# AC31.01 – Concevoir un projet de réseau informatique d’une entreprise en intégrant les problématiques de haute disponibilité, de QoS, de sécurité et de supervision

# Contexte

Dans le cadre de la **SAE CTF** et de la **SAE cycle de vie d'un projet informatique**, il s'agit de concevoir un projet réseau en prenant en compte les contraintes de disponibilité, de qualité de service, de sécurité et de supervision.

* **SAE CTF** : Création d'un scénario immersif permettant aux participants d'explorer divers aspects de la cybersécurité, de l’OSINT et de l’analyse réseau dans un environnement ludique et pédagogique.
* **SAE cycle de vie d'un projet informatique** : Gestion complète d’un projet réseau depuis la conception jusqu’à l’implémentation, incluant la documentation et la supervision de l’infrastructure.

# Savoir mis en œuvre

* **Modélisation et conception d’architectures réseau** en respectant les contraintes d’entreprise.
* **Principes de la haute disponibilité** (redondance, load balancing, clustering).
* **Qualité de service (QoS)** : gestion de la priorité des flux réseau.
* **Sécurisation d’un réseau informatique** : segmentation, firewalling, VPN, gestion des accès.
* **Supervision réseau** avec des outils tels que Zabbix, Nagios, ou Prometheus.
* **Gestion du cycle de vie d'un projet informatique** : rédaction de cahiers des charges, planification et suivi des tâches.

# Savoir-faire mis en œuvre

* Définir une **architecture réseau** adaptée aux besoins métier.
* Mettre en place des **mécanismes de haute disponibilité** pour éviter les interruptions de service.
* Appliquer des **règles de QoS** pour garantir la fluidité du trafic réseau.
* Configurer des **politiques de sécurité réseau** adaptées aux contraintes de l’entreprise.
* Déployer des **outils de supervision** et interpréter les métriques pour anticiper les incidents.
* Documenter chaque étape du projet de manière rigoureuse et claire.

# Savoir-être mis en œuvre

* **Rigueur** dans la conception et l’implémentation des solutions réseau.
* **Esprit d’analyse** pour identifier les points critiques en termes de sécurité et de performance.
* **Collaboration** avec les différentes parties prenantes du projet (techniciens, administrateurs, clients).
* **Autonomie** dans la recherche et la mise en place de solutions techniques adaptées.
* **Capacité d’adaptation** face aux évolutions des besoins et aux contraintes techniques.

# Tâches réalisées et résultats SAE CTF

Conception et mise en place d'un scénario CTF intégrant des aspects réseau et cybersécurité.

Déploiement d’un environnement avec des machines virtuelles simulant une infrastructure réelle.

Création de challenges sur la supervision réseau, la sécurité et la haute disponibilité.

Mise en place de logs et de monitoring pour analyser les tentatives d’attaques des participants.

**Résultat** : Un CTF engageant qui permet aux participants de comprendre concrètement les problématiques réseau et cybersécurité.

# SAE cycle de vie d'un projet informatique

Conception d’un réseau d’entreprise intégrant **redondance et supervision**.

Mise en place d’une **stratégie de QoS** adaptée aux flux critiques.

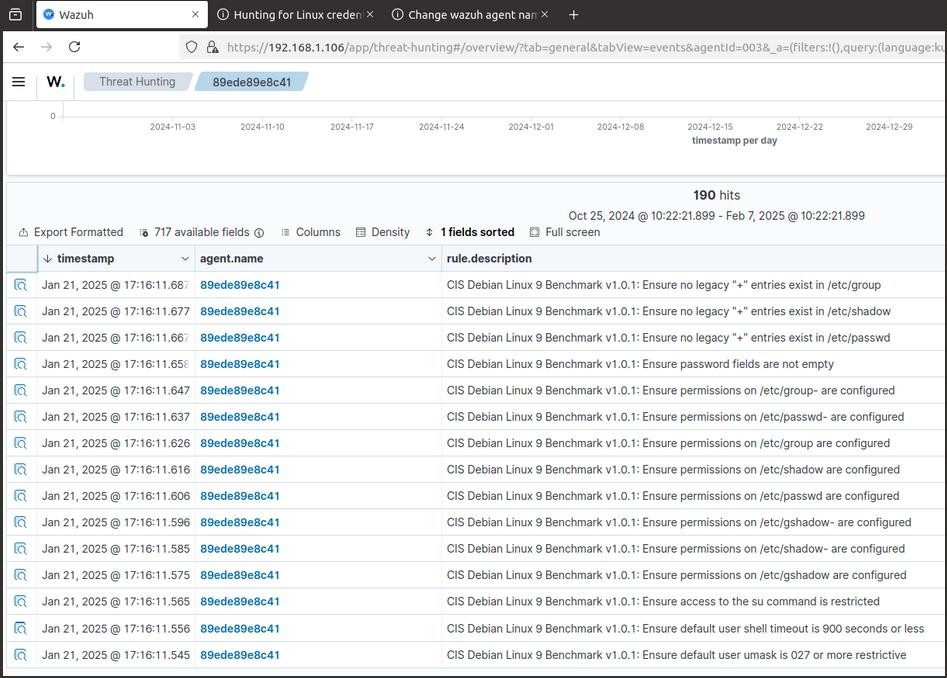
Sécurisation du réseau avec firewall, VLAN et gestion des droits d’accès.

Rédaction d’un dossier de conception détaillant les choix techniques et leur justification.

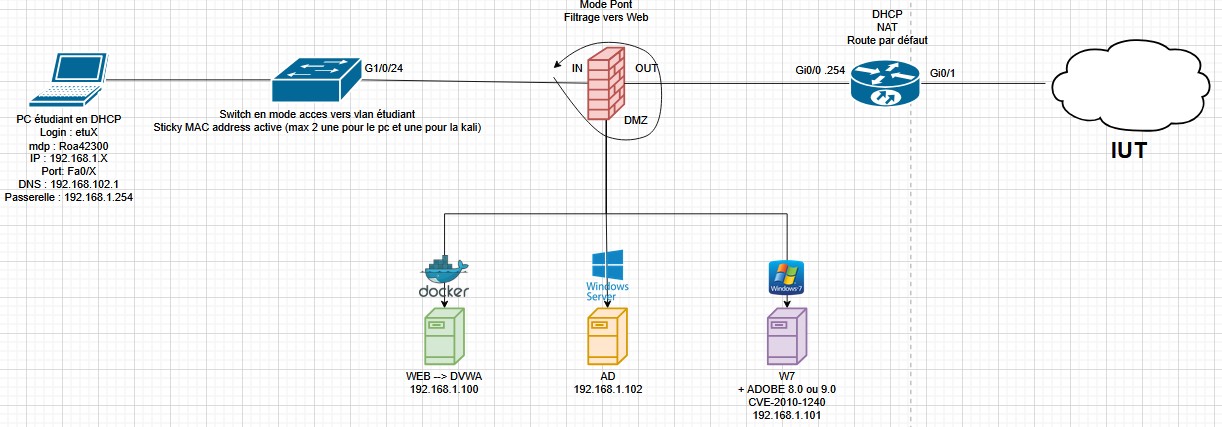
**Résultat** : Un projet réseau documenté et fonctionnel, garantissant une haute disponibilité et une sécurité renforcée.

Capture d’écran :

Wazuh sécurité et supervision, remonté d’alerte lors du ctf :



Ansible permet de justifier les demandes de haute disponibilité : [voir mon github](https://github.com/Holo-Prism/SAE5.02)  Schématisation pour la conception des infrastructures :



Analyse réflexive :

Dans le cadre des SAE CTF et cycle de vie d’un projet informatique, j’ai conçu un réseau intégrant haute disponibilité, QoS, sécurité et supervision. Le CTF a permis d’explorer la cybersécurité via des challenges sur un réseau simulé, supervisé avec Wazuh. En parallèle, j’ai conçu une architecture réseau avec redondance, segmentation et QoS, documentée dans un dossier technique. Cette approche garantit performance et sécurité, mais pourrait être optimisée par une automatisation accrue et une diversification des scénarios, en s’appuyant sur les retours d’expérience des participants.