

DÉPARTEMENT: INFORMATIQUE  
FILIÈRE: ADMINISTRATION RÉSEAUX  
INFORMATIQUES

## PROJET DE FIN D'ÉTUDES

Mise en place d'une infrastructure réseau pour une entreprise.

### RÉALISÉ PAR :

INEDJAREN Taha  
ZEROUAL Khalid  
SOTIH Mohammed Amine  
TRAIK Ahlam  
AMRAN Imane

**ENCADRÉ PAR :**  
M.Badaoui

**Jury :**  
M.Badaoui  
M.Amraoui  
M.Elhaziti  
Mme.Bouhaddour

2022-2023





## REMERCIEMENTS

Avant tout, nous souhaitons exprimer notre gratitude envers notre encadrant, monsieur Badaoui, qui a su nous guider, orienter et conseiller tout au long de ce projet.

Nous voulons également remercier tous les professeurs de l'EST pour leur qualité d'enseignement qu'ils nous ont offert pendant notre DUT Administration des réseaux Informatiques.

# SOMMAIRE

LISTE DES ABRÉVIATIONS.....
INTRODUCTION GENERALE .....
CAHIER DE CHARGES.....
GESTION DE PROJET .....
Infrastructure Réseau et Virtualisation .....
PARTIE I .....
CHAPITRE 1 : Architecture Réseau .....
I.    Architecture Proposée .....
II.    Etude et Configuration Matérielle.....
CHAPITRE 2 : La virtualisation.....
I.    Etude de la virtualisation.....
II.    La virtualisation dans VMware ESXI.....
CONCLUSION .....
PARTIE II .....
Les Méthodes d'Authentification.....
CHAPITRE 1 : Authentification des employés .....
I.    Le protocole RADIUS.....
II.    Les services réseaux.....
III.    Implémentation d'un serveur RADIUS.....
CHAPITRE 2 : Authentification des invitées.....
I.    Le Portail Captif.....
II.    PfSense.....

PARTIE III .....
CHAPITRE 1 : Le Pare-feu.....
I.    Le firewall .....
II.   Configuration.....
CHAPITRE 2 : La zone DMZ.....
I.    La zone DMZ .....
II.   Le serveur de messagerie .....
III.  Le serveur web (Apache).....
CONCLUSION .....
PARTIE IV.....
Supervision et Voip.....
CHAPITRE 1 : La supervision .....
I.    Etude de la supervision .....
II.   Nagios XI .....
CHAPITRE 2 : La Voip.....
I.    Etude de la Voip.....
CONCLUSION GÉNÉRALE .....
TABLE DES MATIERES .....

# LISTE DES ABRÉVIATIONS

AP: Access Point	
DHCP: Dynamic host configuration Protocol	
DNS: Domain Name System	ACL: Access List Control
IMAP: Interactive Message Access Protocol	DMZ: Demilitarized zone
LAN: Local area network	Http: Hypertext markup language
LDAP: Lightweight Directory Access Protocol	Https: Hypertext Transfer Protocol Secure
MDA: Mail Delivery Agent	MAC: Media Access Control
MTA: Mail Transfer Agent	Mib: Management Information Base
MUA: Mail User Agent	NAS: Network Attached Storage
NAS: Network Access Server	OID: Object identifier
NAT: Network Address Translation	Radius : Remote Authentication Dial-In User Service
OS: Operating System	RTC : Réseau Téléphonique Commuté
PoE: Power over Ethernet	RTCP : protocole de contrôle RTP
POP3: Post Office Protocol	RTP : Real-time Transfert Protocole
PPTP: Point-To-Point-Tunneling-Protocol	SIP: Session Initiation Protocol
SMTP: Simple Mail Transfer Protocol	SNMP: Simple Network Management Protocol
SSID: Service Set Identifier	SSH: Secure Shell
TLD: Top Level Domain	SSL: Secure socket layer
UDP: User Datagram Protocol	TCP: Transmission Control Protocol
VLAN: Virtual local area network	Voip : Voice over Internet Protocol
WAN: Wide Area Network	
WAN: Wide area network	
WPA : Wi-Fi Protected Access	

# INTRODUCTION GENERALE

Assurer la sécurité des réseaux informatiques est essentiel pour la protection des informations et le bon fonctionnement d'une organisation, d'un établissement ou d'une entreprise.

Dans le cadre de ce projet de fin d'étude, nous allons mettre en place une infrastructure réseau qui permettra aux personnes internes à l'entreprise (employés, administrateurs et invités) de se connecter en toute sécurité au réseau. Cette infrastructure doit être réalisée en utilisant des technologies qui garantiront la sécurité et le contrôle du réseau.

Nous commencerons par les protocoles et méthodes d'authentification, qui sont des éléments clés dans la protection du réseau et la gestion des différents utilisateurs.

La création d'une zone DMZ pour les services de l'établissement est également une nécessité dans notre architecture. Elle permettra d'isoler ces services accessibles depuis le réseau externe, du réseau interne que nous souhaitons protéger.

En ce qui concerne la supervision et le suivi du bon fonctionnement du matériel et des serveurs, la surveillance est primordiale et son implémentation dans notre architecture servira à l'analyse des ressources et à la prévention des problèmes.

Enfin, nous aborderons le concept de VoIP dans ce projet, afin d'offrir aux utilisateurs la possibilité de communiquer sans coûts supplémentaires.

# CAHIER DE CHARGES

Le système à mettre en place est un système qui permette aux employés et aux administrateurs au sein de l'entreprise de se connecter d'une manière sécurisée au réseau de l'entreprise. De plus, ce système offre aussi la possibilité aux invités de se connecter au réseau en mode sans fil.

Notre système est basé sur les composants ci-dessous :

- Serveurs d'authentification
- Portails captifs
- Points d'accès Wifi avec support VLAN
- Switch et routeurs avec support VLAN
- Firewall (Hardware Software)
- Zone DMZ
- Supervision
- Virtualisation (Type VMWare)

Le système que nous allons mettre en œuvre doit pouvoir assurer trois types de connexion au réseau de l'entreprise :

- Tout ordinateur se connectant sur le réseau sans-fil doit être identifié au même titre qu'un ordinateur filaire.
- L'introduction du réseau sans-fil ne doit pas remettre en cause les principes de sécurité déjà existants.
- Un même ordinateur doit être vu sur le réseau de façon identique qu'il utilise une connexion filaire ou sans-fil.

# GESTION DE PROJET

La gestion de projet est l'ensemble des techniques et compétences utilisées pour planifier, organiser et diriger l'exécution d'un projet afin de réaliser les objectifs dans les délais impartis, en raison de complexité de notre sujet il va falloir fournir un travail conséquent car il ouvre pratiquement l'ensemble de bases que l'on peut trouver au sein d'une entreprise ou école.

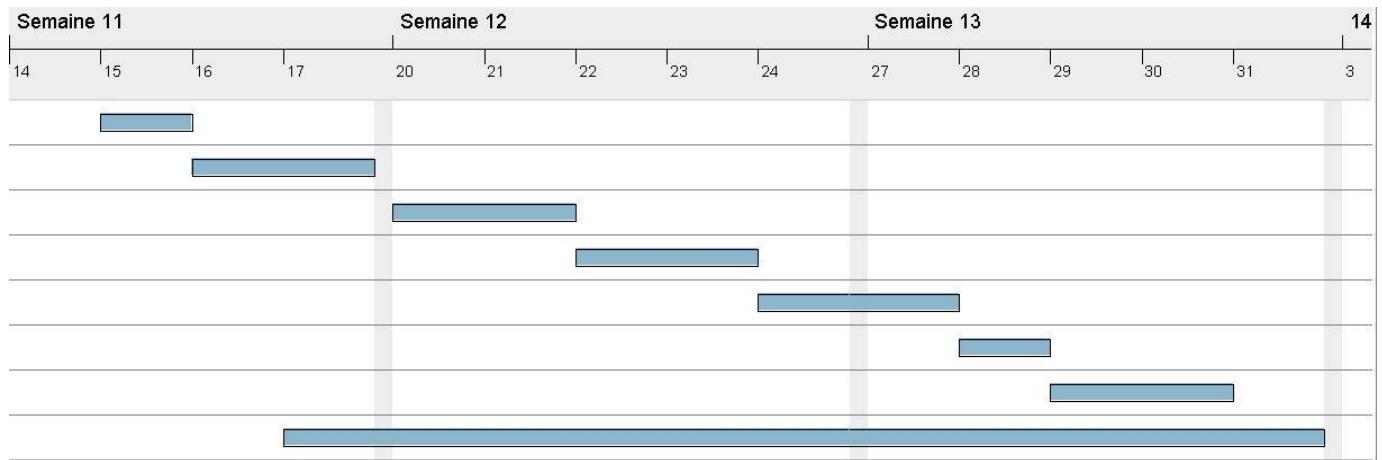
Ainsi, il est important de définir les différentes tâches, de les subdiviser en fonction du délai, puis les attribuer aux membres du groupe afin de mener à bien le projet.

## 1. Tableau des tâches :

GANTT project		
Nom	Date de début	Date de fin ▼
identification de matériels	15/03/2023	15/03/2023
réalisation de la topologie	16/03/2023	17/03/2023
virtualisation du serveur	20/03/2023	21/03/2023
implantation du VLAN des employés (authentification radius)	22/03/2023	23/03/2023
implantation du VLAN des invités (authentification portail captif)	24/03/2023	27/03/2023
implantation du VLAN des administrateurs (supervision Nagios)	28/03/2023	28/03/2023
configuration des services DMZ (web-messagerie)	29/03/2023	30/03/2023
création du rapport	17/03/2023	31/03/2023

## 2. Gantt

Pour Afin d'assurer la réussite de ce projet, nous avons élaboré un diagramme de Gantt, un instrument couramment employé en planification et gestion de projet, qui permet de présenter graphiquement dans le temps les différentes étapes impliquées dans un projet.



# PARTIE I

# Infrastructure Réseau et Virtualisation

## **Introduction :**

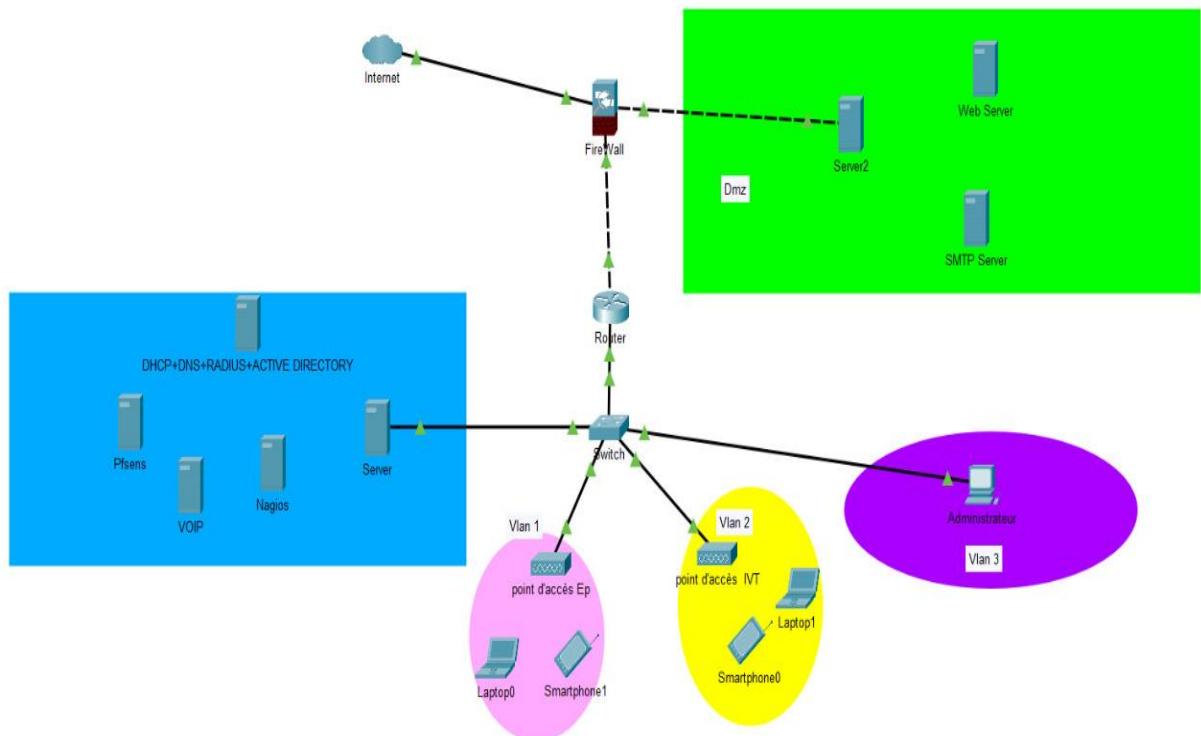
Dans la première partie de notre projet portera sur la mise en place d'une infrastructure réseau qui répondra aux exigences de cahier des charges. Nous procéderons ensuite à l'étude et à la configuration du matériel nécessaire. Enfin, nous aborderons la virtualisation en expliquant notre approche de la virtualisation sous VMware ESXI.

# CHAPITRE 1 : Infrastructure Réseau

Dans Au cours de ce premier chapitre, nous présenterons l'architecture globale de notre réseau et l'adressage correspondant. Nous procéderons ensuite à une étude matérielle des ressources disponibles et de leur configuration.

## I. Architecture Proposée

### 1. Schéma de l'architecture globale de notre réseau



➤ Figure 1 Architecture globale

### 2. Tableaux d'adresses

VLAN	Nomination	Réseau	Passerelle
10	Employés	192.168.10.0 /24	192.168.10.1
20	Invités	192.168.20.0 /24	192.168.20.1
30	Administrateurs	192.168.30.0 /29	192.168.30.1
40	WAN (Pfsense)	192.168.50.0 /28	192.168.50.2
50	DMZ	192.168.50.16 /28	192.168.50.17

➤ Tableau Plan d'adressage des zones

Zone	Réseau	Serveur	Adresse
DMZ	192.168.50.16 /28	Web / messagerie	192.168.50.18
LAN	VLAN 10	DHCP + DNS + Radius + LDAP	192.168.10.254
	VLAN 20	Pfsense + DHCP	192.168.20.254
		DNS	192.168.20.3
	VLAN 30	Nagios	192.168.30.10
	VLAN 40	Pfsense (WAN)	192.168.50.1

Matériel	Interfaces	Adresse / VLAN
Switch	Gi1/o/1 – Gi1/o/6	Vlan 10
	Gi1/o/7 – Gi1/o/12	Vlan 20
	Gi1/o/13 – Gi1/o/18	Vlan 30
	Gi1/o/22 – Gi1/o/25	Vlan 40
	Gi1/o/19 – Gi1/o/20	Trunk
Pare-feu	Port 4(interne)	Vlan 10
		Vlan 20
		Vlan 30
		Vlan 40
	DMZ	192.168.50.17
Routeur	WAN	
	Gio/o	192.168.50.1

## II. Etude et Configuration Matérielle

### 1. Le switch



Figure 2 switch Cisco Catalyst 3750

Un switch, également appelé commutateur, est un équipement sous forme d'un boîtier qui fonctionne comme un pont multiport et qui permet de connecter plusieurs périphériques d'un réseau informatiques.

Le commutateur est responsable de l'analyse des trames qui arrivent sur les ports d'entrée. Il filtre les données afin de les envoyer au bon port (RJ45). Par conséquent, le commutateur a une double fonction de filtrage de connectivité.

#### a. Les caractéristiques de switch Cisco Catalyst 3750

Caractéristique	Description
Marque	CISCO
Catégorie	SWITCH - HUB ETHERNET
Caractéristiques	Contrôle du flux, Fonction duplex intégral, Layer 3 switching, auto-détection par dispositif, routage IP, compatible DHCP, auto-négociation, prise en charge d'ARP, prise en charge du réseau local (LAN) virtuel
Performances	Capacité de commutation : 32 Gbps Performances de transfert : 35,7 Gbps
RAM	128 Mo
Mémoire flash	16 Mo Flash
Interfaces	24 x 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x console - RJ-45 gestion 1 x périphérique réseau empilable x 2

Tableau 4 caractéristiques de switch Cisco Catalyst 3750

b. Configuration du switch

La configuration	Les commandes
<b>La création des vlans</b>	<pre>SW1(config)#vlan 10 SW1(config-vlan)#name employe SW1(config-vlan)#ex SW1(config)#vlan 20 SW1(config-vlan)#name invites SW1(config-vlan)#ex SW1(config)#vlan 30 SW1(config-vlan)#name administrateur SW1(config-vlan)#ex SW1(config)#vlan 40</pre>
<b>Affectation des ports aux vlans</b>	<pre>SW1(config)#interface range Gi1/0/1-5 SW1(config-if)#switchport mode access SW1(config-if)#switchport access vlan 10 SW1(config-if)#ex SW1(config)#interface range Gi1/0/6-10 SW1(config-if)#switchport mode access SW1(config-if)#switchport access vlan 20 SW1(config-if)#ex SW1(config)#interface range Gi1/0/11-15 SW1(config-if)#switchport mode access SW1(config-if)#switchport access vlan 30 SW1(config-if)#ex SW1(config)#interface Gi1/0/16 SW1(config-if)#switchport mode access SW1(config-if)#switchport access vlan 40</pre>
<b>Configuration des ports trunk</b>	<pre>SW1(config)# interface range Gi1/0/24-25 SW1(config)#switchport trunk encapsulation dot1q SW1 (config-if)#switchport mode trunk SW1(config-if)#ex</pre>
<b>Affectations des adresses aux vlans</b>	<pre>SW1(config)#interface vlan 10 SW1(config-if)#ip address 192.168.10.1 255.255.255.0 SW1(config-if)#ex</pre>

Tableau 5 configuration du switch

## 2. Le routeur (Cisco 1900)



➤ Figure 3 routeur Cisco 1900

### a. Définition

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets entre réseaux indépendants. C'est un équipement de couche 3 par rapport au modèle OSI. Le routage est réalisé selon un ensemble de règles formant la table de routage.

### b. Spécifications

Caractéristiques	Description
Protocole de liaison de données	Ethernet, Fast Ethernet, Gigabit Ethernet
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)
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

➤ Tableau 6 caractéristique du routeur Cisco 1900

### 3. Routeur sans fil (Linksys WRT54G)



➤ Figure 4 Routeur sans fil (Linksys WRT54G)

#### a. Définition

Le Routeur haut débit Sans fil-G Linksys WRT54G est un périphérique réseau 3 en 1 qui permet à tout votre réseau de partager une connexion Internet haut débit par Câble ou DSL. Il peut servir de point d'accès sans fil, de commutateur Ethernet à 4 ports, ou de routeur.

#### b. Caractéristiques

Caractéristiques	Description
Ports	4 port lan et 1 wan
Débit de transfert de données	54 Mbits/s
Bande de fréquence	2.4 GHz
Protocole de liaison de données	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g
Poids	0.5 kg
Caractéristiques supplémentaires	Il support Radius et le filtrage par MAC

⊕ Tableau 7 Caractéristiques du routeur sans fil (LinksysWRT54G)

#### 4. Routeur LINKSYS Wireless-N



➤ Figure 5 Modem routeur ADSL2 (TD-W8960N)

##### a. Définition

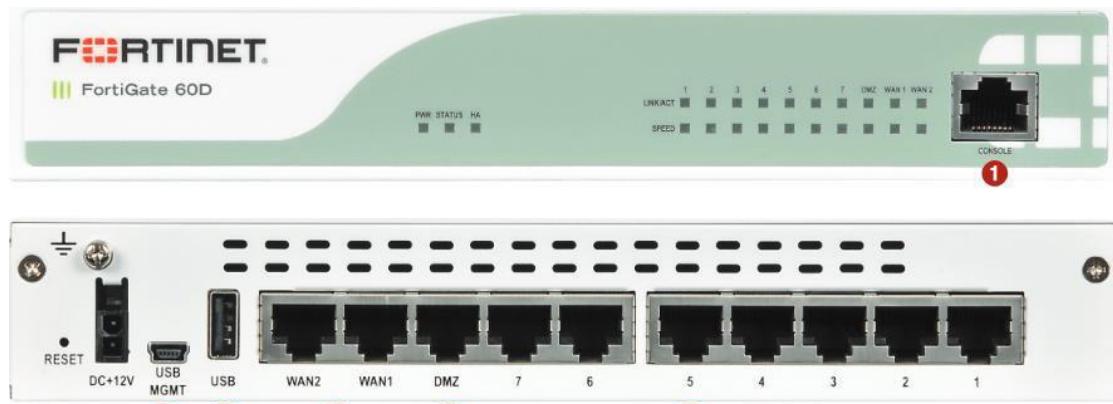
Le Linksys Wireless-N Gigabit Security est un routeur sans fil haut débit de la marque Linksys, qui utilise la norme sans fil N pour offrir une connectivité sans fil rapide et fiable à des vitesses allant jusqu'à 300 Mbps. Il est équipé de plusieurs ports Gigabit Ethernet pour une connectivité filaire rapide et offre également des fonctionnalités de sécurité avancées pour protéger votre réseau contre les menaces en ligne telles que les virus, les logiciels malveillants et les attaques de pirates informatiques. Le routeur prend également en charge des fonctionnalités avancées telles que la gestion du trafic, la QoS (qualité de service), le contrôle parental et la configuration sans fil facile.

##### b. Caractéristiques

Voici les caractéristiques du Linksys Wireless-N Gigabit Security:

- **Norme sans fil :** IEEE 802.11n (jusqu'à 300 Mbps)
- **Ports Ethernet :** 4 ports Gigabit Ethernet pour des connexions filaires rapides
- **Sécurité sans fil avancée :** cryptage WPA/WPA2, pare-feu SPI, protection DoS (Denial of Service), filtrage des adresses MAC, etc.
- **Antennes :** 3 antennes internes pour une couverture sans fil étendue
- **Configuration facile :** utilisation de l'assistant de configuration sans fil Linksys pour une installation rapide et facile.
- **Fonctionnalités avancées :** gestion du trafic, QoS (qualité de service), contrôle parental, support VPN, etc.
- **Interface utilisateur Web :** pour configurer et gérer le routeur via un navigateur Web.
- **Prise en charge IPv6 :** pour une compatibilité avec les futures adresses IP.

## 5. Pare-feu (Firewall)



➤ Figure 6 pare-feu FortiGate-60D

1. Port Console
2. Port USB D'Administration
3. Port USB
4. Deux Interfaces WAN en 10/100/1000 Mbits/s.
5. Une Interface DMZ en 10/100/1000 Mbits/s.
6. Sept Interfaces internes en 10/100/1000 Mbits/s.

### a. Définition

Un pare-feu (Firewall) est un dispositif (matériel ou logiciel) de sécurité réseau qui établit une barrière entre les réseaux internes sécurisés et contrôlés auxquels on peut faire confiance et les réseaux extérieurs non fiables, comme Internet.

Les pares-feux surveillent le trafic réseau entrant et sortant et décident d'autoriser ou de bloquer un trafic spécifique en fonction de critères définis qui dépendent de la politique de sécurité. Le contrôle des accès peut reposer sur l'adresse IP des paquets, le nom de domaine, le protocole d'accès ou encore sur le numéro de port.

### b. Caractéristiques de notre Pare-feu

#### **Fortinet Fortigate-60D :**

FortiGate-60D est un pare-feu de nouvelle génération produit par Fortinet. Il offre une protection puissante contre les menaces pour les entreprises de moyennes tailles. Il Protège contre les logiciels et les sites Web malveillants en utilisant des renseignements continus sur les menaces fournis par les Services de sécurité FortiGuard Labs et détecte les attaques inconnues à l'aide d'une analyse dynamique.

**Caractéristiques :**

Débit maximum du Firewall : 1500 Mbps

Débit maximum de IPS : 200 Mbps

100 tunnels simultanés au maximum pour les connexions VPN IPSec.

Suite de sécurité avec IPS, Antivirus, Filtrage web, Contrôle applicatif, Antispam

### **Conclusion :**

Dans ce chapitre nous avons vu l'architecture réseau qu'on a proposé avec l'adressage, ainsi que les différents équipements et leurs caractéristiques que nous avons utilisé pendant la réalisation de notre projet de fin d'étude.

# CHAPITRE 2 : La virtualisation

Les logiciels modernes, qu'ils soient des systèmes d'exploitation ou des applications, nécessitent de plus en plus de données, de puissance de traitement et de mémoire.

La virtualisation est une méthode qui permet d'exécuter plusieurs systèmes d'exploitation et applications simultanément sur un seul ordinateur, ce qui est une solution économique pour réduire les coûts physiques. Dans ce chapitre, nous allons examiner ce concept et commencer à virtualiser nos serveurs.

## I. Etude de la virtualisation

### 1. Définition

La virtualisation est une technologie qui vous permet de créer des services informatiques utiles à l'aide de ressources qui sont généralement liées au matériel. Elle vous permet d'exploiter toute la capacité d'une machine physique en la répartissant entre de nombreux utilisateurs ou environnements différents.

Les intérêts de la virtualisation sont multiples. On peut citer :

- L'utilisation optimale des ressources d'un parc de machines (répartition des machines virtuelles sur les machines physiques en fonction des charges respectives),
- L'économie sur le matériel (consommation électrique, entretien physique, surveillance),
- L'installation, tests et développements des applications sans endommager le système d'exploitation principal de l'utilisateur (le système hôte).

### 2. La terminologie

La virtualisation consiste donc à faire exécuter plusieurs noyaux en parallèle de façon isolé sur une même machine.

- Le système d'exploitation accueillant les VM est appelé hôte
- Les systèmes virtualisés sont appelés systèmes invités ou VM
- Le composant du système hôte réalisant la virtualisation se nomme l'hyperviseur. Les systèmes invités et hôtes peuvent être totalement différents les uns des autres.

### 3. Le but de la virtualisation

La virtualisation a pour but de faire fonctionner plusieurs systèmes, applications ou bien serveurs sur un seul serveur physique. Voici le principe de fonctionnement :

- Un système d'exploitation est installé sur un serveur physique unique, il a vocation à accueillir d'autres systèmes d'exploitation.
- Un logiciel de virtualisation est ensuite installé sur le serveur physique, il servira à créer des environnements clos qui accueilleront les différents systèmes d'exploitation.
- Chaque machine virtuelle aura un système invité et qui fonctionnera de manière complètement indépendante des autres machines virtuelles. Mais elles auront toutes un accès aux ressources du serveur physique.

La virtualisation est applicable à plusieurs niveaux. Réseaux, données, processeurs, mémoire, environnement de travail, serveurs etc. Elle permet une migration en douceur vers « le cloud computing» .

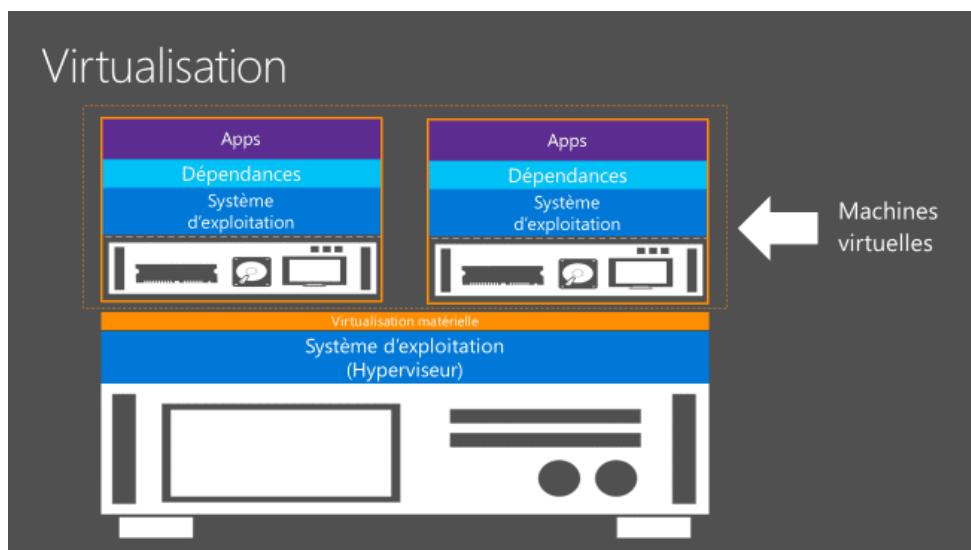
## 4. L'Hyperviseur

Un hyperviseur, également appelé moniteur de machine virtuelle, est un processus qui crée et exécute des machines virtuelles (VM). Il permet à un ordinateur hôte de prendre en charge plusieurs VM clientes en partageant virtuellement ses ressources, telles que la mémoire et la capacité de traitement.

## 5. Fonctionnement

La virtualisation consiste à utiliser efficacement les ressources d'un ordinateur physique (hyperviseur) en créant plusieurs machines virtuelles.

Ces machines virtuelles se partagent les ressources telles que le processeur, la mémoire vive, le stockage, ...Et aussi permettent de mieux exploiter les ressources disponibles d'un système et de procurer une plus grande mobilité informatique, puisque les VM clientes sont indépendantes du matériel de l'hôte. Autrement dit, elles peuvent facilement être déplacées entre différents serveurs.

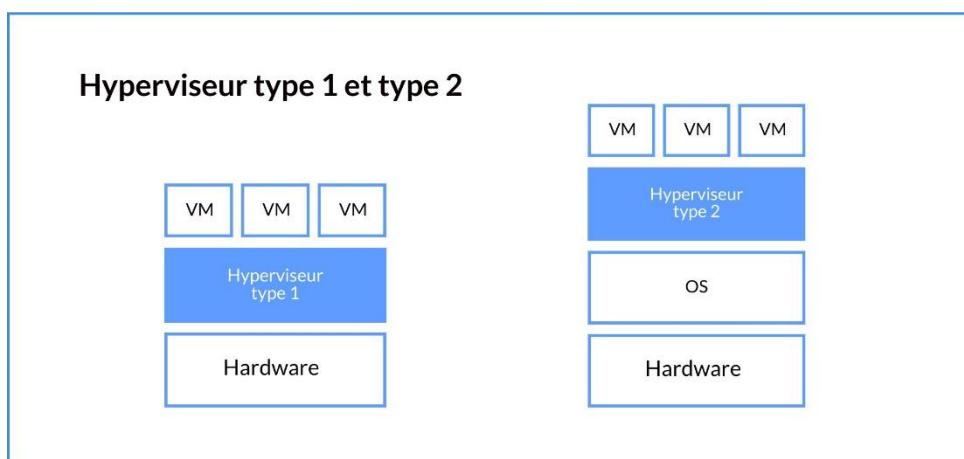


➤ Figure 7 schéma de fonctionnement d'un hyperviseur

## 6. Types d'hyperviseur

Les hyperviseurs sont divisés en deux types principaux :

- Les hyperviseurs de type 1 sont aussi appelés hyperviseurs natifs ou bare-metal, car ils s'exécutent directement sur le matériel physique, ils sont généralement plus performants et plus sécurisés que les hyperviseurs de type 2, qui s'exécutent sur un système d'exploitation hôte.
- Les hyperviseurs de type 2 ne sont pas ou peu utilisés en production. On peut les retrouver pour du test ou du développement par exemple.



➤ Figure 8 schéma les types d'un hyperviseur

## 7. Virtualisation des serveurs

La virtualisation de serveur est une technique permettant d'exécuter simultanément plusieurs systèmes d'exploitation isolés dans des machines virtuelles, sur un seul serveur physique.

### Les intérêts de la virtualisation de serveur :

Les services informatiques subissent une pression croissante afin de prendre en charge avec réactivité et gérer efficacement des ressources informatiques en expansion tout en réduisant les coûts. La virtualisation de serveur permet d'apporter des solutions nouvelles pour réduire les coûts, améliorer la flexibilité et la disponibilité des ressources informatiques.

La virtualisation de serveur permet :

- Une réduction et une meilleure exploitation des serveurs physiques.
- Une réduction des coûts opérationnels (matériel, énergie, espace).
- Une amélioration de la disponibilité des serveurs.

## 8. VMWARE VSphere

VMware vSphere est la plate-forme de virtualisation leader pour la création d'infrastructures de Cloud Computing. Elle permet aux utilisateurs d'exécuter leurs applications métier stratégiques en toute sécurité et de répondre plus rapidement aux besoins de l'activité.



Caractéristiques et composants clés:

Services d'infrastructure :

- **L'architecture d'hyperviseur VMware vSphere ESXi** : offre une couche de virtualisation fiable, ultra-performante et éprouvée en production. Elle permet à plusieurs machines virtuelles de partager les ressources matérielles avec des performances équivalentes (et parfois supérieures) à un débit natif.
- **vSphere Virtual Symmetric Multiprocessing (SMP)** : permet d'utiliser des machines virtuelles ultra-puissantes comportant jusqu'à huit processeurs virtuels.
- **Le matériel virtuel VMware** peut prendre en charge 1 To de RAM et un grand choix de matériel nouvelle génération, tel que les processeurs graphiques 3D et les périphériques USB 3.0.

Services de gestion :

- **VMware vCenter Agent** permet aux hôtes vSphere de se connecter à VMware vCenter Server pour une gestion centralisée de tous les hôtes et machines virtuelles.
- **vSphere Update Manager** automatise le suivi, l'application des correctifs et les mises à jour pour les hôtes VMware vSphere, les applications et les systèmes d'exploitation exécutés sur les machines virtuelles VMware.
- **VMware vCenter Converter** permet aux administrateurs informatiques de convertir rapidement les serveurs physiques et les machines virtuelles tierces en machines virtuelles VMware.
- **Le Client Web vSphere** permet aux administrateurs informatiques de gérer les fonctions essentielles de VMware vSphere à l'aide de tout navigateur depuis n'importe où.

## II. La virtualisation dans VMware ESXI

### 1. Création d'un switch virtuel et des VLANs



➤ Figure 9 : Page d'authentification VMware ESXI

- Ajout d'un switch virtuel est son association à un port physique du serveur
- Accès à la page d'authentification VMware ESXI



➤ Figure 10: Ajout d'un switch virtuel

- Ajout des groupes de ports et leurs associations à notre switch virtuel précédemment créé.

Modifier le groupe de ports - Employes\_GR3

Nom	Employes_GR3
ID VLAN	10
Commutateur virtuel	PFE_GR3
▶ Sécurité	Cliquer pour développer
▶ Association de cartes réseau	Cliquer pour développer
▶ Formation du trafic	Cliquer pour développer

Enregistrer Annuler

➤ Figure 11 Ajout d'un groupe de ports VLAN 10

Modifier le groupe de ports - Invites\_GR3

Nom	Invites_GR3
ID VLAN	20
Commutateur virtuel	PFE_GR3
▶ Sécurité	Cliquer pour développer
▶ Association de cartes réseau	Cliquer pour développer
▶ Formation du trafic	Cliquer pour développer

Enregistrer Annuler

Modifier le groupe de ports - vlan40

Nom	vlan40
ID VLAN	40
Commutateur virtuel	PFE_GR3
▶ Sécurité	Cliquer pour développer
▶ Association de cartes réseau	Cliquer pour développer
▶ Formation du trafic	Cliquer pour développer

➤ Figure 12 Ajout d'un groupe de ports VLAN 20,40

GrAvlan40	0	40	Groupe de ports standard	gr1 vs
GrAvlan20	0	20	Groupe de ports standard	gr1 vs
GrAvlan10	0	10	Groupe de ports standard	gr1 vs
GrAvlan30	0	30	Groupe de ports standard	gr1 vs

➤ Figure 13 Les groupes de ports du switch virtuel

## 2. Choix du système d'exploitation des serveurs



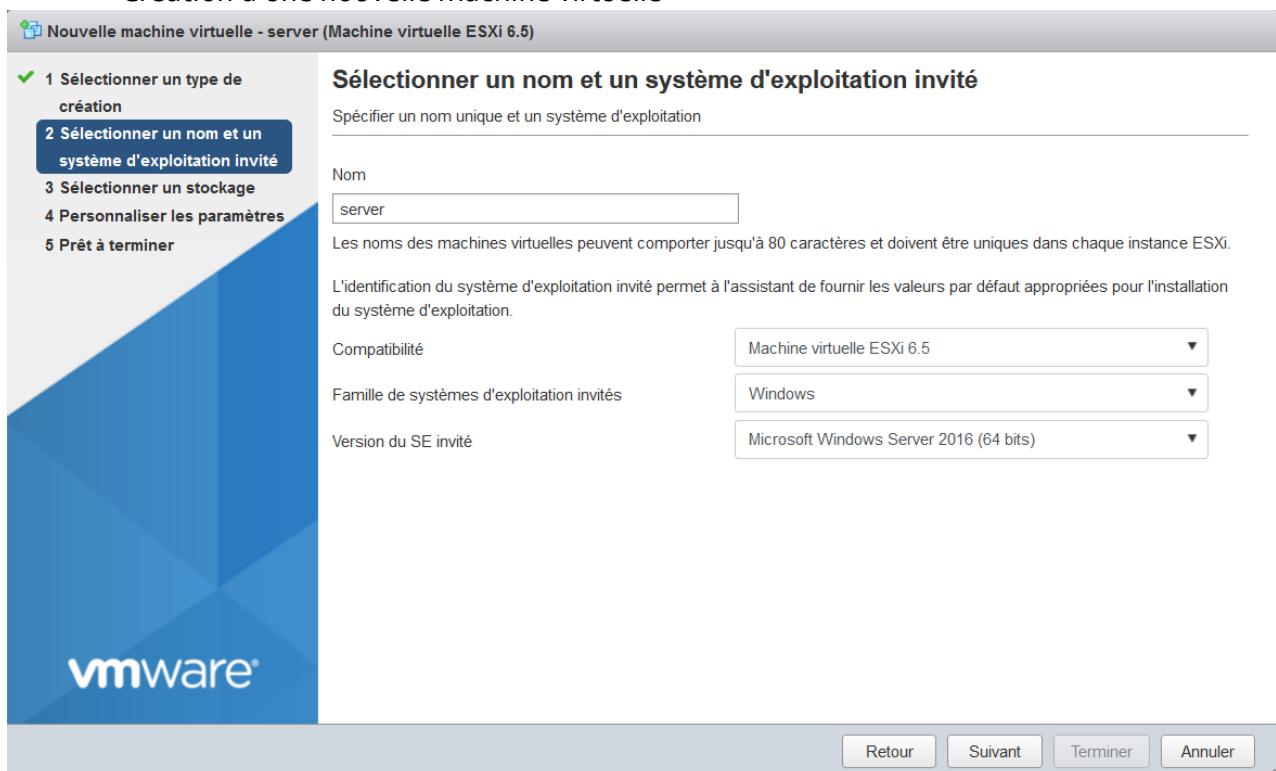
**Windows Server** (formerly **Windows NT Server**) is a group of operating systems (OS) for servers that Microsoft has been developing since July 27, 1993. The first OS that was released for this platform is Windows NT 3.1 Advanced Server. With the release of Windows Server 2003, the brand name was changed to Windows Server.

Microsoft's history of developing operating systems for servers goes back to Windows NT 3.1 Advanced Server. Windows 2000 Server is the first OS to include Active Directory, DNS Server, DHCP Server, and Group Policy.

La structure de Windows Server est plus complexe que celle de Linux, principalement en raison de la volonté de Windows d'offrir aux utilisateurs un système d'exploitation simple à utiliser sans la nécessité d'une administration via des lignes de commande comme c'est le cas avec Linux. Cependant, Windows Server requiert plus de ressources, en particulier en raison de l'interface utilisateur graphique (GUI), et les coûts de licence sont élevés à long terme.

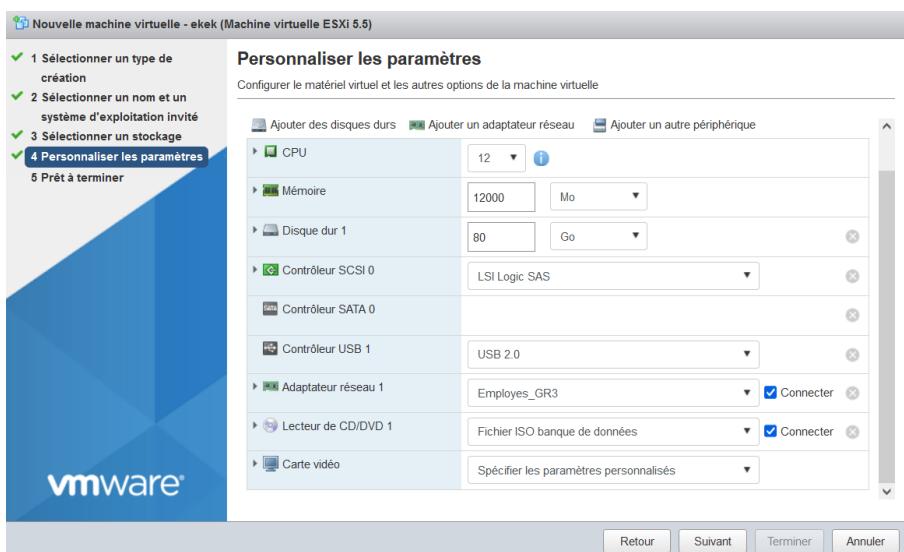
### 3. Création des machine virtuelles

- Création d'une nouvelle machine virtuelle



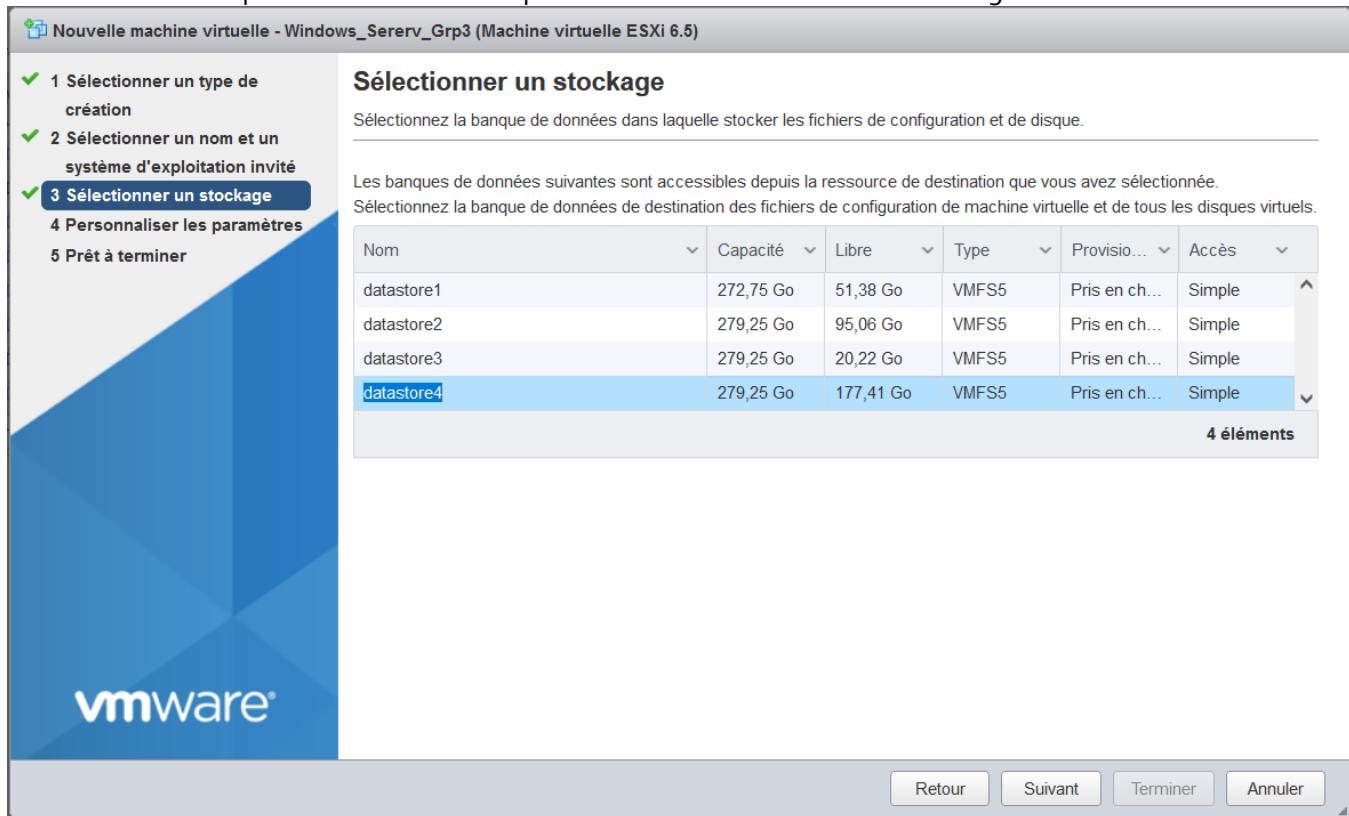
➤ Figure 14 Ajout d'une machine virtuelle

- Configuration du matériel de la machine virtuelle et choix du fichier ISO du système d'exploitation Microsoft Windows Server 2016.

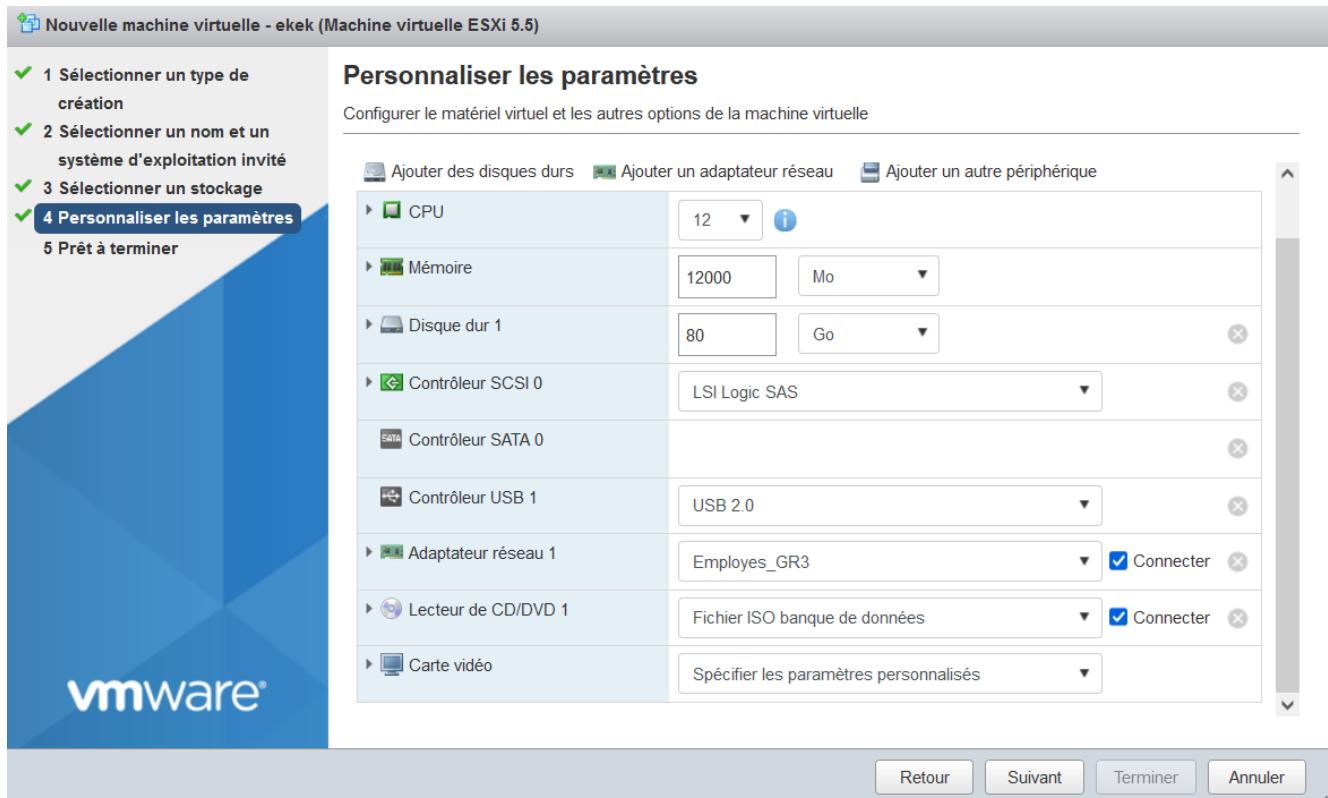


➤ Figure 15 Configuration matérielle de la machine virtuelle.

Sélection de la banque de données dans laquelle on va stocker les fichiers de configuration.



Personnalisation des paramètres



### Conclusion

Le domaine de la virtualisation est en pleine croissance et évolue rapidement, offrant une grande souplesse en matière d'allocation de ressources.

## CONCLUSION

Dans cette section, nous avons présenté l'architecture réseau déployée et son adressage dans le premier chapitre, ainsi que les différents équipements (switch, routeur, pare-feu et points d'accès), avec la configuration du switch. Dans le deuxième chapitre, nous avons discuté des concepts clés de la virtualisation.

# PARTIE II

## Les Méthodes D'Authentification

# CHAPITRE 1 : Authentification des employés

Un serveur RADIUS est un élément permettant l'authentification des utilisateurs souhaitant accéder à un réseau. Dans ce chapitre, nous allons aborder la mise en place d'un Serveur RADIUS pour l'authentification sans fil des employés.

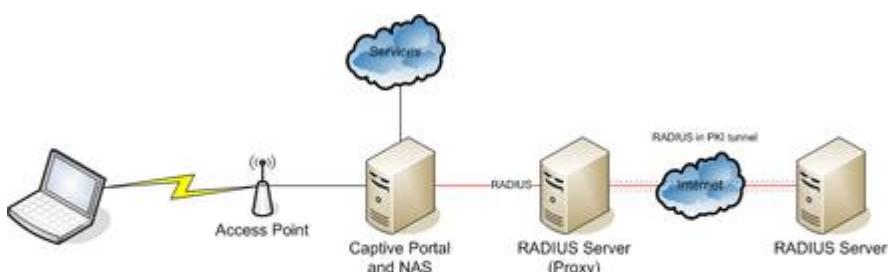
## I. Le protocole RADIUS

### 1. Définition

**RADIUS** (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. Le protocole RADIUS a été inventé et développé en 1991 par la société Livingston entreprise (rachetée par Lucent Technologies), qui fabriquait des serveurs d'accès au réseau pour du matériel uniquement équipé d'interfaces série ; il a fait ultérieurement l'objet d'une normalisation par l'IETF.

### 2. Principe

Le protocole RADIUS se fonde principalement sur un serveur, nommé serveur RADIUS, qui est connecté à une base d'identification telle qu'une base de données ou un annuaire LDAP, ainsi qu'un client RADIUS nommé NAS (Network Access Server) qui agit en tant qu'intermédiaire entre l'utilisateur final et le serveur. Les échanges entre le client RADIUS et le serveur RADIUS sont sécurisés et authentifiés à l'aide d'un secret partagé



➤ Figure 16 Principe de RADIUS

Il convient de souligner que le serveur RADIUS est capable d'agir comme un proxy en relayant les demandes du client à d'autres serveurs RADIUS.

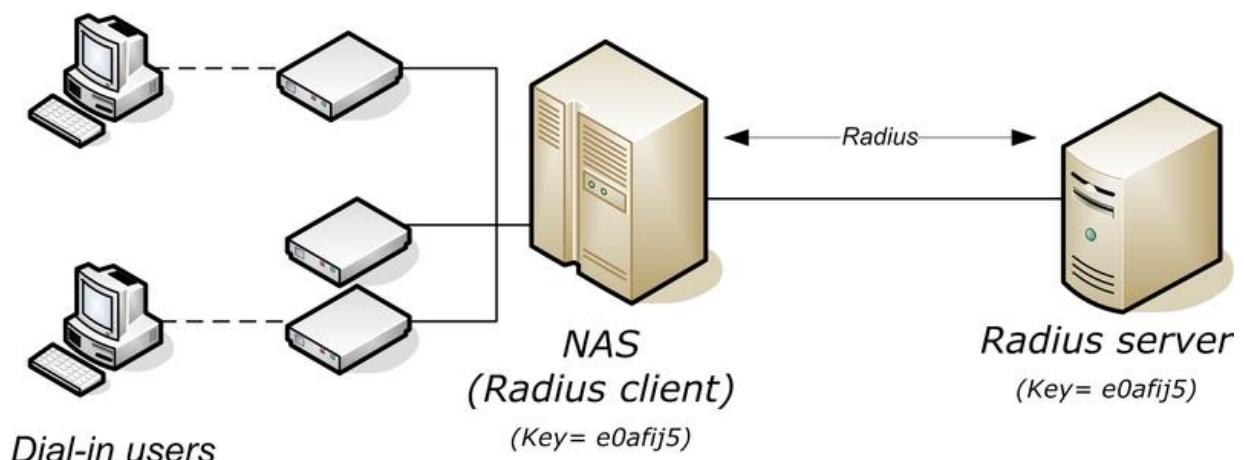
Lorsqu'un utilisateur souhaite accéder au réseau, il envoie une requête d'accès à un client RADIUS à partir de son poste de travail (appelé "supplicant" selon les RFC). Le client RADIUS demande ensuite les informations d'identification de l'utilisateur, telles que son nom d'utilisateur (login) et son mot de passe, par exemple.

Ensuite, selon le protocole RADIUS, le client RADIUS génère une requête

Access-Request contenant les informations d'authentification. Cette requête peut être traitée directement par le serveur RADIUS ou transmise à un autre serveur RADIUS à l'aide du mécanisme Proxy RADIUS. Le serveur RADIUS final, responsable de l'identification de l'utilisateur (appelé "Home RADIUS"), peut traiter la demande si les informations contenues dans la requête

Access-Request sont suffisantes. Sinon, il peut demander des informations supplémentaires en envoyant un paquet "Access Challenge" au client RADIUS, qui répondra par une autre requête "Access-Request", et ainsi de suite. Les échanges sont relayés dans les deux sens par la chaîne de serveurs RADIUS proxy intermédiaires.

### 3. Fonctionnement



➤ Figure 17 Diagramme de séquence de fonctionnement RADIUS

## II. Les services réseaux

### 1. Le service DNS

#### a. Définition

Le **Domain Name System** (Système de nom de domaine) ou **DNS** est un service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP ou d'autres types d'enregistrements. En fournissant dès les premières années d'Internet, autour de 1985, un service distribué de résolution de noms, le DNS est un composant essentiel du développement du réseau informatique.

#### b. Fonctionnement

Le processus de résolution DNS consiste à convertir un nom d'hôte (comme [www.exemple.com](http://www.exemple.com)) en une adresse IP (comme 192.168.1.1).

Le serveur de noms faisant autorité est l'endroit où les administrateurs peuvent gérer les noms de serveurs et les adresses IP de leurs domaines. Lorsqu'un administrateur DNS souhaite ajouter, modifier ou supprimer un nom de serveur ou une adresse IP, il effectue une modification sur son serveur DNS faisant autorité (parfois appelé "serveur DNS maître").

En plus des serveurs DNS faisant autorité, il existe également des serveurs DNS "esclaves" qui contiennent des copies des enregistrements DNS pour leurs zones et domaines.

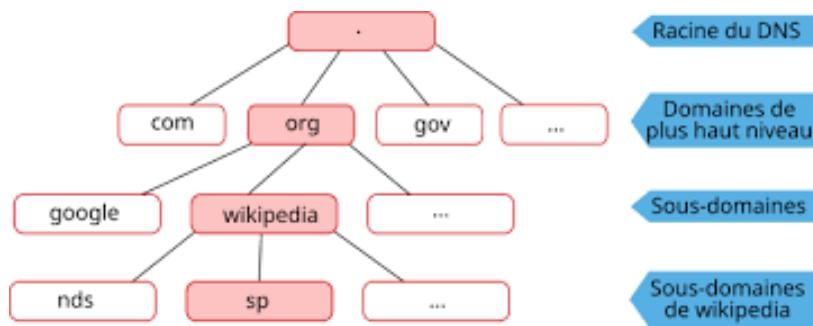
#### c. Types de services DNS

Sur Internet, il existe deux types de services DNS distincts, chacun traitant les requêtes DNS différemment en fonction de leur rôle :

Le résolveur DNS récursif : répond à la requête et recherche le serveur de noms faisant autorité ou un cache DNS contenant le résultat de la requête.

Le serveur DNS faisant autorité : contient le résultat de la requête DNS. Par conséquent, il n'a pas besoin d'interroger un autre serveur pour fournir la réponse à la requête.

#### d. Hiérarchie DNS



➤ Figure 18 Hiérarchie DNS

Le système des noms de domaine est une hiérarchie dont la racine est représentée par un point. Les domaines de premier niveau (TLD : Top Level Domain) se situent immédiatement sous la racine.

Il existe deux types de TLD :

Les ccTLD (country code TLD) : les noms de domaine correspondant à des codes de pays (ma, fr...).

Les gTLD (generic TLD) : les noms de domaine qui ne correspondent pas à une extension de pays, tels que .org ou .com.

Pour représenter un nom de domaine, on indique les domaines successifs séparés par un point, les noms de domaine supérieurs étant à droite. Ainsi, pour résoudre un nom de domaine, on parcourt la hiérarchie depuis le sommet et en suivant les délégations successives, c'est-à-dire en parcourant le nom de domaine de droite à gauche.

#### Résolution Inverse

Pour trouver le nom de domaine associé à une adresse IP, on utilise un principe semblable.

Dans un nom de domaine, la partie la plus générale est à droite : org dans wikipedia.org, le mécanisme de résolution parcourt donc le nom de domaine de droite à gauche. Dans une adresse IP V4, c'est le contraire : 192 est la partie la plus générale de 192.168.0.1.

Pour conserver la même logique que la résolution des noms de domaines, on inverse l'ordre des quatre octets de l'adresse et on la concatène au pseudo domaine in-addr.arpa. Ainsi, par exemple, pour trouver le nom de domaine de l'adresse IP 192.168.0.1, on résout 1.0.168.192.in-addr.arpa.

## 2. Le protocole DHCP

### a. Définition

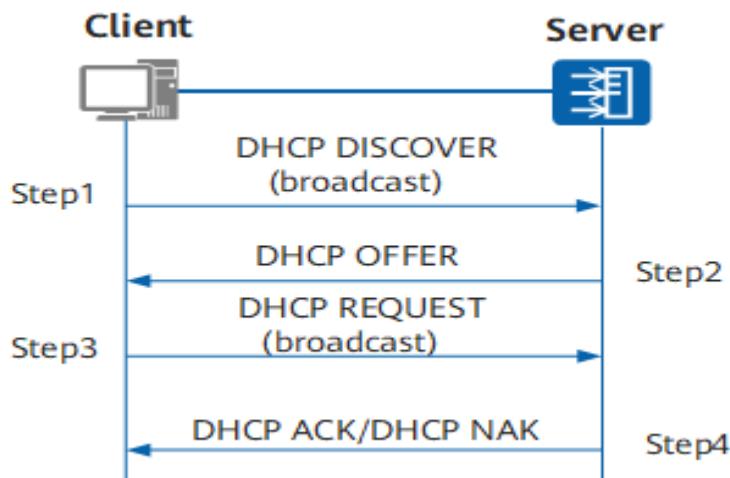
Le protocole DHCP (Dynamic Host Configuration Protocol) est un moyen de communication qui permet aux administrateurs réseau de gérer et d'automatiser la configuration réseau des appareils connectés à un réseau IP (Internet Protocol) de manière centralisée.

### b. Fonctionnement

Tout d'abord, il est nécessaire de disposer d'un serveur DHCP qui se charge de la distribution des adresses IP. Cette machine possède une adresse IP fixe et sert de référence pour toutes les requêtes DHCP.

Ensuite, il existe plusieurs types de paquets DHCP qui peuvent être émis soit par le client vers le ou les serveurs, soit par le serveur vers un client :

- DHCPDISCOVER (pour localiser les serveurs DHCP disponibles)
- DHCPOFFER (réponse du serveur à un paquet DHCPDISCOVER, qui contient les premiers paramètres)
- DHCPREQUEST (requête diverse du client pour par exemple prolonger son bail)
- DHCPACK (réponse du serveur qui contient des paramètres et l'adresse IP du client)
- DHCPNAK (réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau)
- DHCPDECLINE (le client annonce au serveur que l'adresse est déjà utilisée)
- DHCPRELEASE (le client libère son adresse IP)
- DHCPINFORM (le client demande des paramètres locaux, il a déjà son adresse IP)



➤ Figure 19 diagramme séquence DHCP

Dans le but d'optimiser l'utilisation des ressources réseau, les adresses IP sont attribuées avec une période de validité débutant et se terminant à une date précise, ce qui est communément appelé un "bail".

### 3. Le protocole LDAP

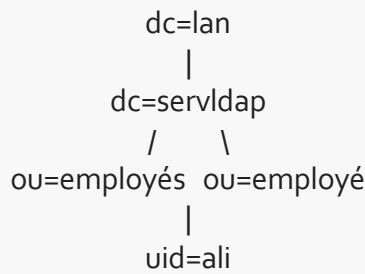
#### a. Définition

**LDAP (Lightweight Directory Access Protocol)** a été initialement conçu comme un protocole pour interroger et modifier les services d'annuaire, étant une évolution du protocole DAP. Ce protocole est basé sur TCP/IP et s'est développé pour devenir une norme pour les systèmes d'annuaires, qui incluent des modèles de données, de nommage, fonctionnels (basés sur le protocole LDAP), de sécurité et de réPLICATION. L'annuaire LDAP est une structure arborescente avec des nœuds composés d'attributs et de leurs valeurs. En comparaison avec le modèle X.500 édicté par l'UIT-T, LDAP est plus simple.

#### b. Structure de l'annuaire

- Un annuaire est un arbre d'entrées.
- Une entrée est constituée d'un ensemble d'attributs.
- Un attribut possède un nom, un type et une ou plusieurs valeurs.
- Les attributs sont définis dans des schémas.

Chaque entrée dans le système d'annuaire LDAP possède un identifiant unique, appelé Distinguished Name (DN). Ce DN est constitué du Relative Distinguished Name (RDN) de l'entrée suivi du DN de son parent, formant ainsi un chemin absolu pour l'entrée. Le RDN quant à lui, représente le chemin relatif de l'entrée par rapport à son parent dans la structure arborescente de l'annuaire. En général, pour une entrée qui représente une personne, l'attribut choisi pour le RDN est l'uid.



Le RDN de ali est rdn:uid=ali, son DN est dn:uid=ali,ou=employés ,dc=servldap,dc=lan.

#### 4. Le protocole 802.1X

##### a. Définition

Le protocole 802.1X est une méthode d'authentification utilisée pour les terminaux connectés à un réseau interne câblé (LAN) ou sans fil (WLAN). Cette méthode est généralement employée dans les entreprises afin de sécuriser l'accès à leur réseau et garantir la protection de leurs données.

##### b. Fonctionnement

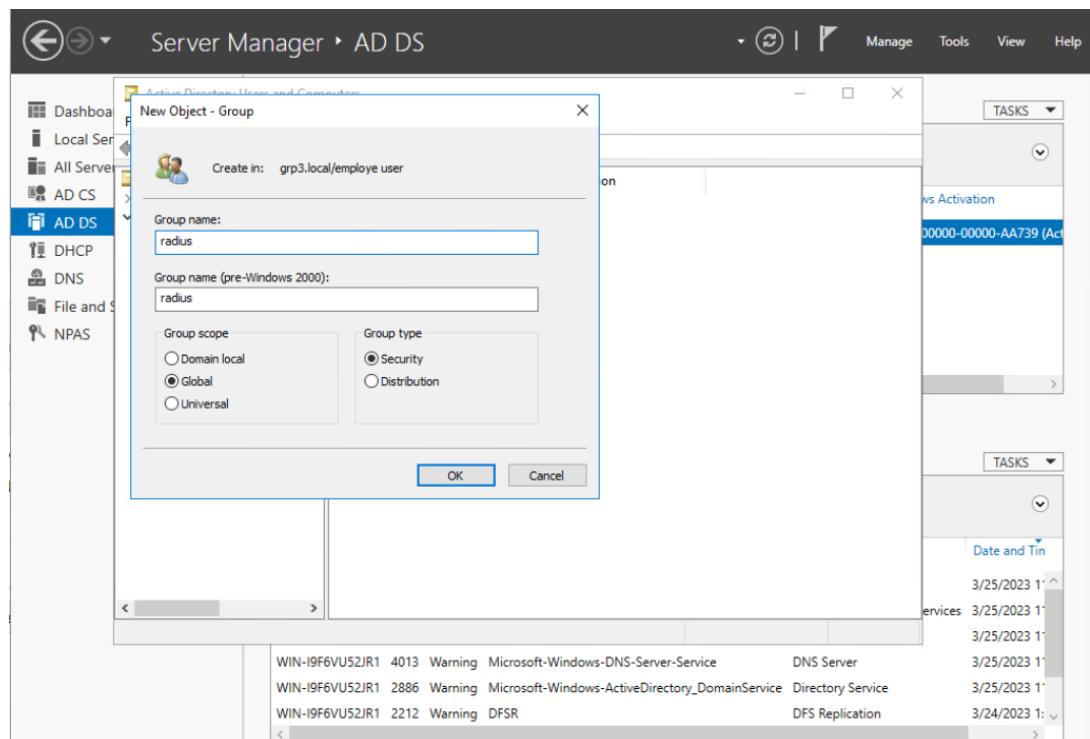
Le protocole 802.1X est constitué de trois éléments distincts : les commutateurs réseau et/ou les points d'accès sans fil (NAS), les équipements connectés au réseau interne (les utilisateurs) et le serveur d'identification RADIUS. Le processus de connexion comporte les étapes suivantes :

- Le serveur RADIUS envoie un certificat électronique au client.
- Le client vérifie ce certificat en utilisant les certificats des autorités de certification.
- L'utilisateur entre ses identifiants (nom d'utilisateur et mot de passe).
- Un tunnel crypté est créé entre le client et le serveur RADIUS.
- Le serveur RADIUS reçoit le mot de passe de l'utilisateur et le vérifie pour déterminer sa validité.
- Le serveur RADIUS autorise ou refuse la connexion auprès du commutateur.

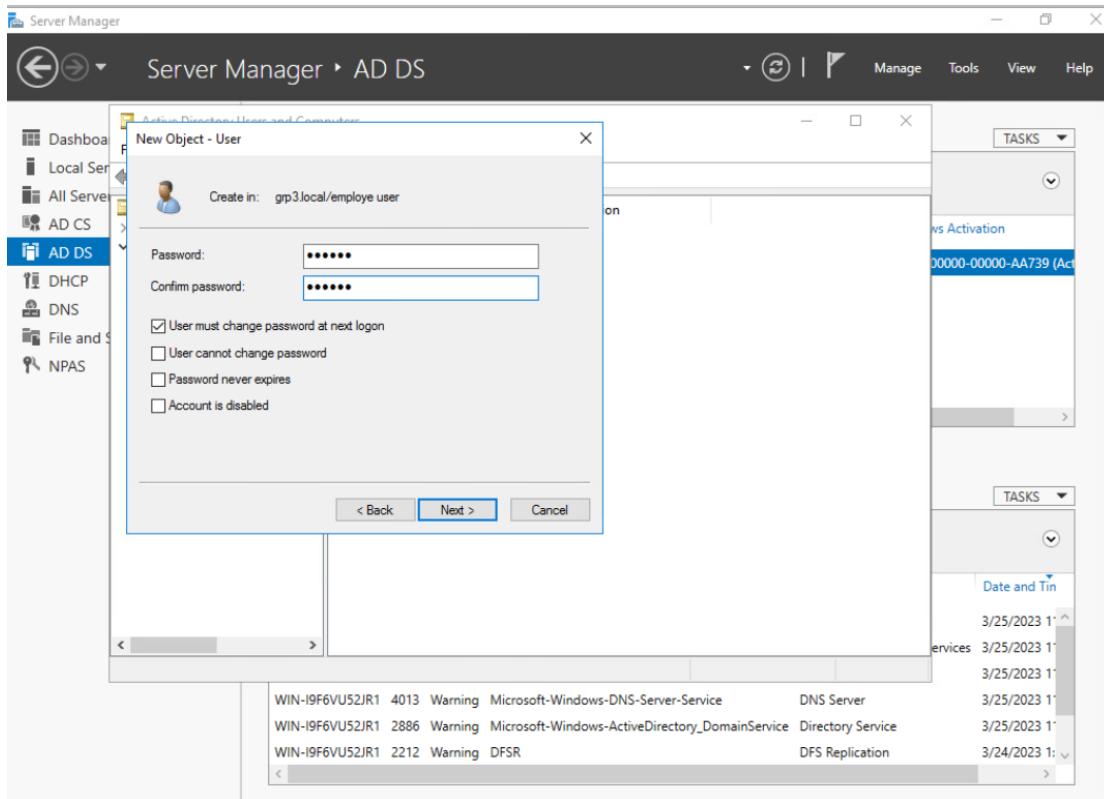
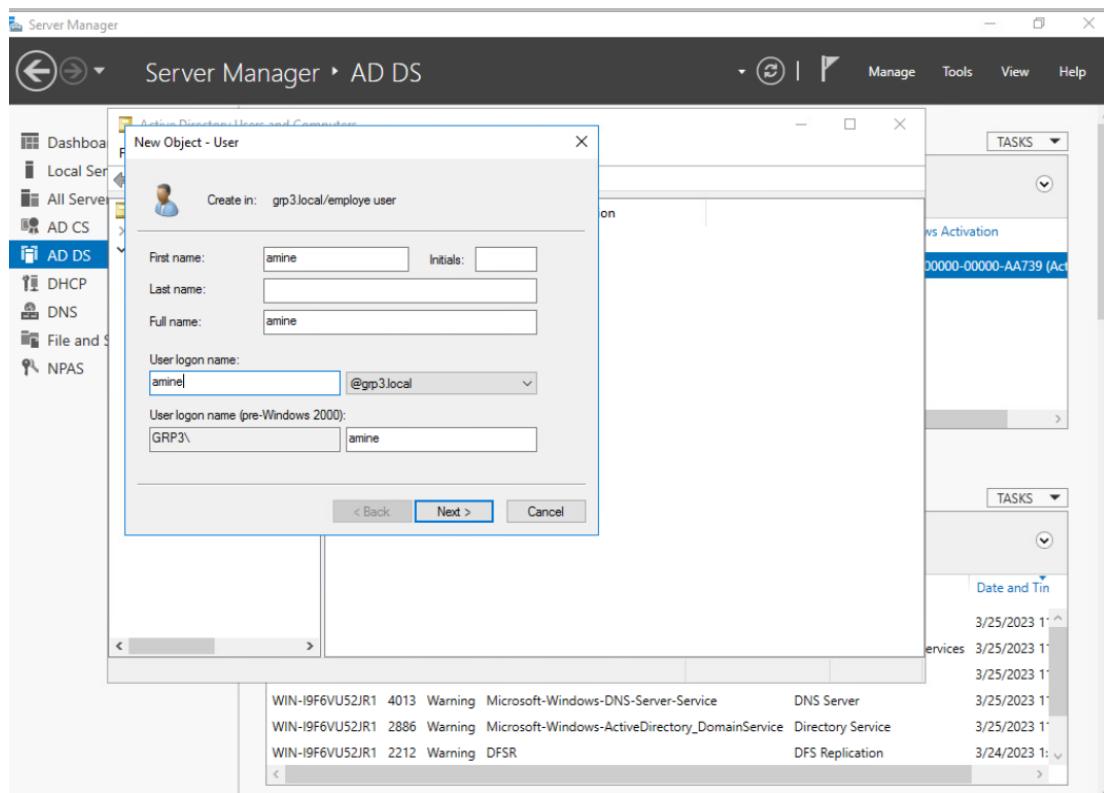
### III. Implémentation d'un serveur RADIUS

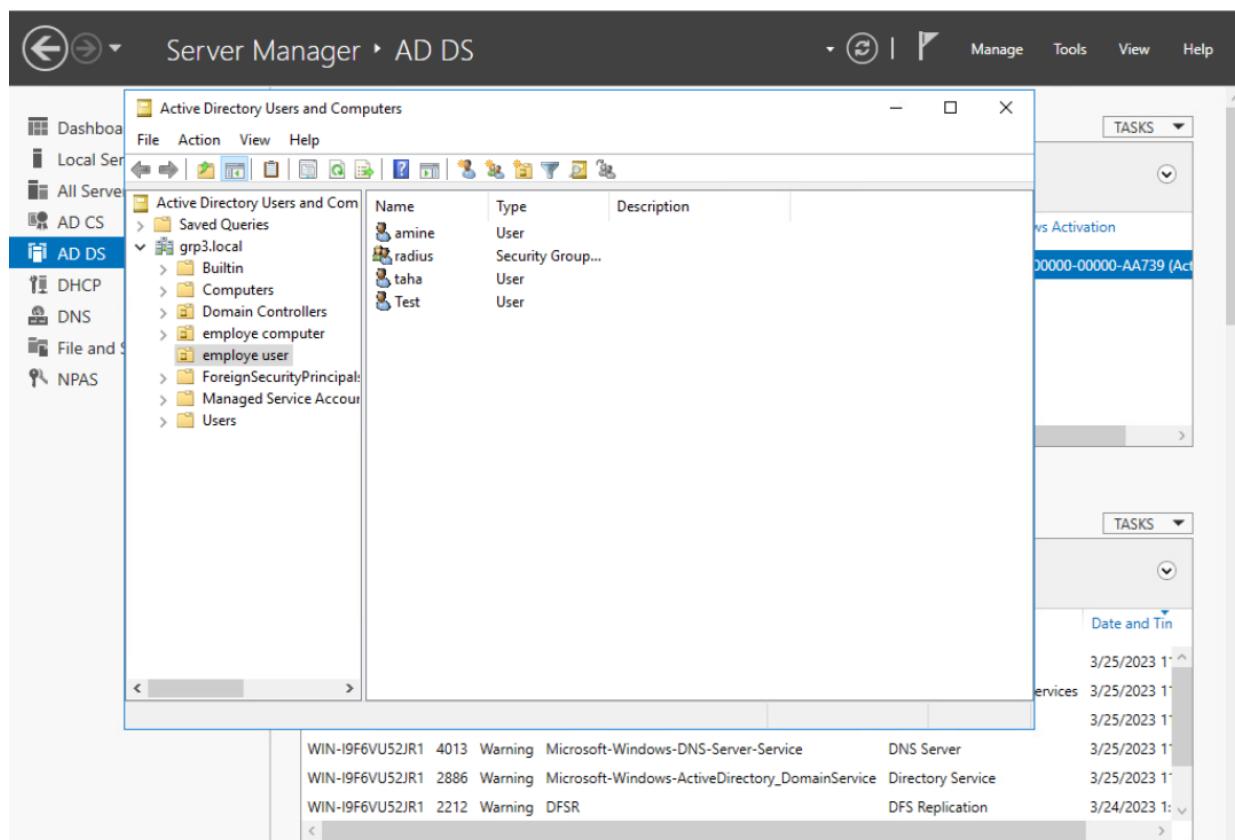
Avant l'implémentation du serveur RADIUS, nous avons créé une machine Windows Server qui fera office d'un serveur DHCP, DNS et qui contiendra l'annuaire LDAP.

Création du groupe radius avec un scope global et type Security



## Création d'un nouveau user « amine » et attribution de son mot de passe

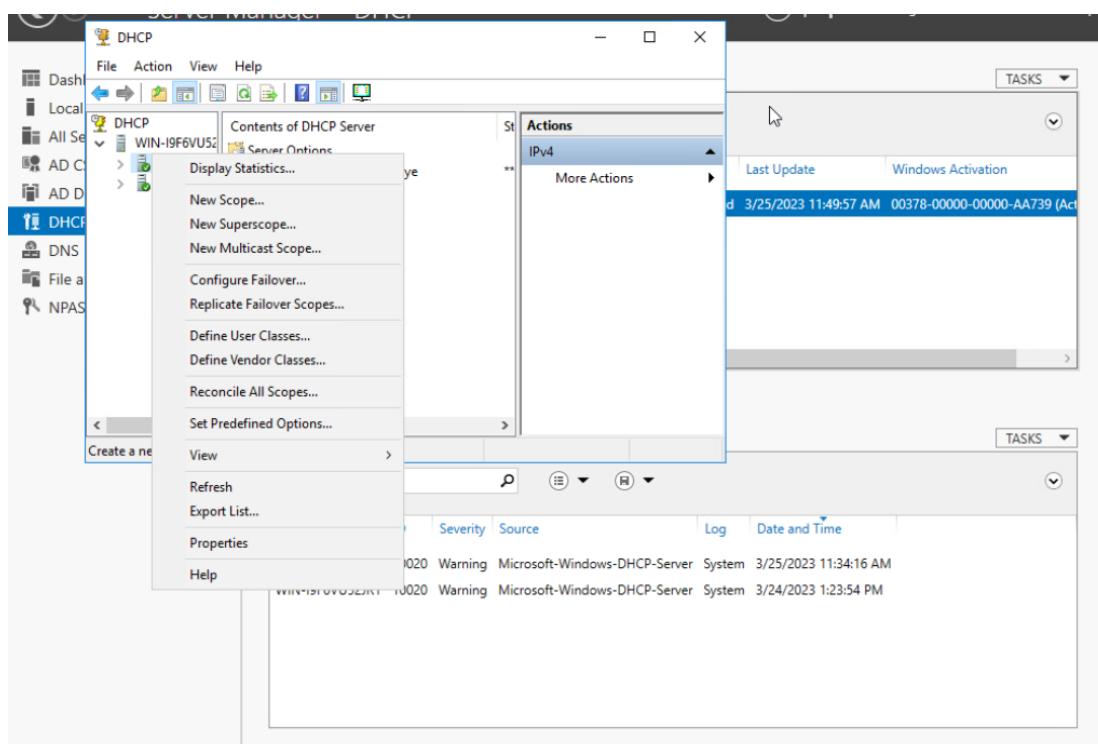


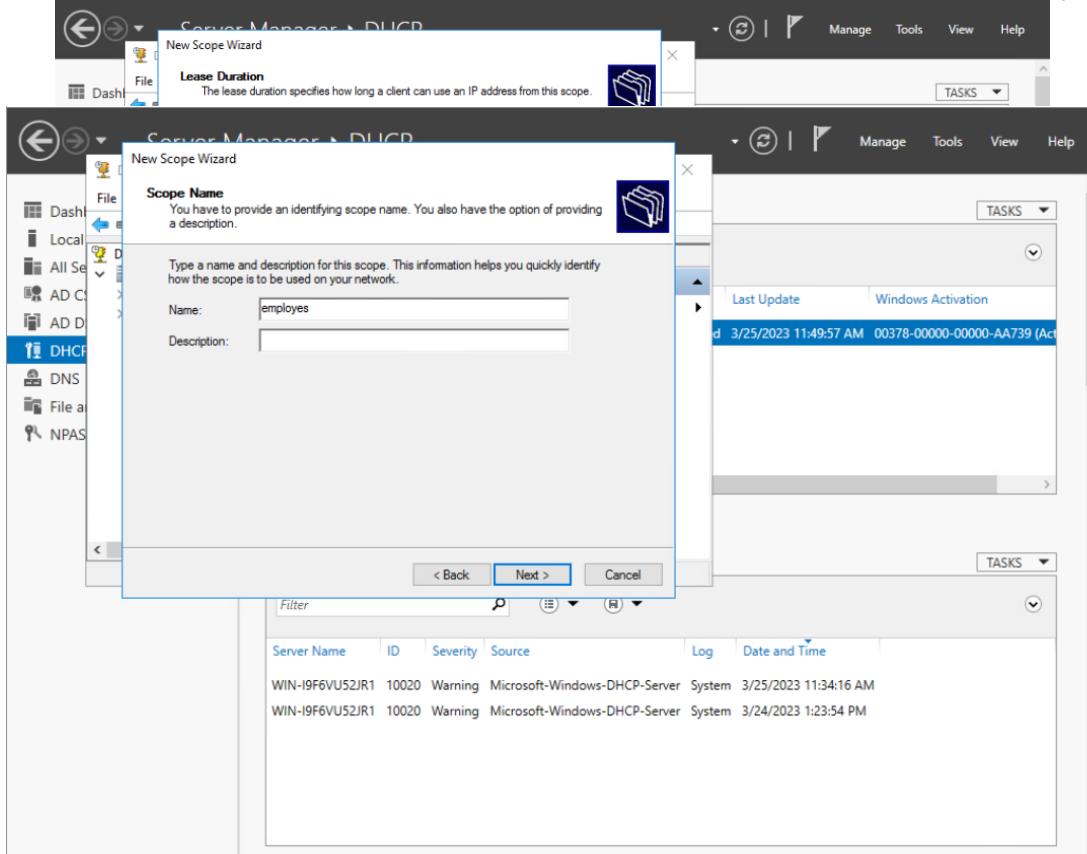


➤ Figure 20 : liste des users

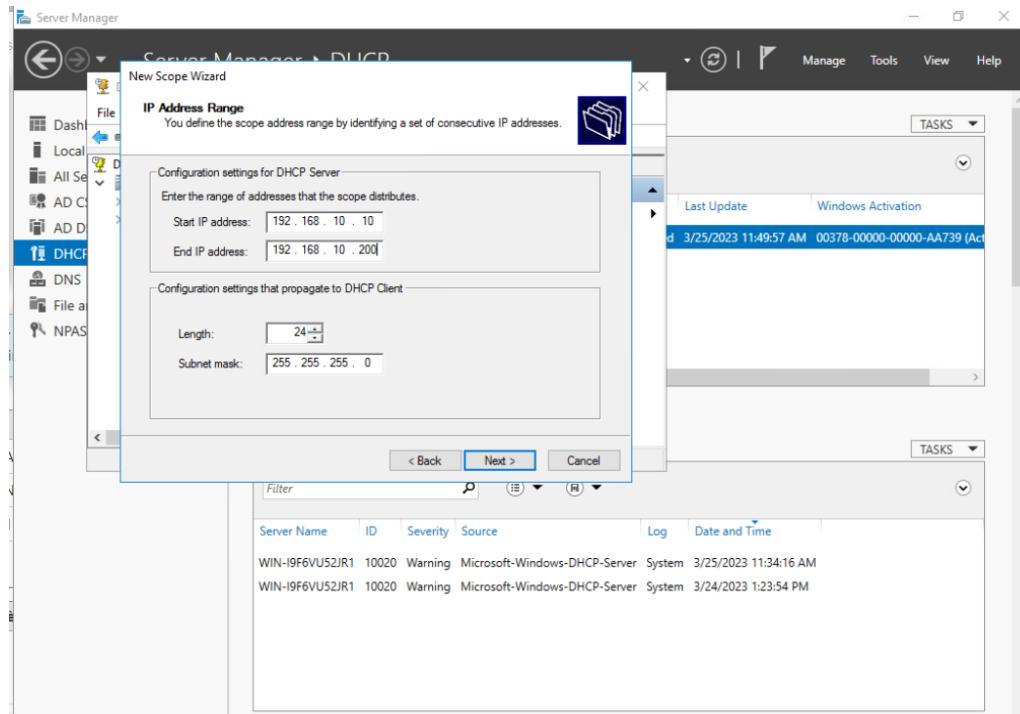
## a. Configuration du serveur DHCP

### Création du scope employés

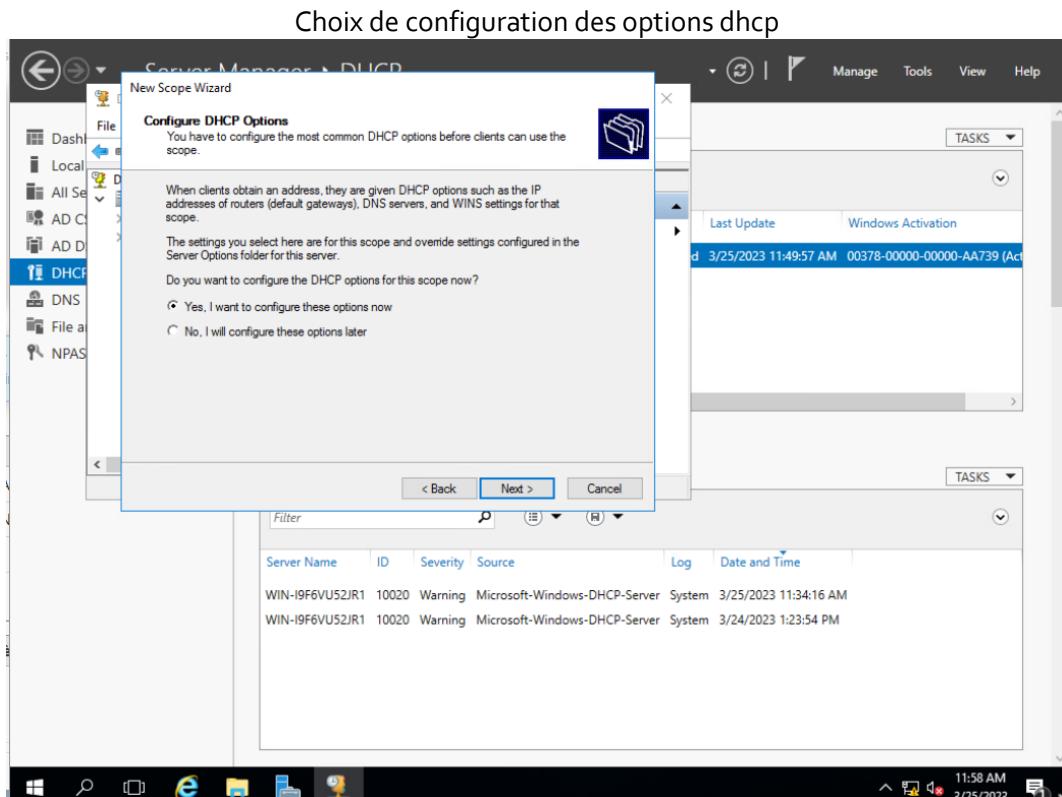




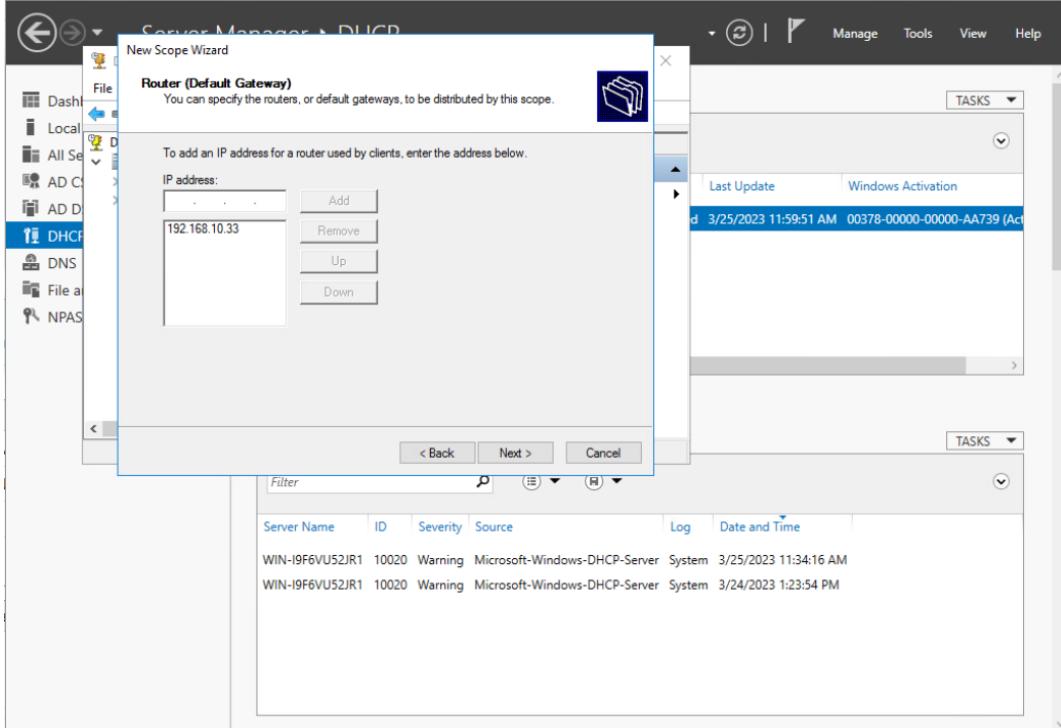
Attribution de la plage d'adresses de scope



Attribution du durée du bail pour le client

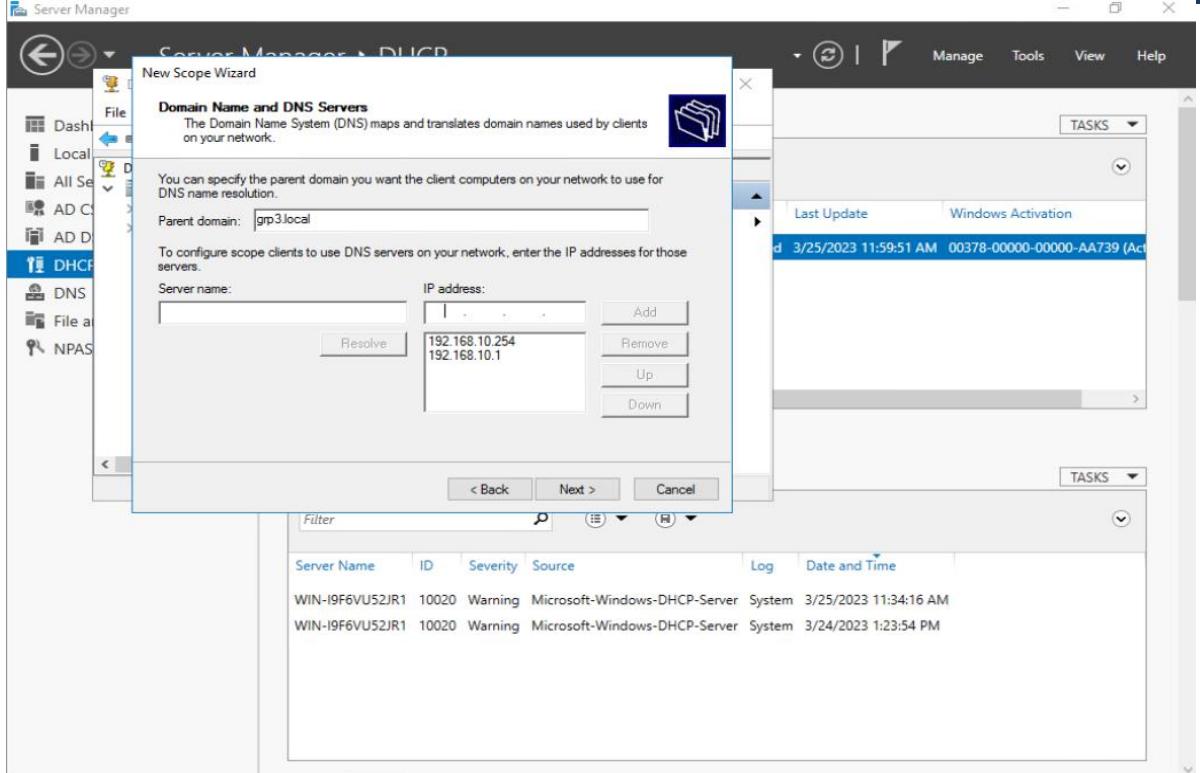


### Attribution de la passerelle

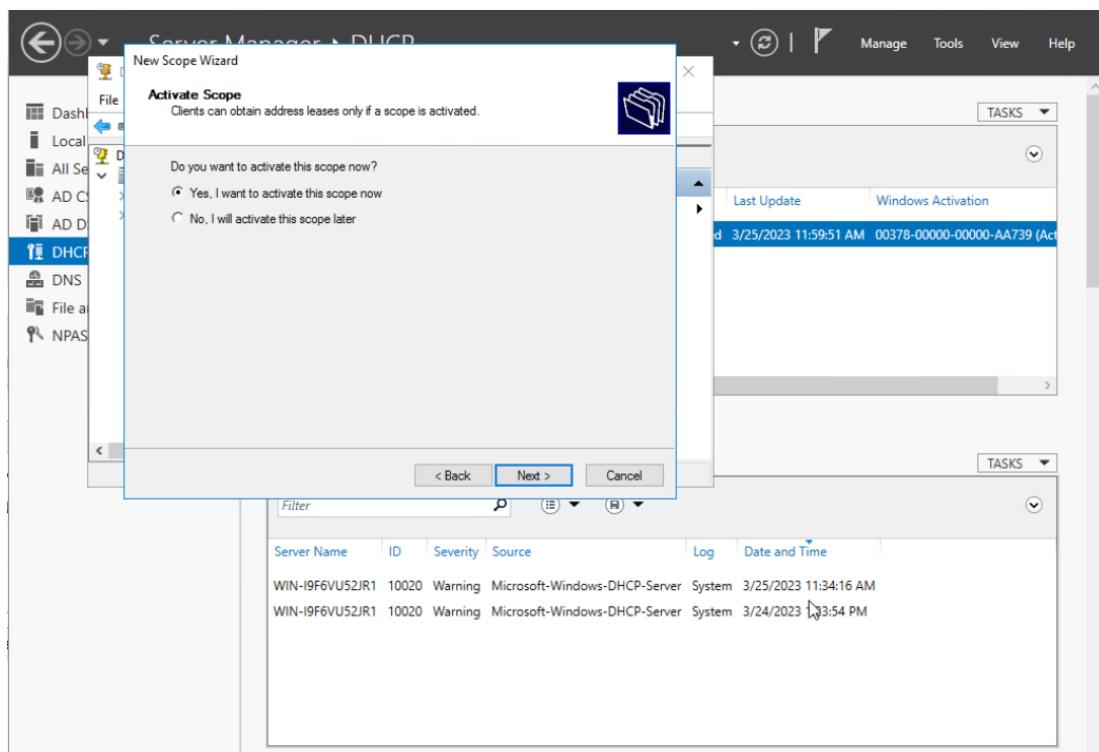


Définition du nom de domaine « grp3.local » et configuration des clients scope pour l'utilisation des serveurs DNS dans le réseau

Choix des adresses IP des serveurs

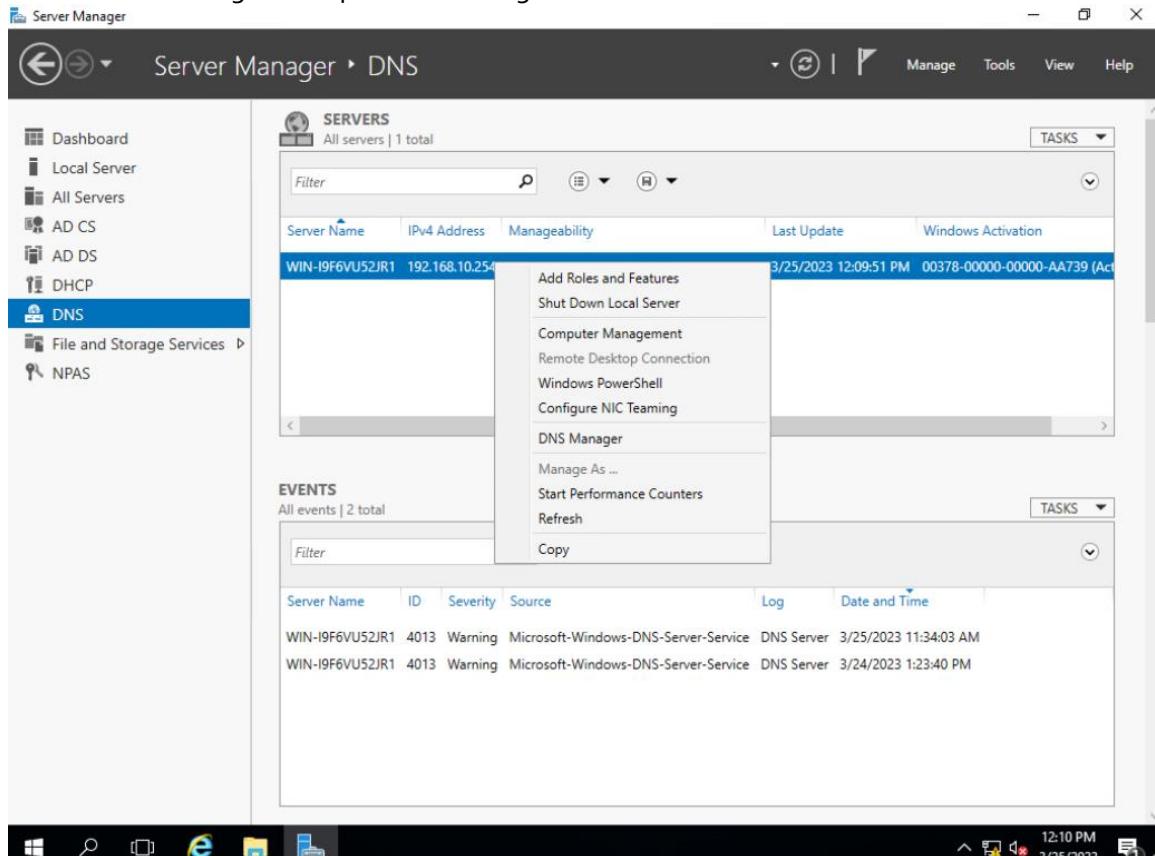


### Activation du scope

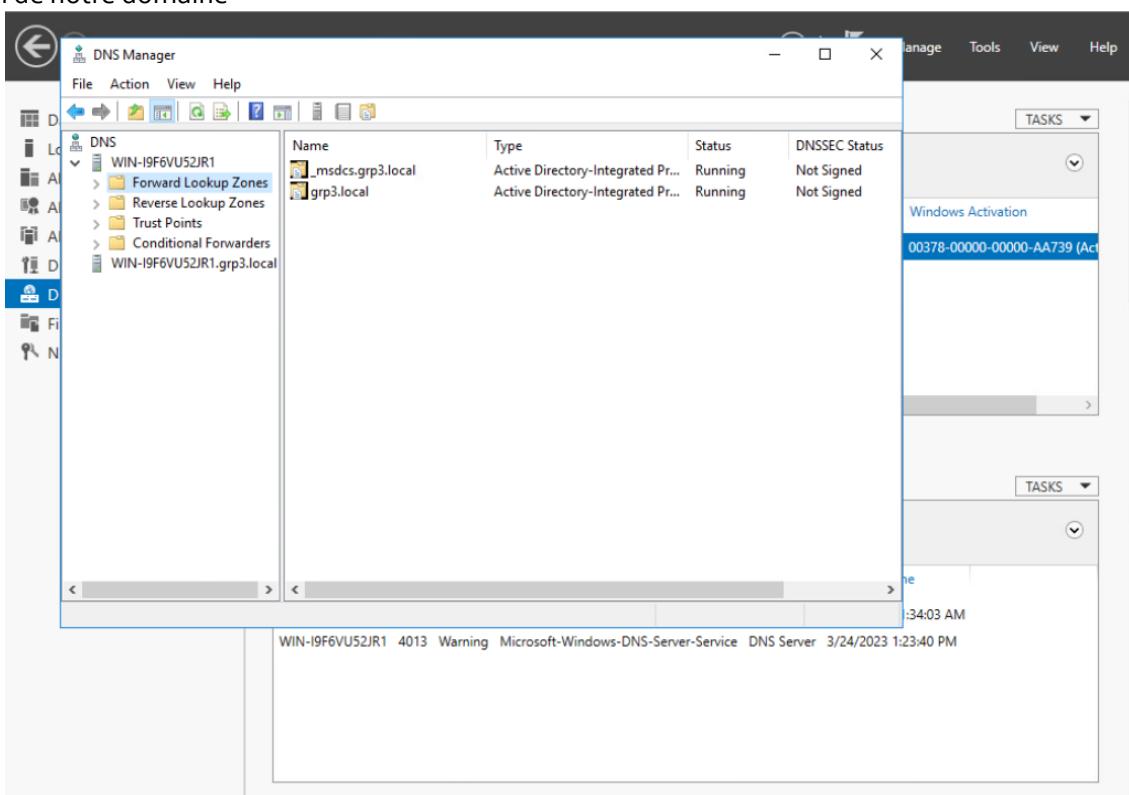


## b. Configuration du serveur DNS

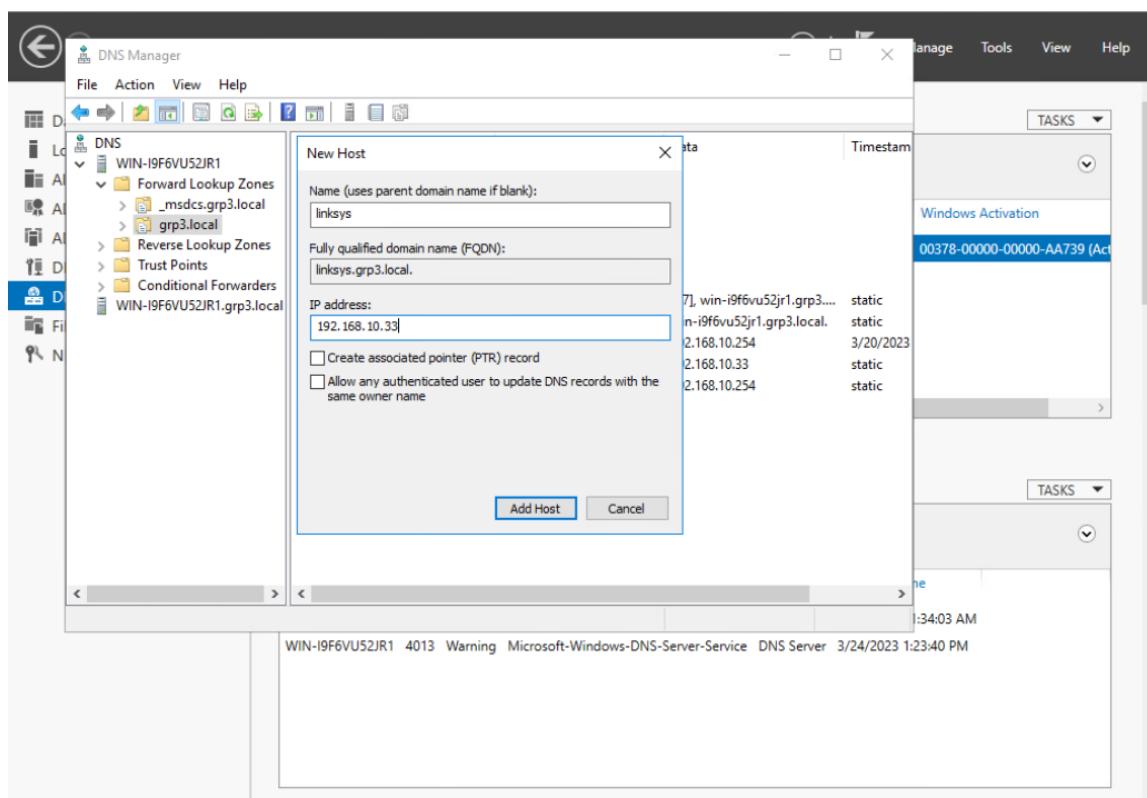
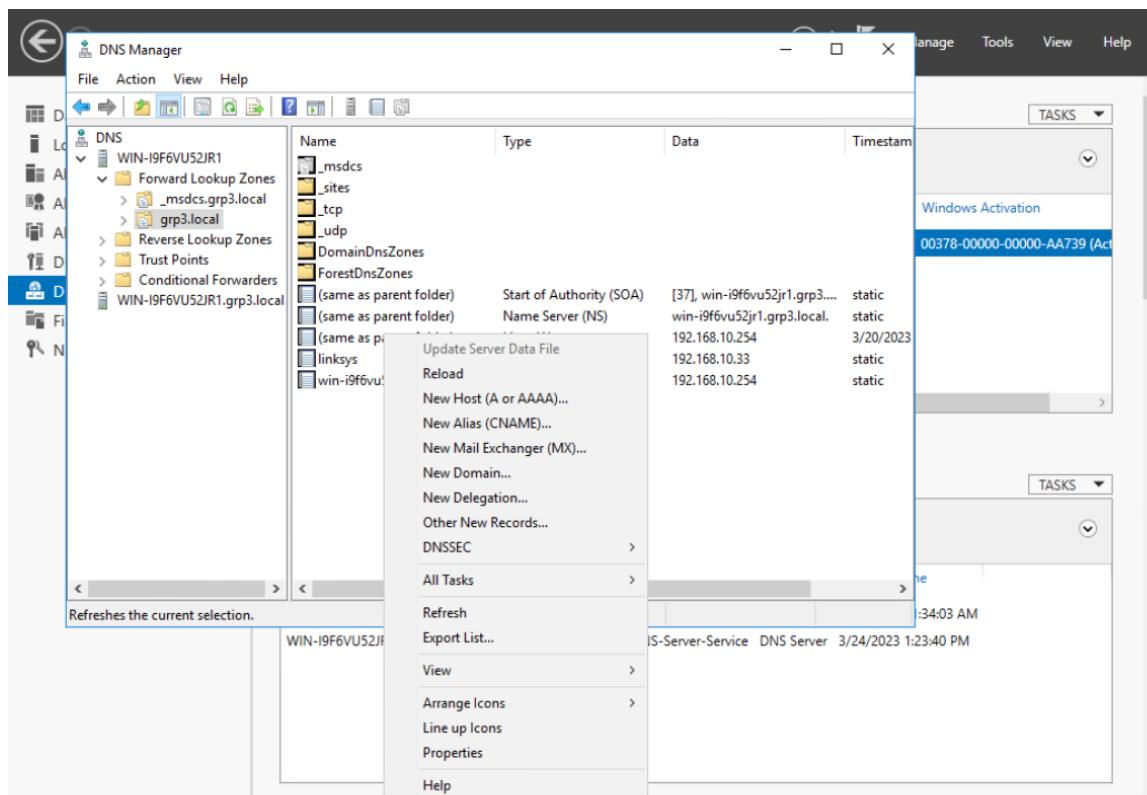
Initialisation de la configuration par DNS manager

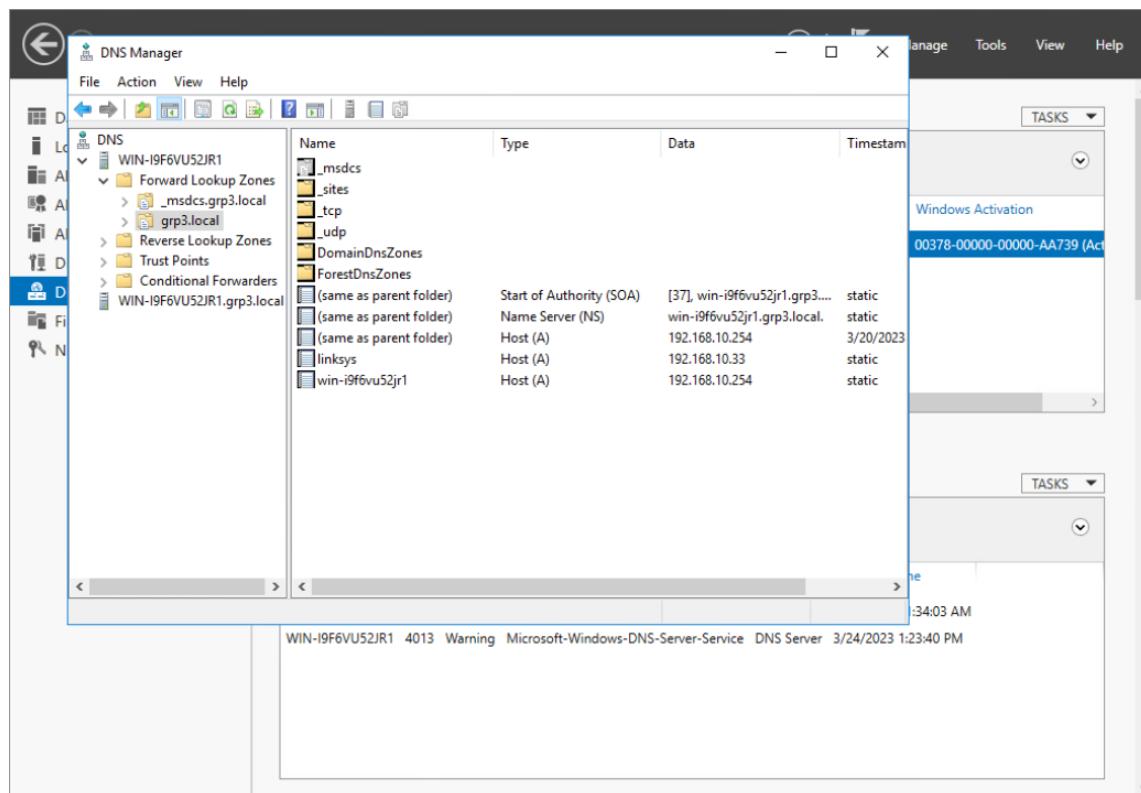


Sélection de notre domaine



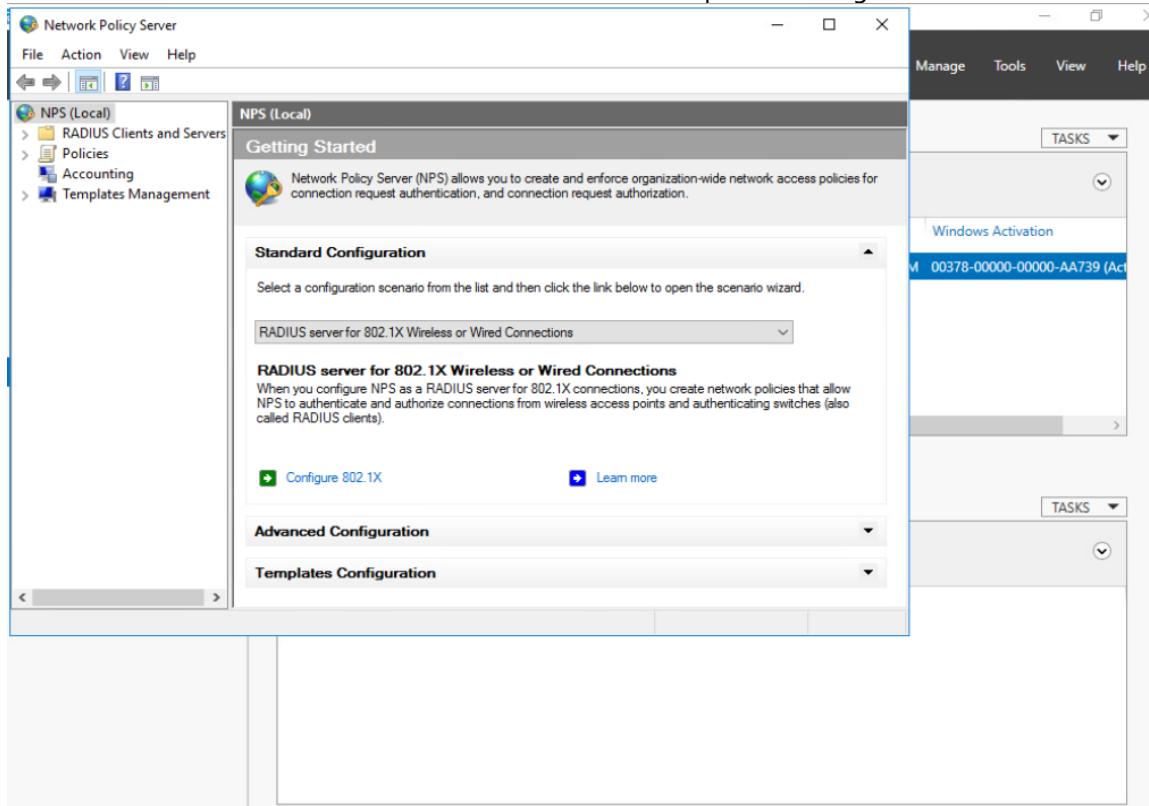
## Création d'une machine routeur et choix de l'enregistrement de résolution avec attribution d'adresse



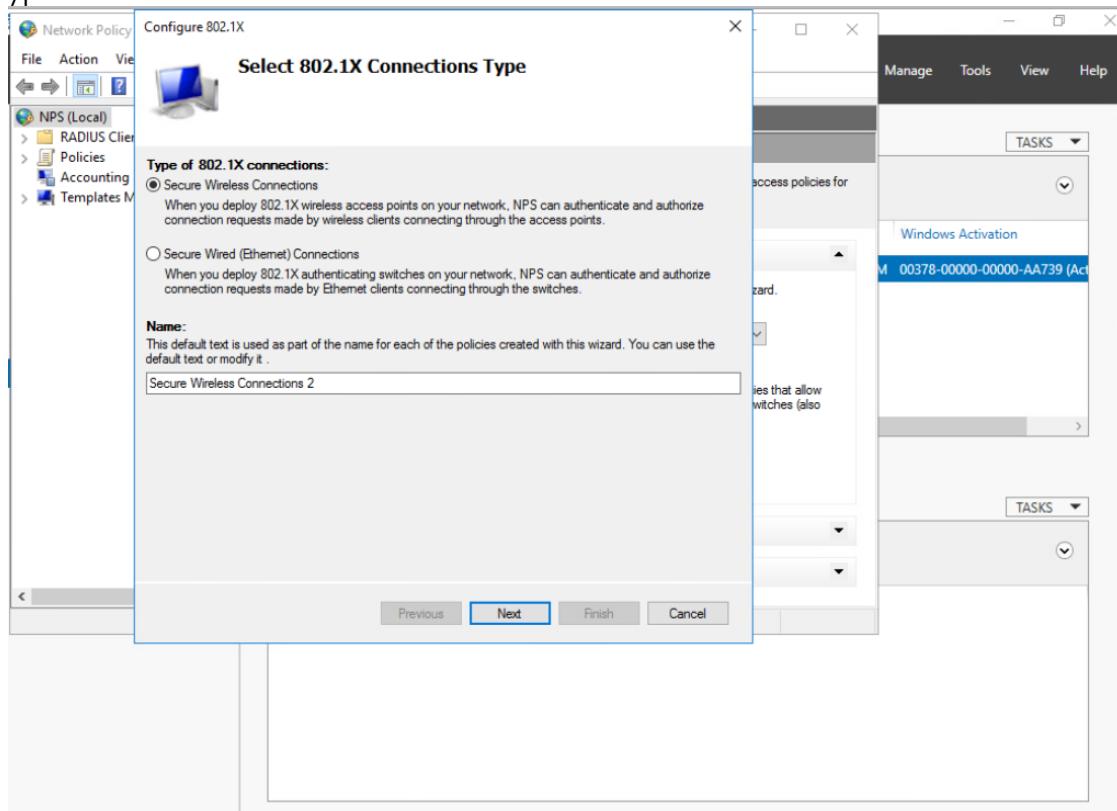


## c. Configuration de RADIUS

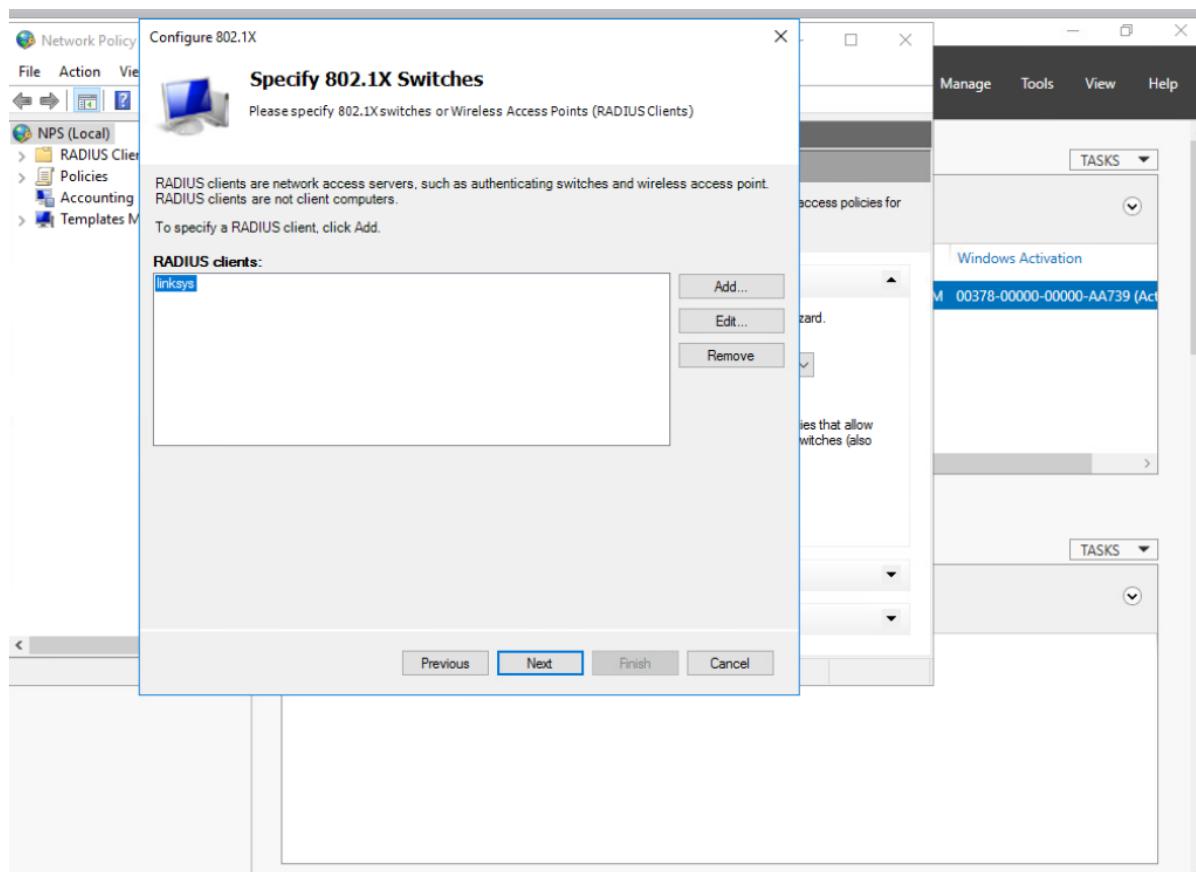
Choix du RADIUS server for 802.1X Wireless or Wired Connections pour la configuration RADIUS



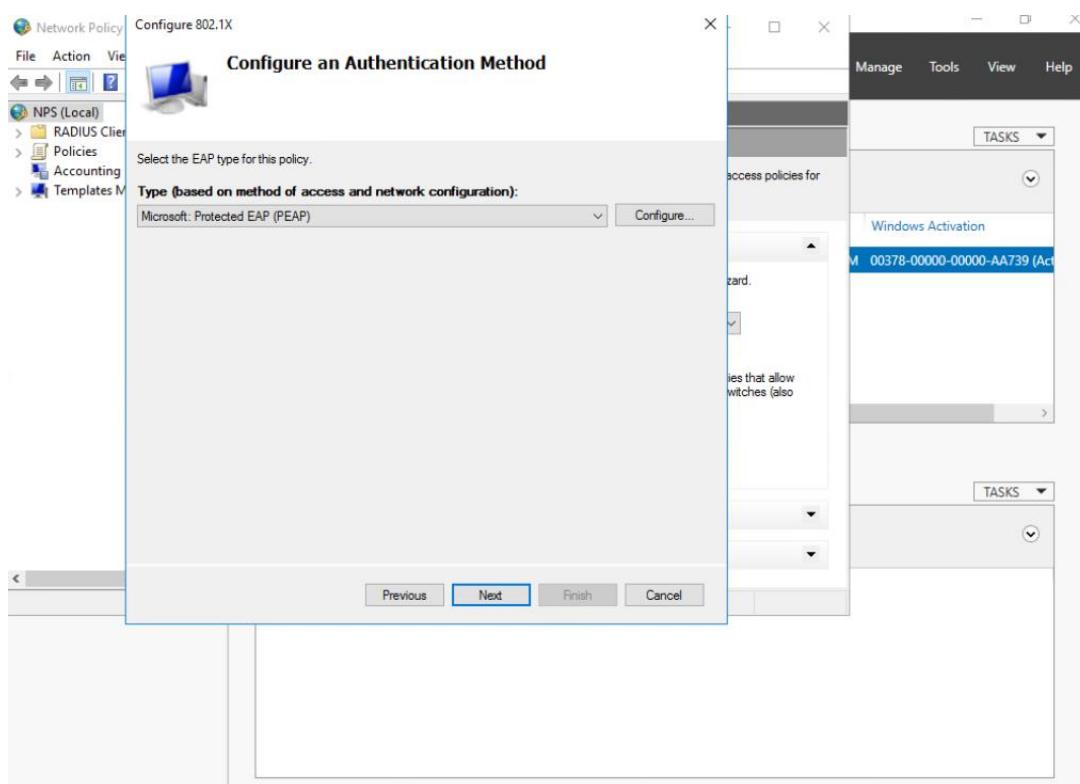
Choix du type de connexion Secure Wireless Connections



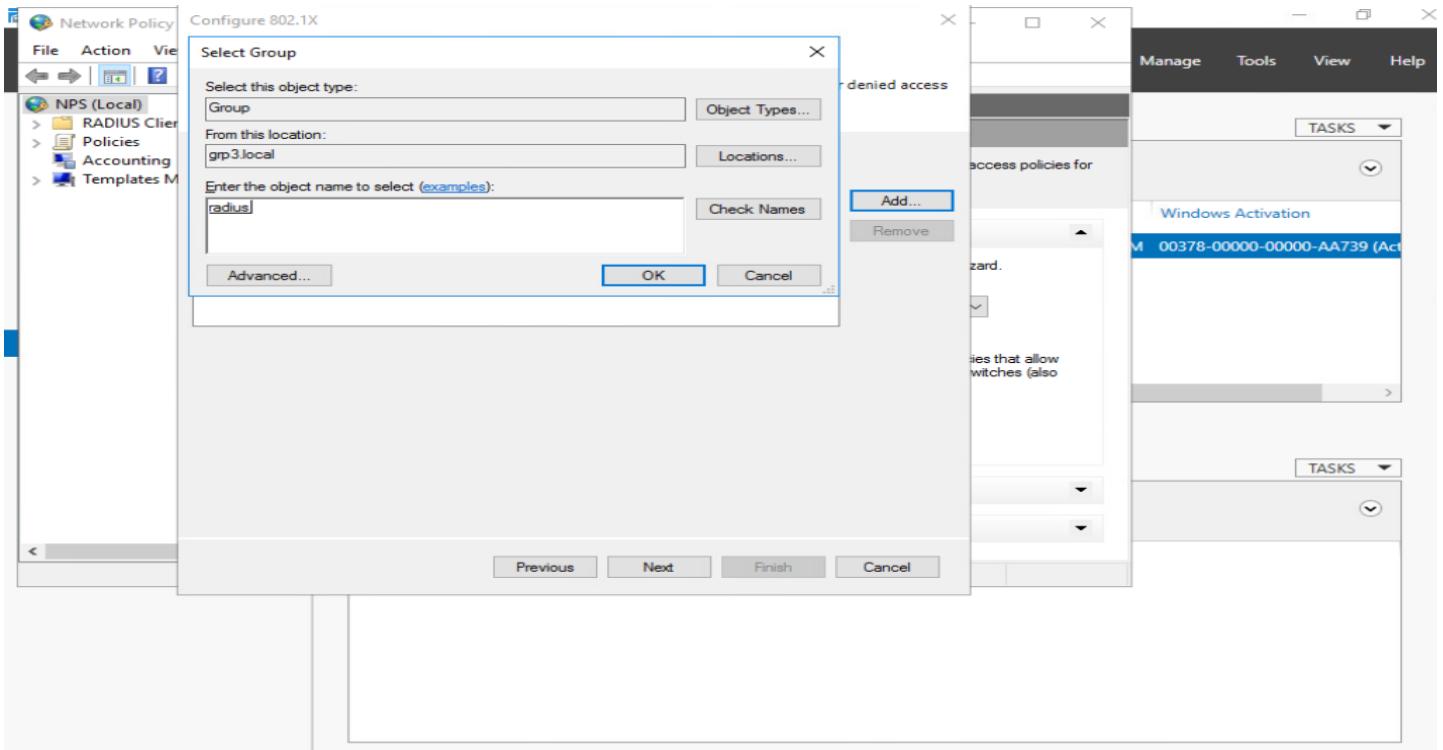
## Choix du client



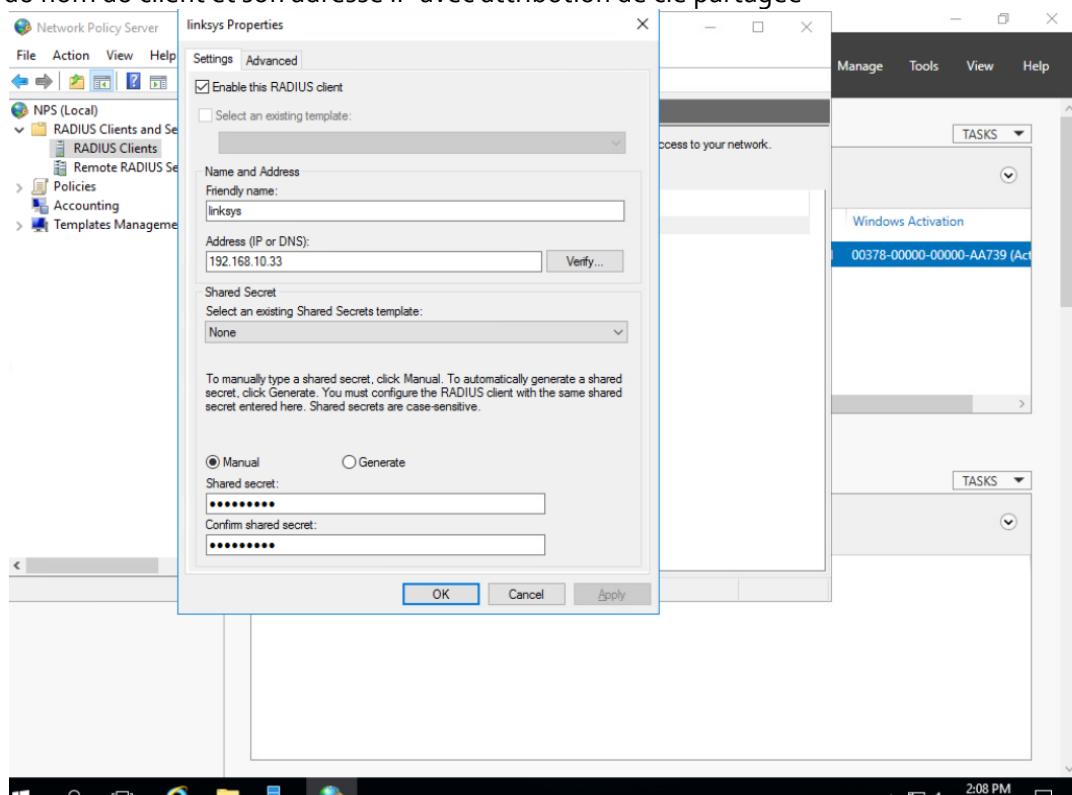
## Choix de la méthode d'authentification Microsoft : Protected EAP(PEAP)



### Selection de notre groupe gr3



### Définition du nom du client et son adresse IP avec attribution de clé partagée



## d. Configuration du Point d'Access

- Changement du SSID en « Employes\_GRP3 ».

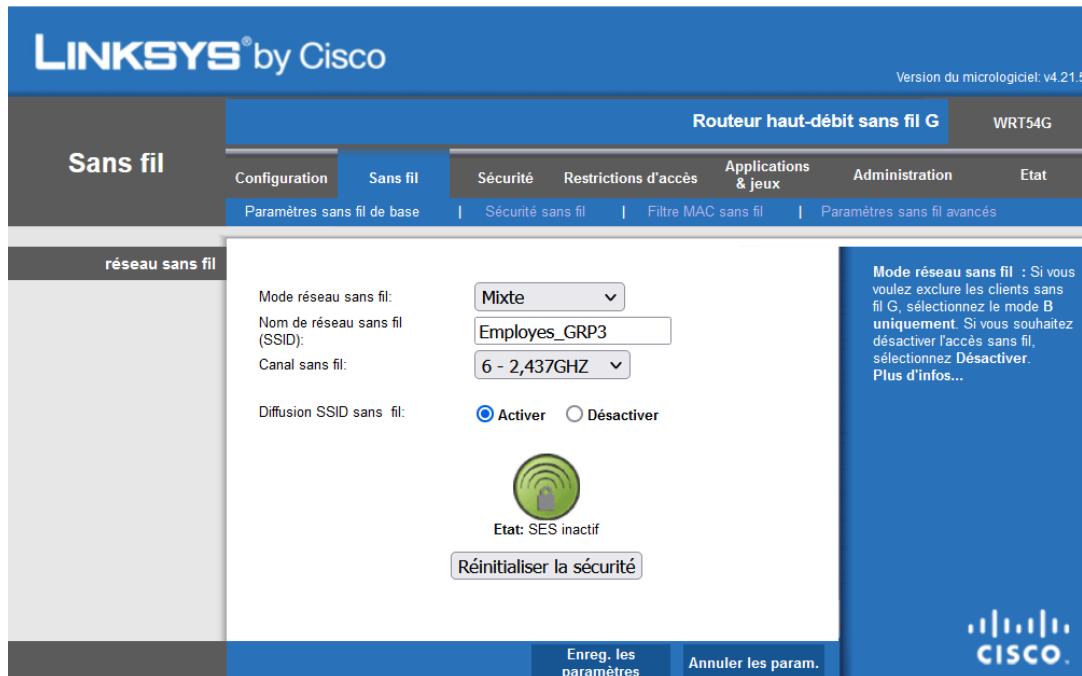


Figure 36 Changement du SSID

- Attribution d'une adresse IP fixe au routeur « 192.168.10.33/24 » et Désactivation du serveur DHCP puisque c'est le Serveur Ubuntu qui sera charger de l'attribution des adresses IP.

The screenshot shows the 'Configuration Internet' (Internet Configuration) and 'Configuration réseau' (Network Configuration) tabs selected. In the 'Configuration Internet' section, 'Type de connexion Internet' is set to 'Configuration automatique - DHCP'. In the 'Configuration réseau' section, 'Adresse IP du routeur' is set to '192.168.10.33' and 'Masque de sous-réseau' is set to '255.255.255.0'. The 'Serveur DHCP' section has 'Activer' (Enable) selected. Other DHCP settings include 'Adresse IP de départ' (192.168.10.100), 'Nombre maximal d'utilisateurs DHCP' (50), 'Plage d'adresses IP' (192.168.10.100 to 149), 'Durée de bail du client' (0 minutes), and DNS/WINS configurations. A note on the right side of the screen provides information about the 'Nom de l'hôte' (Host name), 'Nom du domaine' (Domain name), 'Adresse IP locale' (Local IP address), 'Masque de sous-réseau' (Subnet mask), 'Serveur DHCP' (DHCP server), 'Adresse IP de départ' (Start IP address), 'Nombre maximum d'utilisateurs DHCP' (Maximum number of DHCP users), and 'Réglage de l'heure' (Timezone).

Figure 37 Configuration du Point d'Access

- On configure la partie « Sans Fils » -> « Sécurité sans fil ».

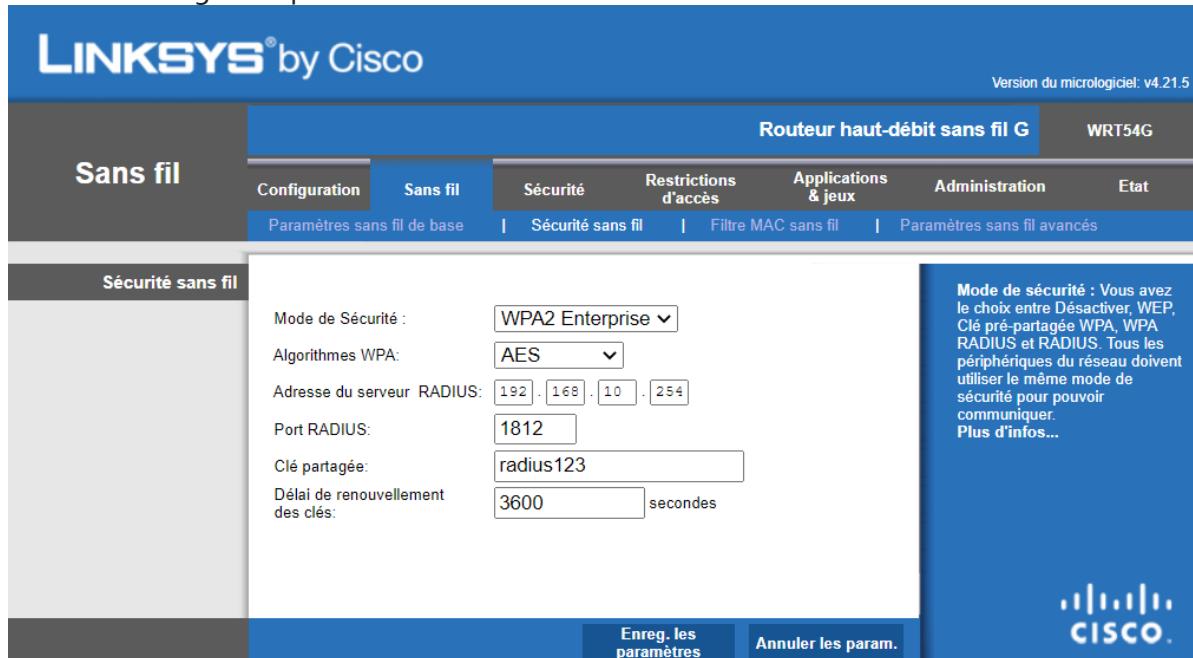


Figure 38 Configuration de la sécurité sans fil

Nous utilisons le protocole WPA2 Entreprise avec l'authentification RADIUS, qui utilise toujours le chiffrement AES pour sécuriser les données. Ce mode nécessite également un serveur RADIUS pour authentifier les utilisateurs. Il permet aux clients WPA et WPA2 de se connecter simultanément.

Nous avons choisi l'adresse IP du serveur RADIUS, qui est 192.168.10.254, ainsi que le port par défaut, qui est 1812. Dans le fichier de configuration de clients sur le serveur RADIUS, nous avons également choisi la clé partagée "radiuspass2023".

## **Conclusion**

Dans ce chapitre, nous avons récemment mis en place le protocole RADIUS pour authentifier les employés avant de leur permettre l'accès au réseau. Il est maintenant temps de passer au prochain chapitre, qui traite de l'authentification des invités.

# Chapitre 2 : Authentification des invités

Dans ce chapitre, nous allons explorer l'intégration d'un portail captif dans pfSense afin de contrôler l'accès des utilisateurs équipés d'un navigateur web au réseau. Cette fonctionnalité permettra d'authentifier les invités se connectant au point d'accès avant qu'ils ne puissent accéder au réseau externe.

## I. Le Portail Captif

### 1. Définition

La technique du portail captif implique de contraindre les navigateurs web des utilisateurs d'un réseau à afficher une page web spécifique, dans la plupart des cas pour des raisons d'authentification, avant de leur permettre un accès normal à Internet. Bien que souvent utilisée pour les accès Wi-Fi, cette méthode peut également être appliquée aux réseaux filaires.

### 2. Fonctionnement

Le portail captif fonctionne en interceptant tous les paquets liés aux protocoles HTTP ou HTTPS, sans tenir compte de leur destination. Dans notre cas, l'utilisateur, c'est-à-dire l'invité, est dirigé vers une page web spéciale pour s'authentifier. Cette méthode peut également être utilisée pour effectuer des paiements, collecter des informations et obtenir le consentement de l'utilisateur en ce qui concerne les conditions d'utilisation.

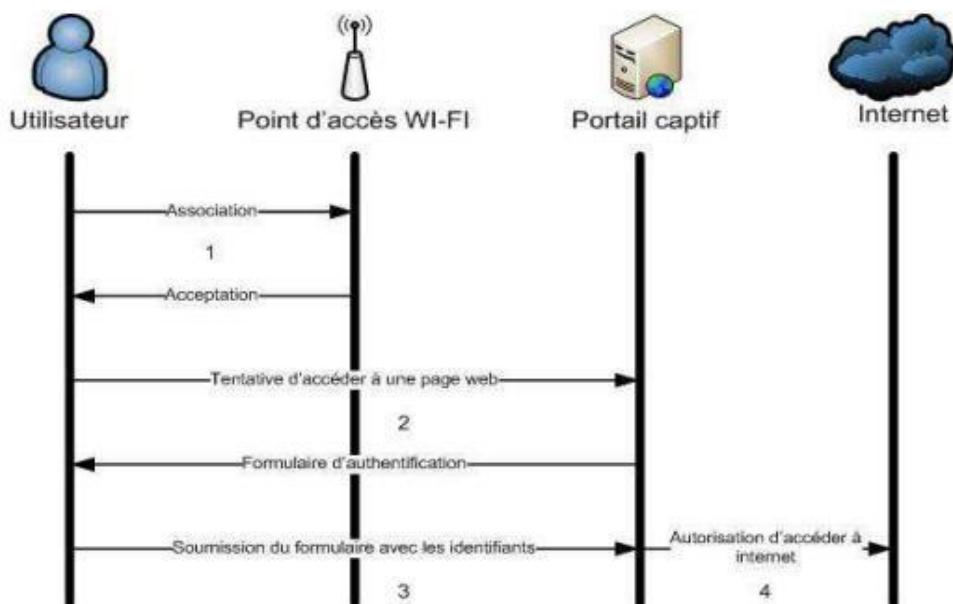


Figure 55 Diagramme de séquences du portail captif

- Dans un premier temps, l'invité se connecte au point d'accès en utilisant le SSID.
- Lorsqu'il souhaite accéder à une URL sur Internet, le portail captif lui envoie un formulaire d'authentification.
- Le formulaire, qui contient les champs requis pour l'authentification, est ensuite envoyé au portail captif.
- Si l'authentification est réussie, le portail autorise alors l'accès à Internet.

## II. PfSense

### 1. Définition

PfSense est un système d'exploitation open source basé sur la distribution BSD (FreeBSD), ce qui lui confère une grande fiabilité et une sécurité informatique élevée. Il offre la possibilité de déployer un pare-feu, un routeur et un portail captif. PfSense propose également des outils et services similaires à ceux des routeurs professionnels propriétaires, mais de manière libre. Il convient donc à la sécurisation des réseaux domestiques et professionnels.



Plusieurs services peuvent être gérés par pfSense, ils peuvent être activés ou arrêtés à l'aide d'une interface graphique. Voici quelques services proposés par Pfsense :

- VPN client PPTP, VPN site à site OpenVPN et IPSec.
- Filtrage d'URL.
- Répartition de charge (LoadBalancer).
- IDS-IPS Snort.
- Serveur DHCP.
- Gestion des VLAN.

## 2. Installation PfSense

- Création une nouvelle machine du type **BSD** et version FreeBSD (64 bits).
- Ajout du fichier iso de Pfsense.
- Dans l'onglet réseaux (Networks), nous activons deux adaptateurs réseaux, le premier sera relié au Lan (vlan20) et le deuxième adaptateur sera lié au Wan (vlan40), après nous lançons la machine et nous choisissons les étapes par défaut.

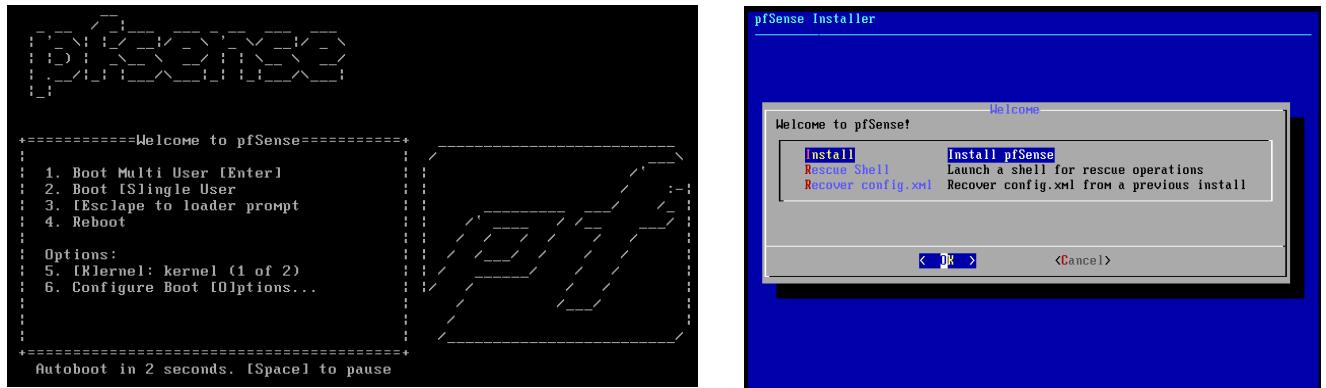


Figure 56 Installation PfSense

À la fin de l'installation et le lancement de Pfsense. La première étape que nous devons faire est de configurer les interfaces réseau.

- Depuis la console de Pfsense, nous choisissons l'option numéro 2 (Set interfaces ip address) et nous sélectionnons l'interface réseau numéro 2 (emo), nous acceptons la configuration IP via le DHCP.
- On sélectionne l'interface numéro 2 (emo), et on lui assigne l'adresse IP 192.168.20.2 avec un masque réseau /24, et la passerelle 192.168.20.1



Figure 57 Menu PfSense

- La plage DHCP est de [192.168.20.10 – 192.168.20.245]

```

Available interfaces:
1 - WAN (em1 - static)
2 - LAN (em0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
>192.168.20.254/24

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 LAN IPv4 subnet bit count (1 to 31):
> 22

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>192.168.20.254/24

Enter the new LAN IPv6 address. Press <ENTER> for none:
> 

```

Figure 58 Configuration interface Lan

- Avec la même méthode, nous sélectionnons l'interface numéro 1 (em1) pour configurer le réseau Wan avec une adresse IP (192.168.50.2) pour l'interface em1 avec un masque réseau /28.

```

The IPv4 WAN address has been set to 172.16.5.130/28
Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 454c087d2d3c11e549c5

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em1      -> v4:192.168.50.2 /28
LAN (lan)      -> em0      -> v4:192.168.20.254/24

8) 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

Enter an option: 

```

Figure 59 Configuration des interfaces

### 3. Interface web pfSense

- Accéder à l'interface web en entrant l'adresse IP du côté LAN de PfSense dans un navigateur sur la machine de l'administrateur, dans notre cas : 192.168.20.1. Dont les identifiants sont : (Username : **admin** – Password : Admin1234)

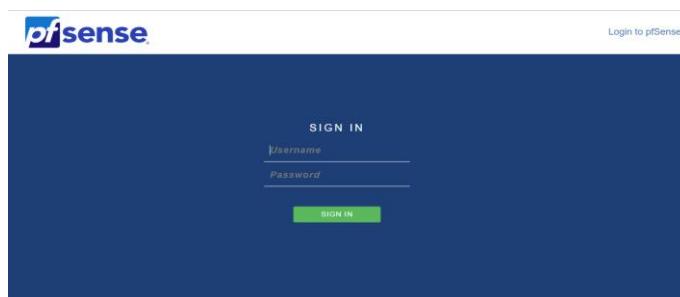


Figure 60 Interface web pfSense

- Nous arrivons donc sur le tableau de bord de notre pfSense. Ici en trouve des informations sur l'utilisation des ressources de la machine elle-même, ses différentes adresses IP, sa version et ses mises à jour si nécessaire etc...

The screenshot shows the pfSense dashboard with the following sections:

- System Information:**
  - Name: pfSense.lan
  - User: admin@192.168.20.100 (Local Database)
  - System: VMware Virtual Machine  
Netgate Device ID: b082dc72fd4875279598
  - BIOS: Vendor: Phoenix Technologies LTD  
Version: 6.00  
Release Date: Tue Apr 5 2016
  - Version: 2.5.2-RELEASE (amdgpu)  
built on Fri Jul 02 15:33:00 EDT 2021  
FreeBSD 12.2-STABLE
  - CPU Type: Intel(R) Xeon(R) CPU E5-2695 v4 @ 2.10GHz  
8 CPUs | 8 package(s) x 1 core(s)  
AES-NI CPU Crypto: Yes (inactive)  
QAT Crypto: No
  - Hardware crypto
  - Kernel PTI: Enabled
  - MDS Mitigation: Inactive
  - Uptime: 02 Hours 21 Minutes 17 Seconds
  - Current date/time: Sat Mar 25 14:05:09 +00 2023
  - DNS server(s): 127.0.0.1, 8.8.8, 8.8.4.4
  - Last config change: Fri Mar 24 17:01:53 +00 2023
  - State table size: 0% (312/1193000) Show states
- Netgate Services And Support:** Retrieving support information.
- Interfaces:**
  - WAN: 1000baseT <full-duplex> 192.168.50.1
  - LAN: 1000baseT <full-duplex> 192.168.20.254

Figure 61 Page d'Accueil pfSense

#### 4. DHCP et DNS

On vérifie la plage DHCP qu'on configurée précédemment, la plage d'adresses : 192.168.20.10 - 192.168.20.245

The screenshot shows the DHCP Server configuration for the LAN interface:

- General Options:**
  - Enable:  Enable DHCP server on LAN interface
  - BOOTP:  Ignore BOOTP queries
  - Deny unknown clients: Allow all clients
  - Ignore denied clients:  Denied clients will be ignored rather than rejected.
  - Ignore client identifiers:  If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
- Subnet:** 192.168.20.0
- Subnet mask:** 255.255.255.0
- Available range:** 192.168.20.1 - 192.168.20.254
- Range:** From 192.168.20.10 To 192.168.20.245

Figure 62 DHCP 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 : lan
- Dns Serveur : 8.8.8.8

Figure 63 DNS PfSense

The screenshot shows the 'System / General Setup' page. Under 'System', the 'Hostname' is set to 'pfSense' and the 'Domain' is set to 'lan'. In the 'DNS Server Settings' section, there are two entries: '8.8.8.8' and '8.8.4.4'. Both entries have their 'DNS Hostname' fields empty. Below this, under 'DNS Resolution Behavior', it says 'Use local DNS (127.0.0.1), fall back to remote DNS Servers (Default)'.

## 5. Pare-feu

- 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.

The screenshot shows the 'Firewall / Rules / LAN' page. The 'LAN' tab is selected. There are three rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1 /295 KIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗ ✓ 27 /606 KIB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✗ ✓ 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

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

Figure 64 pfSense

## 6. Portail Captif

- La configuration de ce portail se fait en plusieurs étapes. Il faut créer une zone dans laquelle le portail captif sera actif puis configurer cette zone.

Captive Portal Zones				
Zone	Interfaces	Number of users	Description	Actions
ari	WAN	0		
ari2	LAN	0		
<a href="#"> Add</a>				

Figure 65 zone portail captif

- On active le portail captif « Enable Captive Portal »
- On sélectionne l'interface sur lequel le portail se déploiera c'est l'interface « LAN »
- Activer « Enable logout popup window » (une fenêtre popup permet aux clients de se déconnecter)

Figure 66 Configuration portail captif 1

The screenshot shows the 'Captive Portal Configuration' section of a network management interface. It includes fields for enabling the captive portal, setting a description, selecting interfaces (WAN and LAN), defining maximum concurrent connections, setting idle and hard timeouts, specifying traffic quotas, and configuring pass-through credits per MAC address.

Captive Portal Configuration	
Enable	<input checked="" type="checkbox"/> Enable Captive Portal
Description	<input type="text"/> A description may be entered here for administrative reference (not parsed).
Interfaces	<input type="checkbox"/> WAN <input checked="" type="checkbox"/> LAN
Maximum concurrent connections	<input type="text"/> Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.
Idle timeout (Minutes)	<input type="text"/> 6 Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout (Minutes)	<input type="text"/> 10 Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
Traffic quota (Megabytes)	<input type="text"/> Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.
Pass-through credits per MAC address.	<input type="text"/> Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for

<b>Waiting period to restore pass-through credits. (Hours)</b>	<input type="text"/> 1	Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 6 hours if pass-through credits are enabled.
<b>Reset waiting period</b>	<input type="checkbox"/> Enable waiting period reset on attempted access	If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.
<b>Logout popup window</b>	<input checked="" type="checkbox"/> Enable logout popup window	If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
<b>Pre-authentication redirect URL</b>	<input type="text"/> https://www.google.com	Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRURL\$ variable in captiveportal's HTML pages.
<b>After authentication Redirection URL</b>	<input type="text"/> https://www.google.com	Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.
<b>Blocked MAC address redirect URL</b>	<input type="text"/>	Blocked MAC addresses will be redirected to this URL when attempting access.
<b>Preserve users database</b>	<input checked="" type="checkbox"/> Preserve connected users across reboot	If enabled, connected users won't be disconnected during a pfSense reboot.
<b>Concurrent user logins</b>	<input type="text"/> Multiple	<p>Disabled: Do not allow concurrent logins per username or voucher.</p> <p>Multiple: No restrictions to the number of logins per username or voucher will be applied.</p> <p>Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected.</p> <p>First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.</p>
<b>MAC filtering</b>	<input type="checkbox"/> Disable MAC filtering	If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

Figure 67 configuration portail captif 2

- Sélection de local database comme premier serveur d'authentification et la base ldap comme deuxième.

<b>Authentication</b>	
<b>Authentication Method</b>	<input type="button" value="Use an Authentication backend"/> Use an Authentication backend
Select an Authentication Method to use for this zone. One method must be selected. - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.	
<b>Authentication Server</b>	<input type="button" value="Local Database"/> Local Database
You can add a remote authentication server in the <a href="#">User Manager</a> . Vouchers could also be used, please go to the <a href="#">Vouchers Page</a> to enable them.	
<b>Secondary authentication Server</b>	<input type="button" value="Local Database"/> Local Database
You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.	
<b>Reauthenticate Users</b>	<input type="checkbox"/> Reauthenticate connected users every minute
If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in. The cached credentials are necessary for the portal to perform automatic reauthentication requests.	
<b>Local Authentication Privileges</b>	<input type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set
<b>HTTPS Options</b>	
<b>Login</b>	<input type="checkbox"/> Enable HTTPS login
When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.	
<input type="button" value="Save"/>	

Figure 68 Serveurs d'authentification ldap

## 7. Création d'un groupe et des utilisateurs

- Dans système, « User Manager », on ajoute un groupe portail. Ce groupe aura dans ses priviléges la connexion au portail captif.

The screenshot shows the 'User Manager / Groups / Edit' interface. The 'Groups' tab is selected. In the 'Group Properties' section, the 'Group name' is set to 'Portail' and the 'Scope' is 'Local'. A warning message states: 'Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.' The 'Description' field contains: 'Group description, for administrative information only'. The 'Group membership' section lists 'Not members' (admin) and 'Members' (khalid, reem). Buttons for moving items between these lists are shown: 'Move to "Members"' and 'Move to "Not members"'. A note says: 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.' In the 'Assigned Privileges' section, there is one entry: 'Name: User - Services: Captive Portal login, Description: Indicates whether the user is able to login on the captive portal.', with an 'Action' column containing a trash icon. A green '+' button labeled 'Add' is available for adding more privileges. At the bottom left is a 'Save' button.

Figure 69 Ajout d'un groupe

The screenshot shows the 'User Manager / Groups / Add Privileges for captive-portal' interface. The 'Groups' tab is selected. In the 'Assigned privileges' section, a list of options is shown, with 'User - Services: Captive Portal login' highlighted. Other options include: 'User - Config: Deny Config Write', 'User - System: Copy files (scp)', 'User - VPN: IPsec xauth Dialin', 'User - VPN: L2TP Dialin', 'User - VPN: PPPOE Dialin', and 'User - System: Shell account access'.

Figure 70 Droit portail captif

- Une fois le groupe créé, la dernière étape va être la création d'un compte utilisateur membre du groupe ari2.

## 8. Test d'authentification

- Lorsque Les invités vont essayer d'accéder à internet, ils vont devoir s'authentifier avant d'accéder au réseau.

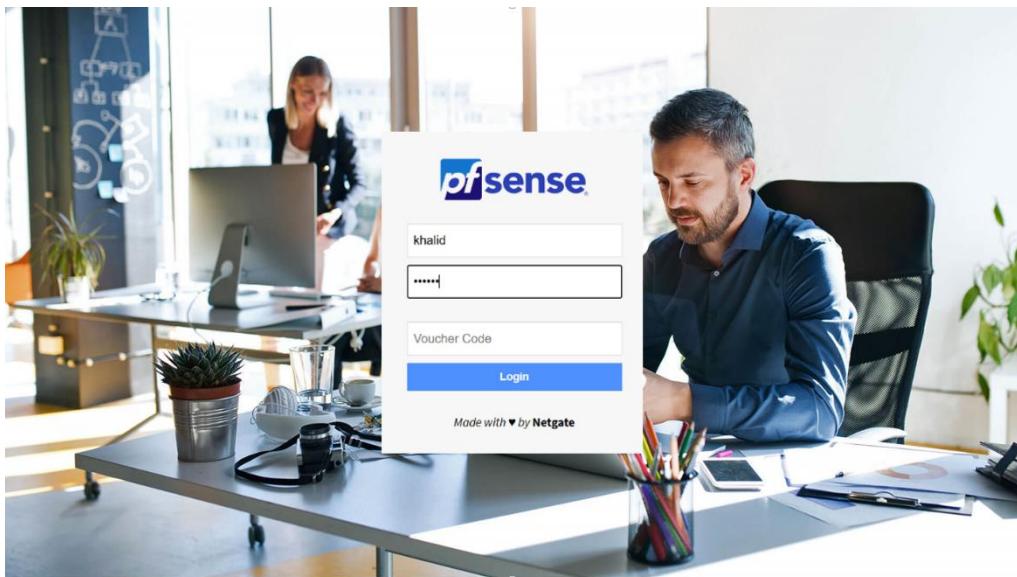


Figure 71 Page d'authentification

- Apres Authentification

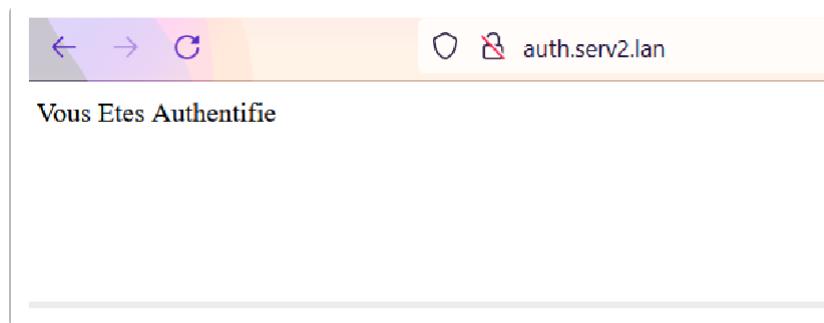


Figure 72 Authentification

En conclusion, ce chapitre a été consacré à la mise en place du portail captif de Pfsense. Ce portail captif est un élément clé pour la sécurité, le contrôle et la gestion du réseau.

# PARTIE III

# Pare-feu et zone DMZ

# Chapitre 1 : Le Pare-feu

Au cours de ce chapitre, nous allons explorer les firewalls, en commençant par définir ce qu'est un pare-feu et en examinant son fonctionnement général ainsi que les différents modes de fonctionnement. Nous aborderons ensuite la configuration de notre pare-feu FortiGate 60D.

## I. Le firewall

### 1. Définition

Un firewall est un appareil de sécurité réseau qui surveille le trafic réseau entrant et sortant et autorise ou bloque les paquets de données en se basant sur un ensemble de règles de sécurité. Il est chargé de dresser une barrière entre votre réseau interne et le trafic entrant provenant de sources externes (comme Internet) afin de bloquer le trafic malveillant des virus et des pirates .

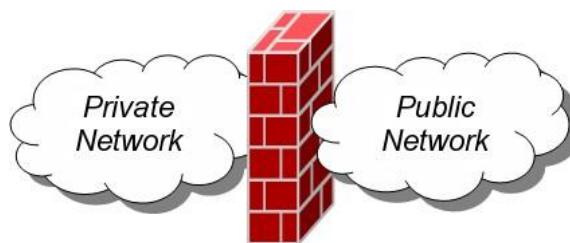


Figure 73 Pare-feu

### 2. Fonctionnement

Les firewalls analysent soigneusement le trafic entrant en fonction de règles préétablies et filtrent le trafic provenant de sources non sécurisées ou suspectes pour empêcher les attaques. Les firewalls surveillent le trafic au point d'entrée d'un ordinateur, appelé port, qui est l'endroit où les informations sont échangées avec des appareils externes.

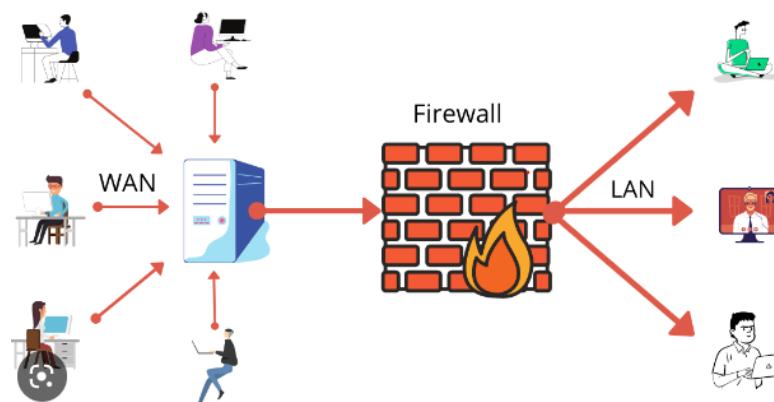


Figure le fonctionnement Pare-feu

### 3. Types de pare-feux

#### a. Les firewall bridge

Les pare-feu bridge sont des équipements relativement répandus qui ont la fonctionnalité de filtrage en plus d'agir comme des câbles réseau. Contrairement aux autres équipements réseau, leurs interfaces ne possèdent pas d'adresse IP et ils se contentent de transférer les paquets d'une interface à une autre en appliquant les règles de sécurité prédéfinies. Cette absence d'adresse IP est particulièrement utile, car elle rend le pare-feu indétectable.

#### b. Les firewalls logiciels

Les pare-feu open source sont généralement basés sur des systèmes d'exploitation tels que Linux ou BSD (Packet Filter), car ces OS offrent une sécurité réseau plus élevée et un contrôle plus adéquat. Leur objectif principal est d'imiter le comportement des firewalls matériels des routeurs, à la différence qu'ils sont configurables manuellement.

#### c. Les firewalls matériels

Les pare-feu intégrés sont directement intégrés dans la machine, fonctionnant comme une sorte de « boîte noire », ce qui leur permet d'avoir une intégration parfaite avec le matériel. Bien que leur configuration puisse parfois être complexe, leur avantage est qu'ils interagissent facilement avec les autres fonctionnalités du routeur en raison de leur présence sur le même équipement réseau.

## 4. Configuration des interfaces

	Status	Name	Members	IP/Netmask	Type	Access	R
<b>Hardware Switch (5)</b>							
	internal		1 2 3 4 5 6 7	192.168.1.99 255.255.255.0	☒ Hardware Switch (7)	PING HTTPS SSH HTTP FMG-Access CAPWAP	6
→	Vlan 10 (vlan_employé)			192.168.10.1 255.255.255.0	⚙ VLAN		0
→	Vlan 20 (Vlan_invité)			192.168.20.1 255.255.255.0	⚙ VLAN		0
→	Vlan 30 (Vlan_admin)			192.168.30.1 255.255.255.0	⚙ VLAN		0
→	Vlan 40			192.168.50.2 255.255.255.0	⚙ VLAN		0

Figure 75 Configuration des interfaces

Cette section explique comment configurer le FortiGate afin qu'il fonctionne sur notre réseau. Les paramètres de base du réseau incluent la configuration des interfaces du FortiGate. Une configuration plus avancée comprend l'ajout de sous-interfaces VLAN et de zones à la configuration réseau du FortiGate.

### a. DMZ

Pour commencer, nous allons configurer l'interface DMZ qui sera connectée à notre port physique DMZ. Dans la section "IP/Network Mask", nous allons entrer l'adresse IP "192.168.5.17" avec le masque 255.255.255.240.

The screenshot shows the 'Edit Interface' configuration for the 'dmz' interface. Key settings include:

- Interface Name:** dmz (90:6C:AC:6F:C2:F1)
- Link Status:** Down (red status icon)
- Type:** Physical Interface
- Role:** DMZ (selected from a dropdown menu)
- Addressing mode:** Manual (selected from a dropdown menu)
- IP/Network Mask:** 192.168.5.17/255.255.255.240

Figure 76 Configuration de la DMZ

The screenshot shows the FortiGate interface under the 'VLANs' tab. A new VLAN named 'dmz' is being configured with the following parameters:

- Name:** dmz
- Type:** IP Range
- Subnet / IP Range:** 192.168.50.16-192.168.50.31
- Interface:** dmz
- Show in Address List:** Enabled (green button)
- Comments:** (empty text area)

Pour configurer les autres interfaces, on suit les mêmes étapes que celles-ci :

- L'interface WAN doit être connectée au port physique WAN avec l'adresse IP 192.168.50.34/28.
- L'interface LAN doit être connectée au port physique interne 4.

### b. VLANs

- Lorsqu'il reçoit des paquets de chacun des quatre VLAN, le commutateur VLAN ajoute des balises d'identification de VLAN et envoie les paquets aux ports locaux ainsi qu'à l'unité FortiGate via la liaison principale. L'unité FortiGate dispose de politiques qui autorisent le trafic à circuler entre les VLAN et de VLAN vers le réseau externe

Edit Interface

Interface Name: Vlan 10  
 Alias: vlan\_employe  
 Type: VLAN  
 Interface: internal  
 VLAN ID: 10

Tags

Role: LAN  
[Add Tag Category](#)

Figure Configuration de VLAN

VLAN	Nomination	IP
10	Employés	192.168.10.0
20	Invités	192.168.20.0
30	Admin	192.168.30.0
40	VLAN 40	192.168.50.0

Tableau 9 Adressage Vlans

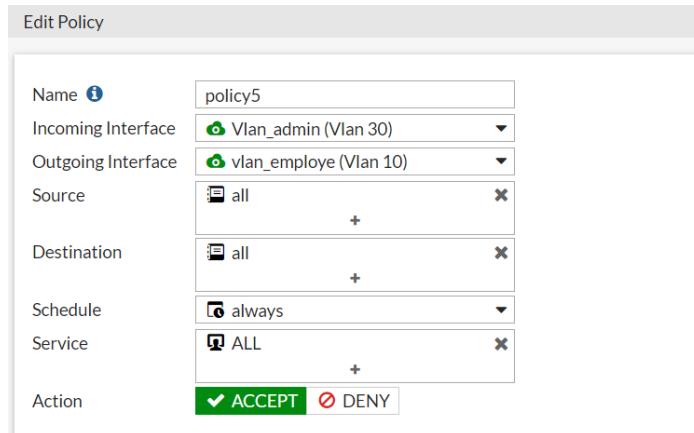
c. Ipv4 Policy (Politique de sécurité)

- Il est impossible pour tout trafic de passer à travers une unité FortiGate, à moins d'avoir été expressément autorisé par une politique de sécurité. Lorsqu'un trafic est ainsi autorisé, pratiquement toutes les fonctionnalités de FortiGate sont appliquées à ce trafic, conformément aux politiques de sécurité en vigueur.

Interface Pair View											By Sequence
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	
1	internal → wan1										
2	Vlan 40 → dmz										
3	Vlan 40 → wan1										
4	Vlan_admin (Vlan 30) → dmz										
5	Vlan_admin (Vlan 30) → internal										
6	Vlan_admin (Vlan 30) → vlan_employe (Vlan 10)										
7	Vlan admin (Vlan 30) → Vlan_invité (Vlan 20)										
8	Vlan_admin (Vlan 30) → wan1										
9	vlan_employe (Vlan 10) → dmz										
10	vlan_employe (Vlan 10) → wan1										
11	wan1 → dmz										
12	Implicit										

Figure 78 ipv4 Policy

- Dans le cadre de la supervision, nous avons d'abord autorisé le VLAN30 (Admin) à accéder aux autres VLAN.
- Pour cela, nous avons ajouté une règle permettant la communication du VLAN 30 vers le VLAN 10.



➤ Figure Admin accède au VLAN des Employés

Les étapes suivantes sont utilisées pour configurer les autres VLAN (10, 40) :

- Pour le VLAN30 vers le VLAN20 : l'adresse source IP est 192.168.30.0/24 et la destination est l'adresse IP 192.168.20.0/24.
- Pour le VLAN30 vers le VLAN40 : l'adresse source IP est 192.168.30.0/24 et la destination est l'adresse IP 192.168.50.0/24.

De plus, les VLAN 10, 30 et 40 sont autorisés à accéder à la zone DMZ et au WAN.

Le WAN, quant à lui, est autorisé à accéder à la zone DMZ.

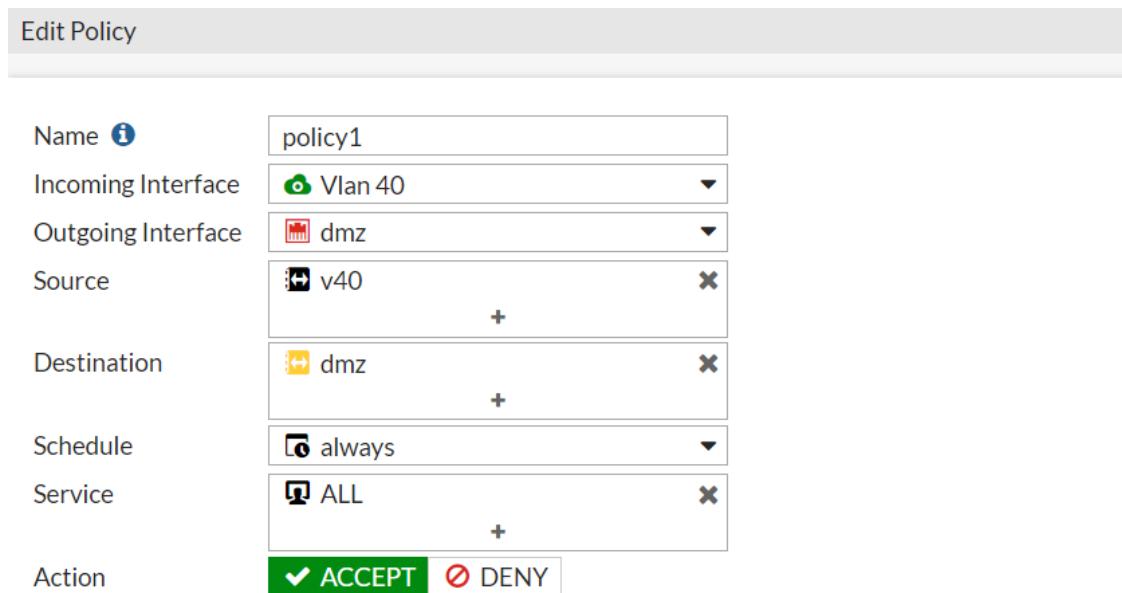


Figure 8o WAN accède au DMZ

Le WAN, quant à lui, est autorisé à accéder à la zone DMZ.

Dans notre configuration actuelle, le Traffic du VLAN 20 n'est pas autorisé vers la zone DMZ et le WAN. Cette mesure a été prise afin que les utilisateurs de ce VLAN soient contraints de s'authentifier via un portail captif avant d'accéder à ces zones.

Une fois authentifiés et ayant accès au VLAN 40, qui dispose des droits d'accès vers ces zones, ils pourront y accéder.

## Conclusion

Ce chapitre a porté sur l'étude du Pare-Feu, un élément d'une importance primordiale dans notre architecture réseau. Le Pare-Feu permet de contrôler le trafic réseau.

## CHAPITRE 2 : La zone DMZ

Ce chapitre décrit le contexte général des zones DMZ . Premièrement, nous présentons une zone démilitarisée, puis nous verrons les différentes architectures Dmz et pourquoi nous avons choisi une architecture DMZ avec un firewall unique.

Les services qui peuvent être consultés à partir d'Internet seront situés dans cette zone, comme le service Web et la messagerie.

## I. La zone DMZ :

### 1. Définition

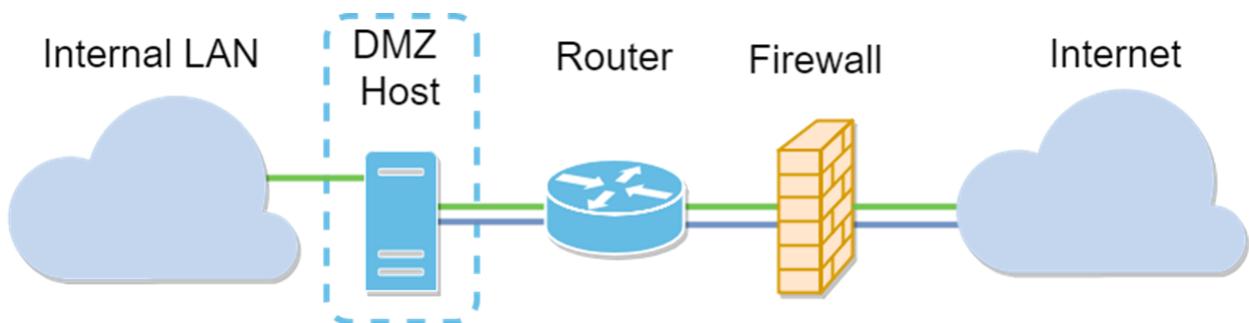
Une zone démilitarisée (DMZ) est un réseau périphérique qui protège le réseau local interne (LAN) d'un organisme contre le trafic non sécuritaire.

Une zone démilitarisée est généralement définie comme un sous-réseau qui se trouve entre l'Internet public et les réseaux privés. Il expose les services externes à des réseaux non fiables et ajoute une couche de sécurité supplémentaire. Pour protéger les données sensibles stockées sur les réseaux internes, grâce à des pare-feux pour filtrer le trafic.

### 2. Fonctionnement

Un réseau DMZ sert de tampon entre Internet et le réseau privé d'une entreprise. La DMZ est isolée par une passerelle de sécurité, telle qu'un pare-feu, qui filtre le trafic entre la DMZ et un réseau LAN. La DMZ est protégée par une autre passerelle de sécurité qui filtre le trafic provenant de réseaux externes.

Elle est idéalement située entre deux pare-feux, et la configuration du pare-feu de la DMZ garantit que les paquets réseau entrants sont contrôlés par un pare-feu, ou d'autres outils de sécurité, avant qu'ils ne soient transmis aux serveurs hébergés dans la DMZ. Cela implique que même si un assaillant complexe parvient à passer le premier pare-feu, il doit également accéder aux services renforcés de la DMZ avant de pouvoir causer des dommages à l'entreprise.



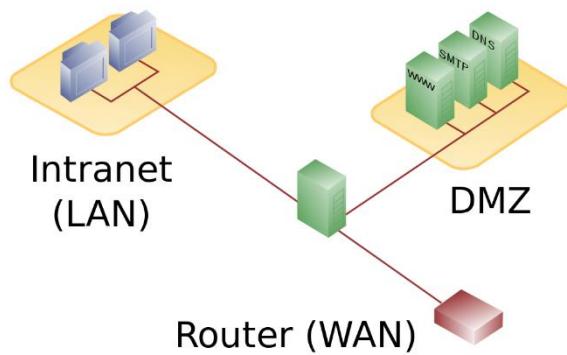
### 3. Architecture

Il existe de multiples façons de concevoir un réseau intégrant une zone démilitarisée. Deux méthodes sont fréquemment employées :

L'utilisation d'un pare-feu unique (parfois appelé « pare-feu à trois interfaces ») et l'utilisation de deux pares-feux. Chacun de ces systèmes peut être étendu afin de créer des architectures complexes répondant aux exigences du réseau.

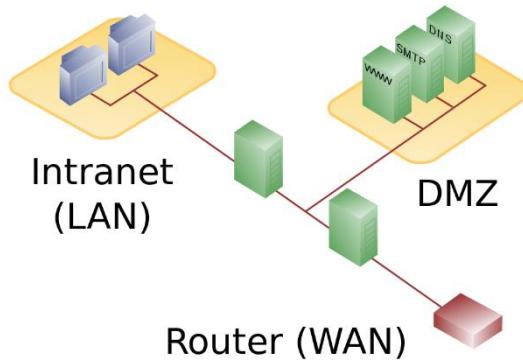
### a. Architecture avec un seul pare-feu

Il est plus rentable de réaliser une DMZ via un seul pare-feu performant (par exemple un routeur incluant un pare-feu) avec trois connections réseaux séparées : une pour Internet, une pour le réseau local et une troisième pour la zone démilitarisée. En ce qui concerne les DMZ protégées, toutes les connexions sont surveillées par le même pare-feu indépendamment les unes des autres, ce qui peut entraîner un point unique de défaillance dans le réseau (de l'anglais Single point of Failure). Par ailleurs, le pare-feu doit, dans une telle architecture, être capable gérer tant le trafic



### b. Architecture avec deux pares feux

Pour prévenir les réseaux d'entreprises contre les accès provenant du réseau public (WAN, Wide Area Network soit le réseau "dispersé"), il convient de mettre en œuvre les concepts de zones démilitarisées en utilisant deux pare-feu. Il peut s'agir de composants matériels indépendants ou d'un logiciel pare-feu sur un routeur. Le pare-feu externe protège la zone démilitarisée du réseau public, le pare-feu interne est quant à lui connecté entre le DMZ et le réseau de l'entreprise.



## II. Le serveur de messagerie :

### 1. Definition

Un serveur de messagerie est un système informatique dont la fonction principale consiste à envoyer et recevoir des e-mails. Lorsqu'un e-mail est envoyé, il traverse une chaîne de serveurs avant d'arriver à sa destination finale. Bien que ce processus soit rapide et efficace, l'envoi et la réception d'e-mails sont des opérations complexes.

### 2. Les types des serveurs de messagerie

On peut classifier les serveurs de messagerie en deux catégories principales : les serveurs de messagerie sortants et les serveurs de messagerie entrants.

#### a. Les serveurs de messagerie entrants :

- ✓ **SMTP** : SMTP (Simple Mail Transfer Protocol) est une application qui permet l'envoi, la réception et le relais des e-mails sortants entre les expéditeurs et les destinataires. Le protocole SMTP est utilisé pour transférer les emails d'un serveur à un autre sur Internet. En résumé, un e-mail SMTP est un e-mail envoyé via le serveur SMTP.

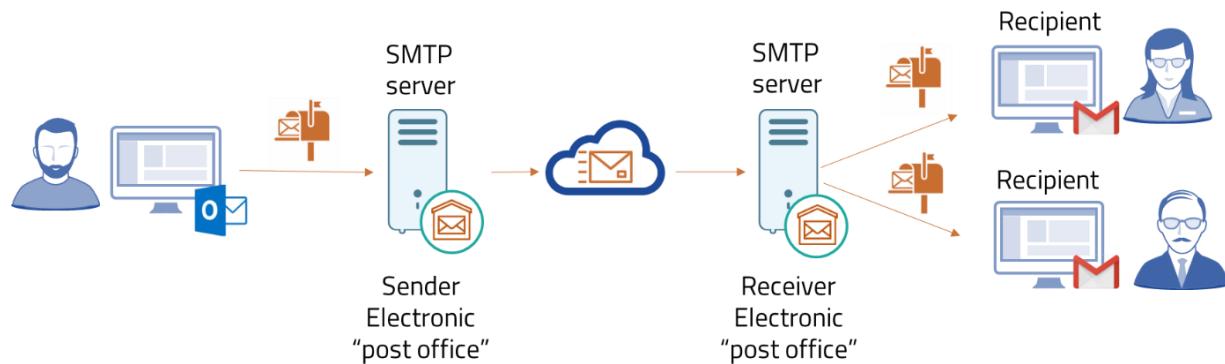


Figure 83 SMTP

Le relais SMTP est défini comme le processus de transfert d'un e-mail d'un serveur à un autre et est utilisé principalement pour envoyer des e-mails d'un domaine à un autre qui diffère de celui de l'utilisateur. Le recours à un service de relais SMTP peut résoudre divers problèmes tels que la délivrabilité des e-mails et les listes noires d'adresses IP.

b. Les serveurs de messagerie sortants :

- **POP3** : Post Office Protocol version 3 (POP3) est un protocole de messagerie standard utilisé pour recevoir des e-mails d'un serveur distant vers un client de messagerie local. POP3 vous permet de télécharger des e-mails sur votre ordinateur local et de les lire même lorsque vous êtes hors ligne.

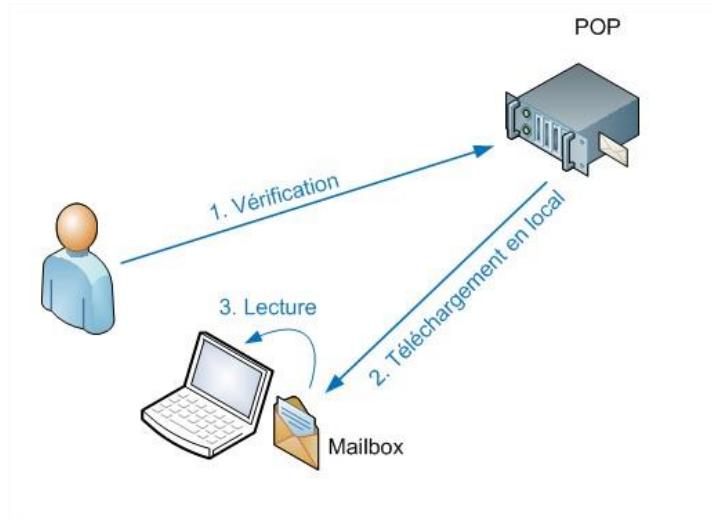


Figure 84 POP3

Lorsqu'on utilise le protocole POP3 pour se connecter à un compte de messagerie, les messages sont téléchargés localement et supprimés du serveur de messagerie. Cela implique qu'il n'est pas possible d'accéder aux messages à partir de plusieurs emplacements. En revanche, en utilisant POP3, les messages sont stockés sur l'ordinateur local, ce qui permet de réduire l'espace occupé par le compte de messagerie sur le serveur Web.

**Port 995** : c'est le port du POP3 sécurisé.

**Port 110** : il s'agit du port POP3 non chiffré par défaut.

- **IMAP** : (Internet Message Access Protocol) désigne un protocole permettant l'accès direct à ses courriels sur un serveur de messagerie. Il permet aux utilisateurs d'accéder à leurs e-mails de n'importe où, sans avoir à les télécharger ni les sauvegarder sur un ordinateur, une tablette ou un smartphone, car ces e-mails sont stockés en permanence sur un serveur. Ainsi, il permet un gain de temps considérable et un accès plus rapide aux courriels.

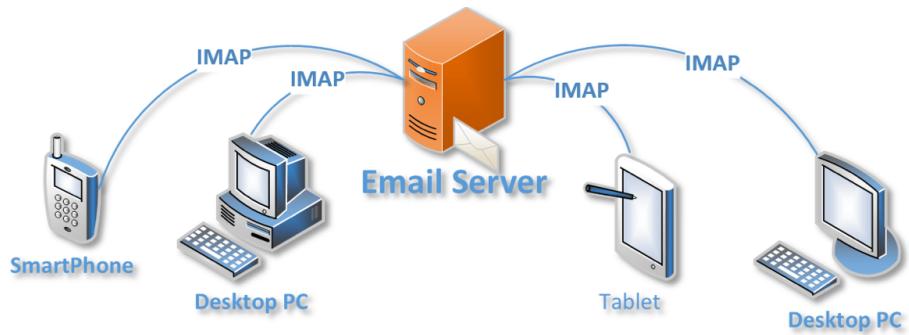


Figure 85 IMAP

Par défaut, le protocole IMAP fonctionne sur deux ports :

**Port 143** : il s'agit du port non crypté IMAP par défaut ;

**Port 993** : c'est le port que vous devez utiliser si vous souhaitez vous connecter en utilisant IMAP en toute sécurité.

#### 4. La différence entre IMAP et POP3

Le protocole POP3 est un standard sur Internet qui permet de récupérer les messages depuis un serveur et de les supprimer, ou de les laisser pendant une certaine durée. Bien que l'accès POP3 soit simple et rapide, il est moins flexible que l'IMAP, car seuls les e-mails de la boîte de réception seront synchronisés. Les autres dossiers tels que les spams, les messages envoyés ou les messages supprimés ne seront pas synchronisés.

En revanche, contrairement à POP3, le protocole IMAP permet non seulement de lire les messages, mais aussi de les enregistrer et de les classer directement depuis le serveur. Tous les dossiers de la boîte e-mail seront synchronisés, ce qui permet de gérer ses e-mails indépendamment de l'endroit où l'on se trouve ou du programme de messagerie utilisé.

## 5. Le fonctionnement du serveur de messagerie

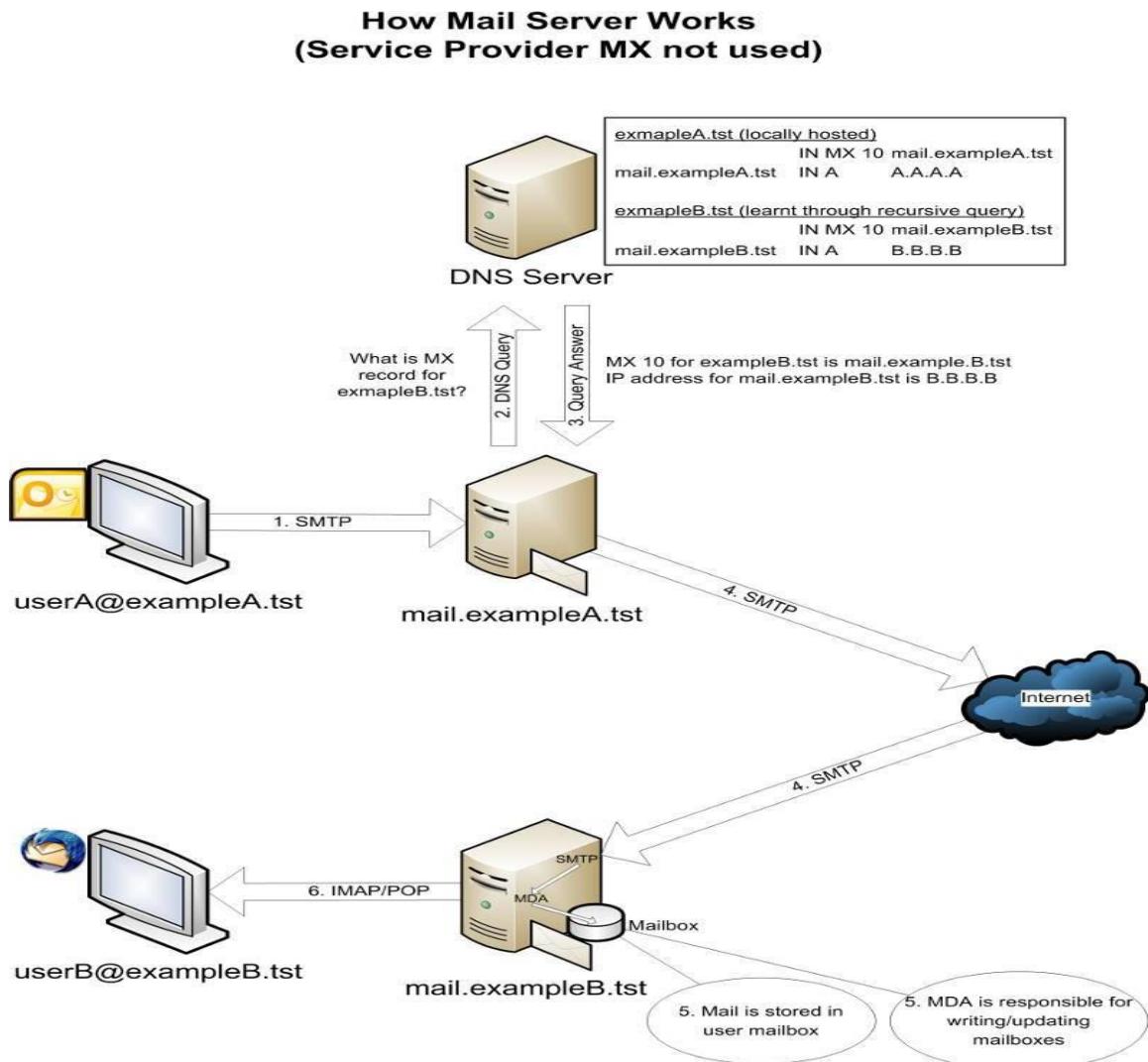


Figure 86 le fonctionnement du serveur SMTP

- Pour comprendre le fonctionnement du serveur de messagerie il faut expliquer les mots clé :
- **Mail User Agent (MUA):** le MUA est un composant qui interagit directement avec les utilisateurs finaux. Thunderbird, MS Outlook, Zimbra Desktop sont des exemples de MUA. Les interfaces de messagerie Web comme Gmail et Yahoo! sont également MUA.
- **Agent de transfert de courrier (MTA):** le MTA est responsable du transfert d'un e-mail d'un serveur de messagerie expéditeur jusqu'à un serveur de messagerie destinataire. **Sendmail** et **postfix** sont des exemples de MTA.
- **Agent de distribution de courrier (MDA):** au sein d'un serveur de messagerie de destination, le MTA local accepte un courrier électronique entrant provenant d'un MTA distant. L'e-mail est ensuite remis à la boîte aux lettres de l'utilisateur par MDA.

Lorsqu'un utilisateur commence à envoyer un e-mail, plusieurs étapes se produisent :

L'application de messagerie d'un expéditeur établit une connexion avec le serveur de messagerie de exampleA.tst en utilisant le protocole SMTP, généralement sur le port TCP 25.

Le serveur de messagerie de exampleA.tst reçoit l'e-mail et apprend que le domaine de destination est exampleB.tst. Il interroge alors un serveur DNS local pour obtenir l'enregistrement MX correspondant à exampleB.tst. Si l'information n'est pas déjà enregistrée dans le cache DNS local, une requête récursive est envoyée au serveur DNS faisant autorité pour le domaine. Une fois que le serveur DNS local reçoit les informations de l'enregistrement MX, il les renvoie au serveur de messagerie de exampleA.tst en guise de réponse.

Avec l'adresse IP du serveur de messagerie de destination, le serveur de messagerie de exampleA.tst envoie l'e-mail directement au serveur de messagerie de mail.exampleB.tst via Internet en utilisant le protocole SMTP.

Lorsque l'e-mail arrive au serveur mail.exampleB.tst, il est reçu par le serveur SMTP local. Une fois que l'e-mail est reçu, il est transmis au MDA, qui écrit ensuite l'e-mail dans la boîte aux lettres du destinataire stockée sur le serveur. Le serveur dispose de boîtes aux lettres distinctes pour chaque utilisateur.

Lorsque le destinataire vérifie l'e-mail via POP ou IMAP, l'e-mail est récupéré par l'application de messagerie à partir du serveur. Selon la configuration de l'application de messagerie, 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 l'application de messagerie sont synchronisés.

## 6. Installation et configuration du serveur de messagerie

### a. Prérequis logiciels :

- Pour installer un serveur de messagerie on doit avoir le MUA qui va prendre le rôle du serveur mail, dans notre cas on va utiliser **POSTFIX**.
  - **POSTFIX** :



Postfix est un serveur de messagerie électronique et un logiciel libre développé par Wietse Venema et plusieurs contributeurs. Il se charge de la livraison de courriers électroniques (courriels) et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que l'historique Sendmail.

- **DOVECOT :**



Dovecot est un serveur IMAP et POP3 pour les systèmes d'exploitation Unix et dérivés, conçu avec comme premier but la sécurité

- b. Configuration du serveur de messagerie :

#### Etape 1 : installation du serveur de messagerie « Postfix » :

- La première chose qu'on doit faire est d'installer le paquet « Postfix » par la commande : **sudo apt-get install postfix**.

```
(khalid@khalid) ~]$ sudo apt-get install postfix
```

- Après, on va modifier le fichier « main.cf » qui se trouve dans le répertoire /etc/postfix/main.cf par la commande.

Dans ce fichier on va attribuer à la variable « **myhostname** » le nom du domaine « **mai.l.ari.ma** », ensuite on va donner à la variable « **mydestination** » notre destination , puis on va ajouter les adresses IP qui peuvent accéder au serveur dans la variable « **mynetworks** » qui sont dans notre cas **192.168.10.0** , **192.168.20.0** , **192.168.30.0** avec le masque **/24** , et pour la variable

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version
#OS
# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no
# appending .domain is the MUA's job.
append_dot_mydomain = no
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
readme_directory = no
# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
# fresh installs.
compatibility_level = 3.6
#route
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may
smtpd_tls_ciphers=HIGH
smtpd_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.ari.ma
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = ari.ma, debian.ari.ma, $myhostname, khalid, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.1.0/24
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

Figure 87 le fichier de configuration de postfix

- Pour le fichier /etc/mailname nous allons le modifier en ajoutant le nom de domaine **ari.ma**

```
ari.ma
~ OS
~ ~
~ ~
~ ~
~ ~
```

### **Etape 2 : installation du serveur IMAP et POP3 « Dovecot » :**

- Concernant l'installation du « dovecot » on va utiliser la commande : **Sudo apt-get Install dovecot-core dovecot-pop3d dovecot-imapds**

```
File Actions Edit View Help
(khalid@khalid)-[~]
$ sudo apt-get install dovecot-core dovecot-pop3d dovecot-imapds
```

- Après l'installation du paquet on va modifier le fichier dovecot qui se trouve dans le répertoire /etc/dovecot/dovecot.conf avec la commande :

**Sudo nano /etc/dovecot/dovecot.conf**

- On va ajouter les protocoles imap et pop3.
- Par défaut, les ID utilisateur sur dovecot utilisant passdb n'incluent pas le nom de domaine (juste le nom d'utilisateur), et pour faire en sorte que les utilisateurs utilisent le format username@domainname on va ajouter la variable « **auth\_username\_format = %n** »

## L'ajout d'enregistrement du type MX (DNS)

- Dans le fichier /etc/bind/db.ari.ma on va ajouter l'enregistrement du type MX avec le nom complet du serveur (mail.ari.ma).

### Résolution du nom de machine et de l'adresse IP

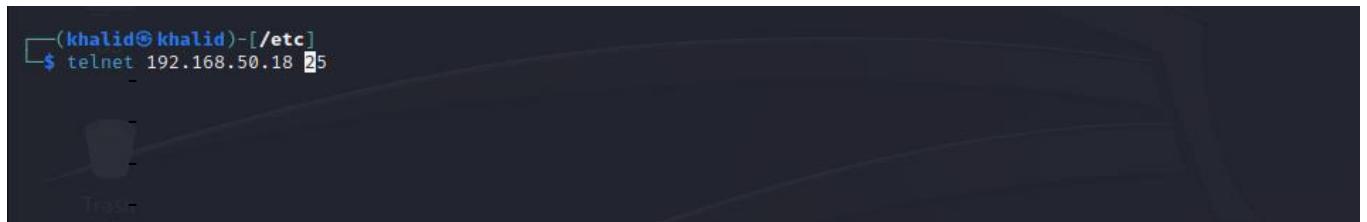
```
; BIND data file for local loopback interface
;
$TTL    604800
@      IN      SOA     debian.ari.ma.  admin.ari.ma (
                      2           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
@      IN      NS      debian.ari.ma.
debian.ari.ma.   IN      A      192.168.50.18
server-web       IN      A      192.168.50.18
www              IN      CNAME  server-web
mail             IN      A      192.168.50.18
~
~
~
~
~
~
~
~
-- INSERT --
```

On démarre postfix avec la commande **service postfix start**



```
(khalid@khalid)-[~/etc]$ service postfix start
```

On va démarrer l'implémentation avec la commande **telnet 192.168.50.18 25**



```
(khalid@khalid)-[~/etc]$ telnet 192.168.50.18 25
```

On accède au serveur messagerie avec la commande « helo mail »

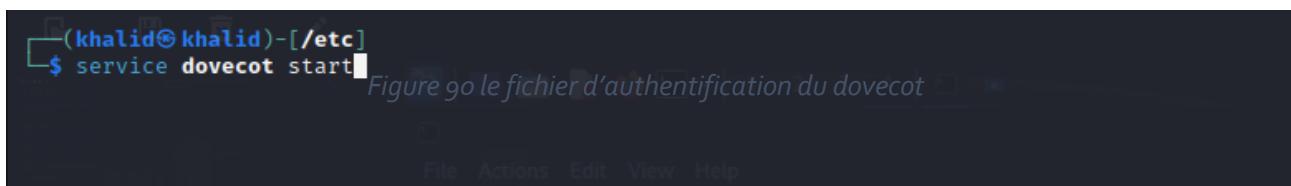
On envoie le message en utilisant la commande « mail from : ali@ari.ma »

On reçoive le message avec la commande « rcpt to : khalid@ari.ma »

On mets le corps du message dans la section « data »

```
Escape character is '^]'.
220 mail.ari.ma ESMTP Postfix (Debian/GNU)
helo mail
250 mail.ari.ma
mail from: ali@ari.ma
250 2.1.0 Ok
rcpt to: khalid@ari.ma
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Hello ari(khalid , Taha, amine , imane, ahlam)
.
250 2.0.0 Ok: queued as 6E2C29213F1
.
221 2.7.0 Error: I can break rules, too. Goodbye.
Connection closed by foreign host.
```

On démarre dovecot avec la commande **service dovecot start**



```
(khalid@khalid)-[~/etc]$ service dovecot start
```

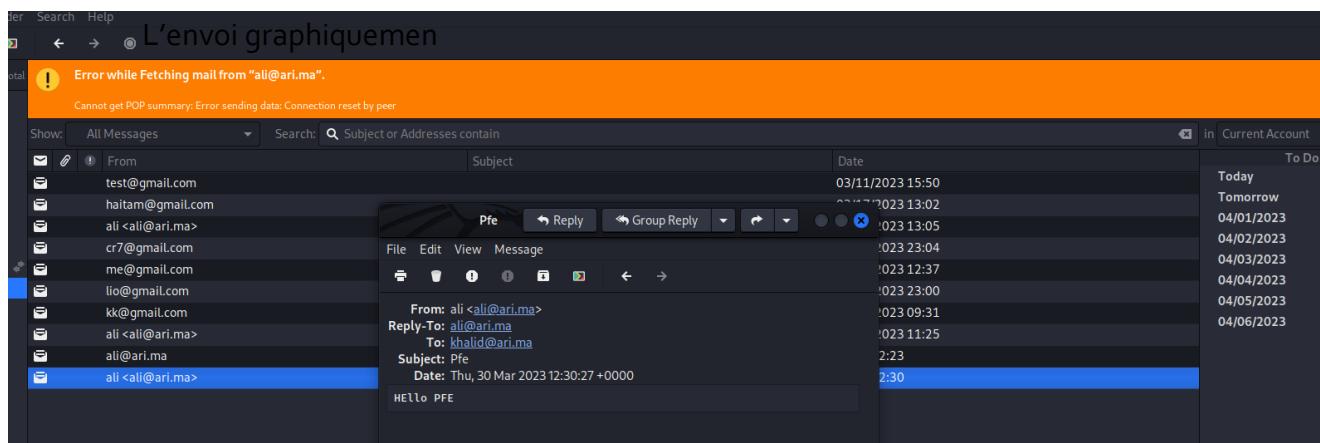
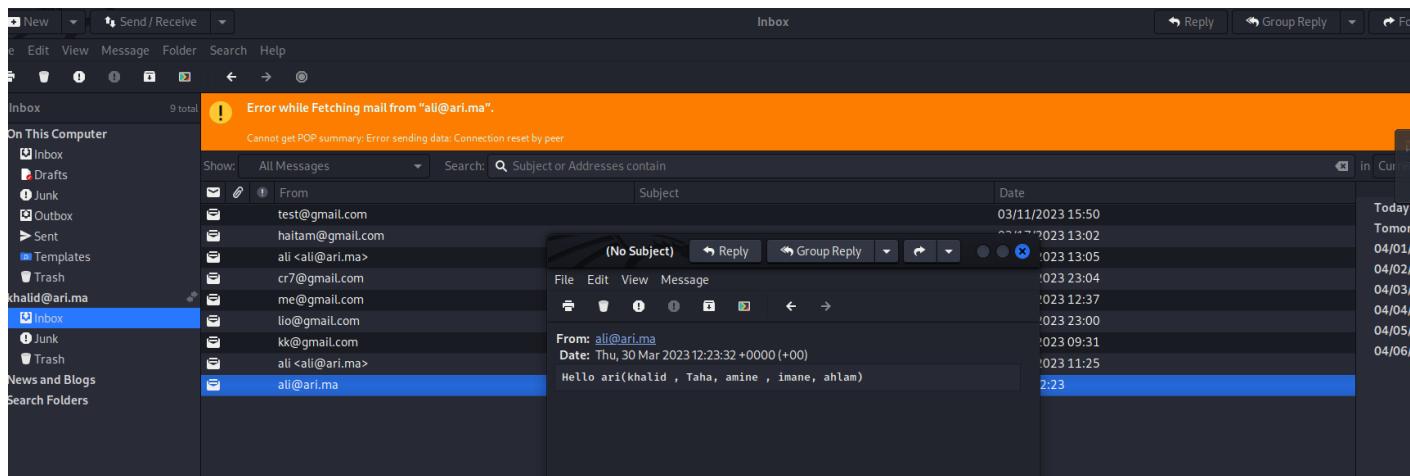
Figure 90 le fichier d'authentification du dovecot

## La reception du message envoyé

```
From ali@ari.ma Thu Mar 30 12:24:20 2023
Return-Path: <ali@ari.ma>
X-Original-To: khalid@ari.ma
Delivered-To: khalid@ari.ma
Received: from mail (khalid [192.168.1.105])
    by mail.ari.ma (Postfix) with SMTP id 6E2C29213F1
    for <khalid@ari.ma>; Thu, 30 Mar 2023 12:23:32 +0000 (+00)
Message-Id: <20230330122348.6E2C29213F1@mail.ari.ma>
Date: Thu, 30 Mar 2023 12:23:32 +0000 (+00)
From: ali@ari.ma

Hello ari(khalid , Taha, amine , imane, ahlam)
```

## La réception graphiquement



### III. Le serveur web (Apache) :

#### 1. Définition :



Un logiciel appelé serveur Web utilise le protocole HTTP (HyperText Transfer Protocol) et d'autres protocoles pour répondre aux demandes des clients sur le World Wide Web. Le rôle principal du serveur Web est d'afficher le contenu d'un site Web en stockant, traitant et livrant les pages Web aux utilisateurs qui les ont demandées.

En plus de cela, le serveur Web prend en charge le protocole SMTP (Simple Mail Transfer Protocol) pour le transfert de courrier électronique, ainsi que le protocole FTP (File Transfer Protocol) et HTTP pour le transfert de fichiers et le stockage.

#### 2. Comment fonctionne le serveur web ?

Lorsqu'un navigateur demande l'affichage d'une page Internet, celle-ci peut être renvoyée par le serveur Web en envoyant le code correspondant. Une illustration simple de ce processus est présentée ci-dessous :



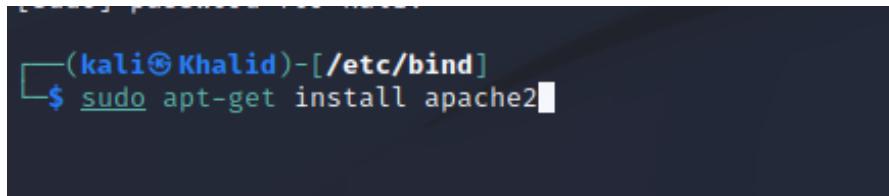
Figure 101 échange client/serveur

Ce processus se compose de 3 étapes, qui sont :

- Obtenir l'adresse IP du nom de domaine : notre navigateur Web obtient d'abord l'adresse IP à laquelle le nom de domaine est rattaché. Il peut obtenir l'adresse IP de deux manières :
  - En cherchant dans son cache.
  - En demandant à un ou plusieurs serveurs DNS (Domain Name System).
- Le navigateur demande l'URL complète : après avoir connu l'adresse IP, le navigateur demande maintenant une URL complète au serveur Web.
- Le serveur Web répond à la demande : le serveur Web répond au navigateur en envoyant les pages souhaitées. Si les pages n'existent pas ou si une autre erreur se produit, il envoie le message d'erreur approprié.

### 3. Installation et configuration du serveur web apache :

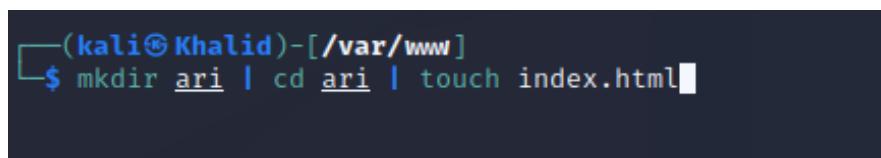
- Nous allons installer le serveur sur la même machine du serveur messagerie
- Premièrement on va exécuter la commande **sudo apt-get update** pour faire une mise à jour des paquets.
- Installation du paquet apache2.



```
(kali㉿Khalid)-[~/etc/bind]
$ sudo apt-get install apache2
```

*Figure 102 Installation Apache*

- Crédation du répertoire « ari » dans le chemin /var/www pour le site ari.ma
- Crédation d'une page index.html dans le répertoire site web en utilisant la commande **touch index.html**.



```
(kali㉿Khalid)-[~/var/www]
$ mkdir ari | cd ari | touch index.html
```

*Figure 103 création du répertoire et fichier site web*

Pour diffuser le contenu de cette page, il est obligatoire de réaliser la création d'un vhost en modifier la configuration par défaut du fichier /etc/apache2/sites-available.

```
(kali㉿Khalid)-[~/etc/apache2/sites-available]
$ touch ari.conf
```

Figure 105 modification des vHosts 1

Nous avons changé le documentroot par le répertoire qu'on déjà créer et le nom de domaine ari.ma

```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # 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) this
    # 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.ari.ma
    ServerAlias ari.ma
    ServerAdmin admin.ari.ma
    DocumentRoot /var/www/ari/

    # 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

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
"ari.conf" 29L, 1306B
```

Figure 106 modification des vHosts 2

Il est important de savoir que les vHosts ne peuvent être mis en place uniquement si un système DNS existe déjà, donc on doit configurer le Dns.

- Dans le fichier direct du dns/etc/bind/db.est.sma on va ajouter un hôte ari et qui correspond à l'adresse du serveur.
- Dans le fichier inverse (/etc/bind/db.50.168.192) on va créer un pointeur qui pointe sur le nom de domaine ari.est.sma

```
(kali㉿Khalid)-[~/etc/apache2/sites-available]
$ sudo a2ensite
sudo: unable to resolve host Khalid: No address associated with hostname
Your choices are: 000-default ari default-ssl
Which site(s) do you want to enable (wildcards ok)?
ari
Enabling site ari.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Et finalement on redémarrer les deux services apache et Dns pour voir le fonctionnement du serveur web, en utilisant les commandes :

- Sudo systemctl restart bind9
- Sudo systemctl restart apache2

On demare le service apache

```
(kali㉿Khalid)-[/etc/apache2/sites-available]
$ service apache2 start
```

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian.ari.ma.  admin.ari.ma. (
                        2           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                       2419200    ; Expire
                       604800 )    ; Negative Cache TTL
;
@       IN      NS      debian.ari.ma.
debian.ari.ma.   IN      A      192.168.50.18
server-web       IN      A      192.168.50.18
www              IN      CNAME  server-web
mail             IN      A      192.168.50.18
~
~
~
```

Voici la page d'Accueil du site web, désormais accessible par le réseau interne

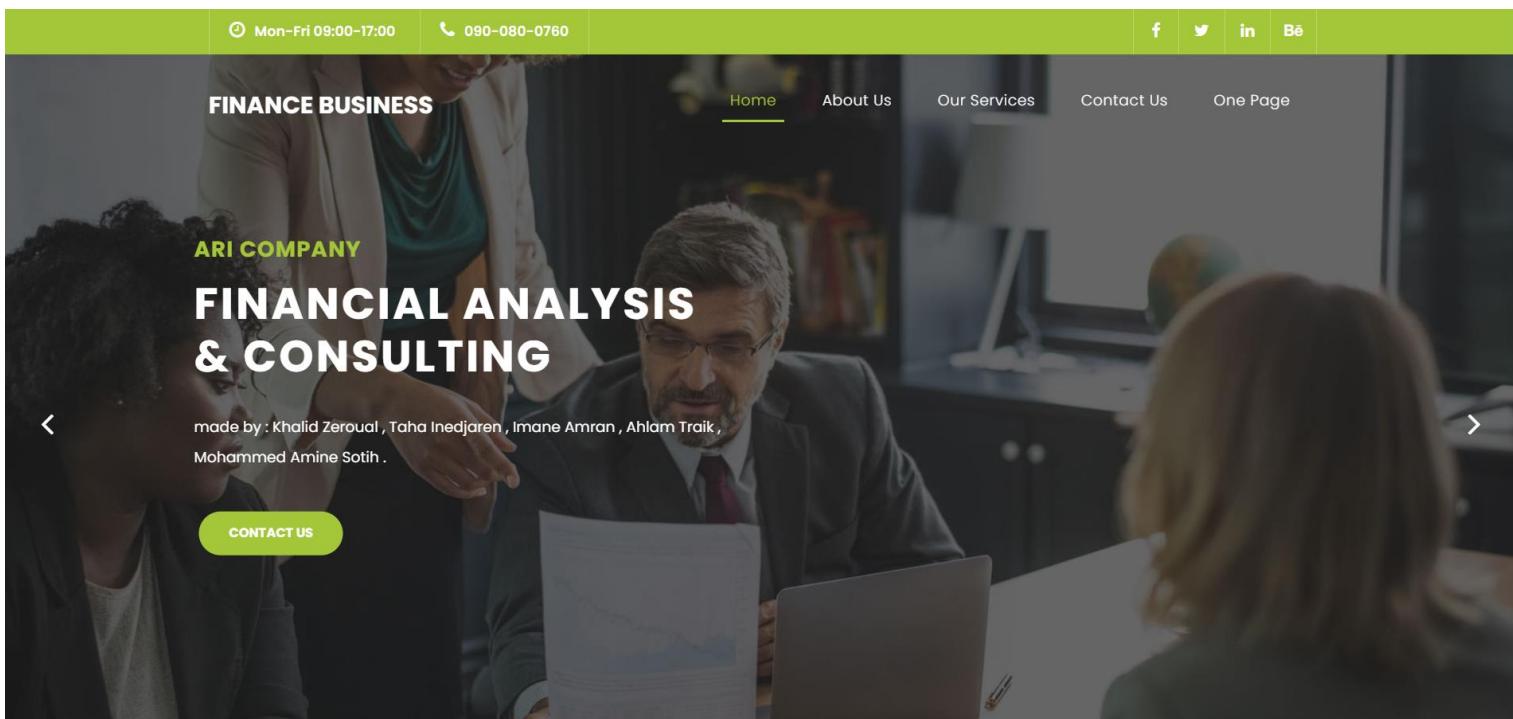


Figure 107 Page d'Accueil du site web

## Conclusion

Dans ce chapitre nous avons configuré des services qu'on peut trouver dans une zone DMZ, et qui sont : le serveur web (apache) et le serveur de messagerie SMTP, nous avons vu le fonctionnement ainsi que la configuration de ces deux serveurs.

## CONCLUSION

Pour conclure, la troisième partie à portée sur l'étude général du pare-feu qui est un élément de sécurité très important. Il permet de contrôler le trafic réseau.

Il est important pour protéger l'accès à des services réseaux tel que le serveur de messagerie et le serveur web qui se trouve dans la zone DMZ qui est une zone permettant d'échanger avec l'extérieur, sans pour autant mettre en danger notre réseau interne.

# PARTIE IV :

## la supervision et la voip

# Chapitre 1 : La supervision

Avec l'avènement de la révolution numérique, les entreprises sont contraintes de se préoccuper davantage de la performance de leur matériel informatique. La gestion de leur parc informatique devient donc d'autant plus cruciale, car elle vise à maintenir, développer et optimiser toutes les ressources informatiques de l'entreprise. En optimisant l'administration et la maintenance de ces ressources, l'entreprise peut améliorer ses performances globales et sa rentabilité.

## I. Etude de la supervision :

### 1. Définition

Le monitoring informatique, également connu sous le nom de supervision informatique, est une méthode de surveillance conçue pour permettre aux analystes de déterminer si les équipements informatiques fonctionnent conformément aux niveaux de service attendus et de résoudre les problèmes détectés. Grâce à la supervision, il est possible d'assurer un service informatique sans interruption, d'améliorer la sécurité des outils informatiques et de prolonger leur durée de vie.

### 2. Protocole Snmp

Le SNMP (Simple Network Management Protocol) est un protocole d'application simple qui facilite l'échange d'informations d'administration entre les équipements réseau. En utilisant le SNMP, le superviseur et les agents peuvent communiquer pour recueillir des objets dans la MIB. Ce protocole est disponible en plusieurs versions (v1, v2, v3), il est indépendant de la plate-forme (Linux, Unix, Windows, etc.) et du type d'équipement (serveur, switch, routeur, etc.). Le diagramme ci-dessous synthétise les différents éléments qui peuvent être identifiés avec le protocole SNMP.

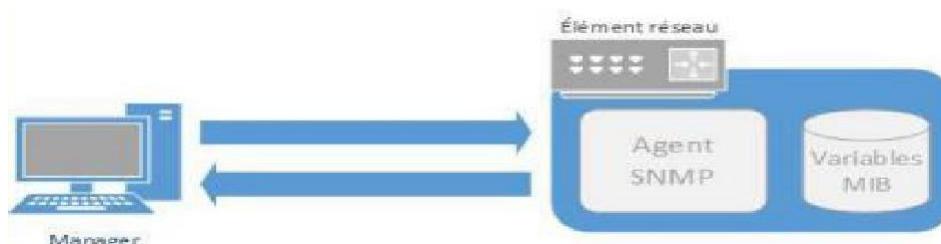


Figure 108 Fonctionnement SNMP

**Le manager** : dispose d'une fonction serveur, il reste à l'écoute sur le port UDP 162

**MIB** : (Management Information Base) est l'un des composants essentiels de la structure de SNMP. C'est une base de données (virtuelle) qui est situé sur les nœuds du réseau à surveiller (switch, routeur...) et c'est elle qui répond aux requêtes SNMP émises par le superviseur

### 3. Les requêtes SNMP

Le protocole SNMP utilise un mécanisme de base composé d'échanges requête/réponse appelé PDU (Unité de Données de Protocole). Les commandes possibles dépendent de la version du protocole SNMP utilisée. La structure des paquets utilisés par SNMP V1 est décrite dans la RFC 1157. Les requêtes SNMP contiennent une liste d'OID (Identificateur d'Objet) à collecter sur l'agent SNMP.

Les différents types de requêtes du gestionnaire SNMP vers l'agent SNMP sont ::

#### a. Pour la recherche des informations :

- Get Request : Le manager interroge un agent sur les valeurs d'un ou de plusieurs objets d'une MIB.
- Get Next Request : Le manager interroge un agent pour obtenir la valeur de l'objet suivant dans l'arbre des objets de l'agent
- Get Bulk Request : Le manager interroge un agent pour obtenir des blocs entiers de réponses de la part de l'agent.

#### b. Modification des valeurs

- Set Request : Le manager positionne ou modifie la valeur d'un objet dans l'agent
- Get Response : L'agent répond aux interrogations du manager.

#### c. Envoie d'informations

- Trap : L'équipement génère un envoi vers son manager pour signaler un événement, un changement d'état ou un défaut

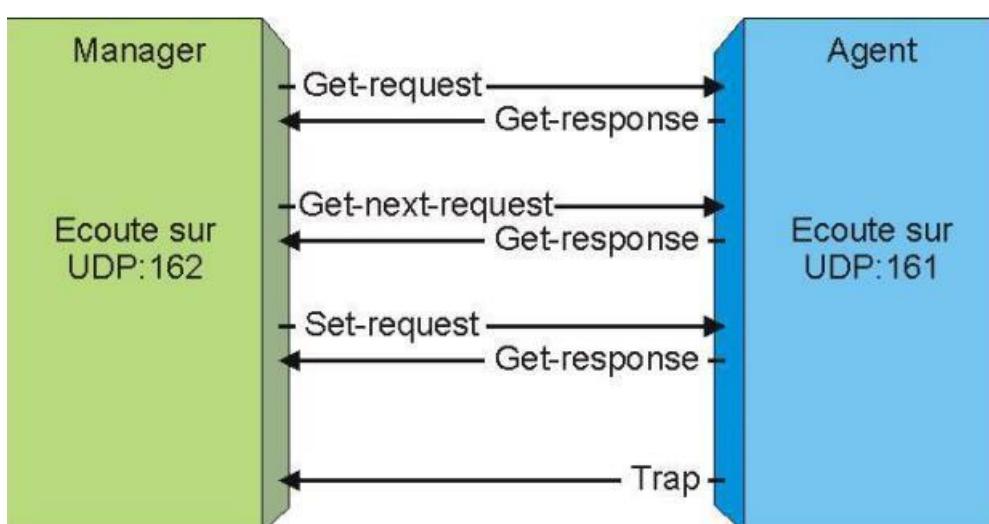


Figure 109 Requête SNMP

Le fonctionnement général de la supervision implique les étapes suivantes :

- Un système de réseau informatique est composé d'objets surveillés et contrôlés par un système d'administration.
- Chaque objet est géré localement par un processus appelé Agent qui envoie régulièrement des informations de gestion relatives à son état et aux événements qui le concernent au système d'administration.
- Le système d'administration comprend un processus appelé Manager ou Gérant qui peut accéder aux informations de gestion de la MIB locale via un protocole d'administration tel que SNMP, ce qui lui permet d'interagir avec les différents agents.

#### 4. Les modes de la supervision

Pour la supervision des machines, on utilise deux modes de contrôle: mode passif et mode actif.

##### a. Mode Passif

La méthode de supervision passive implique les actions suivantes :

- La ressource supervisée surveille son propre état et envoie les informations au serveur de supervision.
- Le serveur de supervision reçoit l'alerte et la gère en conséquence.

##### b. Mode Actif

La supervision active est une méthode qui implique les actions suivantes :

- La plateforme de supervision envoie des requêtes d'interrogation et de mesure à la ressource supervisée.
- Le serveur de supervision analyse les informations reçues et détermine l'état actuel de la ressource.
- La ressource répond à la requête du serveur de supervision. Cette méthode offre l'avantage d'être fiable car les vérifications sont effectuées de manière régulière et en mode question-réponse. Les trois étapes du processus sont donc : envoi de requête, analyse de l'information et réponse de la ressource supervisée.

#### 5. Nagios vs Zabbix

##### a. Nagios

Le logiciel Nagios a été développé en 1999 par Ethan Galstad dans le but de surveiller les réseaux, les infrastructures et les systèmes informatiques de manière continue. Il offre différentes méthodes pour superviser les composants tels que les hôtes, les ressources et les services en fonction de l'architecture de la plateforme de supervision à mettre en place..

## b. Zabbix

Zabbix est un outil de surveillance conçu pour superviser les réseaux et les systèmes tels que le processeur, le disque, la mémoire et les processus. Il propose des vues graphiques générées par RRDtool ainsi que des alertes déclenchées lors de dépassement de seuils. De plus, il permet l'installation d'un agent Zabbix sur des hôtes utilisant les systèmes Linux, UNIX et Windows.

### Nagios XI et Nagios core

L'utilisation de Nagios Core pour superviser l'infrastructure d'une organisation exige des compétences techniques avancées pour la mise en place, la configuration et la gestion des tâches de surveillance quotidiennes. En revanche, Nagios XI fournit une interface utilisateur conviviale qui élimine le besoin pour les utilisateurs de maîtriser le code de ligne de commande.

## II. Nagios XI

### 1. Installation et implémentation de Nagios

Démarrage de l'installation :

#### Installation ncpa

#### Accès à l'accueil

Avec le username « **nagiosadmin** » et le mot de passe « **Admin@123** »

## Nagios XI Installation

Finalize your Nagios XI installation and step the initial configuration. These settings can be changed later.

### Admin Account Settings

Username	<input type="text" value="nagiosadmin"/>
Password	<input type="password" value="Admin@123"/>
Full Name	<input type="text" value="Administrator"/>
Email Address	<input type="text" value="admin@grp3.local"/>

### Admin Notification Settings

<input checked="" type="checkbox"/> Send this account email notifications <small>?</small>	<a href="#">Advanced email notification settings</a>
--	--

[◀ Back](#)

[✓ Finish Install](#)

## Nagios XI Installation

Finalize your Nagios XI installation and step the initial configuration. These settings can be changed later.

### General System Settings

Program URL	<input type="text" value="http://192.168.30.10/nagiosxi/"/>	<small>?</small>
Timezone	<input type="text" value="(UTC+00:00) Casablanca"/>	<small>▼</small>
Language	<input type="text" value="French (Français)"/>	<small>▼</small>
User Interface Theme	<input type="text" value="Modern"/>	<small>▼</small>
<input type="checkbox"/> Use HTTPS only (all HTTP requests will be redirected to HTTPS) <small>?</small>		

### License Settings

License Type	<input type="radio"/> Trial	<input type="radio"/> Licensed	<input checked="" type="radio"/> Free (Limited)
Free license is limited to 7 nodes and up to a total of 100 host/service checks. This option is self-supported only.			

**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](http://library.nagios.com).

Problems, comments, etc, should be directed to our support forum at [support.nagios.com/forum/](http://support.nagios.com/forum/).

- Après l'importation de l'ova de Nagios XI sur l'EXI l'étape suivante est de se connecter.
- Tapez "root" et "nagiosxi" pour se connecter



Figure 110 NagiosXi

Après l'authentification, on va utiliser nmtui, qui est un utilitaire graphique en ligne de commande qui permet de configurer facilement les interfaces réseau dans les distributions Linux



Figure 111 modification de la connexion

- On attribue une adresse statique à l'interface qu'on veut utiliser pour la configuration

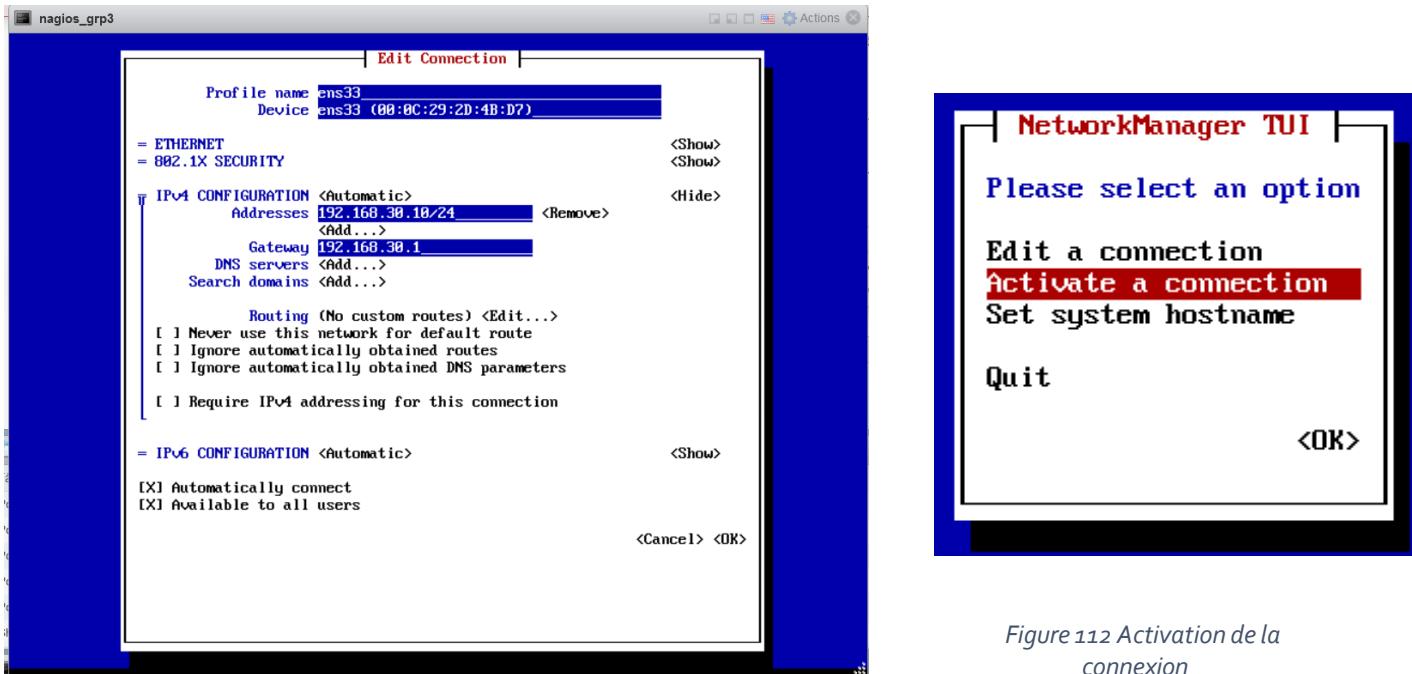
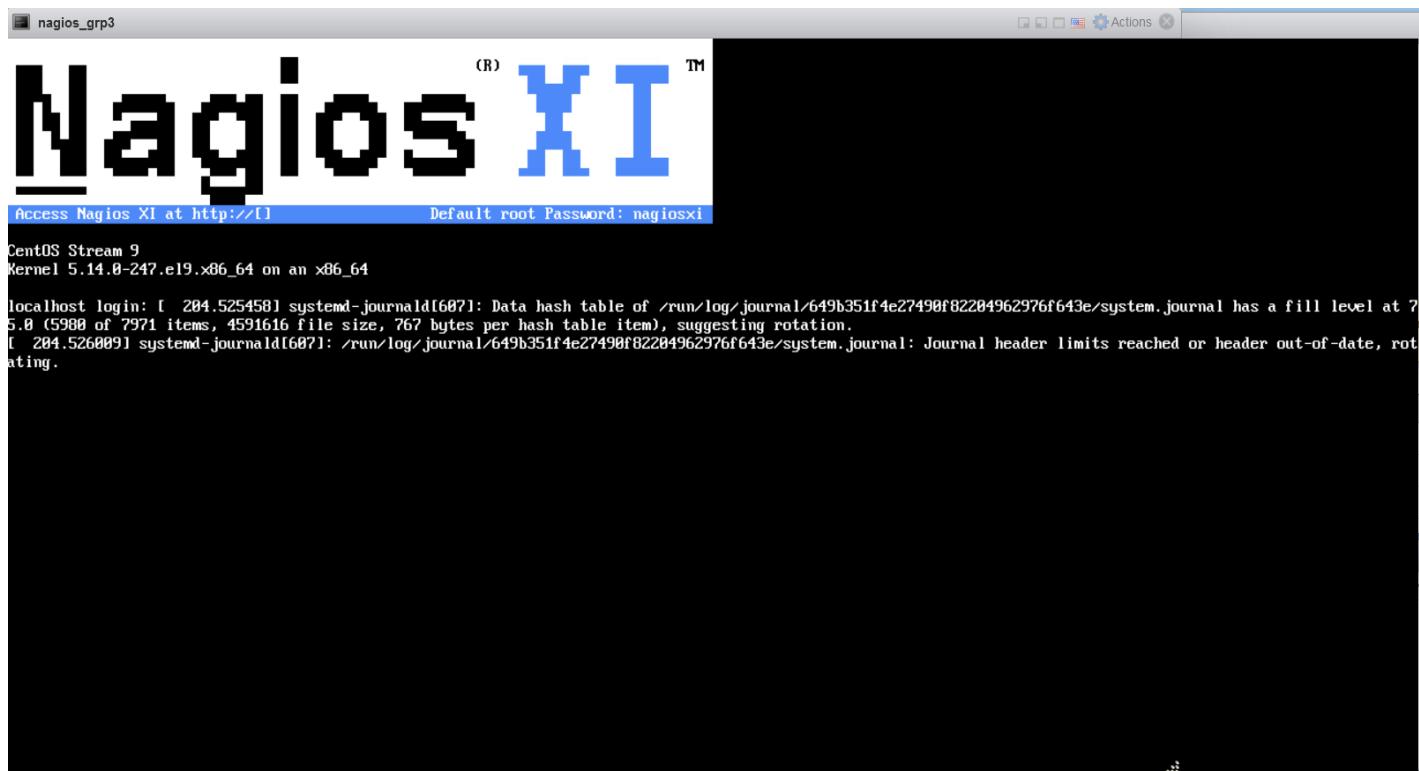


Figure 112 Activation de la connexion

Figure 113 Modification de l'adresse



## 2. Supervision du Pare-feu

- On accède à la page SNMP du pare-feu

The screenshot shows the Nagios XI configuration interface. The top navigation bar includes links for Maison, Vues, Tableaux de bord, Rapports, Configurer, Outils, Aider, and Admin. A banner at the top says "mise à niveau vers une version sous licence de nagios xi et obtenir le soutien et la mise à niveau des prestations." The left sidebar has a tree view with sections like Configurer, Accueil de configuration, déploiement automatique, Configuration avancée, and Plus d'options. The main content area is titled "Assistants de configuration: SNMP - étape 1". It has a sub-section "Des informations SNMP" with a field "Adresse de l'appareil:" containing "192.168.30.1". Below it is a note: "L'adresse IP ou le nom DNS complet du serveur ou du périphérique que vous souhaitez surveiller." Navigation buttons "Arrière" and "Suivant >" are at the bottom.

Figure 114 Page SNMP pare-feu

- On active SNMP sur le pare-feu et on donne l'adresse de l'interface du parefeu qu'on a réservé pour la supervision et l'adresse de Nagios.

The screenshot shows the second step of the SNMP configuration wizard. The top navigation bar and sidebar are identical to the previous screenshot. The main content area is titled "Assistants de configuration: SNMP - étape 2". It has a section "Détails sur l'appareil" with fields for "Adresse de l'appareil:" (192.168.30.1) and "Nom de l'hôte:" (Router). Below it is a note: "Le nom que vous aimeriez avoir associé à ce serveur ou le périphérique." There is also a section "Paramètres SNMP" with "Version SNMP:" set to "2c" and "Port HTTP:" set to "161". A note below says: "le port snmp à utiliser, le port par défaut est le port 161." At the bottom is a section "snmp paramètres de version" with a field "Communauté SNMP:" containing "public". A note below says: "La chaîne de communauté SNMP utilisée pour interroger le dispositif."

Figure 115 Activation SNMP pare-feu

## Mise en place d'une Infrastructure réseau pour une entreprise

**Services SNMP**

Spécifiez les OID que vous souhaitez contrôler via SNMP. Des exemples d'entrées ont été fournis à titre d'exemples.

OID	Afficher le nom	Étiquette de données	Data Units (Option)	Type de correspondance	Avertissement Gamme	Critical Gamme	Chaine Pour correspondre	MB utiliser
<input checked="" type="checkbox"/> sysUpTime.0	Uptime			Aucun				
<input checked="" type="checkbox"/> ifOperStatus.1	Port 1 Status			Chaîne			1	RFC1213-MIB
<input type="checkbox"/> 1.3.6.1.4.1.2.3.51.1.2.1.5.	IBM RSA II Adapter Temper:	Ambient Temp	C	Numérique	29	35		
<input type="checkbox"/> 1.3.6.1.4.1.3076.2.1.2.17.1	Cisco VPN Sessions	Active Sessions		Numérique	:70,:8	:70,:10		
<input type="checkbox"/>				Aucun				
<input type="checkbox"/>				Aucun				

Add Row | Delete Row

[Arrière](#) [Suivant >](#)

- Ajout d'un appareil SNMP dans la page de configuration Nagios, On saisit l'adresse qu'on a attribuée au port du pare-feu et on choisit les ports dont on veut superviser le statut.

**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: SNMP - étape 3**

Paramètres de surveillance des

Définir les paramètres de base qui déterminent la façon dont l'hôte et de service (s) doivent être surveillés.

Dans des circonstances normales:

Surveiller l'hôte et de service (s) à chaque  minutes.

Lorsqu'un problème potentiel est détecté pour la première:

Vérifiez à nouveau l'hôte et de service (s) à chaque  minutes jusqu'à  fois avant d'envoyer une notification.

[Arrière](#) [Suivant >](#) [Terminer](#)

**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.

**SNMP Assistant de surveillance**

Configuration appliquée avec succès

Vos modifications de configuration ont été appliquées avec succès à la surveillance du moteur.

Demande Configuration réussie

Exécuter cet Assistant à nouveau suivri  Exécuter un autre assistant de surveillance

Autres Options:

- Voir détails sur l'état de Router
- Voir les photos récentes de configuration

[Arrière](#) [Suivant >](#) [Terminer](#)

**Détail de l'état d'accueil**

**SNMP Router**

OK - 192.168.30.1 rta 0.381ms lost 0%

Adresse: 192.168.30.1

**Détails sur l'état**

État hôte:	Jusqu'à
Durée:	1m 5s
Stabilité d'accueil:	Immuable (stable)
Dernière vérification:	2023-04-01 10:00:30
Vérifier Suivant:	2023-04-01 10:05:30

**Actions rapides**

- Désactiver les notifications
- forcer une vérification immédiate
- Ping this host
- Connect to Router
- Traceroute to this host

**divers**

pas de notes ou infos diverses

**Remerciements et commentaires**

Pas de commentaires ou remerciements.

**Détail de l'état d'accueil**

**SNMP Router**

**Détails Statut avancé**

État hôte:	Jusqu'à
Durée:	1m 48s
Type d'état:	Dur
Vérifier actuelle:	1 of 5
Dernière vérification:	2023-04-01 10:01:25
Vérifier Suivant:	2023-04-01 10:06:25
Dernier changement d'état:	2023-04-01 10:00:03
Dernière notification:	Never
Vérifier type:	Actif
Vérifier la latence:	0.005034999921917915 seconde
Temps d'exécution:	0.006281 seconde
Changement d'état:	0%
Les données de performance:	rta=0.386ms;3000.000;5000.000;0;pl=0%;80;100;0;100 rtmx=0.511ms;;;;rtmin=0.349ms;;;;

**Attributs d'accueil**

Attribut	État	Action
Les contrôles actifs	●	✗
Les contrôles passifs	●	✗
Notifications	●	✗
Détection rabat	●	✗
Event Handler	●	✗
Les données de performance	●	✗
Obsession	●	✗

**Commandes**

- ajouter un commentaire
- Programmer les temps d'arrêt
- Programmer les temps d'arrêt de tous les services de cet hôte
- vérification immédiate forcée pour l'hôte et tous les services
- Soumettre résultat du contrôle passif
- Envoyer une notification personnalisée
- Retarder la notification suivante

**Plus d'options**

- vue dans le noyau nagios



Au cours de chapitre concernant la supervision, nous avons implémenté dans notre architecture Nagios, un logiciel open source de supervision qui, grâce au protocole SNMP, nous a permis de faire le suivi des appareils et machines du réseau.

## Chapitre2 : La Voip

La technologie émergente de télécommunication vocale appelée Voix sur IP est en train de révolutionner le monde de la téléphonie. Elle permet la transmission de la voix sur un réseau numérique et via Internet, marquant ainsi un tournant dans le monde des communications.

Dans notre réseau, nous avons choisi d'utiliser la Voix sur IP principalement pour faciliter la communication entre les employés.

## I. Etude de la Voip :

### 1. Définition :

La technologie de la Voix sur Protocole Internet, également connue sous le nom de VoIP (Voice Over Internet Protocol), est utilisée pour offrir des fonctions de téléphonie Internet similaires à celles des lignes téléphoniques classiques. Elle repose principalement sur un ensemble de protocoles qui fonctionnent simultanément.

En revanche, le Réseau Téléphonique Commuté (RTC) est basé sur une infrastructure qui permet de connecter les abonnés du système téléphonique à leur commutateur local, qui est à son tour connecté à un commutateur régional, national et international.

### 2. Norme de la VOIP :

#### a. Terminologie

**Le protocole SIP** (Session Initiation Protocol) a été développé par le groupe de travail IETF MMUSIC et est proposé comme standard pour initier, modifier et terminer une session utilisateur interactive.

**Le protocole H.323** permet l'activation, la modification et la terminaison d'une session média, mais il s'agit d'un protocole assez ancien qui est actuellement remplacé par SIP.

**Le protocole RTP** (Real-time Transport Protocol) est utilisé pour transporter des flux multimédias tels que l'audio et la vidéo.

**Le protocole RTCP** (Real-time Transport Control Protocol) est utilisé pour surveiller les statistiques de transmission en envoyant périodiquement des paquets de contrôle à tous les participants d'une session.

L'utilisation conjointe de RTP et de RTCP permet d'assurer une cohérence dans le traitement de l'information en fournissant un contrôle dans la partie applicative.

#### b. Fonctionnement

Le processus de transmission de la voix en utilisant la technologie VoIP implique plusieurs étapes clés. Tout d'abord, la voix est convertie en signal numérique à l'aide d'un Convertisseur Analogique/Numérique. Ce signal est alors compressé sous forme de bits, conformément à un protocole de compression adapté à la transmission. Il existe de nombreux protocoles différents, mais le SIP est le plus couramment utilisé pour la VoIP. Les paquets audio résultants sont à leur tour compressés en paquets de données à l'aide d'un protocole temps réel, généralement RTP sur UDP sur IP. Un protocole de signalisation, comme UIT-T H323, est ensuite utilisé pour appeler les utilisateurs et établir une connexion. Enfin, une fois que les paquets sont arrivés à destination, ils sont décompressés et les signaux vocaux analogiques convertis sont envoyés à la carte son pour être reproduits.

### c. Avantages et inconvénients

Voici un tableau récapitulatif des avantages et des inconvénients de la technologie VoIP :

Avantages	Inconvénients
Coût inférieur à celui des appels téléphoniques traditionnels	La qualité des appels peut être affectée par une connexion Internet faible ou instable
Facilité d'utilisation et de mise en place	Vulnérabilité aux attaques de sécurité, comme l'usurpation d'identité et les attaques par déni de service (DDoS)
Flexibilité et portabilité, car les appels peuvent être passés à partir de n'importe où avec une connexion Internet	Nécessité d'une alimentation électrique et d'une connexion Internet pour faire fonctionner le service
Fonctionnalités avancées, telles que la messagerie vocale, la conférence téléphonique et la redirection d'appel	Le service peut être affecté en cas de panne de courant ou de coupure Internet

Tableau 11

#### *Avantages et inconvénients Voip*

### 3. Elastix :

Elastix, un logiciel IPBX, a été développé en se basant sur Asterisk, un logiciel libre. Grâce à son interface web dédiée, il offre une gestion améliorée du système de téléphonie, et son installation est simple et fluide. De nombreuses entreprises l'utilisent car il répond souvent aux contraintes de téléphonie IP des entreprises. Le système d'exploitation de base est CentOS, et l'administration d'Elastix se fait entièrement via l'interface web, permettant une vue d'ensemble de l'infrastructure. Depuis 2016, Elastix est basé sur le logiciel 3CX.

#### a. Définition

Elastix est un logiciel libre et open-source de gestion de téléphonie. Il offre des fonctionnalités avancées de communication téléphonique telles que la gestion des appels, la conférence téléphonique, la messagerie vocale, la musique d'attente, l'enregistrement des appels, etc. Elastix est facile à installer et à utiliser grâce à son interface web intuitive. Il est souvent utilisé par les entreprises pour la gestion de leur système de téléphonie, car il est flexible et permet une personnalisation avancée en fonction des besoins spécifiques de l'entreprise.

#### b. Installation

Lorsque Elastix est lancé à partir de notre serveur, le mode graphique peut être sélectionné en appuyant sur la touche « Entrée ».

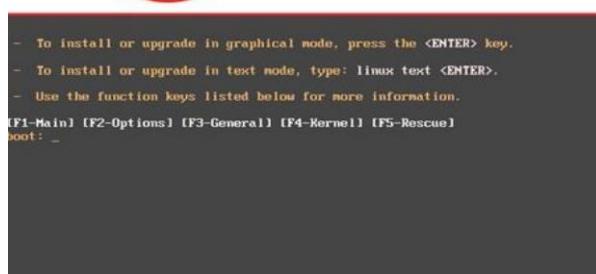


Figure 132 Installation Elastix

Après avoir suivi plusieurs étapes, nous sommes maintenant invités à configurer l'interface réseau de notre serveur. Nous allons utiliser l'adressage IPv4, donc c'est celui que nous allons activer.

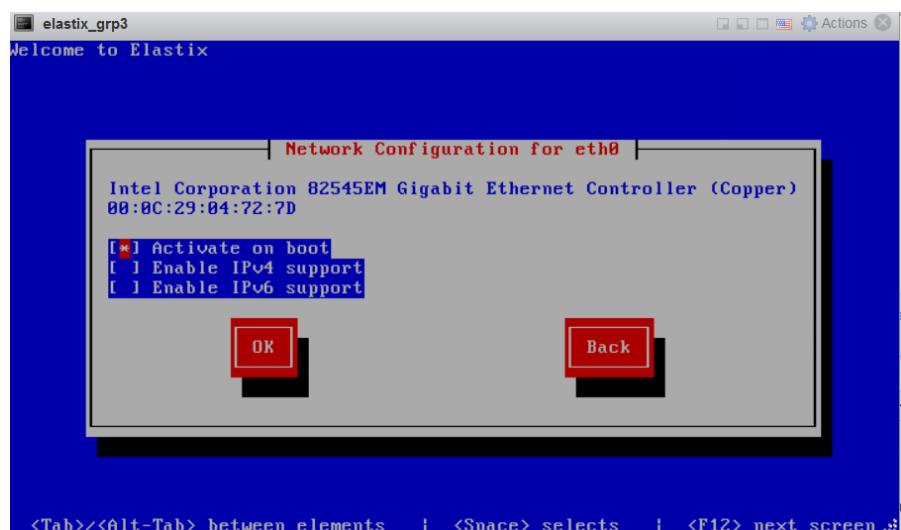


Figure activation support ipv4

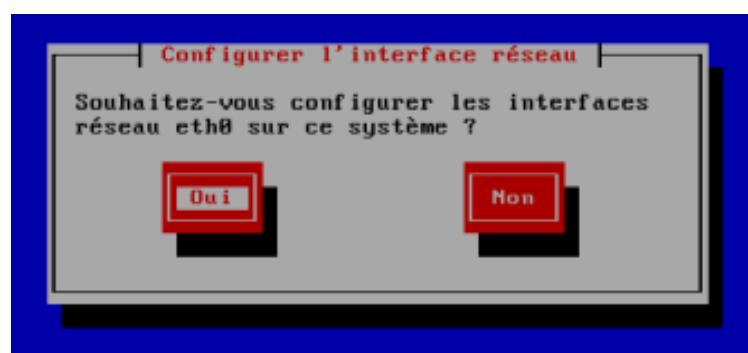


Figure Configuration des interfaces

- Nous allons assigner manuellement une adresse IP et son masque à notre serveur : l'adresse est « 192.168.20.254 » et le masque est « 255.255.255.0 ». Cette adresse appartient au VLAN des employés . Ensuite, il faut spécifier l'adresse de la passerelle.

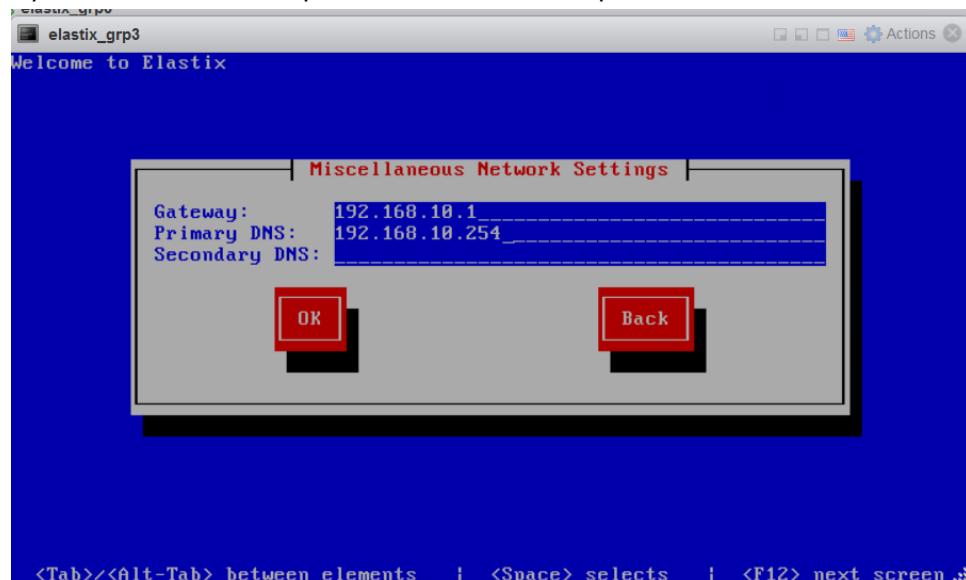


Figure Adresse de la passe

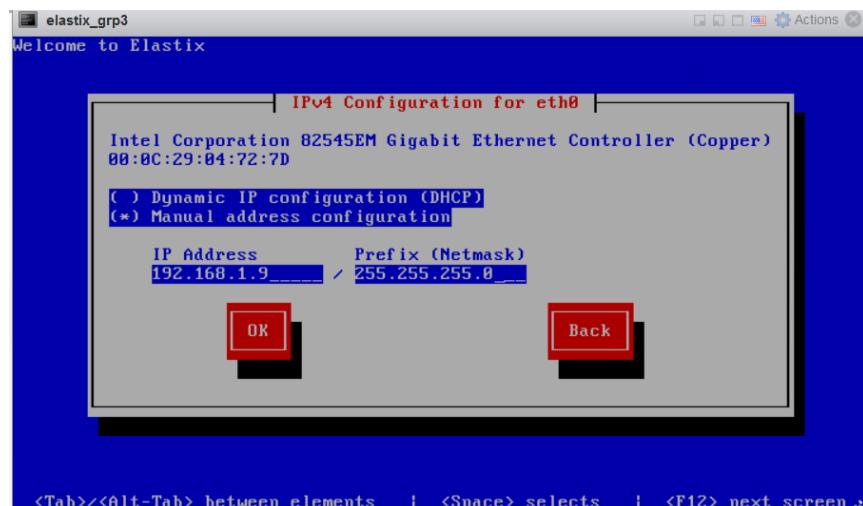


Figure 136 Attribution d'une adresse fixe

Pour terminer l'installation, il est nécessaire d'insérer et de confirmer le mot de passe que vous utiliserez pour le compte root de la base de données MySQL.

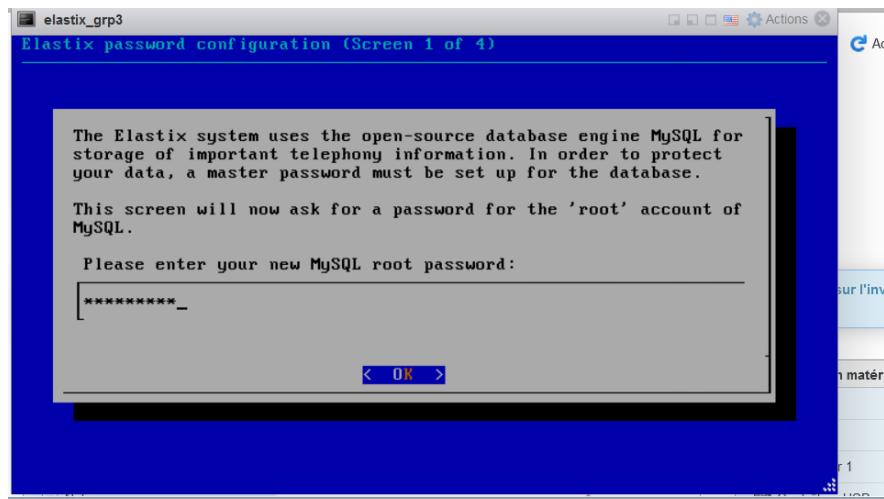


Figure 137 Attribution mot de passe MySQL

- Après cela, vous devez insérer le mot de passe du compte administrateur afin de vous connecter au serveur.



Figure 138 Attribution mot de passe Serveur

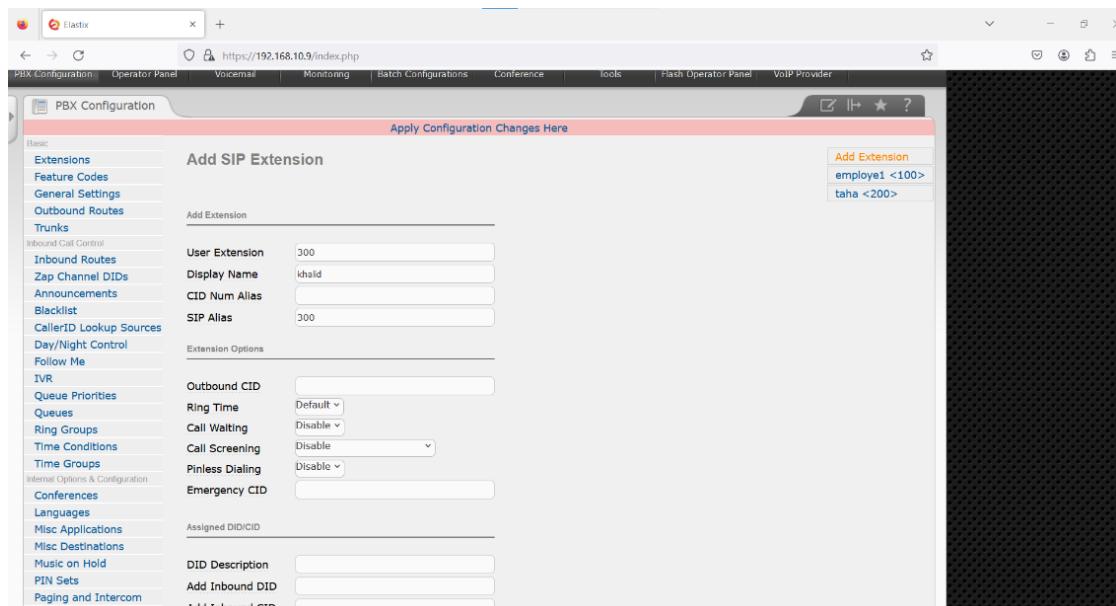
### c. Configuration Elastix



Figure 139 Interface web Elastix

Une fois que l'authentification est effectuée, il sera nécessaire d'ajouter des numéros SIP pour les attribuer à des employés. Pour cela, vous devrez accéder à la rubrique "PBX" de l'interface et sélectionner l'option "périphérique SIP".

Nous procédons à l'ajout d'un nouvel utilisateur nommé khalid avec une extension téléphonique de 200



➤ Figure Ajout périphérique

- Apres l'authentification on va ajouter des numéros SIP qu'on va attribuer à des employés, pour cela il faut accéder à la rubrique « PBX » de l'interface et choisir l'option « périphérique SIP ».

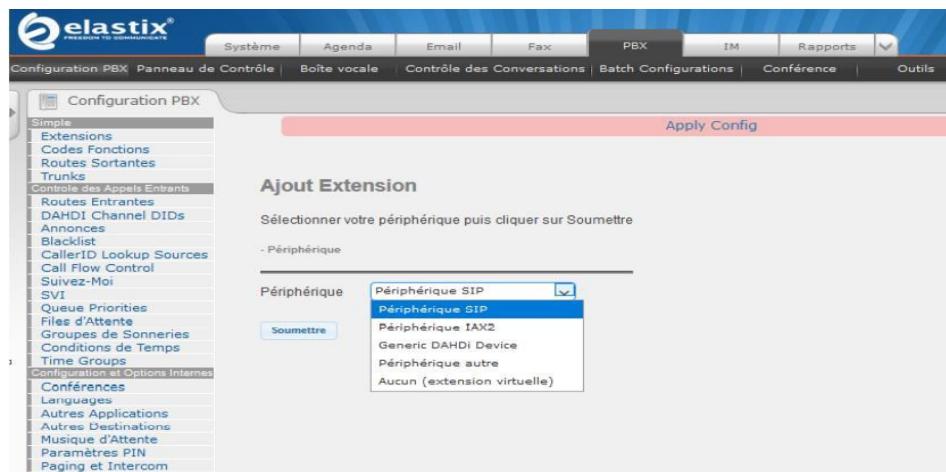


Figure 140 Ajout périphérique

- On ajoute un utilisateur PosteAri3 avec une extension 444

Outbound Routes	Add Extension
Trunks	User Extension <input type="text" value="444"/>
Inbound Call Control	Display Name <input type="text" value="PosteAri3"/>
Inbound Routes	CID Num Alias <input type="text"/>
Zap Channel DIDs	SIP Alias <input type="text"/>
Announcements	Extension Options
Blacklist	Outbound CID <input type="text"/>
CallerID Lookup Sources	Ring Time <input type="button" value="Default"/>
Day/Night Control	Call Waiting <input type="button" value="Disable"/>
Follow Me	Call Screening <input type="button" value="Disable"/>
IVR	Pinless Dialing <input type="button" value="Disable"/>
Queue Priorities	Emergency CID <input type="text"/>
Queues	Assigned DID/CID
Ring Groups	DID Description <input type="text"/>
Time Conditions	Add Inbound DID <input type="text"/>
Time Groups	Add Inbound CID <input type="text"/>
Internal Options & Configuration	Device Options
Conferences	This device uses sip technology.
Languages	secret <input type="text" value="ari2022"/>
Misc Applications	dtmfmode <input type="text" value="rfc2833"/>
Misc Destinations	
Music on Hold	
PIN Sets	
Paging and Intercom	
Parking Lot	
System Recordings	
VoiceMail Blasting	
Remote Access	
Callback	
DISA	
Option	
Unembedded freePBX	

Figure 141 configuration du périphérique

- De la même façon on peut ajouter plusieurs utilisateurs

#### d. Configuration des Clients SIP :

Nous allons installer des clients SIP. Nous avons choisi 3cxPhone pour deux postes de travail qui appartiennent au réseau des employés. Il faut ajouter sur chacun d'eux le compte auquel on souhaite l'affecter en cliquant sur "new".

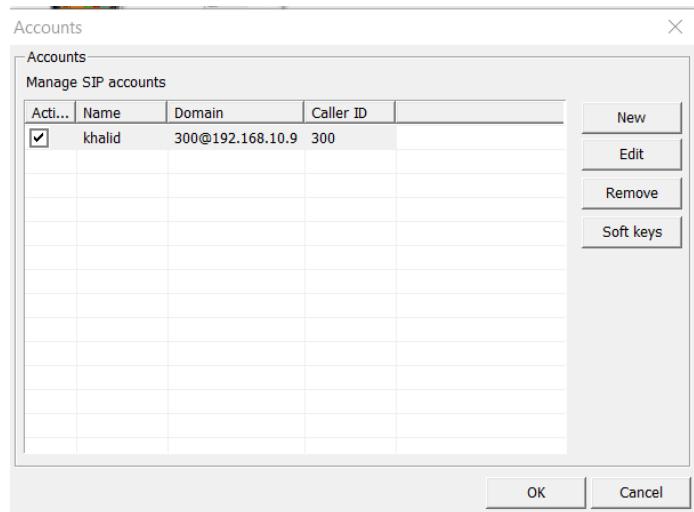


Figure 142 Configuration d'un utilisateur

- Le premier client SIP "khalid" est configuré sur 3cxPhone en saisissant son nom, son extension, son mot de passe et l'adresse du serveur Elastix. Une fois la configuration terminée, on constate que le téléphone est connecté en mode "on Hook".

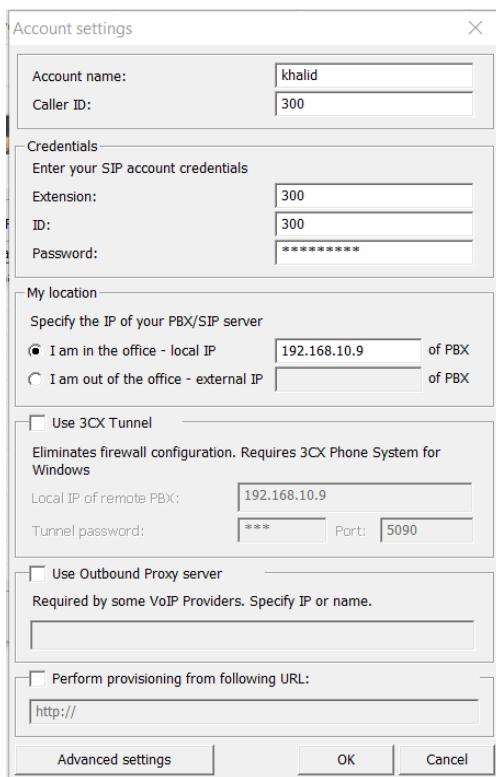


Figure 144 Configuration d'un client



Figure 143 Téléphone 3CX

On appliquera les mêmes étapes pour le deuxième poste. Dans l'onglet « Panneau opérateur » de l'interface Web du serveur Elastix, lors de l'ajout des deux comptes, on peut vérifier les clients SIP connectés en vérifiant que leur case est allumée en orange foncé.

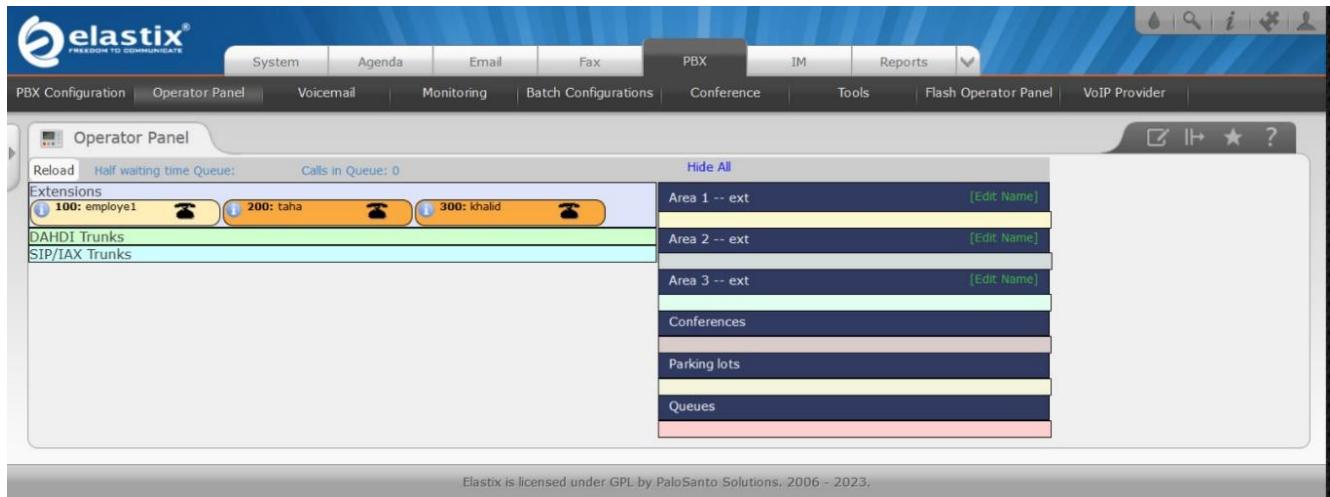


Figure Vérification des utilisateurs

### Test de communication

Nous allons tenter de mettre en place un appel entre deux postes ou clients SIP. Tout d'abord, nous composerons l'extension "300" sur le softphone de "khalid", qui correspond au numéro de "taha". Après avoir composé ce numéro, nous remarquons que le téléphone du client "kalid" se met à sonner et affiche le nom de l'appelant, à savoir "taha", ainsi que son extension et son numéro, qui est "200".



Figure Appel taha



Figure 147 Réception de l'appel de khalid

## Conclusion

La VoIP a été présentée tout au long de ce chapitre comme la solution la plus économique pour les communications. À l'heure actuelle, il est indéniable que la VoIP est un domaine en pleine expansion. La téléphonie IP est une option intéressante car elle offre une intégration facile, une grande fiabilité et des coûts réduits.

# CONCLUSION GÉNÉRALE

Au cours de notre projet de fin d'études, nous avons travaillé sur la mise en place d'une infrastructure réseau sécurisée pour permettre aux utilisateurs internes de l'entreprise (employés, Admin et invités) de se connecter en toute sécurité.

Notre principal objectif était de garantir la sécurité informatique, et pour cela, nous avons commencé par mettre en place le protocole Radius pour l'authentification des employés et le protocole LDAP pour la gestion des utilisateurs.

Nous avons ensuite mis en place un portail captif sous PfSense pour contrôler l'accès des invités au réseau.

Nous avons également déployé un serveur web et un serveur de messagerie dans la DMZ, tandis que le logiciel Nagios nous a permis de superviser les serveurs, les services et le matériel pour détecter toute panne matérielle ou logicielle et nous alerter en cas de problème.

Enfin, nous avons mis en place un système de téléphonie VoIP pour permettre une communication efficace entre les admin.

# TABLE DES MATIERES

REMERCIEMENTS .....	
SOMMAIRE.....	
LISTE DES ABRÉVIATIONS.....	
INTRODUCTION GENERALE .....	
CAHIER DE CHARGES.....	
GESTION DE PROJET .....	
1. Tableau des taches : .....	
2. Gantt .....	
PARTIE I .....	1
Infrastructure Réseau et Virtualisation .....	1
CHAPITRE 1 : Infrastructure Réseau .....	3
III. Architecture Proposée .....	4
1. Schéma de l'architecture globale de notre réseau.....	4
2. Tableaux d'adressages .....	4
IV. Etude et Configuration Matérielle.....	6
1. Le switch .....	6
2. Le routeur (Cisco 1900).....	8
3. Routeur sans fil (Linksys WRT54G).....	9
4. Routeur Linksys wireless-N .....	10
5. Pare-feu (Firewall).....	11
CHAPITRE 2 : La virtualisation.....	13
III. Etude de la virtualisation.....	14
1. Définition .....	14
2. Terminologie.....	14
3. Pourquoi Virtualiser ? .....	14
4. L'Hyperviseur .....	15
5. Types d'hyperviseur .....	16
6. Virtualisation des serveurs .....	16

7. VMWARE VSphere .....	18
IV. La virtualisation dans VMware ESXI.....	18
1. Création d'un switch virtuel et des VLANs.....	18
2. Choix du système d'exploitation des serveurs .....	21
3. Création des machine virtuelles .....	22
CONCLUSION .....	25
PARTIE II .....	26
Les Méthodes d'Authentification.....	26
CHAPITRE 1 : Authentification des employés .....	29
IV. Le protocole RADIUS.....	30
1. Définition .....	30
2. Principe .....	30
3. Fonctionnement.....	31
V. Les services réseaux.....	32
1. Le service DNS .....	32
2. Le protocole DHCP.....	34
3. Le protocole LDAP .....	35
4. Le protocole 802.1x.....	36
VI. Implémentation d'un serveur RADIUS.....	38
a. Attribution d'une adresse fixe à l'interface de la machine.....	39
b. Configuration du serveur DHCP .....	41
c. Configuration du serveur DNS.....	46
d. Configuration de RADIUS.....	49
e. Configuration du Point d'Access.....	52
CHAPITRE 2 : Authentification des invités.....	55
III. Le Portail Captif.....	56
1. Définition .....	56
2. Fonctionnement.....	56
IV. PfSense.....	57
1. Définition .....	57
2. Installation PfSense.....	58
3. Interface web pfSense.....	59

4. DHCP et DNS .....	60
5. Pare-feu .....	61
6. Portail Captif .....	62
7. Création d'un groupe et des utilisateurs .....	64
8. Test d'authentification .....	65
PARTIE III .....	67
Pare-feu et zone DMZ .....	67
CHAPITRE 1 : Le Pare-feu.....	68
III. Le firewall .....	69
1. Définition .....	69
2. Fonctionnement.....	69
3. Types de pares-feux.....	70
IV. Configuration.....	70
1. Configuration des interfaces .....	70
CHAPITRE 2 : La zone DMZ.....	76
IV. La zone DMZ.....	77
1. Définition.....	77
2. Architecture.....	77
V. Le serveur de messagerie .....	79
1. Définition .....	79
2. Les types des serveurs de messagerie.....	79
4. La différence entre IMAP et POP3 .....	81
5. Le fonctionnement du serveur de messagerie .....	82
6. Installation et configuration du serveur de messagerie .....	83
VI. Le serveur web (Apache).....	89
1. Définition .....	89
2. Comment fonctionne le serveur web ? .....	89
3. Installation et configuration du serveur web apache .....	90
CONCLUSION.....	94
PARTIE IV.....	95
Supervision et Voip.....	95
CHAPITRE 1 : La supervision .....	96
III. Etude de la supervision .....	97
1. Définition .....	97

2. Protocole Snmp .....	97
3. Les requêtes SNMP .....	98
4. Les modes de la supervision .....	99
5. Nagios vs Zabbix .....	99
6. Comparaison .....	100
IV. Nagios XI .....	100
1. Installation et implémentation de Nagios .....	100
2. Supervision du Pare-feu .....	104
CHAPITRE 2 : La Voip.....	109
II. Etude de la Voip.....	110
1. Définition .....	110
2. Norme de la VOIP.....	110
3. Elastix.....	111
CONCLUSION GÉNÉRALE .....	122
TABLE DES MATIERES .....	123

Figure 1 Architecture globale	4
Figure 2 switch Cisco Catalyst 3750	6
Figure 3 routeur Cisco 1900	8
Figure 4 Routeur sans fil (Linksys WRT54G)	9
Figure 5 Modem routeur ADSL2 (TD-W8960N)	10
Figure 6 pare-feu FortiGate-60D	11
Figure 7 schéma de fonctionnement d'un hyperviseur	15
Figure 8 Page d'authentification VMware ESXi	17
Figure 9 Ajout d'un switch virtuel	17
Figure 10 Ajout d'un groupe de ports VLAN 10	17
Figure 11 Les groupes de ports du switch virtuel	18
Figure 12 Ajout d'une machine virtuelle	19
Figure 13 Configuration matérielle de la machine virtuelle	19
Figure 14 Choix de la langue	20
Figure 15 Configuration des interfaces	20
Figure 16 Création du profil de l'utilisateur	20
Figure 17 Gestion du disque de stockage	20
Figure 18 Principe de RADIUS	25
Figure 19 Diagramme de séquence de fonctionnement RADIUS	26
Figure 20 Hiérarchie DNS	27
Figure 21 diagramme séquence DHCP	29
Figure 22 Configuration de l'interface de la MV	30
Figure 23 installation d'isc dhcp server	31
Figure 24 Spécification de l'interface DHCP	31
Figure 25 Configuration du DHCP	32
Figure 26 Installation de Bind9	32
Figure 27 Configuration des fichiers de zones DNS	33
Figure 28 Configuration de la zone directe	33
Figure 29 Configuration de la zone inverse	33
Figure 30 Autorisation du Traffic vers le port 53	34
Figure 31 Installation de freeRADIUS	34
Figure 32 : Ajout du client RADIUS	34
Figure 33 Ajout du utilisateurs RADIUS	35
Figure 34 Autorisation du Traffic vers le port 1812	35
Figure 35 Activation des logs	35
Figure 36 Changement du SSID	36
Figure 37 Configuration du Point d'Access	36
Figure 38 Configuration de la sécurité sans fil	36
Figure 39 Ajout du client « Switch » dans freeradius	38
Figure 40 Authentification 802.1x d'un client	38
Figure 41 Tests D'Authentification sans fils	39
Figure 42 Tests D'Authentification avec fils	39
Figure 43 Installation ldap	40
Figure 44 Configuration slapd	40
Figure 45 Configuration Dns slapd	40
Figure 46 Choix du nom de l'organisation slapd	40
Figure 47 Déplacement de la base de données initiale slapd	41
Figure 48 Activation du ldap dans freeRADIUS	41
Figure 49 Configuration du ldap dans freeRADIUS	41

Figure 50 Installation d'apache et de php	42
Figure 51 Installation de ldap account manager	42
Figure 52 Page d'authentification ldap account manager	42
Figure 53 Les groupes dans ldap account manager	42
Figure 54 Les utilisateurs dans ldap account manager	43
Figure 55 Diagramme de séquences du portail captif	45
Figure 56 Installation PfSense	47
Figure 57 Menu PfSense	47
Figure 58 Configuration interface Lan	48
Figure 59 Configuration des interfaces	48
Figure 60 Interface web pfsense	48
Figure 61 Page d'Accueil pfSense	49
Figure 62 DHCP PfSense	49
Figure 63 DNS Pfsense	50
Figure 64 pfSense	50
Figure 65 zone portail captif	51
Figure 66 Configuration portail captif 1	51
Figure 67 configuration portail captif 2	52
Figure 68 Serveurs d'authentification ldap	52
Figure 69 Ajout d'un groupe	53
Figure 70 Droit portail captif	53
Figure 71 Page d'authentification	54
Figure 72 Authentification	54
Figure 73 Pare-feu	58
Figure 74 Pare-feu dmz	58
Figure 75 Configuration des interfaces	59
Figure 76 Configuration de la DMZ	60
Figure 77 Configuration de VLAN	61
Figure 78 ipv4 Policy	62
Figure 79 Management accède au VLAN des employés	63
Figure 80 WAN accède au DMZ	64
Figure 81 DMZ un seul pare-feu	65
Figure 82 DMZ avec deux pares-feux	66
Figure 83 SMTP	67
Figure 84 POP3	68
Figure 85 IMAP	69
Figure 86 le fonctionnement du serveur SMTP	70
Figure 87 le fichier de configuration de postfix	72
Figure 88 le fichier de configuration de dovecot	73
Figure 89 le fichier d'authentification du dovecot	74
Figure 90 le fichier d'authentification du dovecot	74
Figure 91 le fichier de mail du dovecot	75
Figure 92 le fichier master du dovecot	75
Figure 93 le fichier master du dovecot	76
Figure 94 le fichier master du dovecot	76
Figure 95 ajout du nom de domaine mail.est.sma	77
Figure 96 ajout d'un utilisateur	77
Figure 97 création du compte de messagerie 2	78
Figure 98 création du compte de messagerie	78
Figure 99 Envoi d'un mail test	78
Figure 100 Réception d'un mail test	78
Figure 101 échange client/serveur	79
Figure 102 Installation Apache	80

Figure 103 création du répertoire site web	80
Figure 104 création du fichier site web	80
Figure 105 modification des vHosts 1	81
Figure 106 modification des vHosts 2	81
Figure 107 Page d'Accueil du site web	82
Figure 108 Fonctionnement SNMP	86
Figure 109 Requête SNMP	87
Figure 110 NagiosXi	90
Figure 111 modification de la connexion	90
Figure 112 Activation de la connexion	90
Figure 113 Modification de l'adresse	90
Figure 114 Page SNMP pare-feu	91
Figure 115 Activation SNMP pare-feu	91
Figure 117 Ajout du pare-feu dans Nagios	92
Figure 116 Choix des ports à superviser	92
Figure 118 Dashboard supervision Pare-feu	92
Figure 119 Ajout du routeur dans Nagios	93
Figure 120 Configuration du routeur	93
Figure 121 Choix des ports du routeur à superviser	93
Figure 122 Dashboard du routeur	93
Figure 123 Activation d'SNMP sur pfSense	94
Figure 124 ajout pfSense a Nagios	94
Figure 125 nouvel ajout SNMP	94
Figure 126 Dashboard supervision pfSense	94
Figure 127 Configuration snmp client Ubuntu	95
Figure 128 Choix des services	95
Figure 129 Ajout d'une machine linux SNMP	95
Figure 130 Dashboard Ubuntu Server Radius	96
Figure 131 Dashboard des différents hôtes	96
Figure 132 Installation Elastix	100
Figure 133 activation support ipv4	101
Figure 134 Configuration des interfaces	101
Figure 135 Adresse de la passerelle	101
Figure 136 Attribution d'une adresse fixe	101
Figure 137 Attribution mot de passe MySQL	101
Figure 138 Attribution mot de passe Serveur	102
Figure 139 Interface web Elastix	102
Figure 140 Ajout périphérique	103
Figure 141 configuration du périphérique	103
Figure 142 Configuration d'un utilisateur	104
Figure 143 Téléphone 3CX	104
Figure 144 Configuration d'un client	104
Figure 145 Vérification des utilisateurs	105
Figure 147 Appel PosteAri2	105
Figure 146 Réception de l'appel de PosteAri3	105

# WEBOGRAPHIE

## Partie I :

- <https://www.linksys.com/be/support-article?articleNum=140196>
- [https://www.cisco.com/web/FR/pdfs/isr/1941\\_data\\_sheet\\_c78\\_556319.pdf](https://www.cisco.com/web/FR/pdfs/isr/1941_data_sheet_c78_556319.pdf)
- <https://www.tp-link.com/fr/home-networking/dsl-modem-router/td-w8960n/>

## Partie II :

- <https://doc.ubuntu-fr.org/isc-dhcp-server>
- <https://ubuntu.com/server/docs/service-domain-name-service-dns>
- <https://doc.ubuntu-fr.org/dns>
- <https://wiki.freeradius.org/Home#documentation>
- <https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-on-ubuntu-16-04>
- <https://www.pc2s.fr/pfsense-portail-captif-avec-authentification-utilisateur/>

## Partie III :

- [https://fr.wikipedia.org/wiki/Serveur\\_web](https://fr.wikipedia.org/wiki/Serveur_web)
- <https://www.xmodulo.com/how-mail-server-works.html>
- <https://fr.wikipedia.org/wiki/Postfix>
- <https://gatefy.com/blog/what-is-mail-server/>

## Partie IV :

- <https://doc.ubuntu-fr.org/snmp>
- <https://fr.wikipedia.org/wiki/Nagios>
- <https://mixconcept.fr/pourquoi-faut-il-utiliser-la-voip>



