SAE 5.01 – Architecture Wi-Fi sécurisée multi-sites

BUT3 R&T pa. Cyber & pa. ROM (PN 2022) semestre 5

Patrice BRINGUIER

Présentation du projet et de l'évaluation

Formation : BUT 3 R&T – Ressource VCYS501 « Concevoir »

Contexte : projet de déploiement Wi-Fi sécurisé pour une chaîne de salles de sport

Organisation : travail en groupes de trois

Évaluation finale :

- QCM + question ouverte (contrôle écrit) (/13)
- Note sur le dépôt GitLab (/7)

Objectif de la séance : comprendre le « film » complet de la SAE

Contexte professionnel

Chaîne de salles de sport multi-sites

Plusieurs salles de sport, réparties sur différents sites

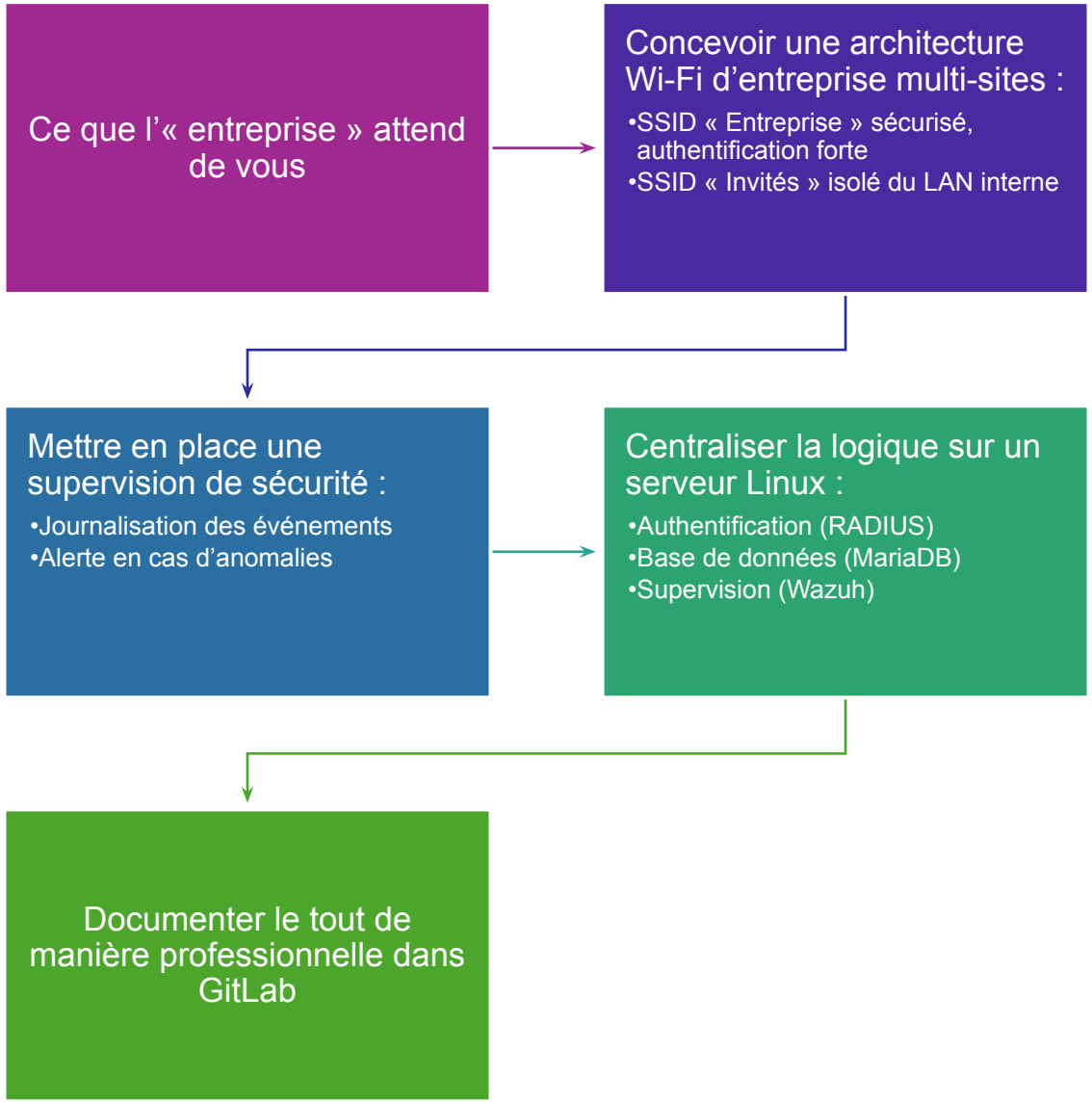
Sur chaque site :

- Routeur 4G TP-Link TL-MR100 pour l'accès Internet
- Besoin de Wi-Fi pour le personnel
- Besoin de Wi-Fi pour les clients (invités)

Problème actuel :

- Wi-Fi hétérogène, peu sécurisé
- Pas de supervision de sécurité centralisée
- Pas de vision globale sur les journaux (logs)

Mission confiée



Calendrier et échéances

À noter dès maintenant

Rendu du dépôt GitLab :

- Date limite : lundi 19 janvier 2026 à 7h (heure de Paris)
- Le dépôt au moment de cette échéance fait foi pour la note /7

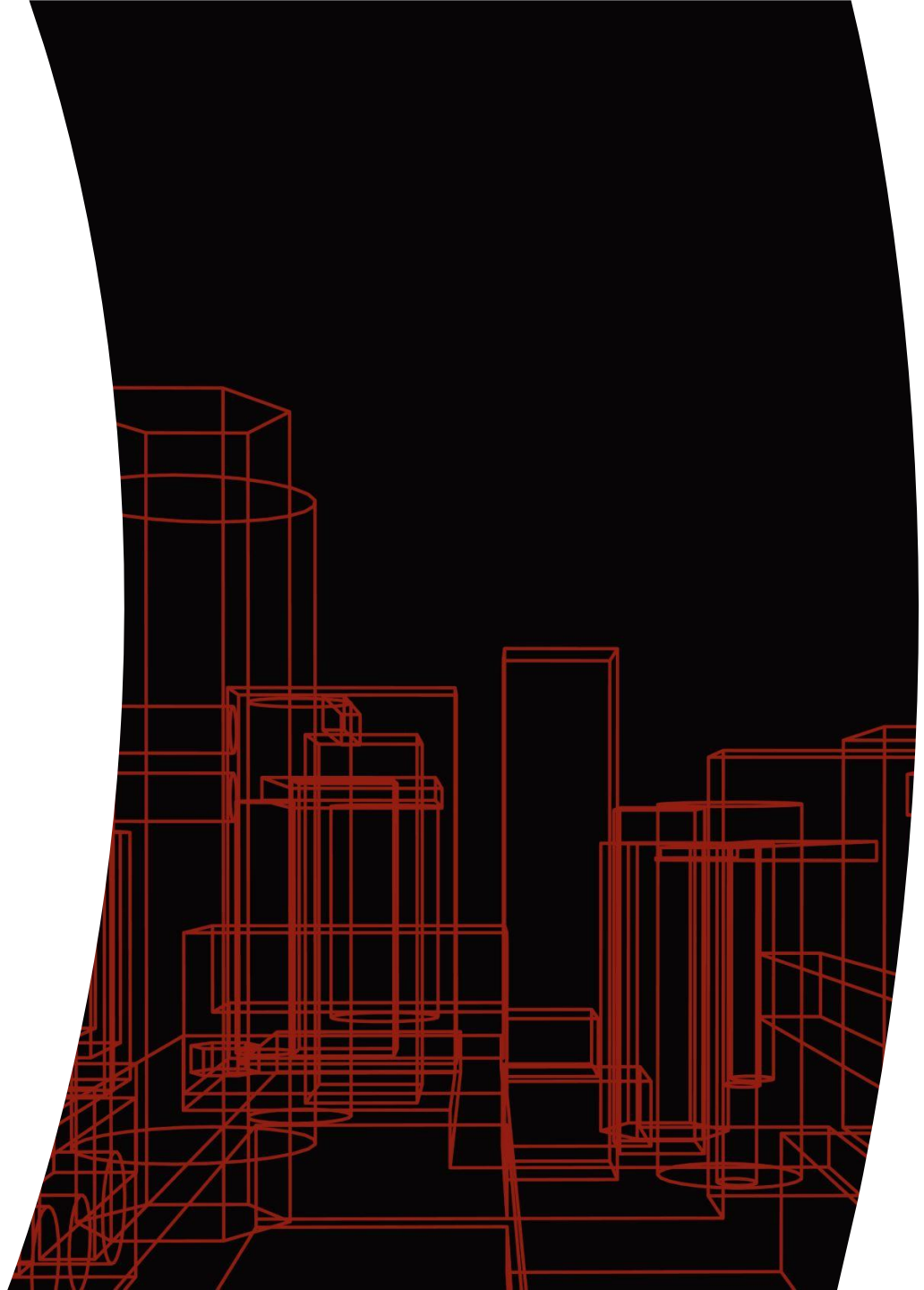
Contrôle sur table (QCM + question ouverte) :

- Date : mardi 10 février 2026
- Durée : 90 minutes
- Aucun document, aucun appareil électronique

Conseil :

- Ne pas attendre la dernière semaine pour compléter la documentation
- Mettre à jour le GitLab au fil de l'eau (journal de bord, captures, scripts, etc.)

Rappel : méthodologie de projet



Les grandes étapes classiques

1. Analyse du besoin
   - Comprendre le contexte, les contraintes, les objectifs
   - Identifier les acteurs, les usages, les risques principaux
2. Conception
   - Proposer une architecture cohérente
   - Choisir les technologies et les solutions
   - Préparer un planning (diagramme de Gantt)
3. Réalisation et tests
   - Mettre en place les services (RADIUS, Wi-Fi, Wazuh…)
   - Tester chaque brique, corriger, itérer
4. Documentation et bilan
   - Rédiger et maintenir les fichiers Markdown
   - Documenter les preuves (captures, logs, scripts)
   - Faire une synthèse claire (utile pour la question ouverte)

Diagramme de Gantt

Pour organiser les tâches et les rôles de chacun

- Le diagramme de Gantt sert à :
  - Lister les tâches du projet
  - Visualiser leur ordre dans le temps
  - Voir quelles tâches peuvent être faites en parallèle
- Dans cette SAE, il permet surtout de :
  - Découper le projet en étapes claires :
    - analyse, architecture, RADIUS, Wi-Fi invités, Wazuh, hardening, documentation…
  - Attribuer les rôles dans le groupe de trois :
    - qui prend le lead sur quelle partie ?
    - qui vérifie, relit, teste ?
- Éviter que tout soit fait dans l'urgence à la fin
- Attendu dans « diagramme-gantt.md » :
  - Liste des tâches, dates approximatives, responsable(s)
  - Une vision lisible de l'avancement prévu du projet

Rôle des étudiant·es

Vous êtes l'équipe technique du projet

- Travail en groupes de trois :
  - Répartition claire des tâches techniques
  - Coordination sur GitLab (commits, branches, issues)
- Attendu : raisonnement structuré et rigoureux :
  - Comprendre les besoins
  - Faire des choix techniques justifiés
  - Tester, documenter, corriger
- Votre dépôt GitLab → le dossier technique du projet et sa mémoire

Vue d’ensemble de l’architecture

Briques principales

- Côté réseau :
  - Routeur 4G MR100 par site
  - SSID « Entreprise » (Wi-Fi interne)
  - SSID « Invités » (Wi-Fi isolé
- Côté serveur central Linux :
  - FreeRADIUS + MariaDB pour l’authentification 802.1X
  - Wazuh pour la supervision de sécurité
  - Services complémentaires (PHP, scripts, etc.)
- Côté sécurité :
  - WPA2-Enterprise, PEAP-MSCHAPv2
  - Hardening du serveur Linux (SSH, pare-feu…)
  - Journalisation et corrélation des événements

Wi-Fi Entreprise

802.1X, PEAP-MSCHAPv2 et FreeRADIUS

- SSID « Entreprise » :
  - Authentification 802.1X (WPA2-Enterprise)
  - Méthode PEAP-MSCHAPv2 :
    - Certificat serveur sur RADIUS
    - Pas de certificat client (plus simple à déployer)
- FreeRADIUS + MariaDB :
  - Comptes utilisateurs stockés dans une base SQL
  - Contrôle des droits d’accès via RADIUS
- Intérêt pédagogique :
  - Comprendre un schéma réaliste d’entreprise
  - Manipuler un vrai serveur RADIUS

Réseau Wi-Fi Invités

Isolement et preuves techniques

- SSID « Invités » :
  - Fournir un accès Internet aux clients
  - Ne jamais laisser accéder le LAN interne
- MR100 :
  - Fonctionnalités « Guest Network »
  - À tester et vérifier (ne pas faire confiance à l'interface marketing)
- Attendu dans le projet :
  - Prouver l'isolement avec des outils :
    - ping, nmap, tcpdump, etc.
    - Documenter l'isolement dans « isolement-wifi.md »
    - Fournir des captures dans « captures/ »

Supervision de sécurité

Wazuh et journaux (logs)

- Rôle de Wazuh :
  - Centraliser les journaux des serveurs et équipements
  - Corréler les événements, déclencher des alertes
- Journaux collectés :
  - Logs du serveur Linux
  - Logs envoyés par le MR100 (via syslog)
- Attendus :
  - Configuration de la collecte (fichiers dans « wazuh/ »)
  - Documentation dans « wazuh-supervision.md »
  - Exemples de journaux / alertes dans « captures/ »

Hardening du serveur Linux

Sécurisation de la machine centrale

- Objectif : réduire la surface d'attaque
- Mesures typiques :
  - SSH par clé uniquement, désactivation du login « root »
  - Pare-feu (ufw, nftables) :
    - RADIUS, syslog, SSH, Wazuh… uniquement
  - Mises à jour, journaux, services minimaux
- Document à produire :
  - « hardening-linux.md » :
    - Liste des mesures
    - Commandes principales
    - Justifications

Dépôt GitLab – vue globale

Arborescence de référence

Arborescence exemple :

```
•sae501-2026-groupeXX/
•|-- docs/
•|   |-- dossier-architecture.md
•|   |-- analyse-ebios.md
•|   |-- hardening-linux.md
•|   |-- journal-de-bord.md
•|   |-- diagramme-gantt.md
•|   |-- wazuh-supervision.md
•|   `-- isolement-wifi.md
•|-- radius/
•|-- php-admin/
•|-- wazuh/
•|-- scripts/
•|-- tests/
•|-- captures/
•|-- README.md
•`-- .gitignore
```

Tout ce qui est important doit être dans ce dépôt

Lisible par une personne externe (tuteur, client, auditeur)

Documentation Markdown

Dossier « docs/ »

dossier-architecture.md :

- Schéma global, flux, choix techniques

analyse-ebios.md :

- Actifs, menaces, scénarios, mesures

hardening-linux.md :

- Mesures de durcissement appliquées

wazuh-supervision.md :

- Ce qui est supervisé, comment, exemples

isolement-wifi.md :

- Résultats des tests d’isolement des invité

journal-de-bord.md :

- Historique des décisions, essais, erreurs, correction

diagramme-gantt.md :

- Gestion du temps et des tâches

Journal de bord & diagramme de Gantt

Mémoire et pilotage du projet

journal-de-bord.md :

- Date / tâche / résultat / problème / décision
- Rédigé au fil de l'eau, pas à la fin

diagramme-gantt.md :

- Planification des phases :
  - Analyse, conception
  - Mise en place RADIUS
  - Supervision Wazuh
  - Hardening
  - Documentation & finition

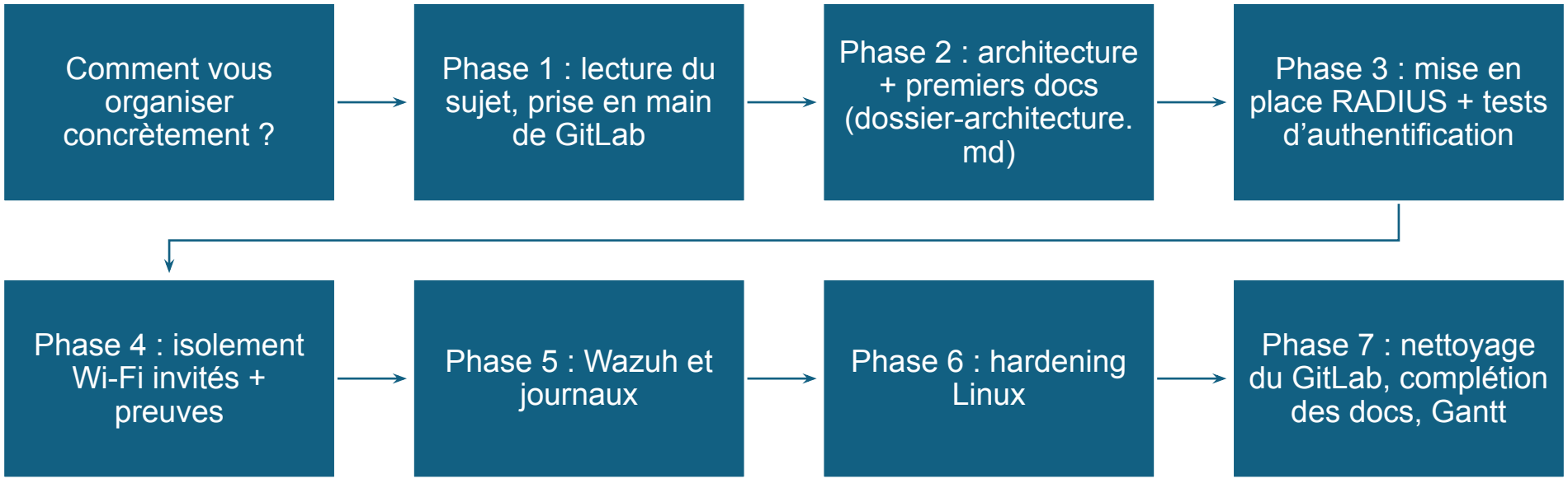
Attribution des rôles dans le groupe :

- qui est responsable de quelle tâche ?
- qui vérifie, relit, teste ?

Intérêt :

- Montrer que le projet est piloté
- Servir de support pour la question ouverte de synthèse

Méthodologie de travail



Important :

- Commits fréquents, messages clairs
- Travail en groupe de trois réellement coordonné

Évaluation – Contrôle écrit

QCM + Question ouverte

- QCM (20 questions) :
  - Tirées au hasard dans une banque de 30
- Notation : 0,5 point par bonne réponse → /10
- Porte sur :
  - Wi-Fi, RADIUS, PEAP-MSCHAPv2, isolement, Wazuh
  - Hardening, logs, Git, documentation…
- Question ouverte Q21 (/3) :
  - « Synthèse : concevoir et réaliser un projet technique complet de type déploiement Wi-Fi sécurisé multi-sites »
  - Demande de raconter :
    - Analyse des besoins
    - Architecture technique
    - Sécurité et supervision
    - Organisation du travail et documentation
- Date du contrôle sur table :
- Mardi 10 février 2026 (durée 90 minutes)

Évaluation – Note GitLab (/7)

Question réservée à l'enseignant·e

- Question Q22 : « Notation du Git (/7) »
- Le dépôt GitLab pris en compte est celui présent en ligne :
  - Le lundi 19 janvier 2026 à 7h
- Critères (non exhaustifs) :
  - Respect de l'arborescence attendue
  - Présence et qualité des documents Markdown
  - Propreté du dépôt (pas de fichiers parasites)
  - Commits réguliers, messages explicites
  - Cohérence entre documentation et réalité déployée
  - Présence de preuves (captures, logs, scripts, tests)
  - Niveau global professionnel (lisibilité, maintenabilité)
- Le dépôt GitLab compte vraiment dans la note finale

Ce qu’on attend de vous

En résumé

- Comprendre le contexte professionnel de la chaîne de salles de sport
- Construire une architecture Wi-Fi sécurisée multi-sites cohérente
- Mettre en place :
  - Authentification 802.1X (PEAP-MSCHAPv2, FreeRADIUS)
  - Isolement des invités avec preuves techniques
  - Supervision de sécurité (Wazuh + logs MR100)
  - Hardening du serveur Linux
- Produire un dépôt GitLab propre, documenté et traçable
- Être capable d’en faire la synthèse le jour du contrôle écrit

Questions / échanges

Avant de démarrer vraiment

- Questions sur :
  - Le contexte de la SAE ?
  - Les attentes techniques ?
  - L’organisation en groupes de trois ?
  - La notation (QCM, QO, Git) ?
- Note importante :
  - Plus vous documentez au fil de l’eau, plus l’examen final sera une mise en mots de ce que vous aurez déjà compris.