

S3.01 - Développement d'application et Gestion de Projet

Enseignant tuteur : Nathalie VALLES-PARLANGEAU

Groupe n°1



## **SAE du Troisième Semestre**

- Pôle Systèmes et Réseaux -

Rapport de la création d'une infrastructure de déploiement web



Application Web Responsive de gestion de clubs sportifs amateurs

Matis Chabanat | Titouan Cocheril

Arthur Le Menn | Ivan Salle

---

TD1 | TP1

BUT Informatique - Parcours A

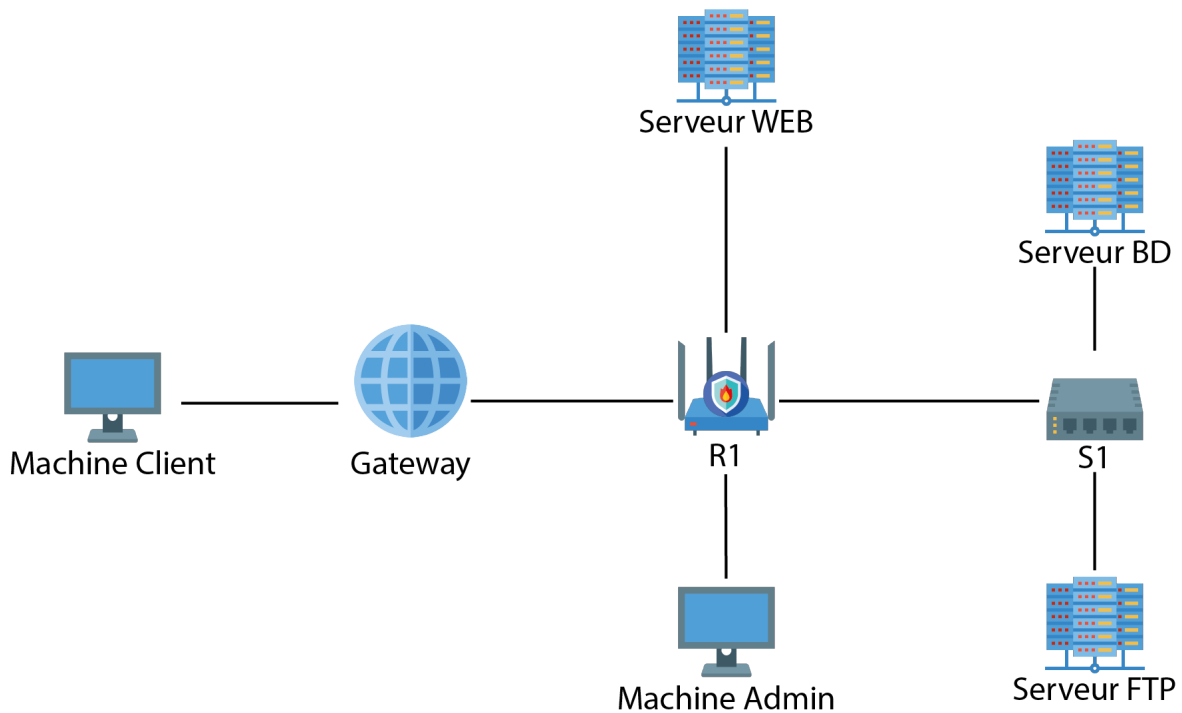
Semestre 3

- 2022 | 2023 -

# Sommaire

<b>1. Expression des besoins</b>	<b>3</b>
<b>2. Infrastructure du réseau</b>	<b>4</b>
<b>3. Matériel/logiciels nécessaire</b>	<b>5</b>
<b>4. Plan d'adressage</b>	<b>5</b>
<b>5. Sécurité du réseau</b>	<b>6</b>
<b>6. Procédures d'installation des services nécessaires</b>	<b>7</b>
<b>7. Configuration des services déployés</b>	<b>7</b>
<b>8. Résultats des tests effectués</b>	<b>7</b>

# Infrastructure de déploiement d'application web



## 1.Expression des besoins

Lors de cette SAÉ, nous allons devoir mettre en place une infrastructure réseau permettant de déployer une application web communicante. Cet exercice sera une simulation d'un environnement réseau réalisé sur le logiciel Marionnet. Héberger notre site web sur un serveur va nous permettre de le rendre accessible à tous via Internet.

Comme notre application web est destinée aux sportifs amateurs, elle accueillera beaucoup d'utilisateurs. Chaque utilisateur aura beaucoup de données correspondant à son profil. De plus, les fonctionnalités calendrier, messagerie et profil apporteront un traitement important de données. On prévoit donc un flux important de données. Enfin, dans la partie profil, on retrouvera des données privées que l'on se doit de protéger de part la structure du réseau.

Notre plateforme se doit d'être rapide d'utilisation pour un confort optimal de l'utilisateur. Il faudra donc que notre réseau d'hébergement soit le plus qualitatif possible afin de gérer les traitements de manière rapide et efficace.

## 2. Infrastructure du réseau

Pour cela, nous allons avoir besoin de plusieurs types de machines : les utilisateurs, les serveurs, sans oublier les routeurs. De plus, notre réseau sera relié à internet grâce à une Gateway (comparable à un routeur).

Nous avons choisi de placer 3 serveurs qui sont : le Serveur Web, le serveur Base de Données ainsi que le Serveur FTP.

Le Serveur Web se trouvera dans un sous réseau représentant la zone démilitarisée (DMZ). Cela aura pour objectif de renforcer le niveau de sécurité de notre réseau local en le séparant de l'Internet qui lui est une zone à risque. Le reste du réseau, lui, sera protégé par un pare-feu au niveau du Routeur.

Le Serveur FTP est nécessaire car nous allons devoir accéder à des fichiers se trouvant sur d'autres serveurs. Le FTP nous sera donc utile car il nous permettra, depuis un ordinateur de copier des fichiers vers un autre ordinateur du réseau ou encore de supprimer ou modifier des fichiers sur cet ordinateur.

Le Serveur BD sera relié avec le Serveur Web. Nous utiliserons MySQL pour modérer les données utilisées.

## 3. Matériel/logiciels nécessaires

- Serveur Web : 1 machine contenant le serveur web (interface HTML/CSS ainsi que traitements PHP).
- Serveur BD : 1 machine nécessaire.
- Serveur FTP : 1 machine nécessaire.

- 1 switch nécessaire pour relier les serveurs BD et FTP
- Machine DHCP : 1 machine à plusieurs cartes réseaux nécessaire.
- 1 machine correspondant à l'utilisateur Admin
- Accès Internet : 1 Gateway
- (Serveur DNS ? = +1 machine)

## 4. Plan d'adressage

Nous avons décidé d'adresser les machines à l'aide d'une machine DHCP car c'est plus rapide pour adresser que manuellement et de plus, c'est plus simple si on souhaite ajouter des machines supplémentaires.

Notre serveur local sera divisé en sous réseaux : la DMZ, les serveurs, ainsi que les machines utilisateurs. Comme il n'y a que 3 sous réseaux et donc pas beaucoup de machines, nous utiliserons des adresses IP privé de classe C.

Nous avons donc choisi comme adresse de réseau 192.168.0.0.

Afin d'établir un réseau supportant nos 3 sous réseaux, nous avons dû adopter un masque de 255.255.255.192 (notation CIDR : /26), réservant 2 bits aux adresses des sous réseaux.

Résumé de l'adressage de notre réseau :

Nom du SR	@sous-réseau	@broadcast	1ère @Machine utilisable	Dernière @Machine utilisable
SR1 (Web)	192.168.0.0	192.168.0.63	192.168.0.1	192.168.0.62
SR2 (BD + FTP)	192.168.0.64	192.168.0.127	192.168.0.65	192.168.0.126
SR3 (Users)	192.168.0.128	192.168.0.191	192.168.0.129	192.168.0.190

SR4 (inutilisé)	192.168.0.192	192.168.0.255	192.168.0.193	192.168.0.254
-----------------	---------------	---------------	---------------	---------------

## 5.Sécurité du réseau

Pour limiter au maximum les risques d'attaques et d'intrusions, nous allons mettre en place certaines mesures. Le réseau sera segmenté en différents sous réseaux, les communications dans le réseau seront régulées par des règles dans les iptables du routeur pour gérer les différents droits accordés à chaque machine et sous réseaux.

Certains sous réseaux seront des Zones Démilitarisées (DMZ) :

- Le sous réseau du serveur Web accessible par des utilisateurs via internet
- Le sous réseau de la zone de conformité.

Les flux entrants depuis internet seront seulement autorisés à accéder au serveur Web via les ports 80 et 443 qui sont respectivement les ports assignés au connexions HTTP et HTTPS.

Enfin, le port 22 des serveurs Web, FTP, et de la Base de Données seront ouverts et accessibles uniquement aux utilisateurs détenteurs d'une clé RSA autorisée en connexion ssh.

Pour que les communications soient chiffrées et que les messages ne circulent pas en clair dans le réseau nous allons créer un certificat SSL dans le serveur web.

Nous avons décidé de ne pas placer de répartiteur de charge car nous filtrons dès l'entrée sur le réseau les types de message possible.

## 6.Procédures d'installation des services nécessaires

7. Configuration des services déployés

8. Résultats des tests effectués