SAÉ303 Concevoir un réseau multi-sites

SAE 303

MULTI-SITES

RT - Group

TEAM RT-GROUP

Kylian seger
Ilyas tunay
Clement Petit
Yohann Mitel
Yassine el hamioui

Du 2 mais au 5 mai 2023

r&t Réseaux et Télécoms
IUT Nord Franche-Comté

IUT NORD FRANCHE-COMTÉ | RÉSEAU & TELECOMS

1. Introduction

Cette SAE 3.03, intitulée *Mettre en place un réseau informatique multi sites*, est encadrée par M.BOUILLET ainsi que M.SPIES du Mardi 2 mai au Vendredi 5 mai où l'objectif était de concevoir une maquette d'infrastructure réseau pour l'entreprise Beerok. Cette maquette impliquait la mise en place d'un cœur de réseau pour relier les trois sites (un showroom, un magasin et un siège) via GNS3. Plusieurs VLAN ont été utilisés, notamment le VLAN WiFi, le VLAN Direction, le VLAN Voix et le VLAN Ventes, chacun étant attribué à un site spécifique. Par ailleurs, nous avons réalisé la configuration de plusieurs serveurs comme NextCloud, DHCP, DNS, Active Directory, Elastix ou encore MQTT. Durant ces 4 jours de travail, nous avons dû nous organiser afin d'avancer plus efficacement mais aussi de manière méthodique pour implémenter les services au fur et à mesure sur notre réseau.

2. Infrastructure réseau

Un **VLAN** est un réseau local virtuel, c'est-à-dire que dans un réseau local (**LAN**), nous pouvons créer plusieurs sous-réseaux virtuels sur un switch qui par défaut ne peuvent pas communiquer entre eux, ce qui permet de limiter des attaques potentielles à l'intérieur de notre réseau local.
Grâce à ces sous-réseaux virtuels, nous pouvons regrouper des utilisateurs selon leur secteur d'activité au sein de l'entreprise et donc de limiter le trafic vers un seul VLAN en particulier et donc de préserver l'efficacité de notre réseau mais aussi de faciliter son administration. De plus, il est possible d'établir des priorités pour certains flux comme la vidéo ou la voix en proposant plus de bande passante pour un type de flux.

Voici notre plan d'adressage IP afin de mieux comprendre comment allons-nous implémenter les VLAN dans notre réseau :

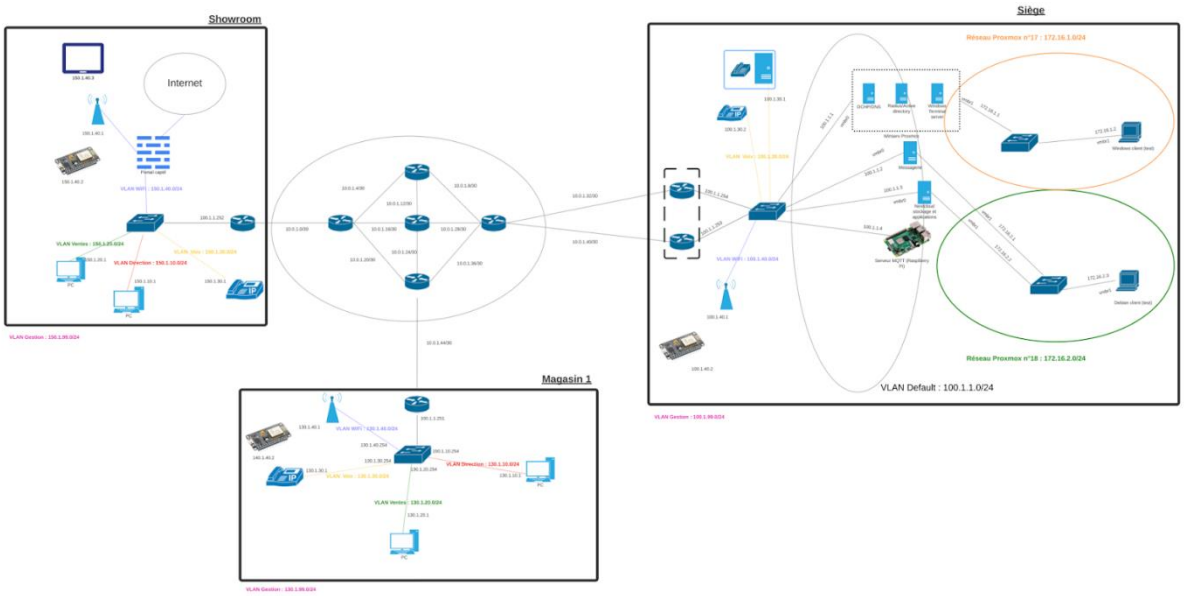


Figure 1 : Plan d'adressage IP

Notre infrastructure réseau contient le réseau du siège, le réseau du showroom ainsi que les réseaux des différents magasins. Prenons comme exemple le réseau du siège :

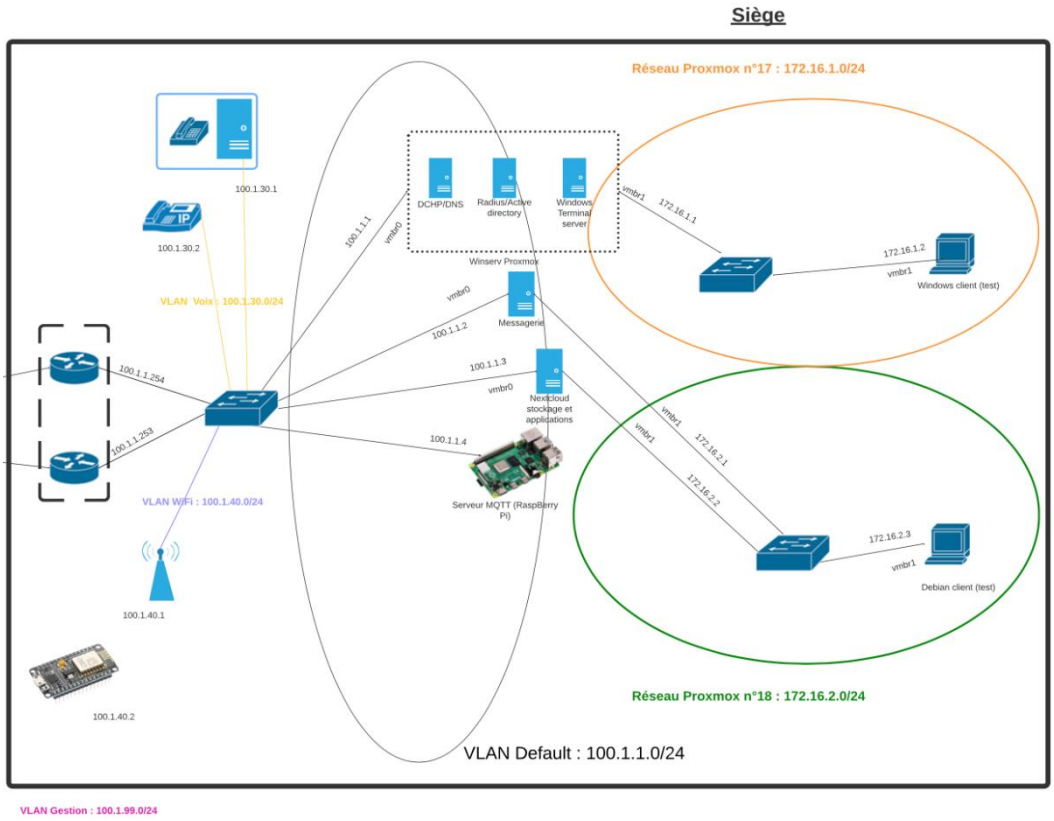


Figure 2 : Réseau du siège situé à Meaux

Nous avons créé 6 VLAN pour ce réseau local dont :

- VLAN 1 Par défaut : VLAN servant à regrouper les différents serveurs
- VLAN 10 Direction : VLAN servant à regrouper tous les salariés faisant parti de la direction
- VLAN 20 Ventes : ce VLAN nous a été utile afin de réaliser différents tests
- VLAN 30 Voix : VLAN servant à regrouper les postes téléphoniques
- VLAN 40 Wifi : VLAN servant à gérer les points d'accès Wifi
- VLAN 99 Gestion : VLAN servant à administrer notre réseau à distance via une connexion SSH

2.1. Création des VLAN

Pour créer un VLAN, nous devons tout d'abord passer en mode configuration sur notre switch *Cisco Catalyst 3750* en entrant la commande ***conf t***. Ensuite, nous devons entrer la commande *vlan* suivi du numéro de ce dernier, par exemple ***vlan 99*** puis lui attribuer le nom gestion à l'aide de la commande ***name Gestion***.

Si nous voulons un accès à distance en **SSH** afin d'administrer notre switch, nous devons attribuer une adresse IP sur une interface virtuelle que nous devons également déclarer puis activer la fonctionnalité SSH sur notre switch. Pour cela, nous devons être en mode configuration et entrer la commande ***interface vlan99*** afin d'attribuer une adresse IP à l'interface que nous venons de déclarer à l'aide de la commande ***ip address 100.1.99.1***

255.255.255.0. Il est possible de protéger un port en limitant le nombre d'adresse MAC apprise sur ce dernier. Pour cela, nous devons activer la sécurité sur le port concerné à l'aide de la commande ***switchport port-security*** pour ensuite définir le type de sécurité que nous allons implémenter, ici une seule adresse MAC maximum apprise sur le port concerné grâce à la commande ***switchport port-security mac-address sticky***. En cas de violation de la règle, nous devons définir l'action à réaliser. Dans notre cas, nous allons désactiver le port avec la commande ***switchport port-security violation shutdown***.

Par défaut, l'interface est désactivée même après l'ajout de la commande ***no shutdown***, ce qui est normal car aucun port de notre commutateur n'est attribué au VLAN 99. Pour cela, nous allons choisir une interface qui aura accès à ce VLAN à l'aide de la commande ***int Fa1/0/24*** puis ***switchport access vlan 99***, si nous voulons l'affecter à plusieurs ports nous utilisons la commande ***int range Fa1/0/20 - 24*** puis spécifier le VLAN auquel ces ports auront accès.

2.2. Configuration des modes Access / Trunk

Afin de finaliser la configuration des switchs, nous devons spécifier quels ports auront accès à quels VLAN mais aussi quels ports seront en mode Trunk ou en mode Access.

Lorsqu'un port est configuré en mode Access, cela signifie qu'il est attribué à un seul VLAN spécifique et ne peut pas transporter de trafic de plusieurs VLAN. Par exemple, pour configurer le port *Fa1/0/4* en mode Access, nous devons tout d'abord spécifier quel VLAN sera disponible sur ce dernier avec la commande ***switchport access vlan 40*** puis mettre ce port en mode Access avec la commande ***switchport mode access***.

Lorsqu'un port est configuré en mode Trunk, cela signifie que ce dernier va être utilisé pour transporter plusieurs VLAN sur un seul et même lien physique qui relie notre switch à un routeur ou alors vers un autre switch, c'est-à-dire qu'il ne fera partie d'aucun VLAN. Ce port ne peut pas être relié à un PC car ce dernier ne saura pas dans quel VLAN il se trouve, ce qui signifie que nous ne pourrions pas communiquer avec les autres VLAN. Pour configurer un port en mode trunk, nous devons tout d'abord entrer la commande ***switchport trunk encapsulation dot1q***, ce qui indique au port que la méthode d'encapsulation des trames est **IEEE 802.1Q** qui permet de modifier la trame Ethernet au niveau de la couche 2 et de taguer les trames pour identifier les VLAN. Ensuite, nous devons spécifier au port qu'il est en mode Trunk avec la commande ***switchport mode trunk***. Pour finir, nous devons également ajouter les VLAN qui feront partie du Trunk à l'aide de la commande ***switchport trunk allowed vlan add 1,10,20,30,40,99***.

```
interface FastEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,10,20,30,40,99
 switchport mode trunk
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa1/0/2, Fa1/0/3, Fa1/0/7
                                                 Fa1/0/9, Fa1/0/10, Fa1/0/11
                                                 Fa1/0/12, Fa1/0/13, Fa1/0/14


                                                 Fa1/0/15, Fa1/0/16, Fa1/0/17
                                                 Fa1/0/18, Fa1/0/19, Fa1/0/20
                                                 Fa1/0/21, Fa1/0/22, Fa1/0/23
                                                 Gi1/0/1, Gi1/0/2
10   Direction                         active    Fa1/0/8
20   Ventes                            active
30   Voix                              active    Fa1/0/5, Fa1/0/6
40   Wifii                             active    Fa1/0/4
99   Gestion                           active    Fa1/0/24
```

Figure 3 : Exemple de configuration du switch SW0

Nous allons avoir 3 phases de tests pour vérifier le bon fonctionnement des VLAN :

- Vérifier qu'un ping entre 2 machines faisant partie du même réseau local ainsi que du même VLAN fonctionne
- Vérifier qu'un ping entre 2 machines faisant partie du même réseau local mais de deux VLAN différents fonctionne
- Vérifier qu'un ping entre 2 machines ne faisant pas partie du même réseau local et de deux VLAN différents fonctionne

Nous avons rencontré des problèmes lors de nos différentes phases de tests. Tout d'abord, les interfaces virtuelles des routeurs n'étaient pas correctement configurées donc un hôte du VLAN 10 ne pouvait pas joindre un hôte du VLAN 20 faisant partie du même réseau local mais aussi à cause du fait que le VLAN 20 n'était pas présent dans le Trunk. Ensuite, deux hôtes ne faisant pas partie du même réseau local et de deux VLAN différents ne pouvaient pas communiquer entre eux car nous avons repéré une erreur dans la configuration du protocole BGP sur nos routeurs.

2.3. Mise en place réseau et interconnexion

Dans le cadre de ce projet, il fallait bien évidemment mettre en place un cœur de réseau pour relier plusieurs sites, tout en activant les protocoles IP, OSPF, BGP et MPLS. Cette infrastructure réseau a été conçue pour améliorer la communication et la connectivité entre les différents sites.

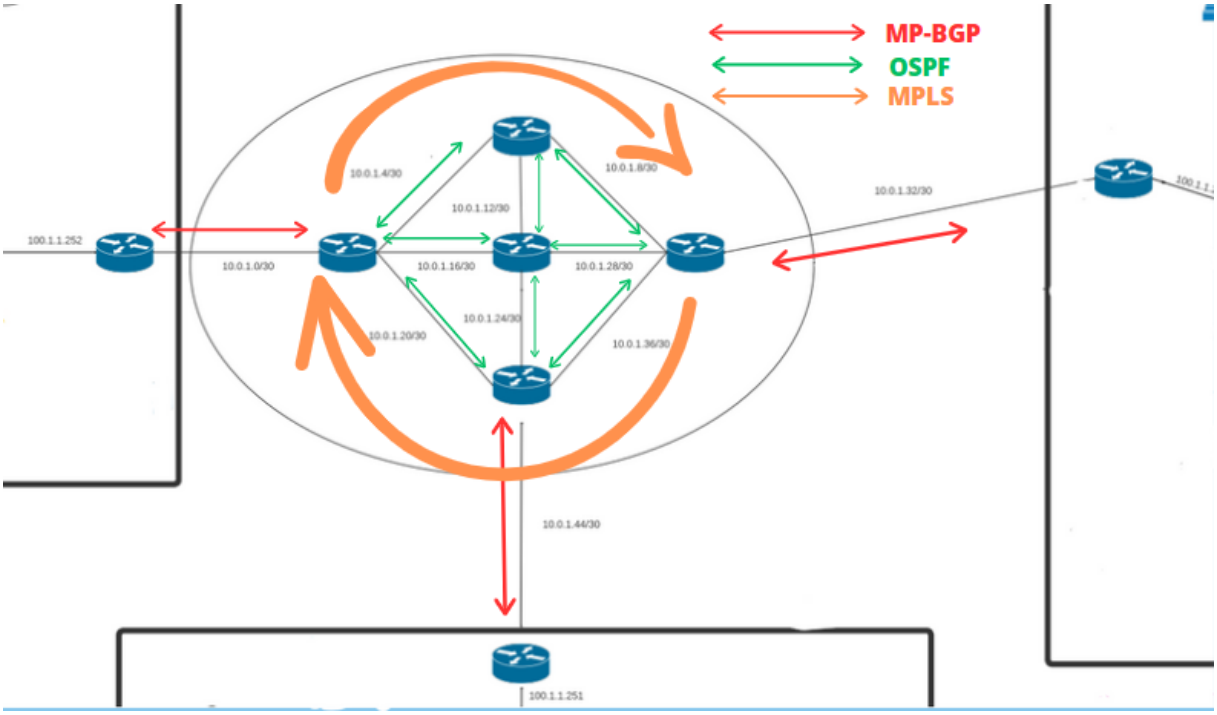


Figure 4 : Coeur de réseau

Le protocole IP (Internet Protocol) est le protocole de communication standard pour les réseaux informatiques. Il permet de transférer des données d'un point à un autre sur Internet.

OSPF (Open Shortest Path First) est un protocole de routage utilisé pour établir des connexions entre différents réseaux. Il permet aux routeurs de découvrir les chemins les plus courts vers les réseaux de destination.

BGP (Border Gateway Protocol) est un protocole de routage utilisé pour acheminer des données entre différents systèmes autonomes (AS) sur Internet. Il permet aux réseaux de communiquer entre eux et d'échanger des informations sur les routes les plus efficaces pour atteindre une destination donnée.

Enfin, MPLS (Multiprotocol Label Switching) est un protocole de commutation de paquets utilisé pour améliorer la qualité de service (QoS) sur les réseaux de télécommunication.

Il permet de créer des chemins de communication plus efficaces pour les données en utilisant des étiquettes.

2.3.1. Méthodologie

Notre approche pour réaliser ce projet a été la suivante :

- Analyse des besoins : Nous avons commencé par évaluer les besoins de chaque site et les exigences de leur connectivité.
- Conception de l'architecture : Nous avons ensuite élaboré une architecture réseau en conséquence, qui répond aux besoins des sites en termes de connectivité et de performance.
- Configuration et mise en place : Nous avons ensuite procédé à la configuration et à la mise en place du cœur de réseau, en activant les protocoles IP, OSPF, BGP et MPLS.
- Tests et vérifications : Une fois la configuration terminée, nous avons effectué des tests et des vérifications pour s'assurer que la connectivité entre les différents sites était stable et fiable.

Grâce à la mise en place de ce cœur de réseau et à l'activation des protocoles IP, OSPF, BGP et MPLS, nous avons réussi à améliorer significativement la connectivité et la communication entre les différents sites.

L'implémentation de ce réseau a permis une distribution efficace des données entre les sites et une gestion plus facile du trafic, améliorant ainsi la collaboration et la productivité des employés pour l'entreprise. Les protocoles activés ont également permis une meilleure fiabilité et une réduction des temps de latence, améliorant ainsi la qualité de service globale.

Nous tenons à souligner que ce projet à été mené en utilisant des compétences et des connaissances approfondies en réseau, en protocole de communication. Le réseau est désormais plus résiliant, grâce à la configuration de protocoles de routage dynamique tels que OSPF et BGP, qui permettent une redondance de chemins en cas de panne d'un lien ou d'un équipement.

Il fallait également, quand tous les protocoles fonctionnaient, mettre en place du routage inter VLAN entre les différents sites de l'entreprise. C'est-à-dire qu'il faut interconnecter les différents VLANs (réseaux locaux virtuels qui permettent de regrouper des équipements réseau) sur les différents sites pour que les communications entre tous les sites puissent passer correctement. Cela, en créant plus précisément des sous interfaces.

Les sous interfaces permettent donc de connecter les différents VLANs, tout en garantissant l'isolation entre les différents réseaux.

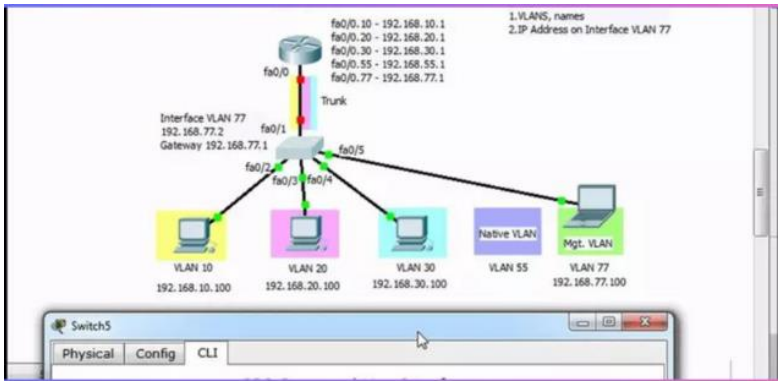


Figure 5 : Topologie réseau

3. Configuration des bornes WiFi

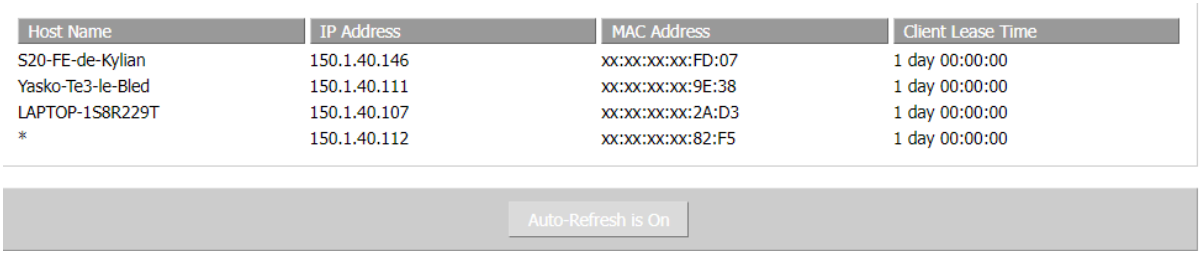
Pour la configuration des bornes wifi, l'objectif est d'avoir un hotspot privé dans chaque magasin et un privé ainsi qu'un public pour les clients dans le showroom. Pour cela il faut se connecter à la borne par son ip de base après l'avoir reset. Il faut donc se connecter a l'adresse 192.168.1.1 pour arriver sur la page web de configuration. Une fois cela fait, il faut installer un autre firmware plus permissif sur la borne que celui de base. Pour cela on vérifie quel firmware est installé sur la borne et si c'est autre chose que dd-wrt on va sur le site officiel de dd-wrt pour télécharger la dernière version et l'installer sur la borne. Si le firmware installé est dd-wrt on vérifie si le firmware est dans la dernière version sinon on la remplace par la plus récente.

Une fois cela fait on vérifie que la borne à le bon nom sinon on le modifie, on vérifie l'ip par défaut pour ne pas avoir de problème de connexion à la page de configuration, on définit l'étendu du dhcp et quels services sont activés. Une fois la configuration de base terminée, il faut créer le réseau et sécuriser la borne. Pour cela on commence par désactiver tout type de connexion a part en SSH, on met la borne en mode bridge et on active le mode de sécurité WPA2 et on définit un mot de passe sécurisé pour la clé WPA avec comme algorithme TKIP+AES.

SSID :	borne groupe 1 showroom
Protocole :	802.11g
Type de sécurité :	WPA2 - Personnel
Fabricant :	MediaTek, Inc.
Description :	MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Version du pilote :	3.0.1.1253
Bande passante réseau :	2,4 GHz
Canal réseau :	6
Vitesse de connexion (Réception/ Transmission) :	54/54 (Mbps)
Adresse IPv6 locale du lien :	fe80::f6a1:b85f:2a68:924d%18
Adresse IPv4 :	150.1.40.107
Serveurs DNS IPv4 :	150.1.40.1 (non chiffré)
Adresse physique (MAC) :	34-6F-24-93-2A-D3

Figure 6 : Informations sur la borne Wifi

Une fois la configuration terminée nous avons ces informations quand on se connecte depuis un client. Le SSID est le bon, la sécurité est bien en WPA2, le canal 6 pour le réseau et enfin la plage d'adressage ip la borne est en 150.1.40.1 et le DHCP nous a donné le 150.1.40.107



Host Name	IP Address	MAC Address	Client Lease Time
S20-FE-de-Kylian	150.1.40.146	xx:xx:xx:xx:FD:07	1 day 00:00:00
Yasko-Te3-le-Bled	150.1.40.111	xx:xx:xx:xx:9E:38	1 day 00:00:00
LAPTOP-1S8R229T	150.1.40.107	xx:xx:xx:xx:2A:D3	1 day 00:00:00
*	150.1.40.112	xx:xx:xx:xx:82:F5	1 day 00:00:00

Figure 7 : Informations sur les connexions

Lorsque nous nous connectons au réseau Wifi, nous voyons les différents appareils connectés.

4. Configuration d’asterisk et des téléphones

La première étape pour configurer le serveur Asterisk qui gère la téléphonie est de se connecter directement au serveur et d'accéder à la page de configuration en entrant son adresse IP dans un navigateur. La première action à effectuer une fois connecté est de réinitialiser la configuration en mode usine. Une fois cette opération effectuée, on se connecte pour commencer la configuration. Pour commencer la configuration, vous devez créer des utilisateurs. Pour cela, il faut le nommer, lui donner un numéro en suivant le plan de numérotation fait au préalable. Il faut aussi ajouter un mot de passe pour activer le numéro et pour la boîte vocale.

Après avoir créé les utilisateurs, on a pu configurer les extensions, les groupes d'appels et les autorisations d'accès. Il est également important de configurer les paramètres de sécurité, tels que les mots de passe et les restrictions d'accès, pour protéger le système contre les menaces potentielles.

Enfin, on a pu faire des tests sur le système après la configuration pour s'assurer que tout fonctionne correctement et que les utilisateurs peuvent passer et recevoir des appels sans problème.

5. Configuration du serveur Windows

Pendant cette semaine d'apprentissage évaluée, nous avons utilisé une machine virtuelle sur un serveur Proxmox pour simuler un serveur Windows. Nous avons effectué plusieurs tests pour configurer le serveur, en utilisant des machines clientes également virtuelles sur le même serveur Proxmox.

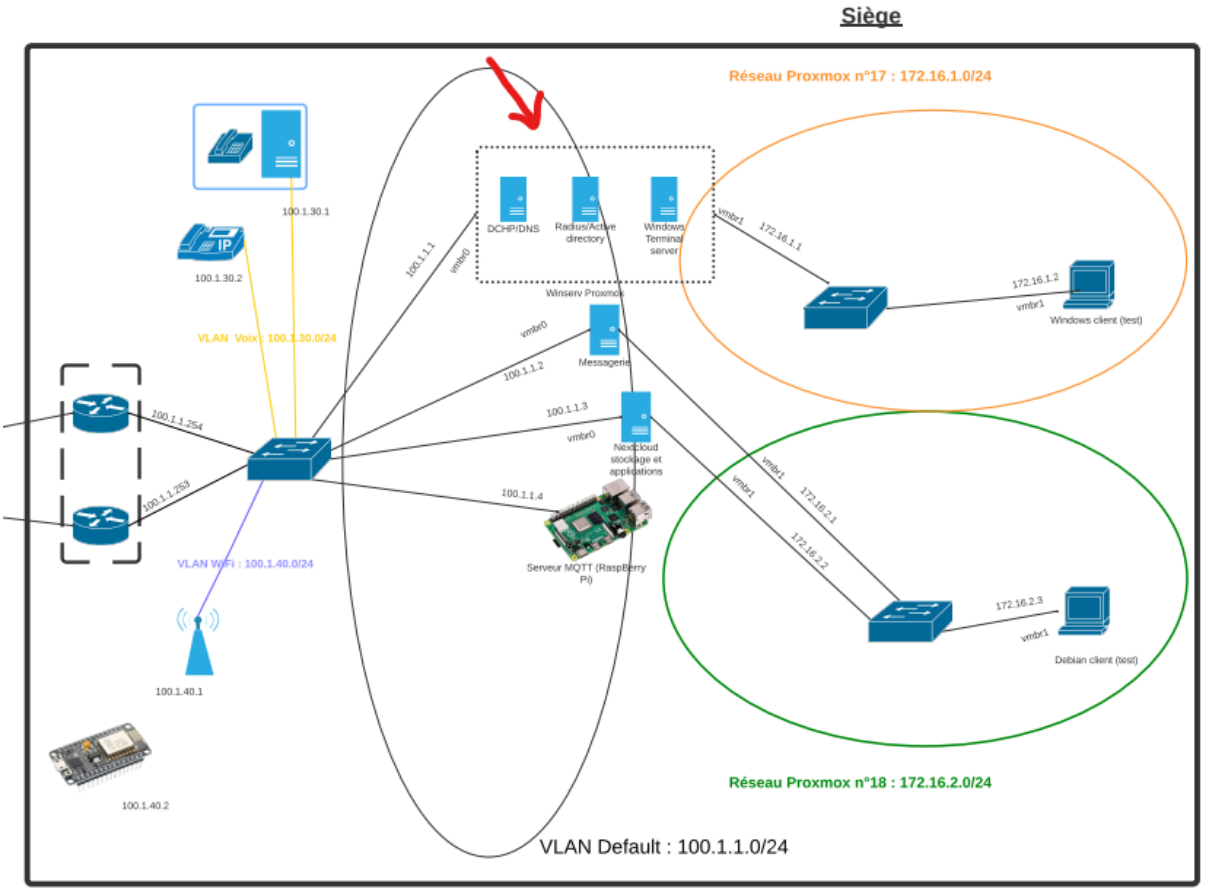


Figure 8 : Réseau du siège situé à Meaux

Le serveur Windows sera installé dans le réseau informatique de l'entreprise, plus précisément dans le siège de l'entreprise. Ce serveur offrira trois services importants.

Le premier service est le DHCP, qui signifie Dynamic Host Configuration Protocol. Ce service permet de distribuer automatiquement des adresses IP aux différents appareils connectés au réseau de l'entreprise, comme les ordinateurs, les téléphones, les tablettes, etc. Cela permet aux appareils de communiquer entre eux et avec internet de manière efficace.

Le deuxième service est le DNS, qui signifie Domain Name System. Ce service permet de traduire les noms de domaines en adresses IP. Par exemple, lorsque vous entrez l'adresse d'un site web dans votre navigateur, le DNS va chercher l'adresse IP correspondante pour que votre navigateur puisse se connecter au serveur où se trouve le site web. Cela permet aux utilisateurs de naviguer sur internet en utilisant des noms de domaines plutôt que des adresses IP complexes.

Le troisième service est l'Active Directory, qui est un service de gestion d'identité et d'accès. Il permet de gérer les utilisateurs et les ordinateurs de l'entreprise, en créant des comptes pour chaque utilisateur et chaque ordinateur, en leur attribuant des permissions d'accès à différents fichiers et dossiers, et en leur fournissant des ressources partagées. Cela permet de sécuriser les informations de l'entreprise en contrôlant qui a accès à quoi et en gérant les droits d'accès de manière centralisée.

En résumé, ces trois services sont essentiels pour le bon fonctionnement du réseau informatique de l'entreprise, en permettant une gestion efficace des adresses IP, des noms de domaines et des accès aux ressources partagées.

5.1. Configuration serveur DCHP sur le serveur Windows

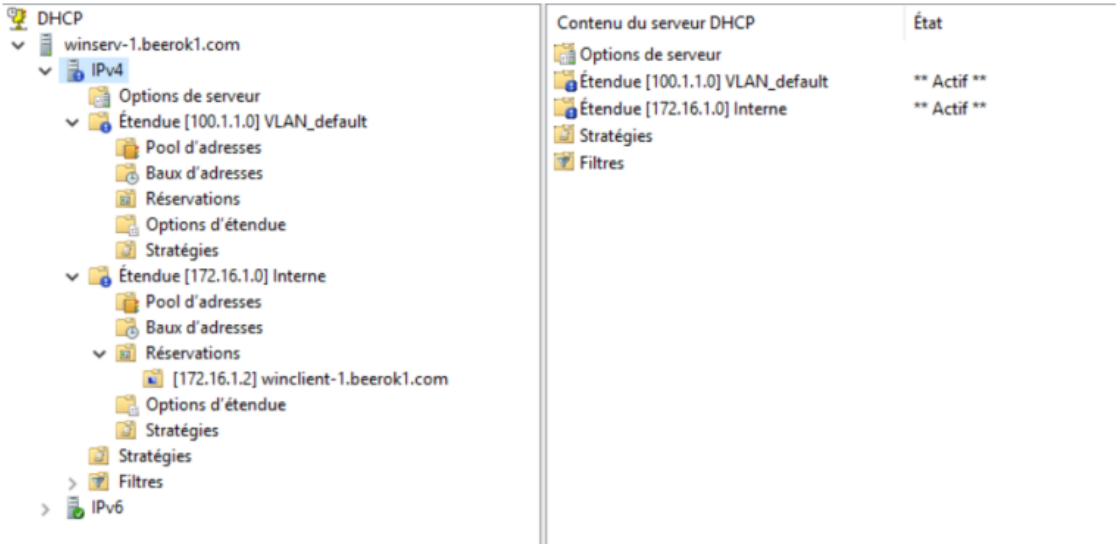


Figure 9 : Configuration étendues DHCP

Deux étendus ont été configurés, l'étendue « Interne » représente le côté Proxmox où se trouve un client test, ci-dessus on peut voir que dans l'étendue « Interne » une réservation @IP a été attribuée à l'@MAC de la machine client.

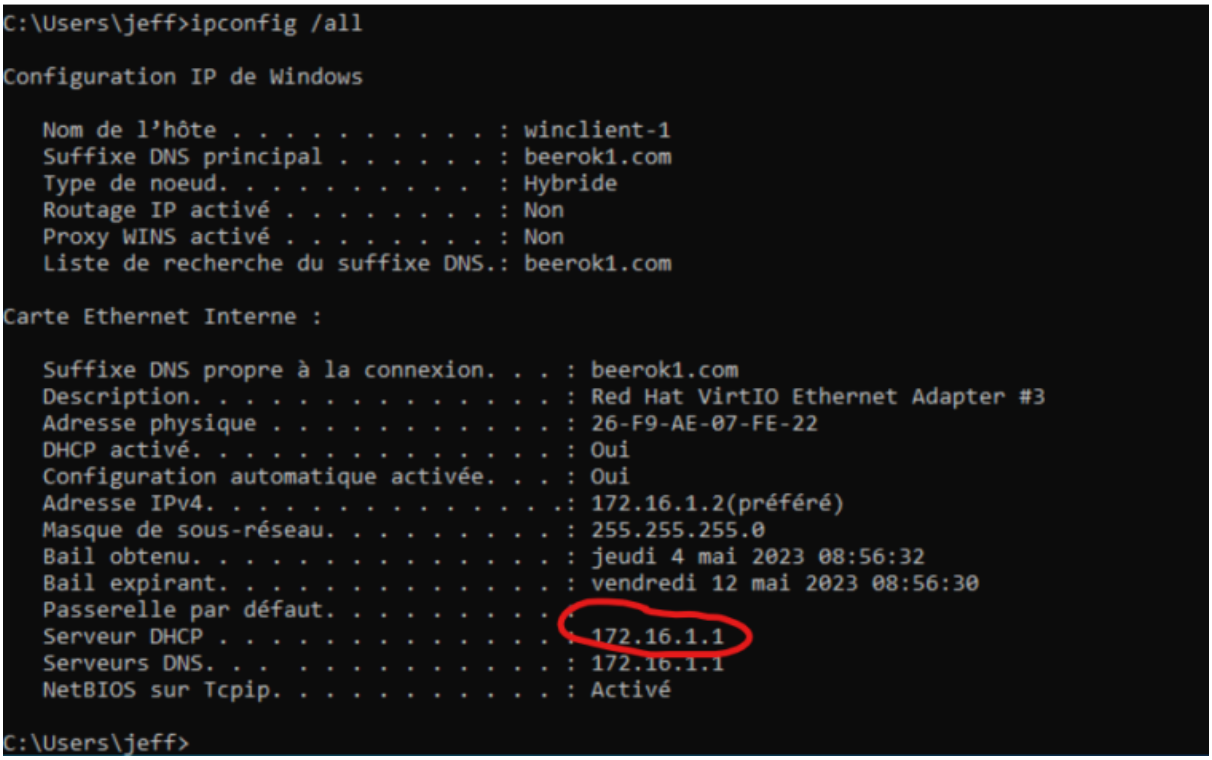


Figure 10 : ipconfig /all sur pc client

Sur le client lorsqu'on effectue la commande ipconfig /release suivi de ipconfig /renew nous pouvons voir qu'une @IP lui a bien été attribuée.

5.2. Configuration du serveur DNS sur le serveur Windows

L'utilisation d'un serveur DNS nous a été essentielle pour la mise en place d'un environnement Active Directory fiable et sécurisé. Active Directory est un service de répertoire utilisé pour centraliser la gestion des utilisateurs, des groupes et des ressources dans un réseau informatique. Il utilise DNS pour résoudre les noms d'hôtes en adresses IP, ce qui permet aux clients de localiser les ressources dans le réseau.

La mise en place d'un serveur DNS pour Active Directory permet de simplifier la gestion des noms d'hôtes et de résoudre les problèmes de conflit de noms. Le serveur DNS permet de créer une zone de recherche directe pour le domaine Active Directory, ce qui permet de résoudre les noms d'hôtes de manière efficace et rapide.

En regardant l'image ci-dessous, on peut constater qu'une zone de recherche directe a été établie pour le domaine beerok1.com. Cette zone contient les noms des machines principales qui sont localisées dans le siège de l'entreprise.

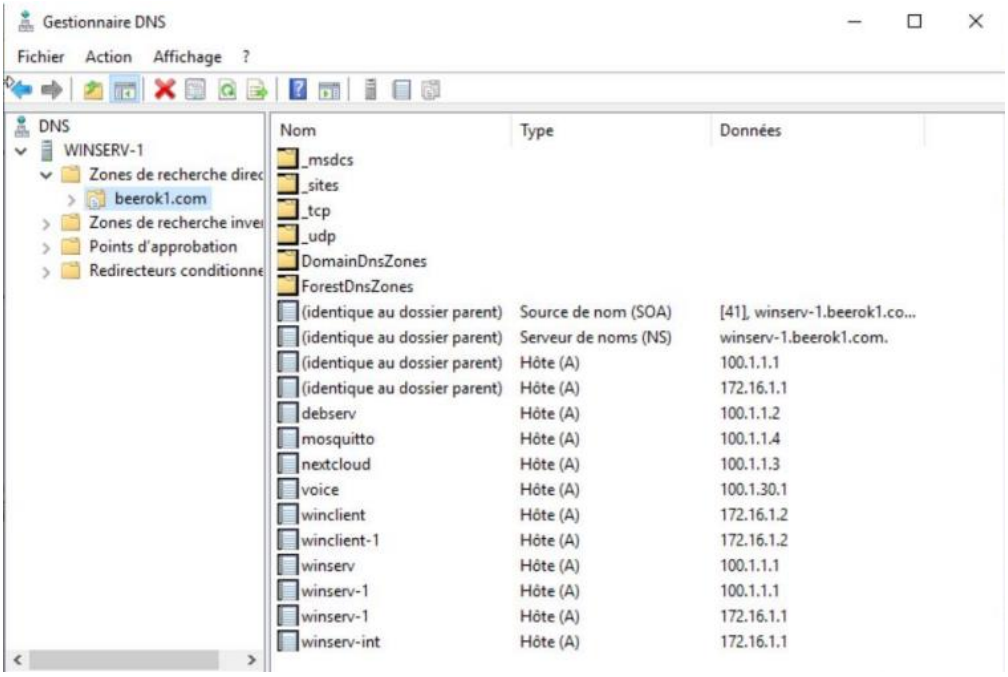


Figure 11 : Gestionnaire DNS

Sur le client en faisant la commande nslookup nous pouvons interroger le serveur DNS sur les différents noms ce qui nous donne :

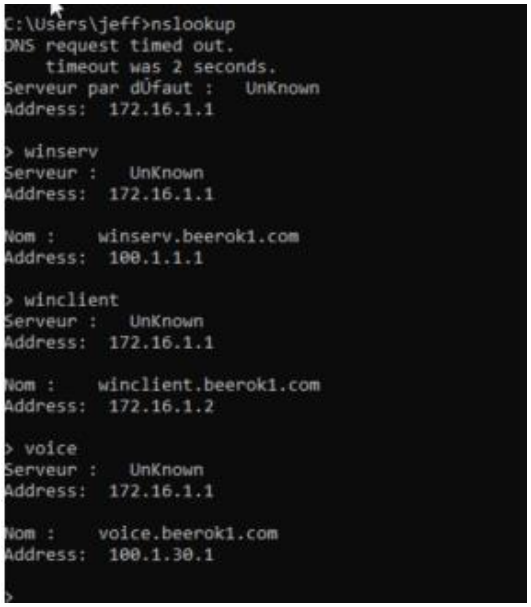


Figure 12 : nslookup sur pc client

En utilisant la commande nslookup suivie du nom d'hôte ou de l'adresse IP du serveur DNS que l'on souhaite vérifier, on peut s'assurer que le DNS est correctement configuré en obtenant la réponse avec l'adresse IP du serveur DNS et son nom d'hôte. Cela permet de s'assurer que le serveur DNS fonctionne correctement et est capable de résoudre les noms d'hôtes en adresses IP, ce qui est essentiel pour le bon fonctionnement du réseau informatique.

5.3. Déploiement d'Active Directory

Active Directory permet de centraliser la gestion des utilisateurs, des groupes, des ordinateurs et des ressources dans un réseau informatique. Il offre une multitude de fonctionnalités, telles que la gestion de la sécurité, la gestion des stratégies de groupe, la gestion de l'authentification et de l'autorisation, la gestion des services réseau, etc.Active Directory simplifie la gestion des ressources informatiques en centralisant leur administration dans un seul endroit.

Tout d'abord, il a fallu créer les groupes globaux « G_dir », « G_prod », « G_ventes ». Il a également fallu créer les groupes locaux qui vont être utiles pour la définition des droits lors du partage des différents dossiers.

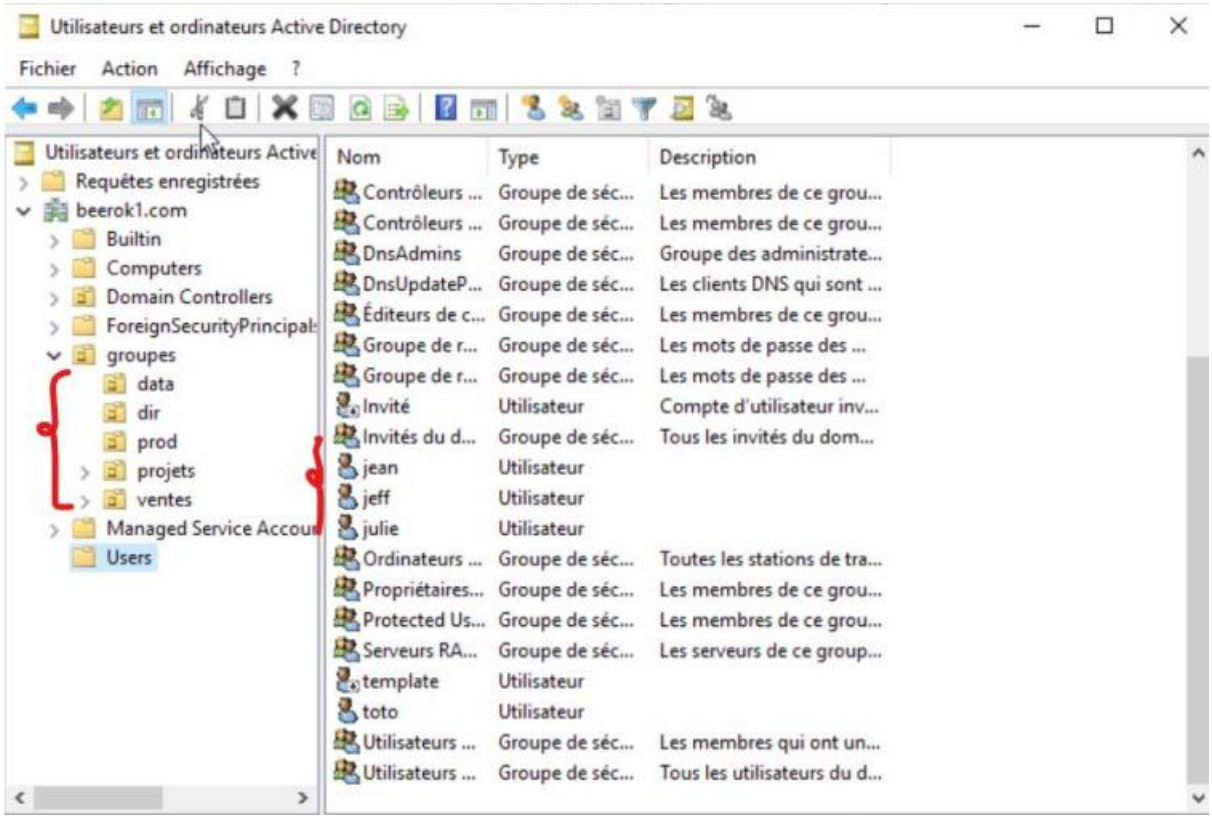


Figure 13 :

Une fois les différents groupes créés nous sommes passé à la création des utilisateurs pour ce faire il a fallu créer un template, dans ce template nous devions définir le chemin de répertoire de profil des différents utilisateurs.

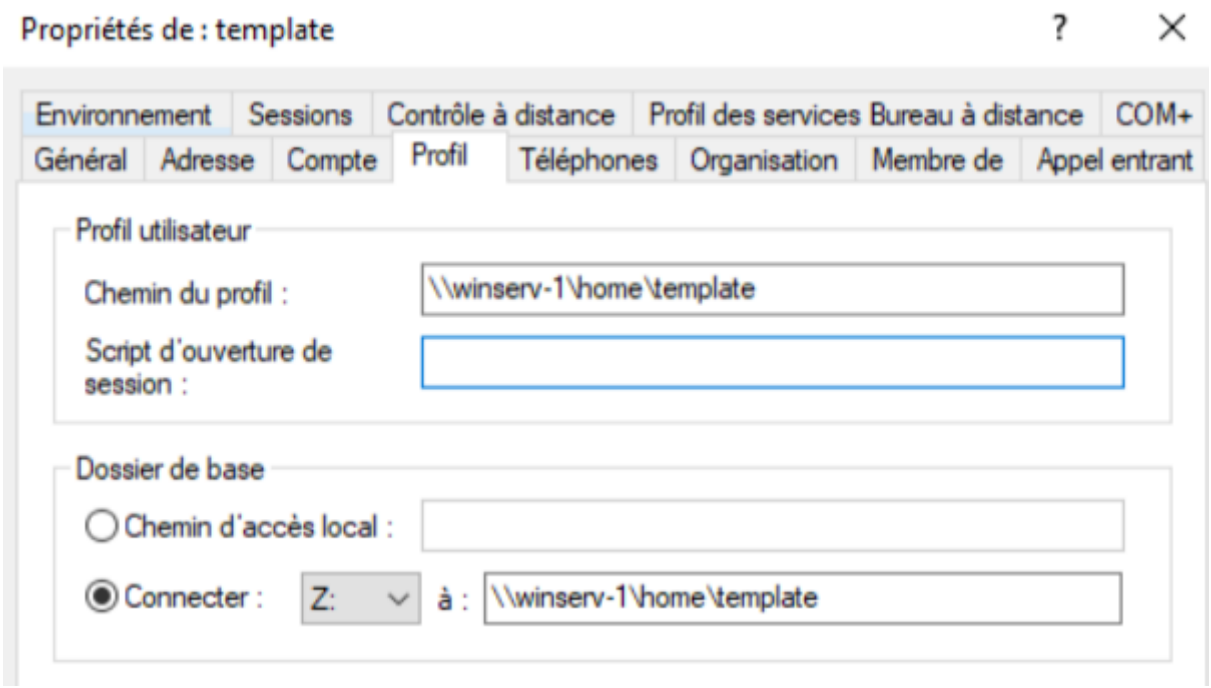


Figure 14 :

Par la suite, il a fallu partager les différents dossiers en utilisant les groupes locaux.

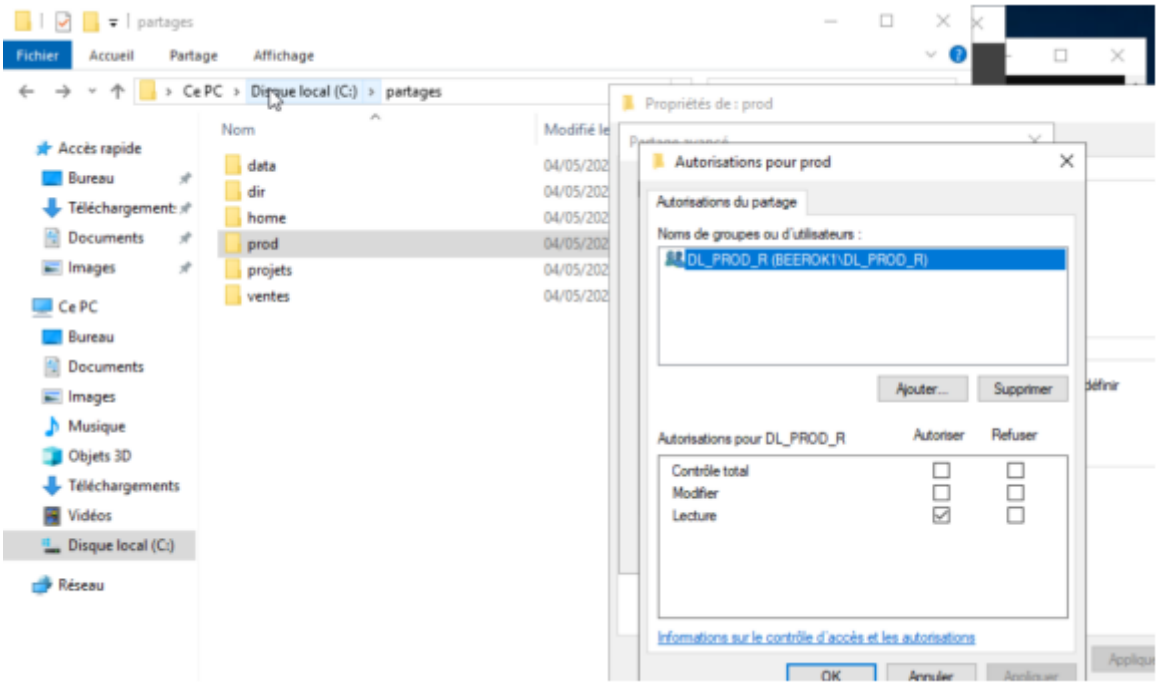


Figure 15 : Autorisation dossiers partagés

Lorsqu'on se connecte à un utilisateur sur le winclient nous pouvons voir que les dossiers partagés sont visibles.

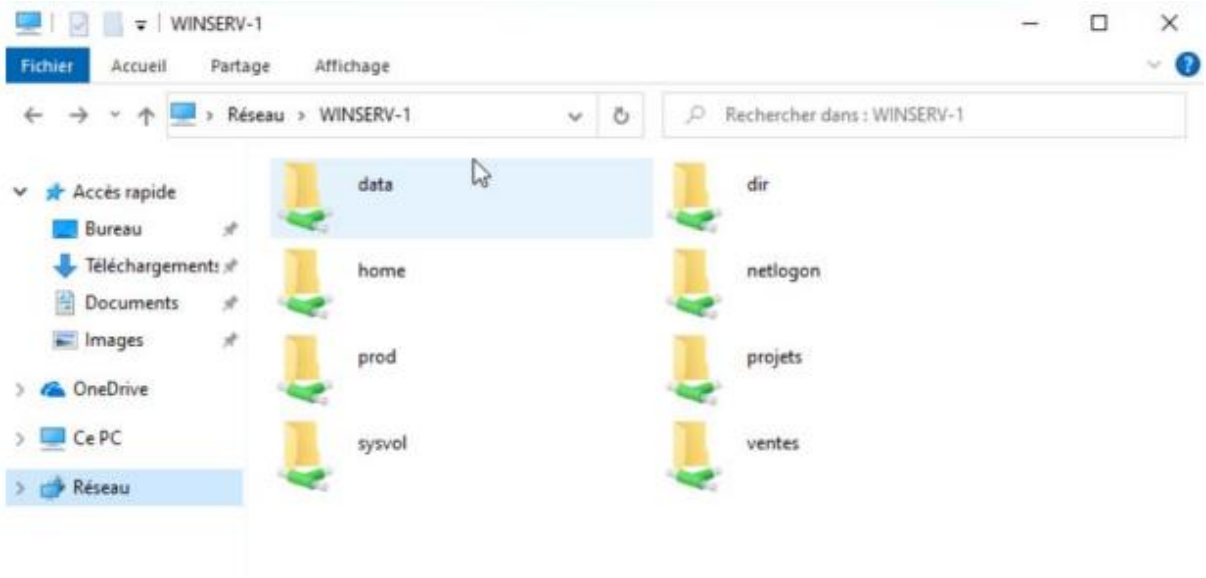


Figure 16 : Dossiers partagés

Enfin, dans le répertoire home nous pouvons voir que les différents répertoires profil ont bien été créés. Grâce à cette configuration les utilisateurs pourront avoir accès à leurs espaces personnels depuis n'importe quelle machine faisant partie du domaine beerok1.com.

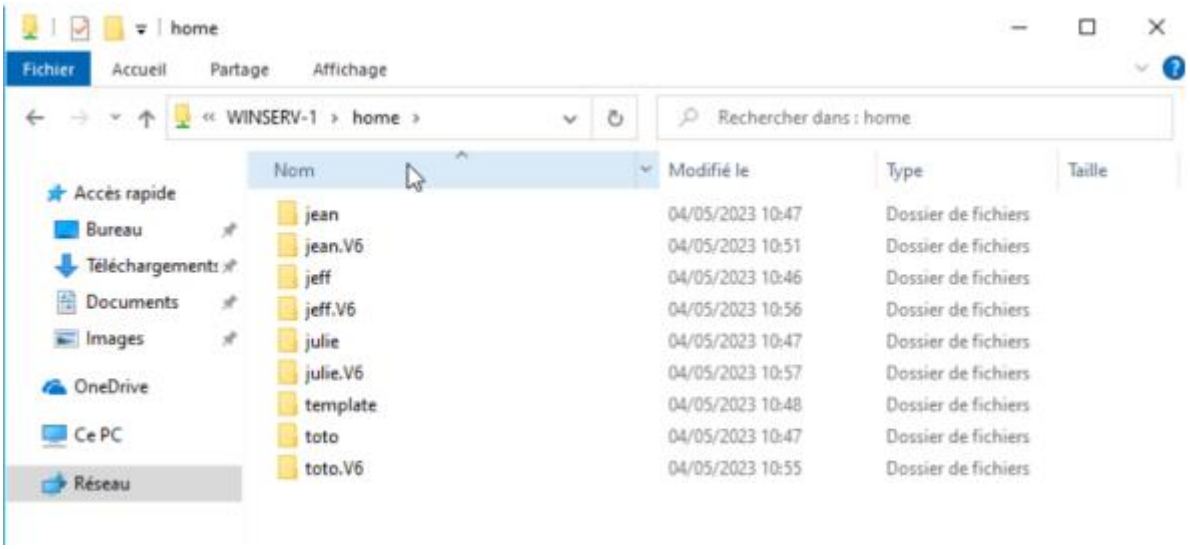


Figure 17 : Répertoire home

6. Nextcloud

6.1. Présentation de NextCloud

Nextcloud est une plateforme en ligne de stockage et de partage de fichiers qui offre de nombreux avantages pour l'entreprise. Elle permet de stocker et de partager des fichiers en toute sécurité, de collaborer en temps réel avec d'autres salariés mais aussi de synchroniser des fichiers entre différents appareils. Avec NextCloud, l'entreprise peut contrôler le stockage de fichiers et offrir aux employés une expérience de travail fluide et homogène, tout en respectant les normes de sécurité et de confidentialité des données. Toutes ces fonctionnalités font de NextCloud un outil essentiel pour les entreprises qui souhaitent gérer efficacement le stockage de fichiers et améliorer la productivité.

Figure 19 : Image issu du site https://www.bujarra.com/

6.2. Installation de NextCloud sur Proxmox

Nous avons décidé d'installer un serveur NextCloud sur une machine virtuelle **Proxmox**.
Les objectifs de cette installation sont les suivants :

- Installation de NextCloud sur une machine virtuelle Proxmox
- Configuration du serveur pour une utilisation interne uniquement
- Permettre l'accès au serveur NextCloud à partir d'un navigateur web

Nous avons installé **Snapd** pour gérer l'installation de Nextcloud et lancé la commande ***sudo snap install nextcloud***.

6.3. Configuration de NextCloud sur Proxmox

Nous avons configuré le serveur en suivant la documentation NextCloud pour une utilisation en interne uniquement. Nous avons exécuté la commande ***snap run nextcloud.occ config:system:set trusted_domains 1 --value=beerok1.com*** pour ajouter notre domaine et ainsi permettre l'accès à partir d'un navigateur web. Il est également possible d'y accéder par l'adresse IP du serveur.

6.4. Authentification LDAP

Nous avons configuré l'authentification **LDAP** en ajoutant l'appli ***LDAP user and group backend*** à NextCloud. Nous avons également renseigné les informations du serveur LDAP, notamment l'adresse IP, le nom d'utilisateur et le mot de passe. Nous avons également spécifié la base DN pour tester la base LDAP.

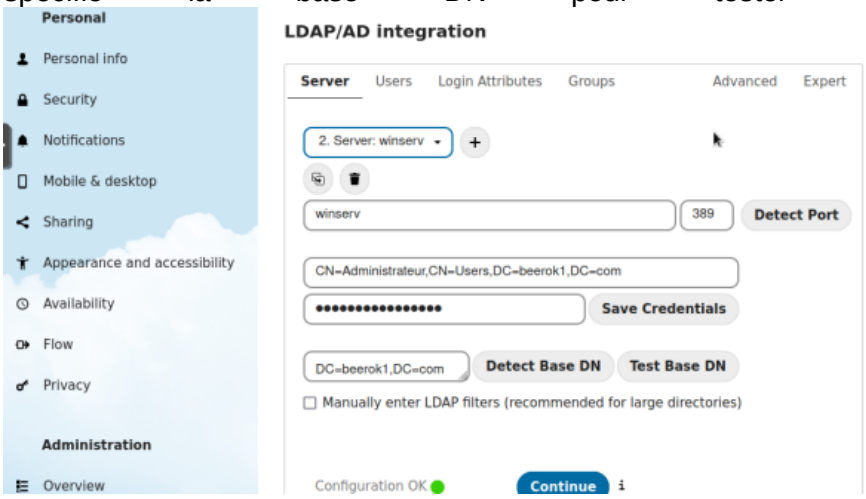


Figure 20 : Screenshot Authentification LDAP beerok1.com

6.5. Résultats NextCloud

Après avoir suivi ces étapes, nous avons réussi à installer NextCloud sur notre machine virtuelle Proxmox. De plus, nous avons configuré le serveur pour une utilisation en interne uniquement mais également autoriser l'accès à partir d'un navigateur web. Nous avons réalisé la configuration de l'authentification LDAP pour une intégration avec notre infrastructure existante.

Cette installation de NextCloud sur Proxmox a été un succès. Nous avons réussi à configurer le serveur pour une utilisation en interne, à permettre l'accès à partir d'un navigateur web. Ce serveur NextCloud sera un outil précieux pour les différentes équipes de l'entreprise, leur permettant de stocker et de partager des fichiers en toute sécurité et de manière efficace.

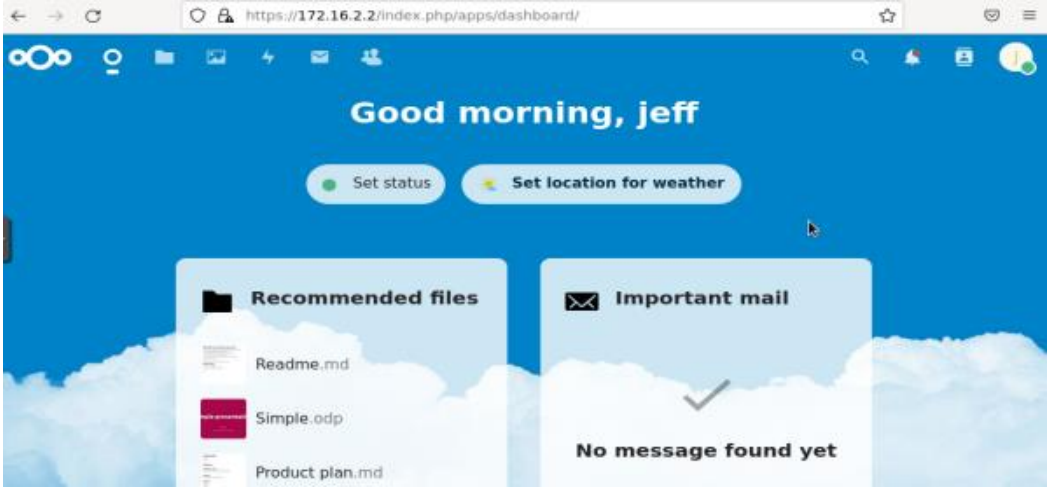


Figure 21 : Screenshot Page d'accueil depuis un client

7. Messagerie

7.1. Présentation de la Messagerie

L'installation d'une messagerie au sein d'une entreprise est une étape cruciale pour permettre une communication fluide et efficace entre les membres de l'organisation. En effet, la messagerie électronique permet une transmission rapide et sécurisée des informations, qu'il s'agisse de simples échanges de courriels ou de partage de documents importants. Ainsi, la mise en place d'une messagerie professionnelle constitue un outil indispensable pour favoriser la productivité et la collaboration au sein d'une entreprise.

Figure 22 : Page d'authentification Messagerie SquirrelMail

7.2. Installation et configuration de Postfix

La première étape a été de configurer Postfix, le MTA (Mail Transfer Agent) utilisé pour acheminer les messages. Nous avons commencé par installer Postfix sur le serveur, puis modifié le fichier de configuration principal pour définir les paramètres suivants :

- myhostname : le nom de domaine complet (FQDN) du serveur de messagerie (servMessagerie.beerok1.com).
- mydomain : le nom de domaine de l'entreprise (beerok1.com).
- mydestination : les noms d'hôtes et les domaines pour lesquels ce serveur de messagerie est considéré comme final.
- inet_interfaces : les interfaces réseau sur lesquelles Postfix écoute les connexions entrantes.

Par manque de temps nous n'avons pas pu configurer davantage la sécurité, pour éviter les spams et les attaques de phishing en utilisant des listes de blocage des adresses IP et des protocoles de sécurité TLS et SMTP AUTH.

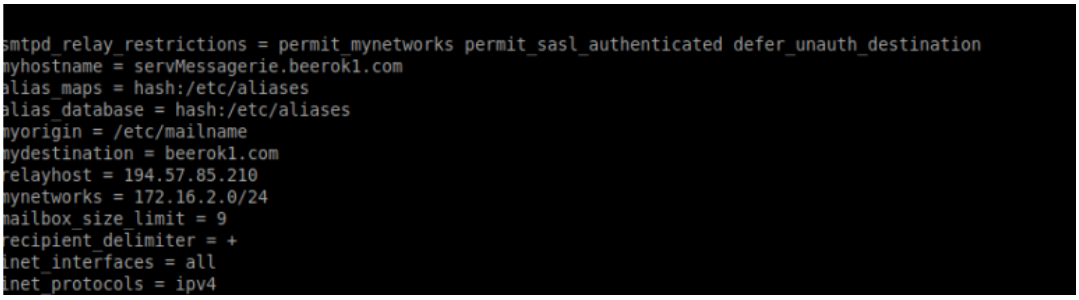


Figure 23 : Fichier de conf postfix “main.cf”

7.3. Installation et configuration de Dovecot

Une fois que Postfix a été configuré, nous avons installé Dovecot, le MDA (Mail Delivery Agent) utilisé pour stocker les messages sur le serveur de messagerie. Puis nous avons modifié le fichier de configuration de Dovecot pour définir les paramètres suivants :

- protocols : les protocoles de messagerie pris en charge (IMAP et POP3).
- mail_location : le répertoire de stockage des messages (/var/mail/%u).
- auth_mechanisms : les mécanismes d'authentification pris en charge (PLAIN et LOGIN).

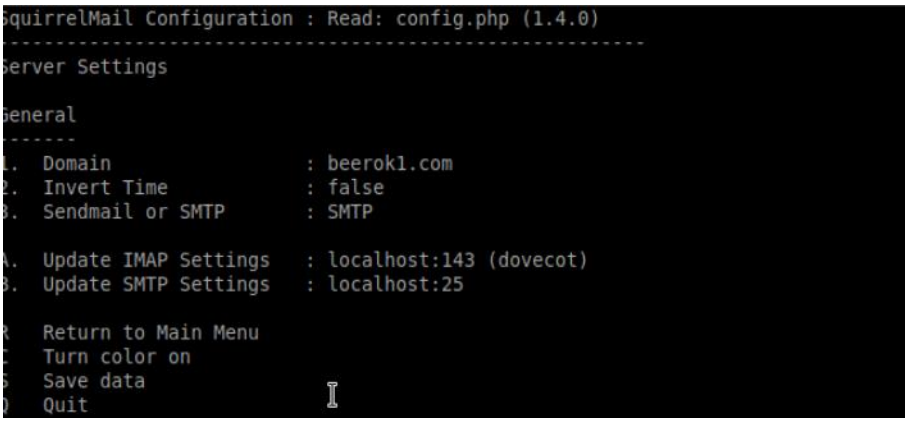
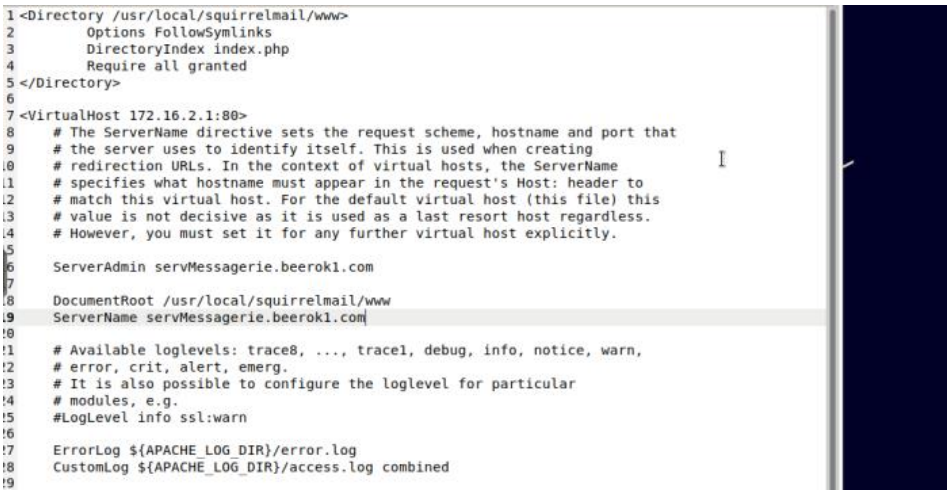


Figure 24 : Screenshot Dovecot “Server settings”

7.4. Installation et configuration de SquirrelMail

Après avoir configuré et testé le serveur de messagerie, nous avons installé SquirrelMail pour permettre aux utilisateurs de se connecter à leur boîte mail via une interface web conviviale. Pour installer SquirrelMail, nous avons d'abord installé les prérequis nécessaires tels que Apache, PHP et les modules PHP requis. Ensuite, nous avons téléchargé la dernière version de SquirrelMail depuis leur site web et l'ai installé sur le serveur.



```
<Directory /usr/local/squirrelmail/www>
        Options FollowSymlinks
        DirectoryIndex index.php
        Require all granted
</Directory>

<VirtualHost 172.16.2.1:80>
    # 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.

    ServerAdmin servMessagerie.beerok1.com

    DocumentRoot /usr/local/squirrelmail/www
    ServerName servMessagerie.beerok1.com

    # 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
```

Figure 25 : Fichier de configuration Server web Apache “001-squirrelmail.conf”

7.5. Résultats Messagerie

Après la configuration, nous avons testé l'interface webmail en accédant à partir de différents navigateurs web nous assurant que tout fonctionnait correctement. Nous avons rencontré un problème lors de l'envoi du mail, puisque ce dernier ne finissait pas sur la boîte de réception. Nous n'avons pas pu résoudre le problème par manque de temps, mais nous avons remarqué que certains mails restaient bloqués dans la file d'attente et cela pourrait être dû à un léger problème DNS ou encore un filtre anti-spam.

En somme, la mise en place de SquirrelMail va permettre aux utilisateurs de l'entreprise d'accéder facilement et rapidement à leurs emails à partir de n'importe quel navigateur web, ce qui améliorera leur productivité et leur efficacité dans la gestion de leurs emails. Le serveur utilise Postfix pour acheminer les messages et Dovecot pour stocker les messages sur le serveur. SquirrelMail quant à lui est une interface web permettant aux utilisateurs d'accéder aux fonctionnalités de messagerie fournies par Dovecot

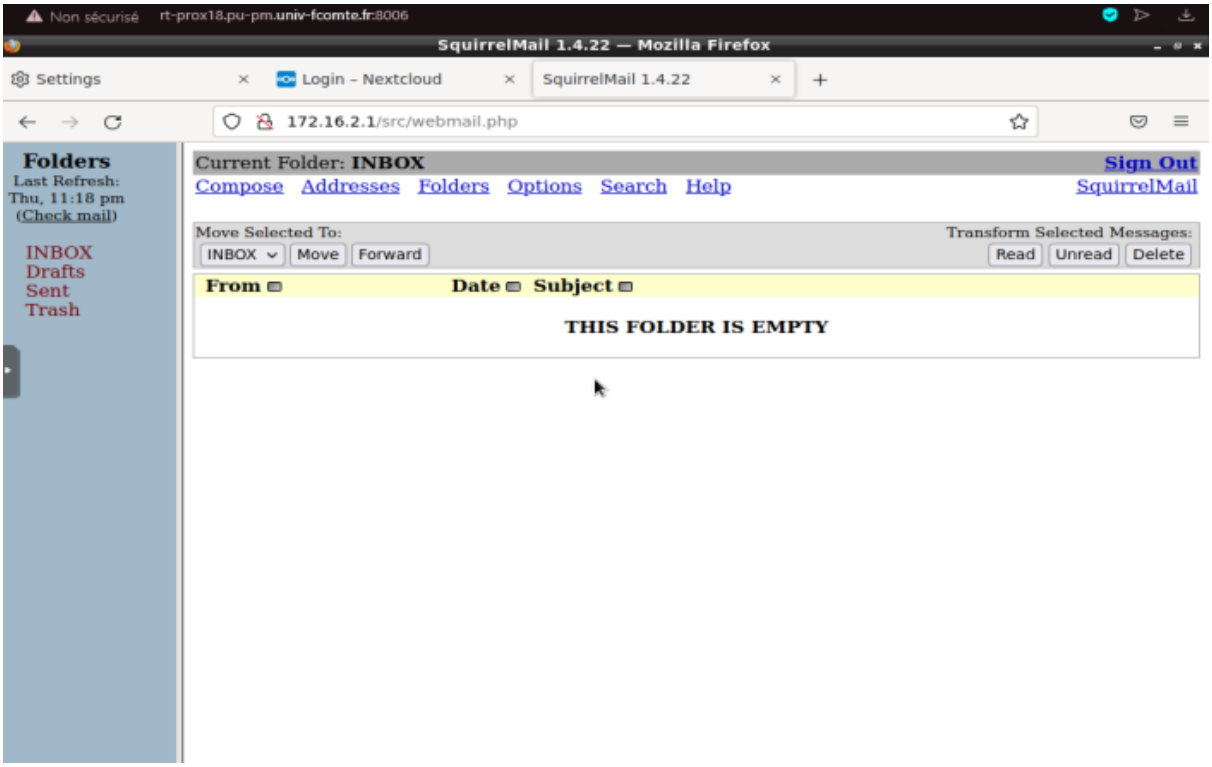


Figure 26 : Screenshot Page d'accueil depuis un client

8. Conclusion

Dans l'ensemble, le projet de création d'un réseau multi-site est un projet complexe et ambitieux qui demande une planification minutieuse, une conception précise et une mise en œuvre experte.

Le projet implique la sélection des protocoles appropriés pour garantir une connectivité fiable et sécurisée entre les différents sites, ainsi que la prise en compte des besoins en bande passante et en capacité de traitement et les exigences en matière de sécurité.

La gestion de projet efficace, la communication claire et régulière entre les parties prenantes, ainsi que la collaboration étroite entre les équipes techniques sont essentielles pour le succès de ce projet.

En fin de compte, la mise en place d'une infrastructure de réseau efficace permettra d'optimiser les communications entre les différents sites, d'améliorer la productivité et de réduire les coûts opérationnels pour les entreprises modernes.