

Mise en place d'une passerelle Linux et d'une DMZ sous Debian

*14/05
Système & Réseaux*

*CUENCA Teva
SIO 1*

Table des Matières

Cahier des charges	3
Maquette.....	4
Configuration des interfaces.....	5
Activation du routeur.....	6
Mise en place BIND9 (DNS).....	7
Connexion BIND9 au serveur Web.....	8
Configuration Name.conf.local.....	9
Configuration IPTABLES.....	8
Configuration SERVEUR WEB.....	10
Configuration VIRTUAL HOST.....	11
Test.....	12

Cahier des Charges

Votre centre de formation regroupant plusieurs enseignes met à disposition des élèves MBWay et DigitalSchool un serveur Web hébergeant un intranet pour chaque enseigne. Dans sa première version, les sites répertoriant les activités et actualités de chaque enseigne étaient hébergées dans le LAN Administratif. 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. La solution qui a été retenue est de créer un sous-réseau nommé DMZ pour héberger 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.lanou> <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.

Travail demandé

Permettre l'accès au serveur Web de la DMZ pour tous, LAN Administratif et Formation.

Permettre l'accès à internet pour tous en utilisant le Routeur R comme passerelle hébergeant le service DNS et de Firewall;

Permettre l'accès au service FTP à 1 seul poste, celui de l'administrateur situé dans le LAN Administratif

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

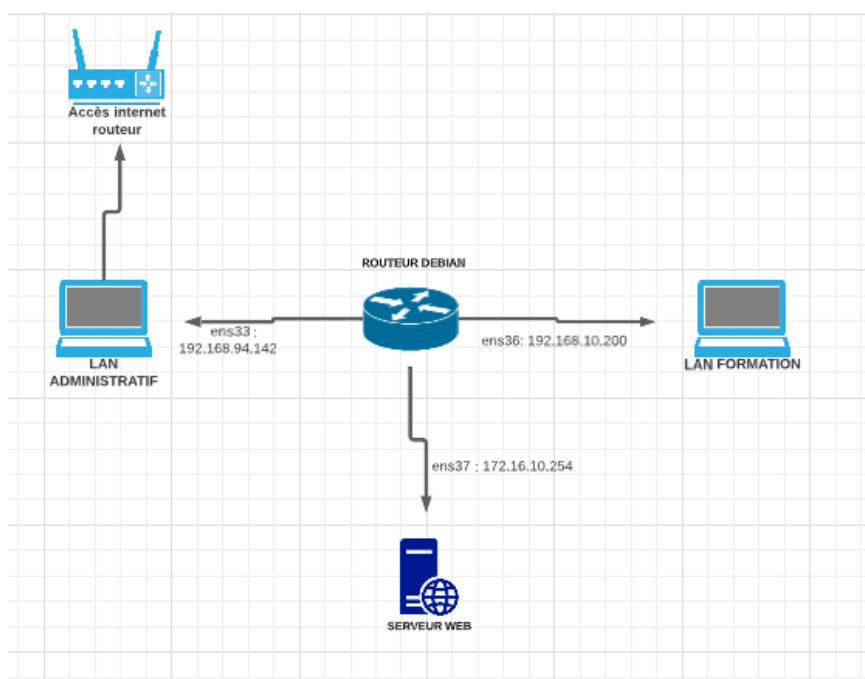
Permettre un accès SSH à 1 seul poste, celui de l'administrateur situé dans le LAN Administratif

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

Mettre en place les tests de validation répondant aux demandes du cahier des charges.

Fournir une documentation expliquant et validant chacune des demandes du cahier des charges

Maquette



Serveur web :172.16.10.1

Configuration des interfaces

Notre serveur Linux aura besoin de 3 interfaces, ens33, ens 36, et ens37.

Pour se faire, il faut ouvrir le terminal et rentrer la commande « su root »

```
administrateur@DEB:~$ su root
Mot de passe :
root@DEB:~/home/administrateur# █
```

Et de rentrer le mot de passer administrateur.

Une fois en mode root, nous allons configurer les interfaces dans le fichier « interfaces » en utilisant la commande :

« nano /etc/network/interfaces »

```
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

auto ens33
iface ens33 inet dhcp

auto ens36
iface ens36 inet static
    address 192.168.10.200
    netmask 255.255.255.0

auto ens37
iface ens37 inet static
    address 172.16.10.254
    netmask 255.255.255.0
```

Pour appliquer les changements nous aurons besoin de redémarrer les services avec la commande :

- Systemctl restart networking

Ensuite on utilise la commande « ip a » pour voir si le changement s'est bien appliqué.

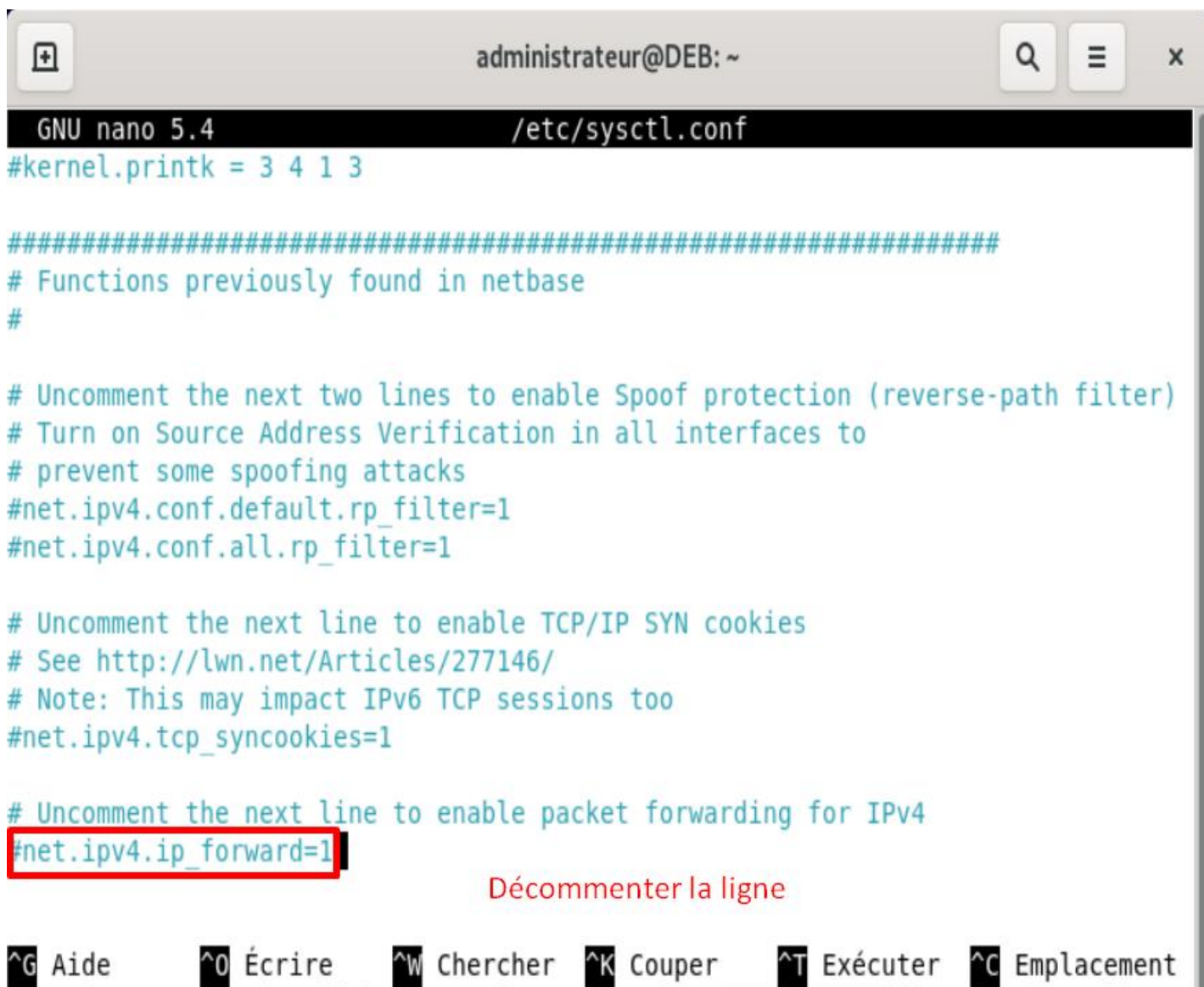
```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group de
fault qlen 1000
    link/ether 00:0c:29:85:ec:95 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.94.142/24 brd 192.168.94.255 scope global dynamic ens33
        valid_lft 1613sec preferred_lft 1613sec
    inet6 fe80::20c:29ff:fe85:ec95/64 scope link
        valid_lft forever preferred_lft forever
3: ens36: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group de
fault qlen 1000
    link/ether 00:0c:29:85:ec:9f brd ff:ff:ff:ff:ff:ff
    altname enp2s4
    inet 192.168.10.200/24 brd 192.168.10.255 scope global ens36
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe85:ec9f/64 scope link
        valid_lft forever preferred_lft forever
4: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group de
fault qlen 1000
    link/ether 00:0c:29:85:ec:a9 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 172.16.10.254/24 brd 172.16.10.255 scope global ens37
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe85:eca9/64 scope link
        valid_lft forever preferred_lft forever
```

Activation du routeur :

Taper la commande

- Nano /etc/sysctl.conf

Activation du routeur :



```
administrateur@DEB: ~
GNU nano 5.4 /etc/sysctl.conf
#kernel.printk = 3 4 1 3

#####
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1

Décommenter la ligne

^G Aide    ^O Écrire  ^W Chercher ^K Couper  ^T Exécuter ^C Emplacement
```

```
administrateur@DEB: ~
sys-devices-pci0000:00-0000:00:10.0-host2-target2:0:0-2:0:0:0-block-sda-sda1.>
sys-devices-pci0000:00-0000:00:10.0-host2-target2:0:0-2:0:0:0-block-sda-sda2.>
sys-devices-pci0000:00-0000:00:10.0-host2-target2:0:0-2:0:0:0-block-sda-sda5.>
sys-devices-pci0000:00-0000:00:10.0-host2-target2:0:0-2:0:0:0-block-sda.device>
sys-devices-pci0000:00-0000:00:11.0-0000:02:00.0-usb2-2\x2d2-2\x2d2.1-2\x2d2.>
sys-devices-pci0000:00-0000:00:11.0-0000:02:01.0-net-ens33.device >
sys-devices-pci0000:00-0000:00:11.0-0000:02:02.0-sound-card0-controlC0.device>
sys-devices-pci0000:00-0000:00:11.0-0000:02:04.0-net-ens36.device >
sys-devices-pci0000:00-0000:00:11.0-0000:02:05.0-net-ens37.device >
sys-devices-platform-serial8250-tty-ttyS1.device >
sys-devices-platform-serial8250-tty-ttyS2.device >
sys-devices-platform-serial8250-tty-ttyS3.device >
sys-devices-pnp0-00:05-tty-ttyS0.device >
sys-devices-virtual-misc-rfkill.device >
sys-module-configfs.device >
sys-module-fuse.device >
sys-subsystem-bluetooth-devices-hci0.device >
sys-subsystem-net-devices-ens33.device >
sys-subsystem-net-devices-ens36.device >
sys-subsystem-net-devices-ens37.device >
-.mount >

root@DEB:~# sysctl -p
root@DEB:~# sysctl -p /etc/sysctl.conf
```

Pour vérifier que la ligne est bien supprimé

```
administrateur@DEB: ~  
sys-devices-pci0000:00-0000:00:11.0-0000:02:00.0-usb2-2\x2d2-2\x2d2.1-2\x2d2.>  
sys-devices-pci0000:00-0000:00:11.0-0000:02:01.0-net-ens33.device >  
sys-devices-pci0000:00-0000:00:11.0-0000:02:02.0-sound-card0-controlC0.device >  
sys-devices-pci0000:00-0000:00:11.0-0000:02:04.0-net-ens36.device >  
sys-devices-pci0000:00-0000:00:11.0-0000:02:05.0-net-ens37.device >  
sys-devices-platform-serial8250-tty-ttyS1.device >  
sys-devices-platform-serial8250-tty-ttyS2.device >  
sys-devices-platform-serial8250-tty-ttyS3.device >  
sys-devices-pnp0-00:05-tty-ttyS0.device >  
sys-devices-virtual-misc-rfkill.device >  
sys-module-configfs.device >  
sys-module-fuse.device >  
sys-subsystem-bluetooth-devices-hci0.device >  
sys-subsystem-net-devices-ens33.device >  
sys-subsystem-net-devices-ens36.device >  
sys-subsystem-net-devices-ens37.device >  
- .mount >  
  
root@DEB:~# sysctl -p  
root@DEB:~# sysctl -p /etc/sysctl.conf  
root@DEB:~# nano /etc/sysctl.conf  
root@DEB:~# sysctl -p /etc/sysctl.conf  
net.ipv4.ip_forward = 1 Cette ligne montre que le routeur est bien fonctionnel  
root@DEB:~# █
```

Mise en place BIND 9 :

Installation des services

```
-.mount

root@DEB:~# sysctl -p
root@DEB:~# sysctl -p /etc/sysctl.conf
root@DEB:~# nano /etc/sysctl.conf
root@DEB:~# sysctl -p /etc/sysctl.conf
net.ipv4.ip_forward = 1
root@DEB:~# apt update
Atteint :1 http://deb.debian.org/debian bullseye InRelease
Réception de :2 http://security.debian.org/debian-security bullseye-security InRelease [48,4 kB]
Réception de :3 http://deb.debian.org/debian bullseye-updates InRelease [44,1 kB]
]
92,4 ko réceptionnés en 1s (179 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
10 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
root@DEB:~#
```

```
Réception de :2 http://security.debian.org/debian-security bullseye-security InRelease [48,4 kB]
Réception de :3 http://deb.debian.org/debian bullseye-updates InRelease [44,1 kB]
]
92,4 ko réceptionnés en 1s (179 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
10 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
root@DEB:~# apt install bind9
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  bind9-utils python3-ply
Paquets suggérés :
  bind-doc resolvconf ufw python-ply-doc
Les NOUVEAUX paquets suivants seront installés :
  bind9 bind9-utils python3-ply
0 mis à jour, 3 nouvellement installés, 0 à enlever et 10 non mis à jour.
Il est nécessaire de prendre 997 ko dans les archives.
Après cette opération, 2 351 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n]
```

Cette commande permet d'installer les services de bind9


```
Dépaquetage de bind9-utils (1:9.16.37-1~deb11u1) ...
Sélection du paquet bind9 précédemment désélectionné.
Préparation du dépaquetage de .../bind9_1%3a9.16.37-1~deb11u1_amd64.deb ...
Dépaquetage de bind9 (1:9.16.37-1~deb11u1) ...
Paramétrage de python3-ply (3.11-4) ...
Paramétrage de bind9-utils (1:9.16.37-1~deb11u1) ...
Paramétrage de bind9 (1:9.16.37-1~deb11u1) ...
Ajout du groupe « bind » (GID 125)...
Fait.
Ajout de l'utilisateur système « bind » (UID 117) ...
Ajout du nouvel utilisateur « bind » (UID 117) avec pour groupe d'appartenance «
bind » ...
Le répertoire personnel « /var/cache/bind » n'a pas été créé.
wrote key file "/etc/bind/rndc.key"
named-resolvconf.service is a disabled or a static unit, not starting it.
Created symlink /etc/systemd/system/bind9.service → /lib/systemd/system/named.se
rvice.
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /lib
/systemd/system/named.service.
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
root@DEB:~# █
```

La carte que nous allons utiliser pour cela sera ens37, il faut donc rentrer l'ip du Lan DMZ dans le name server de BIND9.

Taper les commandes suivantes :

- nano /etc/resolv.conf
- nameserver 172.16.10.254



```
administrateur@DEB: ~
GNU nano 5.4 /etc/resolv.conf *
domain localdomain
search localdomain
nameserver 172.16.10.254 █
```

CTRL + O puis CTRL + X pour sauvegarder et quitter

Ensuite, cette partie de la procédure Linux concerne la résolution des domaines "mbway.lan" et "digitalschool.lan" en modifiant le fichier de configuration named.conf.options. Voici les étapes à suivre :

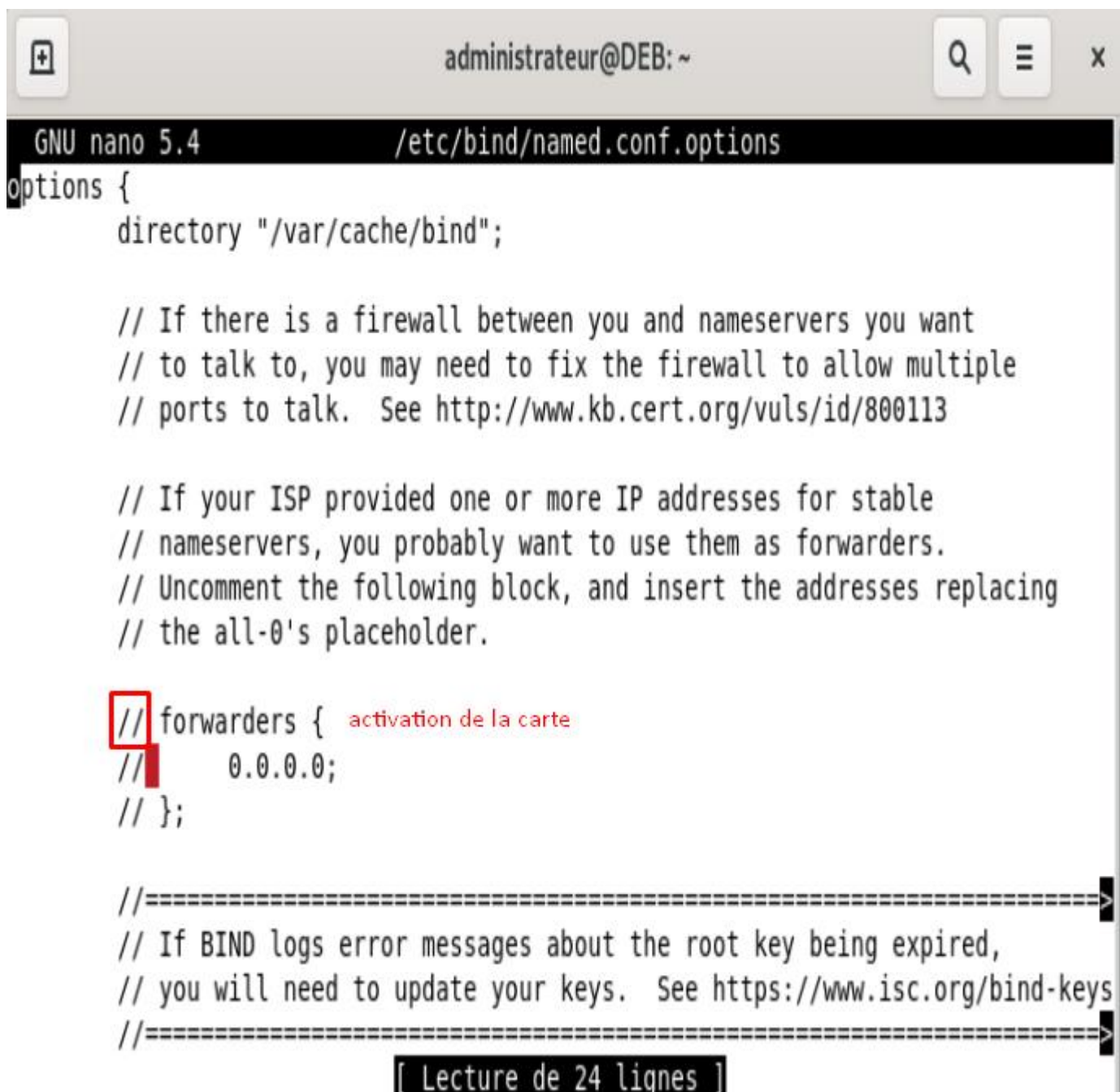
Ouvrez le fichier named.conf.options avec l'éditeur de texte nano. La commande pour ouvrir le fichier est la suivante :

- nano /etc/bind/named.conf.options

À l'intérieur du fichier named.conf.options, recherchez la section "forwarders". Cette section indique les serveurs DNS utilisés pour la résolution des noms de domaine.

Dans cette section, vous trouverez des lignes commençant par "//". Ces "//" signifient que ces lignes sont commentées, c'est-à-dire qu'elles sont ignorées lors de l'exécution de la configuration.

Pour activer la partie "forwarders", vous devez enlever les "//" devant les lignes. Cela signifie que vous devez supprimer les marques "//" des lignes concernées.



```
administrateur@DEB: ~
GNU nano 5.4 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders { activation de la carte
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
[ Lecture de 24 lignes ]
```

Ensuite, vous devez ajouter les adresses IP suivantes dans la section "forwarders" :

172.16.10.254
8.8.8.8 (GOOGLE)
8.8.4.4 (GOOGLE)

Ces adresses IP correspondent aux serveurs DNS que nous souhaitons utiliser pour la résolution des domaines "mbway.lan" et "digitalschool.lan".

```
GNU nano 5.4 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        172.16.10.254
        8.8.8.8
        8.8.4.4;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    [ 26 lignes écrites ]
```

Une fois que les modifications sont terminées, enregistrez le fichier named.conf.options et quittez l'éditeur de texte. CTRL + O / CTRL + X

Après avoir effectué ces étapes, le serveur DNS utilisera les adresses IP spécifiées pour résoudre les domaines "mbway.lan" et "digitalschool.lan".

Connexion de BIND9 au serveur Web

Accédez au répertoire Bind9 :

Bash

`cd /etc/bind/`

Cette commande vous permet de naviguer vers le répertoire où se trouvent les fichiers de configuration de Bind9.

Copiez un fichier exemple pour créer le fichier de route :

`cp db.local db.mbway.lan`

```
root@DEB:~# cd /etc/bind/
root@DEB:/etc/bind# cp db.local db.mway.lan
```

Cette commande crée une copie du fichier "db.local" et le renomme en "db.mbway.lan".

Le fichier "db.mbway.lan" sera utilisé pour définir les enregistrements de route vers le serveur web.

```
GNU nano 5.4 db.mbway.lan
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA    localhost. root.localhost. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@       IN      NS     localhost.
@       IN      A      127.0.0.1
@       IN      AAAA   ::1

[ Lecture de 14 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^I Justifier ^_ Aller ligne
```

La copie a bien fonctionné.

Il faut ensuite ouvrir le fichier "db.mbway.lan" et rechercher la ligne "SOA" dans le fichier.

Modifiez la ligne "SOA" pour remplacer les valeurs "localhost" et "root.localhost" par les valeurs appropriées :

Remplacez "localhost" par "debian-routeur.mbway.lan" dans la première partie de la ligne.

Remplacez "root.localhost" par "root.debian-routeur.mbway.lan" dans la seconde partie de la ligne.

La ligne "SOA" définit l'enregistrement de départ de la zone. En modifiant ces valeurs, vous spécifiez l'origine et l'autorité pour la zone "mbway.lan".

Ajoutez les routes en modifiant le fichier "db.mbway.lan" :

Ajoutez l'enregistrement suivant pour le serveur "DEB" :

```
DEB      A      172.16.10.254
```

Cet enregistrement définit l'adresse IP "172.16.10.254" pour le nom "DEB" dans la zone "mbway.lan".

Vous devez remplacer "172.16.10.254" par l'adresse IP réelle du serveur "DEB".

Ajoutez l'enregistrement suivant pour la passerelle "192.168.150.1" :

```
172.16.10.1      A      172.16.10.1
```

```
GNU nano 5.4                               db.mbway.lan *
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      DEB.mbway.lan. root.mbway.lan. (
                                2          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN      NS       localhost.
DEB      A       172.16.10.254
172.16.10.1  A     172.16.10.1
www      CNAME   172.16.10.1
```

Cet enregistrement définit l'adresse IP "172.16.10.1" pour la passerelle dans la zone "mbway.lan". Ensuite CTRL + O pour enregistrer.

Nous venons donc de créer un fichier de route "db.mbway.lan" dans le service Bind9. Ce fichier permet de définir les enregistrements de route pour le serveur web, y compris l'adresse IP du serveur "DEB" et de la passerelle "172.16.10.1". Ces enregistrements permettent au serveur DNS de résoudre les noms de domaine et de diriger le trafic vers le serveur web approprié.

Il nous est aussi demandé de faire la même chose pour le fichier digitalschool.

```
root@DEB:/home/administrateur# cd /etc/bind
root@DEB:/etc/bind# cp db.mbway.lan db.digitalschool.lan
root@DEB:/etc/bind# █
```

```
GNU nano 5.4 db.digitalschool.lan
DEB;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA DEB.digitalschool.lan. root.digitalschool.lan (
        2 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS localhost.
DEB A 172.16.10.254
172.16.10.1 A 172.16.10.1

WWW CNAME 172.16.10.1
```

CONFIGURATION named.conf.local

Le fichier named.conf.local est utilisé par le service Bind9 pour définir les zones de domaine gérées par le serveur DNS. En ajoutant des lignes dans ce fichier, vous spécifiez les informations de configuration pour chaque zone de domaine.

Dans notre cas, nous ajoutons les lignes suivantes :

```
GNU nano 5.4 named.conf.local *
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "mbway.lan" {
    type master;
    file "/etc/bind/db.mbway.lan";
};

zone "digitalschool.lan" {
    type master;
    file "/etc/bind/db.digitalschool.lan";
};
```

La première ligne "zone "mbway.lan" {" indique que nous allons définir la zone de domaine "mbway.lan". Vous pouvez remplacer "mbway.lan" par le nom de votre propre domaine.

"type master;" spécifie que notre serveur DNS est le serveur maître pour cette zone. Cela signifie que notre serveur est autorisé à fournir les enregistrements DNS pour ce domaine.

"file "/etc/bind/db.mbway.lan";" indique le chemin du fichier de zone associé à la zone "mbway.lan". Ici, nous spécifions que le fichier de zone est "/etc/bind/db.mbway.lan".

De manière similaire, nous ajoutons une autre zone "digitalschool.lan" avec les mêmes informations de configuration, mais avec le chemin du fichier de zone approprié.

En ajoutant ces lignes dans le fichier named.conf.local, nous déclarons les zones de domaine "mbway.lan" et "digitalschool.lan" et spécifions le chemin des fichiers de zone correspondants. Cela permet au serveur DNS de Bind9 de répondre aux requêtes DNS pour ces domaines spécifiques et de fournir les enregistrements DNS correspondants à partir des fichiers de zone associés.

CONFIGURATION IPTABLES

Configuration des accès internet :

- **sudo iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE**

```
root@DEB:/home/administrateur# sudo iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE
```

Configuration du LAN Administratif

```
root@DEB:/home/administrateur# sudo iptables -A FORWARD -s 172.16.10.1 -p tcp --dport 21 -j ACCEPT
root@DEB:/home/administrateur# sudo iptables -A FORWARD -s 172.16.10.1 -p tcp --dport 22 -j ACCEPT
root@DEB:/home/administrateur#
```

Blocage des accès :

```
root@DEB:/home/administrateur# sudo iptables -A FORWARD -p tcp --dport 21 -j DROP
root@DEB:/home/administrateur# sudo iptables -A FORWARD -p tcp --dport 22 -j DROP
```

Sauvegarde des règles IPTABLES :

```
root@DEB:/etc# sudo sh -c "iptables-save > /etc/iptables/fw.v4"
```

Vérification des règles

Nous vérifions les règles en utilisant la commande :

- sudo iptables -L

```
Chain FORWARD (policy ACCEPT)
target     prot opt source                destination           tcp dpt:ftp
ACCEPT    tcp  --  172.16.10.1           anywhere              tcp dpt:ssh
ACCEPT    tcp  --  172.16.10.1           anywhere              tcp dpt:ftp
DROP      tcp  --  anywhere              anywhere              tcp dpt:ssh
DROP      tcp  --  anywhere              anywhere              tcp dpt:ssh

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

root@DEB:/etc# sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@DEB:/etc# sudo iptables -L INPUT -v -n
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target     prot opt in  out  source                destination
```


CONFIGURATION DU SERVEUR WEB ET DE SES SERVICES

Il faut d'abord installer les services avant de configurer les interfaces réseau, nous aurons besoin :

- APACHE2
- PROFTPD
- SSH
- OPEN SSL

APACHE a été installé via Debian lors de la mise en place de Debian, donc nous n'aurons pas à utiliser la commande `sudo apt install apache2`

PROFTPD

APTUPDATE

```
root@DEB2:/home/administrateur# sudo apt install proftpd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Note : sélection de « proftpd-core » au lieu de « proftpd »
proftpd-core est déjà la version la plus récente (1.3.7a+dfsg-12+deb11u2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@DEB2:/home/administrateur#
```

SSH

APTUPDATE

```
root@DEB2:/home/administrateur# apt install ssh
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  ssh
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 252 ko dans les archives.
Après cette opération, 268 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 ssh all 1:8.4p1-5+deb11u1 [252 kB]
252 ko réceptionnés en 0s (2 504 ko/s)
Sélection du paquet ssh précédemment désélectionné.
(Lecture de la base de données... 149057 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../ssh_1%3a8.4p1-5+deb11u1_all.deb ...
Dépaquetage de ssh (1:8.4p1-5+deb11u1) ...
Paramétrage de ssh (1:8.4p1-5+deb11u1) ...
root@DEB2:/home/administrateur# █
```

SSL

APTUPDATE

```
root@DEB2:/home/administrateur# apt install openssl
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openssl est déjà la version la plus récente (1.1.1n-0+deb11u4).
openssl passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@DEB2:/home/administrateur# █
```

CONFIGURATION DES SITES

Il faut maintenant créer les deux différents sites :

MBWAY :

```
root@DEB2:/var/www/html# mkdir mbway      création du dossier
root@DEB2:/var/www/html# cd mbway
root@DEB2:/var/www/html/mbway# touch index.html  Configuration html
```

DIGITALSCHOOL

```
root@DEB2:/home/administrateur# mkdir digitalschool
root@DEB2:/home/administrateur# cd digitalschool
root@DEB2:/home/administrateur/digitalschool# touch intex.html
```

CONFIGURATION HTTPS

```
root@DEB2:/home/administrateur# sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create s
elf-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@DEB2:/home/administrateur# █
```

```
root@DEB2:/home/administrateur# systemctl restart apache2  Redémarrage apache2
```

Création certificat :

```
root@DEB2:/home/administrateur# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/apache2/ssl/apache.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

CONFIGURATION DES INTERFACES RESEAUX

```
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto ens33
iface ens33 inet static
    address 172.16.10.1
    netmask 255.255.255.0
    gateway 172.16.10.254

[ 14 lignes écrites ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier  ^_.
```

Les interfaces réseaux sont correctement configurées, maintenant après un `systemctl restart networking.service`, apache devrait être accessible depuis notre routeur debian pour cela il faut rentrer dans la barre de recherche de notre navigateur http://ip_du_serveur_web donc ici <http://172.16.10.1>, si un affichage APACHE2 s'affiche c'est que tout communique correctement.



Le message « It works ! » nous confirme le bon fonctionnement des services.

VIRTUAL HOST

```
root@DEB2:/home/administrateur# cd /etc/apache2/sites-available
root@DEB2:/etc/apache2/sites-available# cp 000-default.conf mbway.conf
root@DEB2:/etc/apache2/sites-available# CREATION D'UN HOTE
```

Maintenant il faut décommenter certaines lignes et les modifier dans le dossier mbway.conf.

```
GNU nano 5.4 mbway.conf
<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.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

# 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
[ Lecture de 31 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^N Remplacer  ^U Coller    ^J Justifier  ^_ Aller ligne
```

```
GNU nano 5.4 mbway.conf *
<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.mbway.lan

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html

# 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

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^N Remplacer  ^U Coller    ^J Justifier  ^_ Aller ligne
```

```
GNU nano 5.4 mbway.conf
<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.mbway.lan

    ServerAdmin webmaster@localhost
    #DocumentRoot /var/www/html
    Redirect permanent / https://www.mbway.lan/

    # Available loglevels: trace8, ..., tracel, 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
```

[Lecture de 32 lignes]

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

Et faire la même chose pour DIGITAL SCHOOL.

Maintenant il faut tester les accès pour voir si tout fonctionne correctement.

TEST MBWAY /



L'accès fonctionne correctement.



IDEM pour DIGITAL SCHOOL.

Le cahier des charges est donc respecté.