4site.ma » dans le chemin **/var/www** pour le site :

grp4.ari2.pfe.est.sma



```
Ubuntu_grp4
Activités Terminal 28 mars 18:36
grp4@grp4: /var/www
grp4@grp4: ~
grp4@grp4: /var/www$ sudo mkdir -p grp4site.ma
```

Figure 135 : La création du répertoire « grp4site.ma »

- Une fois que nous avons accédé au répertoire **/etc/apache2/sites-available**, nous constatons en exécutant la commande « ls » que seuls les fichiers de configuration sont présents. Ensuite, nous allons copier le contenu du fichier « 000-default.conf » vers notre fichier « grp4site.conf ».

```
grp4@grp4:~$ cd /etc/apache2/sites-available/
grp4@grp4:/etc/apache2/sites-available$ ls
000-default.conf  default-ssl.conf
grp4@grp4:/etc/apache2/sites-available$ sudo cp 000-default.conf grp4site.conf
[sudo] Mot de passe de grp4 :
grp4@grp4:/etc/apache2/sites-available$ sudo nano grp4site.conf
```

Figure 136 : La copie de dossier de configuration

- Ensuite, il est nécessaire de créer un vhost et de modifier la configuration par défaut du fichier /etc/apache2/sites-available/000-default.conf. Nous avons modifié le documentroot avec le répertoire que nous avons déjà créé et le nom de domaine grp4.ari2.pfe.est.s.ma.

The screenshot shows a terminal window titled "grp4@grp4: /etc/apache2/sites-available". The window displays the Apache configuration file "grp4site.conf". A red box highlights the following configuration block:

```

<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) the
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/grp4site.ma
    ServerName grp4.ari2.pfe.estrs.ma
    ServerAlias grp4.pfe
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

```

Below the terminal window, a menu bar contains keyboard shortcuts for various actions: Aide (Help), Quitter (Exit), Écrire (Write), Lire fich. (Read file), Chercher (Search), Remplacer (Replace), Couper (Cut), Coller (Copy), Justifier (Justify), and Orthograp. (Orthography).

Figure 137 : La création d'un « Vhost »

- Une fois que le fichier « index.html » a été créé, en exécutant la commande « ls », nous remarquons la présence du fichier.

The screenshot shows a terminal window titled "grp4@grp4: /var/www/grp4site.ma\$ ls". The command "ls" is run, and the output shows three files: "image.png", "index.html", and "logo.png".

```

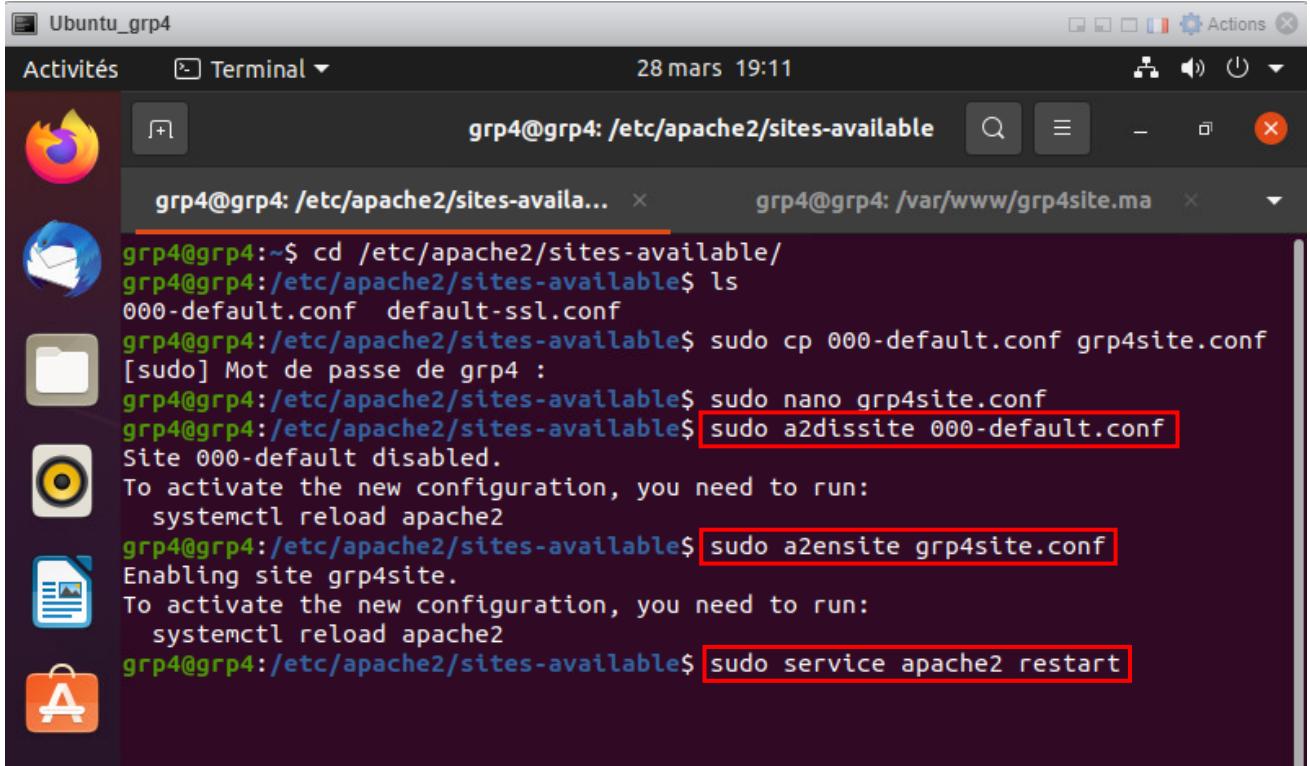
image.png  index.html  logo.png

```

Figure 138 : Le fichier "index.html"

- Nous avons désactivé le site par défaut et activé notre site.

- Ensuite, nous avons redémarré le service Web (apache2).



```
Ubuntu_grp4
Activités Terminal 28 mars 19:11
grp4@grp4: /etc/apache2/sites-available ...
grp4@grp4: /etc/apache2/sites-available...
grp4@grp4:~$ cd /etc/apache2/sites-available/
grp4@grp4:/etc/apache2/sites-available$ ls
000-default.conf default-ssl.conf
grp4@grp4:/etc/apache2/sites-available$ sudo cp 000-default.conf grp4site.conf
[sudo] Mot de passe de grp4 :
grp4@grp4:/etc/apache2/sites-available$ sudo nano grp4site.conf
grp4@grp4:/etc/apache2/sites-available$ sudo a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
    systemctl reload apache2
grp4@grp4:/etc/apache2/sites-available$ sudo a2ensite grp4site.conf
Enabling site grp4site.
To activate the new configuration, you need to run:
    systemctl reload apache2
grp4@grp4:/etc/apache2/sites-available$ sudo service apache2 restart
```

Figure 139 : Redémarrage du service Web

Voici la page d'accueil de notre site web :

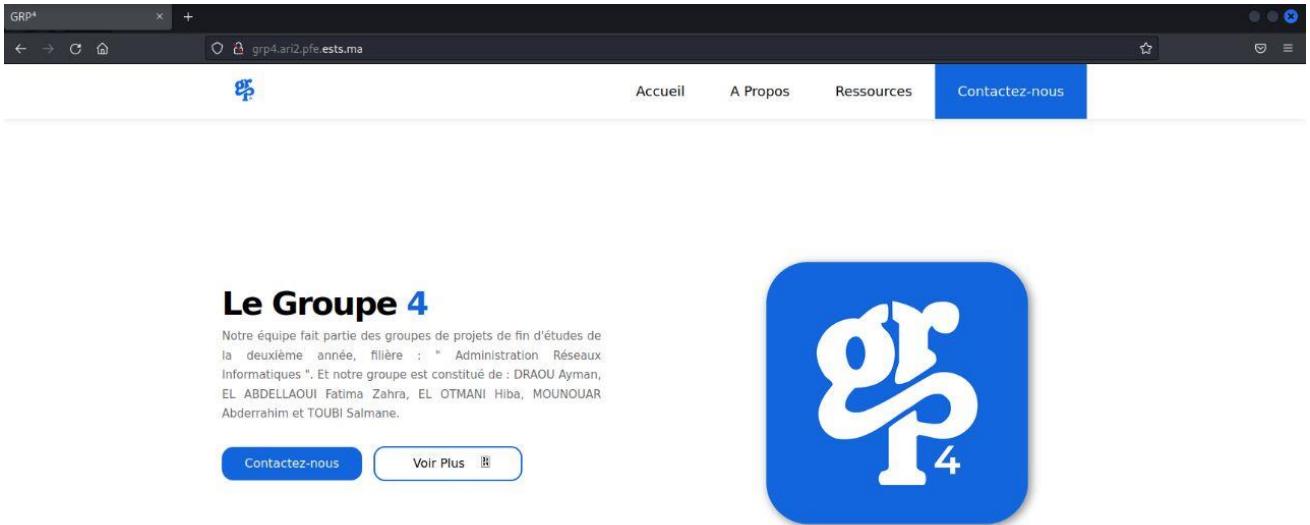


Figure 140 : La page d'accueil du site Web

V.Le serveur de messagerie :

1. Qu'est-ce qu'un serveur de messagerie ?

Un serveur de messagerie est un logiciel ou un système informatique qui permet la gestion et la distribution de courriels (e-mails) entre les utilisateurs d'un réseau, comme Internet.

Lorsqu'un utilisateur envoie un e-mail à un autre utilisateur, le courrier électronique est envoyé à partir du logiciel de messagerie de l'expéditeur à un serveur de messagerie. Ce serveur analyse alors l'adresse e-mail du destinataire pour déterminer où envoyer le courriel. Si le destinataire est sur le même serveur de messagerie, le courriel est directement envoyé à lui. Si le destinataire est sur un autre serveur de messagerie, le serveur d'origine utilise le protocole SMTP (Simple Mail Transfer Protocol) pour transférer le courriel à un autre serveur de messagerie pour atteindre finalement le destinataire.

Le serveur de messagerie est donc essentiel pour la communication électronique, car il assure le traitement, le stockage et la distribution des messages électroniques entre les utilisateurs sur un réseau.

2. Les types de serveur de messagerie :

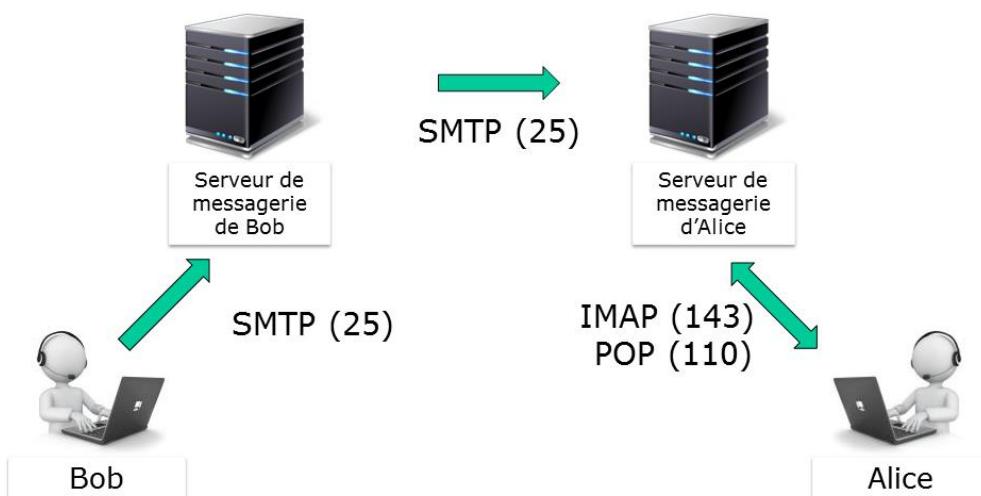


Figure 141 : Schéma serveur messagerie

Il existe différents types de serveurs de messagerie, notamment :

- **Serveurs de messagerie SMTP** (Simple Mail Transfer Protocol) : ils sont utilisés pour transférer les courriels d'un serveur à un autre, en utilisant le **protocole SMTP**.
- **Serveurs de messagerie POP** (Post Office Protocol) : ils permettent aux utilisateurs de récupérer leurs courriels à partir d'un serveur de messagerie. Les e-mails sont téléchargés sur l'ordinateur de l'utilisateur et sont généralement supprimés du serveur.

- **Serveurs de messagerie IMAP** (Internet Message Access Protocol) : ils permettent aux utilisateurs d'accéder et de gérer leurs courriels directement sur le serveur de messagerie, sans avoir à les télécharger sur leur ordinateur. Cela permet une synchronisation entre différents appareils.
- **Serveurs de messagerie Exchange** : développés par Microsoft, ils sont largement utilisés dans les environnements professionnels pour gérer les e-mails, les calendriers et les contacts.
- **Serveurs de messagerie web** : ils permettent aux utilisateurs d'accéder à leur courriel via un navigateur web, sans avoir besoin d'un client de messagerie installé sur leur ordinateur.
- **Serveurs de messagerie instantanée** : ils permettent aux utilisateurs d'échanger des messages instantanés en temps réel, généralement utilisés pour la communication interne dans les entreprises.

Ces différents types de serveurs de messagerie peuvent être utilisés ensemble pour fournir une expérience de communication électronique complète et intégrée.

3. Le fonctionnement du serveur de messagerie :

Le fonctionnement du serveur de messagerie implique trois composants clés : le Mail User Agent (MUA), l'Agent de transfert de courrier (MTA) et l'Agent de distribution de courrier (MDA).

Le MUA est un composant qui interagit directement avec les utilisateurs finaux. Les utilisateurs peuvent accéder aux MUA via des interfaces de messagerie Web telles que Gmail et Yahoo !, ou des logiciels de messagerie tels que Thunderbird, MS Outlook et Zimbra Desktop. Le MUA permet à l'utilisateur de composer, envoyer, recevoir et gérer des e-mails.

Le MTA est responsable du transfert des e-mails d'un serveur de messagerie expéditeur à un serveur de messagerie destinataire. Lorsqu'un utilisateur envoie un e-mail, le MUA envoie le message au MTA local sur le serveur de messagerie expéditeur. Le MTA local sur le serveur de messagerie expéditeur transfère ensuite le courrier électronique via Internet au serveur de messagerie de destination en utilisant le protocole SMTP (Simple Mail Transfer Protocol).

Le MDA est responsable de la réception et de la distribution des e-mails dans les boîtes aux lettres des utilisateurs sur le serveur de messagerie de destination. Lorsque le serveur de messagerie de destination reçoit un e-mail, il est transmis au MDA, qui écrit l'e-mail dans la boîte aux lettres d'un destinataire stockée sur le serveur.

Lorsque le destinataire vérifie l'e-mail via POP (Post Office Protocol) ou IMAP (Internet Message Access Protocol), le MUA du destinataire récupère l'e-mail à partir du serveur. Selon la configuration

du MUA, les e-mails peuvent être téléchargés sur le poste de travail, des copies peuvent être conservées à la fois sur le serveur et le poste de travail, ou les e-mails entre le serveur et le MUA sont synchronisés.

En résumé, le fonctionnement du serveur de messagerie implique l'interaction entre le MUA, le MTA et le MDA pour assurer la livraison des e-mails aux destinataires.

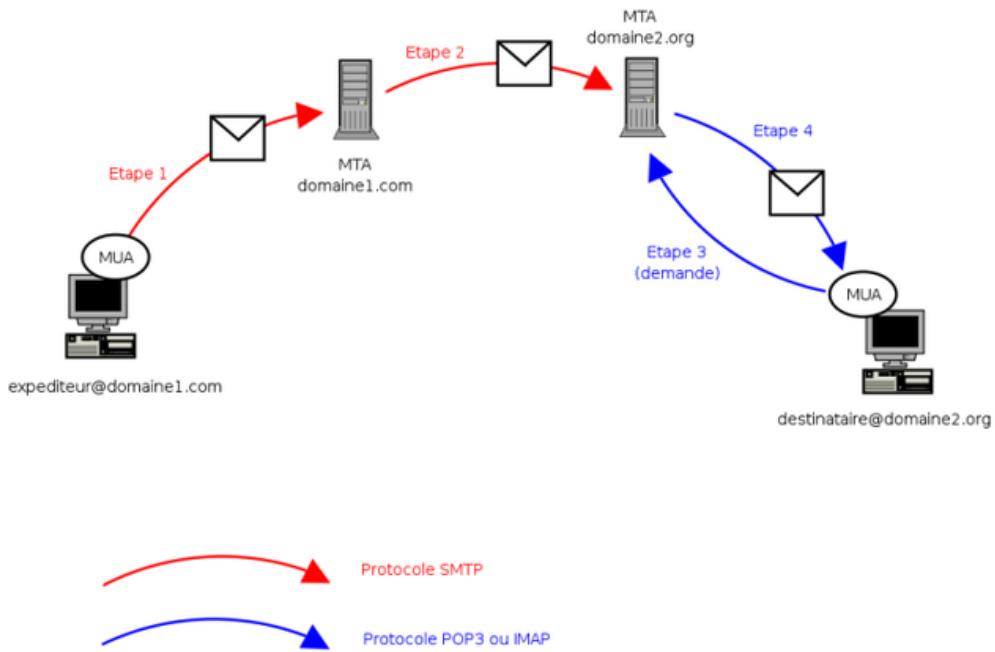


Figure 142 : Le fonctionnement du serveur SMTP

4. Installation et configuration du serveur de messagerie : a) PostFix :

Postfix est un logiciel de serveur de messagerie open source très populaire. Il est utilisé pour acheminer et livrer des courriers électroniques entre les serveurs de messagerie. Postfix est conçu pour être sécurisé, rapide et facile à configurer et à gérer. Il est écrit en langage C et est compatible avec de nombreux systèmes d'exploitation tels que Linux, BSD, MacOs, Solaris, etc.

Postfix est souvent utilisé en combinaison avec d'autres logiciels de messagerie, tels que Dovecot, pour fournir des services de messagerie complets à des utilisateurs individuels ou à des entreprises. En tant que MTA (Mail Transfer Agent), Postfix utilise des protocoles tels que SMTP, TLS et SASL pour transférer et recevoir des courriers électroniques. Il est également

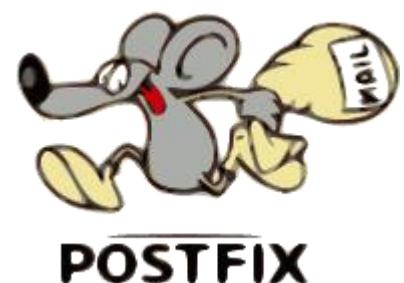


Figure 143 : Logo de Postfix

doté d'un système de filtrage des spams et des virus intégré pour protéger les utilisateurs contre les courriers indésirables.

b) Dovecot :

Dovecot est un logiciel de serveur de messagerie open source qui fournit des services de serveur de messagerie IMAP (Internet Message Access Protocol) et POP3 (Post Office Protocol) pour les clients de messagerie tels que Thunderbird, Outlook ou Apple Mail. Dovecot permet aux utilisateurs de lire, trier et gérer leurs courriers électroniques stockés sur un serveur de messagerie à distance.



Figure 144 : Logo de Dovecot

En plus de fournir des services de messagerie, Dovecot est également capable d'authentifier les utilisateurs via des protocoles standard tels que SASL (Simple Authentication and Security Layer) et LDAP (Lightweight Directory Access Protocol). Il peut également stocker les données utilisateur dans une variété de formats de stockage, tels que le système de fichiers, MySQL, PostgreSQL, SQLite et MongoDB.

c) Evolution :

Evolution est un logiciel de messagerie et de gestion d'informations personnelles open-source, disponible pour les systèmes d'exploitation Linux et Unix. Evolution est capable de se connecter à divers types de serveurs de messagerie, tels que les serveurs de messagerie IMAP, POP et SMTP.



Figure 145 : Evolution logo

d) L'installation du serveur de messagerie « Postfix » :

La première étape consiste à installer le paquet « Postfix » en utilisant la commande indiquée dans la figure ci-dessous :

```
grp4@grp4: ~
Fichier Actions Éditer Vue Aide
grp4@grp4: /etc/bind x grp4@grp4: ~ x grp4@grp4: ~ x
└─(grp4@grp4)-[~]
$ sudo apt install postfix
```

Figure 146 : L'installation du Postfix

- Vers la fin du processus d'installation, une fenêtre ressemblant à celle de l'image ci-dessous s'affichera, il suffit de cliquer sur « Ok ».

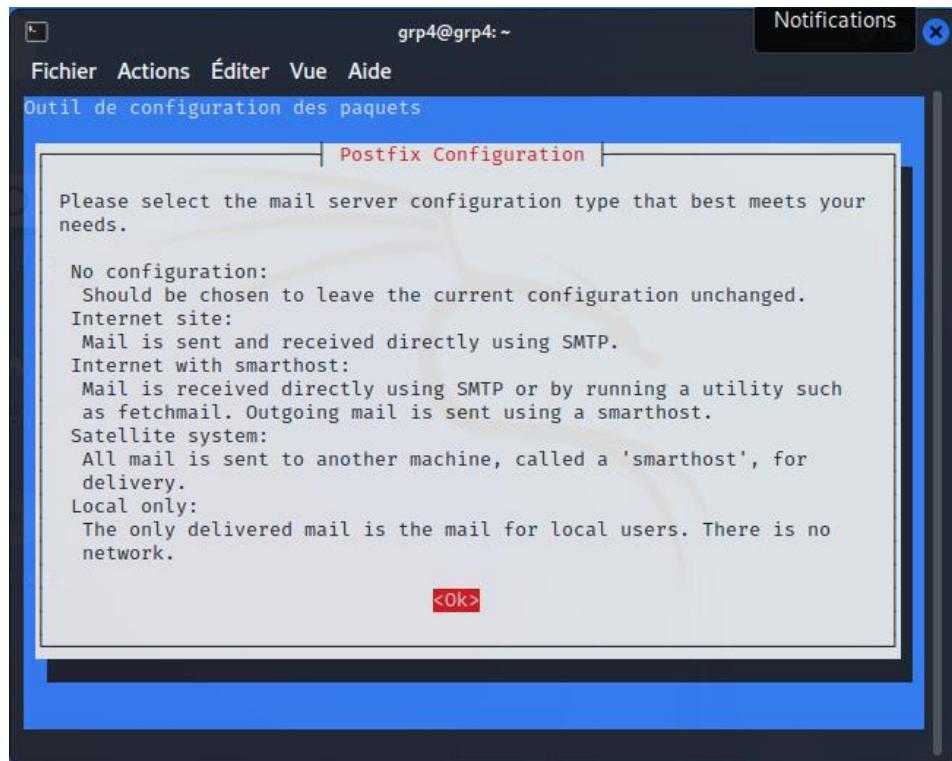


Figure 147 : Configuration du Postfix

- L’option par défaut est Site Internet. C’est l’option recommandée pour ce didacticiel, alors appuyez sur « TAB », puis sur « ENTER ».

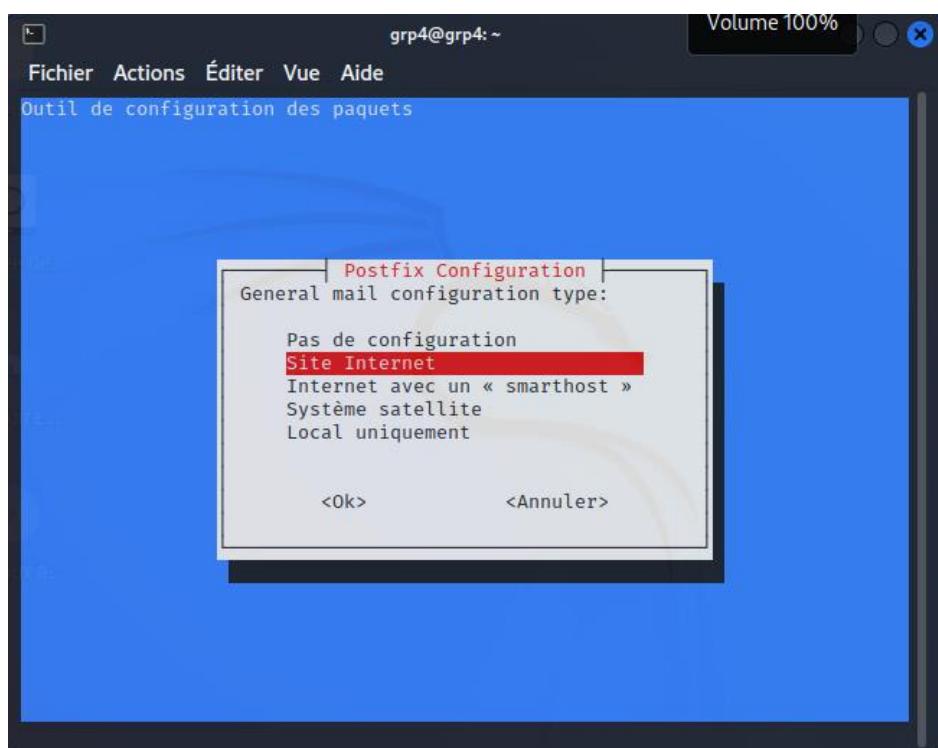


Figure 148 : Configuration des paquets

- Après cela, vous obtiendrez une autre fenêtre comme celle de l'image suivante. Le nom de messagerie système doit être le même que le nom que vous avez attribué au serveur lors de sa création. Lorsque vous avez terminé, appuyez sur « TAB », puis sur « ENTER ».

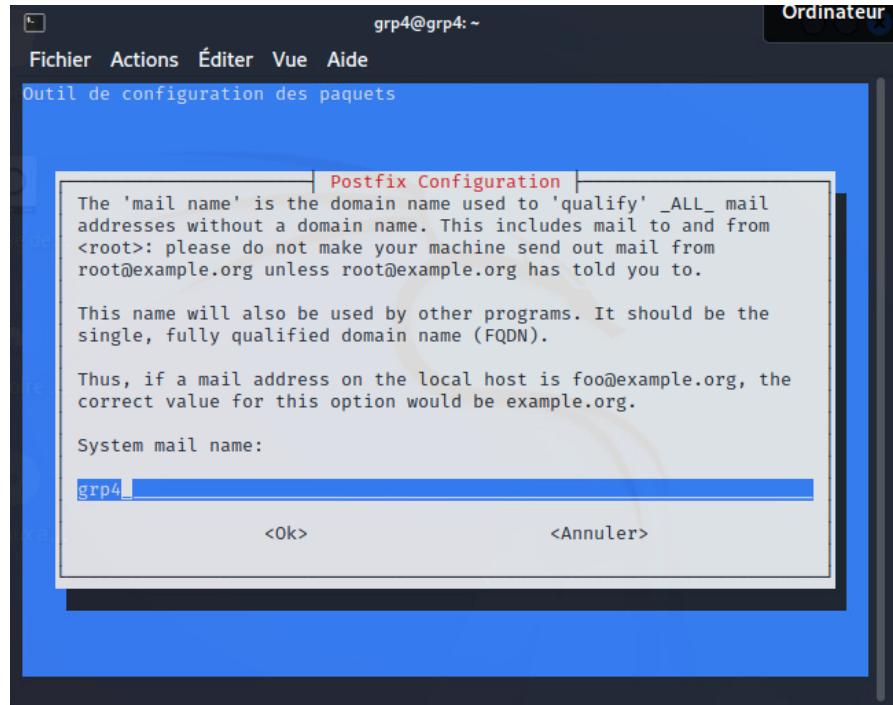


Figure 149 : La configuration de Postix

- Dans le fichier « /etc/bind/grp4.pfe » on va ajouter l'enregistrement du type MX avec le nom complet du serveur « mail.grp4.pfe ».

```

; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     grp4.grp4.pfe. root.grp4.pfe. (
                        2                   ; Serial
                        604800            ; Refresh
                        86400             ; Retry
                        2419200           ; Expire
                        604800            ; Negative Cache TTL
;
@       IN      NS      grp4.grp4.pfe.
@       IN      MX      10      mail.grp4.pfe.
grp4   IN      A       172.120.1.101
www    IN      CNAME   grp4.grp4.pfe.
mail   IN      A       172.120.1.101

```

The screenshot shows a terminal window with the title "grp4@grp4: /etc/bind". It displays the contents of the "grp4.pfe" file using the nano editor. A specific line containing the MX record for "mail.grp4.pfe." is highlighted with a red box. The bottom of the screen shows the nano editor's command bar with various keyboard shortcuts.

Figure 150 : La modification du fichier "grp4.pfe"

- Ensuite, nous allons procéder à la modification du fichier « main.cf » situé dans le répertoire /etc/postfix/main.cf. Dans ce fichier, nous allons ajouter notre domaine « grp4.pfe » à la variable « mydestination », puis nous ajouterons l'adresse IP du serveur à la variable « mynetworks », qui est dans notre cas 172.120.1.0 avec le masque /24.

```

GNU nano 6.4          /etc/postfix/main.cf
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtpd_tls_CApth=/etc/ssl/certs
smtpd_tls_security_level=may
smtpd_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_if_limit_exceeded
myhostname = mail.grp4.pfe
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = mail.grp4.pfe, www.grp4.pfe, $myhostname, grp4, localhost.localdomain
relayhost =
mynetworks = 172.120.1.0/24,127.0.0.0/8 [ ::ffff:127.0.0.0]/104 [ ::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all

^G Aide      ^O Écrire      ^W Chercher      ^K Couper      ^T Exécuter
^X Quitter    ^R Lire fich.  ^\ Remplacer    ^U Coller       ^J Justifier

```

Figure 151 : La modification du fichier « main.cf »

e) L'installation du client messagerie « Evolution » :

Pour commencer, nous devons installer le paquet « Evolution » en exécutant la commande indiquée dans la figure ci-dessous :

```

grp4@grp4: ~
Fichier Actions Éditer Vue Aide
grp4@grp4: /etc/bind x  grp4@grp4: ~ x
└─(grp4@grp4)-[~]
$ sudo apt install evolution

```

Figure 152 : L'installation d'Evolution

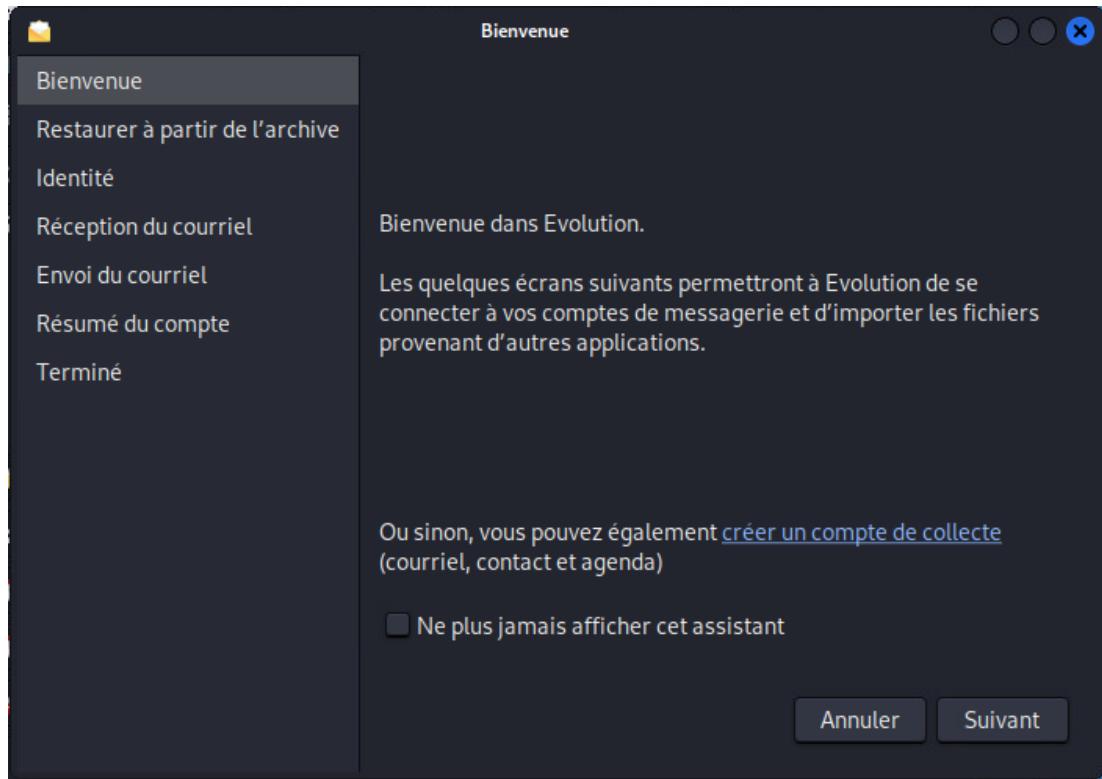


Figure 153 : La page d'accueil Evolution

- Une fois que le paquet est installé, cette page d'accueil s'affichera.
- Puis, il faut saisir votre « adresse électronique » pour pouvoir à la fois envoyer et recevoir des courriels. Il est important de saisir également le « nom complet » et « l'organisation », qui dans notre cas sont respectivement « grp4 » et « grp4_pfe ».

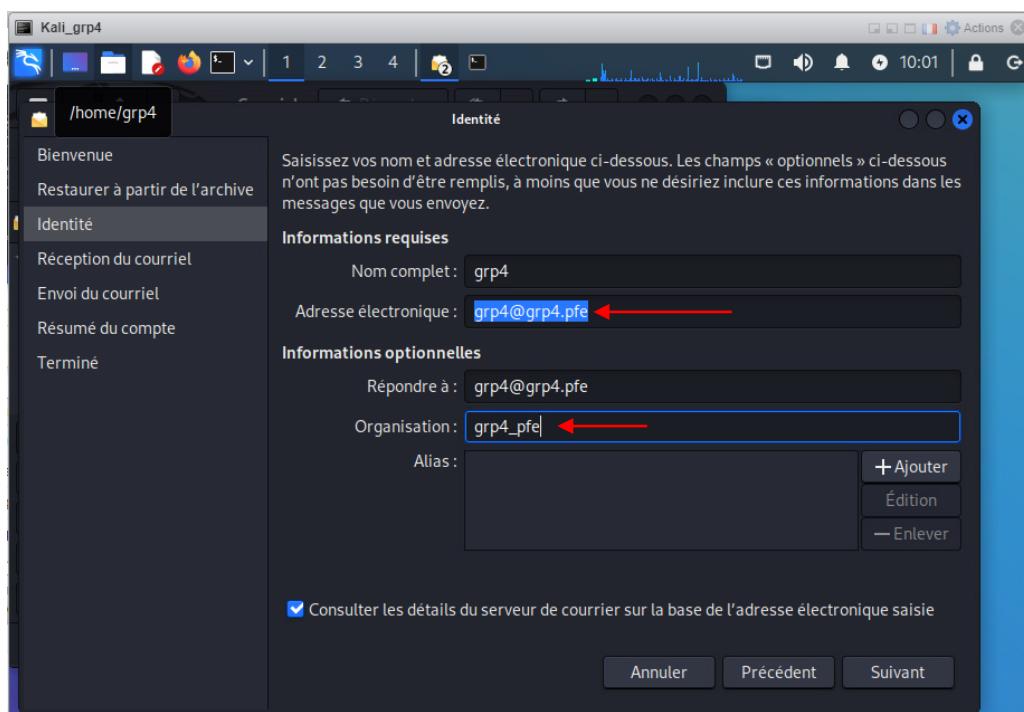


Figure 154 : Les informations du serveur messagerie

- Dans la figure ci-dessous, nous avons sélectionné le type de serveur IMAP pour la réception des courriels. Afin de pouvoir lire et stocker les courriels sur des serveurs IMAP.

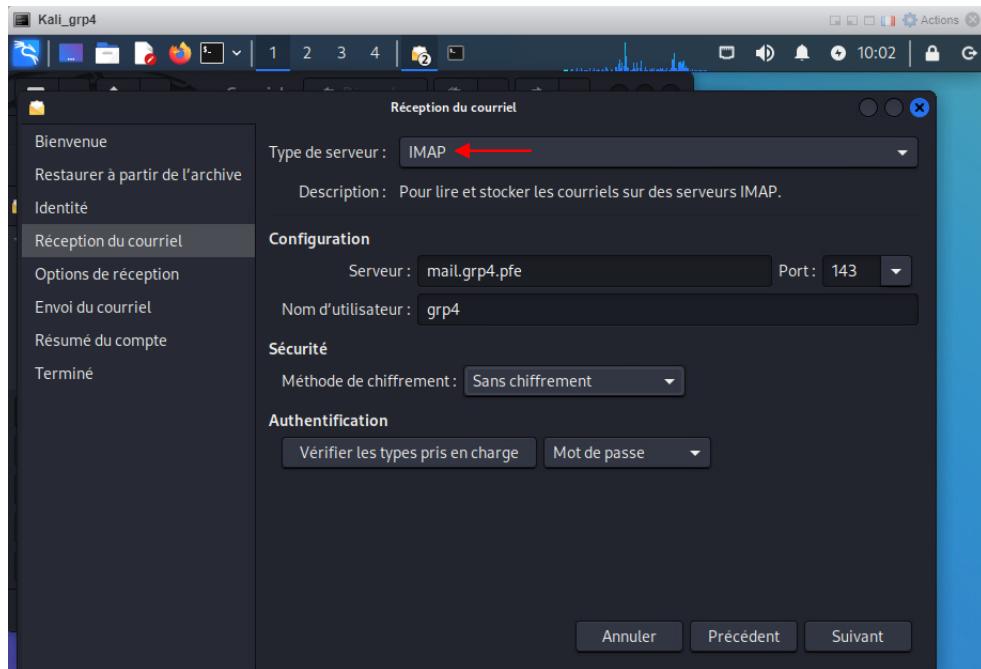


Figure 155 : La configuration de la réception du courriel

- Et pour l'envoi des courriels, nous avons choisi le type de serveur SMTP pour distribuer des courriels via un serveur de courriel distant.

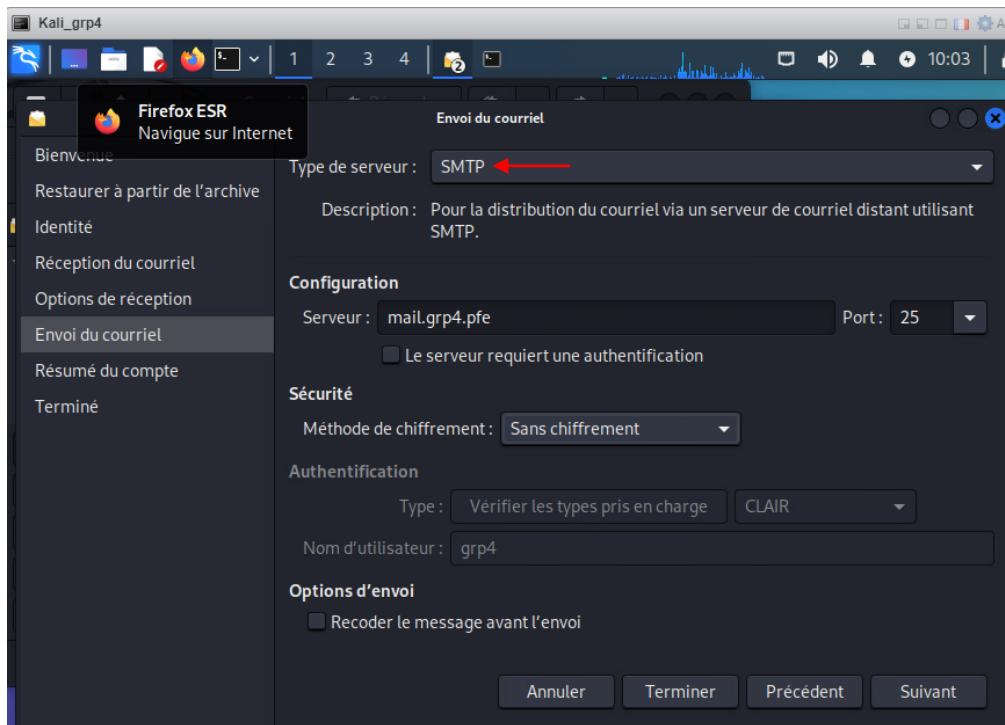


Figure 156 : La configuration de l'envoi du courriel

- Enfin, un aperçu des paramètres qui seront utilisés sera affiché.

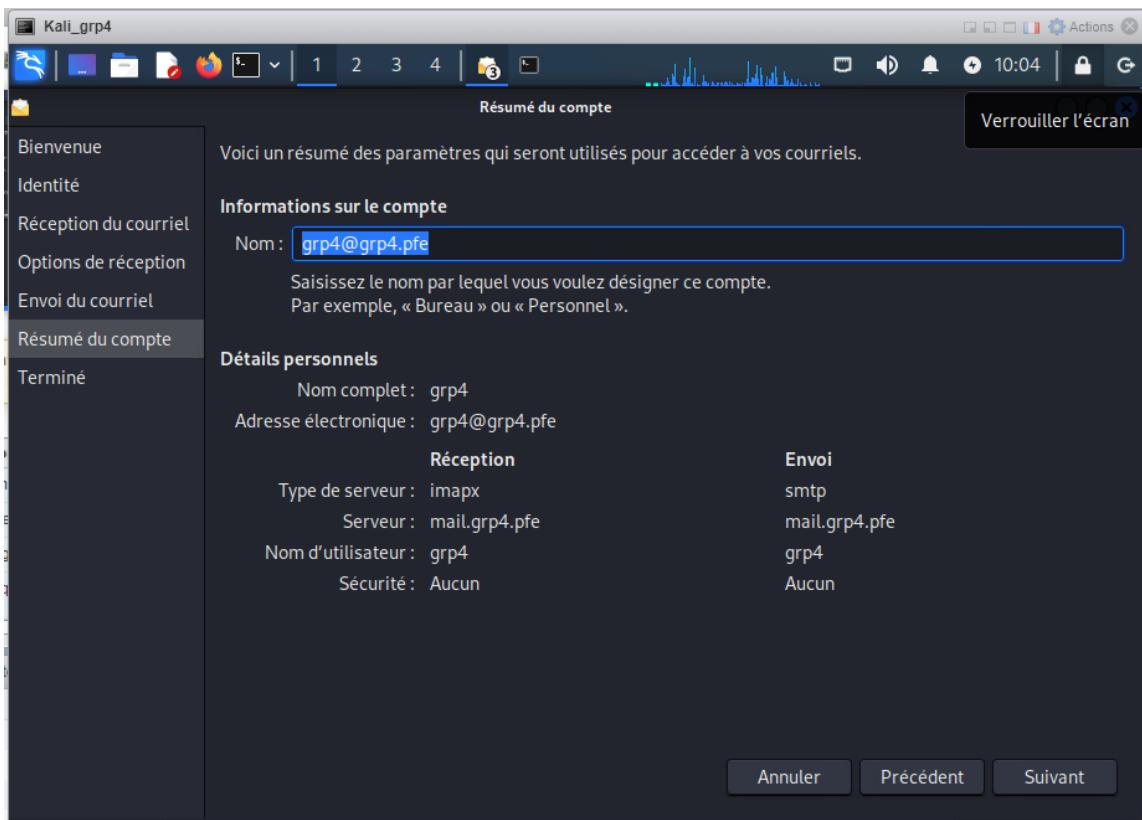


Figure 157 : La finalisation de la configuration "Evolution"

f) L'installation du serveur de messagerie « Dovecot » :

- Pour installer « Dovecot », nous utiliserons la commande suivante :

The terminal window title bar says 'grp4@grp4 - Utilisation : 57%'. The menu bar includes Fichier, Actions, Éditer, Vue, Aide. The window has four tabs at the top: grp4@grp4: /etc/bind, grp4@grp4: ~, grp4@grp4: ~, grp4@grp4: ~. The bottom terminal window shows the command:

```
$ sudo apt install dovecot-core dovecot-imapd dovecot-pop3d
```

Figure 158 : L'installation du serveur de messagerie « Dovecot »

- Afin d'envoyer un e-mail via le serveur de messagerie « dovecot », il faut tout d'abord démarrer le service Dovecot, puis se connecter au serveur en utilisant la commande « sudo telnet mail.grp4.pfe 25 ». Cette dernière permettra d'établir une connexion avec le serveur et d'envoyer les courriels.

```

(grp4@grp4) [~]
$ sudo telnet mail.grp4.pfe 25
Trying 172.100.1.101...
Connected to mail.grp4.pfe.
Escape character is '^'.
he11o grp4.pfe220 mail.grp4.pfe ESMTP Postfix (Debian/GNU)
he11o grp4.pfe
250 mail.grp4.pfe <test@gmail.com>
mail from: test@gmail.com
250 2.1.0 Ok
rcpt to: grp4@grp4.pfe
250 2.1.5 Ok
data
25% End data with <CR><LF>.<CR><LF>
he11o grp4
250 2.0.0 Ok: queued as B952E4015E
^Quit
quit
Connection closed by foreign host.

(grp4@grp4) [~]
$ 
(grp4@grp4) [~]
$ 

```

Boîte de réception (1)

De: test@gmail.com
Date: Fri, 31 Mar 2023 12:06:24 +0000 (+00)

Figure 159 : Test de l'envoi du courriel

- Afin de vérifier que le serveur de messagerie fonctionne correctement, il convient d'accéder à la boîte de réception du compte destinataire du courriel. Dans le cas présent, il s'agit de l'adresse « grp4@grp4.pfe ». Une fois cette étape accomplie, le courriel devrait s'afficher dans la boîte de réception.

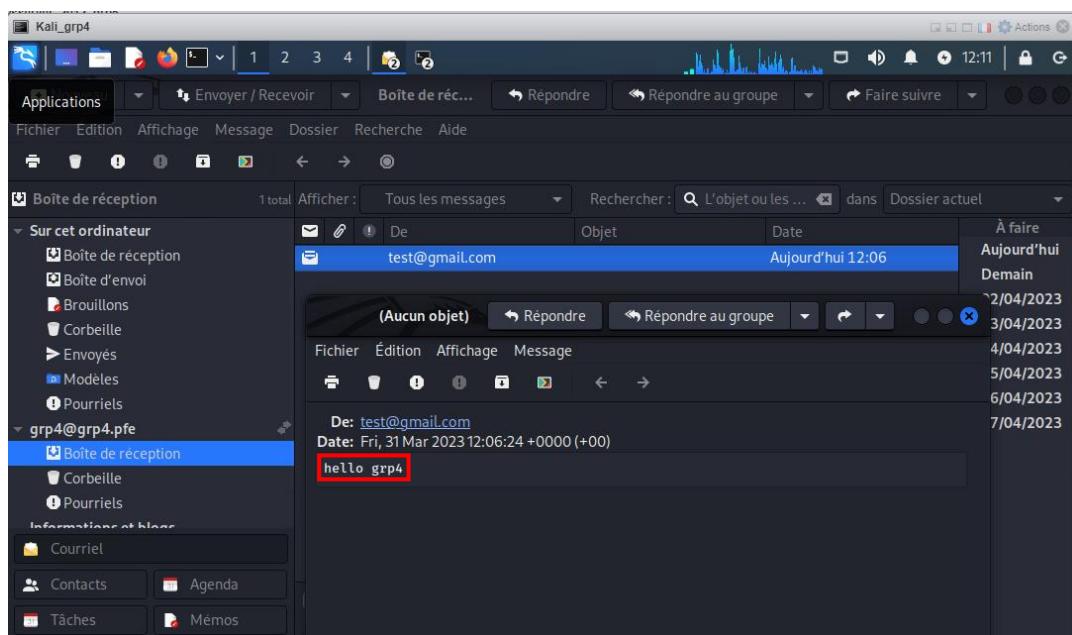


Figure 160 : La réception du courriel

Chapitre VII : La VoIP

I.Etude théorique de la VoIP :

1. Définition :

La VoIP (Voice over Internet Protocol) est une technologie qui permet de faire passer des appels téléphoniques en utilisant une connexion Internet plutôt que les lignes téléphoniques traditionnelles. Elle permet la transmission de la voix en utilisant des protocoles de transmission de données IP (Internet Protocol) plutôt que le réseau de téléphonie traditionnel commuté.

Avec la VoIP, la voix est numérisée, compressée et divisée en petits paquets de données qui sont ensuite transmis via Internet. Les avantages de la VoIP incluent des coûts d'appels moins élevés, une meilleure qualité de son et la possibilité d'ajouter des fonctionnalités telles que la messagerie vocale, la conférence téléphonique et la vidéoconférence.

Cependant, la qualité de la voix peut varier selon la qualité de la connexion Internet, et la VoIP nécessite un équipement et une configuration spécifiques pour fonctionner correctement.

2. Standard de la VoIP :

Il existe plusieurs protocoles standard utilisés dans la VoIP pour la transmission de la voix sur les réseaux IP. Voici les principaux :

- **SIP (Session Initiation Protocol)** : SIP est un protocole de signalisation qui est utilisé pour établir, modifier et terminer les sessions de communication audio et vidéo. Il permet également de gérer les transferts d'appels, les conférences téléphoniques, la messagerie vocale et d'autres fonctionnalités.
- **H.323** : H.323 est un protocole de communication audiovisuelle développé par l'UIT-T (Union Internationale des Télécommunications) pour les réseaux IP. Il est utilisé pour la voix, la vidéo et les données en temps réel.
- **MGCP (Media Gateway Control Protocol)** : MGCP est un protocole de contrôle des passerelles multimédia qui est utilisé pour contrôler les équipements de commutation de circuits traditionnels et les passerelles VoIP.
- **RTP (Real-Time Transport Protocol)** : RTP est un protocole utilisé pour la transmission en temps réel de la voix et de la vidéo sur les réseaux IP. Il est souvent utilisé en conjonction avec SIP ou H.323 pour acheminer les données de voix.

Ces protocoles sont utilisés par les différents fournisseurs de services VoIP pour acheminer les appels et les données vocales sur les réseaux IP. Il est important de noter que les appareils et les équipements

utilisés dans la VoIP doivent être compatibles avec les protocoles de communication en place pour assurer une communication efficace et sans interruption.

3. Fonctionnement :

La VoIP (Voice over Internet Protocol) fonctionne en numérisant la voix en petits paquets de données qui sont envoyés via une connexion Internet plutôt que sur les lignes téléphoniques traditionnelles. Voici les étapes générales du fonctionnement de la VoIP :

- **Conversion de la voix en données** : Le signal vocal est capturé par un microphone et converti en signaux numériques utilisables par l'ordinateur ou le téléphone VoIP.
- **Encodage** : Les signaux vocaux sont ensuite encodés et compressés en utilisant des algorithmes de compression tels que G.711 ou G.729. Cette étape permet de réduire la taille des données pour une transmission plus efficace.
- **Routage des paquets** : Les paquets de données sont ensuite envoyés via une connexion Internet à destination du destinataire de l'appel.
- **Décodage** : Les paquets de données arrivent au destinataire où ils sont décryptés et décompressés pour restaurer la voix originale.
- **Conversion de données en voix** : Les données restaurées sont ensuite converties en signaux vocaux qui sont émis par les haut-parleurs du téléphone ou de l'ordinateur du destinataire.

Il est important de noter que la qualité de la voix peut varier selon la qualité de la connexion Internet et les équipements utilisés pour la VoIP. Les fournisseurs de services VoIP utilisent différents protocoles pour acheminer les données vocales, tels que SIP, H.323 ou MGCP. La qualité de la VoIP peut être améliorée en utilisant une connexion Internet de haute qualité, des équipements de VoIP de qualité supérieure et des protocoles de transmission de qualité.

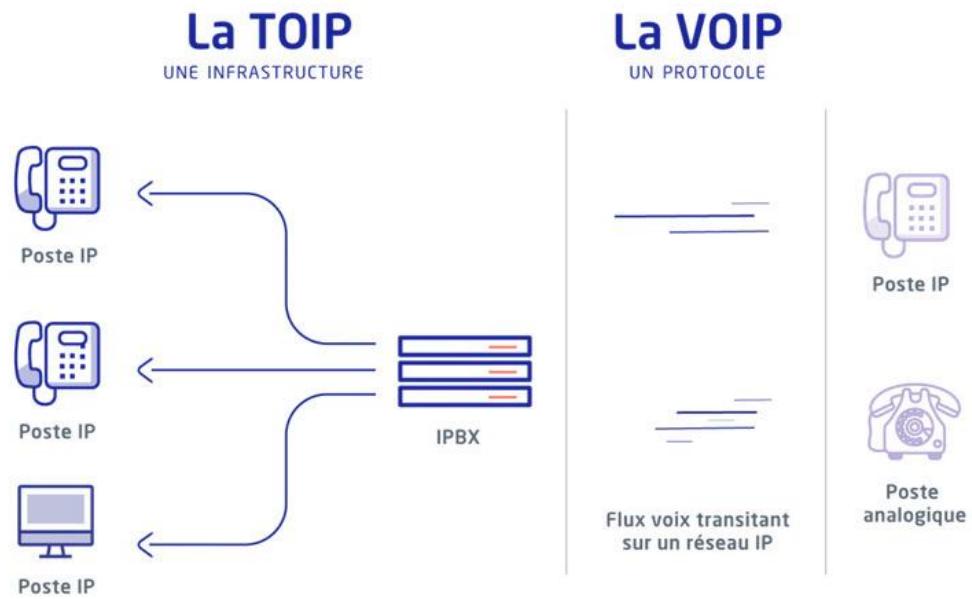


Figure 161 : La VoIP

II.Elastix :

Elastix était une solution logicielle open source pour la communication unifiée basée sur la VoIP. Elle combinait différentes fonctionnalités telles que la gestion des appels téléphoniques, la messagerie instantanée, la conférence téléphonique, la vidéoconférence, la boîte vocale, la messagerie électronique, la gestion des contacts et bien plus encore.

Elastix était basée sur le système d'exploitation CentOS et utilisait des logiciels open source tels que Asterisk (un serveur de téléphonie open source), FreePBX (un système de gestion de téléphonie basé sur le web) et d'autres logiciels pour fournir une solution complète de communication unifiée.

Cependant, depuis la version 5, Elastix n'est plus maintenu et a été remplacé par une nouvelle solution appelée 3CX. La communauté peut toujours accéder aux versions précédentes d'Elastix pour les utiliser ou les adapter, mais sans support officiel.



Figure 162 : Elastix logo

1. Installation de Elastix :

Lorsque nous exécutons Elastix à partir de notre serveur, nous pouvons accéder au mode graphique en appuyant sur la touche « Entrée ».

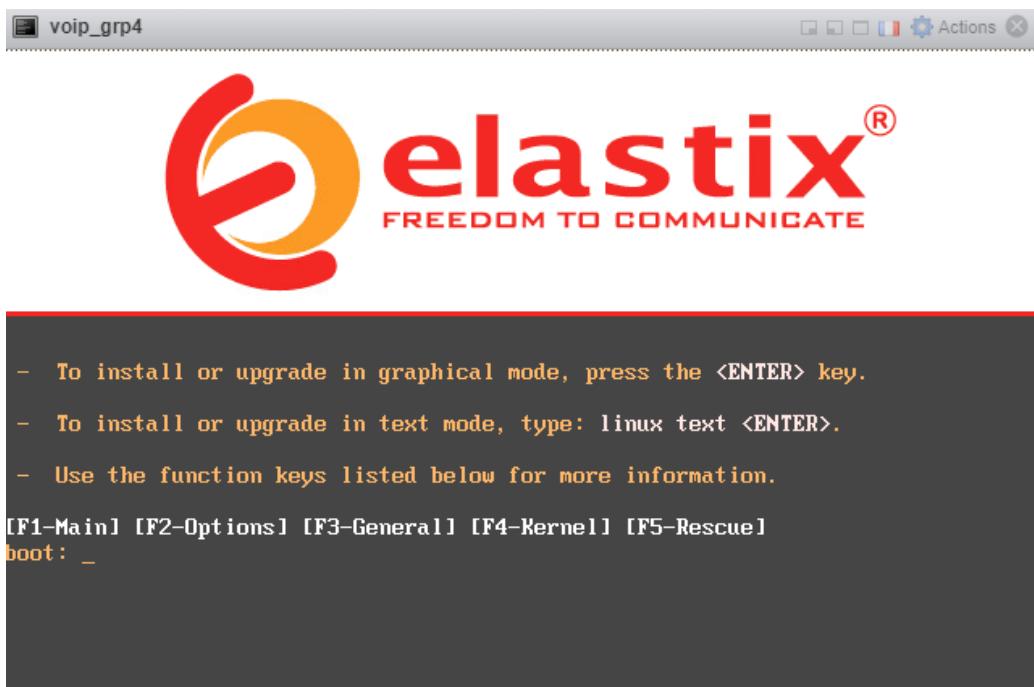


Figure 163 : Installation de Elastix

- Ensuite, nous avons sélectionné le type de partitionnement en optant pour l'espace libre disponible sur les disques.

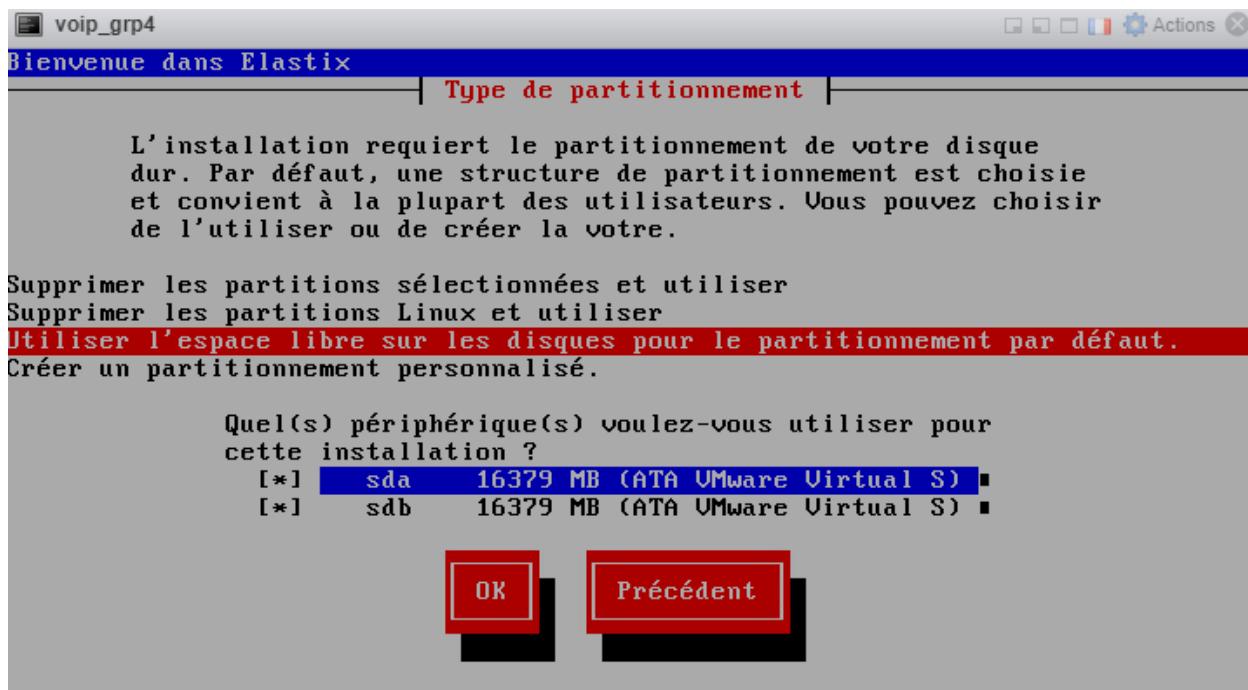


Figure 164 : Le type de partitionnement

- Ci-dessous se trouve la liste des partitions présentes sur notre machine.

Bienvenue dans Elastix					
Partitionnement					
Pérophérique	Début	Fin	Taille	Type	Point de mon
VG VolGroup00			32608M	VolGroup	
LU LogVol01			4032M	swap	
LU LogVol00			28576M	ext3	/
/dev/sda					
sda1	1	13	101M	ext3	/boot
sda2	14	2088	16276M	physical	v
/dev/sdb					
sdb1	1	2088	16378M	physical	v

Nouveau Éditer Supprimer RAID OK Précédent

F1-Aide F2-Ajouter F3-Éditer F4-Supprimer F5-Réinitialiser ☰

Figure 165 : La liste des partitions présentes

- Puis, il est nécessaire de choisir un mot de passe du compte administrateur pour se connecter au serveur par la suite.

Bienvenue dans Elastix

Mot de passe root

Choisissez un mot de passe root.
Vous devez le saisir deux fois pour vous assurer que vous le connaissez et que vous n'avez pas fait d'erreur en le saisissant. N'oubliez pas que le mot de passe root est un élément extrêmement important de la sécurité du système !

Mot de passe : *****

Mot de passe (confirmation) : *****

OK Précédent

Figure 166 : Le mot de passe du compte administrateur

- Par la suite, le processus d'installation démarre.

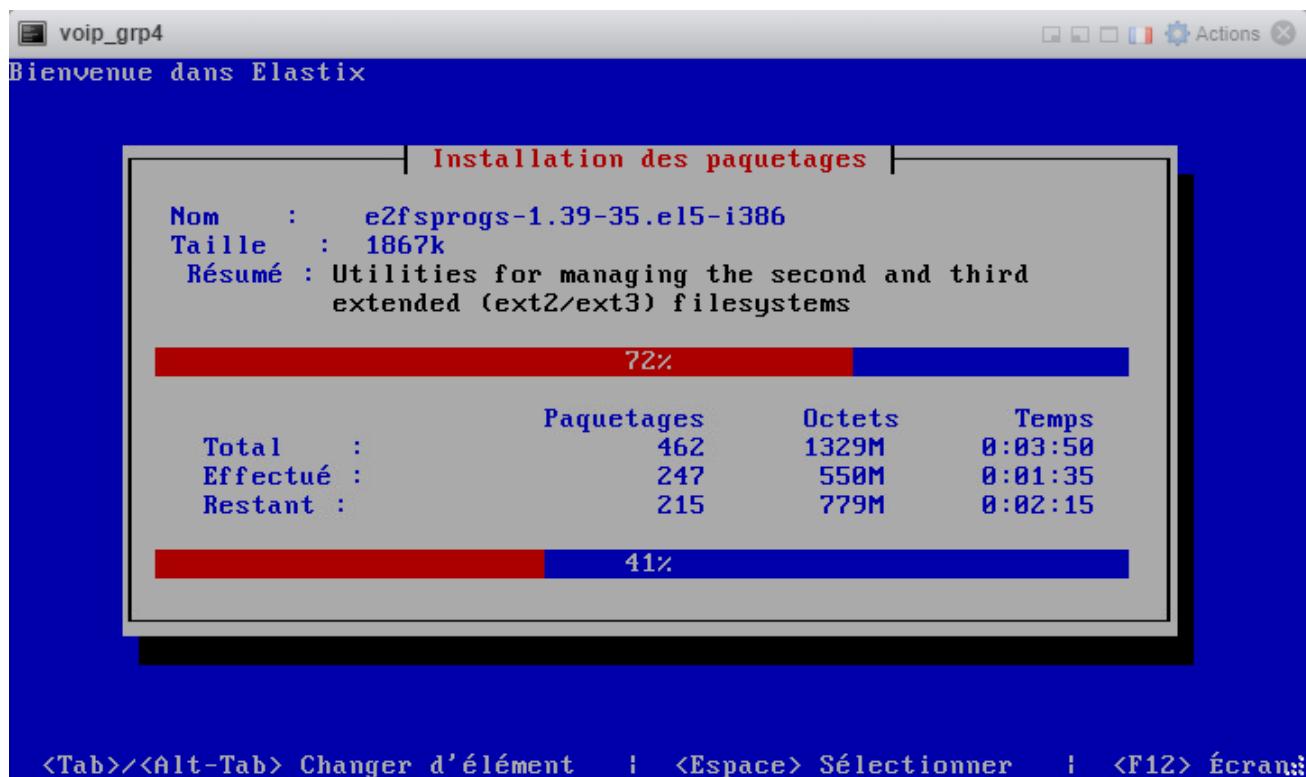


Figure 167 : Début de l'installation de Elastix

- À la fin de l'installation, il est requis d'entrer et de confirmer le mot de passe qui sera utilisé pour le compte root de la base de données MySQL.

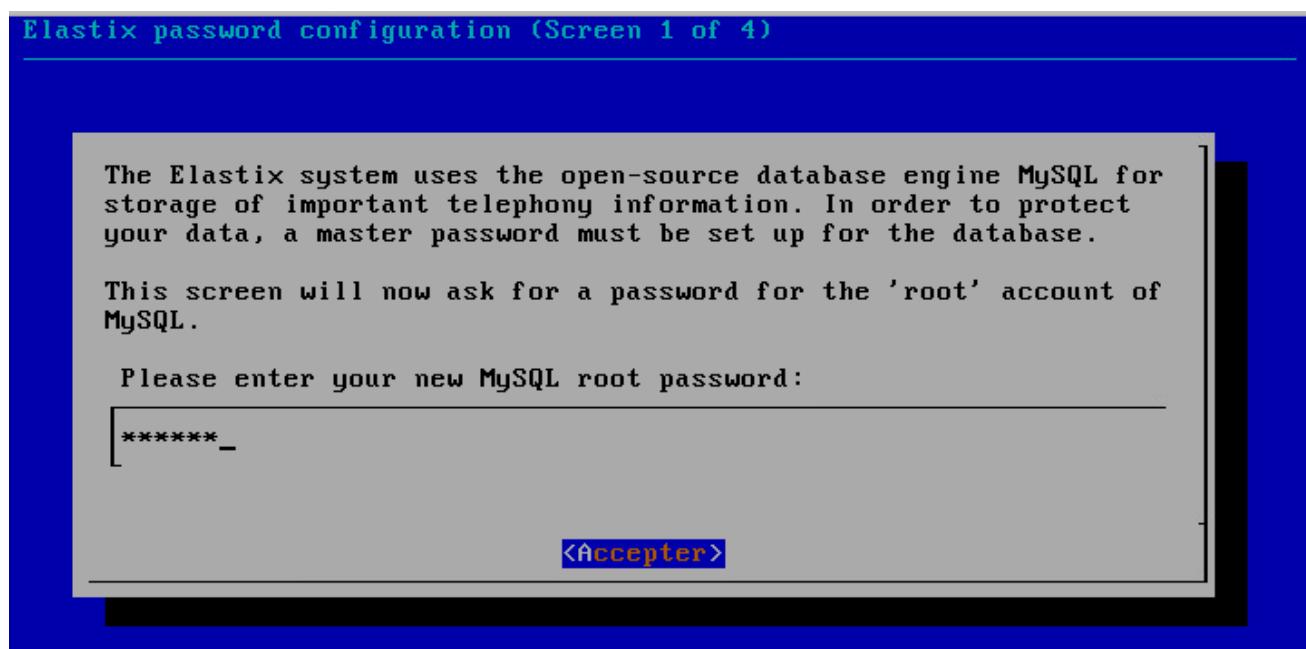


Figure 168 : Le mot de passe du compte root de la base de données MySQL

```

voip_grp4
CentOS release 5.9 (Final)
Kernel 2.6.18-348.1.1.el5 on an i686
localhost login: root
Password:

```

Figure 169 : Authentification en tant qu'administrateur

- Une fois le mot de passe du compte administrateur saisi, il convient d'exécuter la commande « setup ». Cette dernière permettra d'ouvrir la fenêtre présentée ci-dessous.

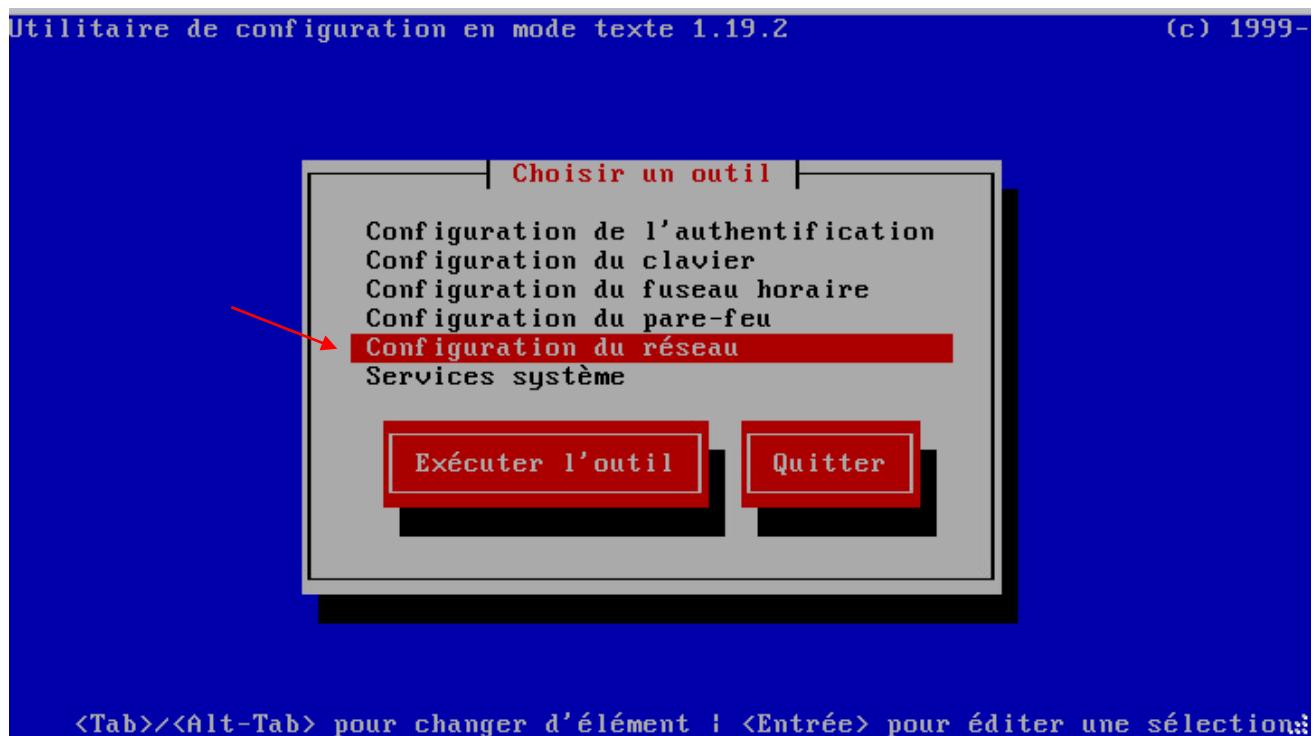


Figure 170 : Configuration du réseau

- Il est nécessaire de sélectionner l'option « Configuration du réseau » afin de pouvoir attribuer manuellement une adresse IP et son masque à notre serveur : l'adresse « 192.168.20.250 » avec le masque « 255.255.255.0 », appartenant au VLAN des employés. Ensuite, il faudra indiquer l'adresse de la passerelle « 192.168.20.254 ».

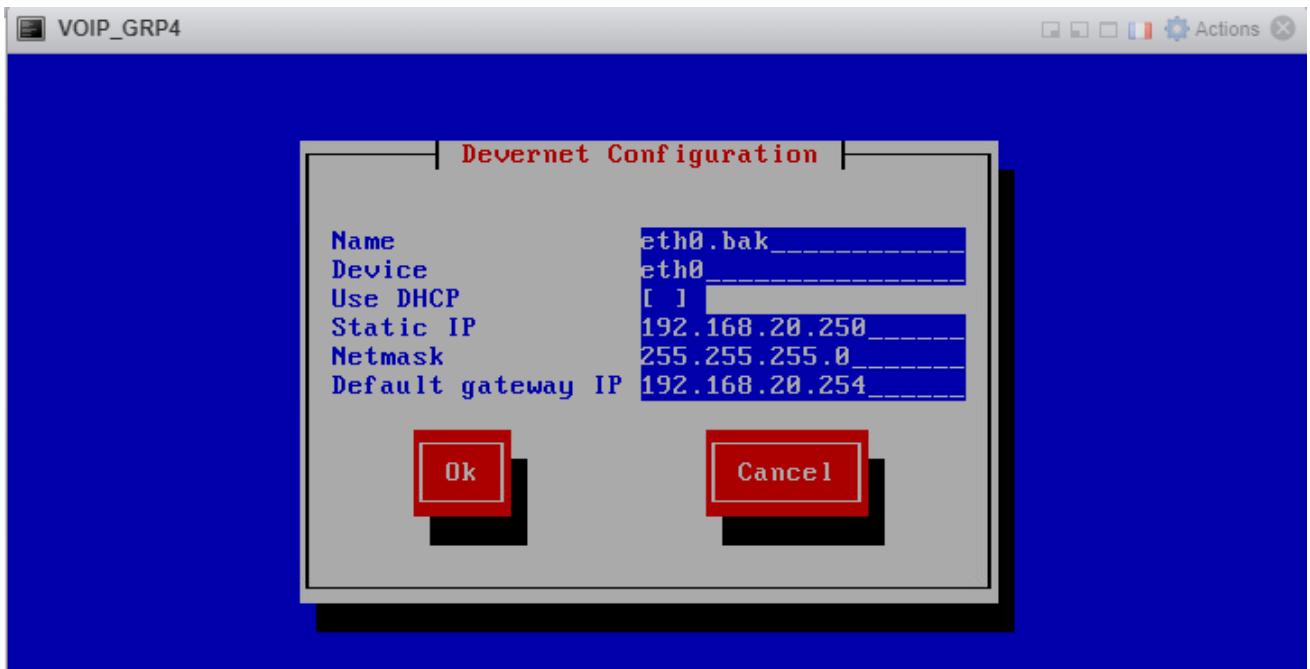


Figure 171 : La saisie de l'adresse IP

a) Configuration Elastix :

L'accès à l'interface web de notre serveur est possible en utilisant l'URL fournie dans une étape précédente sur la console. Il est également nécessaire de s'authentifier avec le compte « admin ».

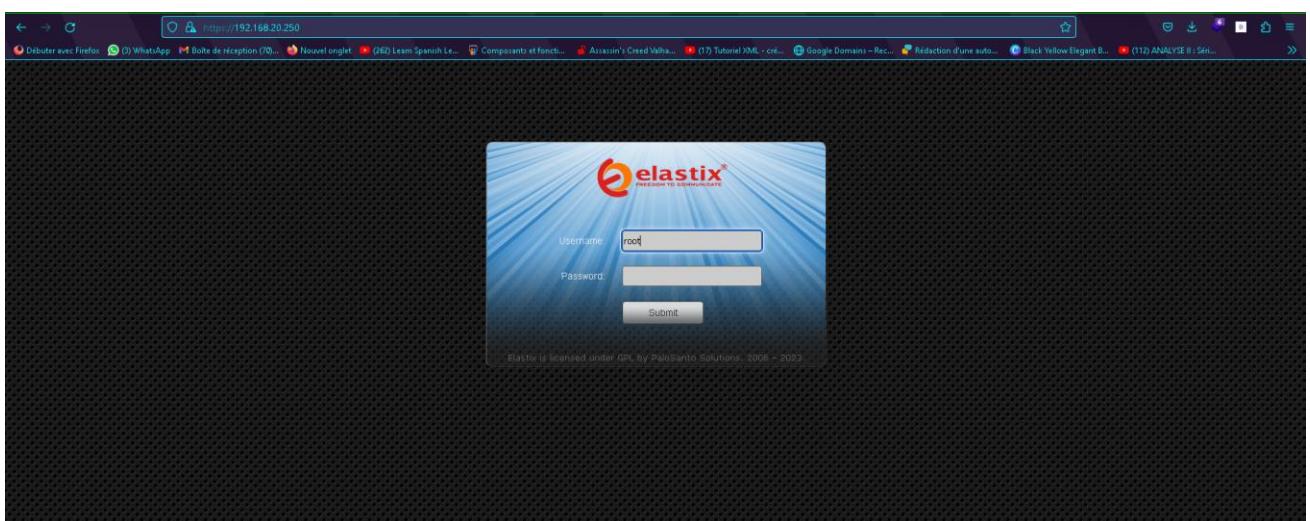


Figure 172 : L'interface Web Elastix

- Une fois que vous avez effectué la connexion, le tableau de bord s'ouvrira :

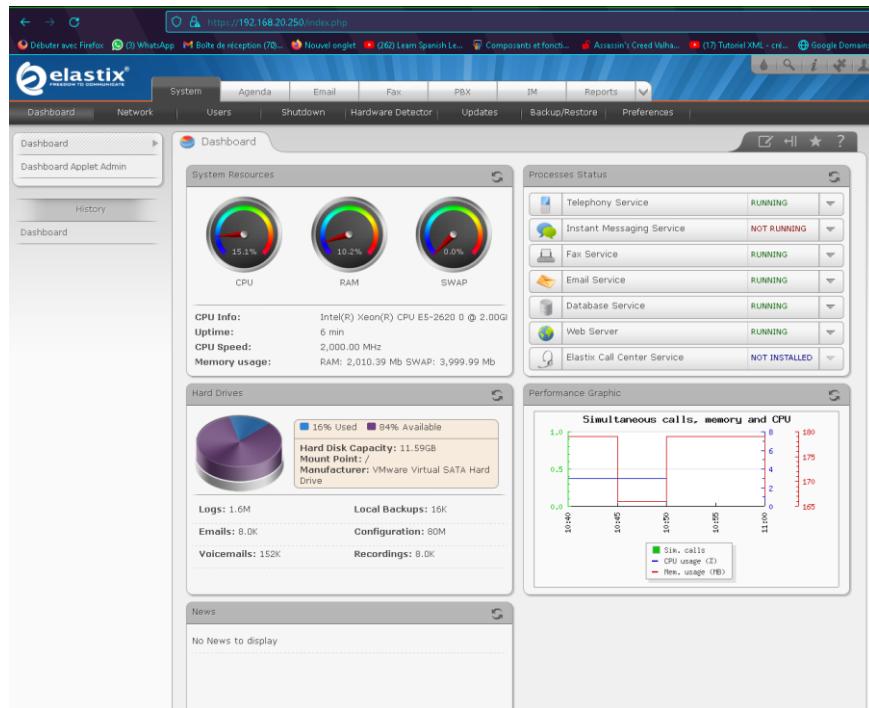


Figure 173 : Le tableau de bord Elastix

- Nous allons attribuer des numéros SIP à des employés en accédant à la section « PBX » de l'interface, puis en sélectionnant l'option « Périphérique SIP ».

The screenshot shows the Elastix PBX Configuration interface. The left sidebar lists various configuration sections like Basic, Extensions, Feature Codes, Outbound Routes, Trunks, Inbound Call Control, and so on. The main panel is titled 'Add an Extension' with the sub-instruction 'Please select your Device below then click Submit'. It has a 'Device' dropdown menu where 'Generic SIP Device' is selected. A 'Submit' button is visible at the bottom left of the dropdown. A small tooltip on the right says 'Add Extension test <111> abdo <444>'.

Figure 174 : L'ajout d'une extension

- La figure ci-dessous illustre le récapitulatif des comptes SIP sur 3cxPhone, aucun compte n'a été créé jusqu'à présent.

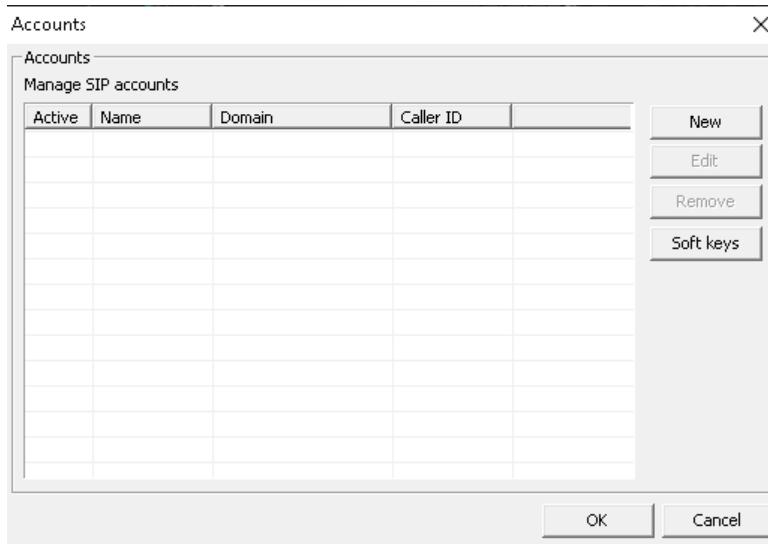


Figure 175 : Les comptes SIP

- Pour le premier client SIP « abdo » sur 3cxPhone, nous renseignons le nom, l'extension, le mot de passe et l'adresse du serveur Elastix. Ensuite, nous constatons que le téléphone est connecté et en mode « on Hook ».

Account settings

Account name: abdo

Caller ID: 222

Credentials

Enter your SIP account credentials

Extension: 444

ID: 444

Password: *****

My location

Specify the IP of your PBX/SIP server

I am in the office - local IP 192.168.20.249 of PBX

I am out of the office - external IP _____ of PBX

Use 3CX Tunnel

Eliminates firewall configuration. Requires 3CX Phone System for Windows

Local IP of remote PBX: _____

Tunnel password: *** Port: 5090

Use Outbound Proxy server

Required by some VoIP Providers. Specify IP or name.

Perform provisioning from following URL:

[http://]

Advanced settings OK Cancel

Figure 176 : Configuration d'un client



Figure 177 : Téléphone 3cx

- Nous pouvons constater l'ajout de l'utilisateur nommé « abdo ».

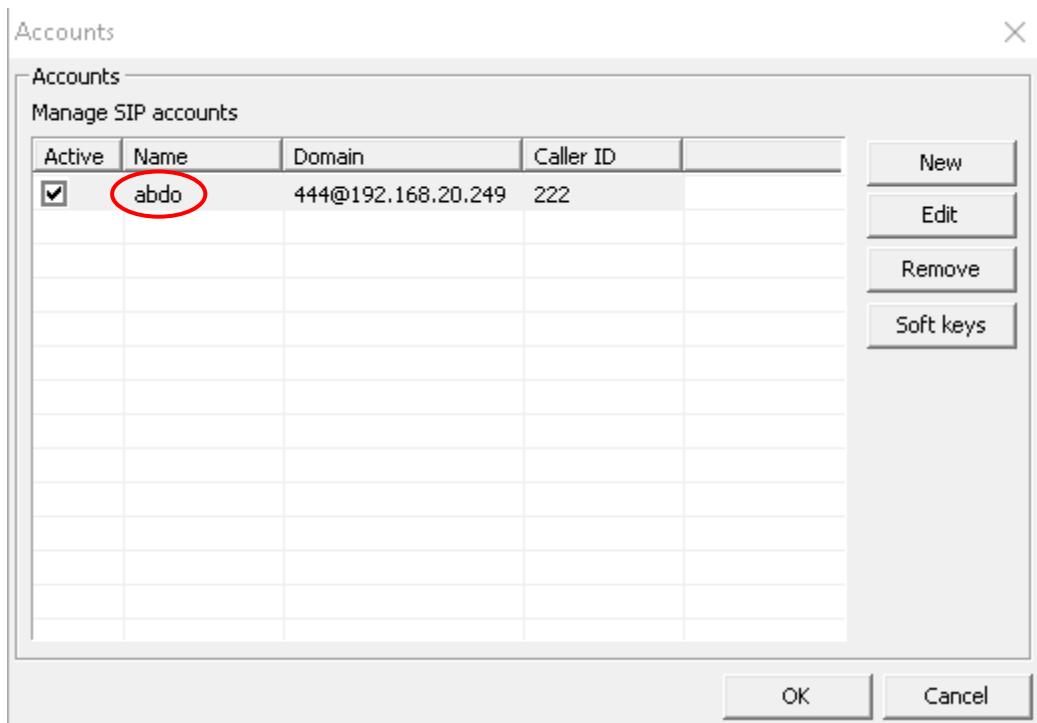


Figure 178 : L'ajout de client "abdo"

- La figure ci-dessous illustre le récapitulatif des comptes SIP sur X-Lite, aucun compte n'a été créé jusqu'à présent.

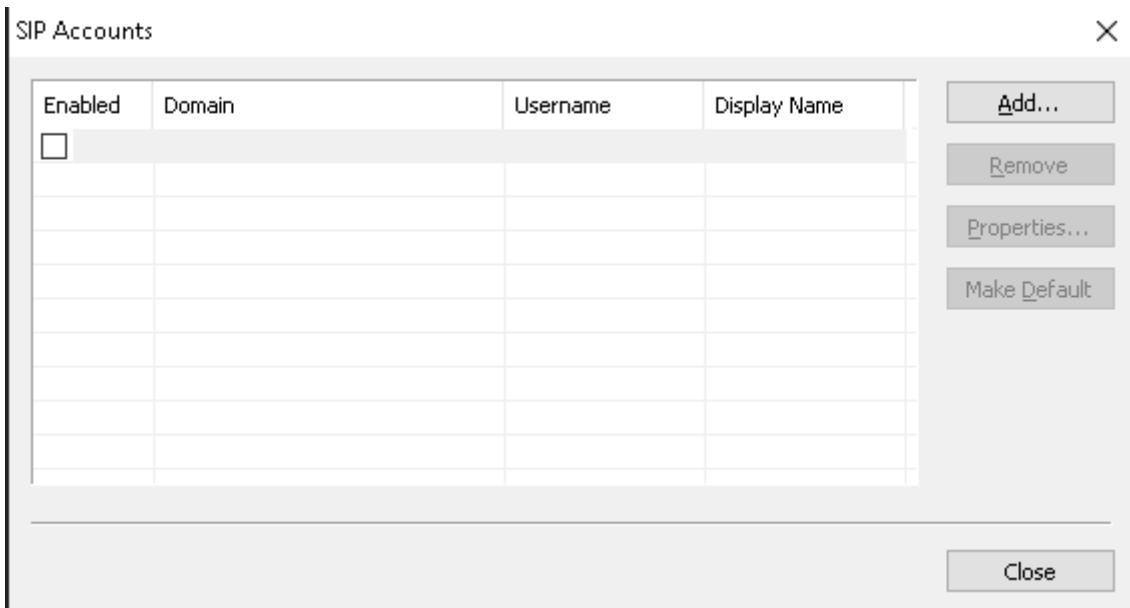


Figure 179 : Les comptes SIP sur X-Lite

- Pour le premier client SIP « post4 » sur X-Lite, nous renseignons le nom, le nom d'utilisateur, le mot de passe et l'adresse du serveur Elastix.

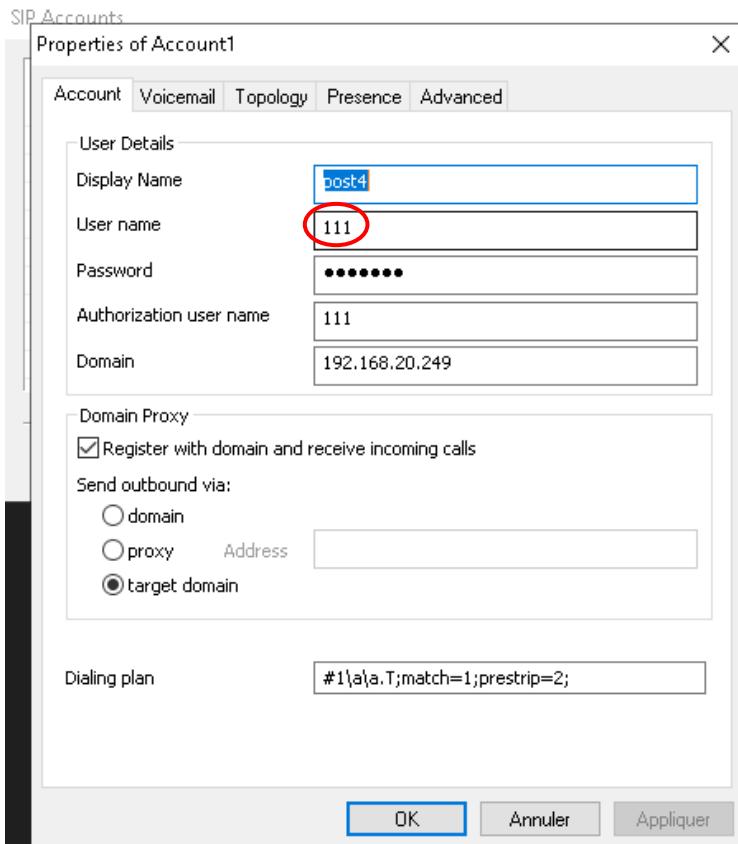


Figure 181 : Configuration du client 2



Figure 180 : Téléphone X-Lite

- En ajoutant les deux comptes sur l'onglet « Operator Panel » de l'interface Web du serveur Elastix, les clients SIP connectés peuvent être identifiés par leur case qui s'affiche en orange foncé.

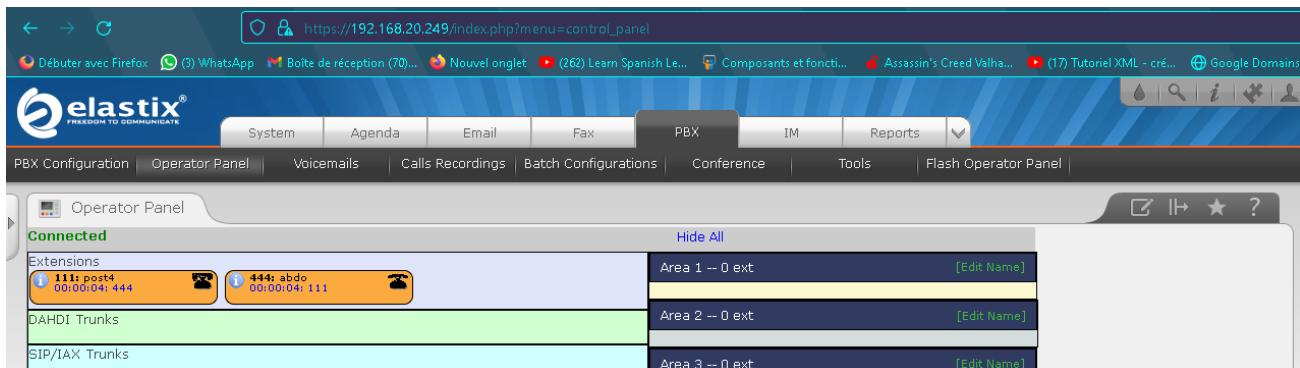


Figure 182 : Vérification des deux clients

b) Test de communication :

Nous allons à présent tenter d'établir une communication entre les deux clients SIP en composant l'extension « 111 » qui correspond au numéro de « abdo » depuis le softphone de « post4 ». Nous constatons que le téléphone du client « post4 » sonne et affiche les informations de l'appelant « abdo », à savoir son nom, son extension et son numéro, qui est « 444 ».

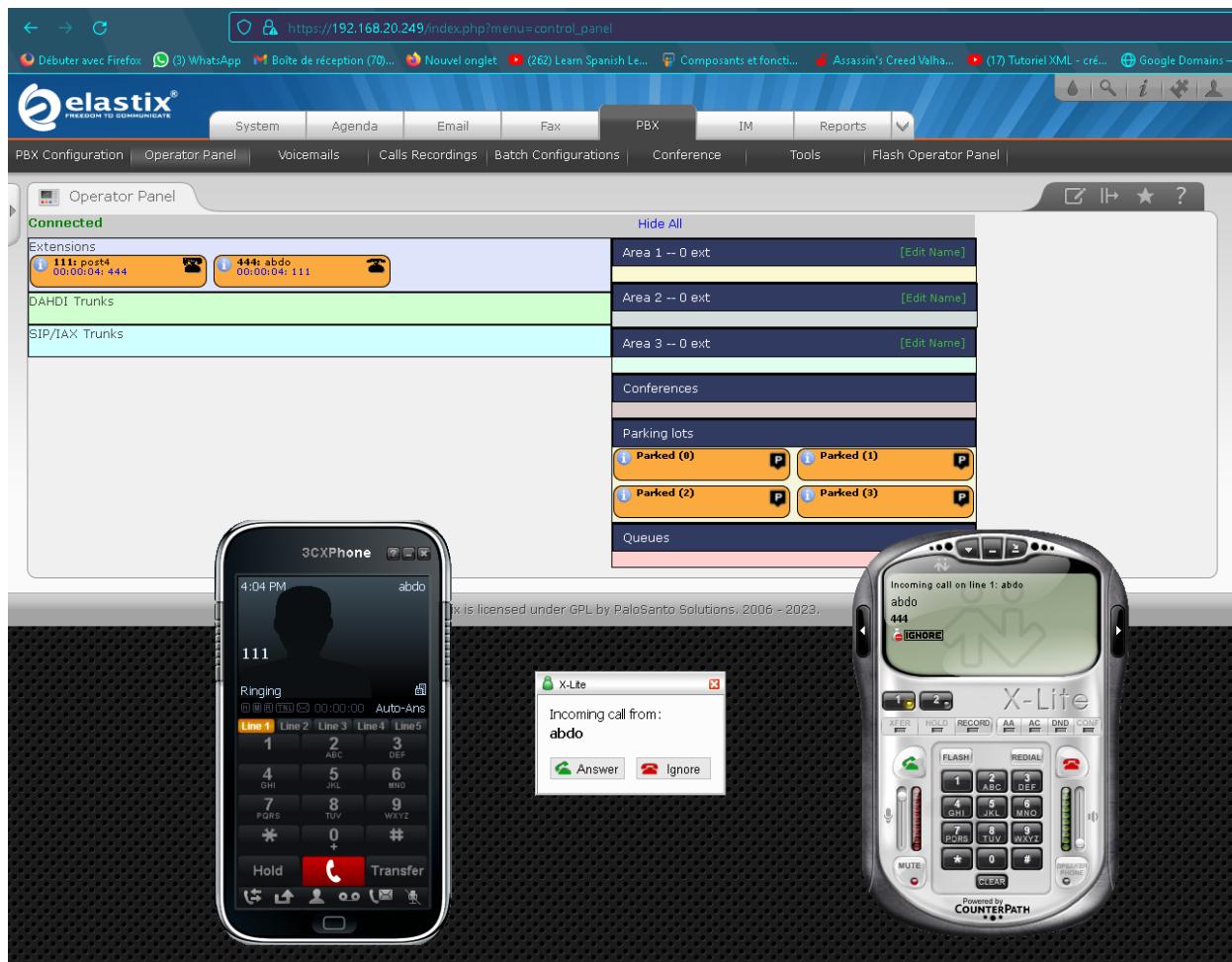


Figure 183 : Réception de l'appel de "abdo"

Chapitre VIII : Mise en place d'un serveur de supervision

De nos jours, il devient de plus en plus complexe de gérer efficacement un réseau en raison de l'augmentation constante du nombre d'équipements à administrer, qu'il s'agisse de composants matériels tels que des commutateurs et des routeurs, ou de composants applicatifs tels que des bases de données, des serveurs web et des services réseau.

Pour un administrateur de réseau, la panne est une source de préoccupation majeure. Il doit être en mesure de réagir rapidement pour effectuer les réparations nécessaires.

I.La supervision informatique :

La supervision informatique est un processus qui consiste à surveiller et à analyser en temps réel les performances des systèmes informatiques et des réseaux pour s'assurer de leur bon fonctionnement. Cette surveillance peut inclure des éléments tels que la disponibilité des ressources informatiques, la qualité des connexions réseau, la consommation des ressources système, les niveaux de sécurité et de conformité, et d'autres indicateurs clés de performance (KPI) pertinents pour l'entreprise. Les outils de supervision informatique peuvent aider les administrateurs à détecter les problèmes potentiels avant qu'ils ne deviennent des problèmes majeurs et à prendre les mesures nécessaires pour y remédier rapidement.

1. Le protocole SNMP :

SNMP (Simple Network Management Protocol) est un protocole de gestion de réseau qui permet à un administrateur de surveiller et de gérer à distance les équipements réseau tels que les routeurs, les commutateurs, les serveurs, les imprimantes, etc.

SNMP est un protocole de couche application qui utilise l'architecture client-serveur. Les équipements réseau, appelés agents SNMP, sont configurés pour envoyer des informations de gestion à un gestionnaire SNMP qui agit comme client. Les informations de gestion envoyées par les agents SNMP incluent des statistiques sur l'utilisation des ressources telles que la mémoire, le processeur, la bande passante et d'autres informations pertinentes pour la supervision du réseau.

Le protocole SNMP fonctionne en utilisant des messages spécifiques appelés « protocol data units » (PDU), qui sont échangés entre les agents SNMP et les gestionnaires SNMP. Les PDUs peuvent être de différents types, tels que « get-request », « get-response », « set-request », « trap », etc.

En utilisant le protocole SNMP, les administrateurs réseau peuvent surveiller l'état de leur réseau, détecter les pannes ou les problèmes de performance et y remédier rapidement, ce qui contribue à garantir une haute disponibilité et une qualité de service élevée pour les utilisateurs du réseau.

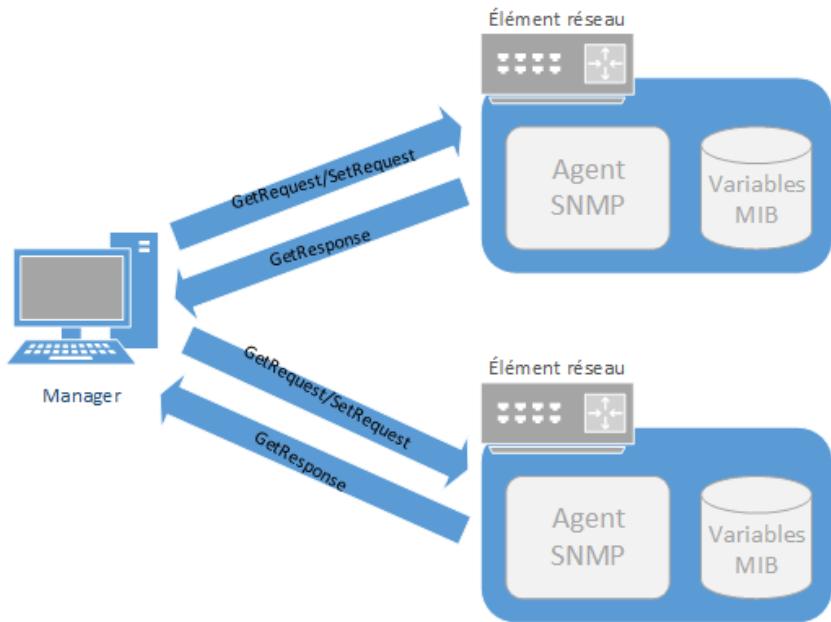


Figure 184 : Protocole SNMP

a) Les requêtes SNMP :

Les requêtes SNMP sont des demandes envoyées par un gestionnaire SNMP à un agent SNMP pour obtenir des informations de gestion sur un équipement réseau. Les requêtes SNMP sont utilisées pour surveiller l'état du réseau et des équipements, pour récupérer des informations de configuration, pour déclencher des actions spécifiques et pour effectuer d'autres opérations de gestion.

Il existe plusieurs types de requêtes SNMP, chacune ayant une fonction spécifique :

- Get-request : demande à l'agent SNMP de fournir une valeur associée à un objet de gestion spécifique.
- Get-next-request : demande à l'agent SNMP de fournir la valeur suivante dans la table d'objets.
- Get-bulk-request : demande à l'agent SNMP de fournir plusieurs valeurs à la fois, pour une plus grande efficacité de la communication.
- Set-request : demande à l'agent SNMP de modifier la valeur d'un objet de gestion.
- Trap : permet à l'agent SNMP d'envoyer une notification au gestionnaire SNMP en cas de détection d'un événement spécifique.

Les requêtes SNMP sont encapsulées dans des paquets SNMP qui sont envoyés via le protocole UDP (User Datagram Protocol). Les réponses aux requêtes SNMP sont renvoyées dans des paquets de réponse SNMP, également envoyés via UDP.

Les requêtes SNMP sont utilisées par les administrateurs réseau pour surveiller l'état de leur réseau et des équipements, pour détecter les pannes et les problèmes de performance, et pour effectuer des actions de gestion telles que la configuration et la mise à jour des équipements.

b) Les modes de la supervision :

Il existe plusieurs modes de supervision, qui peuvent être utilisés individuellement ou en combinaison pour surveiller les systèmes informatiques et les réseaux. Voici quelques exemples :

- **La supervision active** : elle implique l'envoi régulier de requêtes aux équipements pour vérifier leur disponibilité et leur bon fonctionnement. Cette approche est utile pour détecter les pannes et les problèmes de connectivité.
- **La supervision passive** : elle se concentre sur la collecte de données sur les équipements et les réseaux sans provoquer d'activité supplémentaire sur ceux-ci. Cette approche est utile pour surveiller l'utilisation des ressources et détecter les problèmes de performance.

2. Les solutions de supervision :

Il existe une variété d'outils de supervision disponibles, à la fois open source et propriétaires, qui sont largement utilisés.

a) Les solutions propriétaires de supervision :

Les entreprises ont souvent recours à des solutions propriétaires payantes sous licence, car elles offrent une offre globale de fonctionnalités ainsi qu'un support présent et réactif. Toutefois, ces solutions peuvent être coûteuses en termes d'acquisition et de support, et peuvent entraîner des problèmes d'incompatibilité entre les différents fournisseurs.

On peut citer :

- **IBM Tivoli Netcool** : est une solution propriétaire de supervision informatique développée par IBM. Elle est utilisée pour surveiller et gérer les performances des systèmes, des applications, des bases de données et des réseaux. La plateforme offre une variété de fonctionnalités avancées, telles que la surveillance en temps réel, la gestion des événements, la gestion de la configuration, la génération de rapports, la planification de la capacité et la prévision des pannes. Elle est également hautement extensible et peut être intégrée avec d'autres solutions IBM pour une gestion de l'IT plus globale.

- **BMC Patrol** : est une solution propriétaire de supervision de réseau et de système, largement utilisée dans les grandes entreprises pour surveiller les performances des systèmes, des applications, des bases de données et des réseaux. La plateforme offre une gamme de fonctionnalités avancées, telles que la surveillance en temps réel, la génération d'alertes, la gestion des événements, la gestion des configurations et la création de rapports. Elle est également hautement extensible et peut être intégrée avec d'autres solutions BMC pour une gestion de l'IT plus globale.

b) Les solutions propriétaires de supervision :

Il est possible d'utiliser des logiciels de supervision open source pour la surveillance informatique, et il existe plusieurs développés par différentes communautés. Ces outils sont accessibles à tous, gratuits et respectent les standards. Pour choisir l'outil de supervision le plus adapté à nos besoins, il est courant de les comparer en fonction de leurs fonctionnalités et de leur convivialité.

On peut citer :

- **Nagios** est un outil open source de supervision informatique populaire et largement utilisé pour la surveillance des systèmes, des applications, des services et des réseaux. Il utilise des plugins pour surveiller divers paramètres, tels que la disponibilité des services, la performance, les ressources utilisées, etc. Nagios génère des alertes en temps réel pour informer les administrateurs de tout problème de performance ou d'indisponibilité. Il offre également une interface web conviviale pour la configuration, la visualisation des données de surveillance et la gestion des alertes.
- **Zabbix** est un outil open source de surveillance informatique qui permet de surveiller les performances des systèmes, des applications, des réseaux et des services. Il utilise des agents installés sur les machines à surveiller pour collecter des données et générer des alertes en temps réel en cas de problème. Zabbix offre une interface web conviviale pour la configuration, la visualisation des données de surveillance, la gestion des alertes, ainsi que des fonctionnalités avancées telles que la surveillance distribuée, la planification de la capacité, la génération de rapports et la visualisation de carte de réseau. Il est également extensible et peut être intégré avec d'autres outils de surveillance et de gestion de l'IT pour une surveillance et une gestion de l'IT plus globale.

c) Installation et implémentation de Nagios :

i.Nagios XI :

Nagios XI est la version commerciale de l'outil de surveillance informatique Nagios, qui offre des fonctionnalités supplémentaires par rapport à la version open source. Il fournit une interface web plus conviviale pour la configuration, la surveillance et la gestion des alertes, ainsi qu'une console d'administration centralisée pour gérer plusieurs instances de Nagios. Il inclut également des fonctionnalités avancées telles que la planification de la capacité, la prévision des pannes, la corrélation des événements et la génération de rapports personnalisables. Nagios XI est disponible sous forme de licence et est souvent utilisé par les grandes entreprises pour une gestion de l'IT plus globale.

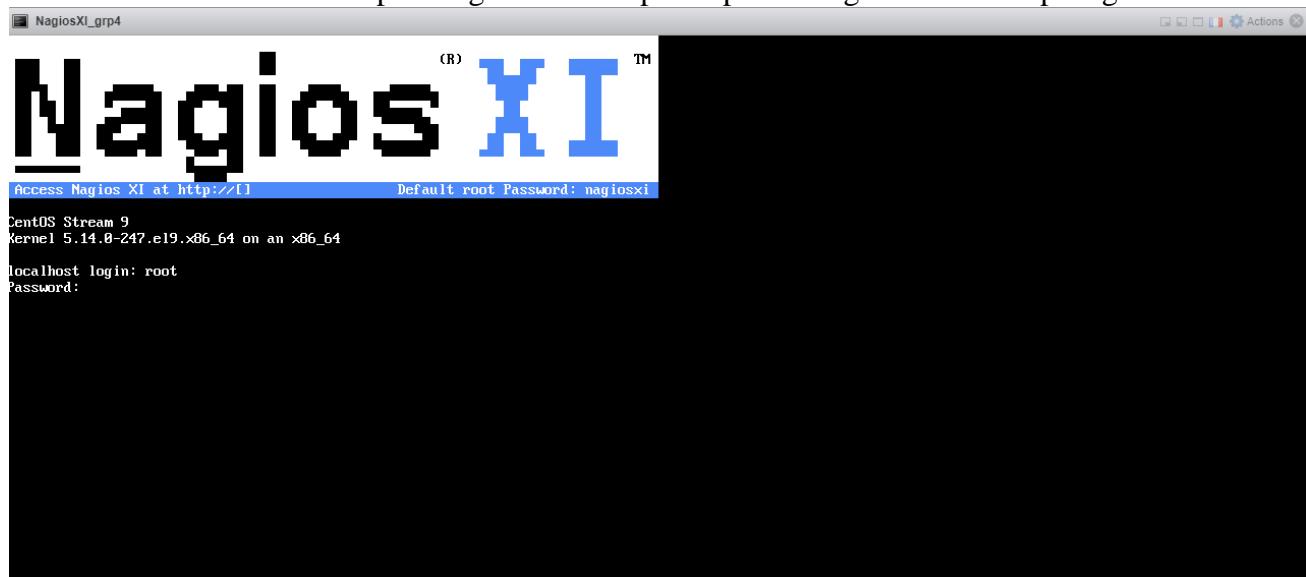


Figure 185 : Installation de Nagios XI

- Une fois que l'authentification est terminée, on peut recourir à nmtui. Cet utilitaire graphique en ligne de commande est conçu pour faciliter la configuration des interfaces réseau dans les distributions Linux.

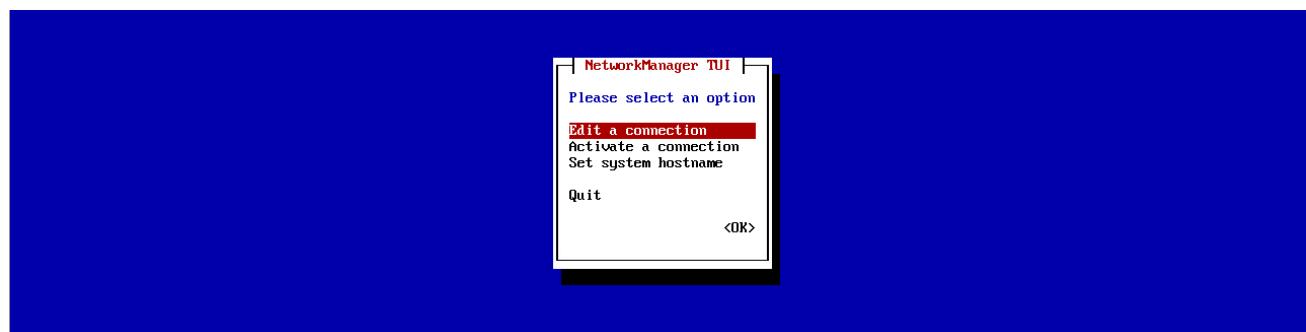


Figure 186 : Modification de la connexion

- Pour configurer l'interface, il est nécessaire d'assigner une adresse statique à celle-ci.

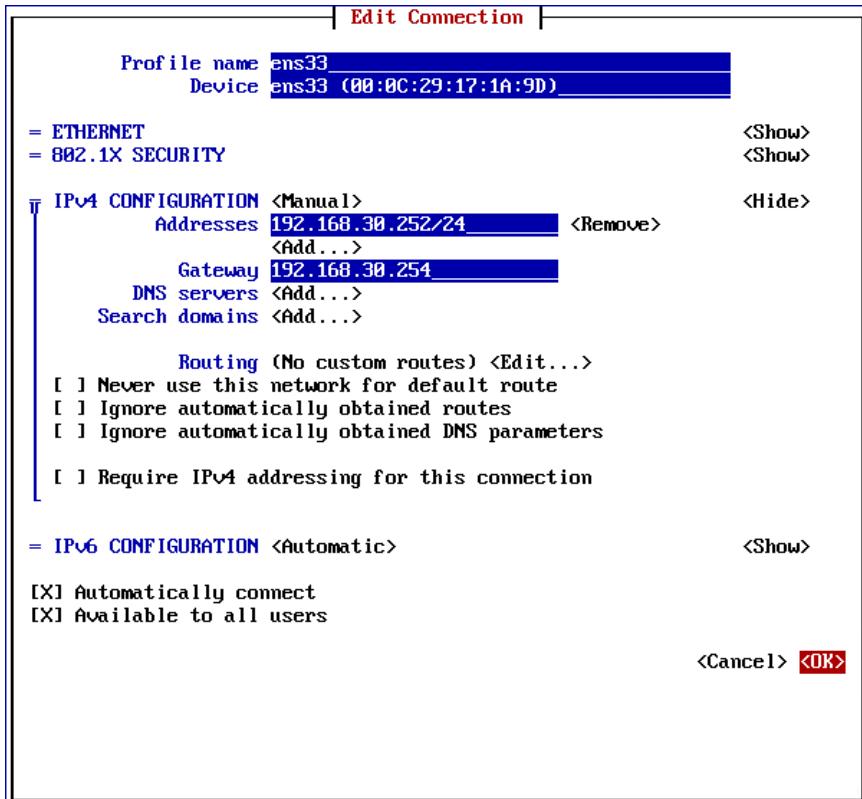


Figure 188 : Activation de la connexion

Figure 187 : Modification de l'adresse IP

- Voici la page d'accueil du configurateur Web :

Nagios® XI

Welcome

Click the link below to get started using Nagios XI.

Access Nagios XI

Check for tutorials and updates by visiting the Nagios Library at library.nagios.com.
Problems, comments, etc, should be directed to our support forum at support.nagios.com/forum/.

Figure 189 : La page d'accueil du configurateur Web

- La finalisation de l'installation Nagios :

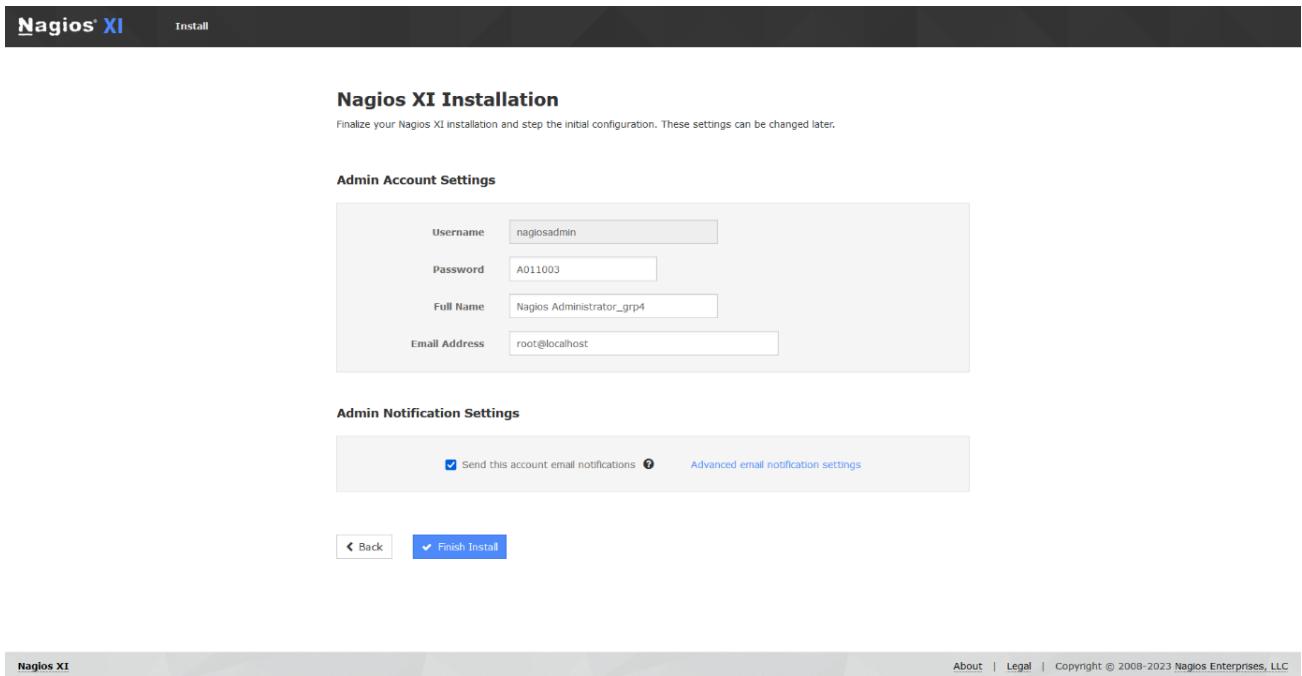


Figure 190 : La finalisation de l'installation Nagios

- Une fois exécutée, la page d'authentification s'ouvrira :

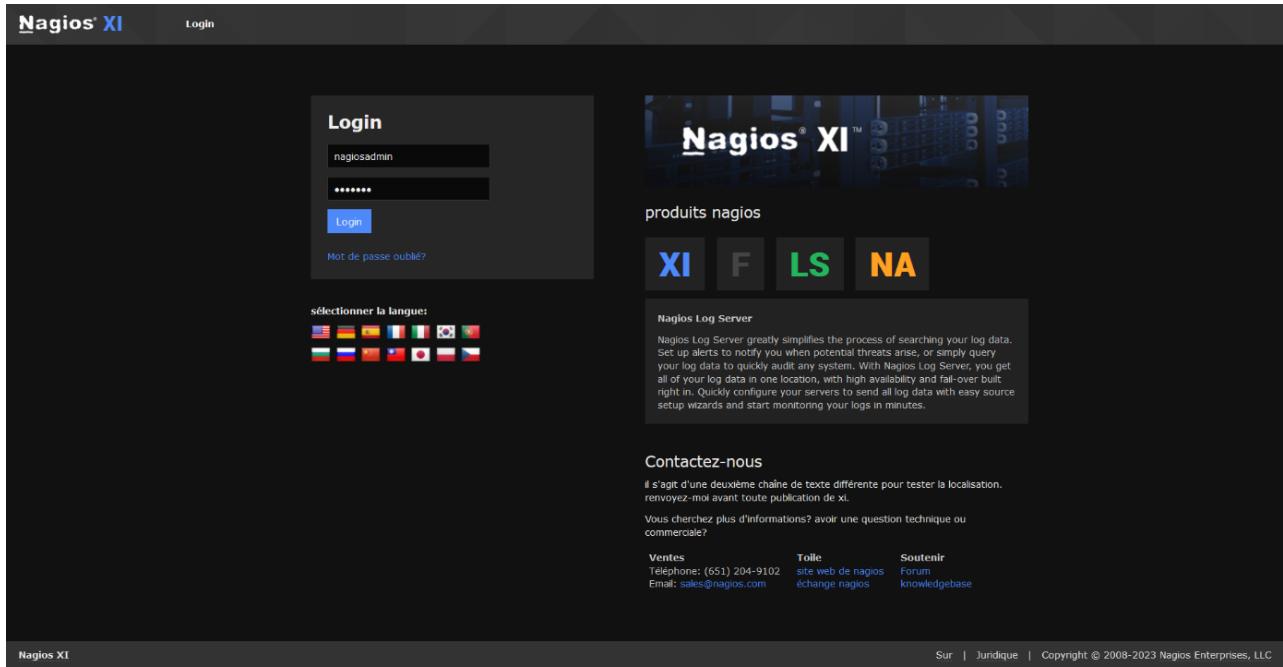


Figure 191 : La page d'authentification de Nagios XI

- Une fois que vous avez effectué la connexion, le tableau de bord s'ouvrira :

The screenshot shows the Nagios XI dashboard with the following sections:

- Vue Rapide:** Accueil Dashboard, Aperçu tactique, Birdseye, Operations Center, Operations Screen.
- Détails:** État du service, Statut d'accueil, Résumé hostgroup, Vue d'ensemble du groupe d'hôtes, Grille hostgroup, Résumé servicegroup, Servicegroup Aperçu, Servicegroup Grille, BPI, Métrique.
- Graphiques:** Graphiques sur le rendement, Graphique Explorateur.
- Cartes:** World Map, Bimap, Hypermap, Minemap, NagVis, Carte d'état du réseau.
- Accueil Dashboard:**
 - Guide de démarrage:** Tâches courantes:
 - Modifiez vos paramètres de compte
 - Changer votre mot de passe et les préférences générales.
 - Modifiez vos paramètres de notification
 - Changer comment et quand vous recevez des notifications d'alerte.
 - Configurez votre installation de surveillance
 - Ajouter ou modifier des éléments à surveiller avec facile-à-utiliser des assistants.
 Mise en route:
 - Renseignez-vous sur XI
 - En savoir plus sur XI et de ses capacités.
 - Inscrivez-vous pour les nouvelles XI
 - Rester informé des dernières mises à jour et des événements pour les XI.
 - Résumé de l'état d'accueil:** Jusqu'à Vers le bas Inaccessible En attendant

1	0	0	0
Non prise en charge	Problèmes	All	
0	0	1	

 Dernière mise à jour: 2023-03-28 09:31:15
 - Résumé de l'état de service:** Bien Avertissement Inconnu Critique En attendant

1	0	0	0	0
Non prise en charge	Problèmes	All		
0	0	12		

 Dernière mise à jour: 2023-03-28 09:31:15
 - Tâches administratives:** Tâche, Tâches de configuration initiales: Configurer les paramètres du système.
- Nous sommes là pour vous aider!** Nos techniciens expérimentés sont heureux de vous aider avec toutes les questions ou problèmes que vous pourriez avoir. Nagios se lever et courir.
- maintenant commencer à surveiller**: exécuter un assistant de configuration, Auto-Discovery emploi.

Figure 192 : Le tableau de bord de Nagios

- Ensuite, il suffit de cliquer sur l'onglet « options de configuration » et de sélectionner l'option « commencer la surveillance maintenant ».

The screenshot shows the 'Options de configuration' window with the following sections:

- Configurer:** Options de configuration.
- Accueil de configuration:** Assistants de configuration, Auto-Discovery emploi, Gérer les modèles.
- déploiement automatique:** déployer l'agent, gérer les agents déployés, paramètres de déploiement.
- Configuration avancée:** Gestionnaire de configuration de base.
- Plus d'options:** Mes Paramètres du compte, Configuration du système, Gérer les utilisateurs, Objets non configurés, Règlements Deadpool.
- Options de configuration:** choisissez ce que la façon dont vous souhaitez configurer nagios xi. à commencer tout de suite, essayez d'utiliser un assistant de configuration sous la rubrique «commencer à surveiller l'entreprise».
- déployer des agents de surveillance et configurer:** déployez rapidement ncpa (notre agent de surveillance) sur un système Linux et configuez ce que vous souhaitez surveiller. exécuter le déploiement automatique >
- maintenant commencer à surveiller:** Contrôlez rapidement un nouvel appareil, serveur, application ou service utilisant un assistant de configuration facile. exécuter un assistant de configuration >
- Auto-Discovery emploi:** exécuter un travail d'auto-découverte pour trouver automatiquement le matériel, les appareils et les services à surveiller. utiliser l'outil d'auto-découverte >
- Configuration avancée:** gérer vos fichiers de configuration de surveillance à l'aide d'une interface Web avancée. recommandée pour les utilisateurs expérimentés. Responsable Nagios Config de base >
- Mes Paramètres du compte:** Modifiez vos informations de compte, les préférences et les paramètres de notification. modifier vos paramètres de profil >

Figure 193 : La fenêtre "Options de configuration"

Tous les matériaux suivent les mêmes étapes, la seule variation est l'adresse IP.

- Une fois que l'option « commencer la surveillance maintenant » est sélectionnée, il convient de choisir l'assistant de configuration approprié.

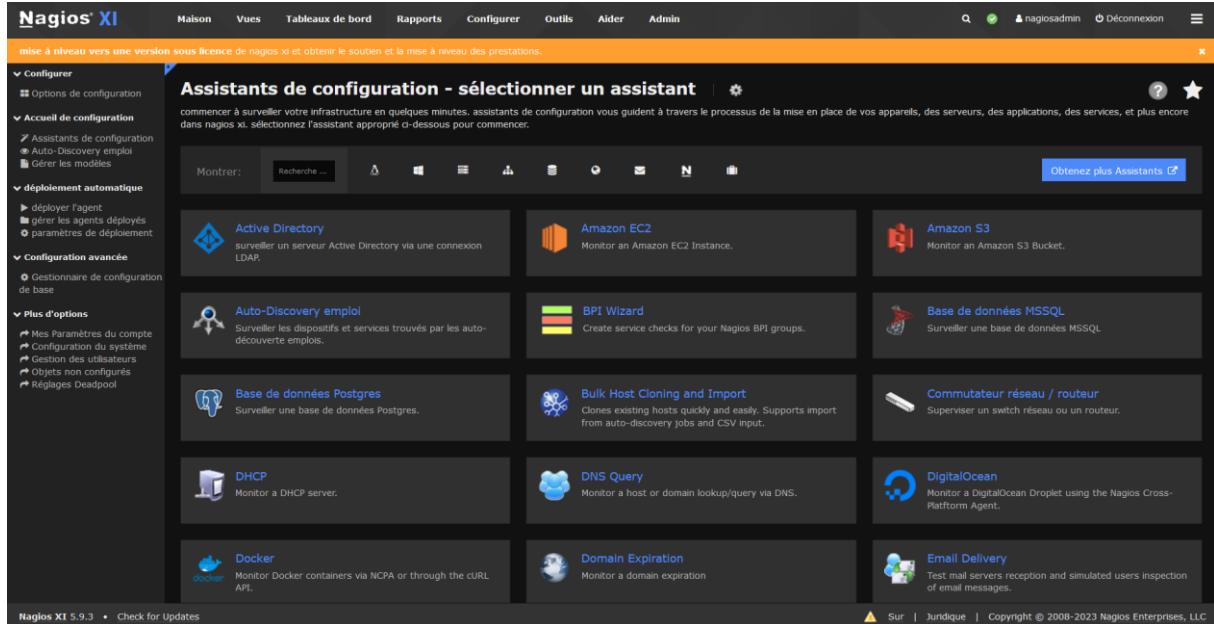


Figure 194 : La sélection de l'assistant de supervision

II. Supervision des matériaux :

1. Supervision du Switch :

L'exécution de cette commande ci-dessous permet d'activer le service SNMP dans le switch :

```
Switch_GRP4(config)#snmp-server community public RO
```

Figure 195 : Le démarrage du service SNMP

Configuration du switch :

```
interface Vlan30
  ip address 192.168.30.253 255.255.255.0
!
interface Vlan40
  ip address 192.168.40.253 255.255.255.0
!
interface Vlan50
  ip address 172.120.1.0 255.255.0.0
!
ip classless
ip http server
ip http secure-server
!
!
!
snmp-server community public RO
!
control-plane
!
```

Figure 196 : Configuration du Switch

- Ensuite, il est nécessaire de saisir l'adresse IP, le port, la version et la communauté SNMP.

Nagios® XI

Maison Vues Tableaux de bord Rapports Configurer Outils Aider Admin

mise à niveau vers une version sous licence de nagios xi et obtenir le soutien et la mise à niveau des prestations.

Assistants de configuration: Commutateur réseau / routeur - étape 1

routeur / switch informations

Adresse IP: 192.168.30.253

Port: 161

SNMPv1 SNMPv2c SNMPv3

Communauté: public

Démons de surveillance

surveiller à l'aide: Numéro de port

Numérisation Interfaces

interfaces administrativement désactivées

Appliquer la configuration

Figure 197 : La saisie de l'adresse IP- Supervision du Switch

- Après la saisie de l'adresse IP, le logiciel Nagios utilise le protocole SNMP pour détecter les ports du switch.

Port Vérifier / Décachez	Nom du port	Description du Port	alias de port	Vitesse maximale	Description du service	Bande passante Vérifier / Décachez	État du port Vérifier / Décachez
<input checked="" type="checkbox"/> Port1	Vl1	Vlan1	Vlan1	1.00 Gbps	Port1	<input checked="" type="checkbox"/> En taux de: Taux Out: 500.0 Avertissement: 500.0 Critique: 800.0 <input type="button" value="800.0 Mbps"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Port10	Vl10	Vlan10	Vlan10	1.00 Gbps	Port10	<input checked="" type="checkbox"/> En taux de: Taux Out: 500.0 Avertissement: 500.0 Critique: 800.0 <input type="button" value="800.0 Mbps"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Port20	Vl20	Vlan20	Vlan20	1.00 Gbps	Port20	<input checked="" type="checkbox"/> En taux de: Taux Out: 500.0 Avertissement: 500.0 Critique: 800.0 <input type="button" value="800.0 Mbps"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Port30	Vl30	Vlan30	Vlan30	1.00 Gbps	Port30	<input checked="" type="checkbox"/> En taux de: Taux Out: 500.0 Avertissement: 500.0 Critique: 800.0 <input type="button" value="800.0 Mbps"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Port40	Vl40	Vlan40	Vlan40	1.00 Gbps	Port40	<input checked="" type="checkbox"/> En taux de: Taux Out: 500.0 Avertissement: 500.0 Critique: 800.0 <input type="button" value="800.0 Mbps"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Port50	Vl50	Vlan50	Vlan50	1.00 Gbps	Port50	<input checked="" type="checkbox"/> En taux de: Taux Out: 500.0 Avertissement: 500.0 Critique: 800.0 <input type="button" value="800.0 Mbps"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Port5182	StackPort2	StackPort2	StackPort2	100.00 Mbps	Port5182	<input checked="" type="checkbox"/> En taux de: Taux Out: 50.00 Avertissement: 50.00 Critique: 80.00 <input type="button" value="80.00 Mbps"/>	<input checked="" type="checkbox"/>

Figure 198 : Détection des ports du Switch

Voici l'état des services du switch :

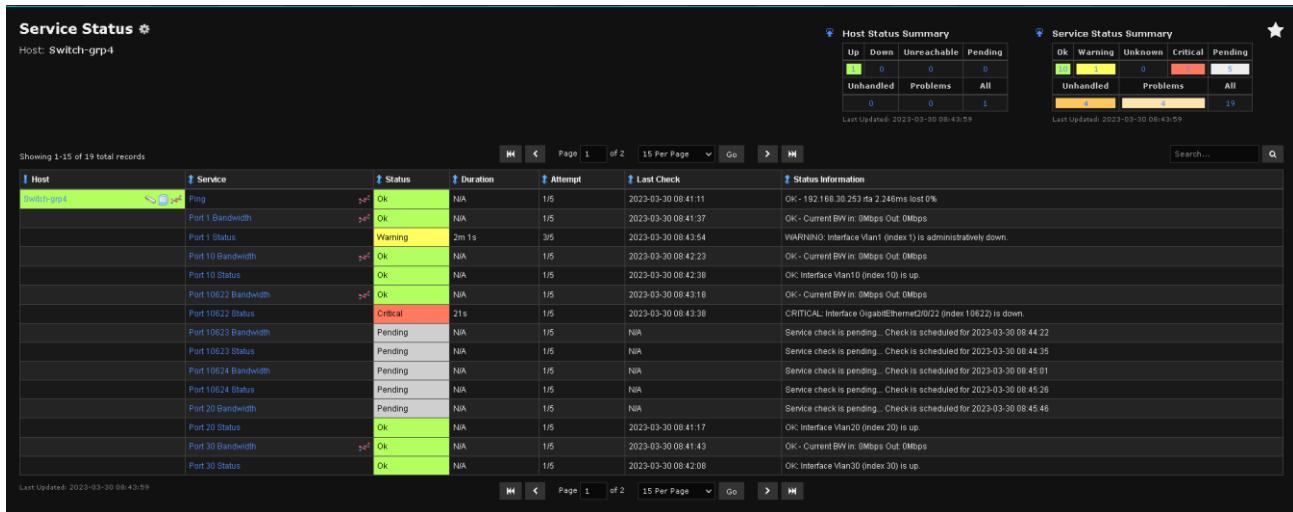


Figure 199 : L'état des services du Switch

2. Supervision du routeur :

L'exécution de cette commande ci-dessous permet d'activer le service SNMP dans le routeur :

```
Router#snmp-server community public RO
```

Figure 200 : L'activation de service SNMP dans le routeur

```
!
!
!
no ip http server
no ip http secure-server
!
snmp-server community public RO
!
!
```

Figure 201 : Le service SNMP est activé dans le routeur

Configuration du routeur :

```
!
interface FastEthernet0
 ip address 192.168.0.254 255.255.255.0
 duplex auto
 speed auto
!
```

Figure 202 : Configuration du routeur

- Après cela, il est essentiel de saisir l'adresse IP, le port, la version et la communauté SNMP.

Nagios XI

Maison Vues Tableaux de bord Rapports Configurer Outils Aider Admin

mise à niveau vers une version sous licence de nagios xi et obtenir le soutien et la mise à niveau des prestations.

Configurer Options de configuration Accueil de configuration Assistants de configuration Auto-Discovery emploi Gérer les modèles déploiement automatique déployer l'agent gérer les agents déployés paramètres de déploiement Configuration avancée Gestionnaire de configuration de base Plus d'options Mes Paramètres du compte Configuration du système Gestion des utilisateurs Objets non configurés Réglages Deadpool

Assistants de configuration: Commutateur réseau / routeur - étape 1

routeur / switch informations

Adresse IP: (pointeur)

L'adresse IP de l'appareil que vous souhaitez surveiller.

Port:

le port de dispositif de réseau

SNMPv1 SNMPv2c SNMPv3

Communauté SNMP:

La chaîne de communauté SNMP utilisée pour nécessaire d'interroger le périphérique.

Démons de surveillance

surveiller à l'aide: Sélectionnez le schéma de nommage port qui doit être utilisé.

Numérisation Interfaces balayer le commutateur ou un routeur de détecter automatiquement les interfaces qui peuvent être surveillées pour le lien haut / bas statut et la bande passante. l'analyse de interfaces administrativement désactivées Scannez le commutateur ou un routeur de détecter automatiquement les interfaces qui peuvent être surveillées pour la liaison haut / bas statut et la bande passante.

Figure 203 : La saisie de l'adresse IP- Supervision du routeur

- Une fois que l'adresse IP a été saisie, le logiciel Nagios utilise le protocole SNMP pour repérer les ports du routeur.

Nagios XI

Maison Vues Tableaux de bord Rapports Configurer Outils Aider Admin

mise à niveau vers une version sous licence de nagios xi et obtenir le soutien et la mise à niveau des prestations.

Configurer Options de configuration Accueil de configuration Assistants de configuration Auto-Discovery emploi Gérer les modèles déploiement automatique déployer l'agent gérer les agents déployés paramètres de déploiement Configuration avancée Gestionnaire de configuration de base Plus d'options Mes Paramètres du compte Configuration du système Gestion des utilisateurs Objets non configurés Réglages Deadpool

Port	Nom	Type	Vitesse	Port	Moniteur	En taux de Taux Out:	En taux de Taux Out:	Critique:	En taux de Taux Out:	En taux de Taux Out:	Critique:	
Port3	No Name 5	BRI0	BRI0	16.00 Kbps	Port3	<input checked="" type="checkbox"/>	En taux de Taux Out: 8.00	8.00	Critique: 12.80	En taux de Taux Out: 12.80	12.80	Kbps
Port4	No Name 2	BRI0:1	BRI0:1	64.00 Kbps	Port4	<input checked="" type="checkbox"/>	En taux de Taux Out: 32.00	32.00	Critique: 51.20	En taux de Taux Out: 51.20	51.20	Kbps
Port5	No Name 4	BRI0:2	BRI0:2	64.00 Kbps	Port5	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port6	Fa2	FastEthernet2	FastEthernet2	100.00 Mbps	Port6	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port7	Fa3	FastEthernet3	FastEthernet3	100.00 Mbps	Port7	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port8	Fa4	FastEthernet4	FastEthernet4	100.00 Mbps	Port8	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port9	Fa5	FastEthernet5	FastEthernet5	100.00 Mbps	Port9	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port10	Fa6	FastEthernet6	FastEthernet6	100.00 Mbps	Port10	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port11	Fa7	FastEthernet7	FastEthernet7	100.00 Mbps	Port11	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port12	Fa8	FastEthernet8	FastEthernet8	100.00 Mbps	Port12	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port13	Fa9	FastEthernet9	FastEthernet9	100.00 Mbps	Port13	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port15	Vl1	Vlan1	Vlan1	100.00 Mbps	Port15	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port17	No Name 6	BRI0-Signaling	BRI0-Signaling	16.00 Kbps	Port17	<input checked="" type="checkbox"/>	En taux de Taux Out: 8.00	8.00	Critique: 12.80	En taux de Taux Out: 12.80	12.80	Kbps
Port20	Fa0.10	FastEthernet0.10	FastEthernet0.10	100.00 Mbps	Port20	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port21	Fa0.20	FastEthernet0.20	FastEthernet0.20	100.00 Mbps	Port21	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps
Port22	Fa0.30	FastEthernet0.30	FastEthernet0.30	100.00 Mbps	Port22	<input checked="" type="checkbox"/>	En taux de Taux Out: 50.00	50.00	Critique: 80.00	En taux de Taux Out: 80.00	80.00	Mbps

Figure 204 : Détection des ports du routeur

Voici l'état actuel des services du routeur :

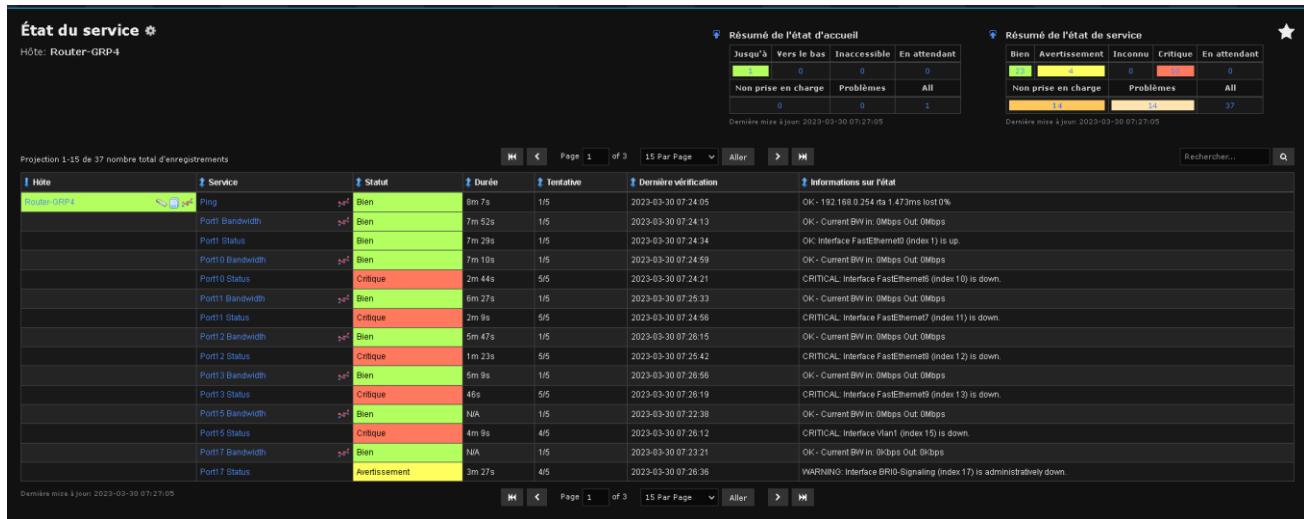


Figure 205 : L'état des services du routeur

3. Supervision de firewall :

Ensuite, il est nécessaire de saisir l'adresse IP, le port, la version et la communauté SNMP.

Figure 206 : La saisie de l'adresse IP- Supervision du Firewall

- Une fois que l'adresse IP a été saisie, le logiciel Nagios utilise le protocole SNMP pour afficher les ports du routeur.

Configuration Wizard: Network Switch / Router - Step 2

Switch Details

Switch/Router Address: 192.168.40.99

Host Name: Firewall-grp4

Services

Specify which services you'd like to monitor for the switch or router.

Ping Monitors the switch/router with an ICMP ping. Useful for watching network latency and general uptime.

Bandwidth and Port Status

Select the ports for which you'd like to monitor bandwidth and port status. You may specify an optional port name to be associated with specific ports.

Port Check / Uncheck	Port Name	Port Description	Port Alias	Max Speed	Service Description	Bandwidth Check / Uncheck	Port Status Check / Uncheck
<input checked="" type="checkbox"/>	wan1	wan1	wan1	10.49 Mbps	Port 1	<input checked="" type="checkbox"/> Rate In: Rate Out: 5.24 Mbps Warning: 5.24 Critical: 8.39 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	wan2	wan2	wan2	10.49 Mbps	Port 2	<input checked="" type="checkbox"/> Rate In: Rate Out: 5.24 Mbps Warning: 5.24 Critical: 8.39 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	dmz1	dmz1	dmz1	10.49 Mbps	Port 3	<input checked="" type="checkbox"/> Rate In: Rate Out: 5.24 Mbps Warning: 5.24 Critical: 8.39 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	dmz2	dmz2	dmz2	10.49 Mbps	Port 4	<input checked="" type="checkbox"/> Rate In: Rate Out: 5.24 Mbps Warning: 5.24 Critical: 8.39 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	modem	modem	modem	100.00 Mbps	Port 5	<input checked="" type="checkbox"/> Rate In: Rate Out: 50.00 Mbps Warning: 50.00 Critical: 80.00 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	ssl.root	ssl.root	ssl.root	100.00 Mbps	Port 6	<input checked="" type="checkbox"/> Rate In: Rate Out: 50.00 Mbps Warning: 50.00 Critical: 80.00 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	internal1	internal1	internal1	104.86 Mbps	Port 7	<input checked="" type="checkbox"/> Rate In: Rate Out: 52.43 Mbps Warning: 52.43 Critical: 83.89 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>						<input checked="" type="checkbox"/> Rate In: Rate Out: 52.43 Mbps Warning: 52.43 Critical: 83.89 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>						<input checked="" type="checkbox"/> Rate In: Rate Out: 52.43 Mbps Warning: 52.43 Critical: 83.89 Mbps	<input checked="" type="checkbox"/>

Figure 207 : Détection des ports du Firewall 1

Configuration Wizard: Network Switch / Router - Step 2

Services

Specify which services you'd like to monitor for the switch or router.

Ping Monitors the switch/router with an ICMP ping. Useful for watching network latency and general uptime.

Bandwidth and Port Status

Select the ports for which you'd like to monitor bandwidth and port status. You may specify an optional port name to be associated with specific ports.

Port Check / Uncheck	Port Name	Port Description	Port Alias	Max Speed	Service Description	Bandwidth Check / Uncheck	Port Status Check / Uncheck
<input checked="" type="checkbox"/>	wan1	wan1	wan1	10.49 Mbps	Port 1	<input checked="" type="checkbox"/> Rate In: Rate Out: 5.24 Mbps Warning: 5.24 Critical: 8.39 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	wan2	wan2	wan2	10.49 Mbps	Port 2	<input checked="" type="checkbox"/> Rate In: Rate Out: 5.24 Mbps Warning: 5.24 Critical: 8.39 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	dmz1	dmz1	dmz1	10.49 Mbps	Port 3	<input checked="" type="checkbox"/> Rate In: Rate Out: 5.24 Mbps Warning: 5.24 Critical: 8.39 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	dmz2	dmz2	dmz2	10.49 Mbps	Port 4	<input checked="" type="checkbox"/> Rate In: Rate Out: 5.24 Mbps Warning: 5.24 Critical: 8.39 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	modem	modem	modem	100.00 Mbps	Port 5	<input checked="" type="checkbox"/> Rate In: Rate Out: 50.00 Mbps Warning: 50.00 Critical: 80.00 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	ssl.root	ssl.root	ssl.root	100.00 Mbps	Port 6	<input checked="" type="checkbox"/> Rate In: Rate Out: 50.00 Mbps Warning: 50.00 Critical: 80.00 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	internal1	internal1	internal1	104.86 Mbps	Port 7	<input checked="" type="checkbox"/> Rate In: Rate Out: 52.43 Mbps Warning: 52.43 Critical: 83.89 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	internal2	internal2	internal2	104.86 Mbps	Port 8	<input checked="" type="checkbox"/> Rate In: Rate Out: 52.43 Mbps Warning: 52.43 Critical: 83.89 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	internal3	internal3	internal3	104.86 Mbps	Port 9	<input checked="" type="checkbox"/> Rate In: Rate Out: 52.43 Mbps Warning: 52.43 Critical: 83.89 Mbps	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	internal4	internal4	internal4	104.86 Mbps	Port 10	<input checked="" type="checkbox"/> Rate In: Rate Out: 52.43 Mbps Warning: 52.43 Critical: 83.89 Mbps	<input checked="" type="checkbox"/>

Figure 208 : Détection des ports du Firewall 2

Voici l'état des services du Firewall :

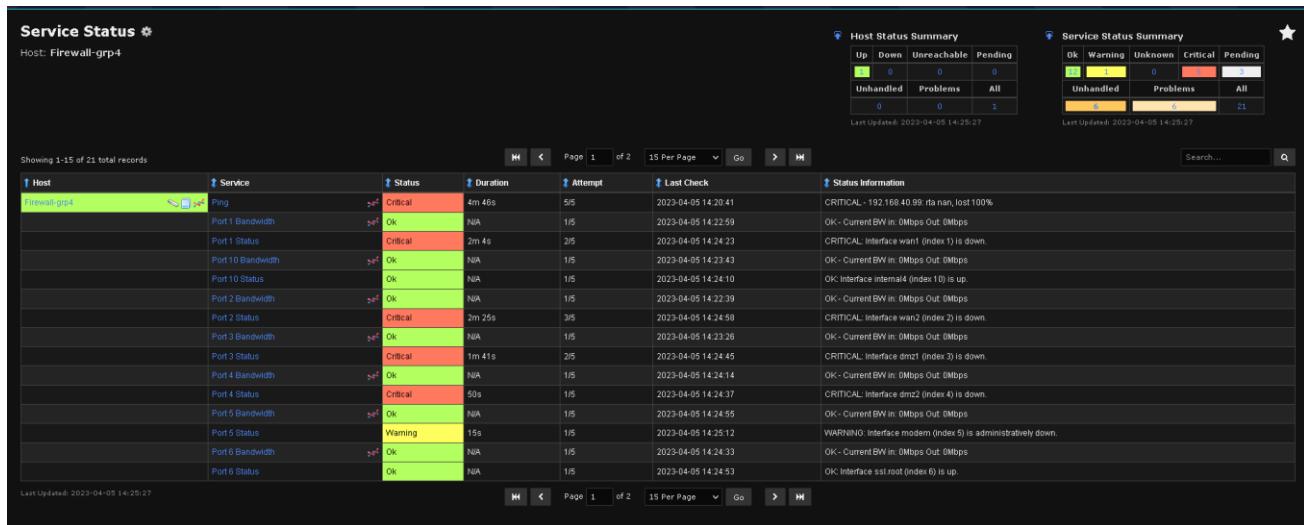


Figure 209 : L'état des services du Firewall

III. Supervision des machines :

1. Windows Serveur :

Dans la fenêtre « Rôles de serveurs », cochez la case correspondant à « Services Bureau à distance ».

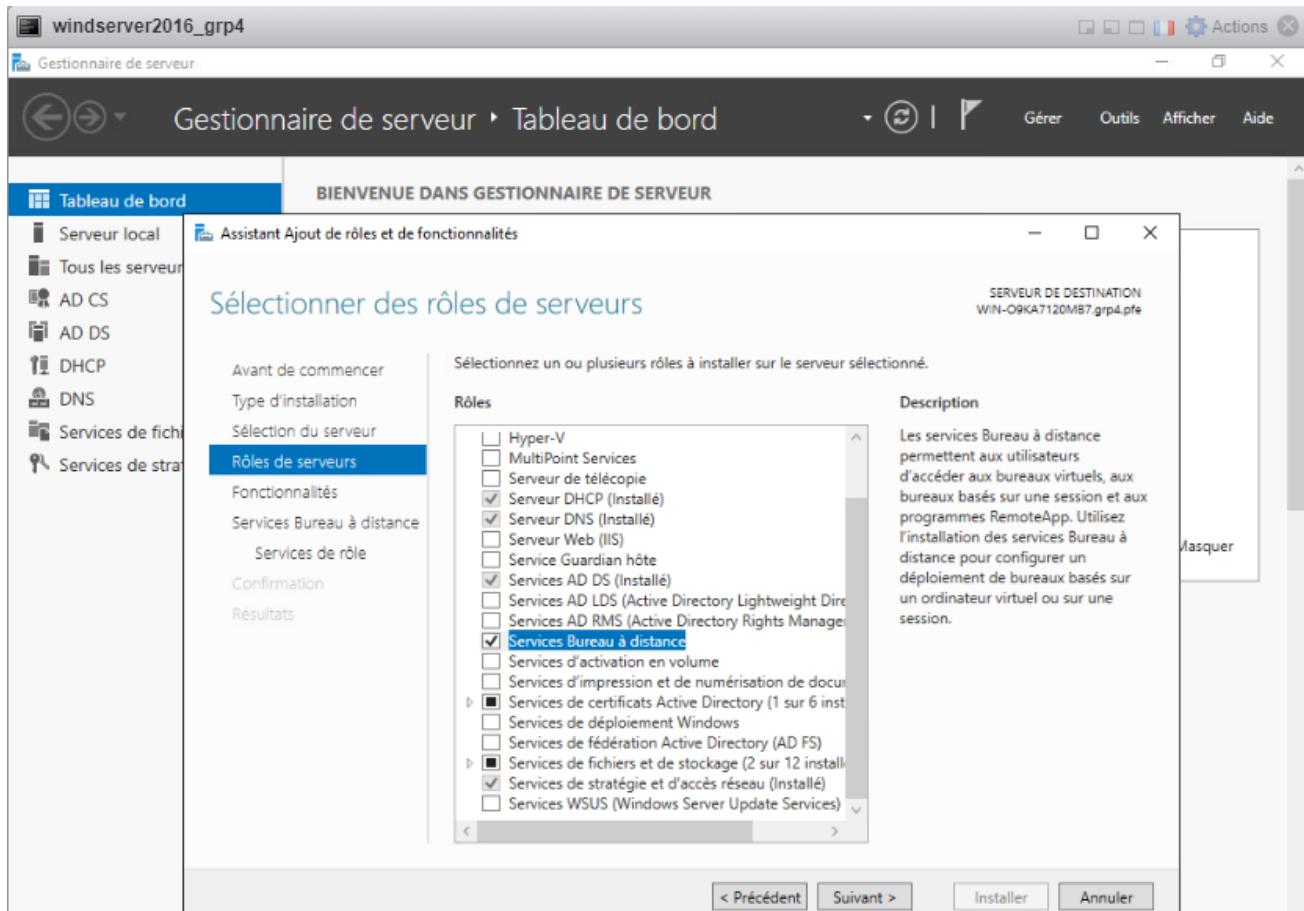


Figure 210 : L'activation de "services Bureau à distance"

- Ensuite, vous cochez « Fournisseur WMI SNMP ».

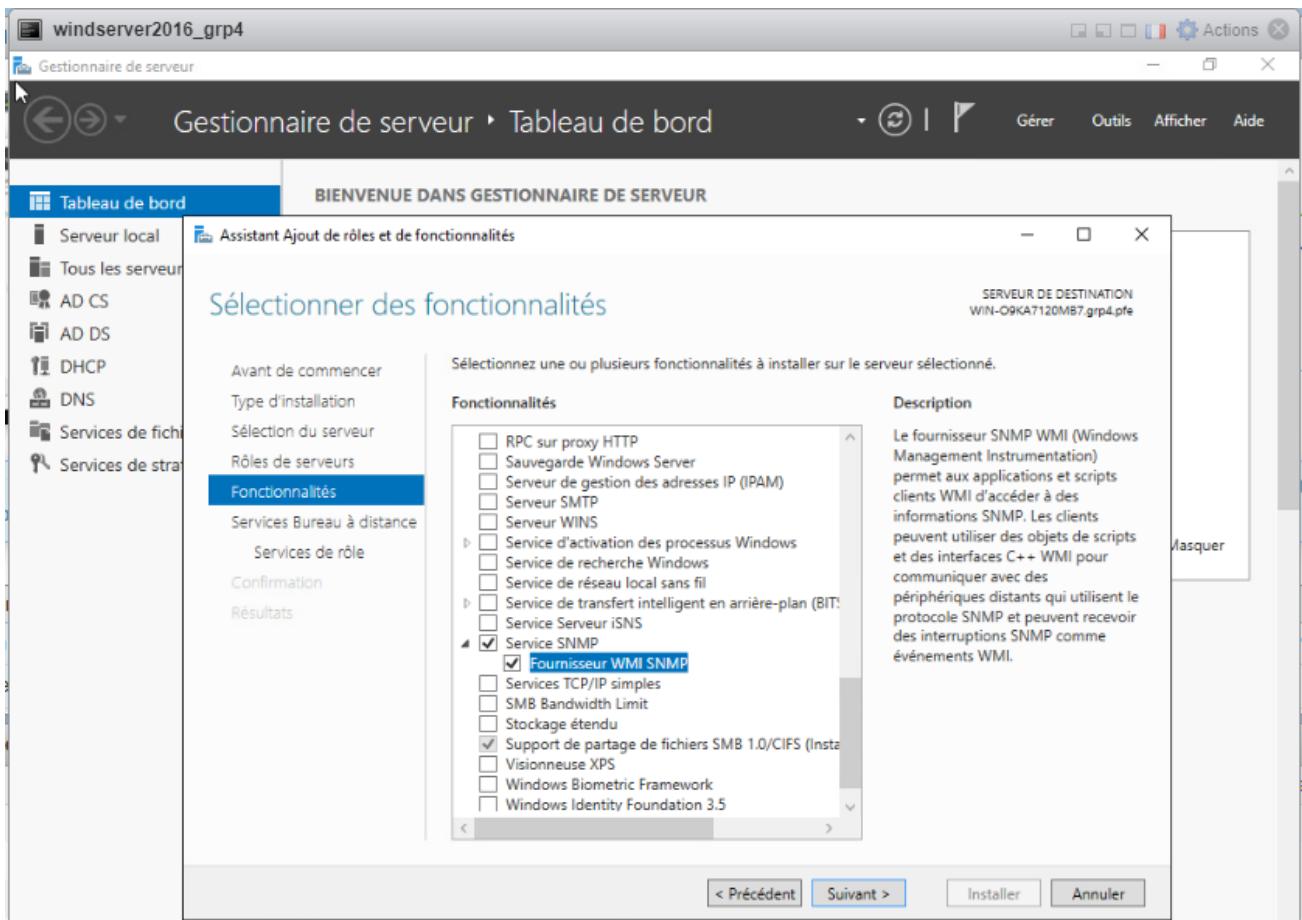


Figure 211 : L'activation du "Fournisseur WMI SNMP"

- Ensuite, une synthèse des options apparaît pour valider vos choix.

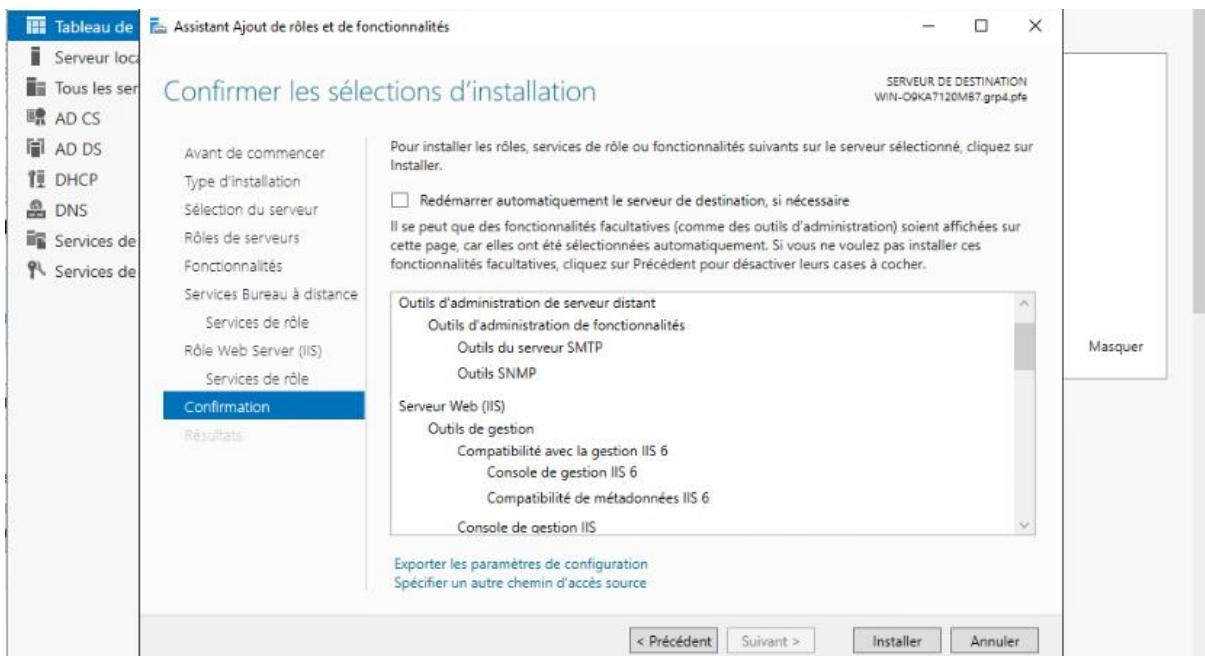


Figure 212 : Confirmation des sélection d'installation

Dans la fenêtre « Services », on accède au « Propriétaires de service SNMP » et on ajoute l'adresse du serveur Nagios qui est dans notre cas : « 192.168.30.252 » et on l'autorise la lecture seulement.

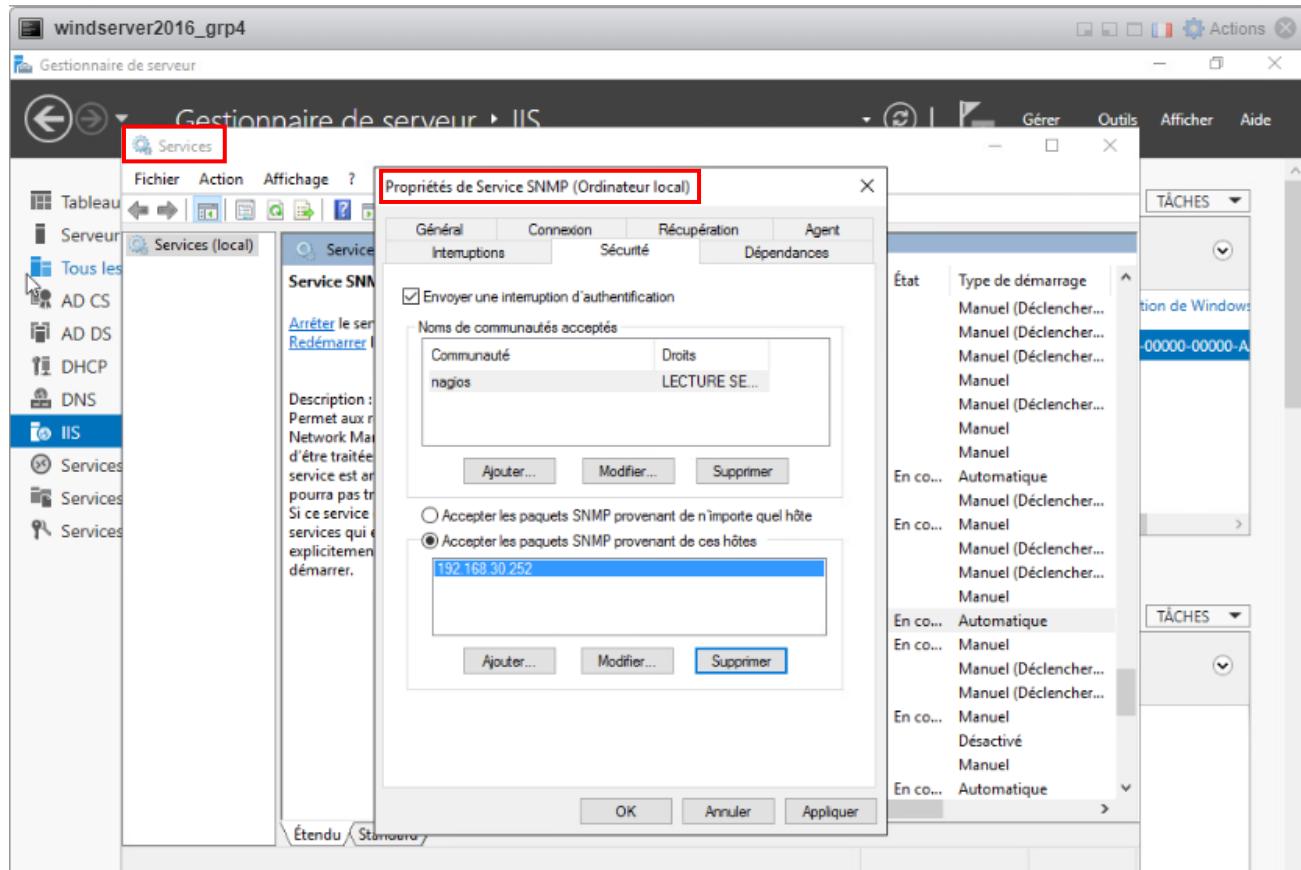


Figure 213 : Propriétaires de service SNMP

Puis, il faut saisir l'adresse IP de notre machine Windows Serveur :

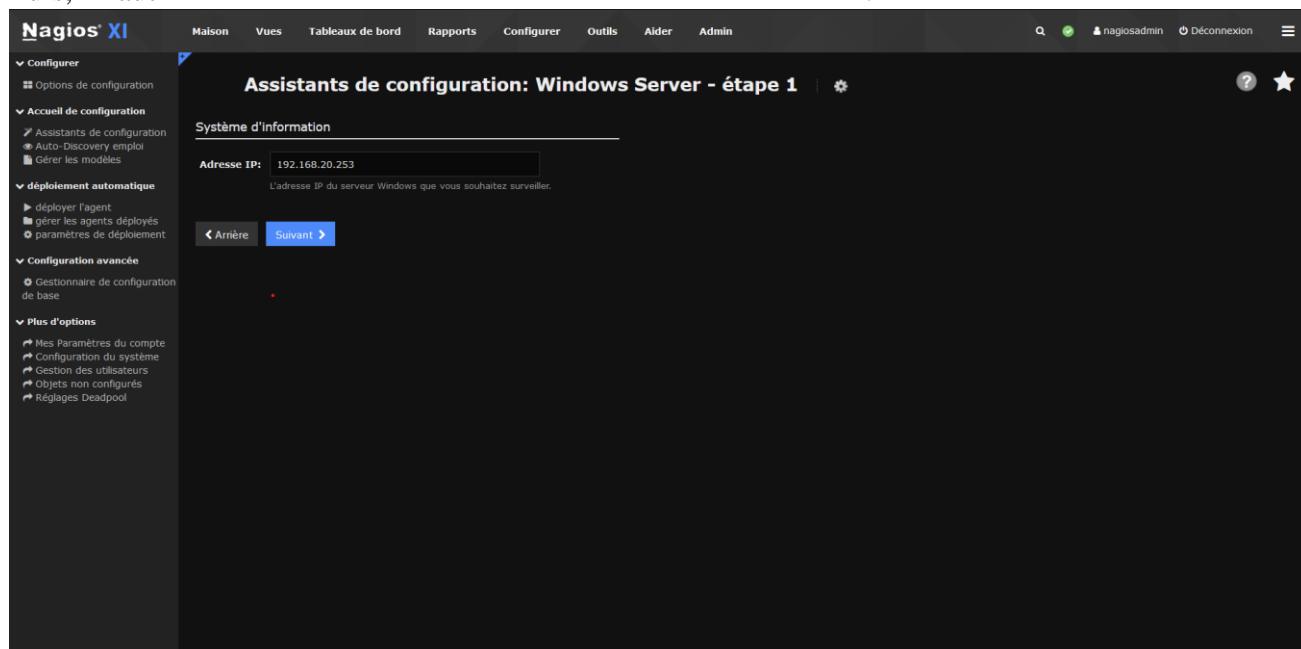


Figure 214 : La saisie de l'adresse IP- Supervision de Windows Server

- La première étape consiste à se connecter à NCPA, lors de la connexion un jeton est demandé, ce dernier permet l'authentification à l'agent NCPA de notre machine à distance.

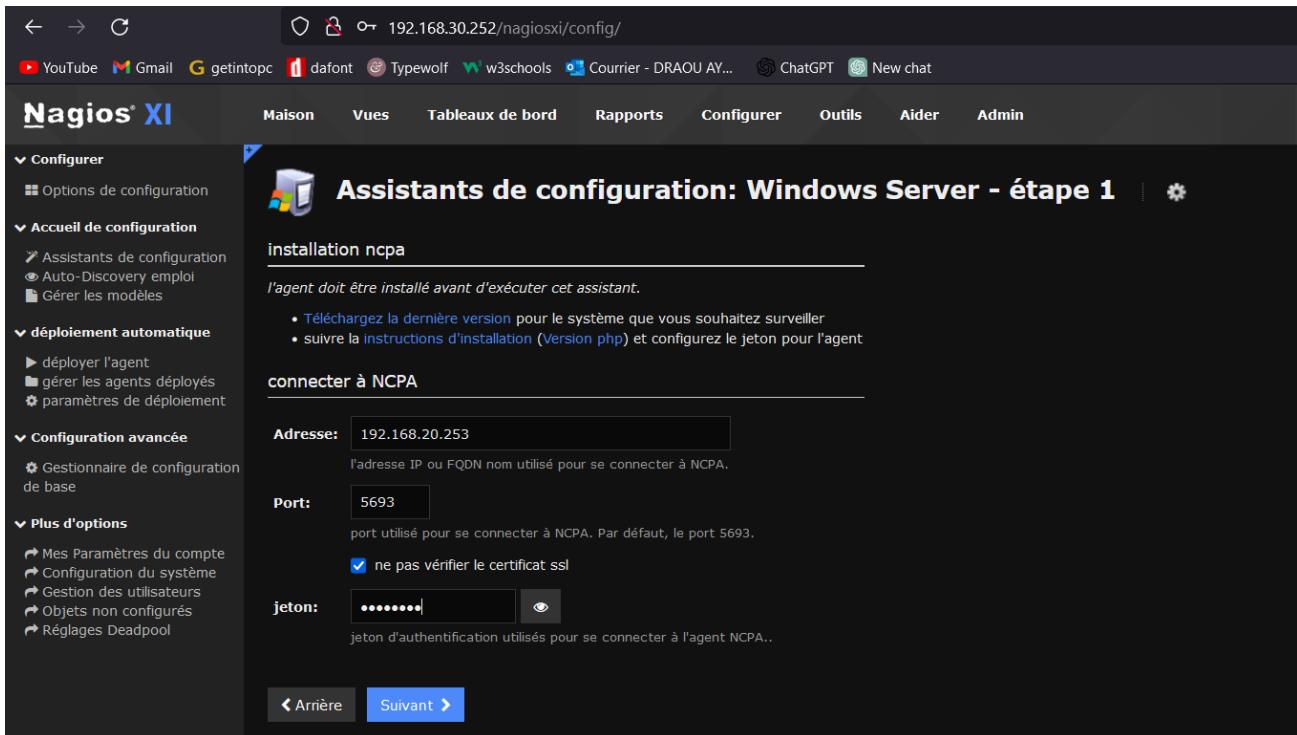


Figure 215 : Authentification NCPA

- Puis, il faut choisir les services qu'on va superviser :

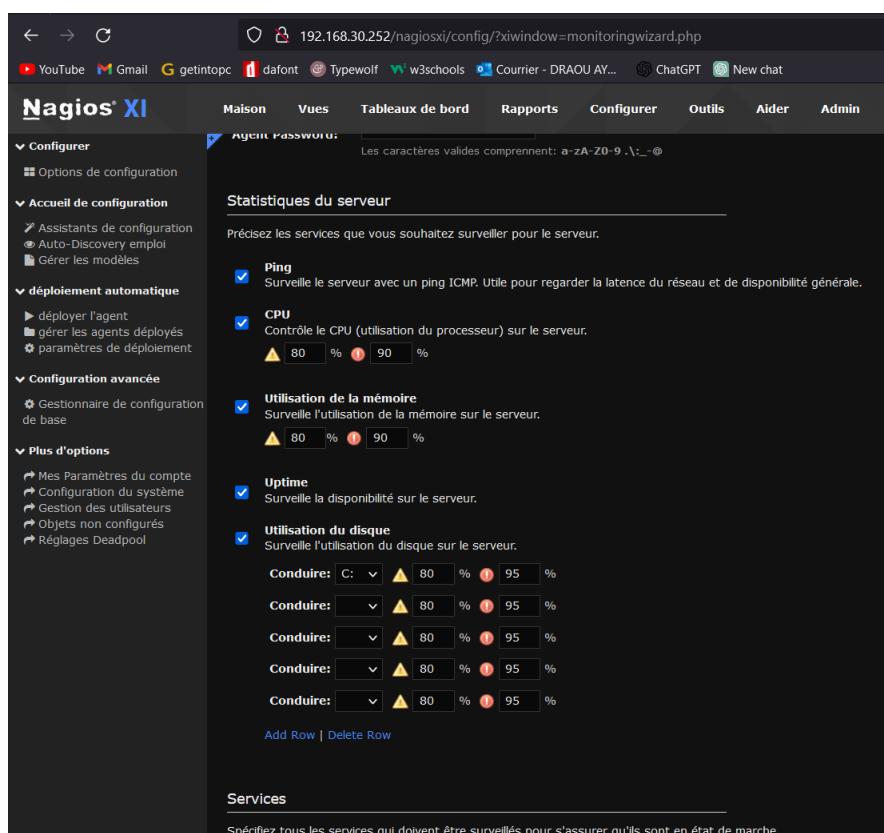


Figure 216 : Les services qu'on va superviser

Voici l'état des services du Windows Server :

The screenshot shows the Nagios XI interface for monitoring a Windows Server 2016 host. Key sections include:

- Etat du service**: Shows the host status as "Windows-server 2016".
- Résumé de l'état d'accueil**: Status counts: Jusqu'à (1), Vers le bas (0), Inaccessible (0), En attendant (0). Non prise en charge (0), Problèmes (Problèmes), All (All).
- Résumé de l'état de service**: Status counts: Bien (3), Avertissement (0), Inconnu (0), Critique (0), En attendant (0). Non prise en charge (0), Problèmes (Problèmes), All (All).
- Tableau de bord**: Shows a projection of 1-5 of 5 total records for service status.
- Détails des services**: A table listing services with their status, duration, and last check time. Services listed include CPU Usage, Drive C: Disk Usage, Memory Usage, Ping, and Uptime.

Figure 217 : L'état des services du Windows Server

2. PfSense :

L'activation de protocole SNMP sur notre machine PfSense.

The screenshot shows the Pfsense configuration interface for the SNMP Daemon. Key settings include:

- SNMP Daemon**: Enabled (checked).
- SNMP Daemon Settings**: Polling Port set to 161. System Location is set to "salle". System Contact is set to "admin". Read Community String is set to "public".
- SNMP Traps Enable**: Enabled (unchecked).
- SNMP Modules**: Several modules are selected: MibII, Netgraph, PF, Host Resources, UCD, and Regex.
- Interface Binding**: Internet Protocol is set to IPv4. Bind Interfaces include All, WAN, and LAN.

Figure 218 : L'activation de protocole SNMP

- Ensuite, il faut saisir l'adresse IP de la machine Pfsense.

The screenshot shows the Nagios XI interface with the title "Configuration Wizard: SNMP - Step 1". On the left, there's a sidebar with various configuration options like "Configuration Options", "Auto-Discovery", and "Deployment Settings". The main panel is titled "SNMP Information" and contains a "Device Address" field with the value "192.168.10.252". Below the field is a note: "The IP address or fully qualified DNS name of the server or device you'd like to monitor." At the bottom, there are "Back" and "Next >" buttons.

Figure 219 : La saisie de l'adresse IP de la machine Pfsense

- Une fois que l'adresse IP a été saisie, le logiciel Nagios utilise le protocole SNMP pour afficher les ports et les services de la machine Pfsense.

The screenshot shows the Nagios XI interface with the title "Configuration Wizard: SNMP - Step 2". The sidebar remains the same. The main panel has sections for "Device Details" (Host Name: "pfsense-grp4") and "SNMP Settings" (SNMP Version: "2c", SNMP Port: "161"). Below these are sections for "SNMP Version Settings" (SNMP Community: "public") and "SNMP Services". The "SNMP Services" section contains a table with several rows of monitoring configurations. The table columns are: OID, Display Name, Data Label, Data Units (Optional), Match Type, Warning Range, Critical Range, String To Match, and MIB To Use. Some entries include checkboxes and dropdown menus.

Figure 220 : Détection des ports et des services de Pfsense

Voici l'état des services du Pfsense :

Host Status Summary				Service Status Summary			
Up	Down	Unreachable	Pending	Ok	Warning	Unknown	Critical
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	2

Last Updated: 2023-03-31 08:21:07 Last Updated: 2023-03-31 08:21:07

Host	Service	Status	Duration	Attempt	Last Check	Status Information
pfsense-grp4	Port1 Status	OK	N/A	1/5	2023-03-31 08:20:39	SNMP OK - up(t)
	Uptime	Ok	N/A	1/5	2023-03-31 08:21:04	SNMP OK - Timeticks: (62572) 0:10:25.72

Figure 221 : L'état des services du Pfsense

3. Linux Server :

Dans le fichier « snmpd.conf » situé dans le répertoire « /etc/snmp », on décommente la ligne « rocommunity public », puis il faut saisir l'adresse du serveur Nagios dans la même ligne.

```

File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/snmp/snmpd.conf          Modified

#
# system + hrSystem groups on $ 
view systemonly included .1.3.6.1.2.1.1
view systemonly included .1.3.6.1.2.1.25.1

rocommunity public 192.168.30.252          # Full access from the local $ 
# Default access to basic sys$ 
# rocommunity6 is for IPv6
# Full access from an example$ 
# Adjust this network addr$ 
# settings, change the com$ 
# and check the 'agentAddr$ 

#rocommunity secret 10.0.0.0/16

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace ^U Uncut Text^T To Spell ^_ Go To Line

```

Figure 222 : Supervision de Linux Server

a) Web server :

- Ensuite, il faut saisir l'adresse IP de la machine Linux Server.

The screenshot shows the Nagios XI Configuration Wizard for setting up a Linux SNMP monitoring. The main title is "Configuration Wizard: Linux SNMP - Step 1". The left sidebar contains navigation links for Configuration, Configuration Tools, Auto Deployment, Advanced Configuration, and More Options. The main content area is titled "Linux Machine Information" and shows the IP Address as 172.120.1.101. Below it is the "SNMP Settings" section, which includes fields for SNMP Version (set to 2c) and SNMP Port (set to 161). There is also a "SNMP Version Settings" section with a "SNMP Community" field containing "public". At the bottom, there are "Back" and "Next >" buttons.

Figure 223 : Supervision du Web Server

- Puis, il faut choisir les services qu'on va superviser :

The screenshot shows the Nagios XI Configuration Wizard: Linux SNMP - Step 2. The left sidebar is identical to the previous step. The main content area is titled "Linux Machine Details" and shows the Host Name as "Web Server". Below it is the "Server Metrics" section, which lists several monitoring items with checkboxes:

- PING**: Monitors the machine with an ICMP ping. Useful for watching network latency and general uptime.
- CPU**: Monitors the CPU (processor usage) on the machine. It includes two threshold sliders: one for warning at 80% and one for critical at 90%.
- Physical Memory Usage**: Monitors the physical (real) memory usage on the machine. To run with memory buffers unselect the checkbox. It includes two threshold sliders: one for warning at 80% and one for critical at 90%.
- Swap Usage**: Monitors the swap usage on the machine. It includes two threshold sliders: one for warning at 5% and one for critical at 10%.
- Disk Usage**: Monitors disk usage on the machine. It includes a note stating "The SNMP wizard detected Disks on 172.120.1.101".

Figure 224 : Les services qu'on va superviser

The screenshot shows the Nagios XI web interface. On the left, a sidebar contains navigation links for Configuration, Configuration Tools, Auto Deployment, Advanced Configuration, and More Options. The main content area has two sections: 'Scanned Disk List' and 'Processes'.

Scanned Disk List: Shows disk usage for several drives. One drive, '/media/abdo/CDROM', is highlighted with a red border and labeled 'Critical' (red) with 95% usage. Other drives show 80% usage.

Drive:	/media/abdo/CDROM	Warning	Critical	%
Drive:		▲	●	80 %
Drive:		▲	●	80 %
Drive:		▲	●	80 %
Drive:		▲	●	80 %
Drive:		▲	●	80 %

Processes: Shows a list of detected processes. Three processes are highlighted with a red border and labeled 'Critical': apache2, named, and NetworkManager.

Linux Process	Display Name	Warning	Critical
apache2	apache2	▲	●
named	named	▲	●
NetworkManager	NetworkManager	▲	●
[]	[]	▲	●
[]	[]	▲	●

At the bottom, there are buttons for 'Add Row' and 'Delete Row'. The footer includes links for 'About', 'Legal', and 'Copyright © 2008-2023 Nagios Enterprises, LLC'.

Figure 225 : Les services du Web Server

Voici l'état des services du Web Server :

The screenshot shows the 'Service Status' page for a host named 'Web Server'. It displays a table of service monitoring results, a 'Host Status Summary' chart, and a 'Service Status Summary' chart.

Service Status: Shows the status of various services. Two services are highlighted with red arrows: 'apache2' and 'named', both marked as 'Ok'.

Host	Service	Status	Duration	Attempt	Last Check	Status Information
Web Server	/media/abdo/CDROM Disk Usage	Critical	23m 36s	5/5	2023-03-31 22:23:36	/media/abdo/CDROM: 100% used(55MB/55MB) (>95%) : CRITICAL
	CPU Usage	Ok	9s	1/5	2023-03-31 22:27:07	2 CPU, average load 1.0% < 80% : OK
	Memory Usage	Ok	4m 47s	1/5	2023-03-31 22:22:29	Physical memory: 41% used(1597MB/3901MB) (<80%) : OK
	NetworkManager	Ok	3m 4s	1/5	2023-03-31 22:24:12	1 process named NetworkManager (> 0)
	Ping	Ok	3m 46s	1/5	2023-03-31 22:23:30	OK - 172.120.1.101 rta 0.614ms lost 0%
	Swap Usage	Ok	3m 19s	1/5	2023-03-31 22:23:57	Swap space: 0% used(0MB/947MB) (<5%) : OK
→	apache2	Ok	2m 35s	1/5	2023-03-31 22:24:41	3 process named apache2 (> 0)
→	named	Ok	2m 17s	1/5	2023-03-31 22:24:59	1 process named named (> 0)

Host Status Summary: Shows the status of the host's own metrics.

Up	Down	Unreachable	Pending
1	0	0	0
Unhandled	Problems	All	
0	0	1	

Service Status Summary: Shows the status of all services across the monitored hosts.

Ok	Warning	Unknown	Critical	Pending
1	0	1	1	0
Unhandled	Problems	All		
2	2	8		

Figure 226 : L'état des services du Web Server

b) Mail server :

Il faut d'abord choisir les services à superviser :

The screenshot shows the Nagios XI configuration interface. On the left, a sidebar lists various configuration sections like 'Configure', 'Configuration Tools', 'Auto Deployment', 'Advanced Configuration', and 'More Options'. The main area is titled 'Scanned Disk List (double click to add)' and shows disk usage for '/dev/shm' and '/run/lock'. Below this is a 'Processes' section with a note about monitoring running processes. A message box says 'The SNMP wizard detected 185 processes on 172.120.1.103'. A table lists processes: 'dovecot', 'named', and 'NetworkManager' are selected and highlighted with a red border. Other processes listed include 'irq/44-pciehp', 'irq/45-pciehp', etc. At the bottom, there are buttons for 'Add Row | Delete Row', 'Back', and 'Next >'.

Figure 227 : Supervision du Mail Server

Voici l'état des services du Mail Server :

The screenshot shows the 'Service Status' page for the 'Mail Server'. It includes a 'Host Status Summary' table with columns for Up, Down, Unreachable, Pending, Unhandled, Problems, and All. The 'Service Status Summary' table shows 1 OK, 0 Warning, 0 Unknown, 0 Critical, and 1 Pending service. Below these are two tables of service details. The first table lists services like 'Disk Usage', 'CPU Usage', 'Memory Usage', 'NetworkManager', 'Ping', 'Swap Usage', 'dovecot', and 'named'. The second table shows detailed status information for each service, such as 'OK' status, N/A duration, and specific metrics like CPU load or disk usage percentages. Both tables have 10 total records shown. Navigation buttons at the bottom include 'Page 1 of 1 15 Per Page Go' and a search bar.

Figure 228 : L'état des services du Mail Server

Chapitre IX : VPN

Un VPN est un service qui crée une connexion sécurisée et privée entre votre appareil et internet. Il permet de masquer votre adresse IP et de protéger vos données en transit. En utilisant un VPN, vous pouvez accéder à des sites internet bloqués et sécuriser vos connexions Wi-Fi publiques.

I.La partie théorique du VPN :

1. Définition :

Un VPN (Virtual Private Network) est un service qui permet de créer un réseau privé virtuel sécurisé entre votre appareil (ordinateur, téléphone, tablette) et internet. Il utilise une technologie de cryptage pour protéger vos données en transit, ce qui les rend inaccessibles aux tiers malveillants.

Lorsque vous vous connectez à internet via un VPN, celui-ci crée un tunnel crypté entre votre appareil et un serveur VPN distant, à travers lequel toutes les données transitent. Votre adresse IP réelle est remplacée par celle du serveur VPN, ce qui vous permet de masquer votre localisation et d'accéder à des sites internet qui peuvent être bloqués dans votre région.

Un VPN est utile pour plusieurs raisons, notamment pour protéger votre vie privée en ligne, accéder à des contenus géo-restruits, contourner la censure sur internet, sécuriser vos connexions Wi-Fi publiques et protéger vos données contre les pirates informatiques et les logiciels malveillants.

Il existe de nombreux fournisseurs de VPN, chacun avec ses propres fonctionnalités, protocoles de cryptage et politiques de confidentialité. Il est important de choisir un fournisseur de VPN de confiance pour assurer la sécurité de vos données. Les meilleurs fournisseurs de VPN offrent une protection contre les fuites de données, ont des protocoles de cryptage robustes et ne conservent pas de journaux de vos activités en ligne.

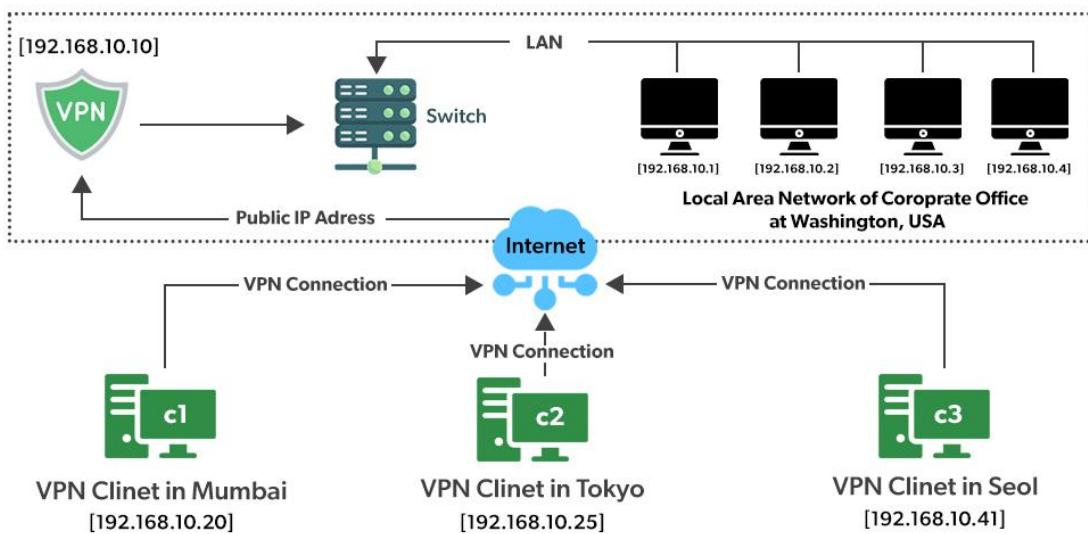


Figure 229 : Architecture VPN

*

2. Les réseaux privés dans les entreprises :

Les réseaux privés sont très courants dans les entreprises car ils offrent des avantages significatifs pour la sécurité, la collaboration et la gestion des ressources informatiques. Voici quelques-uns des avantages spécifiques des réseaux privés pour les entreprises :

- Sécurité renforcée : les réseaux privés permettent de sécuriser les données et les ressources de l'entreprise contre les cyberattaques, les intrusions et les accès non autorisés. Ils offrent également un contrôle d'accès granulaire, permettant aux administrateurs informatiques de gérer l'accès aux ressources en fonction des rôles et des niveaux d'autorisation.
- Connexions distantes sécurisées : les réseaux privés virtuels (VPN) permettent aux employés distants ou mobiles de se connecter en toute sécurité au réseau de l'entreprise via Internet, ce qui leur permet d'accéder aux ressources de l'entreprise de manière sécurisée, peu importe leur emplacement.
- Collaboration améliorée : les réseaux privés permettent aux employés de partager des fichiers, des documents, des imprimantes et des ressources informatiques de manière efficace et sécurisée, améliorant ainsi la collaboration et la productivité de l'équipe.
- Gestion centralisée des ressources : les réseaux privés permettent aux administrateurs informatiques de gérer efficacement les ressources informatiques de l'entreprise, telles que les serveurs, les bases de données et les applications, en centralisant leur gestion à partir d'un emplacement unique.

Donc, les réseaux privés sont un outil précieux pour les entreprises car ils offrent une sécurité renforcée, une connectivité distante sécurisée, une collaboration améliorée et une gestion centralisée des ressources informatiques.

3. Les réseaux privés virtuels :

Les réseaux privés virtuels (VPN) sont des réseaux privés qui utilisent une connexion Internet publique pour créer un tunnel sécurisé entre deux points distants. En d'autres termes, un VPN permet à un utilisateur ou à un ordinateur distant de se connecter à un réseau privé de manière sécurisée via Internet.

Le VPN utilise des protocoles de cryptage pour sécuriser les données en transit et protéger ainsi la confidentialité des informations échangées entre les deux points distants. Cela permet aux employés de se connecter au réseau de l'entreprise depuis n'importe quel endroit, ce qui est particulièrement utile pour les travailleurs distants, les télétravailleurs ou les employés en déplacement.

Les VPN sont également couramment utilisés pour accéder à des sites Web restreints géographiquement ou pour contourner les restrictions de pare-feu d'un réseau. En utilisant un VPN, un utilisateur peut apparaître comme s'il était connecté à partir d'une autre région géographique ou d'une adresse IP différente, ce qui peut être utile pour des besoins de confidentialité et de sécurité.

Pour tout dire, les VPN sont des réseaux privés virtuels qui permettent aux utilisateurs de se connecter à un réseau privé de manière sécurisée via Internet. Ils utilisent des protocoles de cryptage pour protéger la confidentialité des données en transit et sont couramment utilisés pour le travail à distance, l'accès à des sites Web restreints géographiquement ou pour contourner les restrictions de pare-feu d'un réseau.

4. Les cas d'utilisation :

Les réseaux privés virtuels (VPN) ont de nombreux cas d'utilisation dans les entreprises et les particuliers, notamment :

- Le travail à distance : Les employés qui travaillent à distance peuvent utiliser un VPN pour accéder en toute sécurité aux ressources de l'entreprise, telles que les fichiers, les applications et les bases de données, depuis leur domicile ou un autre endroit à distance. Cela permet aux travailleurs distants de se connecter au réseau de l'entreprise et de travailler en toute sécurité, comme s'ils étaient dans le bureau de l'entreprise.
- La sécurité des données : Les VPN peuvent être utilisés pour sécuriser les données sensibles, telles que les informations de compte bancaire, les informations de carte de crédit, les informations médicales, les informations juridiques et les informations gouvernementales. Les VPN peuvent empêcher les pirates informatiques et les cybercriminels d'intercepter et d'accéder à ces données.
- La confidentialité des données : Les VPN peuvent être utilisés pour protéger la confidentialité des données de navigation des utilisateurs en masquant leur adresse IP et en cryptant leur trafic en ligne. Les VPN sont particulièrement utiles pour les utilisateurs qui souhaitent protéger leur vie privée en ligne, tels que les journalistes, les activistes et les dissidents politiques.
- L'accès à des sites Web restreints géographiquement : Les VPN peuvent être utilisés pour accéder à des sites Web qui sont restreints géographiquement, tels que les sites de streaming de contenu, les sites de jeux en ligne et les réseaux sociaux. Les utilisateurs peuvent apparaître comme s'ils étaient situés dans un autre pays, ce qui leur permet d'accéder à des contenus qui sont autrement inaccessibles.

- La sécurité des réseaux Wi-Fi publics : Les VPN peuvent être utilisés pour sécuriser les connexions Wi-Fi publiques qui sont souvent peu sécurisées et vulnérables aux attaques de pirates informatiques et de cybercriminels. Les utilisateurs peuvent se connecter à un VPN pour crypter leur trafic en ligne et protéger ainsi leurs données contre les interceptions.

5. Les termes d'utilisation :

Voici des termes couramment utilisés dans le contexte des réseaux privés virtuels (VPN) :

- **Tunnel VPN** : un canal sécurisé créé entre deux points distants via Internet, permettant aux données de voyager de manière cryptée et sécurisée.
- **Protocoles de cryptage** : les méthodes utilisées pour crypter les données qui transitent par le VPN, tels que l’AES (Advanced Encryption Standard), le SSL (Secure Sockets Layer), le TLS (Transport Layer Security), le PPTP (Point-to-Point Tunneling Protocol) ou l’OpenVPN.
- **Adresse IP** : une série de chiffres unique attribuée à chaque appareil connecté à Internet, permettant de l’identifier et de le localiser. Les VPN peuvent masquer l’adresse IP de l’utilisateur en la remplaçant par une autre adresse IP.
- **Serveur VPN** : un ordinateur distant qui gère le trafic réseau entre le client VPN et le réseau privé, assurant la sécurité et la confidentialité des données.
- **Client VPN** : un logiciel qui permet à l’utilisateur de se connecter au serveur VPN et d’accéder au réseau privé.
- **Authentification** : le processus de vérification de l’identité de l’utilisateur, généralement via un nom d’utilisateur et un mot de passe.
- **Contrôle d’intégrité** : le processus de vérification de l’intégrité des données qui transitent à travers le tunnel VPN pour garantir qu’elles n’ont pas été modifiées ou altérées en cours de route.
- **Pare-feu** : un logiciel ou un matériel de sécurité qui filtre les données entrantes et sortantes d’un réseau pour empêcher les cyberattaques.
- **Réseau privé** : un réseau sécurisé et privé utilisé par une entreprise ou une organisation pour stocker et partager des données confidentielles.

6. Les types de VPN :

L'intranet VPN et l'extranet VPN sont deux types de VPN qui sont utilisés dans des contextes différents

- **L'intranet VPN** : permet aux utilisateurs de se connecter à un réseau privé depuis un emplacement distant, comme une succursale ou un bureau à domicile. Cela permet aux employés de travailler à distance tout en accédant aux ressources internes de l'entreprise, telles que les fichiers, les bases de données et les applications.

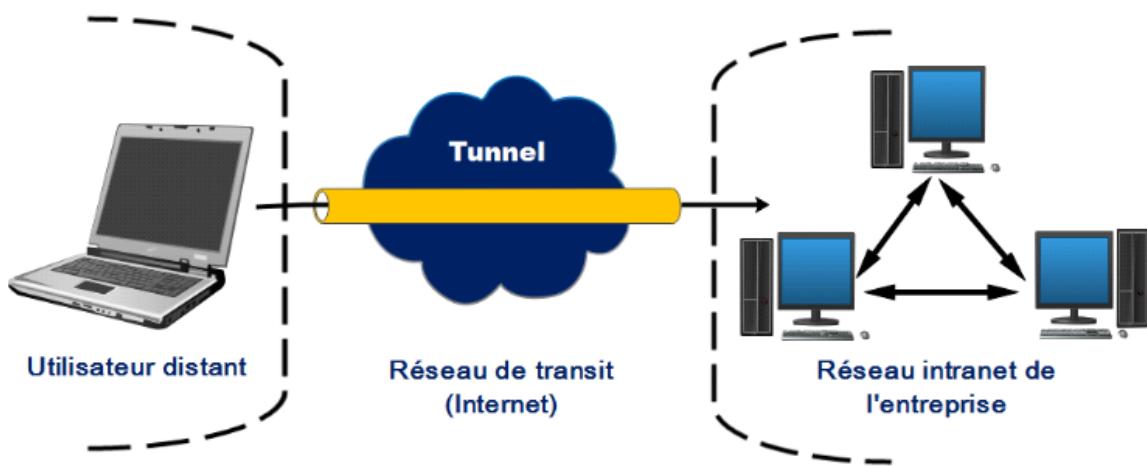


Figure 230 : L'intranet VPN

- **L'extranet VPN** : permet à des partenaires commerciaux, des fournisseurs ou des clients externes de se connecter de manière sécurisée au réseau privé de l'entreprise. Cela permet aux parties prenantes externes de partager des données et des informations avec l'entreprise, tout en maintenant un niveau élevé de sécurité et de confidentialité.

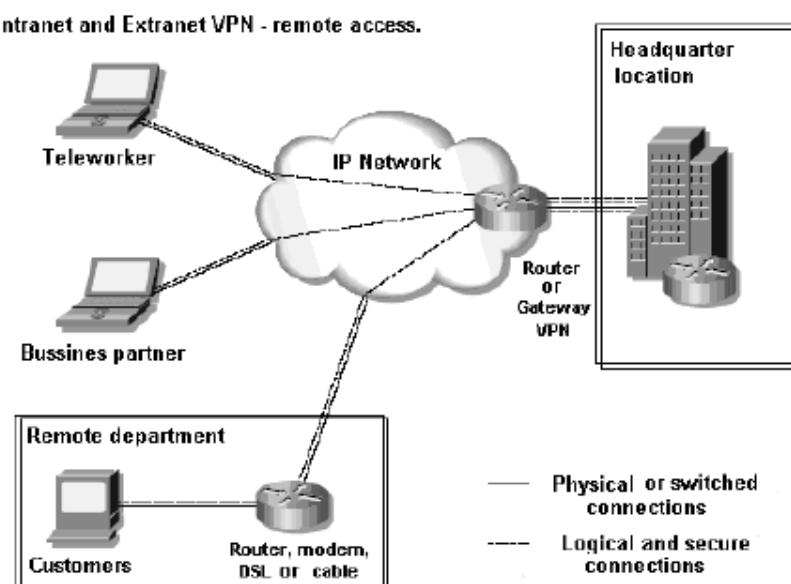


Figure 231 : L'extranet VPN

Pour résumé, l'intranet VPN est utilisé pour permettre aux employés de se connecter de manière sécurisée au réseau privé de l'entreprise depuis un emplacement distant, tandis que l'extranet VPN est utilisé pour permettre à des parties prenantes externes de se connecter de manière sécurisée au réseau privé de l'entreprise.

7. Les avantages et les inconvénients de VPN :

a) Les avantages du VPN :

La sécurité, la simplicité et l'économie sont trois aspects importants liés à l'utilisation du VPN :

- **Sécurité** : Comme expliqué précédemment, l'un des principaux avantages du VPN est la sécurité qu'il offre. Les données sont cryptées et protégées contre les attaques malveillantes, ce qui permet aux utilisateurs de naviguer sur Internet en toute sécurité et de se connecter à distance à des réseaux privés sans risquer la divulgation de données sensibles.
- **Simplicité** : Les VPN sont généralement faciles à utiliser et à configurer, ce qui les rend accessibles aux utilisateurs de tous niveaux de compétence technique. Les fournisseurs de VPN proposent souvent des logiciels conviviaux et des tutoriels pour aider les utilisateurs à se connecter rapidement et facilement à leur service VPN.
- **Économie** : Les VPN peuvent réduire les coûts d'infrastructure en permettant aux entreprises de partager des ressources et des données à distance sans avoir besoin d'une infrastructure physique dédiée. Les VPN peuvent également réduire les coûts liés aux déplacements professionnels, car les employés peuvent accéder aux ressources de l'entreprise de manière sécurisée à distance.

b) Les inconvénients du VPN :

Voici quelques inconvénients du VPN :

- **Performances** : L'utilisation du VPN peut entraîner une diminution des performances, en particulier lorsque l'on utilise des protocoles de cryptage forts qui nécessitent plus de temps de traitement.
- **Disponibilité** : Si le serveur VPN tombe en panne ou si le réseau subit une interruption de service, l'accès à distance au réseau privé peut être interrompu, ce qui peut entraîner des perturbations pour les utilisateurs.
- **Complexité** : La configuration et la gestion d'un VPN peuvent être complexes, en particulier pour les entreprises qui doivent gérer plusieurs utilisateurs et plusieurs réseaux distants.

- **Coûts** : Bien que l'utilisation d'un VPN puisse permettre de réduire les coûts en évitant la nécessité d'une infrastructure physique dédiée, cela peut également entraîner des coûts supplémentaires liés à l'utilisation d'un service VPN tiers.
- **Sécurité** : Bien que le VPN puisse renforcer la sécurité des données en les cryptant et en les protégeant contre les attaques malveillantes, il n'est pas à l'abri des attaques de piratage et de la divulgation de données sensibles en cas de failles de sécurité.

8. Les protocoles du VPN :

Il existe plusieurs protocoles utilisés par les VPN pour assurer une connexion sécurisée et fiable.

Voici quelques-uns des protocoles les plus courants :

- **PPTP** (Point-to-Point Tunneling Protocol) : un protocole obsolète qui offre un niveau de sécurité relativement faible, mais qui est facile à configurer.

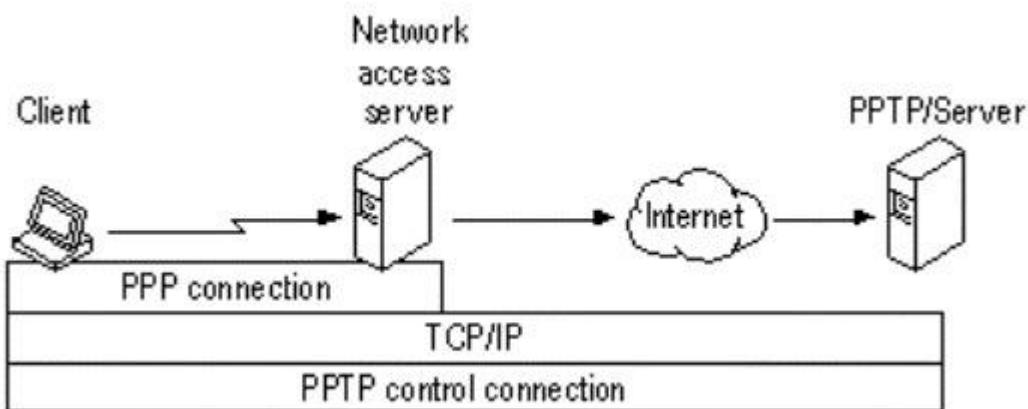


Figure 232 : Le protocole PPTP

- **L2TP** (Layer 2 Tunneling Protocol) : un protocole qui combine les avantages de L2TP (utilisé pour créer des tunnels VPN)

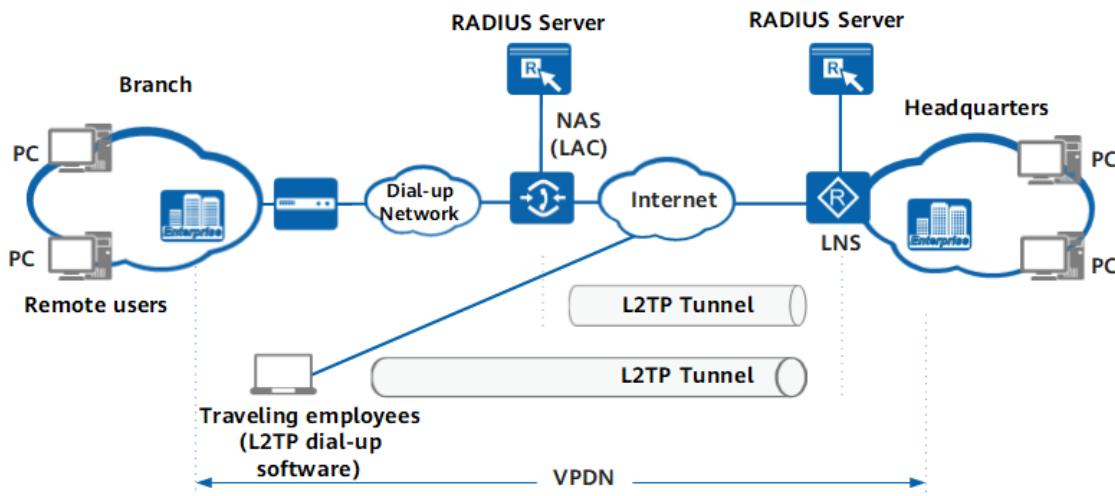


Figure 233 : Le protocole L2TP

- **PPP** : Le protocole PPP permet l’authentification de l’utilisateur, le chiffrement des données, la compression de données et la gestion des erreurs, ce qui en fait un choix populaire pour les réseaux privés virtuels. Il est souvent utilisé en combinaison avec L2TP ou avec d’autres protocoles de tunnelisation pour créer des connexions VPN.
- **OpenVPN** : un protocole open-source qui offre une sécurité élevée, une grande flexibilité et une compatibilité multi-plateforme.
- **SSTP (Secure Socket Tunneling Protocol)** : un protocole développé par Microsoft qui utilise SSL/TLS pour garantir une connexion sécurisée.

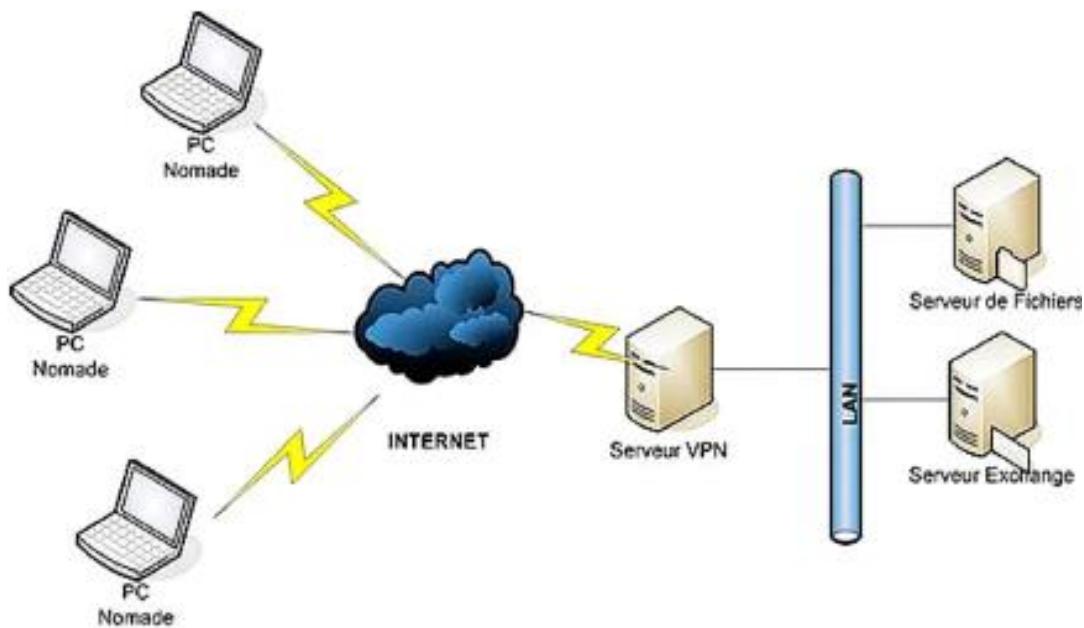


Figure 234 : Le protocole SSTP

- **IKEv2** (Internet Key Exchange version 2) : un protocole qui utilise une authentification forte et une sécurité de cryptage élevée pour garantir une connexion sécurisée.

Le choix du protocole dépend des besoins spécifiques de chaque utilisateur, ainsi que des fonctionnalités et de la compatibilité avec les différents systèmes et plateformes.

9. Les modes de transports du VPN :

Dans le contexte des protocoles de sécurité, le mode de transport fait référence à la manière dont les données sont protégées lorsqu’elles sont transférées entre deux ordinateurs. Il existe deux modes de transport :

- **Mode de transport avec chiffrement de charge utile** : dans ce mode, seules les données à l’intérieur des paquets sont chiffrées. L’en-tête IP n’est pas chiffré. Ce mode est plus rapide et est souvent utilisé pour les connexions point-à-point.

- **Mode de transport avec chiffrement de tout le paquet** : dans ce mode, le paquet entier est chiffré, y compris l'en-tête IP. Ce mode est plus sécurisé, mais il est également plus lent en raison de la surcharge de chiffrement de l'en-tête IP.

Les modes de transport sont utilisés dans le cadre d'IPSec pour protéger les données transférées entre deux systèmes. Les deux modes ont leurs avantages et leurs inconvénients, et le choix dépend des besoins spécifiques de chaque utilisateur.

10. L'installation et configuration du VPN :

a) La mise en place du VPN :

Dans la fenêtre « Sélectionner des rôles de serveurs », il est nécessaire de définir la fonction de l'outil que nous souhaitons développer. Pour un VPN, nous devons choisir l'accès à distance, puis cocher cette option avant de cliquer sur le bouton « Suivant ».

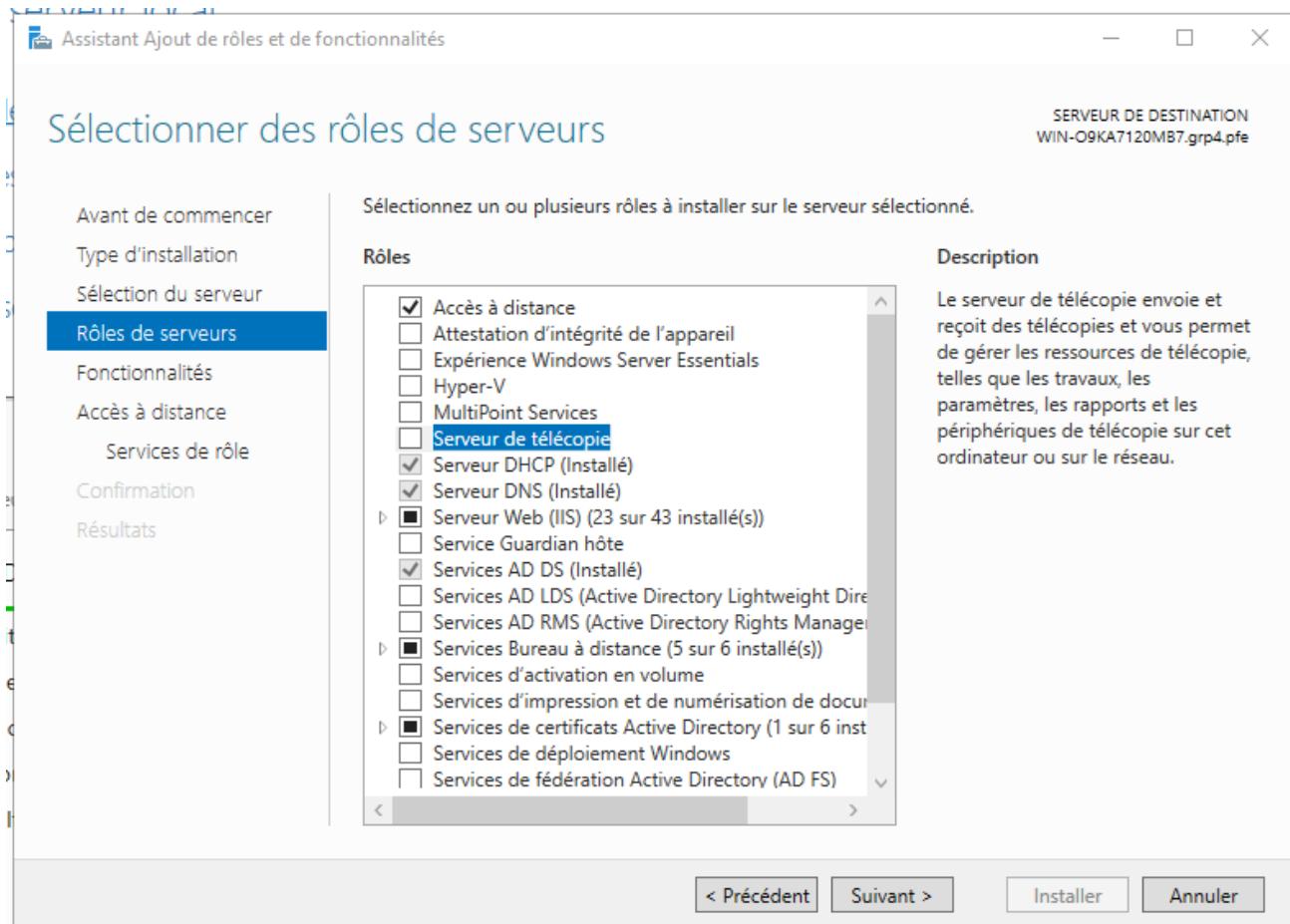


Figure 235 : La mise en place du VPN

- Il n'y a rien à cocher sur cette page, nous pouvons donc cliquer directement sur le bouton « Suivant > ».

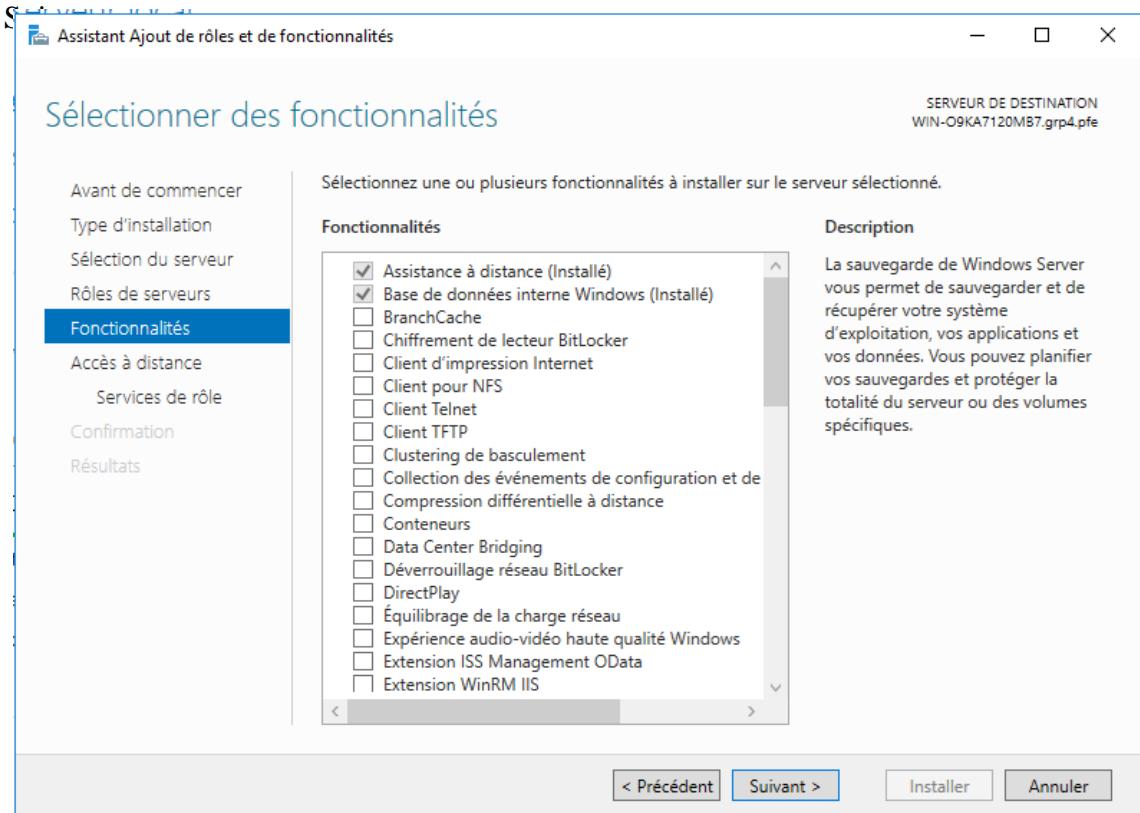


Figure 236 : L'installation du VPN

- Ensuite, pour ajouter des fonctionnalités, il est nécessaire de cliquer sur le bouton « Ajouter des fonctionnalités » .

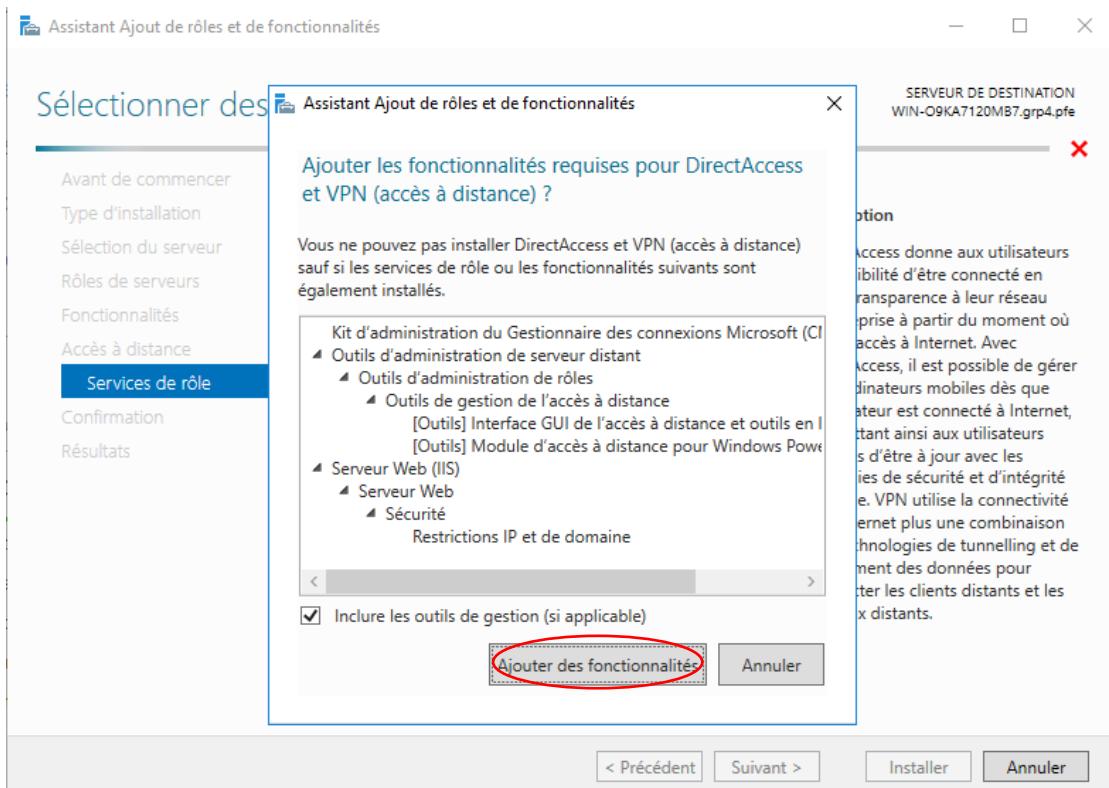


Figure 237 : L'ajout des fonctionnalités du VPN

- En cliquant sur ce bouton, une fenêtre s'ouvrira et vous devrez sélectionner « DirectAccess et VPN (accès à distance) » en cochant la case correspondante.

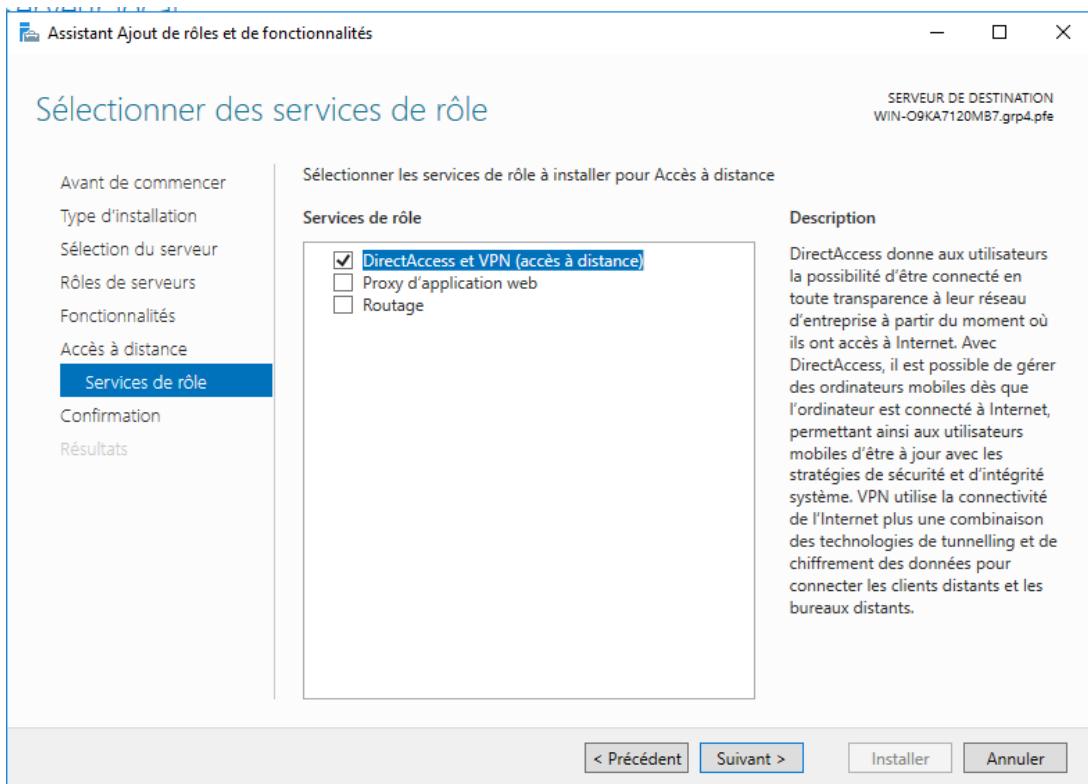


Figure 238 : L'activation de l'accès à distance

- Ensuite, vous devrez confirmer vos sélections d'installation.

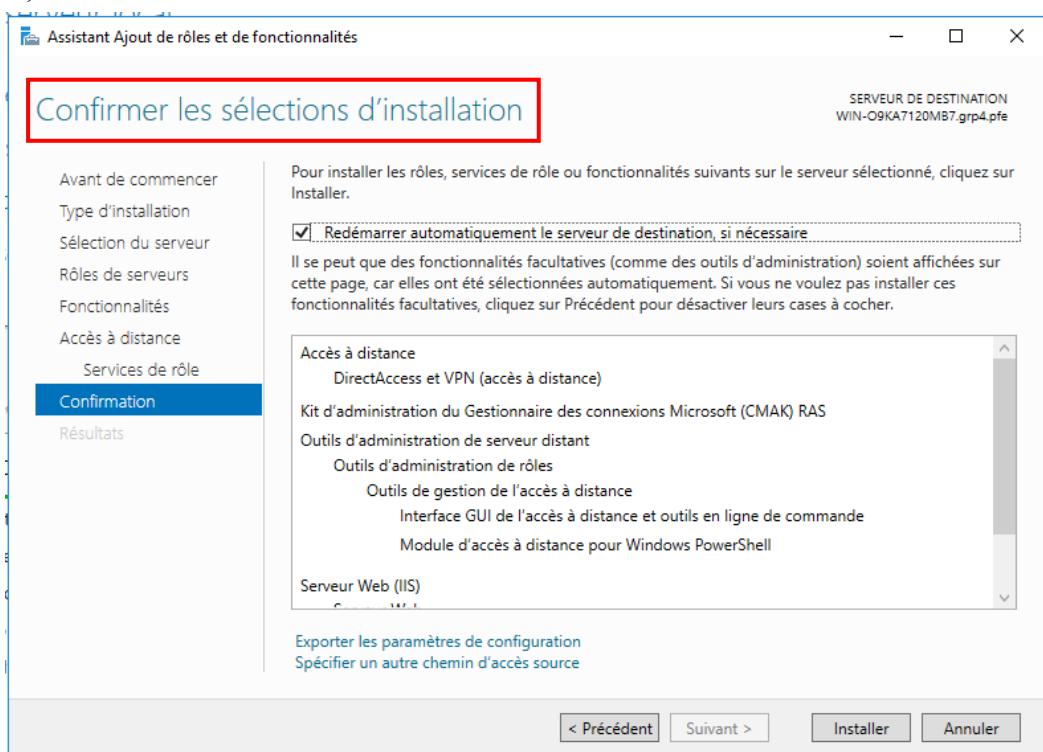


Figure 239 : La confirmation des sélections d'installation VPN

- On procèdera à l'ajout d'une unité d'organisation dans la fenêtre « Utilisateurs et ordinateurs Active Directory » afin de gérer un groupe VPN.

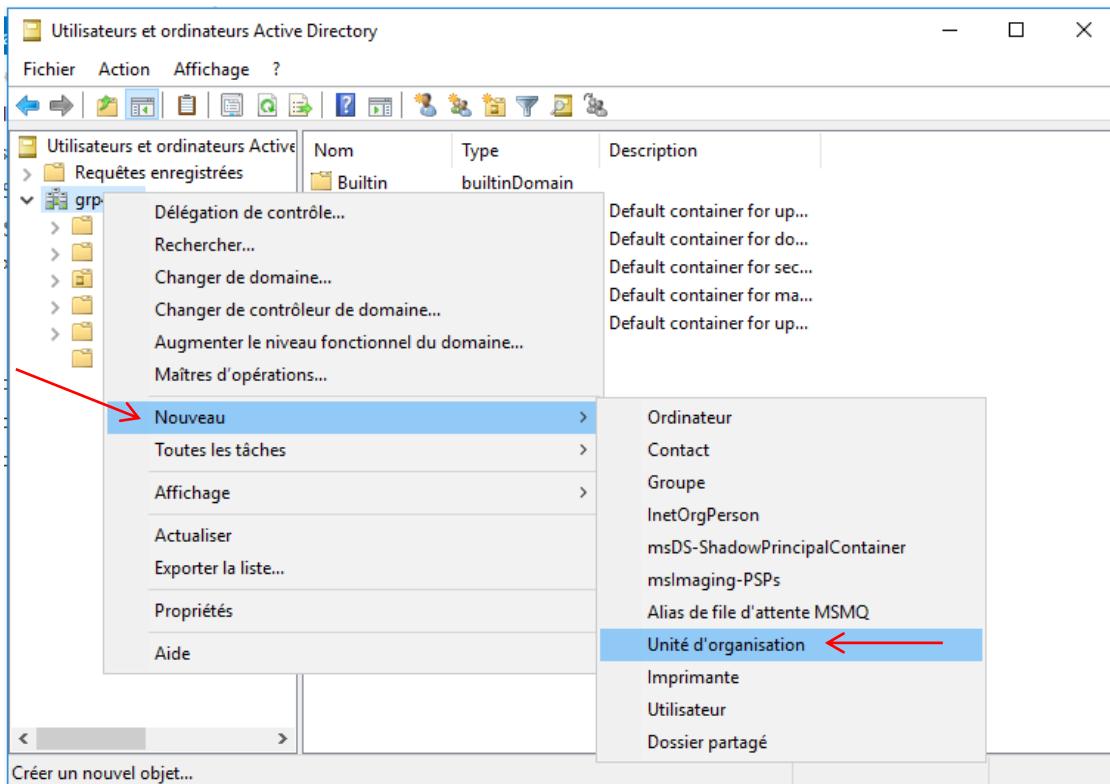


Figure 240 : La création d'une unité d'organisation

- L'unité d'organisation ou le groupe nommé « VPN_USERS ».

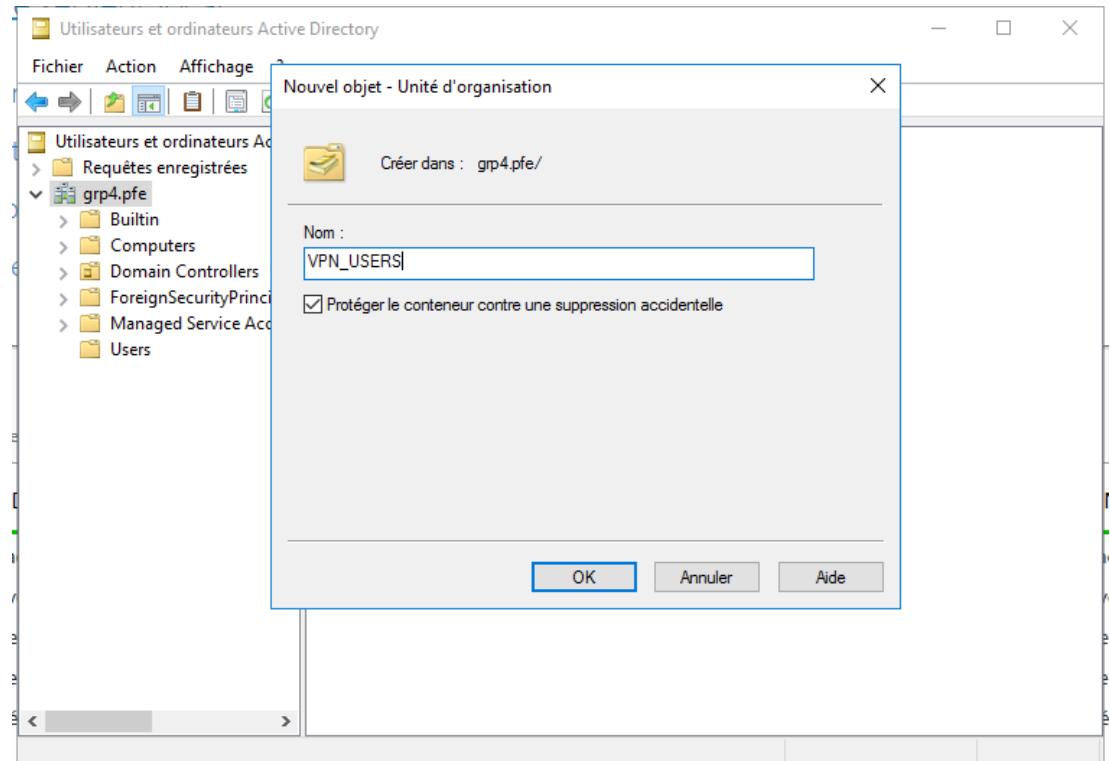


Figure 241 : L'unité d'organisation "VPN_USERS"

- On remarque l'ajout de l'unité d'organisation « VPN_USERS ».
- Ensuite, on va ajouter le groupe nommé « VPN ».

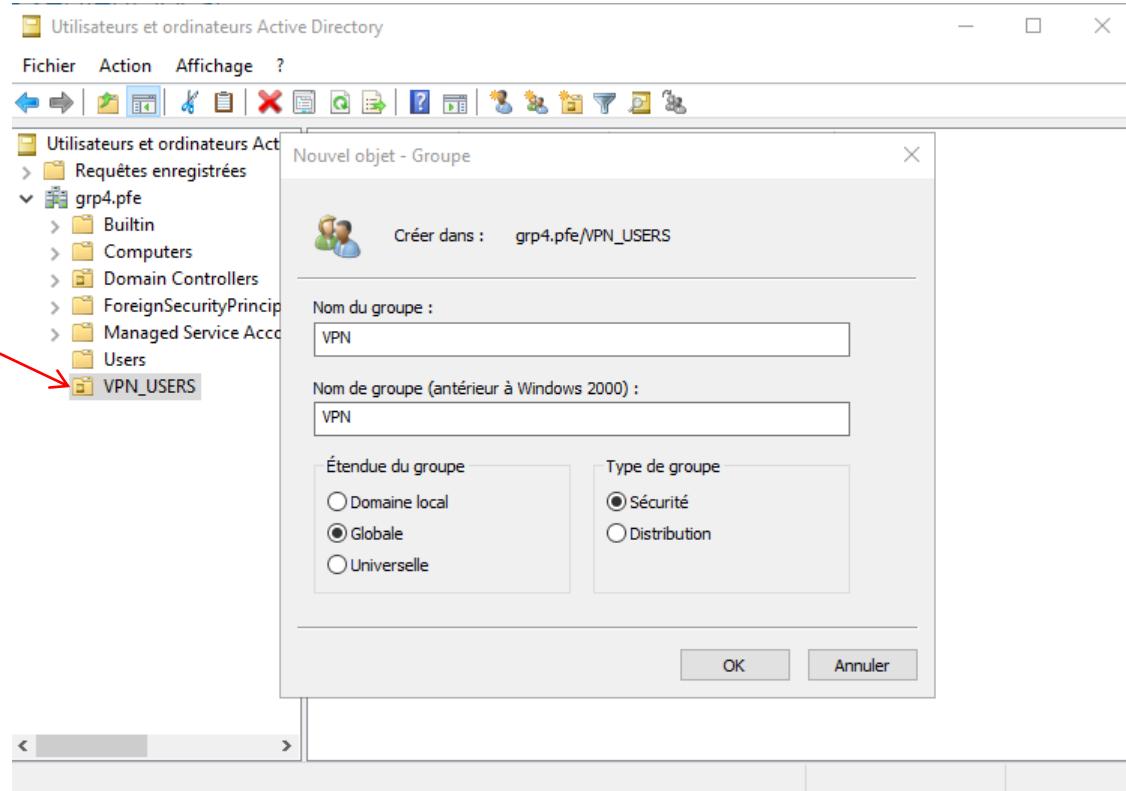


Figure 242 : La création d'un groupe VPN

- Et dans le groupe « VPN », on va ajouter un utilisateur « test » :

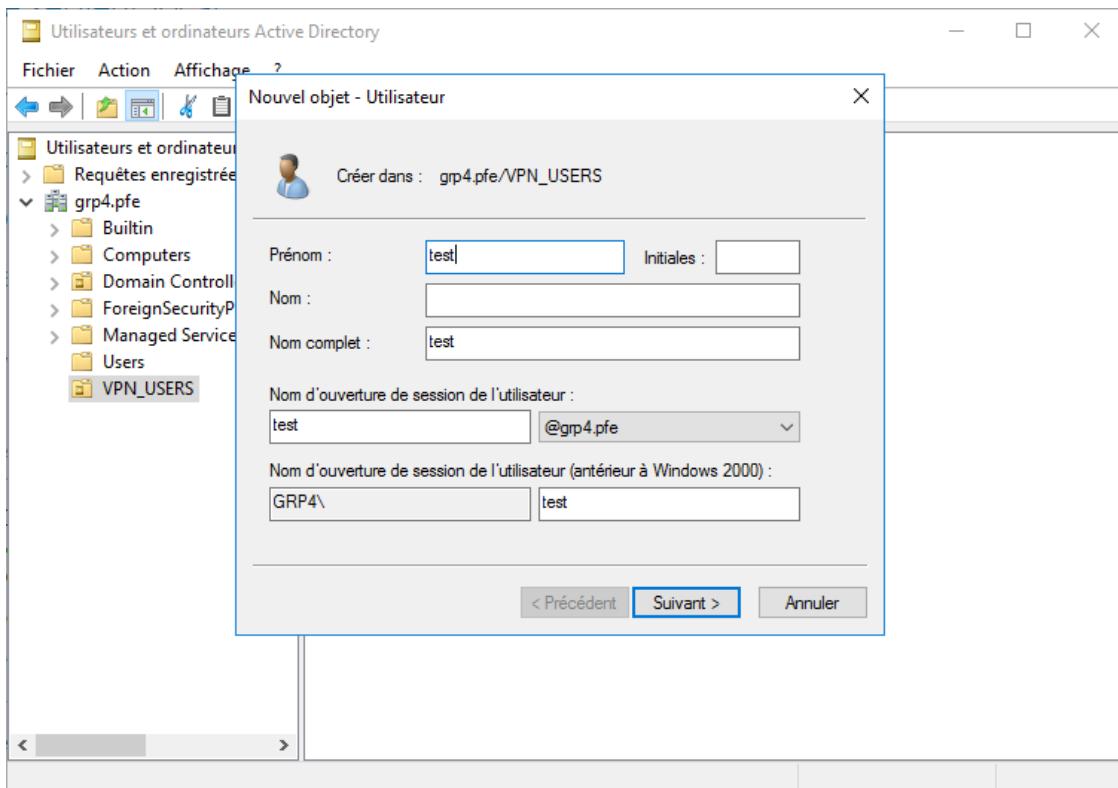


Figure 243 : La création d'un utilisateur dans le groupe "VPN_USERS"

- Puis, il est nécessaire de saisir un mot de passe d'utilisateur.

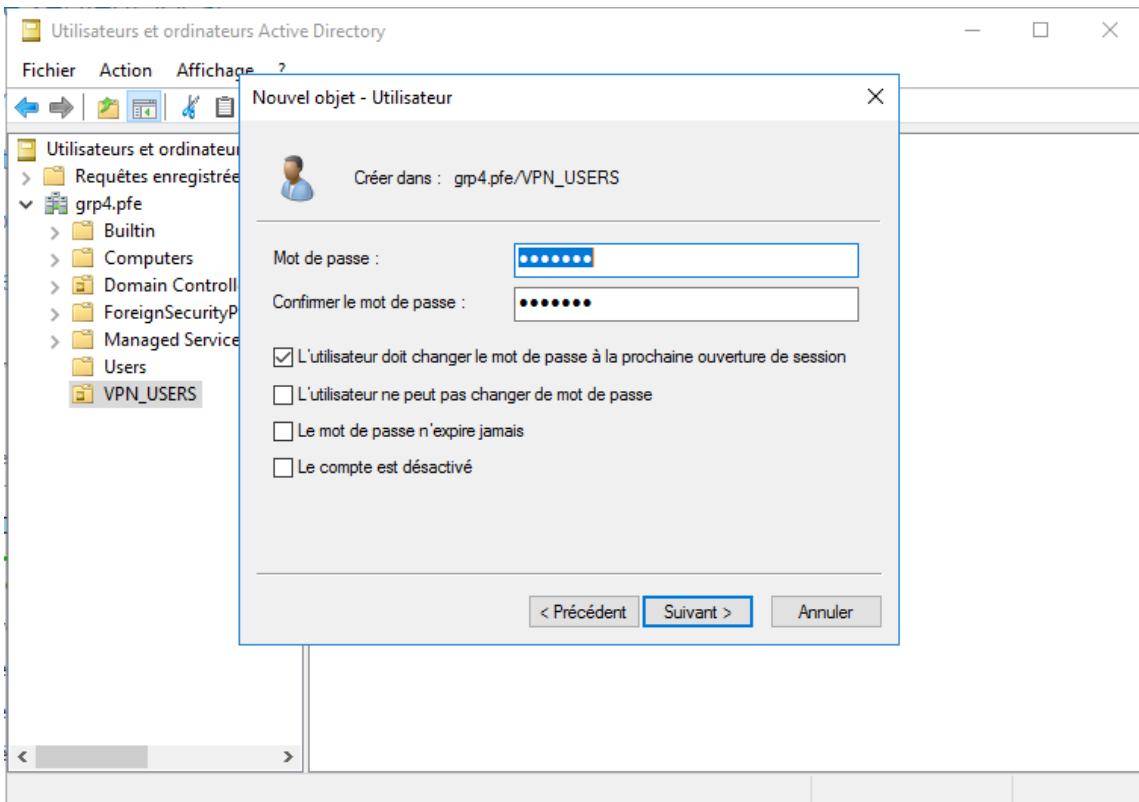


Figure 244 : Le mot de passe de l'utilisateur VPN

b) La configuration du VPN :

- Une fois que nous cliquons sur « Accès à distance », un message d'alerte apparaît nous indiquant qu'une configuration est nécessaire pour que le VPN soit fonctionnel. Pour configurer le VPN, nous cliquons sur « Autres ».
- Ensuite, une nouvelle fenêtre apparaît et nous cliquons sur « Ouvrir l'Assistant Mise en route » pour entamer la configuration du VPN.
- Après cela, une nouvelle fenêtre apparaît et nous choisissons de déployer uniquement le VPN.

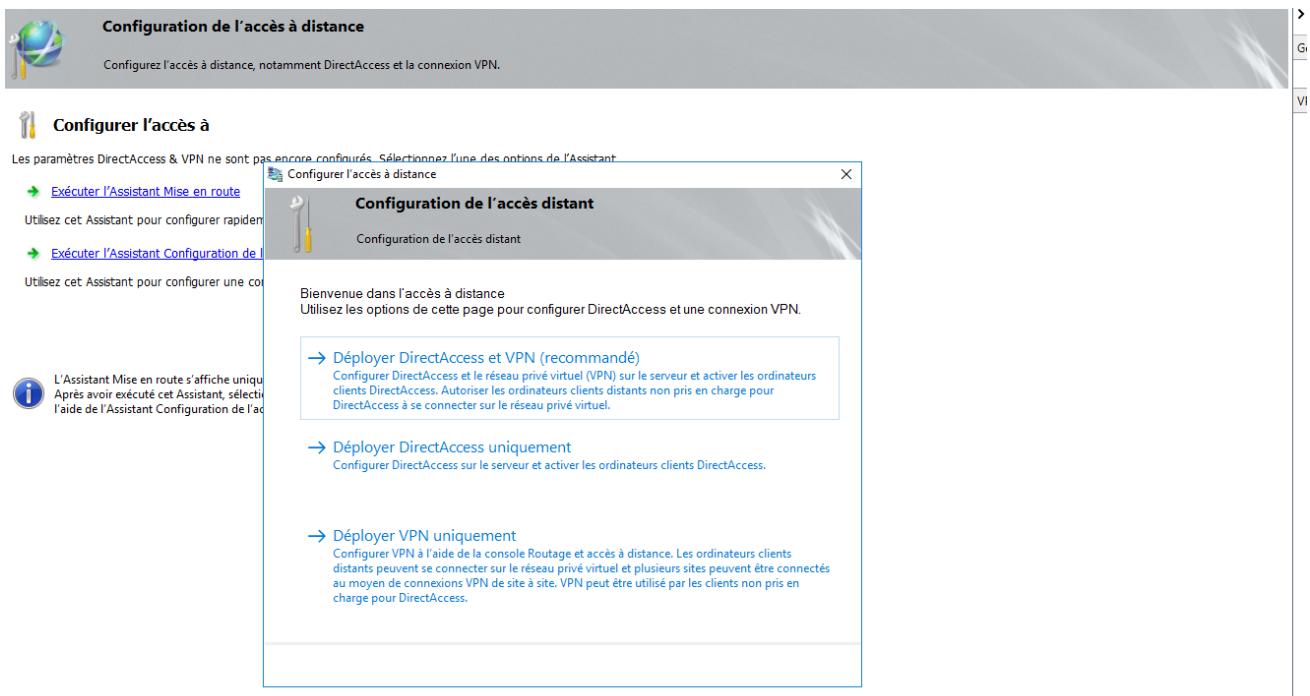


Figure 245 : La configuration du VPN

- Par la suite, une nouvelle fenêtre s'affiche. Nous effectuons un clic droit sur le serveur local et sélectionnons « Configurer et activer le routage et l'accès à distance ».



Figure 246 : La configuration du routage et l'accès à distance

- Un assistant d'installation se lance et nous suivons ses instructions en cliquant sur « Suivant ».

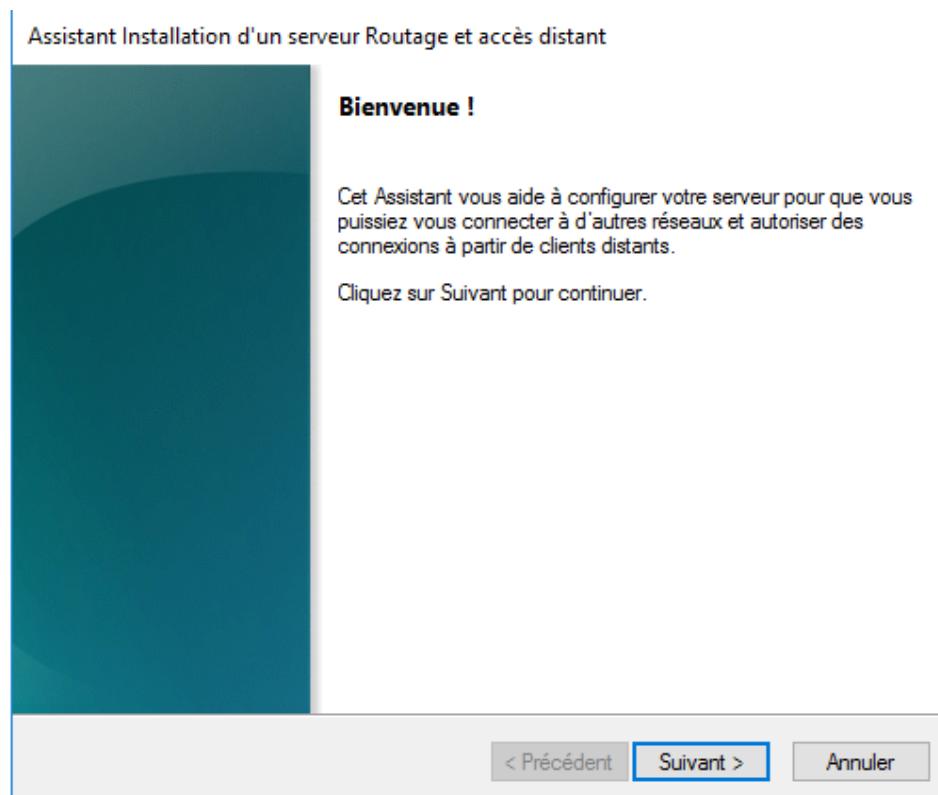


Figure 247 : L'assistant d'installation

- Nous choisissons l'option « Configuration personnalisée » et appuyons sur le bouton « Suivant ».

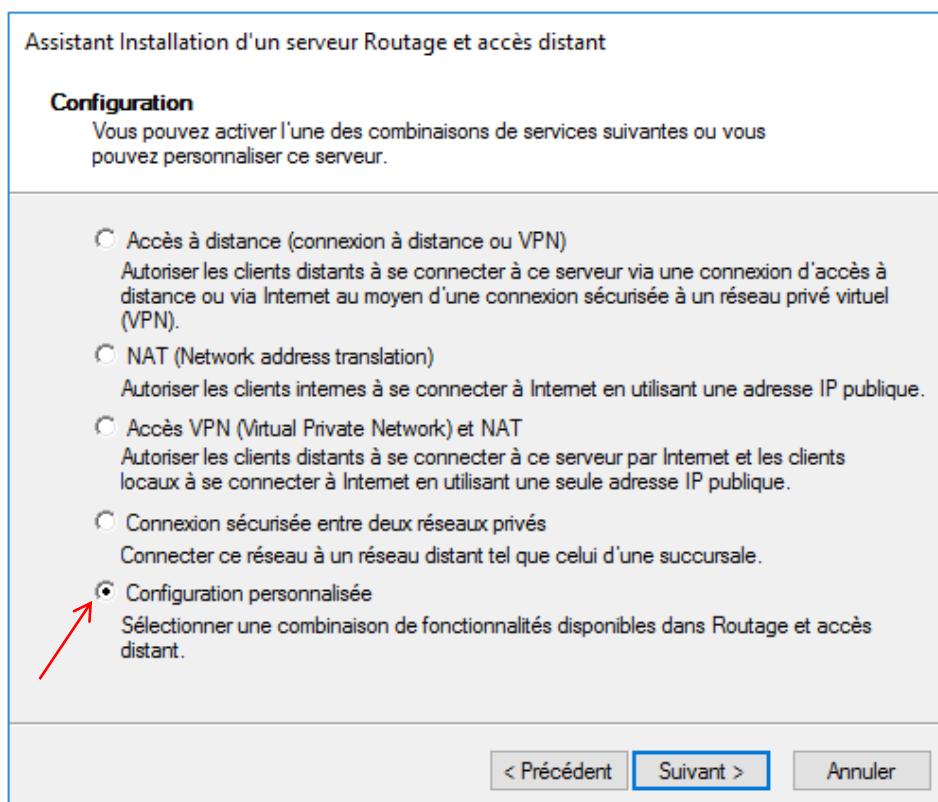


Figure 248 : La configuration personnalisée

- Nous sélectionnons uniquement l'option « Accès VPN » et cliquons sur « Suivant ».

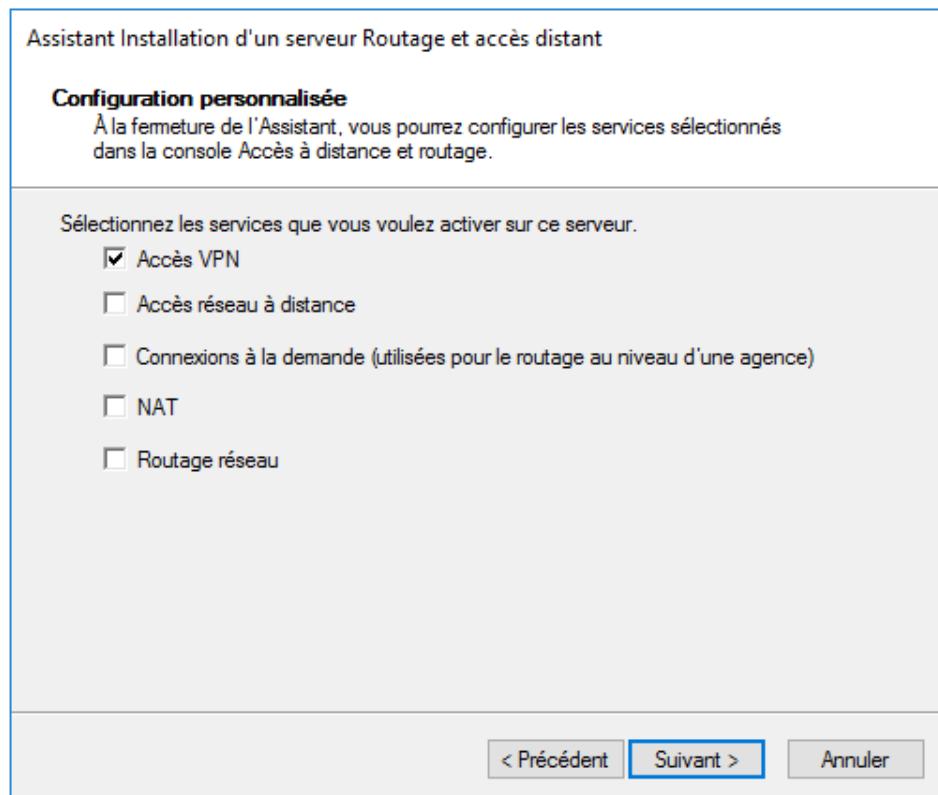


Figure 249 : L'activation de l'accès VPN

- Nous pouvons maintenant finaliser l'installation.

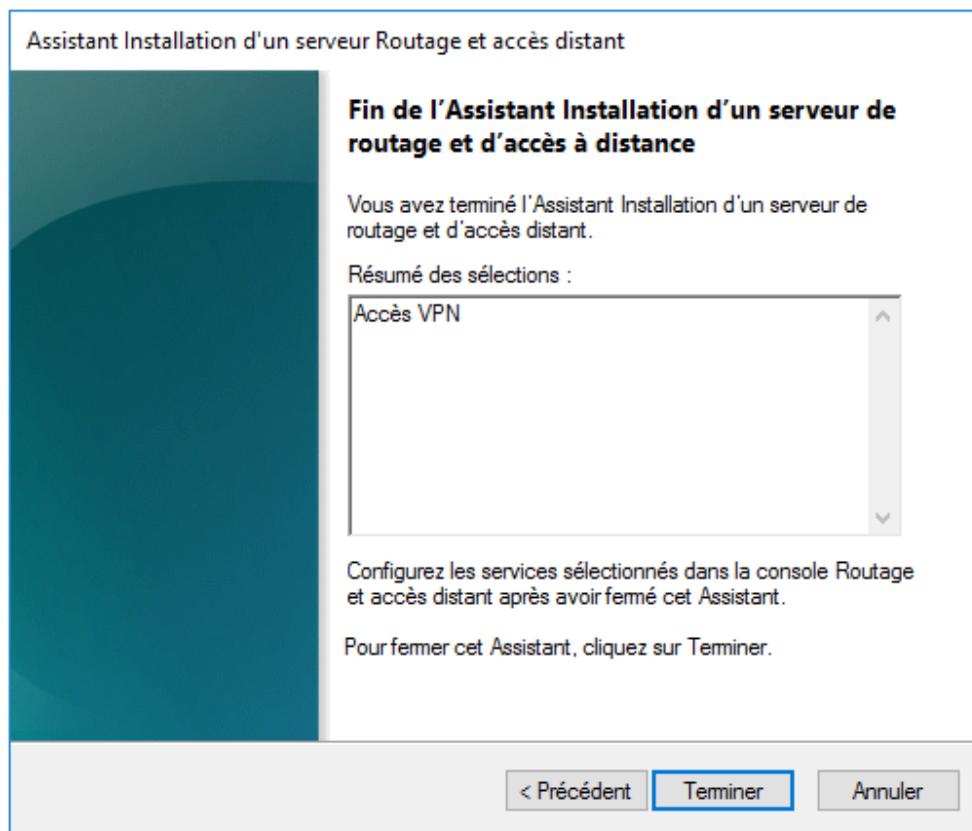


Figure 250 : La finalisation de l'installation d'accès à distance

11. Stratégie accès réseau VPN :

- Dans la fenêtre « Network Policy Server », vous cliquez sur « Stratégies ».

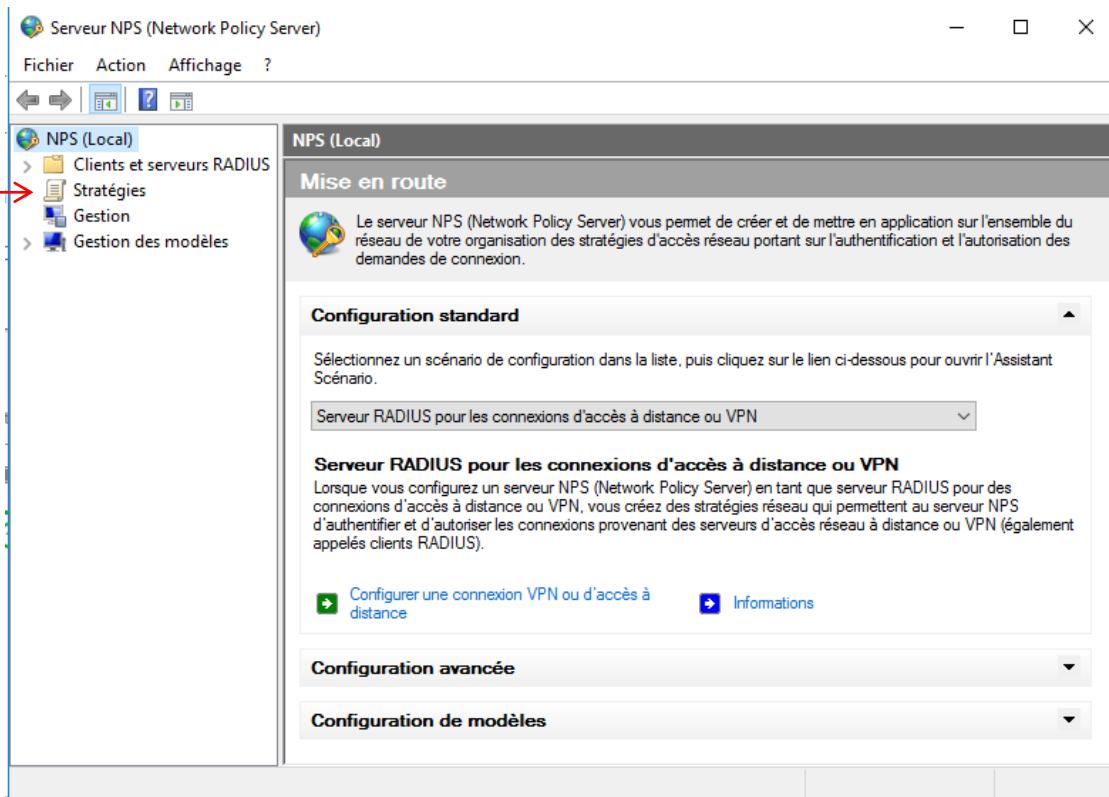


Figure 251 : Stratégie accès réseau VPN

- Nous effectuons un clic droit sur « Stratégies réseau », pour ajouter une nouvelle stratégie réseau.

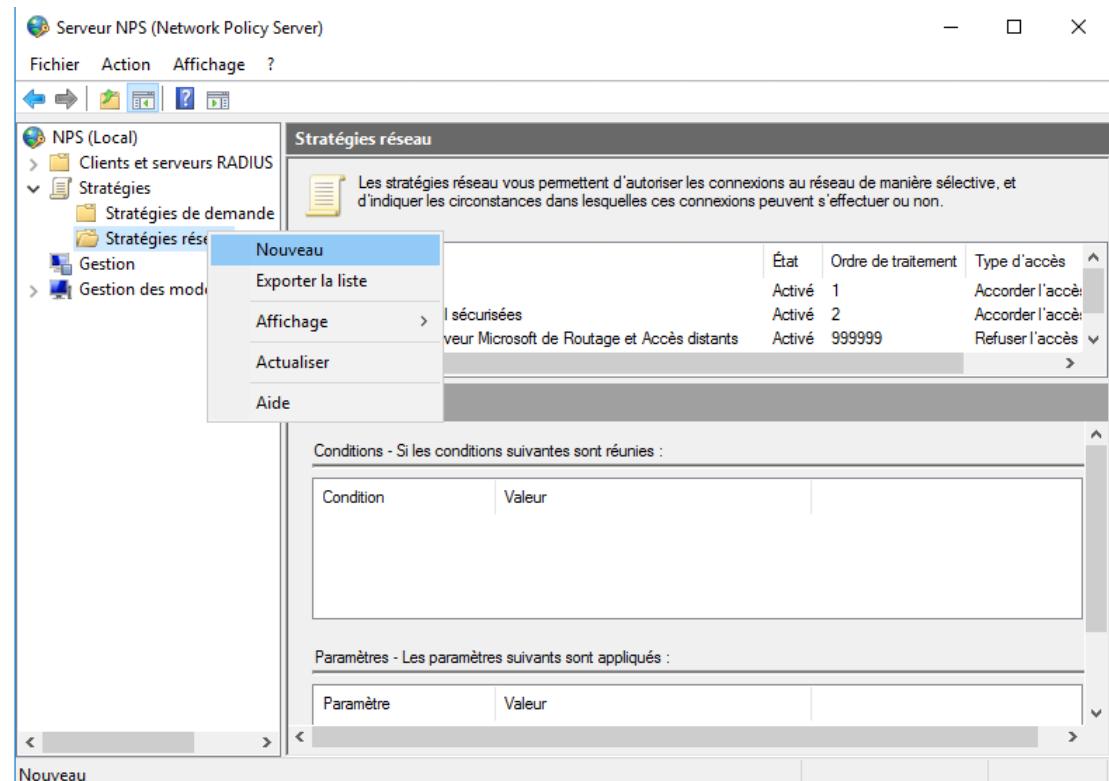


Figure 252 : L'ajout d'une nouvelle stratégie

- Vous saisissez le nom de la stratégie, dans notre cas on a nommé la stratégie « ACCES_VPN », et vous cliquez sur le bouton « Suivant ».

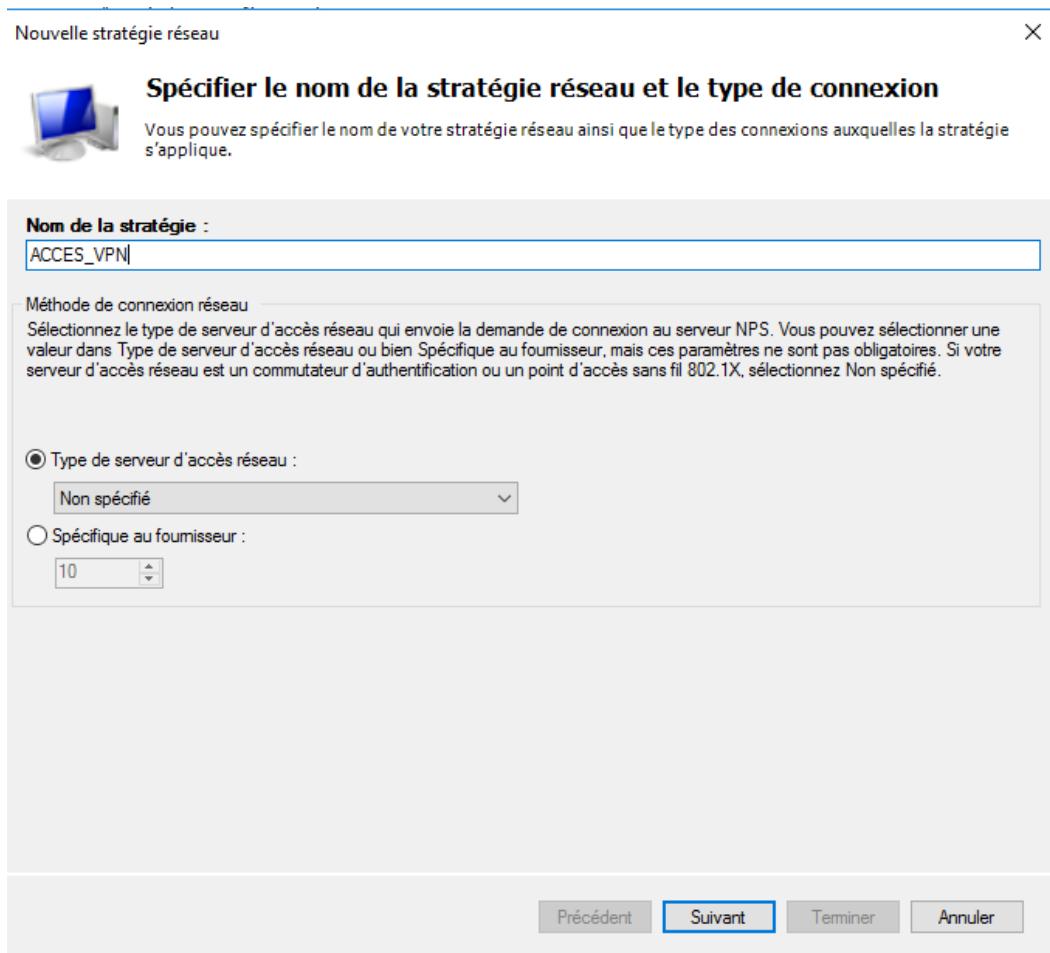


Figure 253 : La saisie du nom de la stratégie

- Puis, on va sélectionner une condition, dans notre cas on a choisi « Groupe d'utilisateurs ».

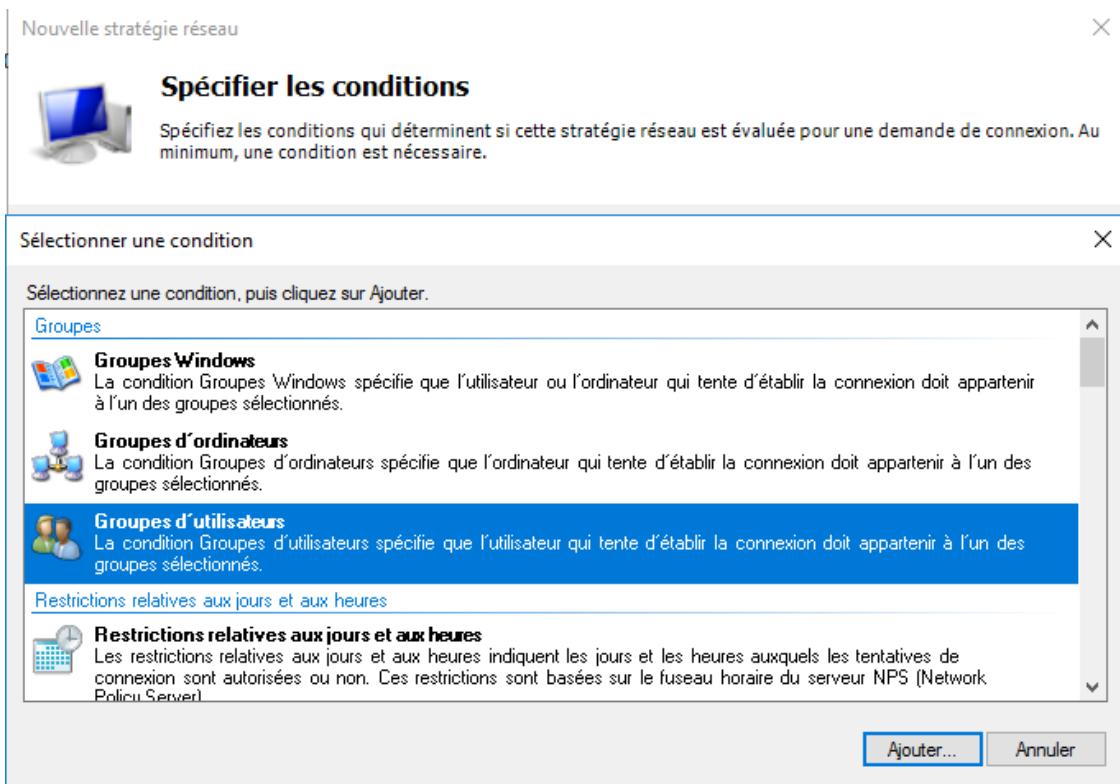


Figure 254 : Spécification des conditions

- Ensuite, vous saisissez le nom du groupe que vous avez ajouté avant.

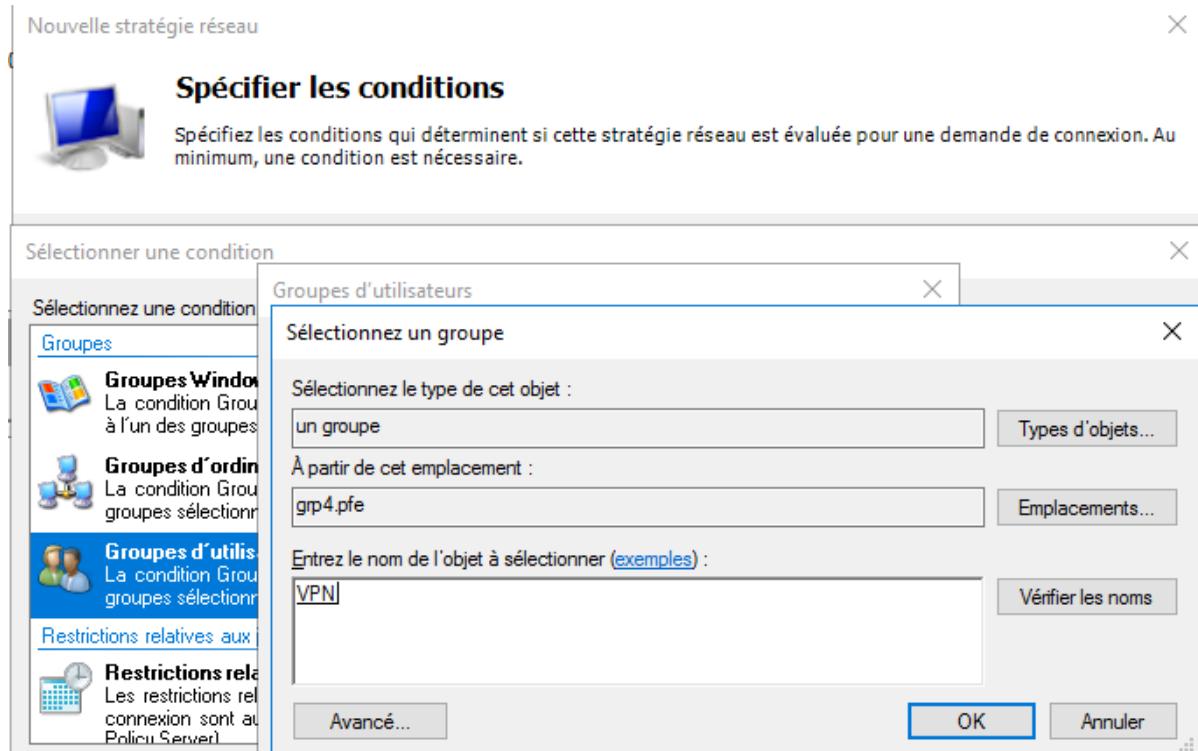


Figure 255 : La sélection du groupe VPN

- Et comme vous pouvez remarquer, la condition est ajoutée avec succès.

Nouvelle stratégie réseau

X

Spécifier les conditions

Spécifiez les conditions qui déterminent si cette stratégie réseau est évaluée pour une demande de connexion. Au minimum, une condition est nécessaire.

Conditions :

Condition	Valeur
Groupes d'utilisateurs	GRP4\VPN

Figure 256 : La condition du VPN est ajoutée

- Puis, vous ajoutez une autre condition « Type de tunnel » et vous sélectionnez l'option « L2TP »

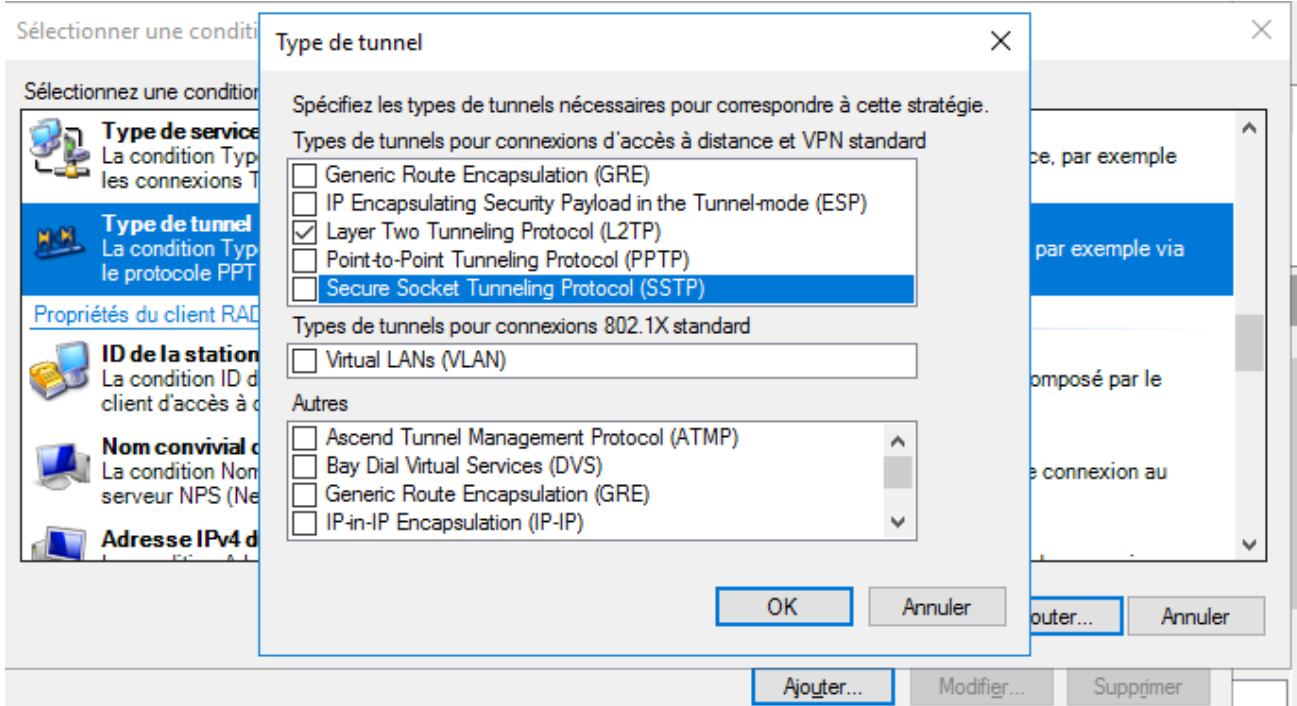


Figure 257 : Type de tunnel

- Ensuite, vous configurez la méthode d'authentification en cliquant sur le bouton « Ajouter »
- Dans notre cas, la méthode est « Mot de passe sécurisé (EAP-MSCHAP version 2) ».

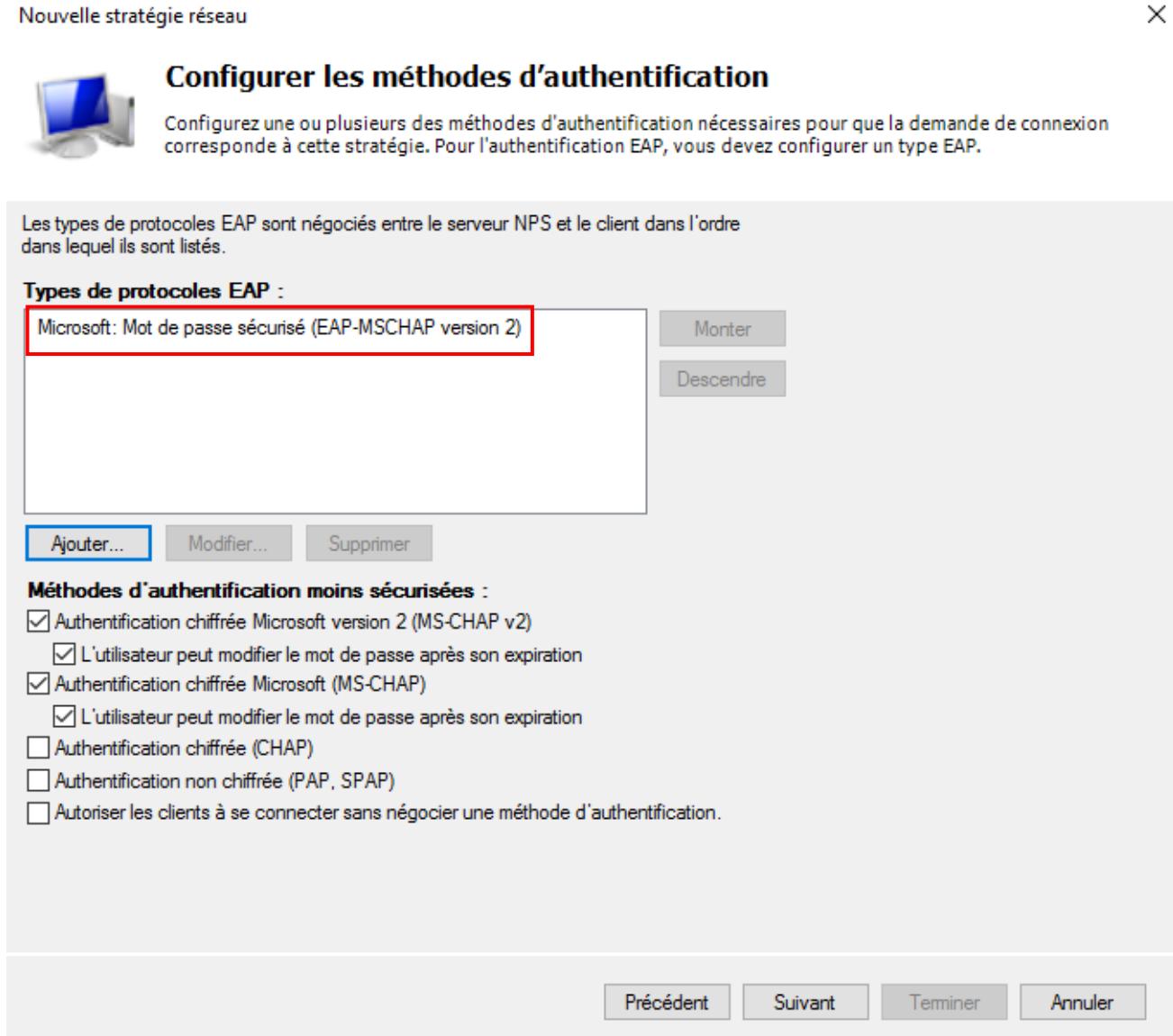


Figure 258 : La configuration de la méthode d'authentification

- Comme vous avez pu le constater, la stratégie est bien ajoutée et configurée.

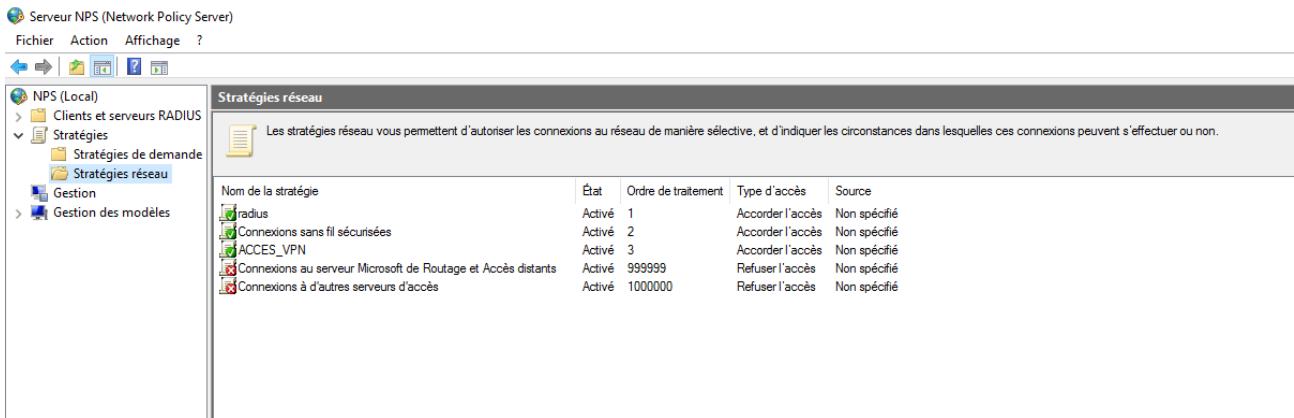


Figure 259 : La finalisation de la configuration de la stratégie

- Ensuite, nous configurons le point d'accès qui fournit Internet à notre réseau local (LAN).
- Tout d'abord, vous tapez l'adresse IP de votre point d'accès sur l'URL pour accéder à l'interface de configuration Web du point d'accès.
- Puis, dans la fenêtre « Application », il faut saisir les informations nécessaires pour configurer une connexion spécifique (ici, une connexion VPN) : le nom de la connexion, le numéro du port autorisé (pour le VPN, le port 1701), ainsi que l'adresse IP du serveur VPN (192.168.20.253). Une fois ces informations renseignées, en cliquant sur « Apply », le point d'accès acceptera la connexion au VPN.

Status	Network	Security	Application	Management																														
DDNS	Application » Port Forwarding » Port Forwarding																																	
Port Forwarding	On this page, you could configure port forwarding.																																	
Port Forwarding	<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Delete All"/>																																	
NAT																																		
UPNP																																		
DMZ																																		
Diagnosis																																		
Port Forwarding Rules List <table border="1"> <thead> <tr> <th>ID</th> <th>WAN</th> <th>Description</th> <th>Public Port</th> <th>IP</th> <th>Private Port</th> <th>Protocol</th> <th>Enable</th> </tr> </thead> <tbody> <tr> <td>---</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <table border="1"> <tr> <td>WAN</td> <td>INTERNET_R_VID_1141</td> </tr> <tr> <td>Description</td> <td>VPN</td> </tr> <tr> <td>Public Port</td> <td>1701 - 1723 * (1-65535)</td> </tr> <tr> <td>IP</td> <td>192.168.20.253 *</td> </tr> <tr> <td>Private Port</td> <td>1701 - 1723 * (1-65535)</td> </tr> <tr> <td>Protocol</td> <td>ALL</td> </tr> <tr> <td>Enable</td> <td>Disable</td> </tr> </table> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>					ID	WAN	Description	Public Port	IP	Private Port	Protocol	Enable	---								WAN	INTERNET_R_VID_1141	Description	VPN	Public Port	1701 - 1723 * (1-65535)	IP	192.168.20.253 *	Private Port	1701 - 1723 * (1-65535)	Protocol	ALL	Enable	Disable
ID	WAN	Description	Public Port	IP	Private Port	Protocol	Enable																											

WAN	INTERNET_R_VID_1141																																	
Description	VPN																																	
Public Port	1701 - 1723 * (1-65535)																																	
IP	192.168.20.253 *																																	
Private Port	1701 - 1723 * (1-65535)																																	
Protocol	ALL																																	
Enable	Disable																																	

Figure 260 . La configuration du point d'accès sur le VPN

- La configuration est bien appliquée.

The screenshot shows a network configuration interface with a sidebar menu on the left containing options like DDNS, Port Forwarding, NAT, UPNP, DMZ, and Diagnosis. The main area is titled "Application » Port Forwarding » Port Forwarding". It displays a "Port Forwarding Rules List" table with one entry:

ID	WAN	Description	Public Port	IP	Private Port	Protocol	Enable
0	INTERNET_R_VID_1141	VPN	1701-1723	192.168.20.253	1701-1723	ALL	Disable

Below the table is a detailed configuration form for the selected rule:

WAN	INTERNET_R_VID_1141
Description	VPN
Public Port	1701 - 1723 * (1-65535)
IP	192.168.20.253 *
Private Port	1701 - 1723 * (1-65535)
Protocol	ALL
Enable	Disable

At the bottom are "Apply" and "Cancel" buttons.

Figure 261 : La finalisation de la configuration VPN dans le point d'accès

12. Connexion au tunnel :

Un employé désire se connecter à distance au serveur de son entreprise en utilisant sa connexion Internet. Pour cela, il peut passer par le VPN. Pour commencer, il est nécessaire de faire un clic droit sur l'icône du réseau et d'ouvrir le « Centre Réseau et partage ». Une fois cette fenêtre ouverte, il convient de cliquer sur « Configurer une nouvelle connexion ou un nouveau réseau » pour créer le tunnel entre le serveur et l'ordinateur.

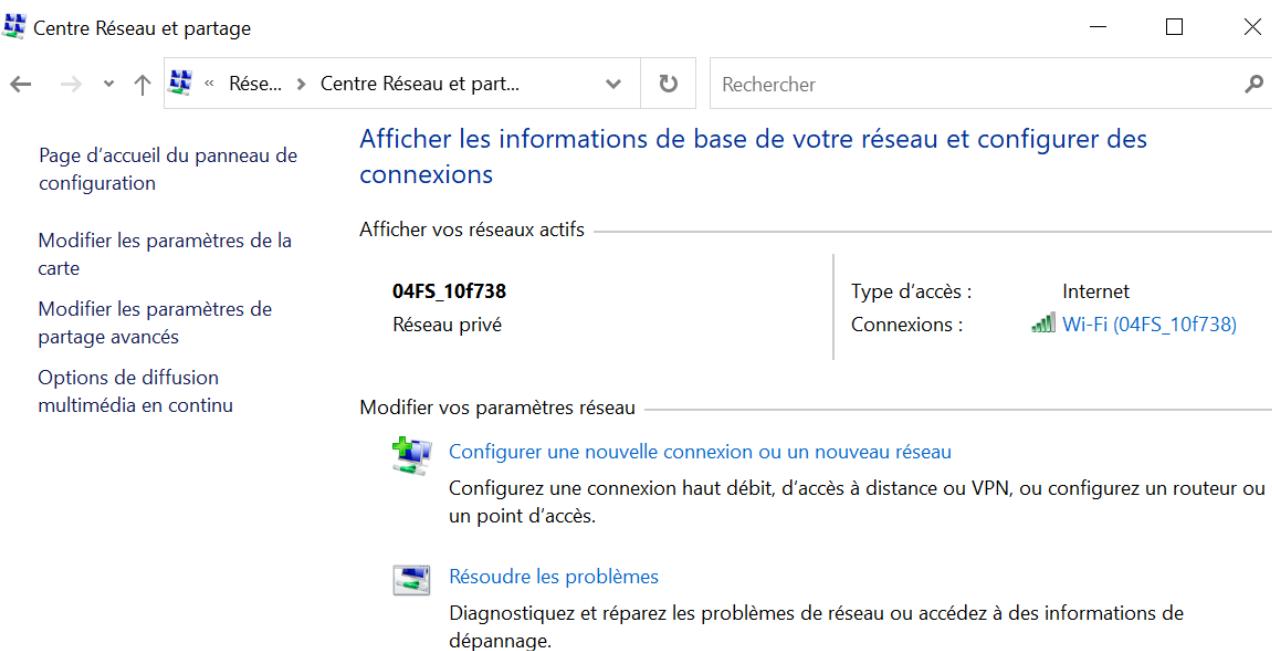


Figure 262 : Centre Réseau et partage

- Nous allons sélectionner l'option « Connexion à votre espace de travail » et ensuite cliquer sur « Suivant ».

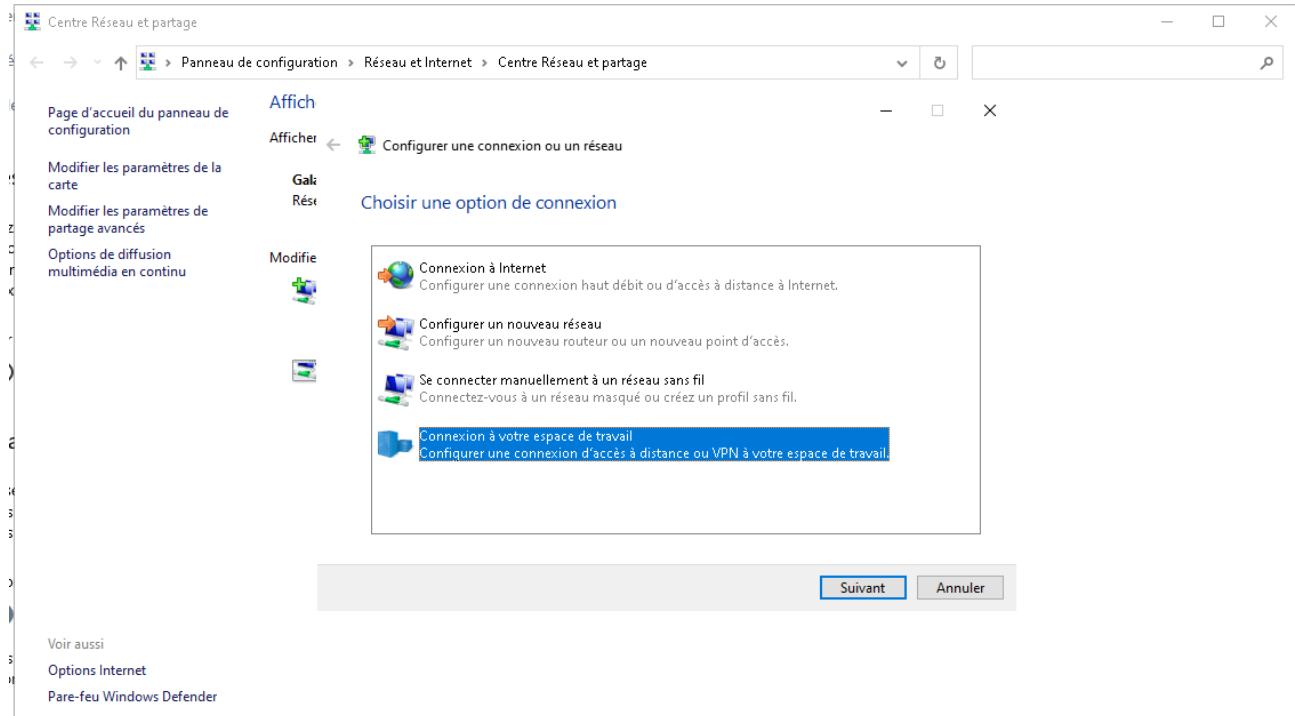


Figure 263 : Connexion à votre espace de travail

- On clique sur « Utiliser ma connexion Internet (VPN) »

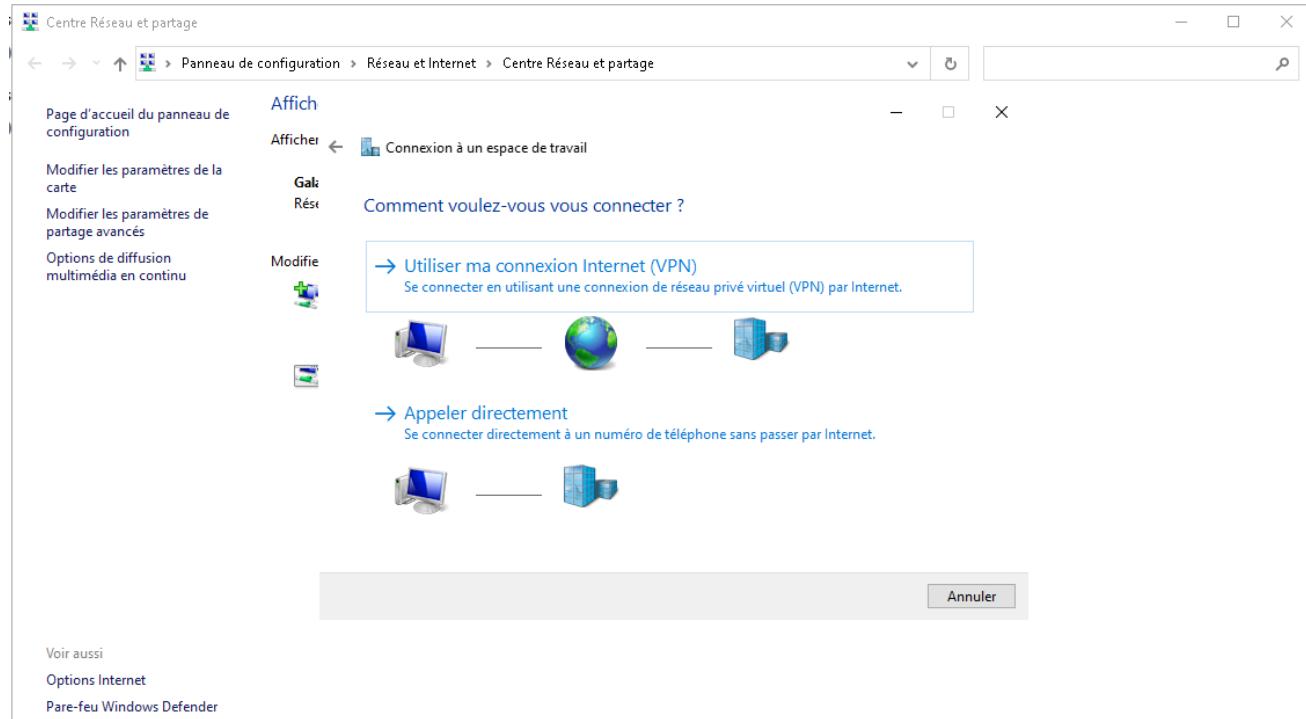


Figure 264 : Utiliser ma connexion Internet « VPN »

- Une nouvelle fenêtre apparaît et vous demande l'adresse Internet ou l'adresse IP du serveur auquel vous souhaitez vous connecter. Il est également possible de renommer le nom de la connexion. Ensuite, cliquons sur « Créer ».
- Pour trouver l'adresse IP publique (Internet-Entreprise), vous pouvez vous rendre sur le site <http://www.mon-ip.com/> à partir de votre serveur.
- Assurez-vous que l'adresse IP est fixe auprès de votre opérateur.

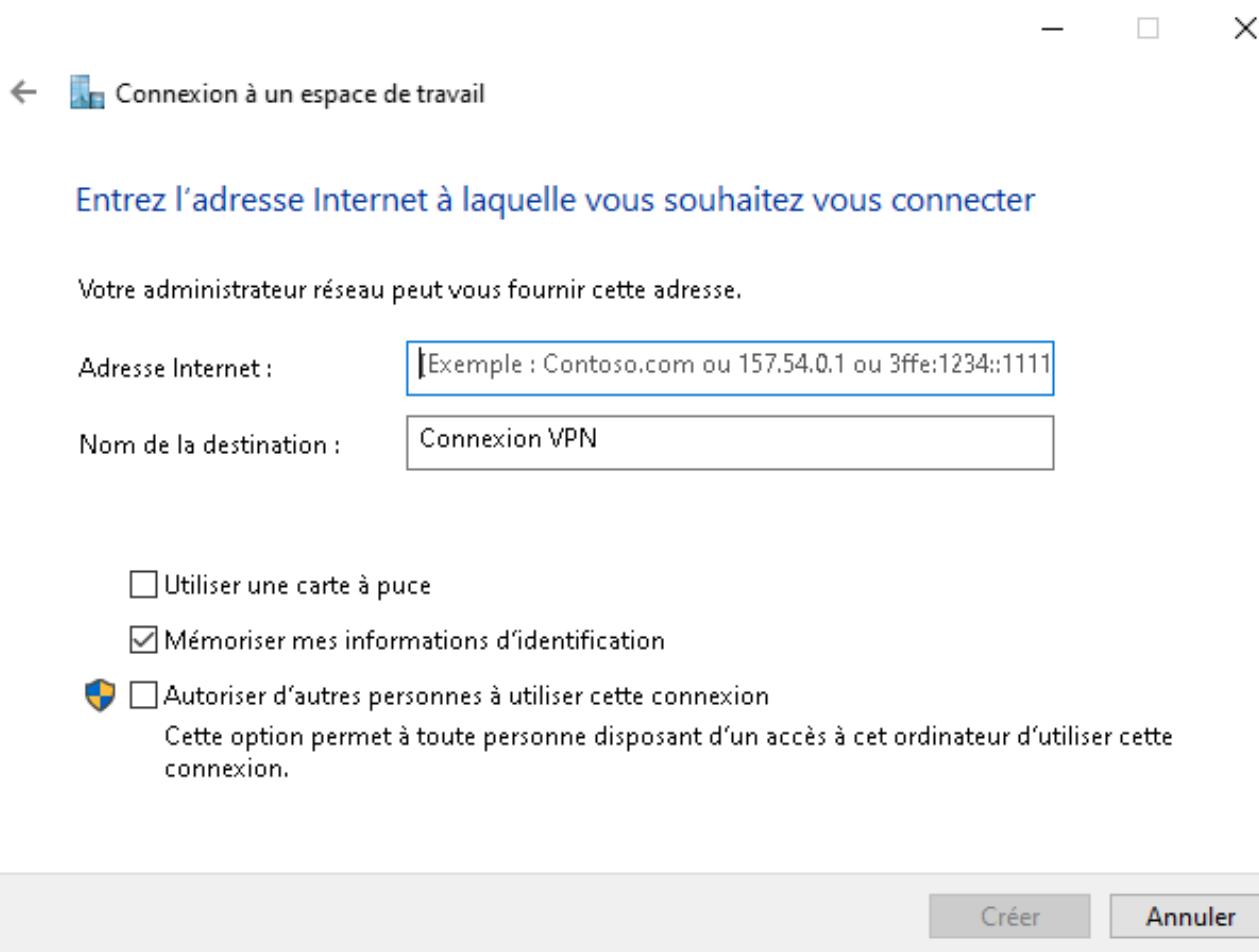


Figure 265 : La saisie de l'adresse Internet

- Nous pouvons maintenant voir que le VPN a été ajouté à la liste des connexions disponibles. Pour se connecter, il suffit de cliquer sur « Connexion ». L'utilisateur doit ensuite saisir ses identifiants liés au serveur de son bureau pour se connecter au VPN.

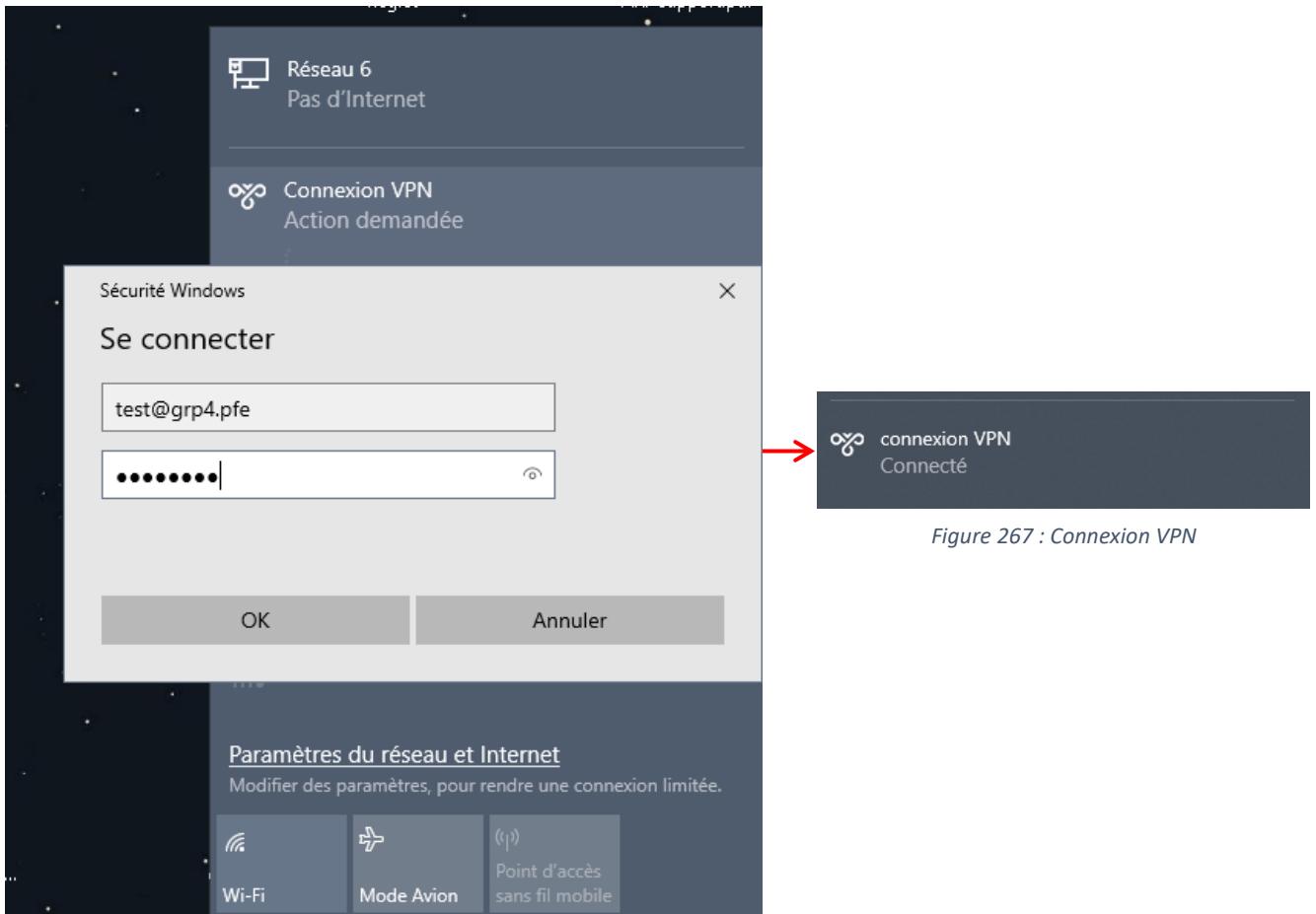


Figure 267 : Connexion VPN

Figure 266 : L'authentification VPN

- Enfin, nous pouvons vérifier que les lecteurs réseau sont désormais accessibles, ce qui signifie que votre VPN fonctionne correctement.

Conclusion générale

Nous avons été chargés de mener à bien un projet de mise en place d'un réseau informatique dans une entreprise dans le cadre de notre projet de fin d'études à l'école supérieure de technologie de Salé (ESTS). Ce projet a été une occasion pour nous de mettre en pratique nos connaissances théoriques et pratiques acquises durant ces deux dernières années à l'ESTS.

Travailler en groupe a été une réussite pour nous. Nous avons tous eu des tâches équitablement réparties. Bien que nous ayons eu des opinions différentes, nous avons trouvé des points d'entente pour que tout le monde soit satisfait, ce qui a rendu le travail en équipe très productif.

Cependant, nous avons également rencontré des difficultés, en particulier le manque de temps car le projet de fin d'études est mené en parallèle avec nos études. Nous avons été contraints de trouver rapidement des solutions efficaces dans un bref délai.

Table de matière

Chapitre I : Étude des matériaux	4
I. Un switch :.....	5
1. Définition :.....	5
2. Les différents types de switches :.....	6
3. Un switch manageable (administrable) :	7
II. Un routeur :.....	7
1. Définition :.....	7
2. Les différents types de routeurs :.....	7
a) Routeur de cœur de réseau :.....	7
b) Routeur de périphérie :	8
c) Routeur de distribution	9
d) Routeur sans fil :	9
e) Routeur virtuel :	9
III. Un serveur :	10
1. Définition :.....	10
2. Les différents types de serveurs :	10
IV. Un point d'accès :	11
1. Définition :.....	11
V. Un pare-feu :.....	12
1. Définition :.....	12
2. Types de pare-feu :	12
Chapitre II : Infrastructure du réseau.....	13
I. Infrastructure du réseau :	14
1. Les services installés :	14
2. Plan d'adressage de réseau :	15
II. Schéma de l'architecture de réseau :	15
1. Plan d'adressage des machines virtuelles :	16
III. Les matériaux utilisés :	16
1. Un switch :.....	16
2. Un routeur.....	18
3. Un serveur :	19
4. Un point d'accès :	20
5. Un pare-feu :	21
IV. Configuration des éléments d'interconnexion :	22
1. Configuration du switch :	22
2. Configuration de routeur :	23
Chapitre III : La virtualisation	24

I.	Contexte de virtualisation :	25
1.	Définition :	25
2.	Historique :	26
3.	Pourquoi virtualiser ?	27
4.	Hyperviseur :	27
a)	Hyperviseur type 1 :	27
b)	Hyperviseur type 2 :	27
II.	Virtualisation des serveurs :	28
1.	VMware vSphere :	28
2.	VMware ESX et ESXI :	28
3.	VMware vSphere 6.7 :	29
4.	Installation de VMware vSphere ESXI 6.7 :	29
III.	Configuration de VMware vSphere ESXi 6.7.0 :	34
1.	La configuration des VLAN :	37
	Chapitre IV : Mise en œuvre du réseau des employés.	45
I.	Services réseaux :	46
1.	Système des noms de domaine DNS :	46
a)	Définition :	46
b)	Fonctionnement d'un DNS :	47
c)	Types de DNS :	47
d)	Hiérarchie d'un DNS :	47
e)	Résolution du nom par un hôte :	48
f)	Résolution inverse :	48
2.	Protocole de configuration dynamique des hôtes (DHCP) :	49
a)	Définition :	49
3.	Les services d'annuaire LDAP :	50
4.	Active Directory (AD) :	51
5.	Active Directory Domain Services (AD DS):	52
a)	Les avantages d'AD DS :	53
b)	Les services fournis par AD DS :	53
II.	Politique de sécurité :	54
1.	Généralité :	54
2.	Vulnérabilité :	54
III.	Serveur RADIUS :	55
1.	Définition :	55
2.	Scénario d'utilisation du serveur RADIUS :	56
IV.	La phase de l'installation :	57
1.	Installation de Windows Server :	57
a)	L'installation et la configuration de l'Active Directory :	61

2. Configuration de l'Active Directory pour un nouveau domaine :	66
a) Etendue du groupe :	74
3. L'installation et la configuration du DNS :	75
4. L'installation et la configuration du serveur RADIUS :	79
a) Installation du Serveur RADIUS (NPS) :	79
b) Configuration du NPS :	80
i. Configuration des clients RADIUS :	80
c) Test de fonctionnement :	84
Chapitre V : Mise en œuvre du réseau des invités.....	87
I. Portail Captif :	88
1. Définition :	88
2. Fonctionnement :	88
II. Pfsense :	89
1. Définition :	89
2. Les services du Pfsense :	90
3. Le cycle de vie de l'authentification :	90
4. L'installation du PfSense :	91
III. Configuration du PfSense :	94
1. L'interface Web PfSense :	94
a) DHCP et DNS :	96
b) Pare-feu :	97
c) Portail captif :	97
2. Création d'un groupe et des utilisateurs :	100
a) Test d'authentification :	101
Chapitre VI : Firewall & DMZ.....	102
I. DMZ :	103
1. Définition :	103
2. L'architecture DMZ :	103
II. Firewall :	104
1. Définition :	104
2. Le but d'un pare-feu :	105
3. Filtrage de contenu :	106
4. Filtrage des paquets :	106
5. Types de filtrage :	106
a) Filtrage simple des paquets (Stateless) :	106
i. Son principe :	106
ii. Ses limites :	107
b) Filtrage des paquets avec état (stateful) :	107
i. Son principe :	107

ii. Ses limites :.....	108
c) Firewall applicatif :.....	109
i. Son principe :.....	109
ii. Ses limites :.....	110
6. Les types de pares-feux :.....	111
a) Firewall bridge :.....	111
b) Firewall logiciel :.....	111
c) Firewall matériel :.....	111
d) FortiGate 100A :.....	112
III. Mise en place d'une DMZ avec FortiGate 100A :	112
IV. Les serveurs implémentés dans la DMZ :.....	119
1. Apache http Server :	119
a) Définition :.....	119
b) Fonctionnalités :	120
c) Modes de fonctionnement :	120
d) Configuration de Apache2 sur Ubuntu :.....	121
V. Le serveur de messagerie :.....	125
1. Qu'est-ce qu'un serveur de messagerie ?	125
2. Les types de serveur de messagerie :.....	125
3. Le fonctionnement du serveur de messagerie :.....	126
4. Installation et configuration du serveur de messagerie :.....	127
a) PostFix :.....	127
b) Dovecot :	128
c) Evolution :	128
d) L'installation du serveur de messagerie « Postfix » :	128
e) L'installation du client messagerie « Evolution » :	131
f) L'installation du serveur de messagerie « Dovecot » :	134
Chapitre VII : La VoIP	136
I. Etude théorique de la VoIP :	137
1. Définition :.....	137
2. Standard de la VoIP :.....	137
3. Fonctionnement :	138
II. Elastix :	139
1. Installation de Elastix :	140
a) Configuration Elastix :.....	144
b) Test de communication :	149
Chapitre VIII : Mise en place d'un serveur de supervision	150
I. La supervision informatique :	151
1. Le protocole SNMP :.....	151

a) Les requêtes SNMP :	152
b) Les modes de la supervision :	153
2. Les solutions de supervision :	153
a) Les solutions propriétaires de supervision :	153
b) Les solutions propriétaires de supervision :	154
c) Installation et implémentation de Nagios :	155
i. Nagios XI :	155
II. Supervision des matériaux :	159
1. Supervision du Switch :	159
2. Supervision du routeur :	161
3. Supervision de firewall :	163
III. Supervision des machines :	165
1. Windows Serveur :	165
2. Pfsense :	169
3. Linux Server :	171
a) Web server :	172
b) Mail server :	174
Chapitre IX : VPN	175
I. La partie théorique du VPN :	176
1. Définition :	176
2. Les réseaux privés dans les entreprises :	177
3. Les réseaux privés virtuels :	177
4. Les cas d'utilisation :	178
5. Les termes d'utilisation :	179
6. Les types de VPN :	180
7. Les avantages et les inconvénients de VPN :	181
a) Les avantages du VPN :	181
b) Les inconvénients du VPN :	181
8. Les protocoles du VPN :	182
9. Les modes de transports du VPN :	183
10. L'installation et configuration du VPN :	184
a) La mise en place du VPN :	184
b) La configuration du VPN :	189
11. Stratégie accès réseau VPN :	193
12. Connexion au tunnel :	199

Webographie

Switch:

https://www.cisco.com/c/dam/global/fr_fr/assets/documents/pdfs/datasheet/switching/Catalyst3750.pdf

<https://www.nowteam.net/commutateur-reseau-role-switch/>

Routeur:

<https://www.cisco.com/c/en/us/products/routers/1800-series-integrated-services-routers-isr/index.html>

<https://www.cisco.com>

Point accès:

https://www.cisco.com/c/fr_ca/solutions/small-business/resource-center/networking/what-is-access-point.html

Firewall:

https://www.cisco.com/c/fr_fr/products/security/firewalls/what-is-a-firewall.html

Serveur VSphere:

<https://www.lebigdata.fr/vsphere-vmware>

RADIUS :

https://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service

<https://web.maths.unsw.edu.au/~lafaye/CCM/authentification/radius.htm>

Pfsense :

<https://www.pfsense.org/>

<https://fr.wikipedia.org/wiki/PfSense>

Firewall:

<https://www.layer7solutions.com/download/datasheet/Fortigate-100a-datasheet.pdf>

Apache2:

<https://doc.ubuntu-fr.org/apache2>

Postfix:

<https://www.postfix.org/>

VoIP:

<https://choisirpro.com/standard-telephonique/elastix>

Nagios XI:

<https://www.nagios.org/>