Dampierre
Lycée privé technologique & professionnel

BTS SIO
Services Informatiques aux Organisations

Rapport de projet
ARCHI-SITE

Équipe

Allan BERTHE
Thibaut ROUSSEAU

Année 2019

Introduction

Ce document a pour but de décrire le déroulement de notre projet PPE. C'est le résultat du travail qui nous a permis de réaliser toute une infrastructure système et réseau. Ce rapport est divisé en trois parties.

La première partie comporte les explications du point de vue technique, en commençant par une explication du contexte (Schéma réseau et configuration IP). Suivi d'une liste des étapes du travail réalisées (Screenshots) et pourquoi nous les avons réalisées.

La seconde partie inclue l'organisation des tâches réalisé par chacun d'entre nous.

La troisième et dernière partie sera nos conclusions personnelle et de groupe ainsi que une sitographie.

SOMMAIRE

I. Rapport technique

1. Cahier des charges

Définition du besoin

Définition de l'objet

Le laboratoire désire mettre à disposition des visiteurs médicaux une application Web permettant de centraliser les comptes-rendus de visite et la gestion des frais engagés.
L'entreprise a choisi d'héberger en interne les serveurs exécutant l'application.
L'achat de nouveaux équipements peut-être envisagé si le besoin le justifie.

Forme de l'objet

On souhaite une application en ligne, sécurisée, accessible par le FQDN visite.gsb.coop.
Le système doit donc être accessible depuis un navigateur.
L'application sera répartie sur plusieurs serveurs (physiques ou virtualisés).

Accessibilité/Sécurité

L'environnement doit être accessible aux seuls acteurs de l'entreprise.
Les données ne doivent pas être accessibles directement de l'extérieur mais uniquement par des interrogations réalisées par le serveur Web.

Le système sera accessible pour plusieurs usages :

- application de gestion des suivis (CR et Remboursement de frais) accessible à l'ensemble de la force commerciale,
- mise à jour des pages du site par les équipes du service développement,
- actualisation des données de traitement des frais par les personnels du service comptabilité

Contraintes

Environnement

L'environnement des serveurs est à déterminer : Linux, Windows Server, autre..
Les utilisateurs sont sous Windows 10.

Services

Pour chaque service, on précise les fonctionnalités à mettre en œuvre.
Pour le service de gestion des rapports:

- Un serveur Web sécurisé (HTTPS, SSL/TLS) exécutant des pages de script côté serveur (PHP...)
- Une base de données relationnelle, éventuellement administrable par interface Web.
- Les deux serveurs sont distincts
- On ne veut pas d'outils pré-configurés (LAMP, WAMP, EasyPHP, etc) mais des modules indépendants de manière à pouvoir changer d'environnement de l'un ou l'autre des modules.

Pour la mise à jour des pages Web :

- un service FTP avec authentification (par base de données, annuaire ou autre gestion d'utilisateurs) limitant l'accès aux seuls développeurs de l'entreprise.
- Ce service FTP est limité à un accès interne. Il ne doit pas être ouvert à l'extérieur.

Pour la gestion des frais

- les visiteurs alimentent les frais engagés par le biais du serveur web de gestion des rapports
- le service comptable met à jour la base de données par une page Web intégrée à l'intranet ou par un module de traitement automatique suite aux enregistrements comptables réalisés sur le PGI.

Contraintes

Les fichiers de configuration spécifiques au besoin seront épurés de tout commentaire inutile et d'options non retenues. Ils doivent être commentés sur les valeurs significatives retenues.

Sécurité

On préférera une authentification des visiteurs par certificat à celle par nom d'utilisateur et mot de passe mais ce n'est pas une obligation première.
Seul les protocoles nécessaires sont autorisés sur le pare-feu.

Aspect réseau

Le schéma fourni (Annexe et fichier GSB.schArchiSite.vsd) présente la solution à obtenir.
Le nombre de machines représenté peut être adapté (recours à de la virtualisation).
Documentation
La documentation complète, rédigée et mise en forme sera à rendre sous format électronique PDF.
Une fiche reprendra tous les éléments de configuration sans rédaction (paramétrages des services, adressage IP, comptes et mots de passe, etc.)

Responsabilités

Le commanditaire fournira à la demande toute information sur le contexte nécessaire à la mise en place de l'infrastructure.
Le commanditaire fournira une documentation et des sources exploitables pour la phase de test : base de données exemple, modélisation, schéma réseau,...
Le prestataire est à l'initiative de toute proposition technique. Notamment, il proposera des noms pertinents pour l'accès aux services (enregistrements DNS).
Le prestataire fournira un système opérationnel, une documentation technique permettant un transfert de compétence, une documentation de description de l'architecture (matériel, services et code) et des options particulières retenues dans le contexte.

2. Explication du contexte

Pour réalisé ce cahier des charges, nous allons installer 4 machines virtuelles sur VMWARE ESX :

- Un routeur : Opnsense avec 3 cartes réseaux (WAN, LAN, DMZ).

- Un serveur de BDD : debian 8 (Mysql)

- Un serveur Web : debian 8 (Apache, PHP 7)

- Un client : Windows 10

Nous allons ensuite faire les configuration Ip de base des machines (adresse IP, Masque, Passerelle, DNS).

Suivi du paramétrage du routeur pour un accès internet.

Puis l'installation des services sur les machines virtuelles (Apache, Mysql).

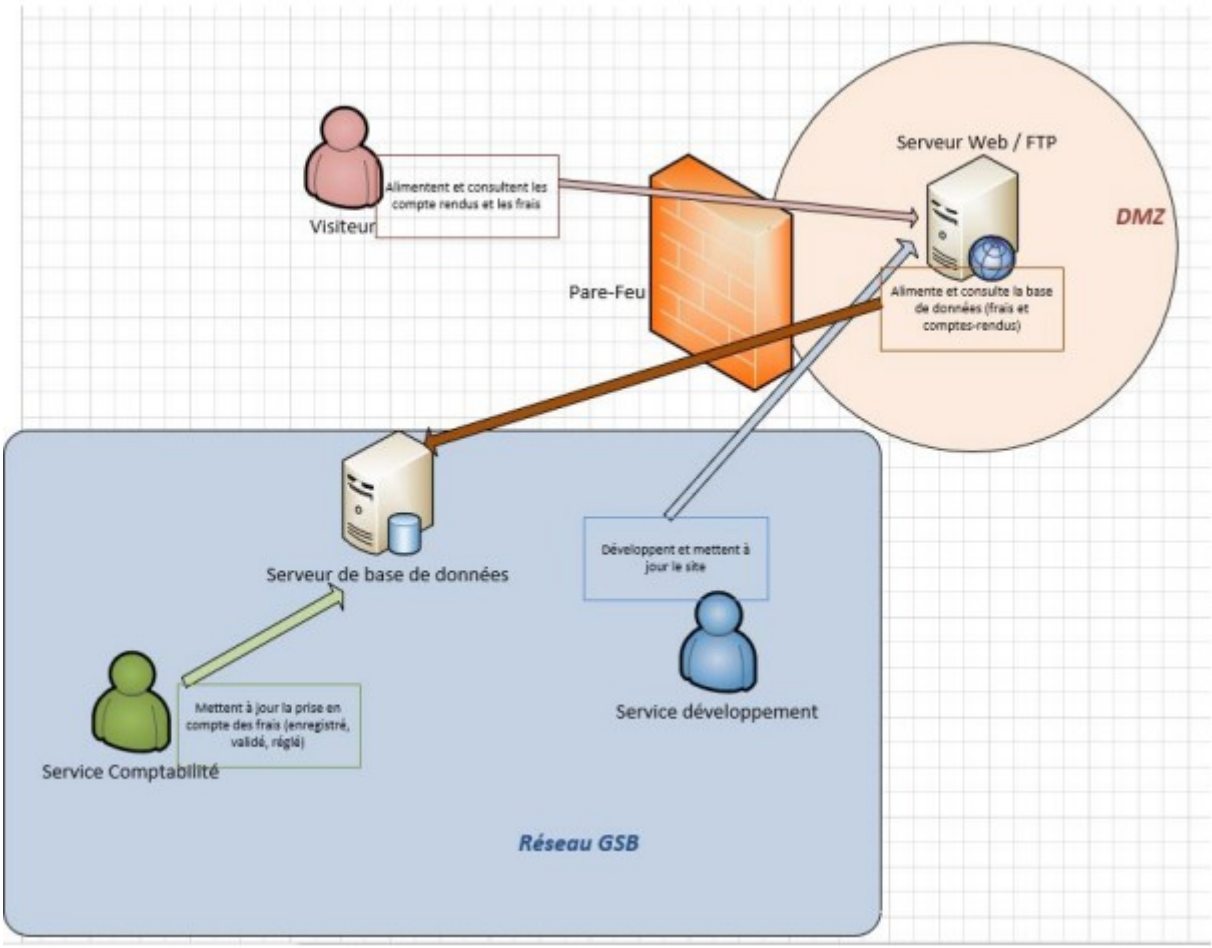
Ensuite l'installation du site : Web (Wordpress), BDD (sql).

Après le paramétrage du nom de domaine (FQDN (Full Quality Domain Name).

Et la configuration HTTPS (Certificat SSL).

Pour finir la configuration du Firewall (Règles, NAT).

Schéma réseau



Configuration IP

IP :

- **SIO : 192.168.0.0/16**

- **DMZ : 10.0.1.254/24**
- web : 10.0.1.1/24
- passerelle : 10.0.1.254/24
- DNS : 192.168.255.11

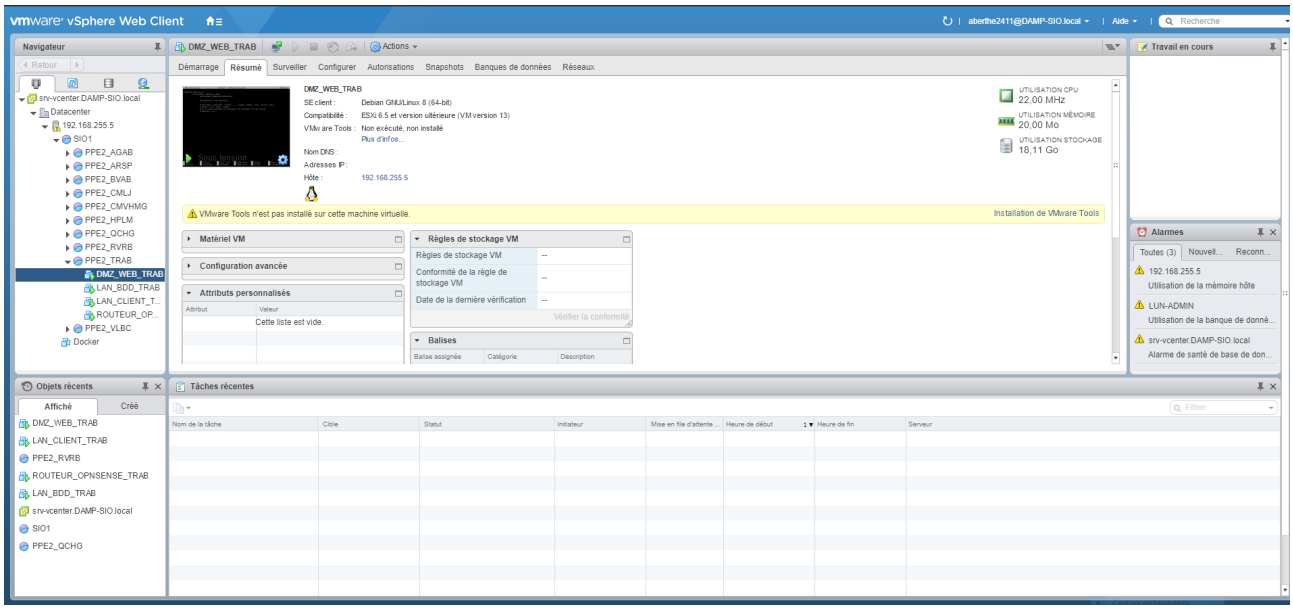
- **LAN : 10.0.0.254/24**
- BDD : 10.0.0.2/24
- client : 10.0.0.1/24
- passerelle : 10.0.0.254/24
- DNS : 192.168.255.11

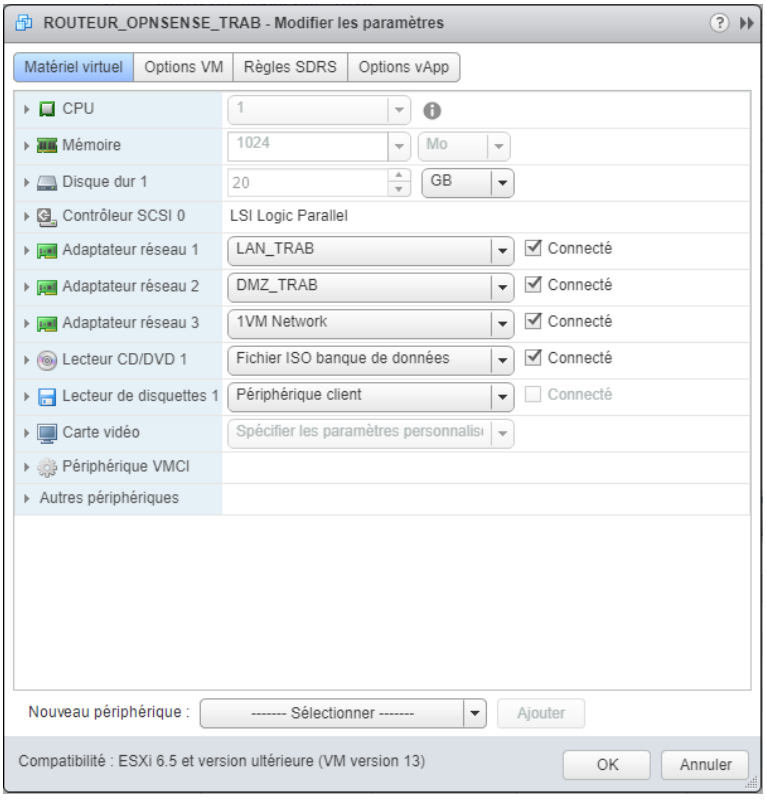
3. Taches réalisées

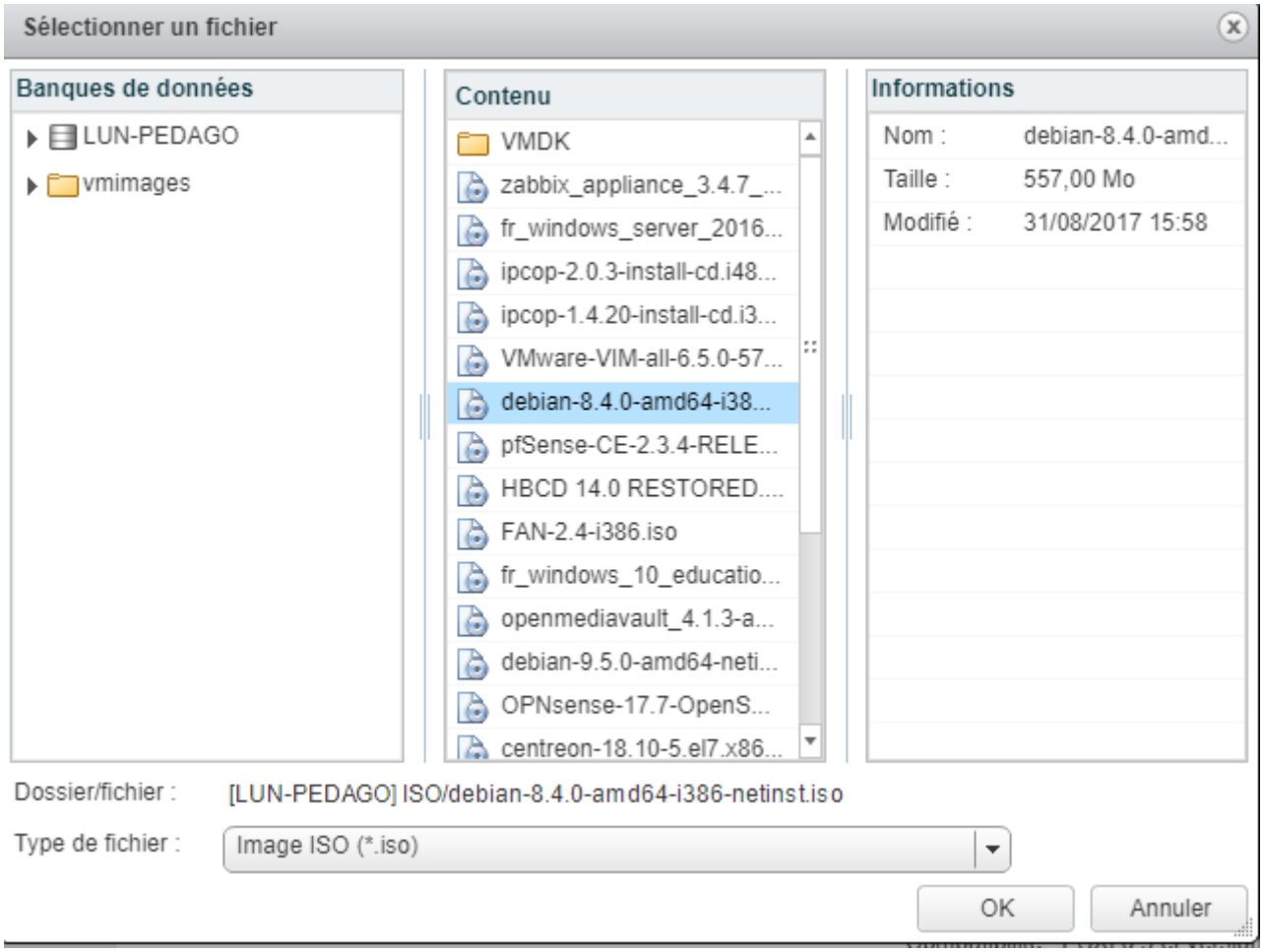
3.1. Création des machines virtuelles avec l'architecture

Sur l'interface VMWARE, nous avons créer nos 4 machines virtuelles:

- pour le routeur, nous avons paramétré 3 carte réseau (LAN, DMZ, 1VM Network ou WAN) pour sélectionner l'iso d'un opnsense dans une banque de donnée.

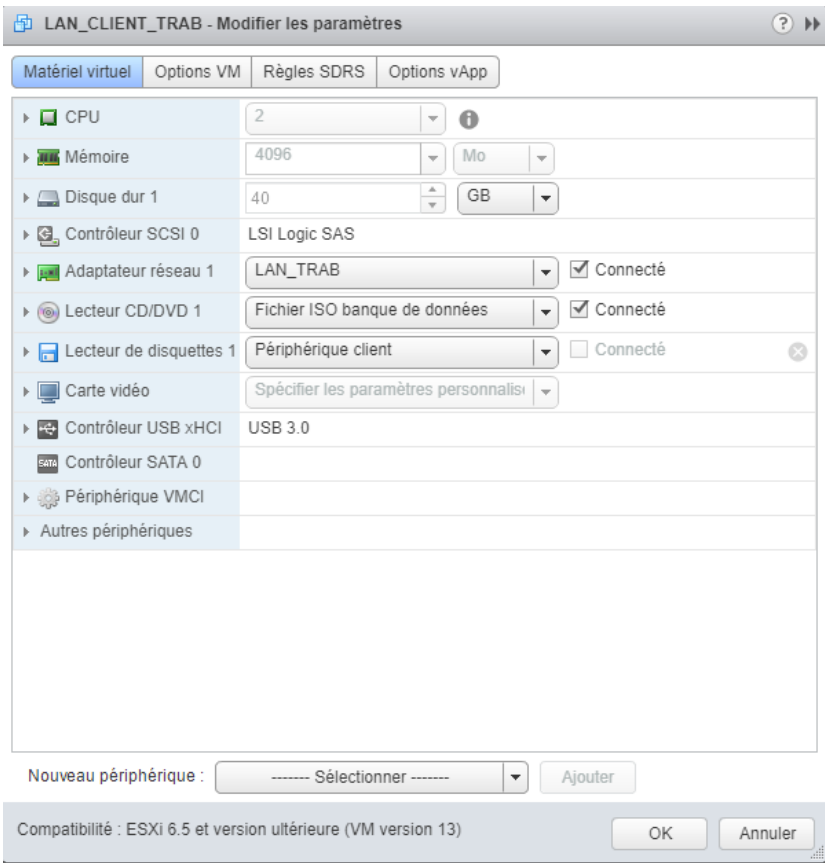




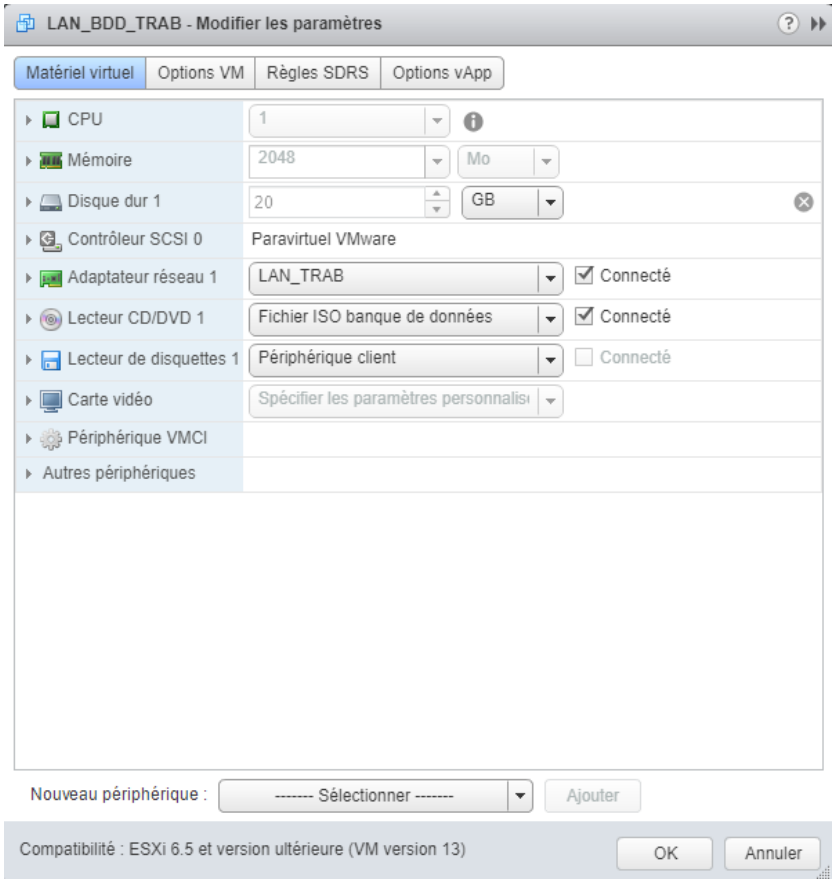


Pour les 3 autres VM, nous avons paramétré une seul carte réseau pour le client (ISO Windows 10) et le serveur BDD (ISO debian 8.4) la LAN, pour le serveur Web (ISO debian 8.4) la DMZ.

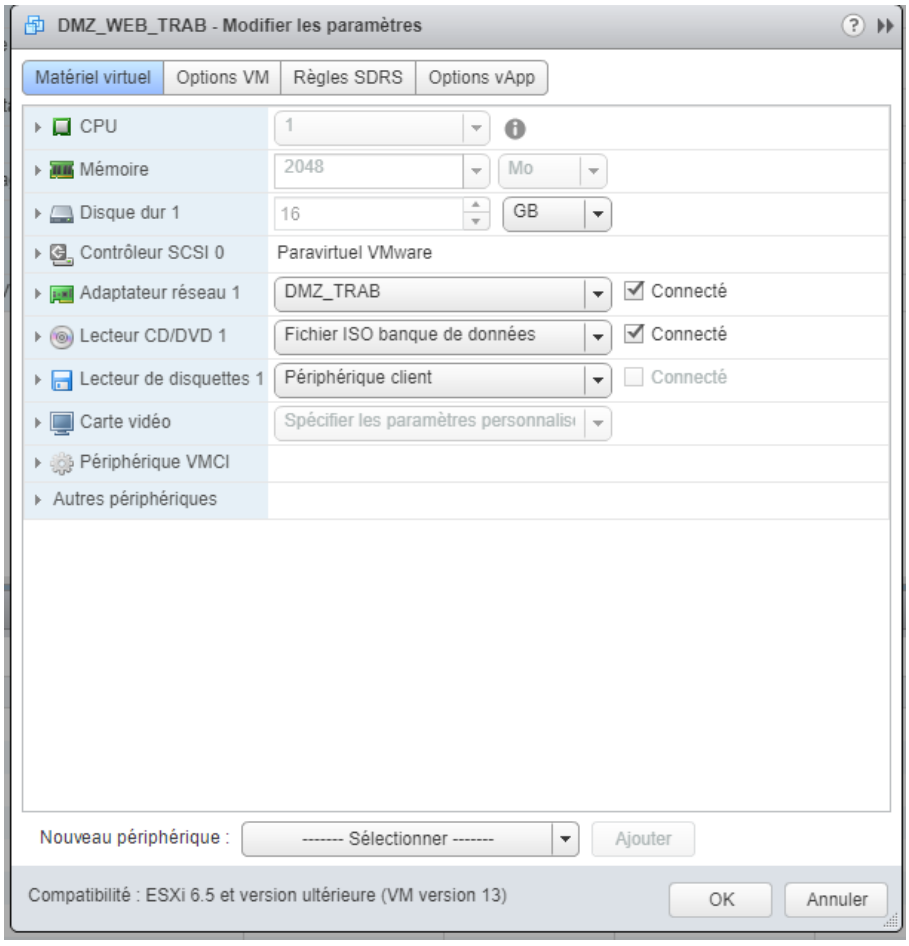
Client:



BDD:


LAN_BDD_TRAB - Modifier les paramètres
Matériel virtuel
Options VM
Règles SDRS
Options vApp
CPU
1
Mémoire
2048
Mo
Disque dur 1
20
GB
Contrôleur SCSI 0
Paravirtuel VMware
Adaptateur réseau 1
LAN_TRAB
Connecté
Lecteur CD/DVD 1
Fichier ISO banque de données
Connecté
Lecteur de disquettes 1
Périphérique client
Connecté
Carte vidéo
Spécifier les paramètres personnalisé
Périphérique VMCI
Autres périphériques
Nouveau périphérique :
------- Sélectionner -------
Ajouter
Compatibilité : ESXi 6.5 et version ultérieure (VM version 13)
OK
Annuler

WEB:


DMZ_WEB_TRAB - Modifier les paramètres
Matériel virtuel
Options VM
Règles SDRS
Options vApp
CPU
1
Mémoire
2048
Mo
Disque dur 1
16
GB
Contrôleur SCSI 0
Paravirtuel VMware
Adaptateur réseau 1
DMZ_TRAB
Connecté
Lecteur CD/DVD 1
Fichier ISO banque de données
Connecté
Lecteur de disquettes 1
Périphérique client
Connecté
Carte vidéo
Spécifier les paramètres personnalisé
Périphérique VMCI
Autres périphériques
Nouveau périphérique :
------- Sélectionner -------
Ajouter
Compatibilité : ESXi 6.5 et version ultérieure (VM version 13)
OK
Annuler

3.2. Configuration de base

Pour que les machines communiquer entre elle et puisse aller sur internet on fait les configuration Ip de base.

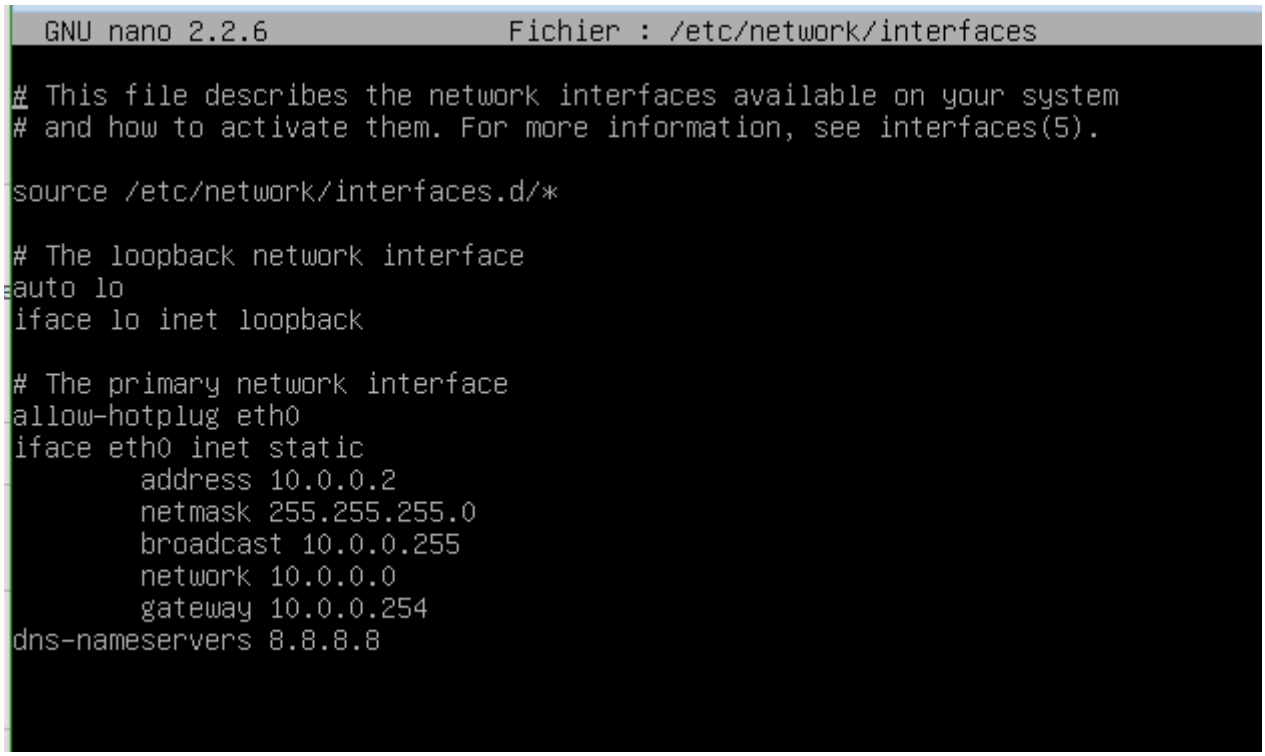
Pour le serveur de BDD et Web on utilise la commande **/etc/network/interfaces** puis on y ajoute l'adresse Ip, le masque, la passerelle, de réseau, de diffusion et le DNS:

Pour le serveur Web :

Ip : 10.0.1.1/24
Adresse réseau : 10.0.1.0
Adresse réseau : 10.0.1.255
Passerelle : 10.0.1.254/24 (Adresse Ip "patte" réseau de la DMZ)
DNS : 192.168.255.11 (Adresse Ip "patte réseau du WAN)

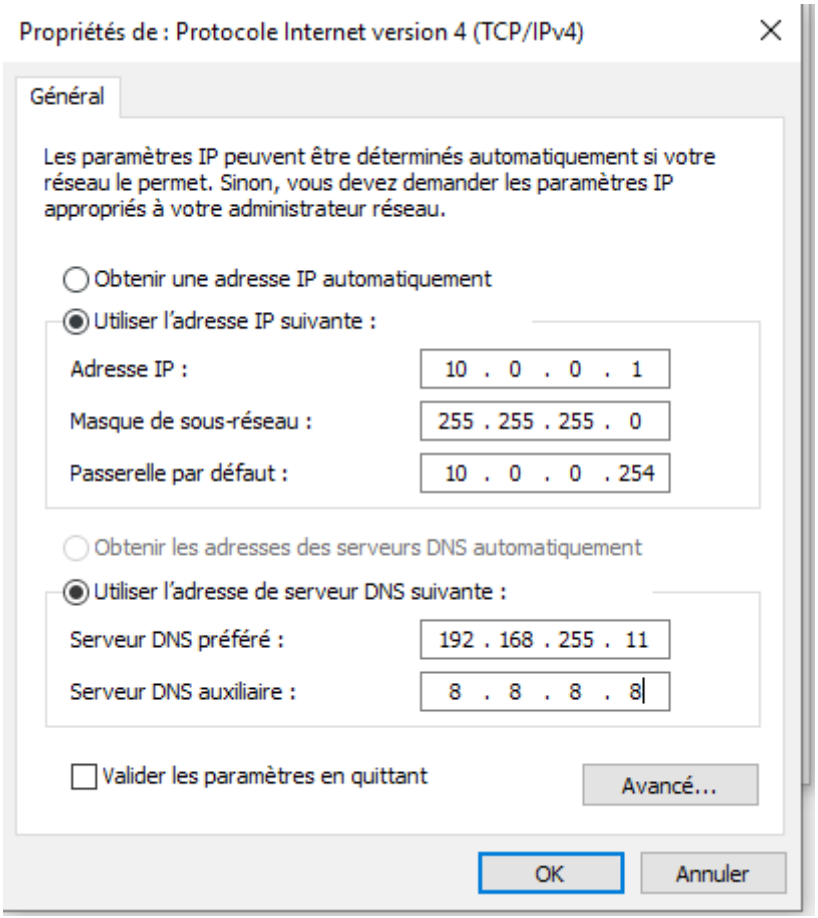
Pour le serveur de BDD :

Ip : 10.0.0.2/24
Adresse réseau : 10.0.0.0
Adresse réseau : 10.0.0.255
Passerelle : 10.0.0.254/24 (Adresse Ip "patte" réseau de la LAN)
DNS : 192.168.255.11 (Adresse Ip "patte réseau du WAN)



Pour changer le nom du serveur de BDD et Web on fait la commande **/etc/hostname**, puis on y place le nouveau nom, suivi de la commande **hostname + nouveau no** pour valider les changements.

Pour le client Windows 10, on va dans **"Panneau de configuration\Réseau et Internet\Connexions réseau"** puis on va dans les propriété IPV4 de la carte réseau et on y rentre Adresse Ip, masque de sous-réseau, passerelle et DNS principale et auxiliaire.



Pour renommer le client on va dans **"Système/information système"** puis renommer ce PC et on inscrit le nouveau nom.

3.3. Paramétrage du routeur OPNSENSE

Après l'installation d'opnsense, on va configuré les interfaces du routeur tout d'abord, on va assigner les 3 interfaces avec leur bonne adresse MAC
pour le WAN, LAN, DMZ.

```
0)     Logout                              7)     Ping host
1)     Assign interfaces                   8)     Shell
2)     Set interface(s) IP address         9)     pfTop
3)     Reset the root password             10)    Filter logs
4)     Reset to factory defaults           11)    Restart web interface
5)     Reboot system                       12)    Upgrade from console
6)     Halt system                         13)    Restore a configuration
```

Ensuite on va configuré des IP pour chaque interface.

DMZ : 10.0.1.254
LAN : 10.0.0.254
WAN : auto DHCP

```
0)     Logout                              7)     Ping host
1)     Assign interfaces                   8)     Shell
2)     Set interface(s) IP address         9)     pfTop
3)     Reset the root password             10)    Filter logs
4)     Reset to factory defaults           11)    Restart web interface
5)     Reboot system                       12)    Upgrade from console
6)     Halt system                         13)    Restore a configuration
```

3.4. Installation des services

Installer les services Apache, Php et mysql permettront de créer un serveur web en HTTP (voir HTTPS avec certificat SSL) qui aura accès a une BDD en mysql.

I - Pour le serveur Web, on doit installer les services apache2, PHP 7 et mysql client.

Pour le service Apache, on commence par mettre a jour le système avec la commande **apt-get update** puis on installe les paquet avec la commande **apt-get install apache2** pour vérifier que le service est bien démarré on utilise la commande **systemctl status apache2.service.**

Pour le service PHP, on va tout d'abord ajouté le dépôt Dotdeb aux sources logicielles car PHP 7 n'est pas dans les dépôts débian :
echo "deb http://packages.dotdeb.org jessie all" > /etc/apt/sources.list.d/dotdeb.list
wget https://www.dotdeb.org/dotdeb.gpg && apt-key add dotdeb.gpg

Puis on met a jour les sources logicielles :
apt-get update

Puis on installe les paquet PHP 7 :
apt-get install php7.0 php7.0-fpm

On rajoute un module pour qu'il soit compatible avec Apache2 :
apt-get install libapache2-mod-php7.0

Étant donné que Php est installé mais pas encore fonctionnel, on va modifier la config.

Ouvrez le fichier php.ini de php7.0-fpm avec nano
nano /etc/php/7.0/fpm/php.ini

La ligne :

cgi.fix_pathinfo=1

On la modifie pour :

cgi.fix_pathinfo=0

On va ensuite modifier le socket d'écoute de php7.0-fpm.

nano /etc/php/7.0/fpm/pool.d/www.conf

La ligne:

listen = /run/php/php7.0-fpm.sock

On la remplace par :

listen = 127.0.0.1:9000

On va donc redémarrer les différents services et tester :

service php7.0-fpm restart

Pour le service mysql client, on utilise la commande :
apt-get install mysql-client

II - Pour le serveur de BDD, on doit installer le service mysql.

Pour installer le service mysql-server, on utilise la commande
apt-get install mysql-server

3.5. Installation du site

Pour installer Wordpress, on utilise la commande :

apt install wordpress

Ensuite pour configurer le nom de domaine on fait:

nano /etc/apache2/sites-available/wp.conf

Puis on remplace le example.com par gsb.coop dans serverAdmin mais pour ServerName on remplace tout par visite.gsb.coop.

```
<VirtualHost *:80>
        ServerName myblog.example.com

        ServerAdmin webmaster@example.com
        DocumentRoot /usr/share/wordpress

        Alias /wp-content /var/lib/wordpress/wp-content
        <Directory /usr/share/wordpress>
            Options FollowSymLinks
            AllowOverride Limit Options FileInfo
            DirectoryIndex index.php
            Require all granted
        </Directory>
        <Directory /var/lib/wordpress/wp-content>
            Options FollowSymLinks
            Require all granted
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

3.6. Configuration HTTPS (certificat SSL)

Pour configuré le HTTPS, on configure un certificat SSL

On commence par activer le module avec la commande :

a2enmod ssl

Puis pour activer le site SSL on utilise la commande :

a2ensite visite.gsb.coop-ssl

Pour activer la nouvelle config on reload Apache2 :

service apache2 reaload

Pour verifier la config de visite.gsb.coop-ssl

cat *etc*apache2/sites-enabled/visite.gsb.coop-ssl.conf

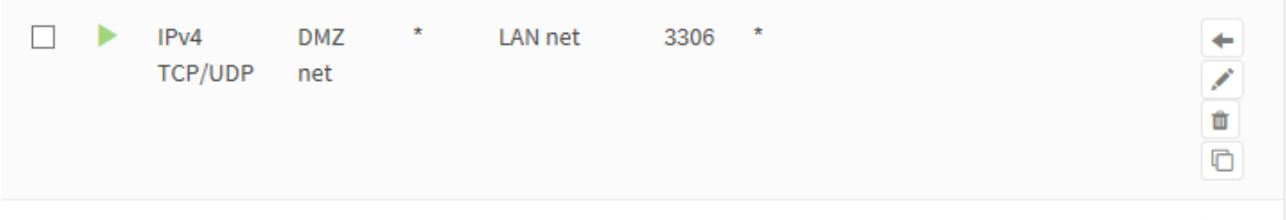
Pur vérifier le certificat ssl on accède au site avec un navigateur Web

https://10.0.1.1

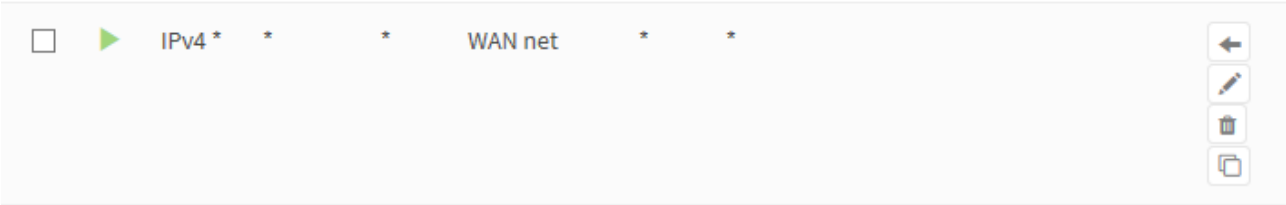
3.7. Configuration des règles du Firewall

On configure plusieurs règles :

- Une qui autorise la DMZ a communiquer avec le LAN sur le port 3306 en UDP/TCP.



- Une qui autorise que la DMZ et le LAN à communiquer avec le WAN sur tout les ports



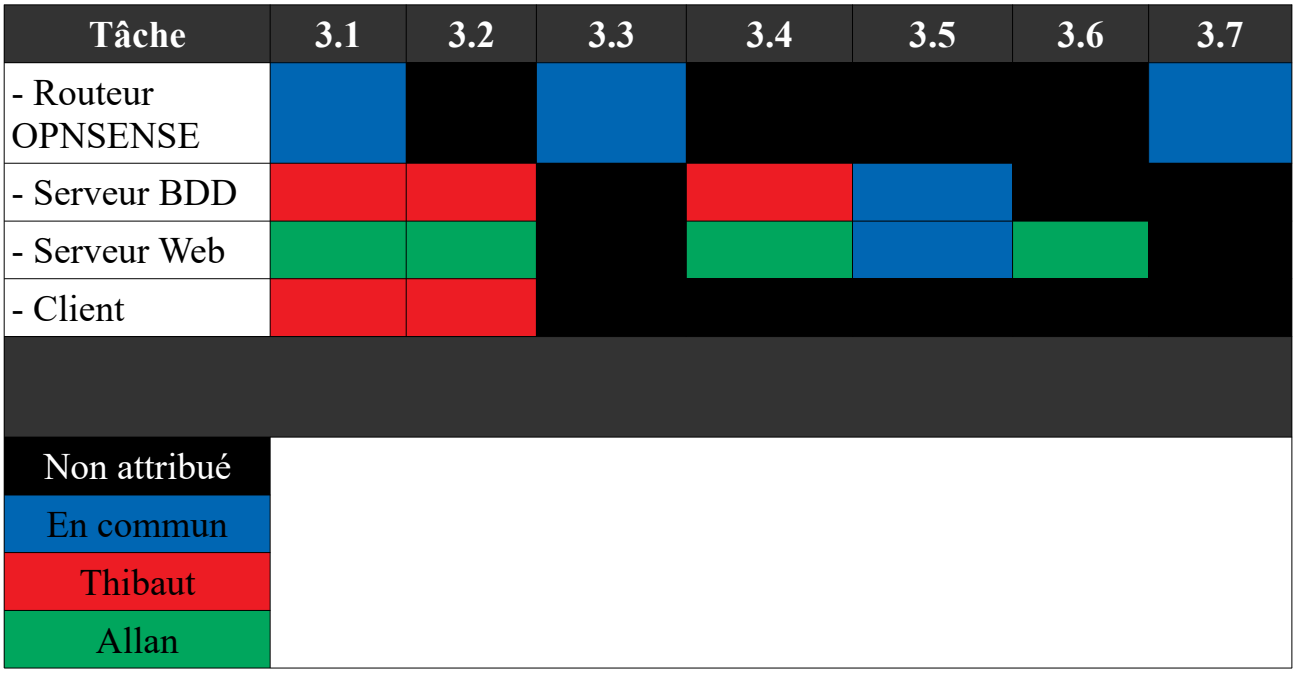
- Une qui autorise que le LAN à communiquer avec la DMZ sur tout les ports

- Une règle NAT qui redirige tout sur l'adresse 10.0.1.1 du serveur web avec le port 80

I. Organisation du groupe

1. Répartition des tâches

La quasi-totalité des taches ont étais réalisé ensemble mais étant donné qu'il y avait plusieurs machines ont avait chacun au moins une machine sur laquelle ont travaillé.



3.1. Création des machines virtuelles avec l'architecture
3.2. Configuration de base
3.3. Paramétrage du routeur OPNSENSE
3.4. Installation des services
3.5. Installation du site
3.6. Configuration HTTPS (certificat SSL)
3.7. Configuration des règles du Firewall

I. Conclusion

1. Conclusion personnelle

1.1 Conclusion de Thibaut

Pour conclure, je peux remarquer que toute nos tâches sont a la fois variées mais toute liées. Elle mon permit d'approfondir et de consolider mes connaissances dans les commandes Linux ainsi que sur le paramétrage de routeur (règles FW et NAT). Ce projet PPE a permet aussi que commencé a comprendre le faite de gérer toute une infrastructure réseau.

1.2 Conclusion d' Allan

Les diverses tâches de ce projet m'ont permis de rencontrer des problèmes jamais perçus auparavant, ce qui m'as permis d'acquérir de nouvelles compétences Linux et Windows dans la résolution de problèmes, j'ai également appris des commandes Linux utiles pour mes futures expériences professionnelles.

2. Conclusion de groupe

Le projet PPE ARCHI-SITE, nous demandé de travaillé avec des personnes avec lesquelles on avait pas travaillé avant, cela nous a fait comprendre l'importance du travail d'équipe a notre niveau mais aussi en entreprise, le faite de se partager les tâches pour avancer plus rapidement dans le projet.

3. Sitographie

Nous avons utilisé plusieurs sites web pour nous aider ainsi que des vidéos explicatives exemple :

https://www.youtube.com/watch?v=PXuXlXfByag
https://wiki.debian.org/WordPress#Installation_-_Debian_8_.28Jessie.29
https://www.alsacreations.com/tuto/lire/615-installation-configuration-MySQL.html
https://www.youtube.com/watch?v=0o0tSaVQfV4
https://wiki.debian.org/fr/MySql
https://www.osnet.eu/fr/content/tutoriels/installation-et-configuration-initiale-dopnsense
https://www.linode.com/docs/web-servers/apache/apache-web-server-debian-8/