



IUT de Paris - Rives de Seine
Université Paris Cité

SAE 4.01 Parcours B FA – Rapport final
Application WEB de sondage & sécurité

Antonin RASKOPF

Ulrich SCHMITH

Yohan RUDNY

Allan HERILUS

Groupe 209

BUT 2 FA Parcours B – Semestre 4

Promotion 2022-2023

Partie I : Application WEB de sondage

1. Mise en contexte.....	3
1.1. Rappels sur la rénovation du site du Beauvaisis	3
1.2. Objectifs de l'application WEB mise en place	3
2. Développement Frontend.....	5
2.1. Page d'accueil.....	5
2.2. Formulaire de sondage.....	6
3. Développement Backend	7
3.1. Base de données relationnelle.....	7
3.2. Contrôles de saisie du formulaire.....	8
3.3. Aspects sécurité.....	9
3.4. Consultation des résultats.....	10

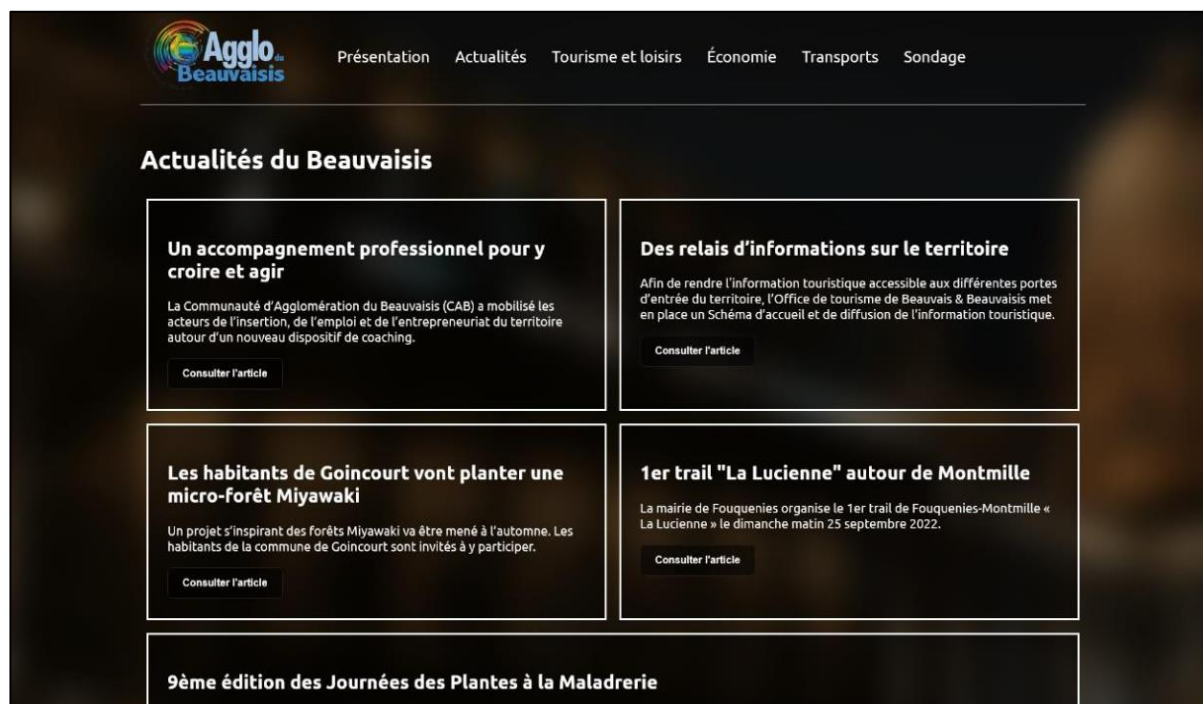
Lien vers l'application finale hébergée pour visualisation et tests :

<https://yohan-rudny.fr>

1. Mise en contexte

1.1. Rappel sur la rénovation du site du Beauvaisis

En fin d'année 2022, nous avons eu pour mission de proposer une version renouvelée, moderne et ergonomique d'un site d'agglomération de notre choix. Nous avons choisi d'effectuer des rénovations sur le site internet de l'agglomération du Beauvaisis. Le site a été rendu plus esthétique et accessible à tous par nos soins et tout le système d'actualités a été revu.



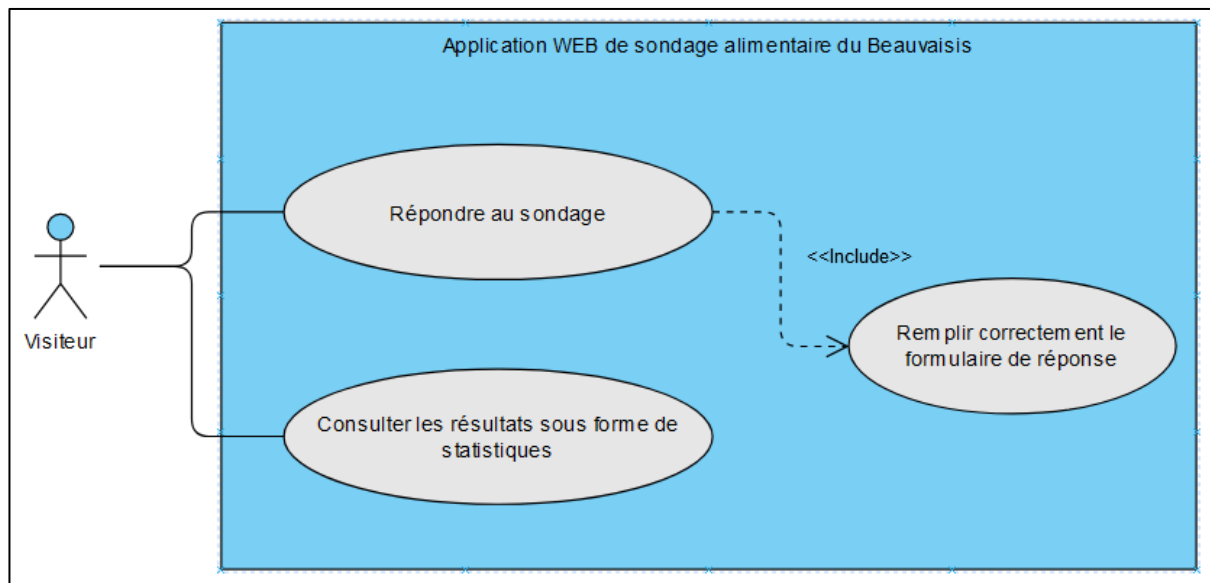
Le site internet, à ce moment-ci, proposait six sections distinctes consultables librement par tous les visiteurs.

1.2. Objectifs de l'application WEB mise en place

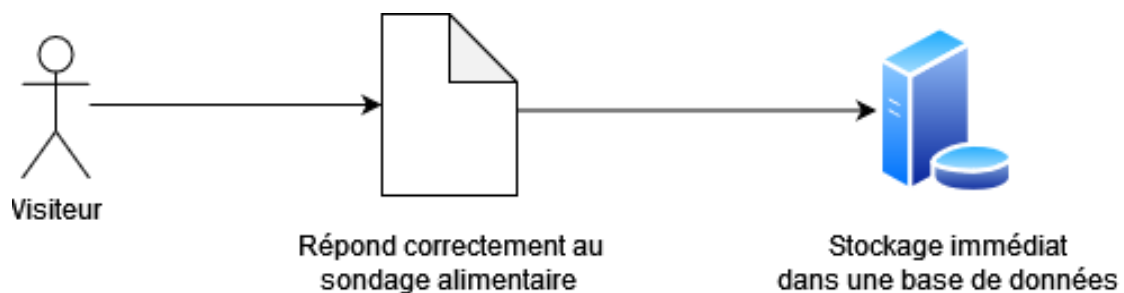
Notre site final proposait ainsi une section « Sondage » permettant de consulter sans aucune restriction les habitudes alimentaires ainsi que le score santé des personnes ayant répondu à un sondage sur leurs aliments préférés. Ces résultats reposaient uniquement sur des résultats pré-saisis. L'objectif ici est de développer une vraie page WEB de sondage (qui pourrait être intégrée au site) pour que, de manière intuitive, les habitants du Beauvaisis puissent répondre en indiquant leurs informations ainsi que leurs dix aliments préférés parmi un très large éventail de choix.

L'objectif primordial de ce sondage sera de rendre le formulaire le plus intuitif et contrôlé possible, de sorte que l'erreur de saisie devienne quasiment impossible par le visiteur. Il devra également s'adapter à tous types d'écran mais aussi proposer une consultation des résultats **sous forme statistiques uniquement** (et non pas en clair, ce qui remettrait en question **l'aspect éthique de notre service et la confidentialité** des informations fournies par les sondés).

En résumé : un visiteur du site aura comme pouvoir de répondre au sondage qui lui est proposé à condition de remplir correctement les champs du formulaire et il pourra également consulter les statistiques de réponses ayant été apportées au sondage.



Les réponses fournies par les visiteurs devront bien sûr être stockées dans une base de données qui sera exploitées par la page de consultation des résultats.

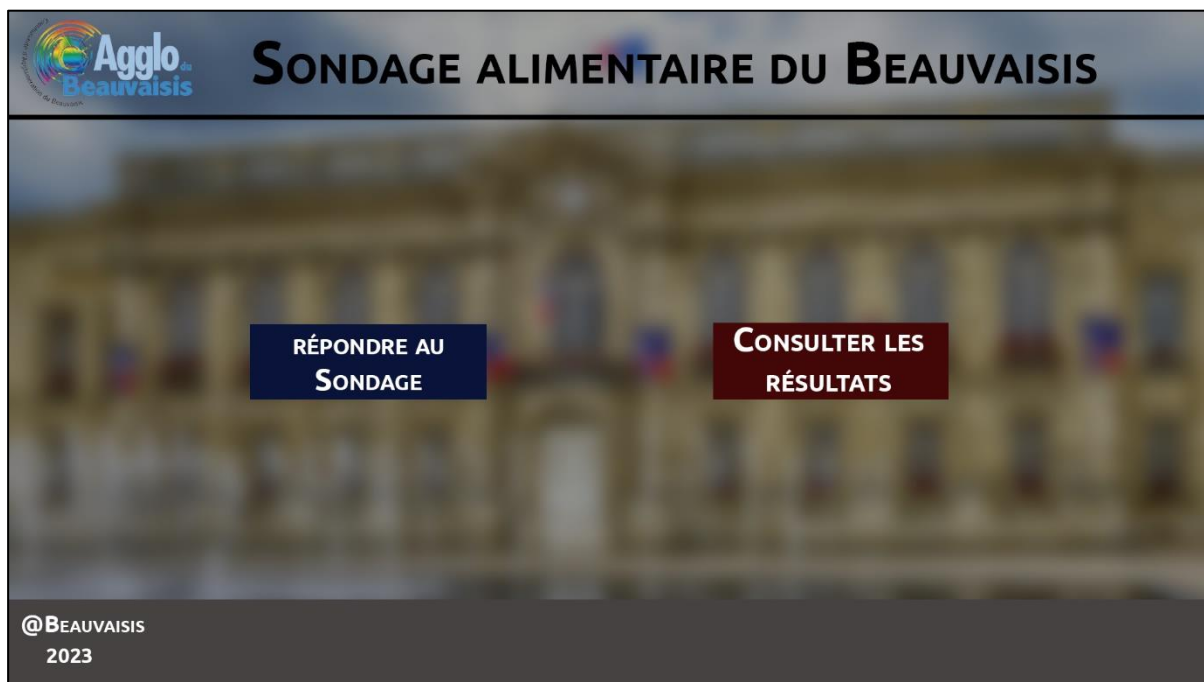


2. Développement Frontend

2.1. Page d'accueil

Pour réaliser la page d'accueil de notre service, nous avons gardé le même aspect graphique que le site rénové de l'agglomération du Beauvaisis. Le thème général est plutôt sombre pour un meilleur confort visuel et un message d'accueil nous indiquant les intentions (fictives ici) du sondage alimentaire et les deux boutons d'accès.

Maquette premièrement réalisée :

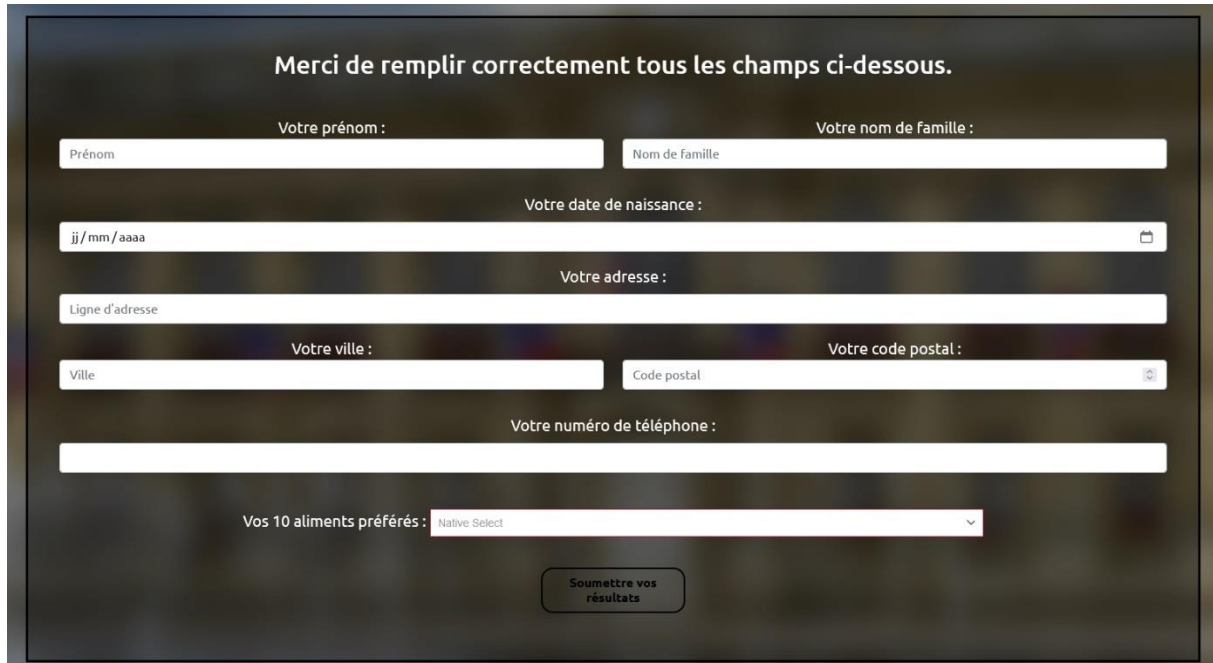


Page d'accueil finale du site :



2.2. Formulaire de sondage

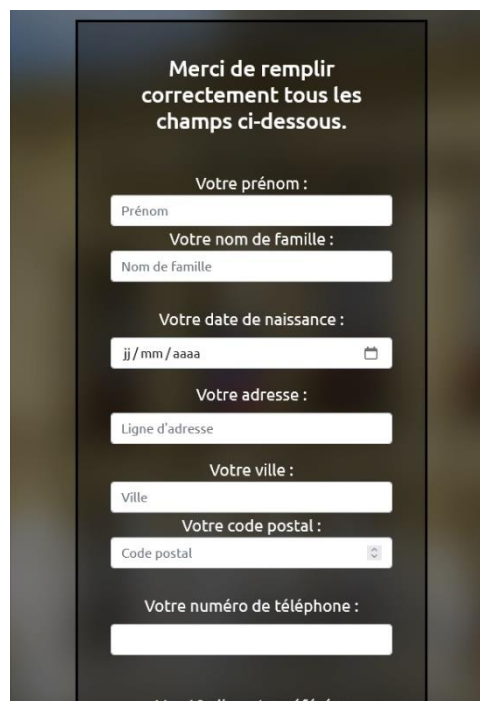
La mise en forme du formulaire permettant aux visiteurs de répondre au sondage à été faite à l'aide de Bootstrap afin de gagner du temps sur l'aspect esthétique (Bootstrap fournissant des formulaires très acceptables). Nous avons donc pu nous concentrer davantage sur le contrôle de saisie ainsi que la sécurité de ce formulaire.



The image shows a survey form titled "Merci de remplir correctement tous les champs ci-dessous." (Thank you for correctly filling out all the fields below). The form is set against a dark background with light-colored text and input fields. It includes the following fields: "Votre prénom :" (Your first name) with a text input labeled "Prénom"; "Votre nom de famille :" (Your last name) with a text input labeled "Nom de famille"; "Votre date de naissance :" (Your date of birth) with a date picker showing "jj/mm/aaaa"; "Votre adresse :" (Your address) with a text input labeled "Ligne d'adresse"; "Votre ville :" (Your city) with a text input labeled "Ville"; "Votre code postal :" (Your postal code) with a text input labeled "Code postal" and a location icon; "Votre numéro de téléphone :" (Your phone number) with a text input; and "Vos 10 aliments préférés :" (Your 10 favorite foods) with a dropdown menu labeled "Native Select". A "Soumettre vos résultats" (Submit your results) button is at the bottom.

Certains champs sont directement gérés nativement par Bootstrap pour contrôler la saisie (le bouton de soumission sera désactivé tant que ceux-ci ne seront pas corrects) et d'autres, plus techniques, sont gérés au niveau du backend et d'une API.

Le fichier style CSS du projet gère le responsive de ce formulaire qui s'adapte aux appareils mobiles.



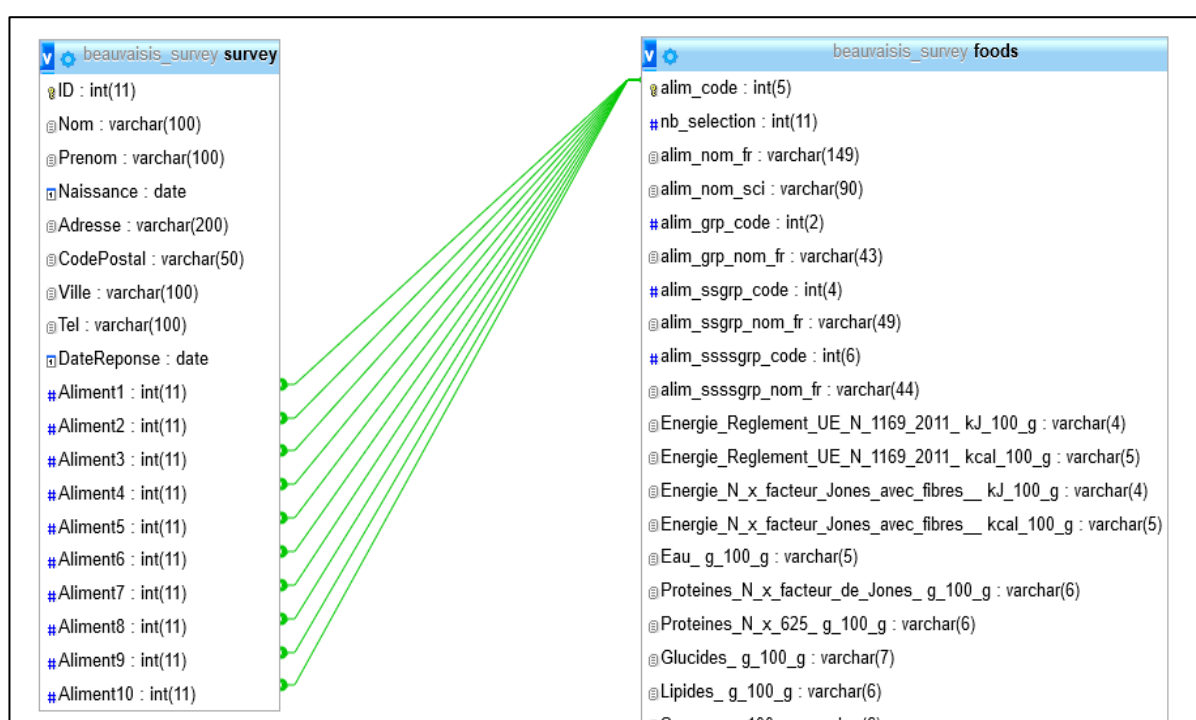
The image shows the same survey form as above, but adapted for a mobile device. The layout is vertical, with fields stacked one on top of the other. The text and input fields are centered and scaled appropriately for the smaller screen. The "Soumettre vos résultats" button is at the bottom. The form title "Merci de remplir correctement tous les champs ci-dessous." is also present.

3. Développement Backend

3.1. Base de données relationnelle

Notre base de données ne se compose que de deux tables :

- « **foods** » : représente, colonnes par colonnes, le fichier Excel qui nous a été fourni et répertoriant tous les aliments disponibles pour répondre au sondage. Tous les renseignements y figurent. Nous y avons ajouté une colonne supplémentaire « **nb_selections** » indiquant le nombre de fois qu'un aliment a été sélectionné.
- « **survey** » : stock tous les résultats saisis par les visiteurs (leurs informations et les dix aliments qu'ils ont sélectionnés).



Deux triggers sont présents dans cette base de données et ont pour effet de mettre à jour les valeurs de la colonne « **nb_selection** » de chacun des aliments. Après l'insertion d'un nouveau résultat dans la table « **survey** », ce trigger incrémente ou, dans le cas d'une suppression de résultat, décrémente le nombre de sélections d'un aliment.

Nom du déclencheur	T_ADD_RECORD
Table	survey
Moment	AFTER
Événement	INSERT
Définition	<pre>1 UPDATE foods SET foods.nb_selection = foods.nb_selection + 1 2 WHERE NEW.Aliment1 = foods.alim_code 3 OR NEW.Aliment2 = foods.alim_code 4 OR NEW.Aliment3 = foods.alim_code 5 OR NEW.Aliment4 = foods.alim_code 6 OR NEW.Aliment5 = foods.alim_code 7 OR NEW.Aliment6 = foods.alim_code 8 OR NEW.Aliment7 = foods.alim_code 9 OR NEW.Aliment8 = foods.alim_code 10 OR NEW.Aliment9 = foods.alim_code 11 OR NEW.Aliment10 = foods.alim_code</pre>

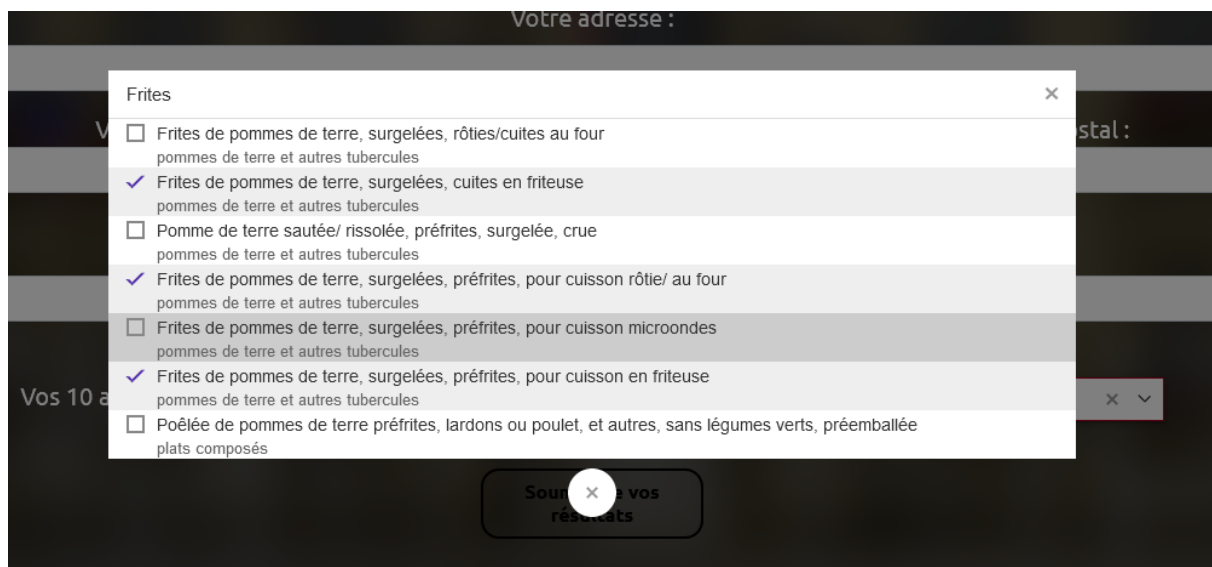
3.2. Contrôles de saisies du formulaire

La partie backend a principalement été développée à l'aide des langages **PHP** et **Javascript**. Les contrôles de saisie ne pouvant pas être gérés par Bootstrap se trouvent dans le fichier « **submitSurvey.php** »

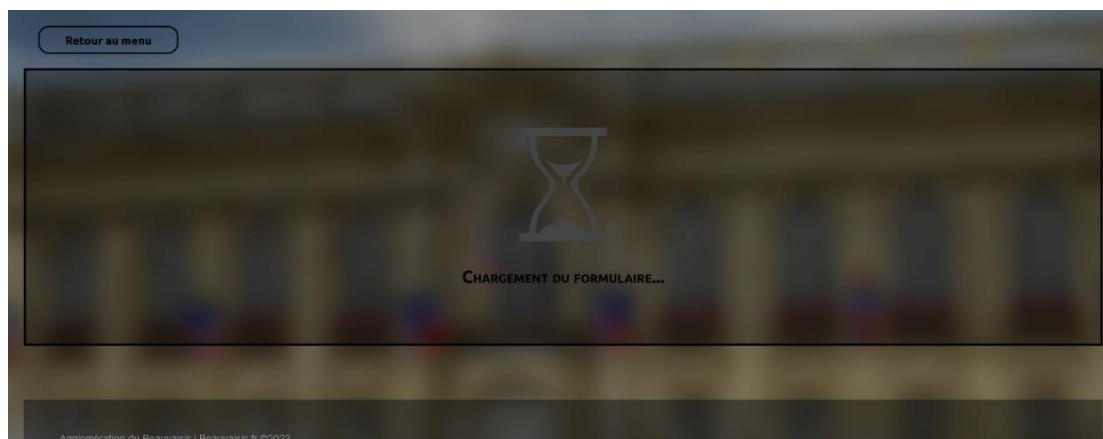
Pour que la saisie fonctionne, il ne faut qu'aucun champ de ne soit vide ou mal formaté selon l'information demandée.

Le choix des aliments a été fait à l'aide d'une API nommée « **VirtualSelect** » qui permet de proposer une interface de sélection multiples modulables et très esthétique pour tous formats d'écrans. Tout cela est configuré dans le fichier « **scriptSurvey.js** » qui, en utilisant l'API, récupère tous les aliments ainsi que toutes les catégories pour les ranger dans une liste déroulante. Il a alors été possible de contrôler ces aspects :

- Le nombre maximum d'aliments sélectionnables qui est de 10.
- Le nombre minimum de sélections pour que le formulaire soit validable, donc 10.
- Interdire de sélectionner plusieurs fois le même aliment.



Étant donné que la base de données est très conséquente et met quelques secondes à charger, nous avons mis en place un script permettant de bloquer la fenêtre avec un écran de chargement en attendant que toutes les données soient chargées et d'afficher le formulaire.



3.3. Aspects sécurité

L'accès à la base de données et la modification de celle-ci par un formulaire PHP nous oblige à mettre en place quelques mesures de sécurité au niveau du code de validation de celui-ci pour éviter plusieurs failles.

- Les injections SQL

Celles-ci consistent à **entrer volontairement des requêtes SQL** dans les cases du formulaire afin d'espérer que celui-ci s'exécute à la soumission de celui-ci et cause des dégâts sur la base de données. Pour éviter celle-ci, nous utilisons la fonction « **prepare** » qui permet de **préparer une requête** avant d'exécuter celle-ci en insérer simplement des attributs, qui ne seront donc jamais considérés comme du code SQL mais de simples données.

```
$insert = $db->prepare('INSERT INTO `survey` (`ID`, `Nom`, `Prenom`, `Naissance`, `Adresse`, `CodePostal`, `Ville`, `Tel`, `DateReponse`,
$insert->execute(array(
    'firstname' => $firstName,
    'lastname' => $lastName,
    'birthdate' => $birthDate,
    'address' => $address,
    'postalcode' => $postalCode,
    'city' => $city,
    'phone' => $phone,
    'answerdate' => date('y-m-d'),
```

- La faille XSS

De son côté, la faille XSS permet d'**injecter du contenu dans une page WEB** à des fins malveillantes en insérant du code JavaScript dans les champs de réponses. Pour éviter cette faille, nous encadrons les balises important les données en PHP avec la fonction « **htmlspecialchars** » qui permet d'éviter cette faille.

```
$firstName = ucfirst(strtolower(htmlspecialchars($_POST['firstName'])));
$lastName = strtoupper(htmlspecialchars($_POST['lastName']));
$birthDate = htmlspecialchars($_POST['birthDate']);
$address = htmlspecialchars($_POST['address']);
$city = htmlspecialchars($_POST['city']);
$postalCode = htmlspecialchars($_POST['postalCode']);
$phone = htmlspecialchars($_POST['phone']);
$food = explode(",", $_POST['foods']);
```

3.4. Consultation des résultats

Comme résultats consultables par les visiteurs, nous avons choisi deux statistiques qui peuvent être intéressantes à consulter :

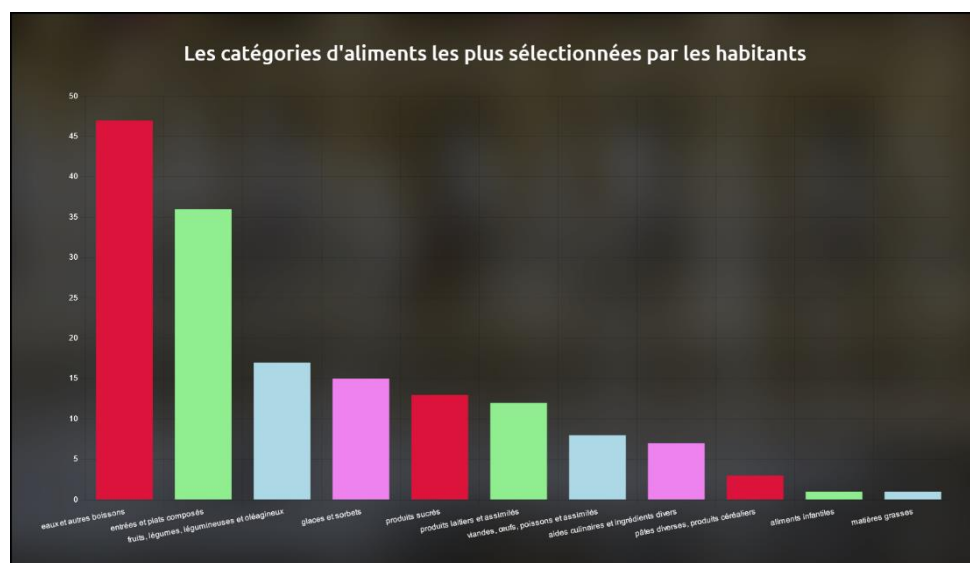
- Le top 20 des aliments les plus sélectionnés

Sous forme d'un tableau, nous pouvons consulter les 20 aliments les plus sélectionnés par les sondés. Pour se faire, nous avons simplement, dans « **getTop20.php** » récupérer avec une limite de 20 les aliments par nombre de sélections décroissant. Le tout a été rangé dans un tableau HTML.

Retour au menu		
Les 20 aliments les plus sélectionnés par les habitants		
Produit	Catégorie	Sélections
Pâtes à la carbonara (spaghetti, tagliatelles...)	plats composés	10
Épinard, cuit	légumes	6
Hamburger, provenant de fast food	sandwichs	5
Jus d'orange, pur jus	boissons sans alcool	5
Quiche lorraine, préemballée	pizzas, tartes et crêpes salées	5
Jus de pomme, pur jus	boissons sans alcool	5
Vodka	boisson alcoolisées	4
Salade César au poulet (salade verte, fromage, croûtons, sauce), pr...	salades composées et crudités	3
Saumon à l'oseille, préemballé	plats composés	3
Profiterole avec glace vanille et sauce chocolat	desserts glacés	2
Aligot (purée de pomme de terre à la tomme fraîche), préemballé	plats composés	2
Cocktail à base de rhum	boisson alcoolisées	2
Jus de pomme BIO, pur jus	boissons sans alcool	2

- Graphique des catégories les plus sélectionnées

Depuis un graphique en bâton, chaque visiteur peut consulter les catégories d'aliments les plus prisées par les personnes sondées. Nous avons ici utilisé une autre API nommée « Charts » permettant de créer des diagrammes en bâtons. Les données sont récupérées depuis « **getTopCateg.php** » et exploitées par « **scriptResult.js** ».



Partie II : Installation d'une architecture de sécurité

4. Prérequis & outils à mettre en œuvre.....	12
4.1. Système d'exploitation.....	12
4.2. Matériel physique à installer	12
5. Plan d'adressage des réseaux.....	13
5.1. Réseau privé GAUCHE.....	13
5.2. Réseau internet MILIEU.....	13
5.3. Réseau intranet DROITE.....	13
6. Configurations des machines	14
6.1. Ordre de configuration.....	14
6.2. Serveur WEB public : machine n°3	14
6.3. Serveur WEB privé : machine n°5.....	16
6.4. Serveur NAT : machine n°2.....	16
6.5. Serveur VPN : machine n°4.....	18
6.6. Client final (NAT + VPN) : machine n°1 (User guide)	20
6.7. Tableau récapitulatif de l'architecture	24
7. F.A.Q sécurité & maintenance	25
8. Synthèse globale du projet	26

Introduction

Cette notice d'installation a pour objectif de démontrer la procédure d'installation d'une architecture réseau permettant l'accès à un intranet depuis un réseau privé via un réseau intermédiaire. L'installation présentée ici est a pour but de **tester le fonctionnement** de l'architecture directement depuis un réseau local déjà configuré. Dans un cas d'utilisation réel, il est nécessaire de déployer l'architecture plus globalement sur de vrais serveurs distants, le fonctionnement restant identique

4. Prérequis et outils à mettre en œuvre

4.1. Système d'exploitation

Pour commencer à créer notre architecture réseau, il nous faut sélectionner le système d'exploitation qui sera installé et utilisé par les différents serveurs. Il en existe plusieurs qui peuvent être spécialisés pour fonctionner sur des machines serveurs (Debian, Ubuntu, Windows Server, CentOS...). Nous devons mettre en place à la fois des serveurs WEB et des serveurs VPN/NAT, ce qui demande des fonctionnalités supplémentaires qui ne se configurent pas de la même manière suivant le système d'exploitation utilisé.

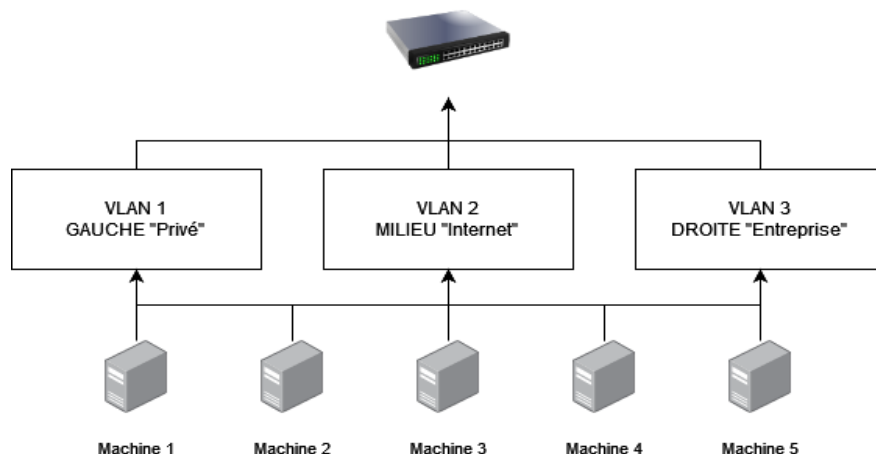
L'objectif étant de créer une architecture facilement maintenable, robuste et intuitive : **nous avons choisi de faire fonctionner le tout sur des machines Windows Server 2022**. Ce choix s'explique par l'intégration possible d'une interface graphique à l'OS (il est aussi possible de n'utiliser que du PowerShell) ce qui simplifie énormément l'installation des différents services. Le gestionnaire de serveur est très intuitif et n'importe quelle personne formée à la configuration de services est capable (à l'aide de ce document) de maintenir l'architecture et d'ajouter des fonctionnalités si besoin.

Les cinq machines ont donc une distribution Windows Server 2022 d'installée et activée (à l'aide d'une licence d'entreprise déployée). Il a été choisi la dernière édition et non pas une ancienne car celle-ci reçoit encore les mises à jour de sécurité Microsoft contrairement à son prédécesseur de 2019 dont la fin du support standard est prévu pour début 2024.



4.2. Matériel physique à installer

L'installation se décompose en trois réseaux distincts portant chacun un rôle spécifique (privé, internet et entreprise). Afin d'isoler au mieux ceux-ci, l'idéal est de mettre en place des **réseaux virtuels (VLAN)** pour qu'il n'y ait besoin que d'un seul switch. Celui-ci doit donc être compatible VLAN avec une interface graphique et les cinq machines doivent y être reliées. Depuis l'interface WEB de configuration du switch, **il nous faut créer trois VLANs** avec les ports associés (à déterminer en fonction du nombre de machines sur chacun des réseaux). Les routes entre les VLANs sont également à configurer depuis l'interface.



5. Plans d'adressage des réseaux

Chacun des trois réseaux en place possède une plage d'adresse choisie distinctement afin de répondre au mieux aux besoins exprimés. Un plan d'adressage est donc proposé pour ces réseaux, ceux des machines seront dévoilés dans la partie de la notice qui leur est dédiée. Les adresses IP sont toutes de classe C car le nombre d'hôtes connectés n'est supposé pas élevé dans le cadre de la mise en place de notre configuration.

5.1. Réseau privé GAUCHE – VLAN 1

Cette partie est un réseau local (LAN) accueillant les clients VPN et NAT qui se connecteront à l'intranet du réseau droite. Elle suit le plan d'adressage suivant :

- Masque de sous-réseau : **255.255.255.0**
- Plage d'adresses disponibles pour les clients : **192.168.1.1 à 192.168.1.254**
- Adresse de réseau : **192.168.1.0**
- Adresse de broadcast : **192.168.1.255**

Seule la machine n°1, représentant le client, est connectée à ce réseau. Il est géré par le

5.2. Réseau internet MILIEU – VLAN 2

Ce réseau joue, dans notre architecture, le rôle d'internet et sert d'intermédiaire entre le réseau privé et l'intranet. Il s'agit d'un réseau public contenant un serveur WEB destiné à accueillir tous les potentiels clients de notre site.

- Masque de sous-réseau : **255.255.255.0**
- Plage d'adresses disponibles pour les clients : **192.168.2.1 à 192.168.2.254**
- Adresse de réseau : **192.168.2.0**
- Adresse de broadcast : **192.168.2.255**

Les machines n°3 (Serveur WEB Internet) et n°4 (Serveur VPN + NAT) seront connectés à ce réseau.

5.3. Réseau entreprise/intranet DROITE – VLAN 3

Ce dernier réseau est celui qui est destiné à l'entreprise sur lequel sera connecté un serveur WEB qui hébergera l'intranet. Celui-ci est protégé par un accès VPN dans le but que seuls les clients VPN puissent y accéder.

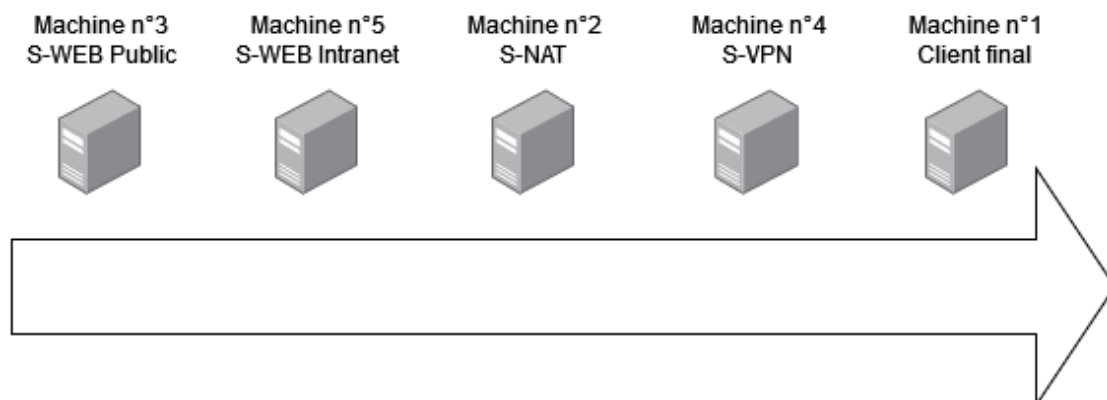
- Masque de sous-réseau : **255.255.255.0**
- Plage d'adresses disponibles pour les clients : **192.168.3.1 à 192.168.3.254**
- Adresse de réseau : **192.168.3.0**
- Adresse de broadcast : **192.168.3.255**

La machine n°5 sera la seule connectée à cette partie, elle héberge le site WEB intranet de l'entreprise.

6. Configuration des machines

6.1. Ordre de configuration

Avant de commencer, il est important de **suivre un ordre précis dans la configuration des cinq machines** de notre plan. Elle doit se faire des machines ayant le moins au plus de fonctionnalités en terminant par la mise en route du client final. Le schéma ci-dessous résume l'ordre dans lequel il faut mettre en place notre architecture sans problème.



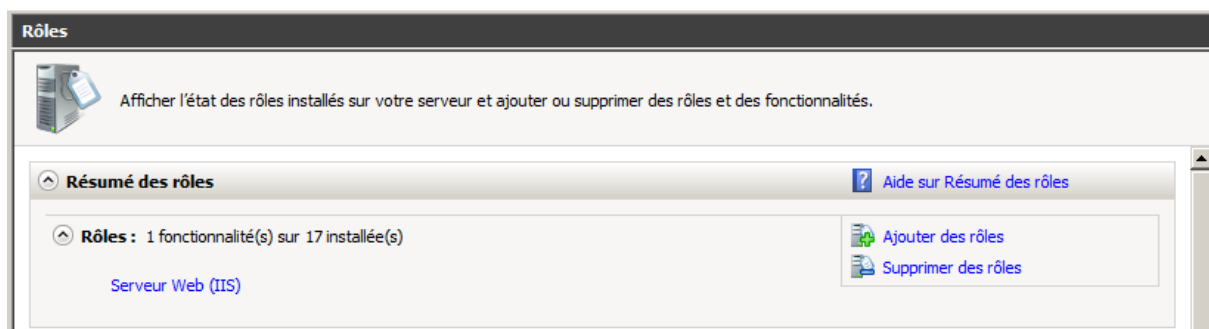
6.2. Serveur WEB public : machine n°3

Cette machine comporte un service de serveur WEB public et consiste en l'hébergement de notre application de sondage qui sera disponible au grand public. La base de données utilisée par l'application doit également être hébergée sur cette machine.

- Rôle : **Serveur WEB internet**
- Nombre de cartes réseaux : 1
- Emplacement réseau : **Réseau internet MILIEU**
- Adresse IPv4 : **192.168.2.20/24**
- Masque de sous-réseau : **255.255.255.0**
- Passerelle par défaut : **192.168.3.10**

Pour installer le rôle de serveur WEB, il faut se rendre dans le gestionnaire de serveurs Windows et installer le rôle « Serveur WEB IIS ». En laissant tout par défaut, terminer l'installation et vérifier que le rôle soit fonctionnel et que la machine ait un accès à un internet.

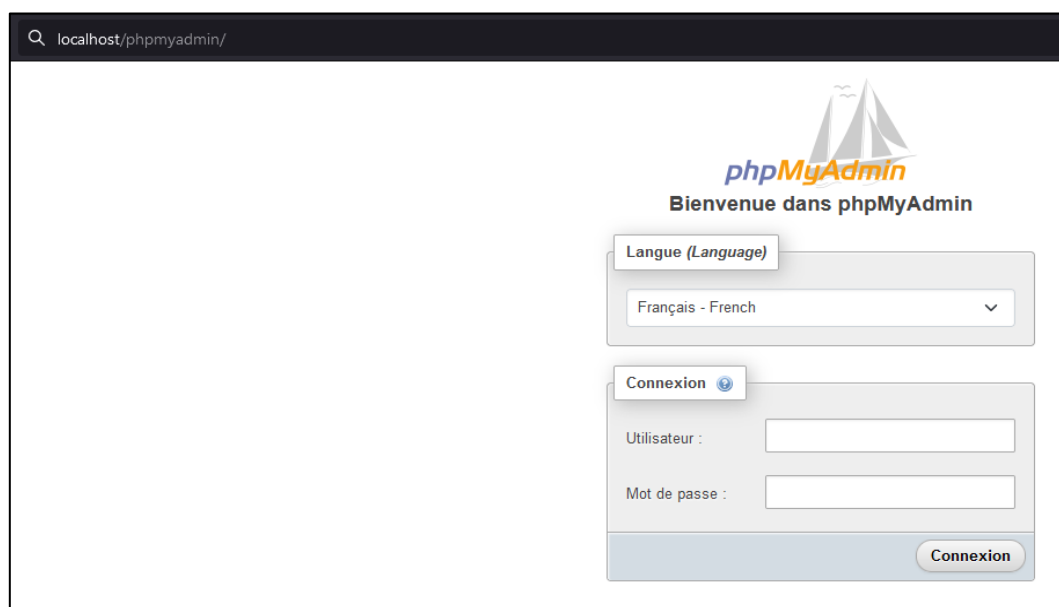
Une fois le rôle installé, il suffit de copier les fichiers de l'application WEB de sondage du Beauvaisis à l'intérieur de l'emplacement `C: \inetpub \wwwroot`.



Vérifier ensuite que le site WEB est bien fonctionnel en localhost depuis le navigateur de Windows Server.



La base de données utilisée par l'application doit également être hébergée sur cette machine au port utilisé par MySQL (3306). Cela peut se faire en installant le SGBD utilisé (PhpMyAdmin) sur la machine.



La configuration de cette machine est terminée. Celle-ci ne servant qu'à héberger le site, il sera accessible en passant par le serveur NAT de la machine n°2 qui permettra créer une règle autorisant les clients du réseau privé à accéder à l'application (sur le réseau internet) et de bloquer l'accès depuis internet au réseau privé.

6.3. Serveur WEB Intranet : machine n°5

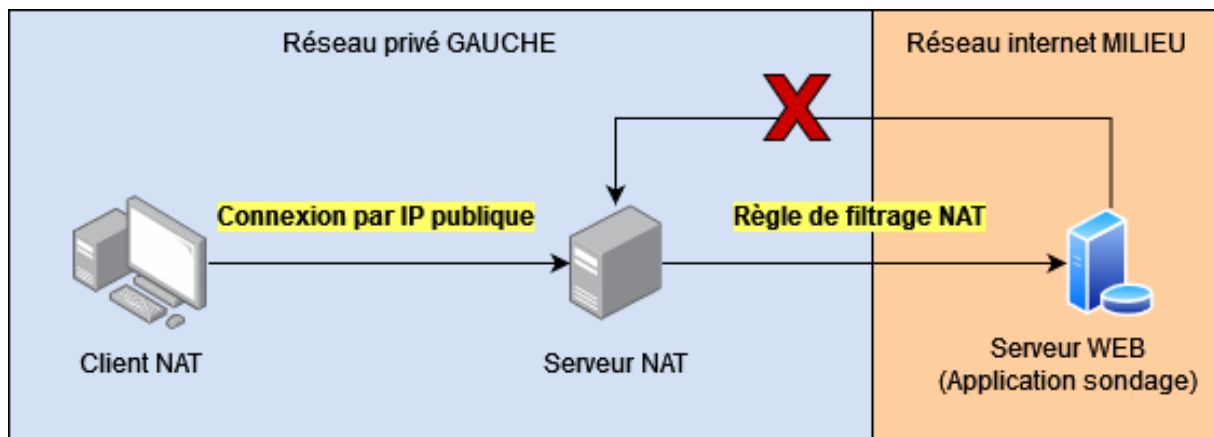
La cinquième machine a sensiblement le même fonctionnement que la troisième mais héberge cette fois-ci l'intranet de l'entreprise (qui est donc un autre serveur WEB). Il doit être sécurisé par un tunnel VPN que nous configurerons pour la machine n°4.

- Rôle : **Serveur WEB intranet**
- Nombre de cartes réseaux : 1
- Emplacement réseau : **Réseau entreprise DROITE**
- Adresse IPv4 : **192.168.3.20/24**
- Masque de sous-réseau : **255.255.255.0**
- Passerelle par défaut : **Aucune**

Le rôle de serveur WEB IIS doit être installé de la même manière que pour la machine précédente. Ce qui change est le contenu du serveur WEB. On placera dans le répertoire « wwwroot » les fichiers de l'intranet de l'entreprise.

6.4. Serveur NAT : machine n°2

La machine n°2 sert à sécuriser notre réseau avec du NAT. L'objectif est de permettre un accès au serveur WEB internet par une adresse publique et de protéger les accès venant de l'extérieur. Les clients du réseau privé pourront donc accéder à l'application WEB publique (sur le réseau du milieu) en utilisant l'adresse public du serveur NAT. Le serveur NAT redirigera les clients voulant s'y connecter vers le serveur WEB internet en appliquant la règle de filtrage.

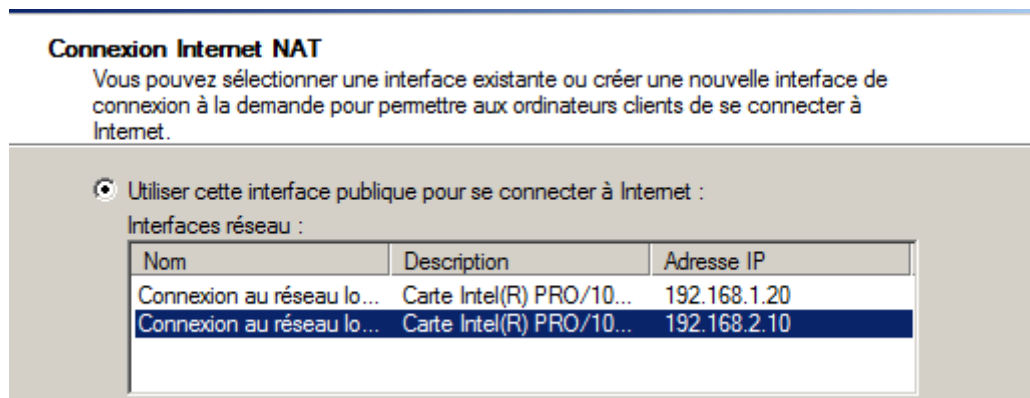


- Rôle : **Serveur WEB NAT + Serveur NAT**
- Nombre de cartes réseaux : 2
- Emplacement réseau : **Réseau privé GAUCHE + réseau internet MILIEU**
- Adresse IPv4 GAUCHE : **192.168.1.20/24**
- Adresse IPv4 MILIEU : **192.168.2.10/24**
- Masque de sous-réseau : **255.255.255.0**
- Passerelle par défaut : **Aucune**

Les rôles à installer sont ceux de serveur WEB IIS et routage et accès distant. Ils sont installables depuis le gestionnaire de serveur.



Afin d'activer le routage NAT, il faut se rendre sur la page « Routage et accès distant » de Windows Server. Nous configurons ainsi un routage de type « NAT » en sélectionnant bien la carte réseau correspondant au réseau internet comme interface publique. L'accès au serveur se fera ainsi bien du réseau privé (192.168.1.20) au réseau public (192.168.2.10) mais la route inverse ne sera pas possible.



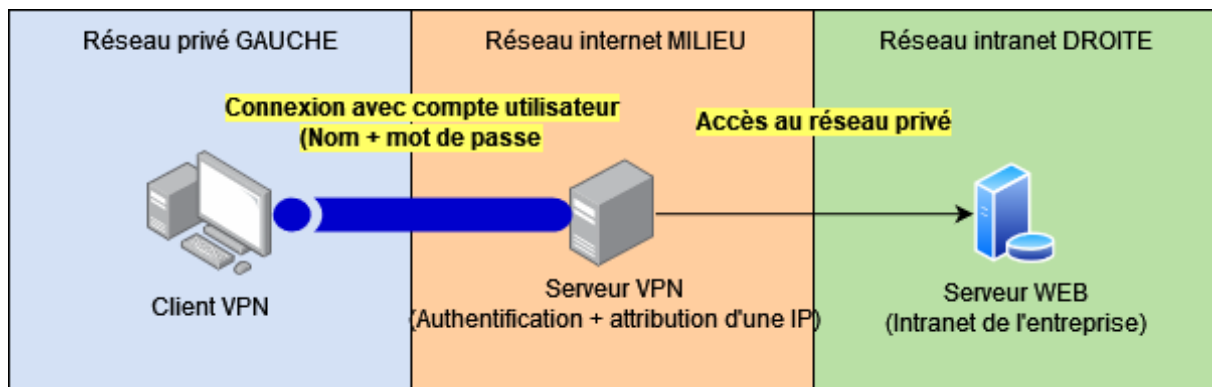
Une redirection de port est par la suite nécessaire pour pouvoir rediriger les connexions au serveur NAT vers notre application WEB. Pour arriver à ce résultat, il faut configurer (sur l'interface publique) un nouveau service de redirection au sein du routage NAT. Celui-ci utilise le protocole TCP et permet à tous les clients d'accéder au serveur WEB de l'application de sondage en utilisant un port spécifique de redirection. Il a été décidé d'utiliser le port 99 qui redirigera vers le port 80, correspondant au HTTP.

Enfin, pour rendre notre application WEB disponible depuis une adresse publique : Nous devons ouvrir les ports 80 et 99 dans l'interface de configuration du FAI (souvent accessible depuis 192.168.1.1 depuis le WEB). L'ouverture de ces ports et donc, la création de nouvelles règles de filtrage, diffère selon le point d'accès internet sur lequel est connecté le serveur WEB NAT.

Le routage NAT est ainsi bien mis en place sur notre machine. Les machines du réseau de gauche pourront se connecter au serveur du réseau du milieu en utilisant son adresse publique suivi du port 99 (IPPUBLIC:PORT). Du côté du réseau du milieu, aucune machine ne pourra accéder au réseau privé grâce au filtrage du serveur NAT.

6.5. Serveur VPN : machine n°4

Le serveur VPN que l'on doit mettre en place sur cette machine a pour but d'authentifier les clients VPN (qui seront prédéfinis côté serveur) en leur distribuant une adresse IP choisie parmi un pool d'adresses qui sera lui aussi prédéfinis. Tous les clients de ce serveur VPN seront ainsi autorisés à se connecter au serveur intranet du réseau de droite (accès par tunnel sécurisé). L'utilité recherchée est, dans un contexte réel, de permettre aux employés d'une entreprise d'avoir accès à l'intranet depuis leur réseau privé personnel s'ils s'authentifient en tant que clients VPN.



- Rôle : **Serveur WEB VPN + Serveur VPN**
- Nombre de cartes réseaux : 2
- Emplacement réseau : **Réseau internet MILIEU + réseau privé DROITE**
- Adresse IPv4 MILIEU : **192.168.2.30/24**
- Adresse IPv4 GAUCHE : **192.168.3.10/24**
- Masque de sous-réseau : **255.255.255.0**
- Passerelle par défaut : **Aucune**

Les rôles à installer sont les mêmes que pour la machine n°2, à avoir : un serveur WEB IIS et un service de routage et accès distant.

Dans la configuration du routage, nous devons cette fois-ci sélectionner un accès à distance par connexion VPN (en ne sélectionnant que l'option « VPN »). L'interface réseau à sélectionner est cette fois-ci le réseau de gauche, représentant l'intranet de l'entreprise.

Connexion VPN

Au moins une interface réseau doit être connectée à Internet afin de permettre aux clients VPN de se connecter à ce serveur.

Sélectionnez l'interface réseau qui connecte ce serveur à Internet.

Interfaces réseau :

Nom	Description	Adresse IP
Connexion au réseau local	Carte Intel(R) PRO/1000 ...	192.168.2.30
Connexion au réseau local 2	Carte Intel(R) PRO/1000 ...	192.168.3.10

La distribution des adresses IP aux clients VPN doit suivre un pool d'adresses défini. Lors de la configuration du routage, nous spécifierons le pool suivant (à adapter en fonction du nombre de clients VPN susceptibles de se connecter). Également, nous utilisons « routage et accès distant » pour l'authentification et non un serveur RADIUS.

Assignation de plages d'adresses
Vous pouvez spécifier les plages d'adresses que ce serveur utilisera pour assigner des adresses aux clients distants.

Entrez les plages d'adresses (pools statiques) que vous voulez utiliser. Ce serveur va attribuer toutes les adresses de la première plage d'adresses avant de continuer avec la suivante.

Plages d'adresses :

De	à	Numéro
200.200.200.1	200.200.200.50	50

Nouveau... Modifier... Supprimer

Une fois les services d'authentification et distribution d'adresses mis en place, il faut créer les différents profils utilisateurs devant se connecter au serveur VPN (les employés de l'entreprise qui doivent accéder à l'intranet depuis chez eux). Depuis la gestion de l'ordinateur, nous ajoutons autant d'utilisateurs que nécessaire dans *Utilisateurs et groupes locaux > Utilisateurs*. La création d'un client VPN se fait comme-ci :

Nouvel utilisateur

Nom d'utilisateur : clientVPN1

Nom complet :

Description :

Mot de passe :

Confirmer le mot de passe :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

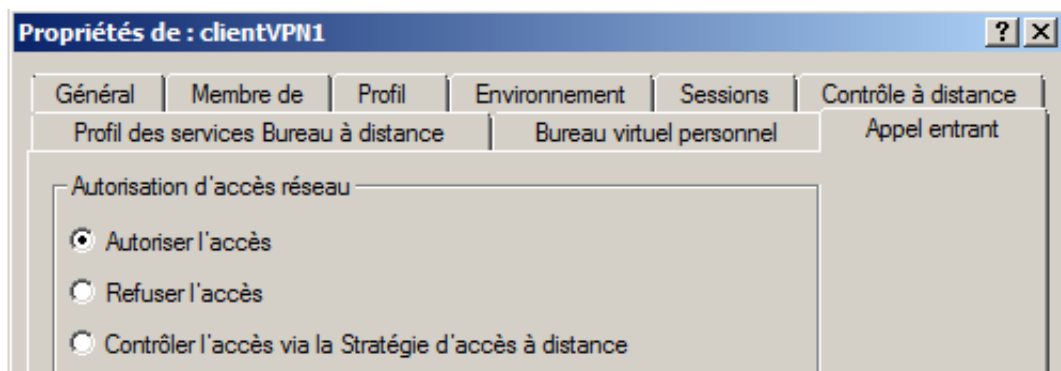
☒ L'utilisateur ne peut pas changer de mot de passe

☐ Le mot de passe n'expire jamais

☐ Le compte est désactivé

Aide Créer Fermer

Il est également nécessaire d'accorder l'accès au réseau en se rendant dans les propriétés de l'utilisateur nouvellement créé.



Le serveur VPN gérant l'authentification des clients VPN et la distribution des adresses IP est ainsi mis en place. Tout client se connectant à celui-ci à l'aide de son nom et de son mot de passe aura accès au serveur intranet de l'entreprise par l'IP 192.168.3.20.

6.6. Client final (NAT + VPN) : machine n°1 (User guide)

Maintenant que l'architecture finale est en place, nous devons tester si celle-ci est fonctionnelle en définissant un client NAT + VPN qui aura accès au serveur public contenant l'application de sondage ainsi qu'à l'intranet en s'authentifiant en tant que client VPN. Un serveur WEB privé va servir à tester que celui-ci n'est pas accessible depuis internet.

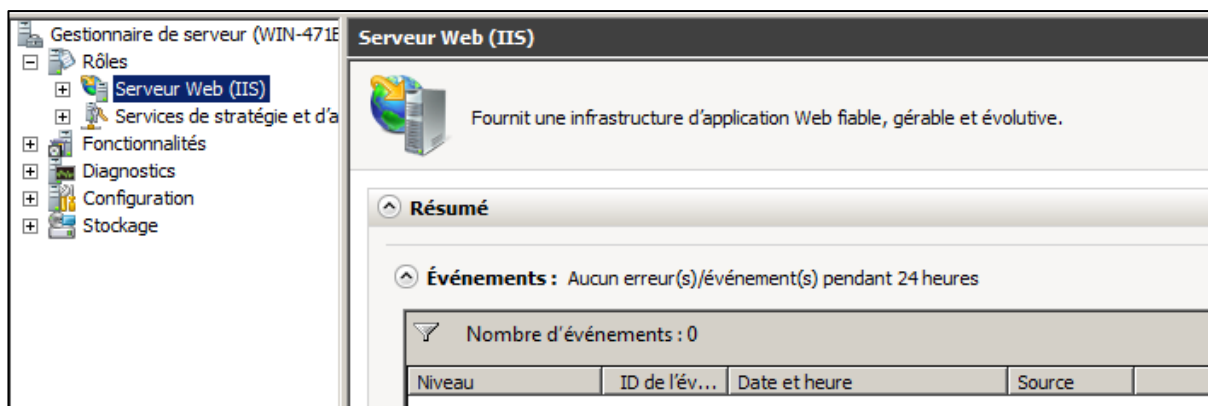
Cette partie sert de **guide d'installation** pour chaque utilisateur souhaitant accéder au à l'application WEB (depuis le NAT) ou à l'intranet de l'entreprise (en tant que client VPN).

- Rôle : **Client VPN + Client NAT + Serveur WEB privé**
- Nombre de cartes réseaux : 1
- Emplacement réseau : **Réseau privé GAUCHE**
- Adresse IPv4 GAUCHE : **192.168.1.10/24**
- Masque de sous-réseau : **255.255.255.0**
- Passerelle par défaut : **192.168.2.10/24**

Contrairement aux serveurs mis en place, le client peut se connecter à l'internet/intranet de notre architecture **avec un système d'exploitation Windows autre que Windows Server**. Dans notre cas de figure, étant donné que nous voulons lui attribuer le rôle de serveur WEB pour vérifier le fonctionnement du NAT, il sera également sous Windows Server 2012.

Pour accéder à l'application de sondage publique (via du NAT) :

Nous devons d'abord installer le rôle « Serveur WEB IIS » comme dans toutes les autres machines configurées. Celui-ci nous servira à vérifier que la machine n°3 (sur le réseau du milieu) ne peut bel et bien pas accéder à notre client (sur le réseau privé) grâce au NAT. Autrement (pour un cas concret), cette étape n'est pas obligatoire.

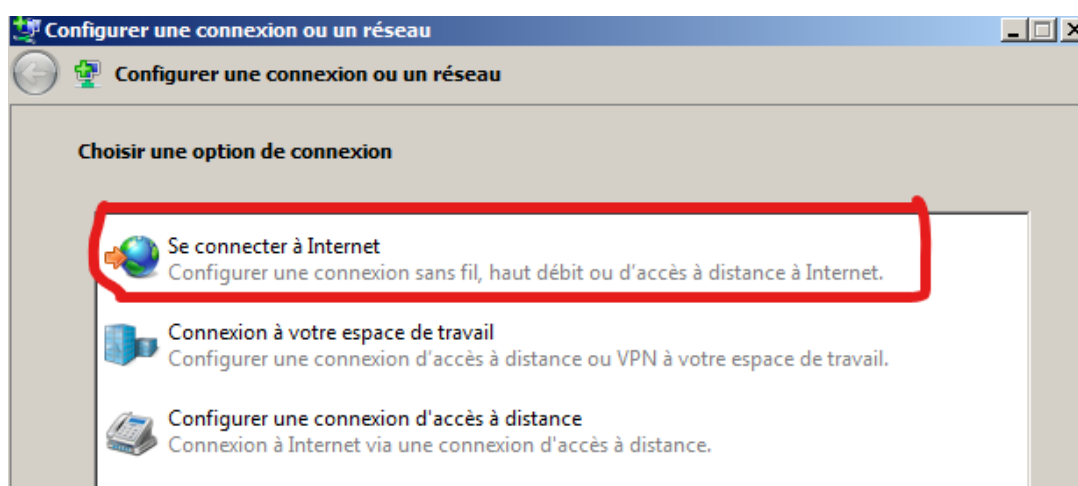


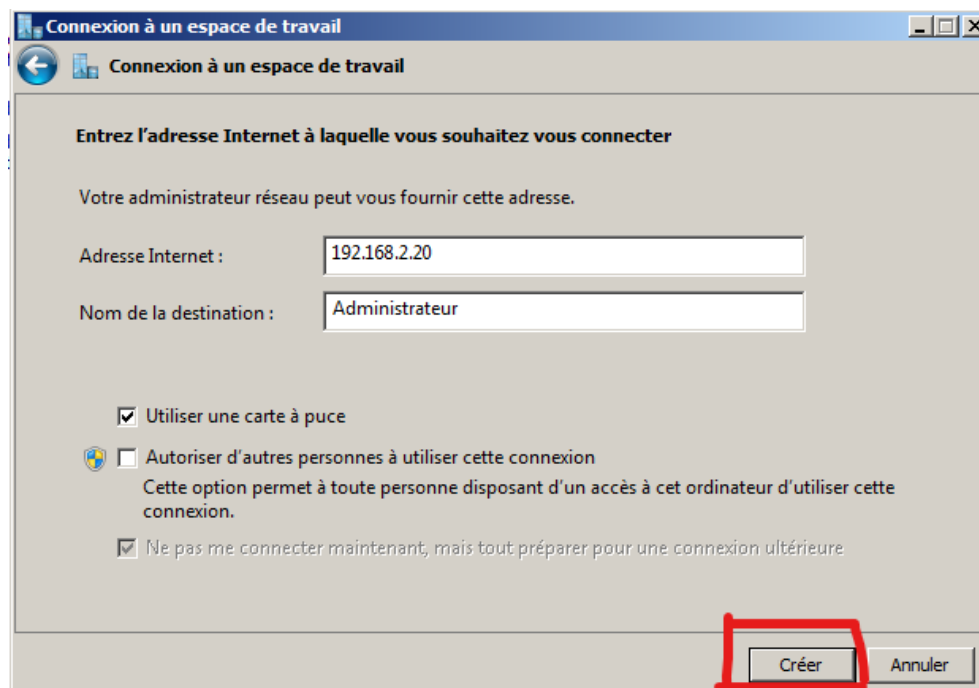
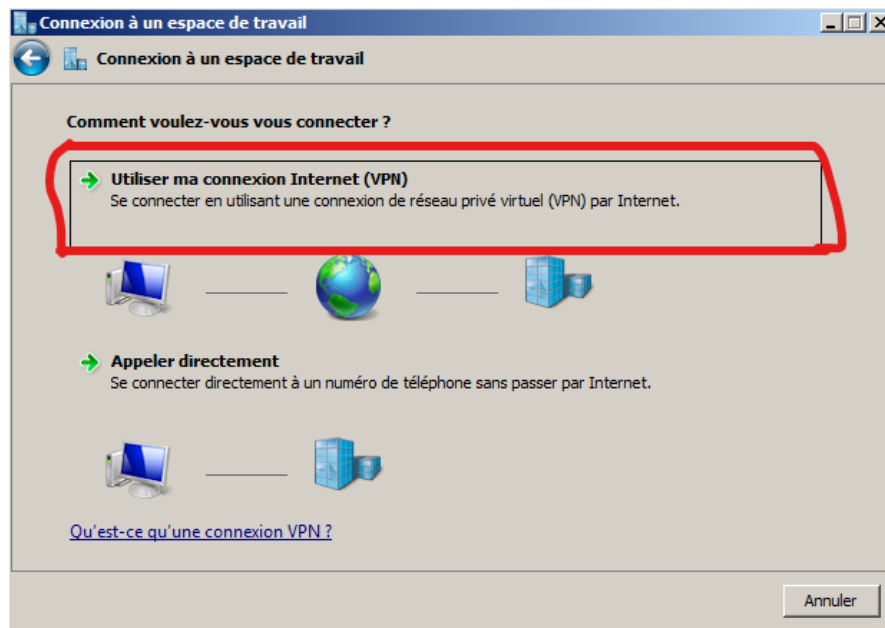
Le client, appartenant au réseau de GAUCHE, doit utiliser l'adresse IP publique de la machine n°2 qui contient le serveur NET et une redirection de port vers l'application.

Le client final peut ainsi bien accéder à l'application WEB de sondage mise en place de manière sécurisée par l'adresse « IPUBLIQUEMILIEU:99 ». Les machines présentes sur le réseau internet du milieu ne peuvent bel et bien pas accéder aux clients du réseau privé.

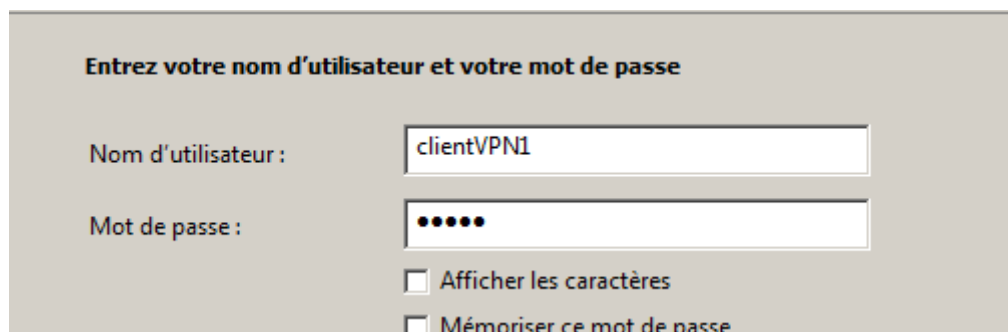
Pour accéder à l'intranet de l'entreprise (via un VPN) :

Si le client est un employé de l'entreprise voulant accéder à l'intranet de celle-ci, il possède un profil utilisateur VPN dans la machine n°4. Il doit, pour cela, configurer une nouvelle connexion à un espace de travail depuis le centre réseau et partage de Windows et suivre les étapes ci-dessous :





Enfin, l'employé rentre son nom d'utilisateur et mot de passe VPN qui lui ont été fournis.



La connexion étant prête, le client n'a plus qu'à se connecter à celle-ci depuis le centre réseau et partage.



Le client a ainsi accès à l'intranet de l'entreprise de manière sécurisée en passant par un tunnel VPN assuré par la machine n°4. L'application WEB est désormais hébergée et sécurisée par du NAT accessible depuis une adresse publique.

6.7. Tableau récapitulatif de l'architecture

Machine	Réseau	Adresse IP GAUCHE	Adresse IP MILIEU	Adresse IP DROITE	Passerelle par défaut
Machine n°1	Privé	192.168.1.10	X	X	192.168.2.10
Machine n°2	Privé + Internet	192.168.1.20	192.168.2.10	X	X
Machine n°3	Internet	X	192.168.2.20	X	192.168.3.10
Machine n°4	Internet + Intranet	X	192.168.2.30	192.168.3.10	X
Machine n°5	Intranet	X	X	192.168.3.20	X

7. F.A.Q sécurité & maintenance

Cette F.A.Q a pour but de fournir les informations nécessaires à la maintenance de l'installation expliquée précédemment.

- Comment se prémunir d'une intrusion sur la base de données publique ?
 - ➔ Il est important d'effectuer régulièrement des sauvegardes de données sur le serveur WEB du réseau du milieu. Si une intrusion se produit, il sera toujours possible d'en connaître la nature depuis les journaux système. Il est très important de choisir un mot de passe robuste pour l'accès administrateur de phpMyAdmin.
- Que faire si un problème de routage survient durant l'utilisation de l'architecture ?
 - ➔ Si un problème de routage est rencontré, il faut tout d'abord vérifier l'installation physique (dans le cas où rien n'a été changé dans la configuration des routes des machines 2 et 4) au niveau des VLANs et surtout de l'accès à internet du serveur WEB du milieu. Sinon, vérifier la configuration de chacune des machines manuellement en suivant la notice d'installation rédigée.
- Que faire si un employé utilisant de VPN oublie son mot de passe utilisateur lors de la connexion à celui-ci ?
 - ➔ Le profil utilisateur de l'employé doit être supprimé puis recréé au niveau de la machine n°4 qui joue le rôle de serveur VPN.
- Un niveau de sécurité supérieur peut-il être appliqué au serveur WEB public hébergeant l'application de sondage ?
 - ➔ Oui. Il serait judicieux de générer et utiliser un certificat SSL en questionnant une autorité de certification (des programmes tels que certbot le font très simplement). Cela permettra de faire passer le site en HTTPS, ce qui est un gage de confiance auprès des clients sur leurs navigateurs.
- Comment sécuriser le serveur VPN de la machine n°4 ?
 - ➔ Pour assurer un niveau de sécurité supérieur à l'avenir, il sera possible de remplacer le système d'authentification VPN de Windows Server par un service de tunneling plus moderne et sécurisé tel que IPSec, OpenVPN ou WireGuard. Ces services garantissent une sécurité contre les attaques de force brute.
- Comment sécuriser le serveur WEB public face aux attaques DDoS ?
 - ➔ Pour se protéger contre les attaques DDoS, vous pouvez mettre en place des pare-feux avec des fonctionnalités de détection et de prévention des attaques DDoS, utiliser des services anti-DDoS externes (CloudFlare), configurer des seuils de trafic pour bloquer les requêtes suspectes.

8. Synthèse globale du projet

Pour conclure sur cette SAE, nous avons appris énormément de notions utiles et surtout manipulé la plupart de ce que nous avons vu autant en cours de développement WEB et SQL qu'en cours de sécurité réseaux. Ce qui nous a le plus plu était la partie sécurité de l'application car nous n'avions jamais été confronté à un type de projet comme celui-ci. La mise en place d'un service de VPN pour assurer l'accès sécurisé à un intranet nous a paru très instructif au vu du parcours d'étude et des projets de poursuite d'étude que nous avons envisagés.

Cette SAE étant abouti, elle servira de preuve sur nos GitHub et LinkedIn respectif que nous sommes capables de réaliser un développement d'application côté client et serveur mais également d'assurer la sécurité des services proposés.