TD 11 – Environnement WIFI

Attaque en DDoS et Réponse avec un équipement de répartition de charge

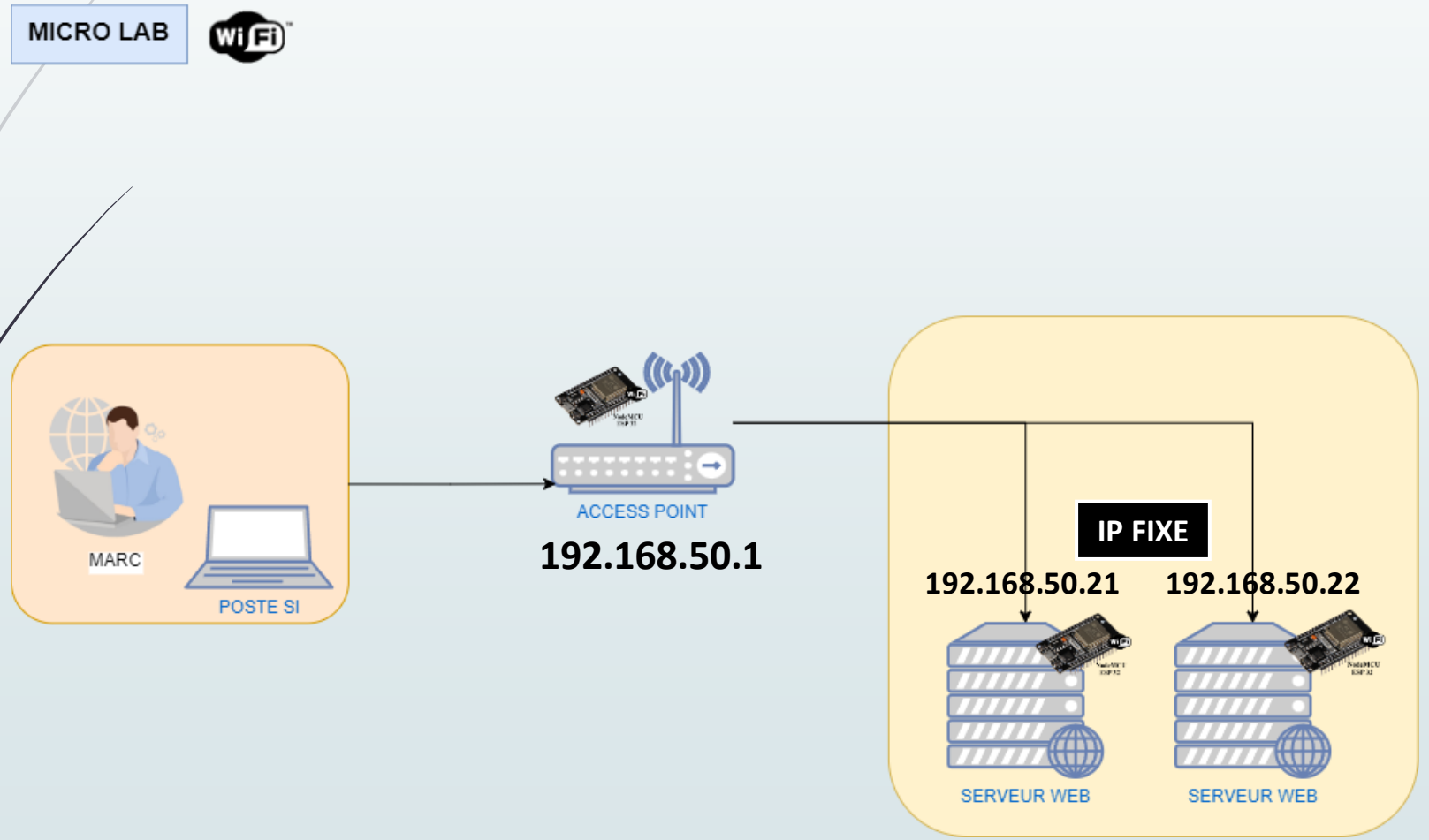
Marc est un ingénieur architecte sur le SI du micro lab et dispose d'un Lan réalisé avec des microcontrôleurs ESP32 fournissant un point d'accès wifi et de deux serveurs web de micro-services (La page Web affichera les caractéristiques du système, du réseau et sa charge mise à jour à chaque demande)

Travail :

- ❑ Mettre en place un point d'accès Wifi sur ESP32
- ❑ Mettre en place deux serveurs Web sur des ESP32

TD 11 – Environnement ESP32

Attaque en DDoS et Réponse avec un équipement de répartition de charge



TD 11 – Environnement WIFI

Attaque en DDoS et Réponse avec un équipement de répartition de charge

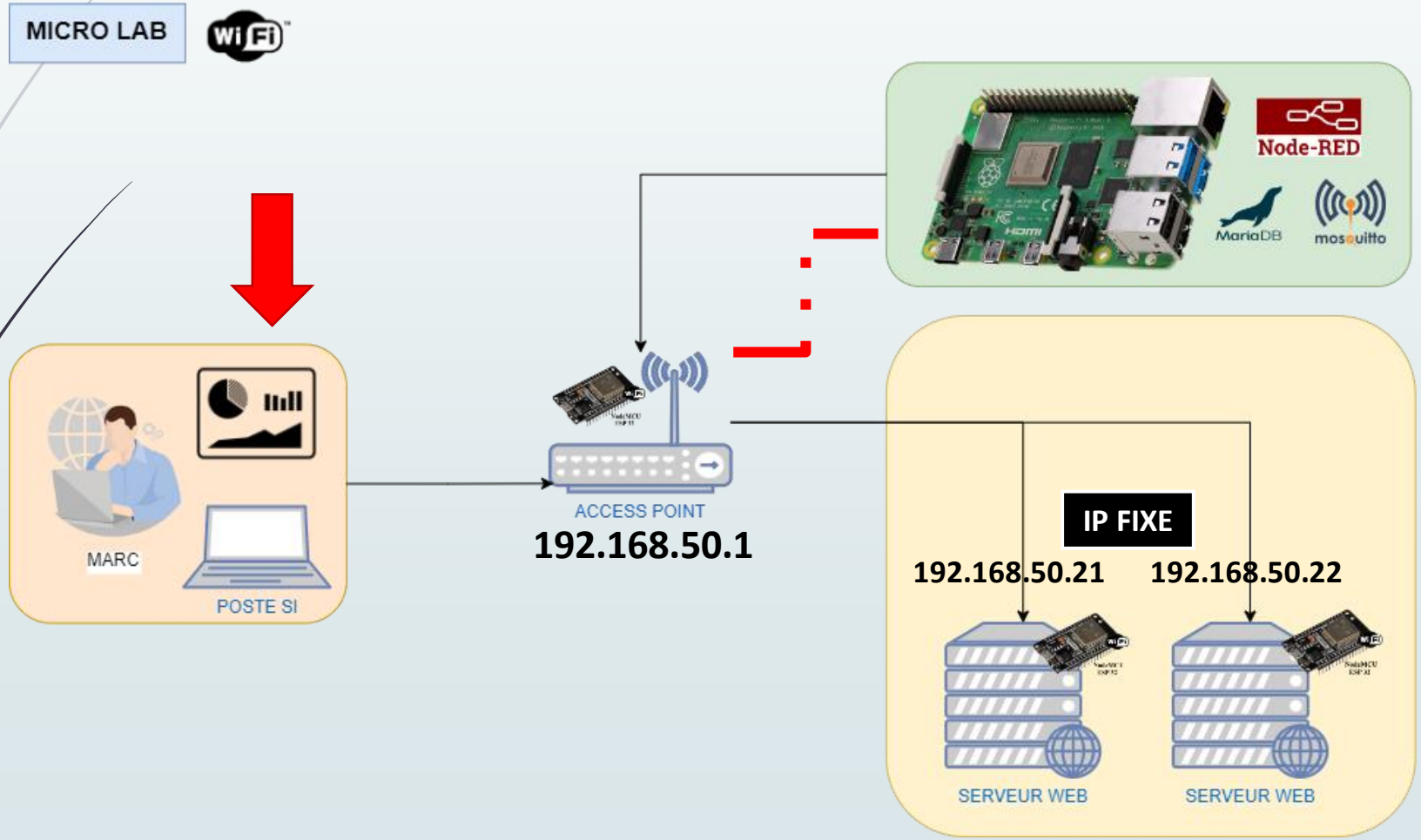
Marc intègre un serveur Node-Red/Mosquito/MySQL pour se fabriquer un Dashboard lui permettant de superviser les services qu'il souhaite déployer. La base MySQL possède une table avec le couple M@C adresse et Nom de machine, les données publiées via MQTT par le point d'accès sont enregistrées toutes les 5 secondes permettant la mise à jour des informations sur le Dashboard.

Travail :

- ❑ Mettre en place un serveur Node-Red/Mosquito/MySQL sur un Raspberry PI qui sera intégré au Lan
- ❑ Toutes les 5 secondes le point d'accès publie la liste des adresses IP/M@C connectées qui seront stocké dans la base de données et envoyé au Dashboard
- ❑ Le serveur Node-Red affiche la liste actualisée des unités connectés en Wifi

TD 11 – Environnement ESP32

Attaque en DDoS et Réponse avec un équipement de répartition de charge



TD 11 – Environnement WIFI

Attaque en DDoS et Réponse avec un équipement de répartition de charge

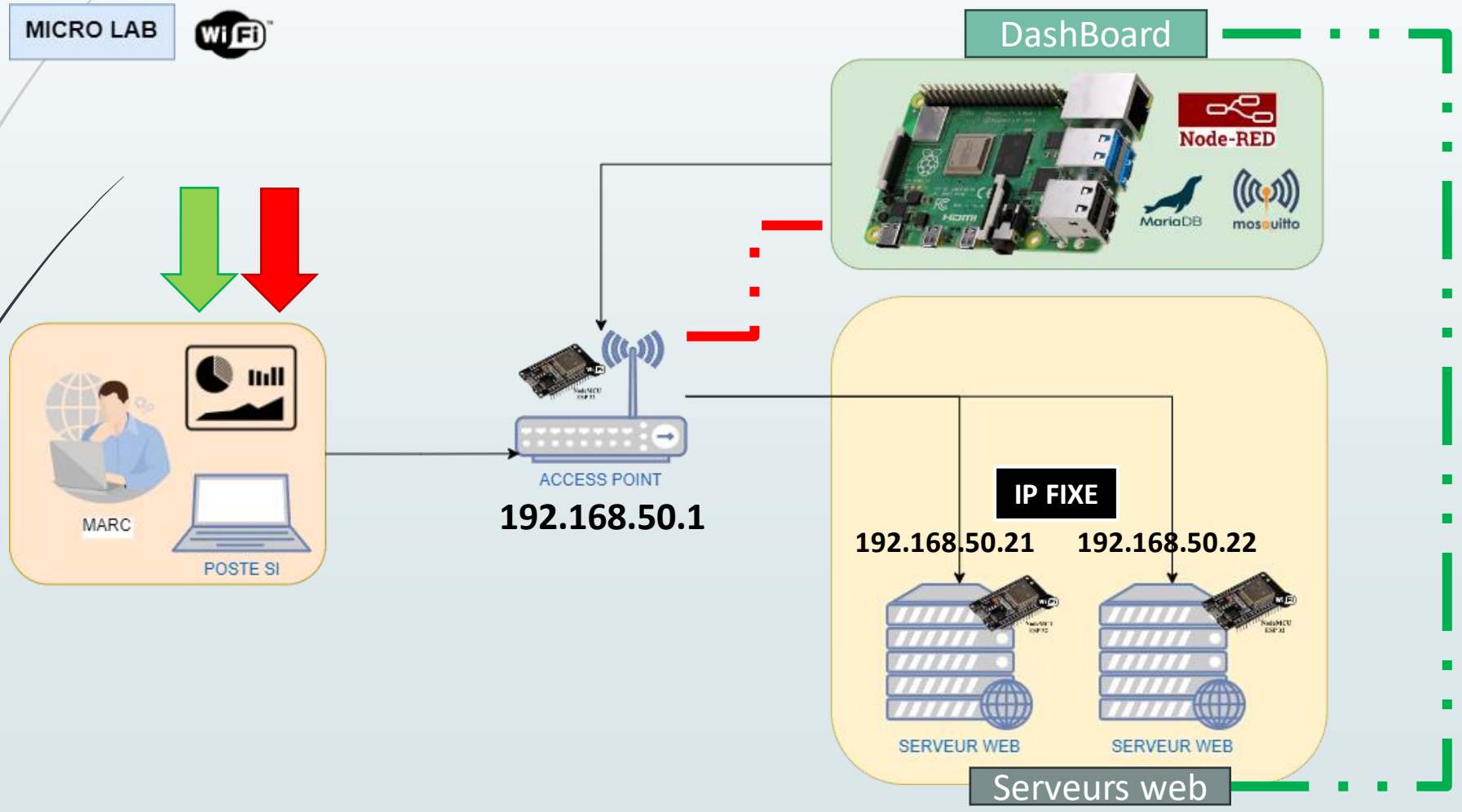
Marc souhaite journaliser les connexions des serveurs web, ces derniers publient une trame de log horodatée avec l'adresse IP du client, sa charge actualisée, sa mémoire disponible .

Travail :

- ❑ Mettre en place la journalisation sur les serveurs Web (serveur01 et serveur02)
- ❑ Transmettre la trame {json} lors d'une nouvelle connexion client au broker MQTT dans un topic « serveur01/Charge »
- ❑ Transmettre toutes les 3 secondes la charge actualisée du serveur au broker MQTT dans un topic « serveur01/trame »
- ❑ Enregistrer les trames sur le serveur
- ❑ Lister sur le Dashboard les 30 derniers évènements des deux serveurs dans deux listes séparées

TD 11 – Environnement ESP32

Attaque en DDoS et Réponse avec un équipement de répartition de charge



TD 11 – Environnement WIFI

Attaque en DDoS et Réponse avec un équipement de répartition de charge

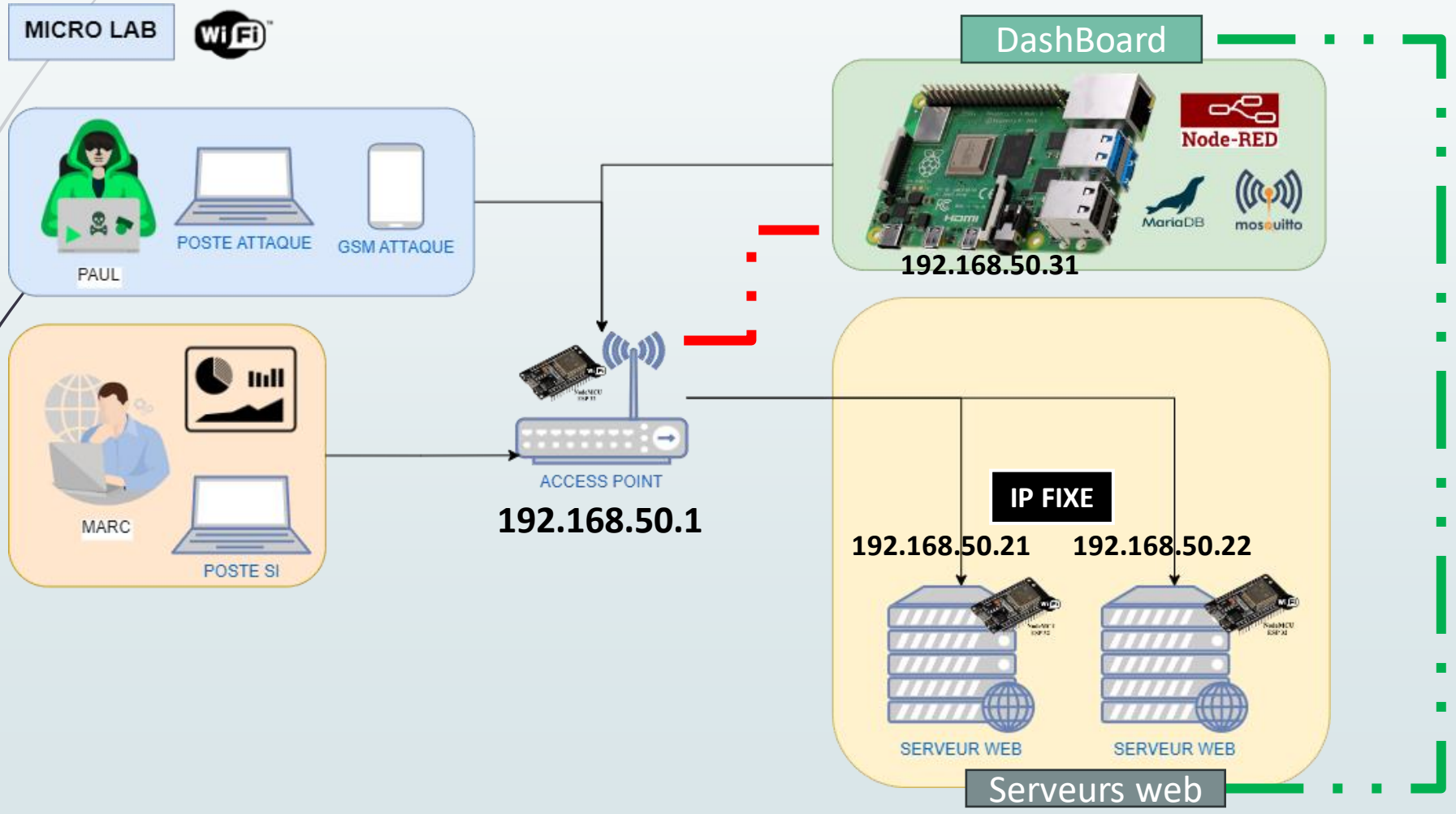
Paul pentester travaillant avec **Marc** a pour mission d'étudier la charge maximum d'un serveur web afin de tester sa résilience à une attaque en Déni de service distribué.

Travail :

- ❑ Concevoir en python en script d'attaque réalisant cette mission sur le serveur web 1 adresse 192.168.50.21
- ❑ Mesurer la charge MAX à l'aide des Topic « serveur01/Charge » supporté par ce serveur lui permettant d'assurer son service

TD 11 – Environnement ESP32

Attaque en DDoS et Réponse avec un équipement de répartition de charge



TD 11 – Environnement WIFI

Attaque en DDoS et Réponse avec un équipement de répartition de charge

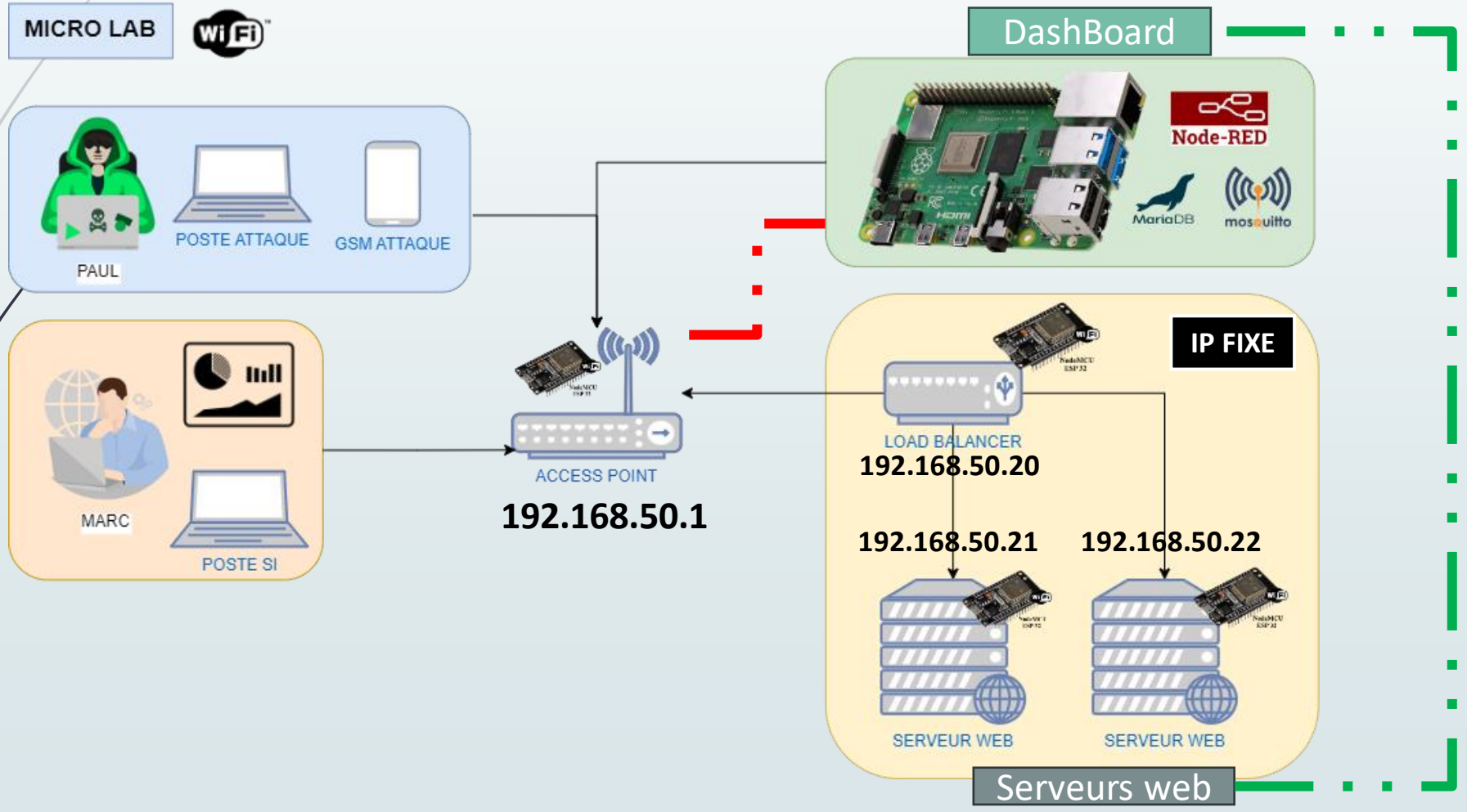
Le résultat des tests montre la nécessité de mettre en place un répartiteur de charge. **Paul** et **Marc** décide de le mettre en place à l'aide d'un ESP32.

Travail :

- ❑ Mettre en place le répartiteur de charge
- ❑ S'abonner au flux des charges des serveurs et extraire la charge des serveurs
- ❑ Effectuer les tests de monter en charge (Graphique)
- ❑ Répartir les charges entre les serveurs à l'aide du script de Paul

TD 11 – Environnement ESP32

Attaque en DDoS et Réponse avec un équipement de répartition de charge



TD 11 – Environnement WIFI

Attaque en DDoS et Réponse avec un équipement de répartition de charge

Etienne est pentester sénior dans le microlab, il dispose de multiples dispositifs pour compromettre l'environnement. Son travail est de découvrir les faiblesses de l'environnement global pour empêcher l'exécution des services.

Travail :

- ❑ Rechercher d'autres moyens pour affaiblir les performances de notre environnement que l'on pourra observer sur le Dashboard

Marc réfléchi à un mécanisme de survie pour les serveurs web leur permettant de s'autoprotéger face à une attaque DDoS leur permettant d'alerter.

Travail :

- ❑ Proposer et mettre en place votre solution

TD 11 – Environnement ESP32

Attaque en DDoS et Réponse avec un équipement de répartition de charge