

**Mise en place d’une passerelle et d’une DMZ sous Debian**

**Sommaire**

INTRODUCTION .......................................................................................................................................

CONTEXTE................................................................................................................................................

OBJECTIF..................................................................................................................................................

EXIGENCE.................................................................................................................................................

SOLUTION ...............................................................................................................................................

Schéma.................................................................................................................................................

MISE EN PLACE........................................................................................................................................

A) Serveur & Routeur.............................................................................................................................

1. *Configuration des cartes réseaux...............................................................................*
2. *Configuration du routage...........................................................................................*
3. *Configuration et installation du DNS..........................................................................*

*B) Serveur Web......................................................................................................................................*

1. *Mise en place de Debian 12.......................................................................................*
2. *Mise en œuvre et paramétrage de PHP.....................................................................*
3. *Installation et configuration MariaDB.......................................................................*
4. *Élaboration des répertoires du site web....................................................................*
5. *Établissement des VirtualHosts..................................................................................*
6. *Mise en service de la sécurité HTTPS.........................................................................*
7. *Installation et configuration du service SSH..............................................................*
8. *Installation et configuration ProFTP..........................................................................*

C) Intégration d’une DMZ...................................................................................................................

1. *Mise en place d’une DMZ.......................................................................................*
2. *Création des règles de filtrage................................................................................*

CAHIERS DES RECETTES...........................................................................................................................

1. *Connexion serveur web .............................................................................................................*
2. *Connexion SSH...........................................................................................................................*
3. *Connexion FTP FileZilla...............................................................................................................*

CONCLUSION...........................................................................................................................................

|  |
| --- |
| INTRODUCTION |

Notre centre de formation regroupant plusieurs enseignes à disposition des élèves MBWay et DigitalSchool un serveur Web hébergeant un intranet pour chaque département.

|  |
| --- |
| CONTEXTE |

Dans sa première version, les sites répertoriant les activités et actualités de chaque enseigne étaient hébergées dans le LAN administratif

Pour donner suite à quelques tentatives d’intrusion dans les serveurs locaux du réseau administratif, il a été décidé de sécuriser celui-ci en le limitant strictement aux employés

|  |
| --- |
| OBJECTIF |

La solution qui a été retenue est de créer un sous-réseau nommé DMZ pour hébérger les services partagés par le personnel et les stagiaires (Formation). A termes, ce réseau DMZ devrait être accessible depuis Internet.

Le serveur Web héberge un site pour chaque établissement. Pour sécuriser les transactions les sites ne doivent être accessibles qu’en https soit https://www.mbway.lan ou https://www.digitalschool.lan. Les sites web sont accessibles à TOUS.

Dans le cadre d’un stage, vous avez été chargé par votre centre de formation de mettre en place une maquette, au moindre coût, pour montrer la faisabilité de la solution. Vous avez à votre disposition un ancien serveur que vous pouvez recycler pour héberger des machines virtuelles.

|  |
| --- |
| BESOIN |

Voici les éléments dont nous aurons besoin pour répondre au cahier des charges.

2 VM Debian 12 pour nous libre à vous de choisir, qui nous servirons de ROUTEUR et de SERVEUR.

2 VM sous Windows 10 utilisé en tant que Poste CLIENT et qui nous seront utile pour réaliser par la suite pour réaliser nos tests.

Don une qui nous servira pour accéder au le LAN Administratif depuis notre poste client et une autre pour le LAN Formation.

Pour pouvoir répondre au cahier des charges ci-dessous :

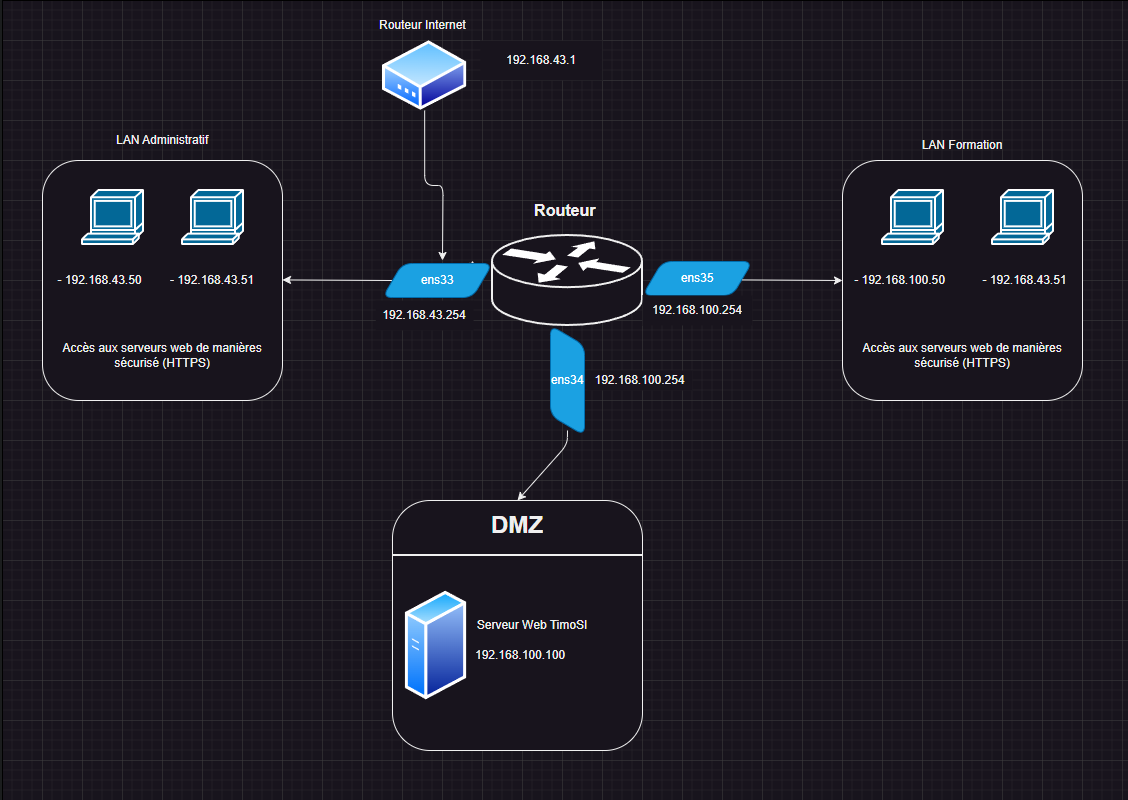
1. Permettre l’accès au serveur Web dans la DMZ pour tous, LAN Administratif et Formation.
2. Permettre l’accès à internet pour tous en utilisant le Routeur Debian (R) comme passerelle. Ce routeur hébergera aussi les service DNS et fera office de Firewall pour filtrer les accès à la DMZ ;
3. Permettre l’accès au service FTP à un seul poste, celui de l’administrateur situé dans le LAN Administratif • Les postes de l’espace Formation ne pourront pas accéder au service FTP.
4. Permettre un accès SSH à un seul poste, celui de l’administrateur situé dans le LAN Administratif
5. Les autres périphériques du réseau Administratif et ceux du réseau Formation ne pourront pas accéder en SSH au serveur Web. • Mettre en place les tests de validation des règles ci-dessus.
6. Fournir une documentation expliquant et validant chacune des demandes du cahier des charges

|  |
| --- |
| SOLUTION |

Pour satisfaire les exigences des écoles, nous allons mettre en place deux sites web hébergés sur un serveur web (WebTimoSI) situé dans une zone démilitarisée (DMZ) :

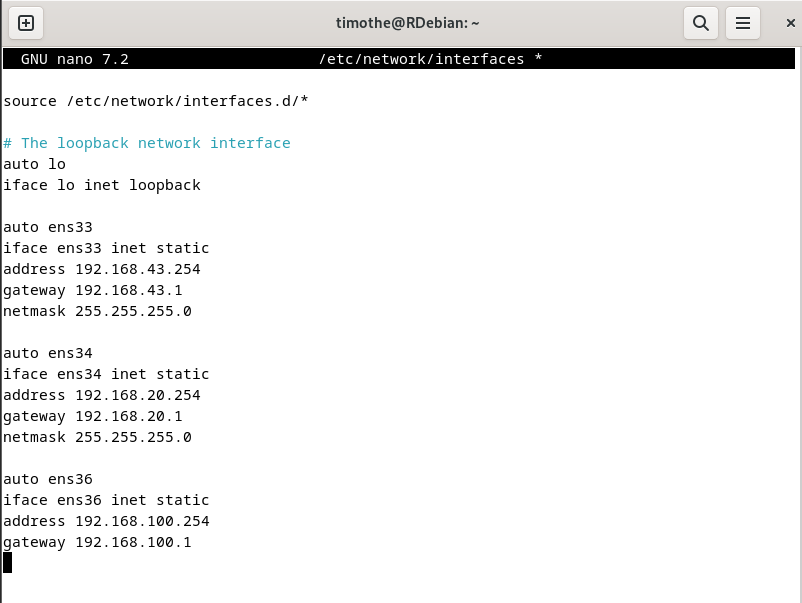
Chaque établissement disposera d'un site web dédié sur ce serveur. Afin d'assurer la sécurité des transactions, les sites seront uniquement accessibles via le protocole HTTPS, à savoir https://www.mbway.lan et https://www.digitalschool.lan. Ces sites web seront accessibles à tous les utilisateurs.

Schéma de solution proposé tous en répondant au cahier des charges :



1. **MISE EN PLACE**
2. **Serveur & Routeur**

Configuration des interfaces réseaux via la commande : */etc/network/interfaces*



|  |  |  |  |
| --- | --- | --- | --- |
| LAN Administratif | eth0 | ens33 | 192.168.43.0 |
| LAN Formation | eth1 | ens34 | 192.168.110.0 |
| Serveur Web | eth2 | ens35 | 192.168.100.0 |

1. **Configuration du routage**

Nous allons activer le routage des paquets sur notre serveur Linux pour que celui-ci se comporte comme un routeur (une passerelle).

Pour cela, modifiez le fichier :

|  |
| --- |
| *nano /etc/sysctl.conf* |

Et décommentez la ligne : *"net.ipv4.ip\_forward=1"*

Ensuite, modifiez le fichier

|  |
| --- |
| *nano /etc/rc.local* |

Et ajoutez ceci avant la ligne "exit"

|  |
| --- |
| *. /sbin/iptables -P FORWARD ACCEPT*  */sbin/iptables --table nat -A POSTROUTING -o ens33 -j MASQUERADE* |

Maintenant, à chaque démarrage, ces 2 lignes seront exécutées et le pare-feu de Linux acceptera donc de routeur les paquets entre nos 3 interfaces réseau (cartes réseau).

Redémarrer votre serveur pour appliquer les changements :

|  |
| --- |
| *Systemctl reboot* |

*Nous activons le routage de manière définitive en suivant la méthode suivante :*

|  |
| --- |
| *Sudo nano /etc/sysctl.d/routeur.conf* |

On positionne cette ligne :

|  |
| --- |
| *net.ipv4.ip\_forward=1* |

On enregistre et on quitte On valide :

|  |
| --- |
| *sysctl -p /etc/sysctl.d/routeur.con* |

1. **Installation Service DNS**

Prérequis à la l'installation d'un DNS :

Il s'agit là de la partie cliente du système sur lequel va être installé Bind. Un même système peut être à la fois client et serveur, c'est-à-dire, serveur DNS “pour lui-même”.

|  |
| --- |
| *nano /etc/host*  *conf order hosts, bind*  *multi on* |

Il s'agit là encore de l'aspect client du système. On renseigne tous les clients du réseau local. On renseigne aussi le nom de domaine de ce système en tant que client.

|  |
| --- |
| *nano /etc/hosts* |

|  |
| --- |
| 127.0.0.1 localhost.mbway.lan localhost  127.0.0.1 localhost.digitalschool.lan localhost  192.168.100.100 Server Web  192.168.110.50 PC 1 Test formation  192.168.110.51 PC 2 Test formation  192.168.43.50 PC 1 Test administration  192.168.43.51 PC 1 Test administration |

Il faut déclarer un nom de domaine dans /etc/resolv.conf. Et retirer les DNS extérieurs, afin que Bind soit consulté.

|  |
| --- |
| *domain mbway.lan*  *search mbway.lan*  *nameserver 192.168.100.100*  *domain mydigitalschool.lan*  *search mydigitalschool.lan*  *nameserver 192.168.100.100* |

**Redémarrer le réseau :**

|  |
| --- |
| */etc/init.d/networking start* |

**Installation des packets:**

|  |
| --- |
| *apt-get update apt-get install bind9* |

**Configuration de bind:**

On créer les fichiers “/etc/bind/db.mbway.lan ” et “/etc/bind/db.mydigitalschool.lan ” :

|  |
| --- |
| *cp /etc/bind/db.local /etc/bind/db.mbway.lan*  *cp /etc/bind/db.local /etc/bind/db.mydigitalschool.lan* |

Une fois nos deux fichiers éditaient et configuré comme souhaiter on redémarrera alors le service de bind9.

|  |
| --- |
| *Systemctl restart bind9* |

1. **SERVEUR WEB**
2. **Mise en place de Debian 12**

Configuration ip statique dans le fichier : */etc/network/interfaces*

INSTALLATION APACHE :

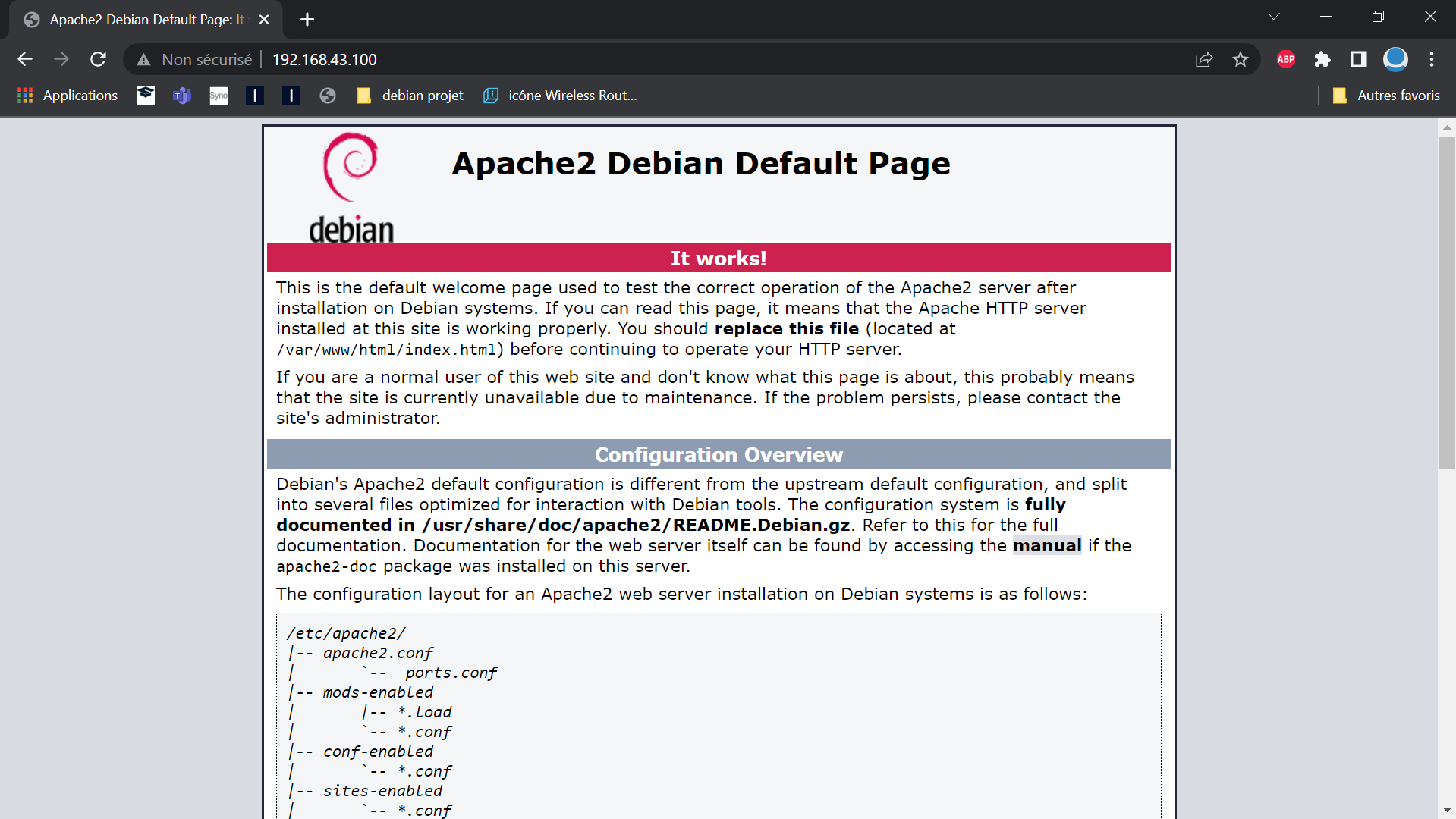
|  |
| --- |
| *sudo apt-get update*  *sudo apt-get install -y apache2*  *systemctl enable apache2* |

Nous activons les modules suivants :

* Le module "deflate" pour la gestion de la compression, notamment en gzip, pour utiliser la mise en cache des pages sur votre site
* Le module "headers" afin de pouvoir agir sur les en-têtes http
* Et pour finir le module "ssl" pour gérer les certificats SSL et donc l'utilisation du protocole HTTPS

Pour ce faire, voici les commandes :

|  |
| --- |
| *sudo a2enmod rewrite*  *sudo a2enmod deflate*  *sudo a2enmod headers*  *sudo a2enmod ssl*  *systemctl restart apache2* |



1. **Mise en œuvre et paramétrage de PHP**

|  |
| --- |
| *Sudo apt get install –y php*  *Sudo apt get install –y php-pdo php-mysql php-zip php-gd php-mbstring php-curl php-xml php-pear php-bcmath* |

1. **Installation et configuration MariaDB**

Pour ce faire on utilisera les commandes tel :

|  |
| --- |
| *Sudo apt-get install –y mariadb-server*  *Sudo mariadb-secure\_installation* |

1. **Élaboration des répertoires du site web**

Dans cette rubrique nous verrons comment crée les dossiers de sorte à pouvoir héberger nos deux sites.

|  |
| --- |
| *cd/var/www/html*  *Mkdir digitalschool*  *Cd digitalschool*  *Nano/cd/var/www/html/digitalschool.lan/digitalschool.lan.html* |

|  |
| --- |
| *Cd/var/www/html*  *Mkdir digitalschool*  *Cd mbway.lan*  *Nano/cd/var/www/html/mbway.lan/mbway.lan.html* |

Pour Digitalschool :

Une fois nos dossiers compléter et modifier, nous pouvons récupère l’accès via l’URL ci-dessous :

http://192.168.43.10/digitalschool/digitalschool.html

Pour Mbway :

http://192.168.43.10/digitalschool/digitalschool.html

1. **Établissement des VirtualHosts**

Passons ensuite à l'activation de nos deux sites :

|  |
| --- |
| *sudo a2ensite digitalschool.conf*  *sudo a2ensite mbaway.lan* |

Si l’on veut effectuer une suppression :

|  |
| --- |
| *a2dissite digitalschool.conf*  *a2dissite mbaway.lan* |

N’oubliez pas de redémarrer le service Apache après avoir effectué ces modifications :

|  |
| --- |
| *sudo systemctl restart apache2.service* |

1. **Mise en service de la sécurité HTTPS**

*Nous mettons en place le service HTTPS, cella grâce à l’outils OpenSSH au préalable installé.*

*Voici les commandes à insérer :*

|  |
| --- |
| *sudo a2enmod ssl*  *sudo a2ensite default-ssh* |

1. **Installation et configuration du Serveur SSH**

Pour cela nous procédons en premier par l'installation :

|  |
| --- |
| *apt-get update*  *apt-get install openssh-server* |

*On édite ensuite le fichier OpenSSH :*

|  |
| --- |
|  |

1. ***Installation et configuration du serveur FTP***

*Installation du serveur FTP*

|  |
| --- |
| *Sudo apt-get install proftpd* |

*Configuration du serveur FTP*

|  |
| --- |
| *Nano/etc/proftpd/proftpd.conf* |

*Création d’un utilisateur FTP :*

|  |
| --- |
| *Sudo echo “bin/false” >> /etc/shells*  *Sudo adduser admin 1* |

*Activation SSL dans ProFTPD*

|  |
| --- |
| *Apt-get install openssl* |

# Nous utiliserons l’outil FileZilla afin de tester si notre connexion au serveur ProFTPD.

# Nous autorisons seulement le poste “admin1” :

1. **INTEGRATION D’UNE DMZ**

1. Mise en place d’une DMZ

Pour ce faire nous allons procéder étapes par étapes :

1) Pour la suppression de règles de filtrages déjà existante

|  |
| --- |
| *Iptables-L* |

2) Nous mettons toutes les regles de filtrage par défaut

On bloque les trames traversant le routeur :

|  |
| --- |
| *Iptables-P FORWARD DROP* |

On bloque toutes les trames entrant dans le routeur :

|  |
| --- |
| *Iptables-P INPUT DROP* |

On accepte les trames sortant du routeur :

|  |
| --- |
| *Iptables-P OUTPUT ACCEPT* |

3) Autoriser le trafic établi :

|  |
| --- |
| *Iptables-A FORWARD –m state -- ESTABLISHED –j ACCEPT*  *Iptables-A INPUT –m state -- ESTABLISHED –j ACCEPT*  *Iptables –A OUTPUT –m state -- ESTABLISHED –j ACCEPT* |

4) Règle de filtrage du LAN vers la DMZ et réglage du routeur vers le WAN

Le but est de permettre à toutes les données quittant le réseau local d'interagir avec toutes les zones de notre configuration initiale.

|  |
| --- |
| *Iptables –A FORWARD –i ens33-j ACCEPT* |

*Par la suite nous accepterons les trames d’entre du LAN vers le Routeur avec la commande ci-dessous*

|  |
| --- |
| *Iptables-A INPUT –i ens33 –j ACCEPT* |

5) Règle de filtrage de la DMZ vers le WAN

|  |
| --- |
| *Iptables –A FORWARD –i ens35 –o ens33 –j ACCEPT* |

6) Autorisation des trames du WAN vers le Serveur WEB

Lorsque le serveur web envoie des paquets, il est crucial que le destinataire puisse lui répondre. C'est pourquoi il est essentiel d'ajouter ce paramètre au script.

|  |
| --- |
| *Iptables-A FORWARD –i ens33 –o ens35-d 192.168.100.100-p tcp –dport 80-j ACCEPT* |

7) Permettre l'accès en consultation au serveur web depuis l'extérieur

|  |
| --- |
| *Iptables-t nat –A PREROUTING –i ens35 –p tcp—dport 80 –j DNAT – to destination 192.168.100.100* |

8) Sauvegarde de la configuration sur les règles de filtrages

|  |
| --- |
| *Iptables-persistent* |

1. CREATION DU FICHIER DES REGLES DE FILTRAGE

1) Création du dossier et du fichier

Pour le dossier :

|  |
| --- |
| *Mkdir/root/scripts* |

Pour le fichier :

|  |
| --- |
| *Nano/root/scripts/scripts\_filtrage* |

2) Rendre le fichier note en un script

|  |
| --- |
| *#!/bin/sh* |

Pour résumer nous devons avoir quelque chose de cette forme-là :

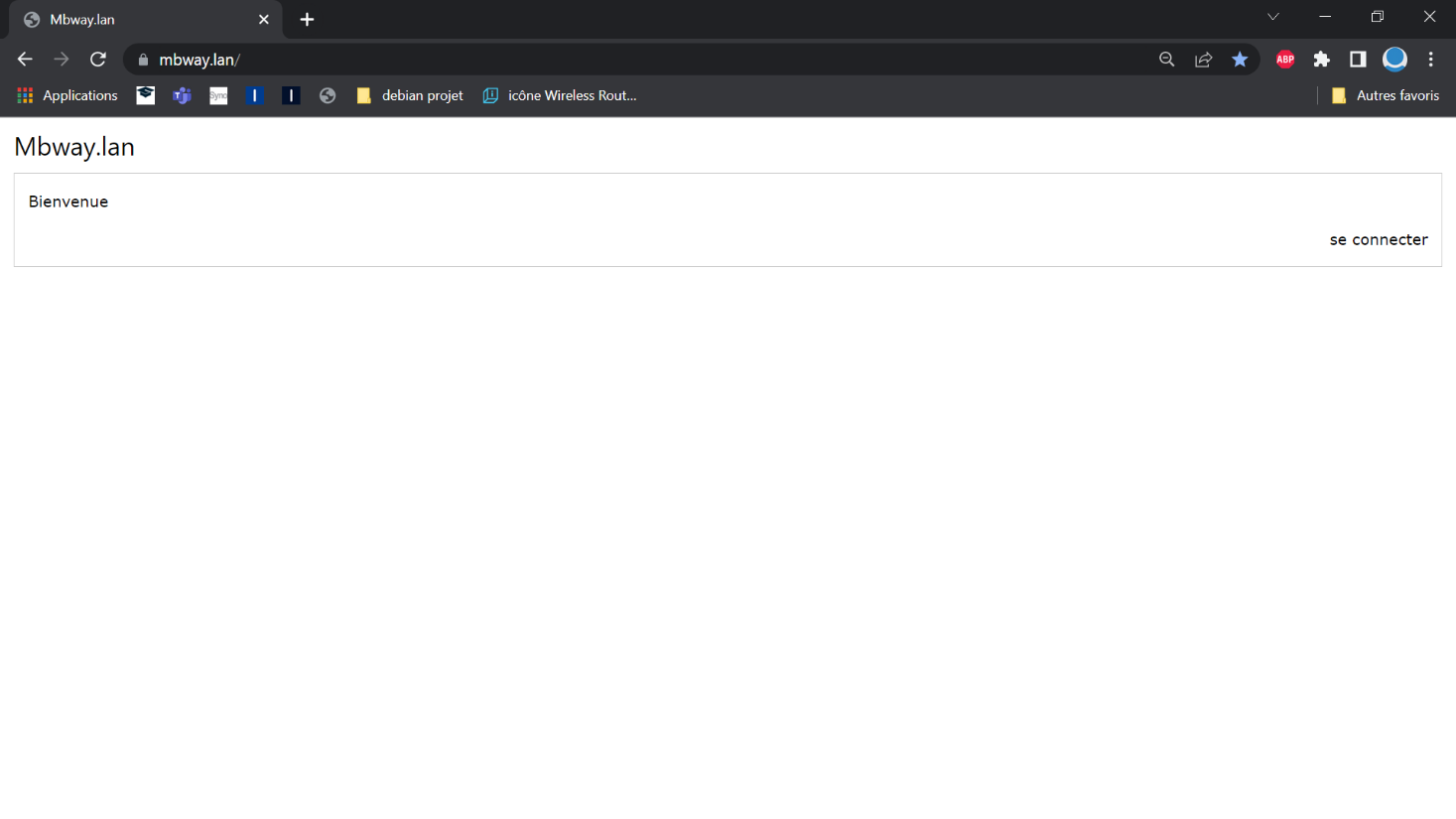
|  |
| --- |
| CAHIER DES RECETTES |

1. Conexion Serveur Web

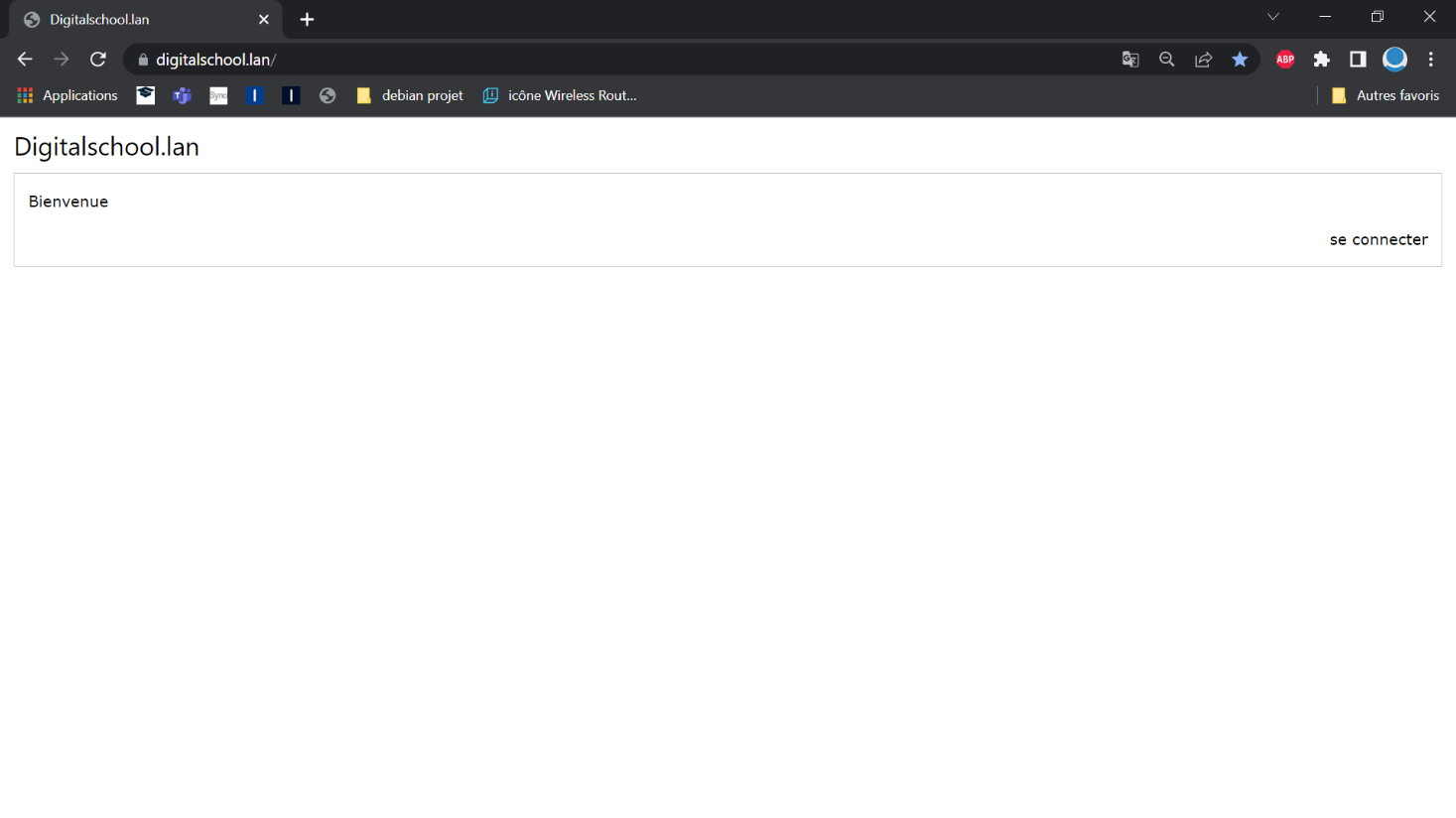
L'accès au serveur Web est disponible depuis n'importe quelle machine du LAN Administratif et de Formation.

L'accès à Internet se fait via le Routeur ASI, qui agit comme la passerelle de notre réseau et héberge les services DNS et Firewall.

Nous constatons que le site Mbway.lan est accessible, la résolution DNS est correcte, et la connexion est sécurisée (HTTPS).



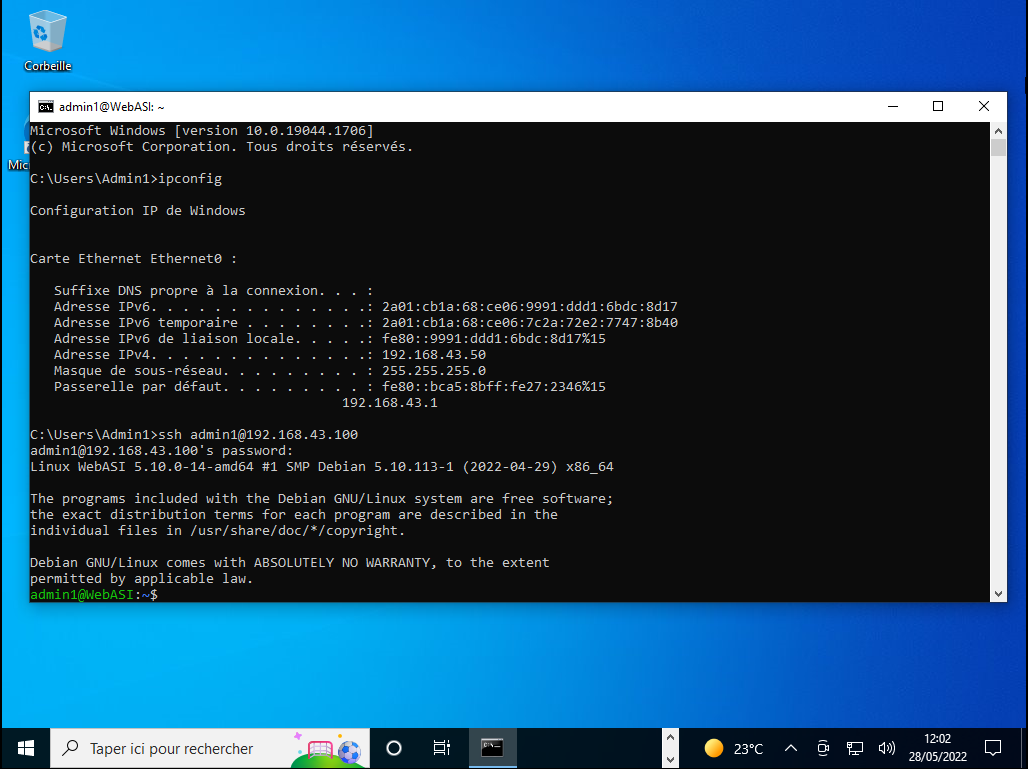
Nous pouvons voir que le site Digitalschool.lan est bien accessible, que la résolution DNS est correcte et que nous sommes connectés de manière sécurisée.



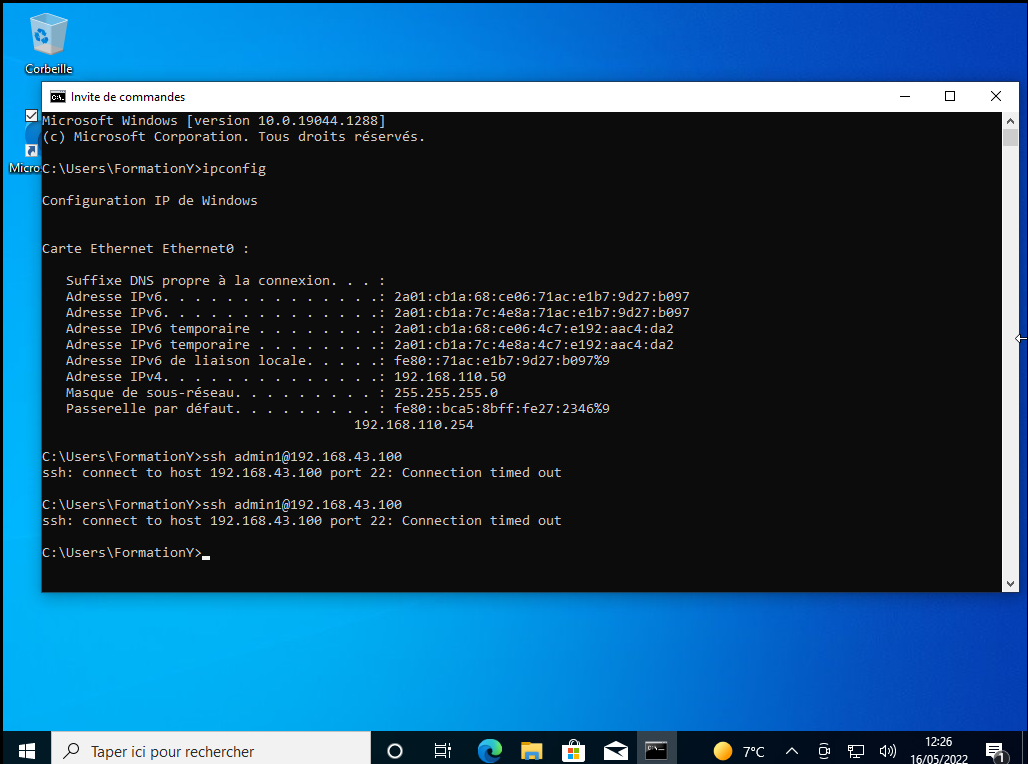
1. Conexion SSH

L’accès SSH est possible seulement sur le poste Admin1 sur le Lan Administratif grâce au compte admin1. Tout autre connexion sera refusée sur un autre poste.

Nous utilisons la machine Admin1 sur le Lan Administratif



Nous testons alors la machine Formation Y



Nous n’avons pas accès au serveur Web via une connexion SSH sur le réseau formation. Nous nous connectons grâce au compte autorisé admin1 mais la connexion est refusée

1. Conexion FTP (Fillezila)

(Je n’arrive pas exécuter l'installation de FilleZila cella me met le même message d’erreur que quand on avait fait les tests chez nous avant le projet)

|  |
| --- |
| CONCLUSION |

Pendant votre stage, vous avez été chargé par votre centre de formation de créer une maquette à faible coût pour démontrer la faisabilité de la solution. Vous disposez d'un ancien serveur que vous pouvez réutiliser pour héberger des machines virtuelles.

La solution retenue consiste à mettre en place un sous-réseau appelé DMZ pour héberger les services utilisés par le personnel et les stagiaires (Formation). Ce réseau DMZ est accessible depuis Internet. Le serveur Web héberge un site pour chaque établissement. Pour sécuriser les transactions, les sites ne sont accessibles qu'en HTTPS, soit https://www.mbway.lan ou https://www.digitalschool.lan. Ces sites web sont accessibles à tous.

Voici les principales actions réalisées :

- Accès autorisé au serveur Web de la DMZ pour tous les utilisateurs du LAN Administratif et de la Formation.

- Accès à Internet autorisé pour tous en utilisant le Routeur R comme passerelle, hébergeant les services DNS et Firewall.

- Accès au service FTP limité à un seul poste, celui de l'administrateur situé dans le LAN Administratif (Admin1).

- Les postes de l'espace Formation ne peuvent pas accéder au service FTP.

- Accès SSH autorisé à un seul poste, celui de l'administrateur situé dans le LAN Administratif (Admin1).

- Les autres périphériques du réseau Administratif et ceux du réseau Formation ne peuvent pas accéder aux accès SSH.

- Mise en place des tests de validation conformément aux exigences du cahier des charges.

- Fourniture d'une documentation expliquant et validant chacune des exigences du cahier des charges.

CLOTTES Timothé