

**Mise en place d’une passerelle et Firewall Linux**

**SOMMAIRE**

Table des matières

1. **Introduction**………………………………………………………………………………………………………………………………3
2. Une DMZ c’est quoi ?..................................................................................................................3
3. Contexte ………………………………………………………………………………………………………………………….……3
4. Besoin…………………………………………………………………………………………………………………………………… 3
5. Schéma…………………………………………………………………………………………………………………………………..3
6. **Mise en Place**…………………………………………………………………………………………………………………………….**4**
7. Mise en place réseau internet ……………..…………………………………………………………………………….4

1 -Paramétrage carte réseaux……………………………………………………………………………………………….4

2 -Paramétrage en mode Routeur…………………………………………………………………………………………4

1. Mise en place des services applicatif sur la DMZ…………………………………………………………………. 6
2. Installation des services
3. Configuration SSH Client
4. Configuration FTP Client
5. Configuration du serveur web sous apache2
6. **Mise en place du DNS……………………………..…………………………….…………………….9**
7. Installation et configuration de Bind9
8. Mise ne place des certificats de sécurité HTTPS
9. **Mise en place des Règles d’accès avec IpTables.……………………………………….……………………….…13** 1- Listing des demandes pour la création des règles.

# **Introduction**

## **Une DMZ c’est quoi ?**

En informatique, une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci ainsi que d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local.

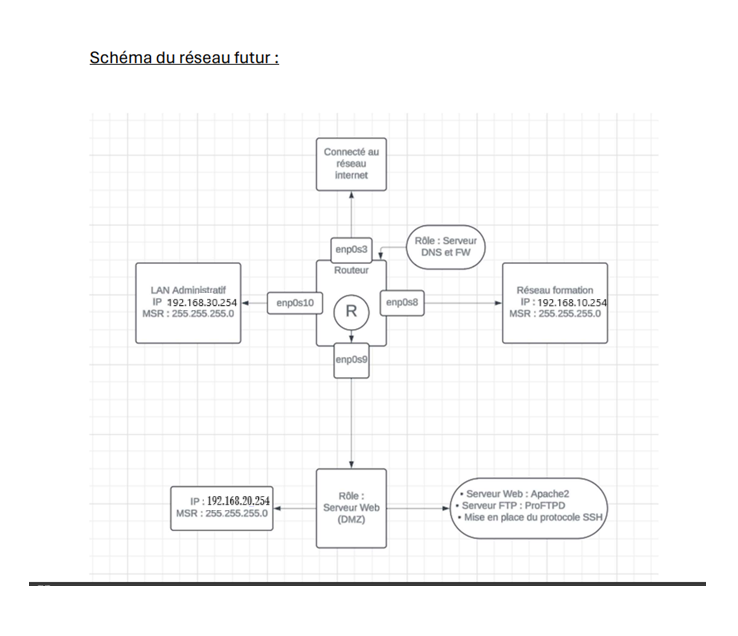
## **Contexte :**

Chargé par notre centre de formations de sécuriser l’infrastructure du réseau, nous allons mettre en place un réseau exclusif aux employer du centre, et eƯectuer la création d’un serveur web mutualiser pour les enseignes MBWay et DigitalScool du centre de formation.

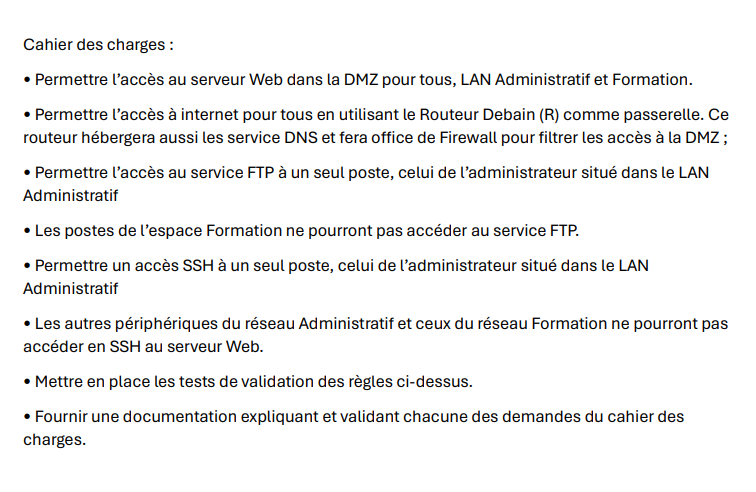
## **Besoin :**

Je voulais un système centralisé et pratique. Un moyen de rassembler tout mon contenu multimédia en un seul endroit, d'y accéder facilement depuis n'importe quel appareil et, idéalement, d'avoir une interface qui me permette de retrouver rapidement mes films et séries. Je voulais aussi éviter d'avoir à investir dans un abonnement à un autre service de streaming qui ne correspondrait pas forcément à mes goûts et à mes besoins.

## **d - Schéma :**



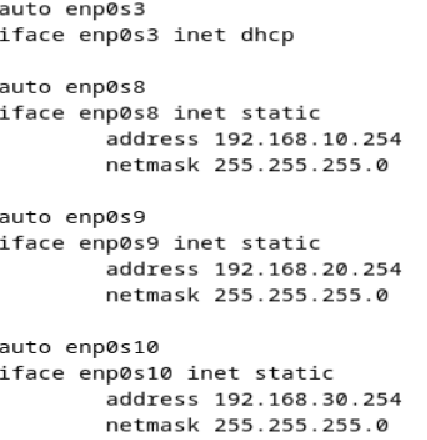
# **e-Cahier des charges**



# **Mise en place**

1. **Mise en place réseau Internet**
2. **Paramétrage cartes réseau**
3. On va commencer par configurer les cartes réseau

****

****

1. Faites de même pour les différentes machines à configurer

## **2-Paramétrage en mode routeur**

Pour le passage en mode routeur il y a deux étapes, l’activation du mode routeur et l’activation du NAT.

1. On va activer le mode routeur pour cela il faut entrer dans le fichier /etc/sysctl.conf et décommenter la ligne suivante :



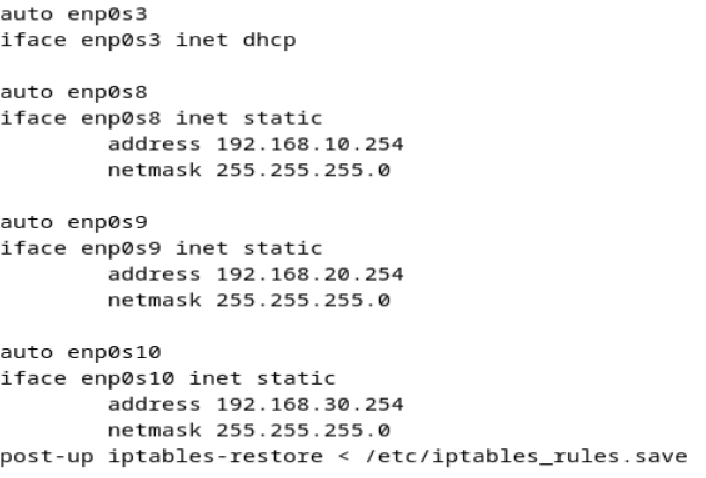
1. Ensuite on va activer le NAT, il faut donc installer l’extension iptables si elle n’est pas déjà installée



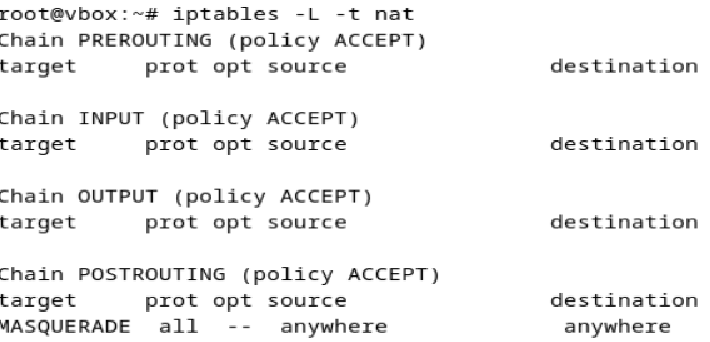


Faire attention à bien mettre les majuscules, pour la carte réseau prendre bien l’interface extérieur pour ce sujet ce sera enp0s3 du routeur.

1. Il faut maintenant ajouter une ligne dans le fichier /etc/network/interfaces pour pouvoir faire l’automatisation des règles iptables



1. Pour vérifier si les règles sont bien appliquées on va faire la commande qui suit :



1. **Mise en place des services applicatifs sur la DMZ**
2. **Installation des services**

Pour mettre en place les différents services nous avons besoin de plusieurs applications Apache2, ProFTPD, SSH.

1. Nous pouvons faire une installation grouper avec cette commande :



Pour l’installation il vous faudra internet, vous pouvez changer la configuration statique de l’adresse IP et la passer en DHCP pour que la connexion se fasse naturellement il vous faudra redémarrer la carte réseaux vous pouvez le faire avec ces commandes : Sudo ifdown enp0s3 Sudo ifup enp0s3

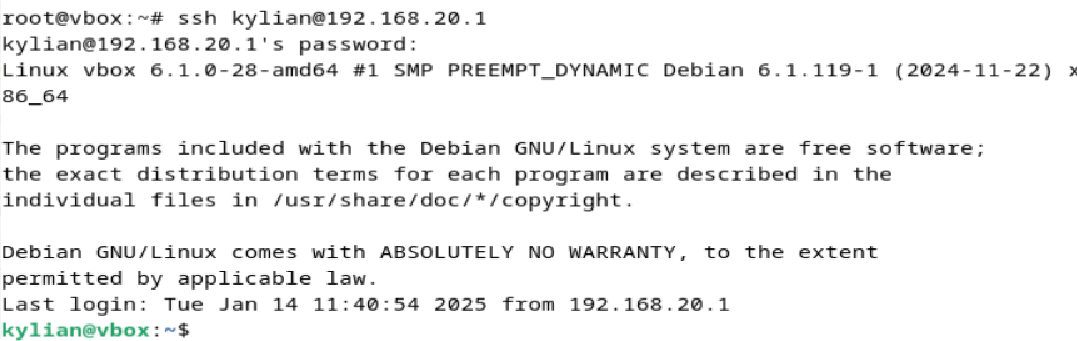
1. **Configuration SSH Client**

Configuration SSH Client Pour l’administrateur nous allons utiliser une machine sous Debian, donc nous allons configurer le SSH client sur le poste du réseau 192.168.30.254

1. Nous allons utiliser ssh-client pour l’installer, il faut donc taper la commande suivante :



Pour nous connecter il faut suivre le format suivant : Ssh @ La réponse attendue doit être comme ci-dessous :

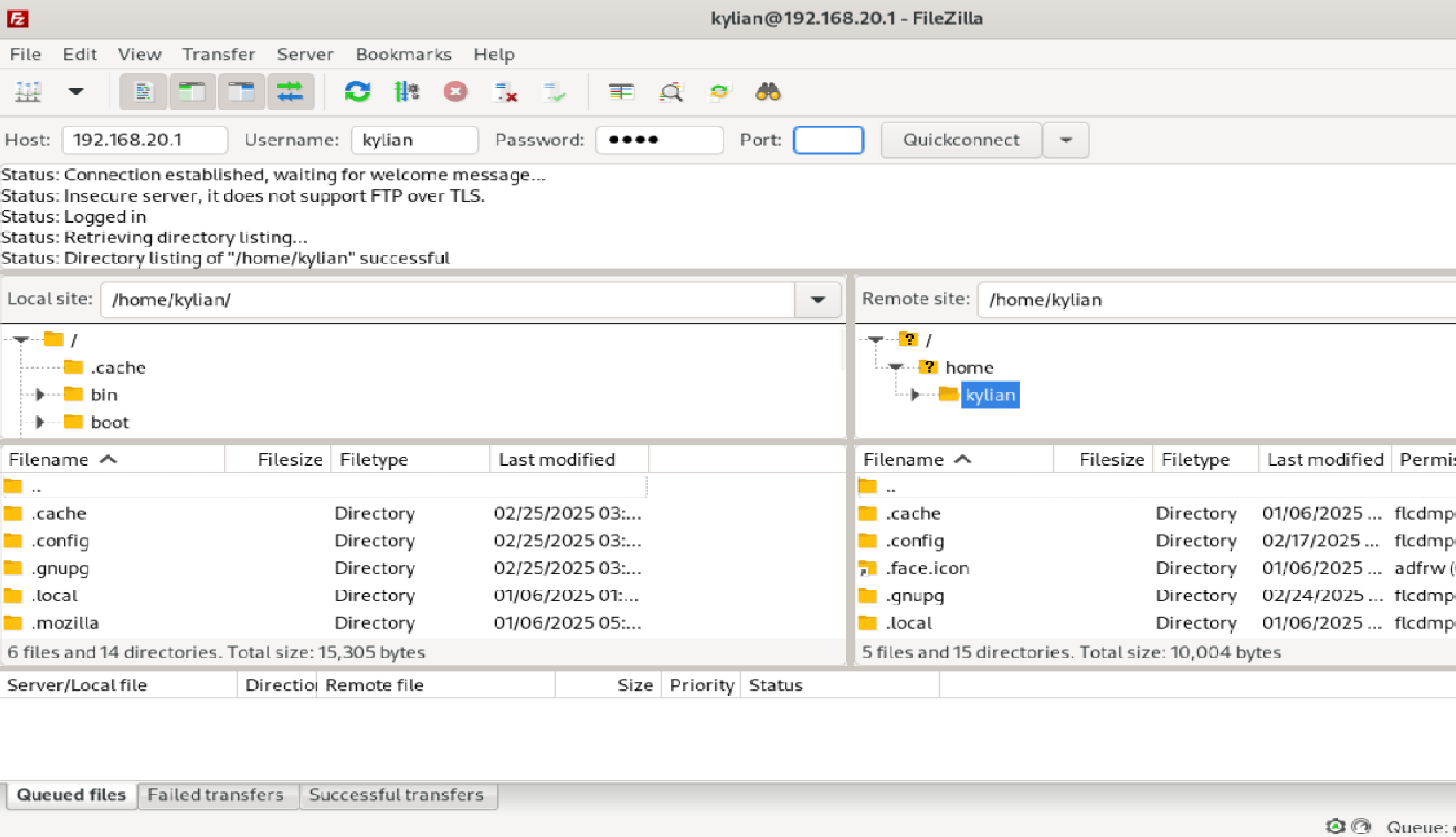


3. Configuration FTP Client

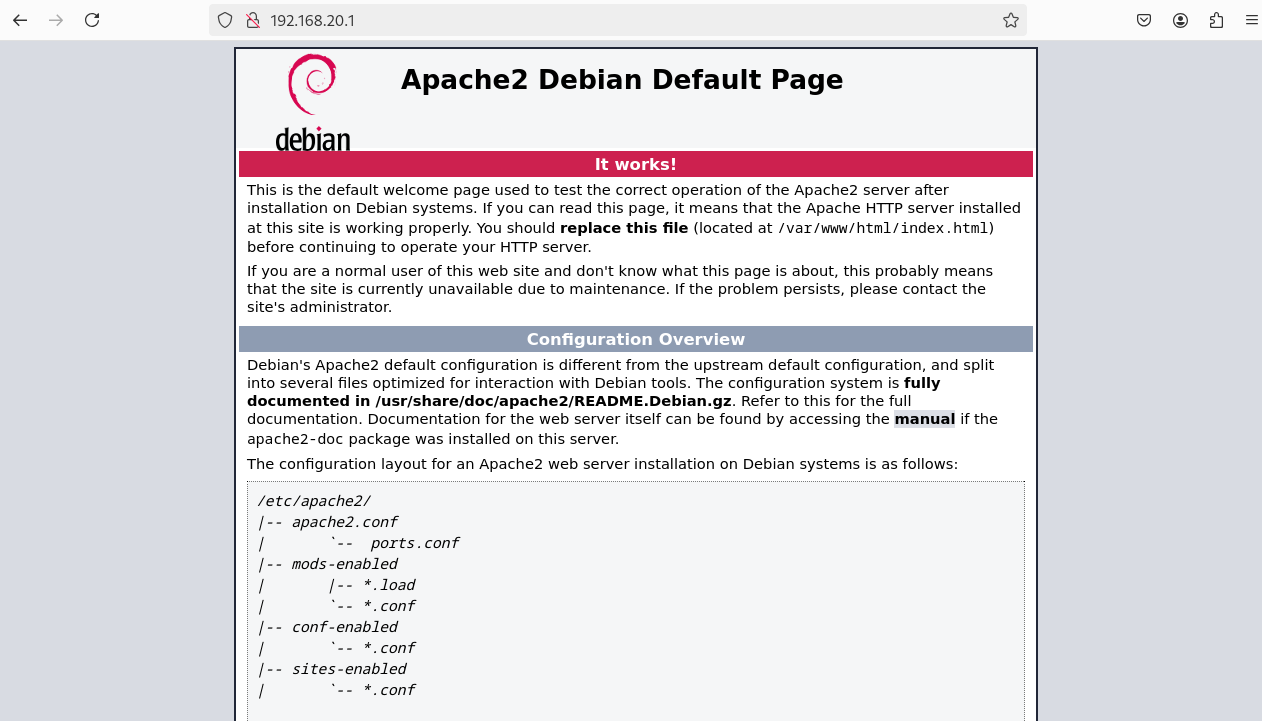
1. L’utilisation du serveur FTP passe par l’application Filezilla voici la commande pour le téléchargement :



1. Ensuite nous allons ouvrir l’application, pour se connecter au serveur nous allons avoir besoin de 3 éléments, remplir comme ci-dessous avec le résultat suivant :



1. Configuration du serveur web sous apache2 L’installation d’Apache est vérifiable en tapant l’adresse IP du serveur sur internet vous devriez voir la page standard « Apache2 Debian Default Page »



1. Ensuite nous allons créer un répertoire pour les 2 site avec les commandes :

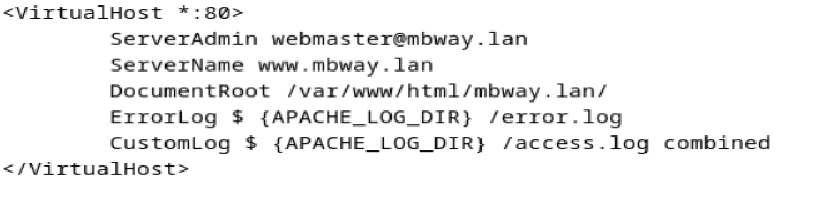




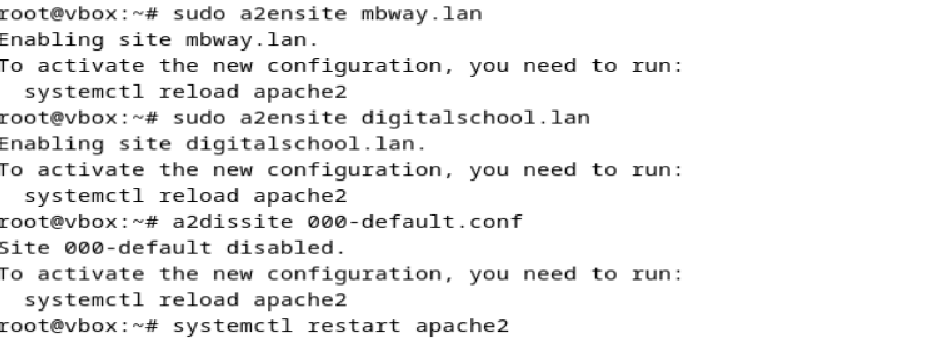
1. Nous allons maintenant configurer les Virtual Hosts en créant un fichier pour chaque site dans le répertoire 



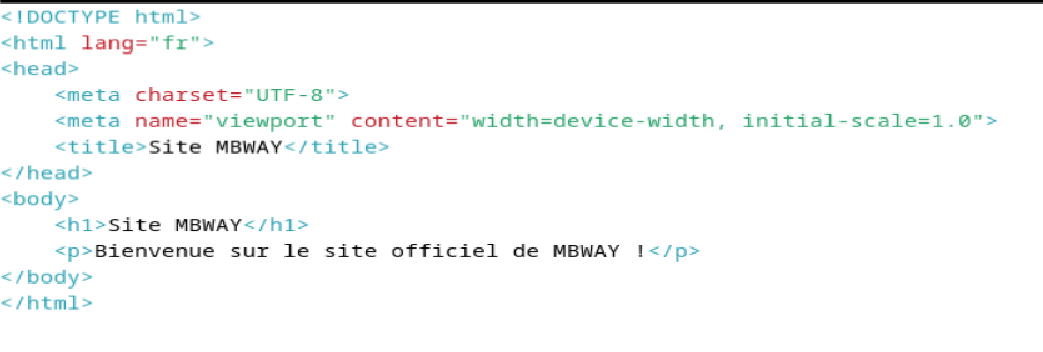
1. Ajoutez-y la configuration suivante en fonction du site :

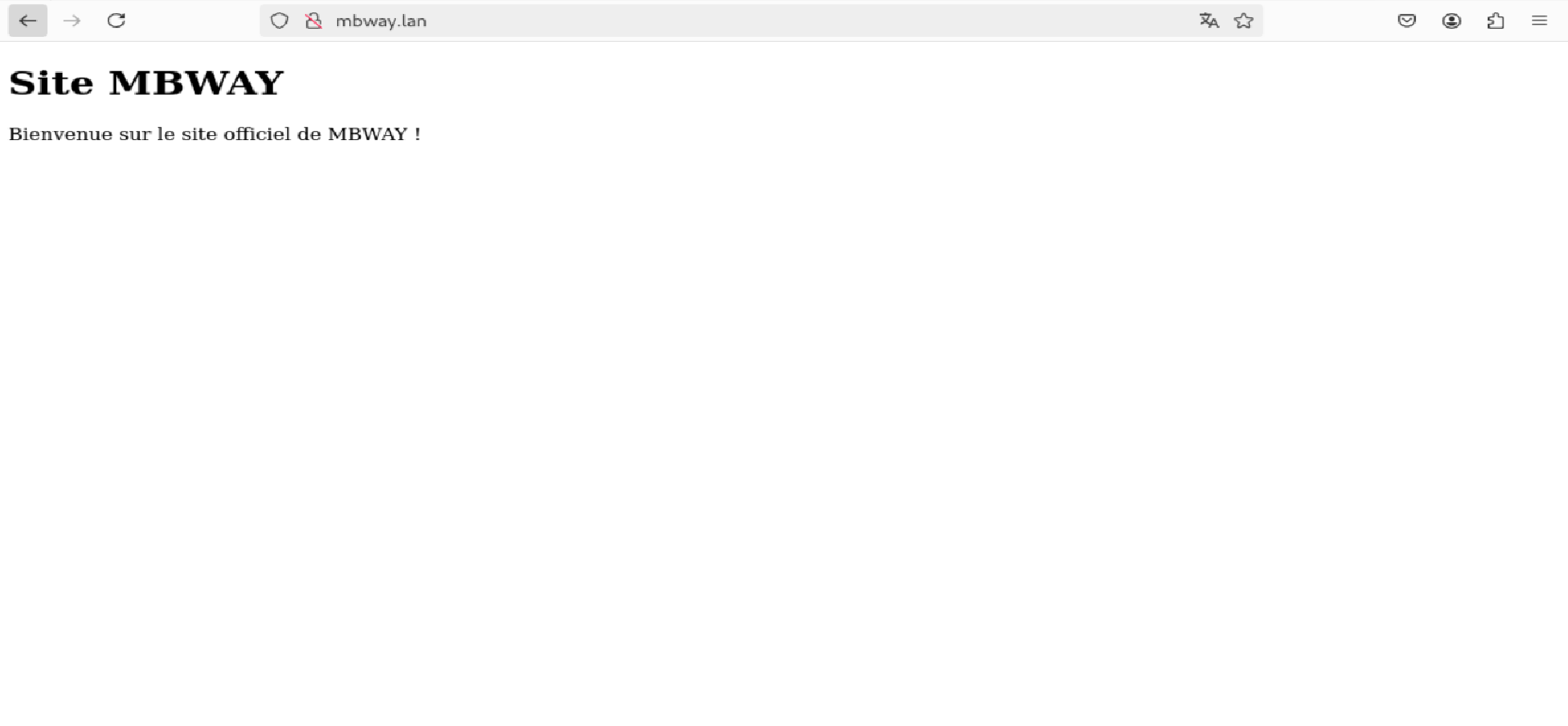


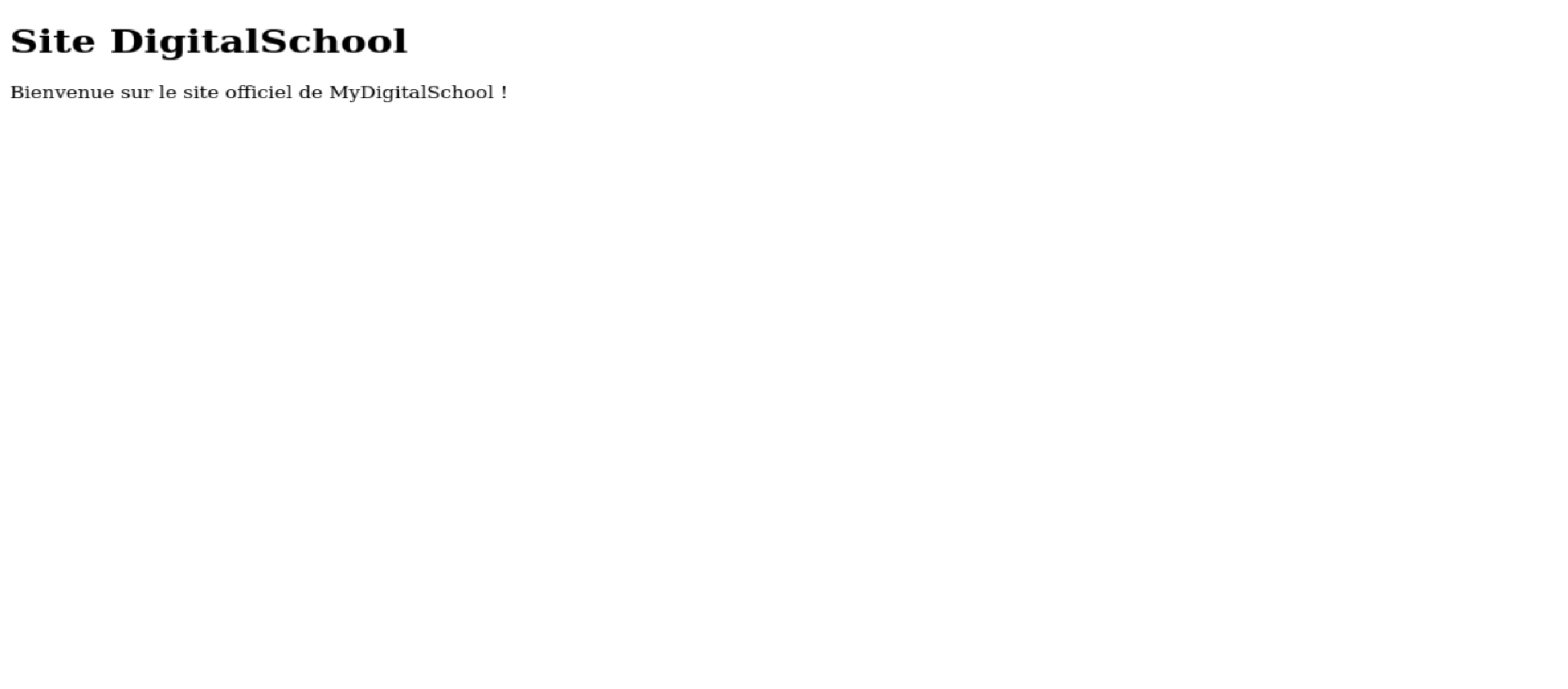
1. Ensuite on active les Virtual host avec la commande :



1. Nous allons maintenant créer la page du site index.html dans chaque répertoire, avec le model suivant :







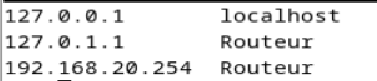
Bien sauvegarder le fichier, pour tester si tous cela fonction il suffit de taper dans la barre de recherche internet 172.10.0.2/mbway.lan.

3-Mise en place du DNS

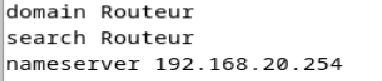
1. **Installation et configuration de Bind9**
2. Nous allons dans un premier temps nous allons identifier le nom du domaine avec la commande



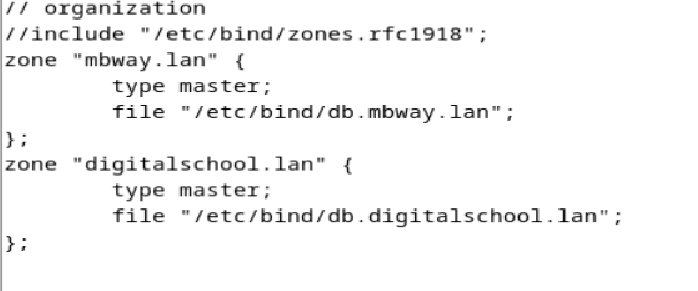
1. Il faut modifier le fichier /etc/hosts comme ci-dessous :



1. Après cela nous allons installer les paquets de bind9
2. Ensuite nous allons changer le nom du serveur DNS dans le fichier /etc/resolv.conf :

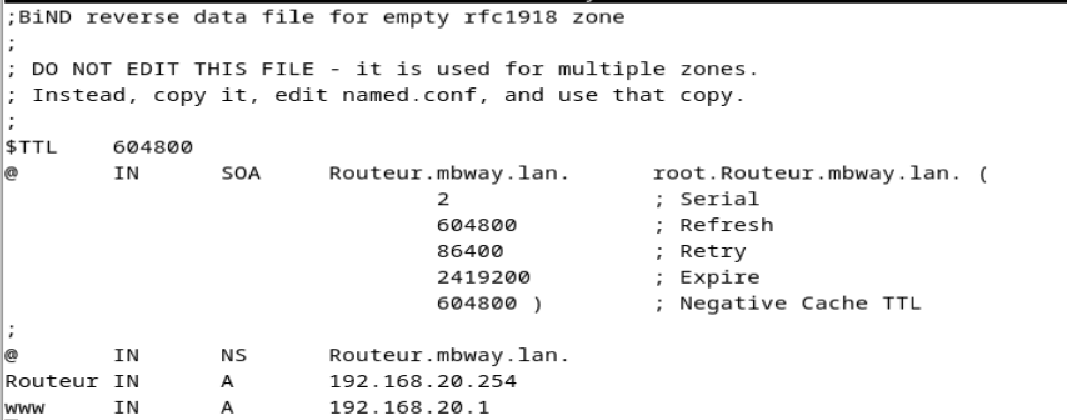


1. Il nous faut configurer maintenant les deux zones pour nos sites dans le fichier /etc/bind/named.conf.local :

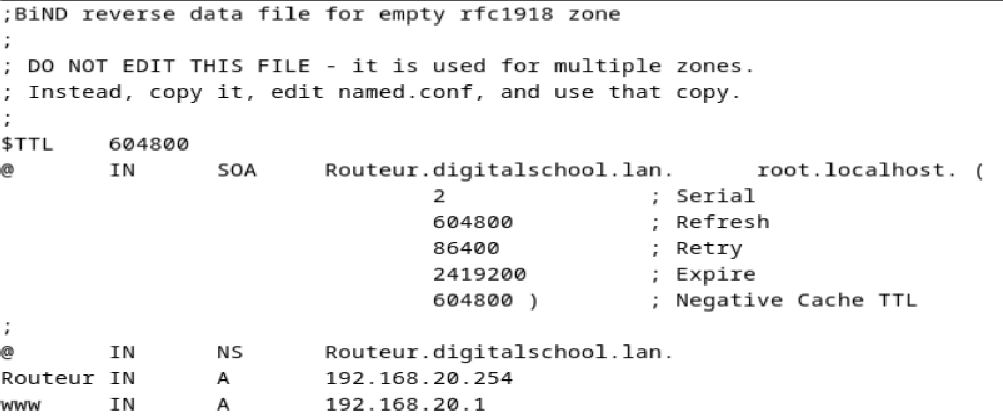


1. Maintenant on créer les fichiers de configuration des zones :

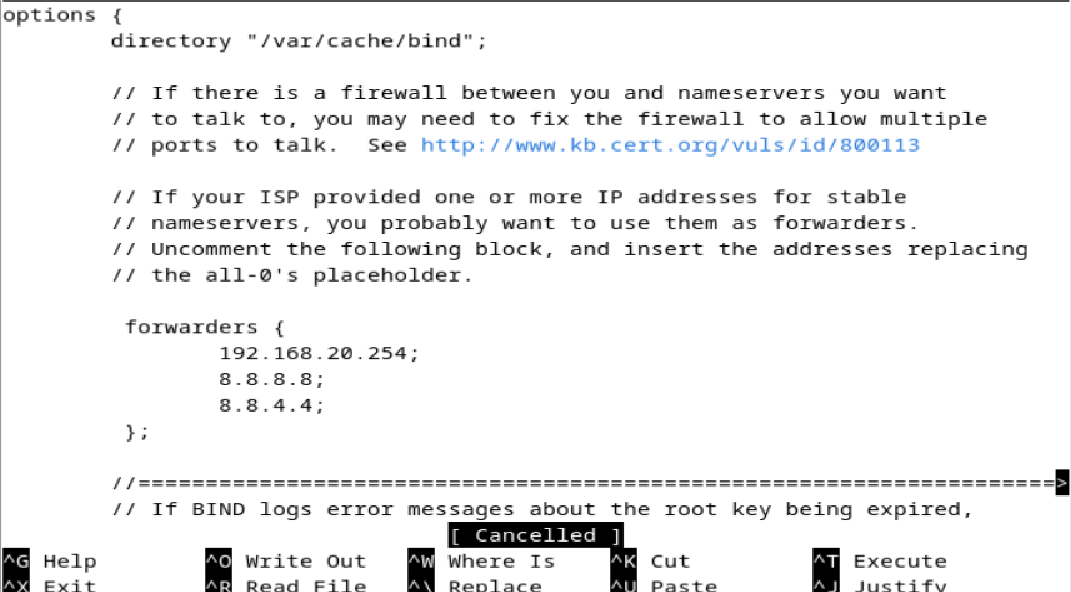








1. Il faut Integer le DNS dans le fichier /etc/bind/named.conf.options :



1. Après ses manipulations nous allons recharger le service bind9



1. Nous pouvons faire la vérification directement sur le routeur sur internet en tapans : <http://www.mbway.lan>

Pour que les configurations soit terminer il nous faudra changer les fichier /etc/resolv.conf dans les diƯérent poste comme ci-dessous : 2. Mise ne place des certificats de sécurité HTTPS 3. Pour la mise en place de la sécurisation des sites web, nous allons activer le mod ssl avec la commande : Sudo a2enmod ssl Pour déclarer les certificat ssl nous devons copier le fichier etc/apache2/sitesavaibles/default-ssl.conf , les remplir avec les bon chemin comme si dessous : Ensuite il faut activer les deux certificats avec la commande : Sudo a2ensite mbway.lan-ssl.conf Sudo a2ensite digitalschool.lan-ssl.conf Puis redémarrer le serveur apache2 : Sudo service apache2 restart Tester les diƯérentes pages vous devrez avoir un message d’avertissement accepter le risque : Comme résultat vous devrait avoir comme les captures d’écran si dessous. Mise en place des Règles d’accès avec IpTables. 1. Listing des demandes pour la création des règles. Pour les règles nous devons autoriser : - L’accès aux sites a tout le monde (port 443) - L’accès du poste administrateur (192.168.1.1) au server ftp et ssh (port 21 et 22) Il nous faut bloquer tout le reste des échanges. Nous allons suivre plusieurs commandes pour supprimer les règles installer : Sudo iptables -F Pour la suite nous allons mettre en place les règles autorisant internet : iptables -A FORWARD -s 192.168.1.0/24 -p tcp --dport 443 -j ACCEPT iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 443 -j ACCEPT iptables -A FORWARD -s 172.10.0.0/24 -p tcp --dport 443 -j ACCEPT iptables -A OUTPUT -p udp -j ACCEPT Access FTP et SSH pour le poste administrateur : iptables -A FORWARD -s 192.168.1.1 -p tcp --dport 21 -j ACCEPT Iptables -A FORWARD -s 192.168.1.1 -p tcp --dport 22 -j ACCEPT Enfin nous allons bloquer les accès qui ne sont pas dans les règles : iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 21 -j DROP iptables -A FORWARD -s 192.168.1.0/24 -p tcp --dport 21 -j DROP iptables -A FORWARD -s 172.10.0.0/24 -p tcp --dport 21 -j DROP iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 22 -j DROP iptables -A FORWARD -s 192.168.1.0/24 -p tcp --dport 22 -j DROP iptables -A FORWARD -s 172.10.0.0/24 -p tcp --dport 22 -j DROP