**PR02 – Mise en place**

**d’une passerelle et Firewall Linux**

**Une image contenant Graphique, obscurité, cercle

Description générée automatiquement**

**Une image contenant Graphique, symbole, clipart, graphisme

Description générée automatiquement**

Table des matières

[**Contexte 3**](#_Toc196727400)

[**Cahier des charges 3**](#_Toc196727401)

[**Configuration du routeur 9**](#_Toc196727402)

[**Configuration du Serveur Web & FTP 10**](#_Toc196727404)

[**Installation de ProFTP : 15**](#_Toc196727405)

[**Règles iptables 15**](#_Toc196727406)

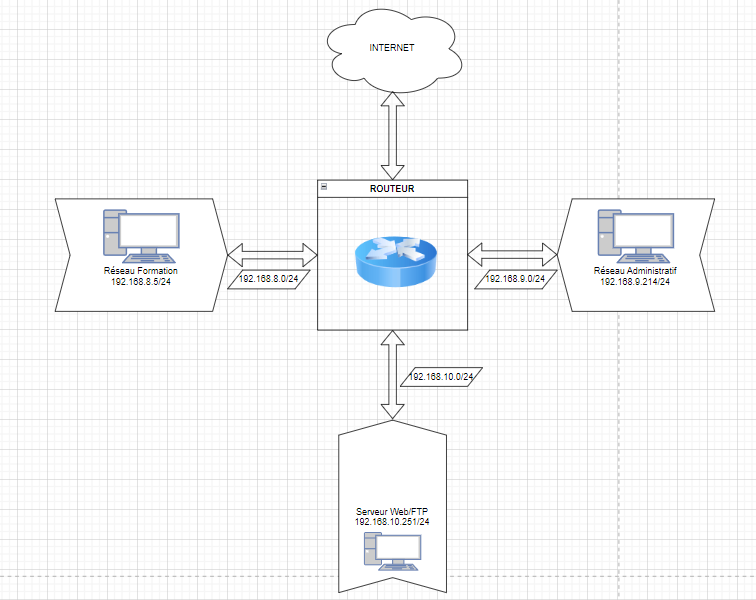
[**Vérification du bon fonctionnement des règles 16**](#_Toc196727407)

# Contexte

Votre centre de formation regroupant plusieurs enseignes dont MBWay et DigitalSchool, met à disposition des élèves un serveur Web hébergeant un intranet pour chacune d’elle : il s’agit d’un serveur web mutualisé. Dans l’architecture initiale, les sites web de chaque enseigne étaient hébergés sur un serveur dans le LAN Administratif. À la suite de 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. 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.

# Cahier des charges

* Permettre l’accès au serveur Web dans la DMZ pour tous, LAN Administratif et Formation.
* Permettre l’accès à internet pour tous en utilisant le Routeur Debian comme passerelle. Ce routeur hébergera aussi les service DNS et fera office de Firewall pour filtrer les accès à la DMZ;
* 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.
* Permettre un accès SSH à un 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 en SSH au serveur Web.
* Mettre en place les tests de validation des règles ci-dessus.
* Fournir une documentation expliquant et validant chacune des demandes du cahier des charges

****

**Configuration Réseau**

**Configuration du Projet :**

**1 VM Debian ROUTEUR, 1 VM Serveur Web/FTP, 1 VM Admisnitratif, 1 VM Formation**

**Logiciels/services/applications/OS : Debian11, Apache2, ProFTPD**

# **Configuration du routeur**

Il faut mettre plusieurs cartes réseaux afin de pouvoir gérer entièrement le réseau et ses sous réseaux.

# **Une image contenant texte, capture d’écran, Police, document Le contenu généré par l’IA peut être incorrect.**

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.Il faut également avec le mode NAT (Network Address Translation). Il suffit de décocher la ligne dans « /etc/sysctl.conf ».

Ne pas oublier d’annoter post-up etcc.. dans /etc/network/interfaces.

# **Configuration du Serveur Web & FTP**

Pour la bonne configuration d’un Serveur Web il faut Apache2 et Bind9.  




Une fois l’installation faite, il faut créer des fichiers index ( le contenu de la page web)

Une image contenant texte, Police, reçu, blanc

Description générée automatiquement

Une image contenant texte, reçu, Police, blanc

Description générée automatiquementfichiers index de chaque site

Une image contenant texte, capture d’écran, Police, document

Description générée automatiquementUne image contenant texte, capture d’écran, Police, nombre

Description générée automatiquementPuis un fichier de configuration pour chaque site web (ici mbway & digitalschool)

Il faut maintenant démarrer les sites à l’aide d’une commande





Une image contenant texte, capture d’écran, Police

Description générée automatiquementLes sites sont démarrés, on peut maintenant y accèder en tapant l’adresse IP du serveur suivit du nom du fichierUne image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

page d’accueil de nos 2 sites

La première partie est terminée, il faut maintenant mettre en place un DNS et le certificat HTTPS.

Pour le certificat HTTPS, nous utiliserons le certificat dèjà fournit par apache2.  
Il suffit de reprendre la configuration des sites mais d’avoir en Virtual Host le port 443.

Une image contenant texte, capture d’écran, Police, algèbre

Description générée automatiquementUne image contenant texte, capture d’écran, Police, algèbre

Description générée automatiquementconfiguration des sites

Nos 2 sites ont leurs virutals hosts de configurer, on peut maintenant les réactiver avec la même commande précedemment utilisée.





Il faut maintenant créer nos zones et les déclarer.

Une image contenant texte, capture d’écran, reçu, Police

Description générée automatiquement

Fichier de zones des deux sites

Une image contenant texte, capture d’écran, Police, reçu

Description générée automatiquement

Une fois créer il faut les déclarer

Fichier de déclaration de zone : « named.conf.local

Une image contenant texte, capture d’écran, Police, algèbre

Description générée automatiquement

Une fois chose faite, il ne faut pas oublier de rajouter en tant que DNS, l’adresse ip du serveur dans le fichier /etc/resolv.conf



Une fois toutes ces étapes terminées, on peut accèder à nos sites en utilisant respectivement [www.mbway.laUne image contenant texte, capture d’écran, Police, nombre

Description générée automatiquementn](http://www.mbway.lan) et [www.digitalschool.lan](http://www.digitalschool.lan).

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Le serveur Web ainsi que les sites sont correctements configurés.

# **Installation de ProFTP :**



Il faut maintenant installer filezilla, une application permettant le transfert de fichier avec le protocole FTP.

Pas besoin de configuration particulière, tout ce fait via l’application.

# **Règles iptables**

SERVEUR WEB/FTP/SSH : 192.168.10.251

Machine Admin : 192.168.9.214/25

Machine employé : 192.168.9.5/25

iptables -P INPUT ACCEPT

iptables -P OUTPUT ACCEPT

iptables -P FORWARD ACCEPT

# Autoriser le trafic HTTP et HTTPS vers le serveur 192.168.10.251 depuis n'importe où

iptables -A FORWARD -p tcp --dport 80 -d 192.168.10.251 -j ACCEPT

iptables -A FORWARD -p tcp --dport 443 -d 192.168.10.251 -j ACCEPT

# Autoriser FTP et SSH uniquement depuis la machine Admin (192.168.9.214)

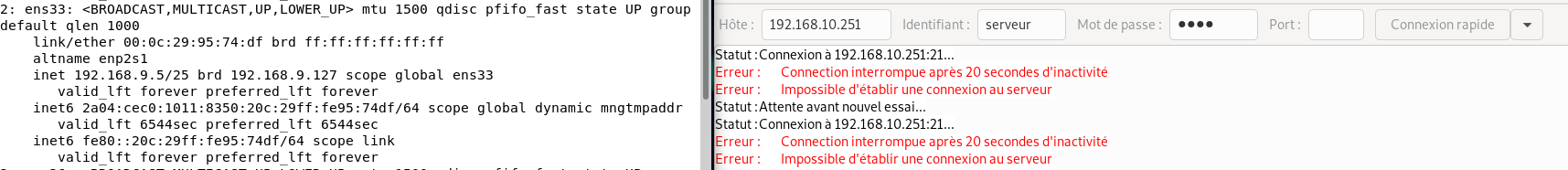
iptables -A FORWARD -p tcp --dport 21 -s 192.168.9.214 -d 192.168.10.251 -j ACCEPT

iptables -A FORWARD -p tcp --dport 22 -s 192.168.9.214 -d 192.168.10.251 -j ACCEPT

iptables -A FORWARD -p tcp --sport 20 -s 192.168.10.251 -d 192.168.9.214 -j ACCEPT

iptables -A FORWARD -p tcp --sport 22 -s 192.168.10.251 -d 192.168.9.214 -j ACCEPT

# **Vérification du bon fonctionnement des règles**

Tentative de connexion FTP de machine employé vers serveur

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.Tentative de connexion FTP de machine Admin vers serveur

Une image contenant texte, Police, ligne, nombre

Le contenu généré par l’IA peut être incorrect.Accès au serveur web depuis la machine Admin vers le serveur

Une image contenant texte, Police, nombre, capture d’écran

Le contenu généré par l’IA peut être incorrect.Accès au serveur web depuis la machine Employé vers le serveur