|  |  |
| --- | --- |
|  |  |
| Mise en place d’une passerelle Linux et d’une DMZ sous Debian |  |
|  |  |
|  | 14/05Système & Réseaux |
|  | CUENCA TevaSIO 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 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.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

O 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

O 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*

Une image contenant texte, capture d’écran, diagramme, ligne

Description générée automatiquementServeur 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 »

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

Description générée automatiquement

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 »

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

Description générée automatiquement

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.

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

Description générée automatiquement

***Activation du routeur :***

Taper la commande

* Nano /etc/sysct.conf

Activation du routeur :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

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

Description générée automatiquement

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

Description générée automatiquement

***Mise en place BIND 9 :***

Installation des services

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

Description générée automatiquement

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

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, noir et blanc

Description générée automatiquement

**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**

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

Description générée automatiquement

**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.**

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

**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".**

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

Description générée automatiquement

**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

Une image contenant texte, Police, blanc, calligraphie

Description générée automatiquement

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.

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

Description générée automatiquement

**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**

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

Description générée automatiquement

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.

Une image contenant texte, Police, blanc

Description générée automatiquement

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

Description générée automatiquement

***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 :

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

Description générée automatiquement

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".

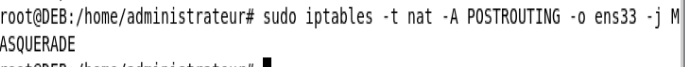
De manière similaire, nous ajoutons une autre zone "digitalschool.lan" avec les mêmes informations de configuration, mais avec le chemin du fichier de zone approprié.

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.

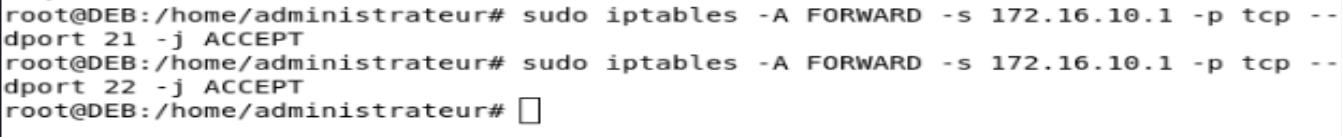
***CONFIGURATION IPTABLES***

Configuration des accès internet :

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



Configuration du LAN Administratif



Blocage des accès :



Sauvegarde des règles IPTABLES :



***Vérification des règles***

Nous vérifions les règles en utilisant la commande :

* sudo iptables -L

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

Description générée automatiquement

***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 sudp apt install apache2

***PROFTPD***

**APTUPDATE**

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

Description générée automatiquement

***SSH***

**APTUPDATE**

Une image contenant texte, capture d’écran, Police, noir et blanc

Description générée automatiquement

***SSL***

**APTUPDATE**

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

Description générée automatiquement

***CONFIGURATION DES SITES***

Il faut maintenant créer les deux différents sites :

**MBWAY :**





**DIGITALSCHOOL**



***CONFIGURATION HTTPS***

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

Description générée automatiquement



***Création certificat :***

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

Description générée automatiquement

***CONFIGURATION DES INTERFACES RESEAUX***

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquement

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.

Une image contenant texte, Appareils électroniques, capture d’écran, Police

Description générée automatiquement

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

***VIRTUAL HOST***



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

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

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

Description générée automatiquement

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

Description générée automatiquement

Et faire la même chose pour DIGITAL SCHOOL.

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

TEST MBWAY /



L’accès fonctionne correctement.



IDEM pour DIGITAL SCHOOL.

Le cahier des charges est donc respectté.